Implantació d'un sistema de gestió d'esdeveniments i informació de seguretat per una organització

Marc Cama Hidalgo
Grau de Tecnologies de la Telecomunicació

José Manuel Castillo Pedrosa

6 de Gener de 2019

FITXA DEL TREBALL FINAL

Títol del treball:	*Implantació d'un sistema de gestió d'esdeveniments i informació de seguretat per una organització*
Nom de l'autor:	*Marc Cama Hidalgo*
Nom del consultor:	*José Manuel Castillo Pedrosa*
Data de lliurament (mm/aaaa):	*01/2019*
Àrea del Treball Final:	*Administració de xarxes i sistemes operatius*
Titulació:	*Grau de Tecnologies de la Telecomunicació*

Resum del Treball (màxim 250 paraules):

Donat l'actual paradigma de processament massiu de dades i incidents de seguretat on la gestió és cada cop més complexa, i donat el número d'actius d'una organització, es proposa la integració d'una plataforma de gestió d'esdeveniments i informació de seguretat.

Per el projecte SIEM(Security Information and Event Management) s'ha escollit la plataforma ElasticSearch-LogStash-Kibana (ELK) una solució Open Source, que permet la gestió de logs, a aquesta plataforma s'afegirà Wazuh una solució de gestió i creació d'esdeveniments de seguretat que monitoritza les activitats d'una màquina i crea esdeveniments segons la seva gravetat per després poder prendre mesures de protecció. Per poder incorporar els esdeveniments de xarxa, s'inclourà Logstash Netflow, un col·lector, normalitzador i visualitzador de fluxos de xarxa que permet tindre un històric del tràfic i permetrà fer un anàlisis detallat dels possibles incidents de seguretat.

El resultat potencial que s'espera és crear una plataforma que agrupi totes les possibles eines de seguretat que ens ajudin a la resolució de problemes en un sistema centralitzat, fàcil de controlar i ens permeti tindre la capacitat de visualitzar esdeveniments de seguretat, realitzar anàlisi forense d'incidents i avançar-nos a possibles amenaces.

Abstract (in English, 250 words or less):

Given the current paradigm of mass data processing and security incidents where the management is more complex every time, and given the number of assets of an organization, the integration of a security information and event management platform is proposed.

For the SIEM project the platform ElasticSearch-LogStash-Kibana (ELK) has been chosen. An open source solution which allows the management of logs. Wazuh will be added to this plattform: a management and creation of security events solution which monitorizes the activities from a machine and creates events according to their importance to be able to prevent them later.

In order to incorporate the events, Logstash Netflow will be added: a collector, normalizer and visualizer of net flow which allows to have a history for the traffic and will allow to make a detailed analysis of the possible security incidents.

The potential result is to create a platform which gathers all the possible security tools which might help to the resolution of problems in a centralized system, easy to control and which allows us to be able to visualize security events, make forensic analysis of incidents, and to anticipate possible threats.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Actualment la seguretat és un dels principals productes i serveis de mercat que més creix, a 2018 va augmentar la seva inversió en un 12.4% aconseguint 114.000 milions de dòlars, per a 2019 segons Gartner s'espera que les inversions en seguretat creixin un 8.7% arribant als 124.00 milions.

Els principals factors d'aquestes inversions són els creixents riscos de seguretat per a les empreses, necessitats comercials, canvis a la industria i la privacitat de les dades.

Degut a que el nivell d'atacs e intrusions als sistemes ha crescut en molt poc temps i a la complexitat dels mateixos, els sistemes com Antivirus, Firewalls, IPS o IDS no són suficients per poder mitigar tots els atacs que es produeixen, a més al tindre tants sistemes descentralitzats és molt costos correlar i fer el 'matching' de tots els esdeveniments.

Per aquets motius s'ha escollit com a projecte de final de grau una solució on un sistema de gestió d'esdeveniments i informació de seguretat centralitzat analitzarà i crearà esdeveniments automàticament, es podrà fer el seguiment forense d'un incident i es recol·lectaran totes les dades dels sistemes que monitoritzem.

1.2 Objectius del Treball

L'objectiu principal del projecte és crear una solució de gestió esdeveniments i seguretat utilitzant diferents eines Open Source. Aquesta solució tindrà dos tipus de configuració, la primera serà per una petita o mitjana empresa on la arquitectura del SIEM serà d'una màquina amb tota la solució implementada i la segona constarà d'una arquitectura distribuïda on cada component base per tindre un SIEM en funcionament estarà instal·lat en diferents màquines. Una vegada la solució funcioni, aconseguirem que s'estableixi una convergència entre totes les eines i així poder visualitzar en una sola plataforma la generació d'alertes de seguretat, emmagatzematge/indexació de logs i fluxos de xarxa. Amb això s'aconseguirà que la resolució de problemes per una empresa sigui molt més àgil i automatitzada.

Els objectius parcials i les seves tasques associades serien les següents:

- Gestió d'actius e indicadors - Es configurà l'enviament d'indicadors per part dels actius i es revisaran/configuraran els indicadors generats per les diferents eines amb l'objectiu de poder processar i visualitzar tots els esdeveniments generats d'una manera clara i fàcil.

- Estadístiques de rendiment - Una vegada fet el filtre dels indicadors es trauran estadístiques del tipus d'alertes i notificacions que es generen del actius controlats i es generaran informes de control, per determinar els requeriments del hardware per a que la plataforma funcioni correctament depenent dels actius a monitoritzar.

- Generació d'alertes – Es realitzarà una fase de test on es posaran a prova les diferents regles d'alertes, com detecció d'atacs de força bruta, intrusions i modificació d'arxius als servidors, etc.

- Prevenció – Es revisaran les alertes i informació proporcionada per la plataforma i s'establirà quines millores es poden aplicar a la organització i quines avantatges obtenim d'aquest sistema.

- Gestió – S'establirà el circuit de la gestió d'incidents, i es definiran les tasques que ha de seguir una organització una vegada tingui una plataforma de gestió de la seguretat en producció.

- Comparació de solucions – Es farà un petit estudi dels costos d'una solució i un altre i es determinarà quina és la millor arquitectura depenent de la volumetria de les dades i la capacitat econòmica de cada organització.

1.3 Enfocament i mètode seguit

L'estratègia a seguir alhora de realitzar el treball és conèixer les característiques entre una arquitectura d'un sol node o una arquitectura distribuïda per un sistema de gestió d'esdeveniments i seguretat. El mètode que es seguirà serà veure els costos d'instal·lació/configuració entre les dues arquitectures i determinar que ens pot aportar la solució si som una organització que ens plantegem la inclusió d'una tecnologia com aquesta que no requereix de llicenciament anual.

1.4 Planificació del Treball

Tot seguit es mostra el diagrama de Gantt on estan totes les tasques definides per la realització del projecte.

Nombre de tarea	Duraci	Comienzo	Fin	Prec
Planificació TFG	**13 días**	**mié 19/09/18**	**vie 05/10/18**	
Elecció i descripcció del projecte	8 días	mié 19/09/18	vie 28/09/18	
Planificació	5 días	lun 01/10/18	vie 05/10/18	2
Entrega PAC1	0 días	vie 05/10/18	vie 05/10/18	3
Redacció de la Memòria	**65 días**	**lun 08/10/18**	**dom 06/01/19**	**4**
Anàlisi de mercat i cerca de característiques	10 días	lun 08/10/18	vie 19/10/18	
Entorn Laboratori	**15 días**	**lun 22/10/18**	**vie 09/11/18**	**6**
Instal·lació màquines virtuals	1 día	lun 22/10/18	lun 22/10/18	
Instal·lació eines SIEM	3 días	mar 23/10/18	jue 25/10/18	8
Configuració Eines SIEM	6 días	vie 26/10/18	vie 02/11/18	9
Test de les aplicacions	1 día	lun 05/11/18	lun 05/11/18	10
Documentació	14 días	mar 23/10/18	vie 09/11/18	
Entrega PAC2	0 días	vie 09/11/18	vie 09/11/18	
Entorn Real	**13 días**	**lun 12/11/18**	**mié 28/11/18**	**7**
Preparació entorn	5 días	lun 12/11/18	vie 16/11/18	
Configuració eines SIEM	8 días	lun 19/11/18	mié 28/11/18	15
Documentació	13 días	lun 12/11/18	mié 28/11/18	
Exemple d'ús	**11 días**	**jue 29/11/18**	**jue 13/12/18**	**14**
Definició flux de treball	2 días	jue 29/11/18	vie 30/11/18	
Definició pla de gestió de riscos	4 días	lun 03/12/18	jue 06/12/18	19
Test d'intrusions	3 días	vie 07/12/18	mar 11/12/18	20
Ús de la eina	2 días	mié 12/12/18	jue 13/12/18	21
Entrega PAC3	0 días	vie 14/12/18	vie 14/12/18	
Preparació entrega final	**16 días**	**vie 14/12/18**	**dom 06/01/19**	**23**
Perfilar i completar apartats marcats	4 días	vie 14/12/18	mié 19/12/18	
Definició de les conclusions	1 día	jue 20/12/18	jue 20/12/18	25
Redacció del Glosari i Bibliografia	1 día	jue 20/12/18	jue 20/12/18	25
Preparació Power Point	10 días	vie 21/12/18	jue 03/01/19	27
Entrega Final	0 días	dom 06/01/19	dom 06/01/19	

Il·lustració 1 - Diagrama de Gantt

1.5 Breu descripció dels altres capítols de la memòria

Per a la nostra memòria s'ha optat per la següent estructura de capítols.

Introducció: Es definiran els objectius del projecte, un resum explicant el perquè s'ha triat aquest tema i una petita planificació.

Estat de l'art: Es farà un petit estudi de les diferents solucions que hi ha al mercat per comparar-la amb la nostre i poder incorporar possibles millores ja que la solució escollida és Open Source i ens permet integrar més funcions de les definides per defecte.

Proposta: A la proposta és on està el gruix del projecte, aquí tenim diferents subapartats.

Primer tenim un resum de la nostra solució amb totes les característiques i funcions que ens permet la plataforma SIEM.

Per altre banda tenim els passos que s'han seguit per instal·lar i configurar tant en l'entorn de laboratori, com l'entorn real de tota la plataforma de gestió d'esdeveniments i seguretat.

Com a tercer apartat tenim l'exemple d'ús, que consta de la definició del procés alhora de gestionar un incident de seguretat, la definició per la realització d'un anàlisi de risc, una petita demostració de com detectar diferents atacs i com protegir-nos dels mateixos, una petita demostració d'us de la plataforma i monitorització i finalment la valoració econòmica del que ens costaria la implementació de les dues arquitectures.

2. Estat de l'art

Per preparar la nostra proposta primer indagarem en les solucions de que disposa el mercat per donar cabuda a un projecte de gestió d'esdeveniments de seguretat i gestió de logs. Tot seguit farem una petita descripció de les eines més rellevants.

2.1 Splunk

Splunk és una solució de pagament que busca arribar a un mercat de grans empreses gracies al seu potencial per correlar i analitzar grans quantitats d'esdeveniments alhora. El seu punt fort és la escalabilitat horitzontal que ofereix, ja que el rendiment del motor de cerca segueix sent excel·lent tot i que el volum de dades sigui molt elevat. Donat al gran volum de clients amb diferents solucions ofereix gran compatibilitat amb la majoria de fabricats i dispositius. Per contra ens trobem amb un cost per llicencia força elevat, $173/GB per mes, encara que les màquines es poden obtenir per separat, únicament indiquen quins recursos per sistema operatiu i carrega es necessita.

Il·lustració 2 - Logo Splunk

Com ja em dit el punt fort de Splunk és la seva escalabilitat ja que el rendiment de les cercas no es veu agreujat per el gran volum de dades que es capaç de manipular, i això permet donar un valor afegit a la intel·ligència operacional, ja que treballan molt en la compatibilitat amb tot tipus de dispositius, que és el valor que se li treu a un SIEM, poder correlar tot tipus de logs i informació extra que li pugi arribar per poder treure conclusions que puguin beneficiar a la teva organització.

Un altre dels beneficis de Splunk empresarial són les solucions de que disposes, com Haddop Data Roll, que proporciona la opció de reduir els costos del emmagatzematge enviant els logs a un pool de dades on ens permet seguir fent cerques de dades, cosa que altres sistemes comprimeixen les dades però no les fan indexables amb el que no es possible realitzar l'explotació de les dades. A més gracies a que la plataforma de desenvolupament és de codi obert tenim la opció de crear les aplicacions personalitzades amb les funcions desitjades i després integrar-la amb la plataforma fent una solució totalment personalitzada als nostre interès.

Característiques destacades

- ✓ Indexació multifont
- ✓ Xifratge de dades
- ✓ Personalització de Splunk
- ✓ Escalabilitat
- ✓ Anàlisis automatitzat a temps real
- ✓ Solució al núvol

Punts dèbils

- ☒ Enfocat per grans empreses
- ☒ Utilització de servidors potents

2.2 Ossim (AlienVault)

En aquest cas tenim una solució mixta, la plataforma Ossim és OpenSource, amb el que la podem instal·lar en qualsevol servidor recomanat i no tindríem problema per funcionar, però només tindrem disponible la part de gestió d'esdeveniments de seguretat, analitzador de fluxos de xarxa, monitorització, i auditoria de servidors (OpenVAS), la part de gestió de logs i realització d'anàlisi forense és una part que te bloquejada i només es pot optar mitjançant llicencia. Aquesta solució va més dirigida a una petita/mitjana empresa que vulgui tindre una visualització de les alertes de seguretat dels seus servidors d'una manera centralitzada.

Il·lustració 3 - Logo OSSIM

Una de les característiques que fa a Ossim un SIEM molt valorat és la eina Open Threat Exchange (OTX) una plataforma que es connecta via API amb el nostre SIEM y que permet compartir totes les amenaces que s'hagin detectat en altres organitzacions i les emmagatzema a la base de dades classificant-les amb diferents nivells de reputació, per tant els usuaris de tot el mon és troben amb les direccions IP que han efectuat els atacs, les signatures del malware que han instal·lat, el comportament que ha tingut i una sèrie de dades que permeten a la resta d'usuaris poder avançar-se a les amenaces.

Com a solució de llicencia lliure és una de les més completes ja que ens permet fer descobriment de la xarxa per tindre identificats els actius amb els sistemes operatius i software que després s'explotarà mitjançant l'anàlisi de

vulnerabilitats, també ens proporciona eines d'integració de logs no estandarditzats per poder-los indexar al correlador o la possibilitats de crear alertes personalitzades on es podran realitzar accions proactives, com crear regles al Firewall corporatiu, notificar per correu als administradors o reiniciar serveis entre d'altres mesures.

Característiques destacades

- ✓ OTX
- ✓ Llicencia OpenSource
- ✓ Anàlisis de vulnerabilitats
- ✓ Alertes reactives

Punts dèbils

- ☒ Enfocat per petites/mitjanes empreses
- ☒ No disposa de plataforma al núvol
- ☒ Utilització de servidors potents
- ☒ No disposa d'arquitectura distribuïda

2.3 Prelude

Com a tercera solució tenim Prelude una eina totalment Open Source que recopila informació de diferents sensors correlant i gestionant alertes. Aquesta eina es converteix en una solució SIEM gracies a la seva cohesió amb les diferents eines de llicencia lliure que ho fan possible com Snort, Prewikka, suricata, OSSEC, auditd, etc. Aquesta pot ser una bona eina de gestió per mitjanes i petites empreses que necessitin d'una gestió d'esdeveniments de seguretat i auditoria dels seus sistemes a cost de llicenciament zero, encara que te la opció d'arquitectura distribuïda per poder manegar grans volums de dades la eina encara no està del tot madura com per donar el salt a una gran empresa.

Il·lustració 4 - Logo Prelude

La particularitat de Prelude és les peticions que pots fer als desenvolupadors per a que millorin la eina, el seu sistema es recollir les peticions dels seus clients ajuntar-les i quan estiguin completes treuen la versió definitiva. És una bona manera de millorar en base a les necessitats dels clients i així fer un bon sistema per consolidar als teus usuaris, i no acabin marxant a altres solucions.

Il·lustració 5 - Procés de peticions

Un altre de les característiques que fan a Prelude una bona solució és la integració amb software de tercers, ja que treballa per integrar solucions que ja estan consolidades en el mercat per fer la seva eina millor això fa que els esforços siguin menors i la evolució de la eina sigui molt més rapida i potent.

Característiques destacades

- ✓ Llicencia OpenSource
- ✓ Anàlisis de vulnerabilitats
- ✓ Alertes reactives
- ✓ Arquitectura distribuïda
- ✓ 3rd Party Agents

Punts dèbils

- ☒ No disposa de plataforma al núvol
- ☒ Enfocat per petites/mitjanes empreses
- ☒ Utilització de servidors potents

2.4 Conclusions

Com podem veure al mercat hi ha diferents solucions disponibles tant de llicenciament gratuït com de pagament, per una gran organització que tingui una infraestructura crítica la opció de llicencia lliure no és la millor opció ja que tindre una solució de pagament et dona les avantatges d'una total integració en la teva infraestructura, alertes al dia, i suport d'un tercer especialitzat que pugi resoldre les incidència que pugin sorgir. Com podem veure en el següent quadre de Gartner, Splunk, IBM i LogRhythm són els líders en el mercat, tant per lideratge a nivell de número de vendes, número d'usuaris i expansió del producte com per visionat de tendència tecnològica i necessitats. Respecte al quadre de Gartner també veiem com les solucions Prelude o ELK-Wazuh no apareixen en cap punt del quadrant, això és degut a que aquestes dues solucions no són SIEMs purs sinó que aprofiten diferents eines de tercers i les integren al seu ecosistema convertint-se així en una solució totalment completa i funcional.

Il·lustració 6 - Gartner SIEM 2017

Si analitzem les solucions descrites en els punts anterior i les comparem amb la solució de ELK+Wazuh, podem veure com s'assimila molt a la solució de Prelude ja que és de llicenciament lliure i una part de la integració és a partir d'eines de tercers, però si analitzem el perquè s'ha escollit aquesta solució podem veure com ELK+Wazuh és una solució molt madura, començant perquè ELK és un correlador de logs dels més potents del mercat amb gran recorregut i junt a Wazuh fan una solució molt estable i potent, capaç de manegar grans volums de dades mitjançant els diferents sensors i el tractament de les dades que es reben abans de la indexació. A més aquestes dues solucions tenen disponible suport professional amb el que tens una garantia de qualitat i de que cada dia es treballa per a que la eina segueixi millorant cosa que et dona confiança de que no s'implantarà una eina a la teva organització que es quedarà obsoleta en un temps i es tingui que optar per una nova solució.

<u>Característiques destacades</u>

- ✓ Llicencia OpenSource
- ✓ Anàlisis de vulnerabilitats
- ✓ Alertes reactives
- ✓ Arquitectura distribuïda
- ✓ Suport Professional
- ✓ Xifratge de dades
- ✓ Escalabilitat

Punts dèbils

- ☒ No disposa de plataforma al núvol
- ☒ Utilització de servidors potents

3. Proposta

3.1 Resum

Tot seguit exposarem les característiques de les eines que instal·larem a la solució proposada, per determinar quin potencial té.

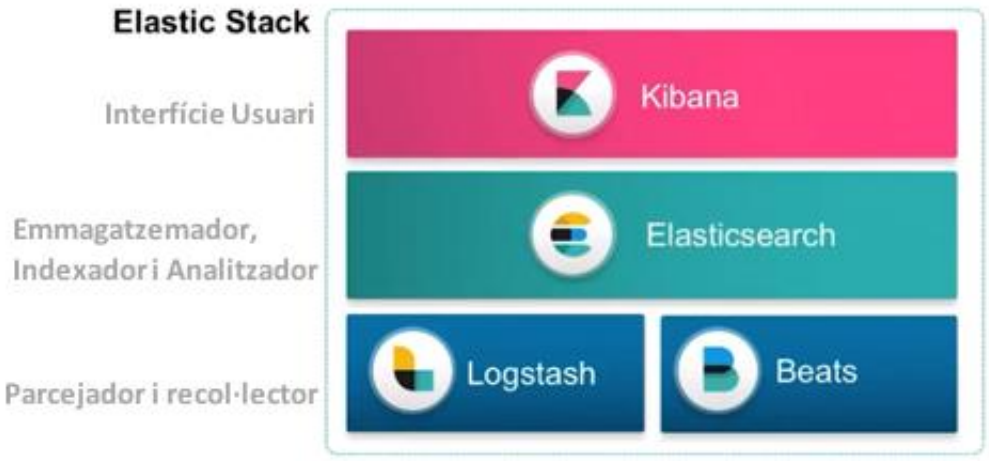
Aquesta proposta constarà de dues parts, la primera es muntarà un petit laboratori amb una arquitectura d'una sola màquina que inclourà la plataforma ELK, Wazuh i mòdul Netflow, on un servidor web tindrà instal·lat un agent Wazuh per generar alertes de seguretat, un agent (beats) que enviarà els logs del servidor i un mòdul de Netflow que exportarà les dades del iptables instal·lat. Per últim es realitzaran alguns test d'intrusió per veure les com es generen les alertes de seguretat mitjançant la monitorització del agent Wazuh. En aquest cas s'indicarà com instal·lar i configurar la solució que menys la part de configuració es pots extrapolar a la part del entorn real.

Per un altre banda s'explicarà un cas real d'utilització de la plataforma en una Universitat, on l'arquitectura d'un sol host no es viable, ja que el recursos que consumeix la plataforma són massa grans i s'ha d'optar per una arquitectura distribuïda.

Per últim es compararan els dos entorns i es trauran les conclusions de quin és el millor model alhora d'implementar la solució en una organització.

3.1.1 Elastic Stack

Elastic Stack és un paquet de programari (Filebeat, Logstash, Elasticsearch, Kibana) utilitzat per recopilar, analitzar, indexar, emmagatzemar, buscar i presentar dades de registre. Proporciona un front-end web que ofereix una vista de tauler d'alt nivell d'esdeveniments que permet anàlisis avançats i mineria de dades.



Il·lustració 7 - Composició Elastic Stack

Les avantatges d'utilitzar la plataforma ELK són les següents:

- **Escalabilitat**: Amb els clústers de Elasticsearch es poden gestionar terabytes de dades amb facilitat gracies a la escalabilitat horitzontal i la possibilitat d'estendre els recursos i equilibrar la carrega entre tot els nodes del clúster.

- **Cerca de dades avançada**: Ens permet la implementació de gran quantitat de funcions com cerca en temps real, Fuzzy Searching o cerca assistida i personalitzada.

- **Velocitat**: Ens permet fer cerques complexes extremadament ràpid, gracies a la estructura de dades DSL basada en JSON, la indexació i la utilització de filtres en cache.

3.1.2 Wazuh

El següent conjunt de capacitats que ens proporciona Wazuh és gracies a la integració d'OSSEC, OpenSCAP i Elastic Stack amb el que aconseguim una solució unificada, i simplifiquem la seva configuració i administració. A més Wazuh proporciona un conjunt de regles d'anàlisi de registre actualitzat, una API RESTful que li permet controlar l'estat, i la configuració de tots els agents de Wazuh. Totes aquestes característiques s'inclouen en una aplicació web enriquida, completament integrada amb Kibana.

Il·lustració 8 - Logo Wazuh

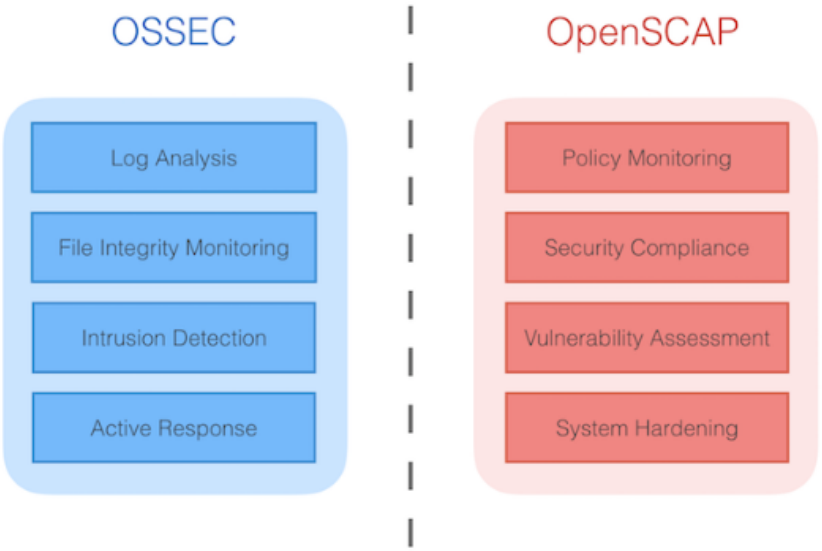
- **Supervisió d'integritat d'arxius**: Wazuh supervisa el sistema d'arxius, identificant els canvis en el contingut, permisos, propietat i atributs dels arxius que ha de monitoritzar.

- **Detecció d'intrusions i anomalies**: Els agents escanegen el sistema a la recerca de malware, rootkits o anomalies sospitoses. Poden detectar arxius ocults, processos encoberts o escoltes de xarxa no registrades, així com incoherències en les respostes de crides al sistema.

- **Anàlisi de registre automàtic**: Els agents de Wazuh llegeixen el sistema operatiu i els registres de l'aplicació, i els envien de manera segura a un administrador central per a l'anàlisi i emmagatzematge basat en regles. Les regles de Wazuh l'ajuden a conèixer els errors de l'aplicació o del sistema, les configuracions incorrectes, les activitats malicioses, intents o activitats amb èxit, les infraccions de les polítiques i una varietat de problemes de seguretat.

- **Monitoratge de polítiques i compliment**: Wazuh supervisa els arxius de configuració per assegurar-se que compleixin amb les seves polítiques de seguretat, estàndards i / o guies de reforç. Els agents realitzen escanejos periòdics per detectar aplicacions que se sap que són vulnerables, que no disposen de pegats o configuracions no segures.

Wazuh és un projecte per a la detecció, visibilitat i compliment de la seguretat. Va néixer com un fork de OSSEC HIDS, i més tard es va integrar amb Elastic Stack i OpenSCAP, evolucionant cap a una solució de seguretat més completa.



Il·lustració 9 - Funcions de Monitoratge

A continuació es descriuran la funció d'aquestes eines.

3.1.2.1 OSSEC

OSSEC HIDS és un Sistema de detecció d'intrusos (HIDS) propietat de Trend Micro, que està basat en host, s'utilitza per a la detecció, la visibilitat i la supervisió del compliment de la seguretat. És basa en un agent multiplataforma que envia dades del sistema (per exemple, missatges de registre, hash d'arxius i anomalies detectades) a un administrador central, on s'analitza i es processa, el que dona com a resultat alertes de seguretat. Els agents transmeten dades d'esdeveniments a la supervisora per el seu anàlisi a través d'un canal segur i autenticat.

Il·lustració 10 - Logo OSSEC

3.1.2.2 OpenSCAP

OpenSCAP és un intèrpret OVAL (Open Vulnerability Assessment Language) i XCCDF (Format de descripció de llista de verificació de configuració extensible) utilitzat per verificar els valors del sistema i detectar aplicacions vulnerables. És una eina dissenyada per verificar el compliment de la seguretat, i l'enduriment dels sistemes, utilitzant línies de base de seguretat estàndard de la indústria per a entorns empresarials, que te el recolzament d'organismes de seguretat tan assentats com CIS i NIST.

Il·lustració 11 - Organismes de seguretat

3.1.3 Logstash Netflow

LogstashNetflow és una eina que analitza els fluxos de xarxa, amb el que simplifica la recopilació, normalització y visualització creant panells en Kivana per explorar les dades extretes. Aquesta informació és important ja que ens permet tindre d'una manera simplificada el tràfic que es genera a la xarxa conservant dades com direccions IP, port de destinació/origen, protocols, capçaleres, etc. Per tant ens permet fer el seguiment d'un incident traient estadístiques de volum i tipus de tràfic.

Les possibilitats que ens permet aquest mòdul de Logstash són les següents:

- **Overview:** Veurem el resum de dades bàsiques de tràfic i es podrà veure ràpidament si hi ha algun esdeveniment que ressalti respecte la resta.

- **Geo Location:** Podrem obtenir una visualització ràpida amb mapes de calor les destinacions i orígens del tràfic de la nostra xarxa.

- **Traffic Analysis:** Es poden detectar grans volums de dades ordenat per paquets per segon o bytes per sego.

- **Conversation Partners:** Mitjançant els filtres podem veure origen i destinació de qualsevol transferència de dades.

- **Top-N:** Es visualitza per volum decreixent aplicacions, serveis, bytes, sessions, etc.

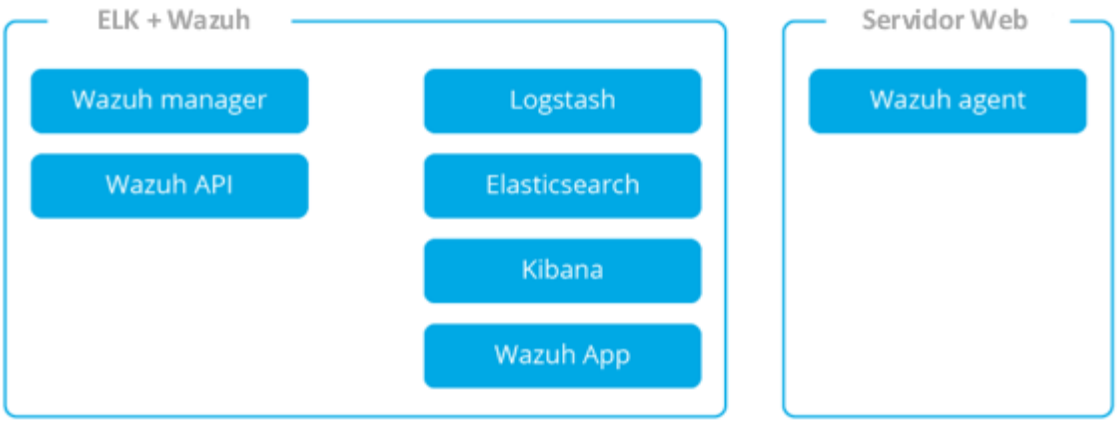
3.1.4 Arquitectura

3.1.4.1 Arquitectura d'una màquina (Entorn laboratori)

L'arquitectura del SIEM es dividirà en dos, una part serà tota la infraestructura d'Elastic Stack que s'encarregarà de tractar els logs de servidors i generar informació per detectar problemes tècnics, i un altre la part del sistema Wazuh que és la part més especifica per detectar incidents de seguretat.

Il·lustració 12 - Capes del SIEM

Per el nostre laboratori s'optarà per una arquitectura d'una màquina en la que tant el sistema Elastic Stack i Wazuh aniran instal·lats en la mateixa màquina virtual, ja que els requisits necessaris i la informació generada no serà molt gran. Aquesta arquitectura estaria pensada per una petita o mitjana empresa que vulgui monitoritzar la seva xarxa.



Il·lustració 13 - Programari Client-Servidor Laboratori

3.1.4.1.1 Components

Tota la estructura estarà virtualitzada en una estació personal amb l'aplicatiu VirtualBox 5.2.20, aquest components són els següents:

ELK stack + Wazuh

En aquest servidor s'allotjarà tot els sistema de gestió SIEM, les característiques de la màquina virtual són les següents:

	ELK-Wazuh
IP	192.168.1.10
Memòria	4GB
CPU's	2 cores
Disc	50GB
S.O.	Debian 9.5.0 x64
Memòria de Vídeo	32MB
Software Base	Standard System Utilities

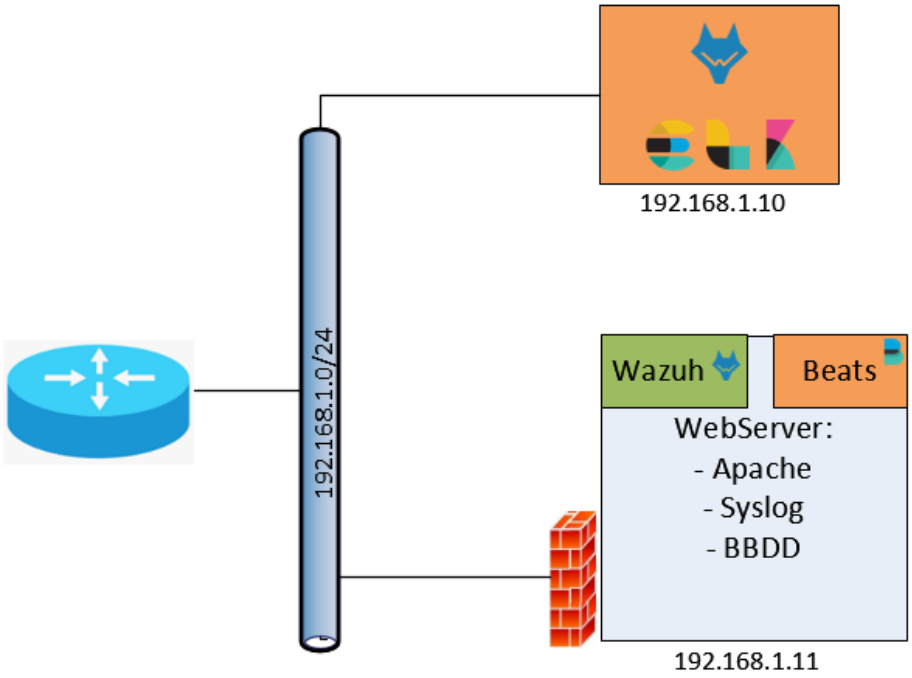
Servidor Web

Aquest servidor tindrà instal·lat un servidor web i un servidor ssh, les característiques de la màquina virtual són les següents:

	Web-Server
IP	192.168.1.11
Memòria	2GB
CPU's	2 cores
Disc	15GB
S.O.	Debian 9.5.0 x64
Memòria de Vídeo	32MB
Software Base	SSH Server, Web Server, IPtables

3.1.4.1.2 Diagrama

Aquesta arquitectura consta d'un node central ELK Stack on es rebran els logs de dades per part del agent Wazuh, Beat i Netflow instal·lat en el servidor web.



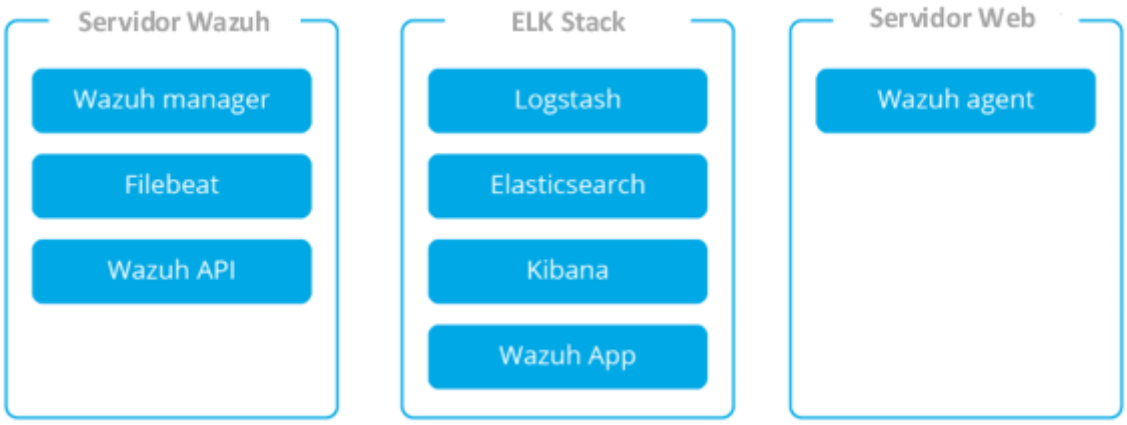
Il·lustració 14 - Arquitectura Laboratori

3.1.4.2 Arquitectura distribuïda (Entorn real)

Quan tenim volums de tràfic elevat i diferents zones de xarxa on es troben els servidors a monitoritzar, el més adient es escollir l'arquitectura distribuïda, aquesta ens permetrà no sobrecarregar els routers de zona amb tràfic innecessari, ja que tindrem servidors Logstash que parcejaran els logs en brut per després passar-ho al clúster d'ElasticSearch, que s'encarregarà d'indexar

les dades, per tant només necessitarem obrir el tràfic entre zones per l'accés dels col·lectors als indexadors.

Una vegada l'arquitectura de ELK Stack està muntada, caldria afegir els servidor wazuh independents, que serien els encarregats de rebre la informació dels agents instal·lats, en aquest cas tindríem un servidor wazuh que actuaria com a master i seria l'encarregat de distribuir la carrega entre els 'workers'.



Il·lustració 15 - Programari Client-Servidor Real

3.1.4.2.1 Components

SERVIDOR KIBANA	
Memòria	4GB
CPU's	2 de 2 cores
Disc	2 discs de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

SERVIDOR BALANCEADOR ELASTICSEARCH	
Memòria	2GB
CPU's	2 de 2 cores
Disc	2 discos de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

SERVIDOR ELASTIC1-ELASTIC2-ELASTIC3	
Memòria	12GB
CPU's	2 de 2 cores
Disc	2 discos de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB. Espai al NAS de 900GB mapejats a /var/lib/elasticsearch
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

SERVIDOR LOGSTASHFE-LOGSTASHBE-LOGSTASHDE	
Memòria	4GB
CPU's	2 de 2 cores
Disc	2 discos de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

SERVIDOR BALANCEADOR WAZUH	
Memòria	2GB
CPU's	2 de 2 cores
Disc	2 discos de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

SERVIDOR WAZUH1-WAZUH2-WAZUH3	
Memòria	8GB
CPU's	2 de 2 cores
Disc	2 discos de 20GB
S.O.	Debian 9 x64
Particions	/ de 20GB, /var de 20GB, swap de 1.5GB
Software Base	SSH Server y Standard System Utilities
Software Base Addicional	Open-vm-tools, Shorewall, ocs, nagios

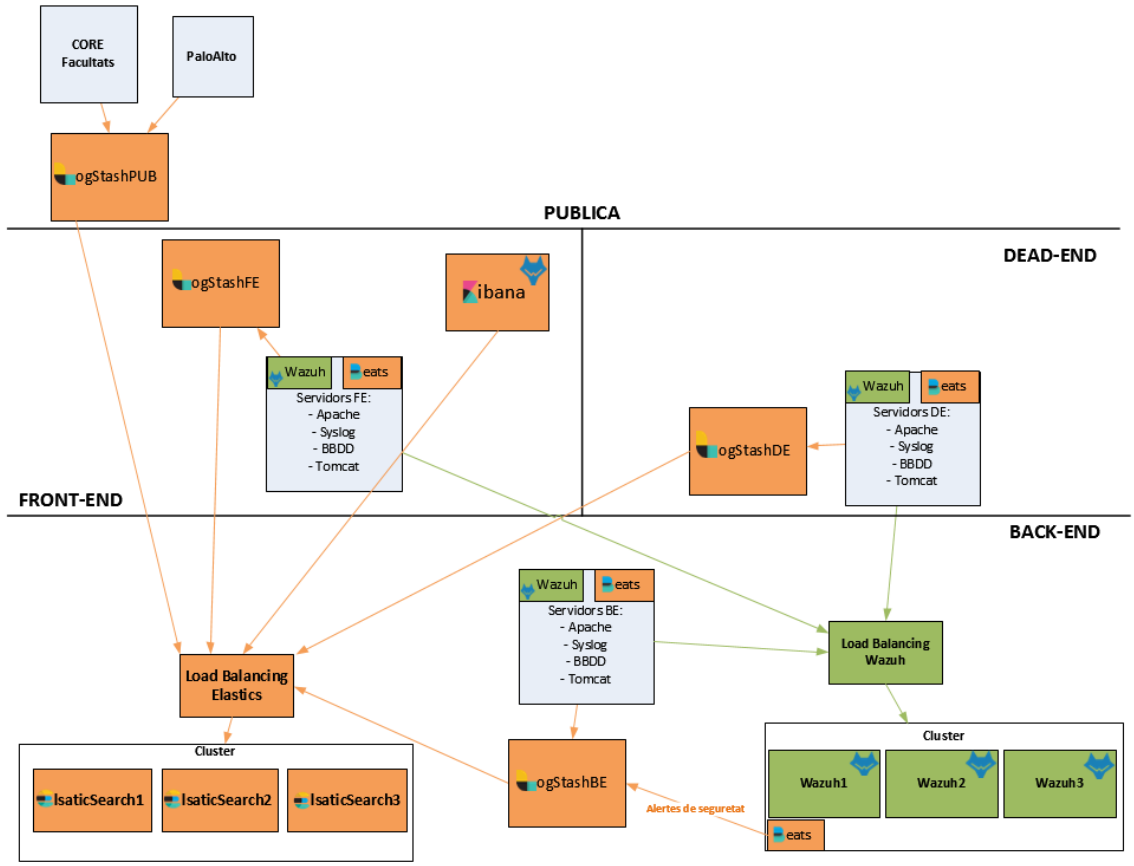
3.1.4.2.2 Diagrama

Al següent diagrama veiem la arquitectura distribuïda que consta de quatre zones de xarxa, pública, front-end, dead-end i back-end. Per la zona del segment de publica el servidor de Logstash serà l'encarregat de rebre els logs dels switchs centrals de facultat, Firewall perimetral (PaloAlto) i servidors de la xarxa pública.

Per altre banda tenim el segment de front-end on estarà el panell d'administració de la nostre plataforma (Kibana), que es connectarà amb el clúster d'ElasticSearch per poder mostrar totes les dades que s'han emmagatzemat dels servidors a monitoritzar. A més tindrem un altre servidor Logstash que s'encarregarà de rebre els logs de tots els servidors d'aquest segment de xarxa.

En el segment de dead-end no tindrem cap element del ELK Stack fora del Logstash, que s'encarregarà com en les altres zones de rebre tots els logs, formatar-los i enviar-los al clúster d'Elastic. A part tindrem els agents Wazuh que tan en aquesta zona com a la resta, enviaran la informació dels anàlisis de servidors i logs al clúster de Wazuh.

Per últim tenim back-end, la zona on resideix pràcticament tota la infraestructura de pes de la solució, aquí tenim el clúster d'ElasticSearch on un dels nodes màster fa la funció de balancejador i distribueix la carrega entre els altres tres nodes. A part tenim el clúster de servidors Wazuh on com en el cas dels indexadors un dels nodes de Wazuh es configura com a màster i s'encarrega de repartir la carrega entre els workers. Com a últim element tindrem el servidor de Logstash de la zona que com a les altres zona serà l'encarregat de rebre la informació dels beats de servidor.

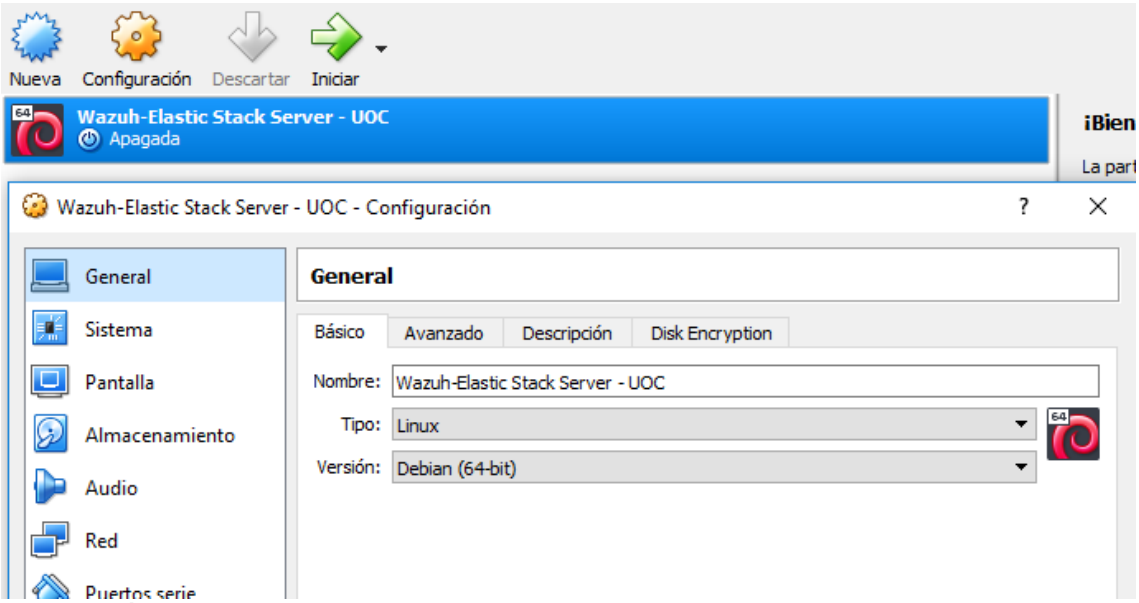


Il·lustració 16 - Arquitectura distribuïda

3.2 Entorn laboratori

En aquesta part ens centrarem en una arquitectura d'un sol node, aquesta arquitectura està destinada per petites o mitjanes empreses que tenen un pool de servidors d'entre 1-20 servidors amb una tassa d'indexació d'uns 500-700 shards per segon, encara que es podria ampliar una mica més aquests valors donant-li més recursos al servidor o gestionant l'emmagatzematge d'índex.

Primer de tot crearem una màquina virtual amb sistema operatiu Debian 9.5.0 on instal·larem la plataforma de gestió Wazuh + Elastic Stack:



Il·lustració 17 - VirtualBox SIEM

3.2.1 Wazuh

El primer pas és afegir els repositositoris per poder descarregar el paquet wazuh-manager, per fer-ho executarem la següent comanda per afegir la clau GPG:

**Perquè tot el procés s'executi correctament ens caldrà tindre instal·lat en el nostre servidor els paquets [curl, apt-transport-https, lsb-release].*

```
root@elk-wazuh:~# curl -s https://packages.wazuh.com/key/GPG-
KEY-WAZUH | apt-key add -
```

Ara afegim el repositori i actualitzem la informació dels paquets:

```
root@elk-wazuh:~# echo  "deb https://packages.wazuh.com/3.x/apt/
stable main"  | tee -a /etc/apt/sources.list.d/wazuh.list

root@elk-wazuh:~# apt-get update
```

Procedim a instal·lar el paquet wazuh-manager amb el repositori afegit anteriorment:

```
root@elk-wazuh:~# apt-get install wazuh-manager
```

Per comprovar que el procés s'ha completat correctament i el servei està funcionant farem la següent comanda:

```
root@elk-wazuh:~# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/etc/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2018-11-03 17:37:19 CET; 5min ago
   CGroup: /system.slice/wazuh-manager.service
           ├─4750 /var/ossec/bin/wazuh-db
           ├─4764 /var/ossec/bin/ossec-execd
           ├─4770 /var/ossec/bin/ossec-analysisd
           ├─4775 /var/ossec/bin/ossec-syscheckd
           ├─4781 /var/ossec/bin/ossec-remoted
           ├─4785 /var/ossec/bin/ossec-logcollector
           ├─4805 /var/ossec/bin/ossec-monitord
           └─4810 /var/ossec/bin/wazuh-modulesd

Nov 03 17:37:16 elk-wazuh env[4736]: Started wazuh-db...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-execd...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-analysisd...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-syscheckd...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-remoted...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-logcollector...
Nov 03 17:37:16 elk-wazuh env[4736]: Started ossec-monitord...
Nov 03 17:37:17 elk-wazuh env[4736]: Started wazuh-modulesd...
Nov 03 17:37:19 elk-wazuh env[4736]: Completed.
Nov 03 17:37:19 elk-wazuh systemd[1]: Started Wazuh manager.
```

Il·lustració 18 - Comprovació Wazuh

3.2.1.1 Wazuh API

Per a que en el nostre panell Kivana on visualitzarem totes les dades dels logs puguem veure un nou apartat on trobarem totes les funcionalitats de Wazuh, s'haurà d'instal·lar una API que es comuniqui entre el ELK stack i Wazuh Manager.

**Per poder executar la API de Wazuh ens caldrà tindre instal·lat nodejs, per fer-ho afegirem el repositori oficial.*

```
root@elk-wazuh:~# curl -sL https://deb.nodesource.com/setup_8.x
| bash
root@elk-wazuh:~# apt-get install nodejs
root@elk-wazuh:~# apt-get install wazuh-api
```

Comprovem que el servei esta aixecat correctament:

```
root@elk-wazuh:~# systemctl status wazuh-api
● wazuh-api.service - Wazuh API daemon
   Loaded: loaded (/etc/systemd/system/wazuh-api.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2018-11-03 18:15:22 CET; 4s ago
     Docs: https://documentation.wazuh.com/current/user-manual/api/index.html
 Main PID: 13519 (nodejs)
   CGroup: /system.slice/wazuh-api.service
           └─13519 /usr/bin/nodejs /var/ossec/api/app.js

Nov 03 18:15:22 elk-wazuh systemd[1]: Started Wazuh API daemon.
```

Tot seguit s'explicarà les configuracions necessàries per un bon funcionament de la eina, però primer de tot es desactivaran les actualitzacions Wazu per fer-ho sempre des d'un entorn controlat.

```
root@elk-wazuh:~# sed -i "s/^deb/#deb/"
/etc/apt/sources.list.d/wazuh.list
root@elk-wazuh:~# apt-get update
```

3.2.1.1.1 Connexió amb Wazuh API

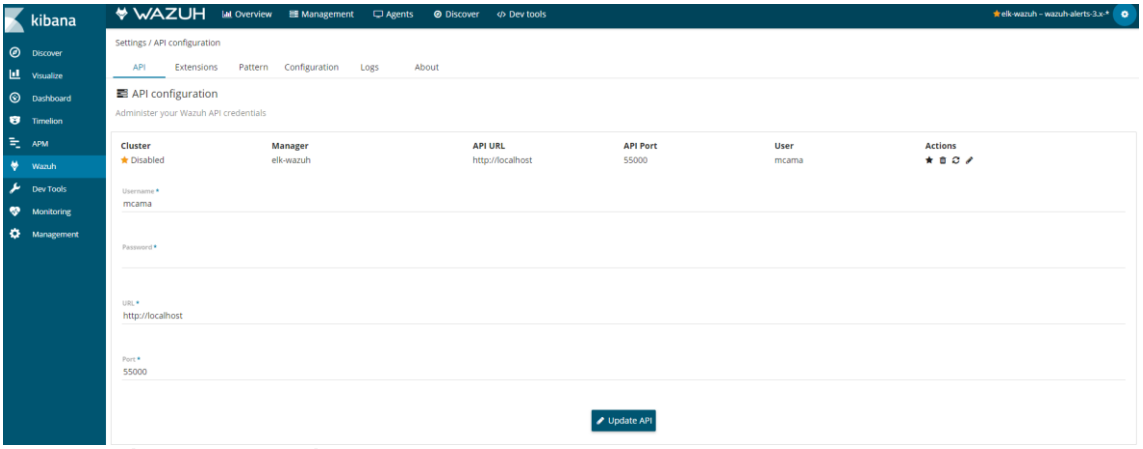
Per a poder visualitzar les dades gestionades per Wazuh Server, s'ha de lligar la Wazuh APP instal·lada a Kibana mitjançant la Wazuh API, per tant assignarem un usuari i paraula de pas per poder-nos connectar.

```
root@elk-wazuh:~# cd /var/ossec/api/configuration/auth

root@elk-wazuh:~# node htpasswd -c user mcama
```

Reiniciem la API:

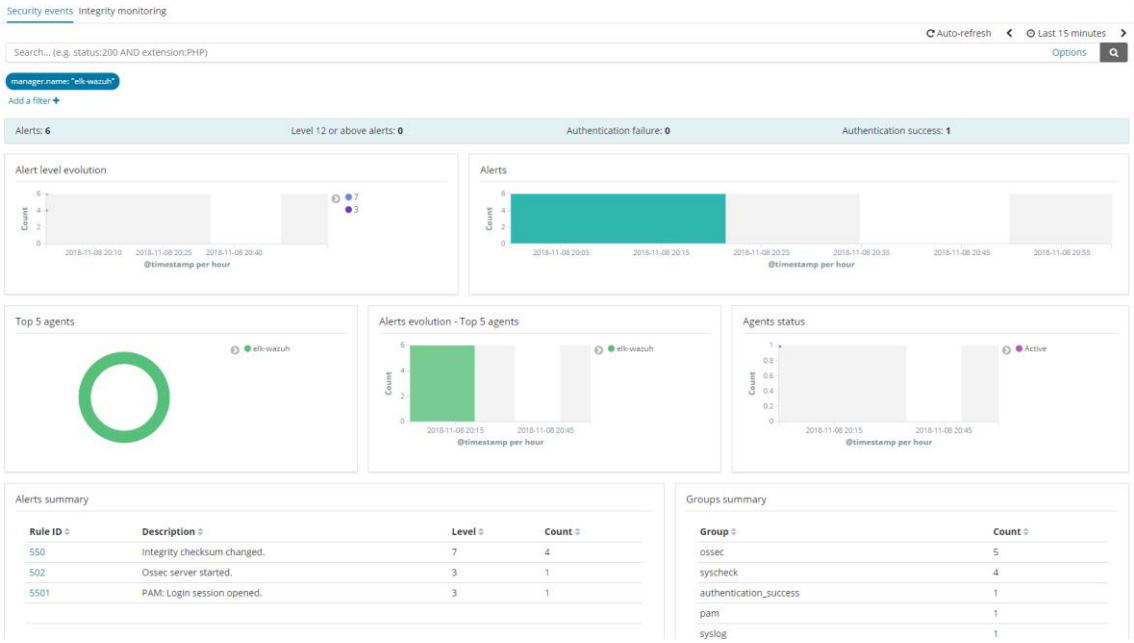
```
root@elk-wazuh:~# systemctl restart wazuh-api
```

Realitzem la connexió a la APP:



Il·lustració 19 - Connexió API

Ja podem veure com comença a graficar, per tant la connexió és correcte.



Il·lustració 20 - Comprovació connexió API

3.2.1.2 Registre Servidor

Per monitoritzar i auditar un actiu necessitem d'un agent que estigui instal·lat en local i enviï les dades al manager, en aquest cas el nostre SIEM (ELK-Wazuh). Per fer-ho instal·larem un servidor Linux (Servidor Web) on s'instal·larà l'agent Wazuh.

**Per poder fer us de les eines com OpenScap i Vulneraibilities necessitarem tindre instal·lats els següents paquets libopenscap8 i xsltproc.*

Afegim els repositoris e instal·lem wazuh-agent:

```
root@web-server:~# curl -s https://packages.wazuh.com/key/GPG-
KEY-WAZUH | apt-key add -

root@web-server:~# echo "deb https://packages.wazuh.com/3.x/apt/
stable main" | tee /etc/apt/sources.list.d/wazuh.list

root@web-server:~# apt-get update

root@web-server:~# apt-get install wazuh-agent
```

Ara ens dirigim al manager per donar d'alta el servidor especificant el nom i la IP:

```
root@elk-wazuh:~# /var/ossec/bin/manage_agents

****************************************
* Wazuh v3.6.1 Agent manager.          *
* The following options are available: *
```

```
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: web-server
   * The IP Address of the new agent: 192.168.1.11
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:web-server
   IP Address:192.168.1.11

Confirm adding it?(y/n): y
Agent added with ID 001.
```

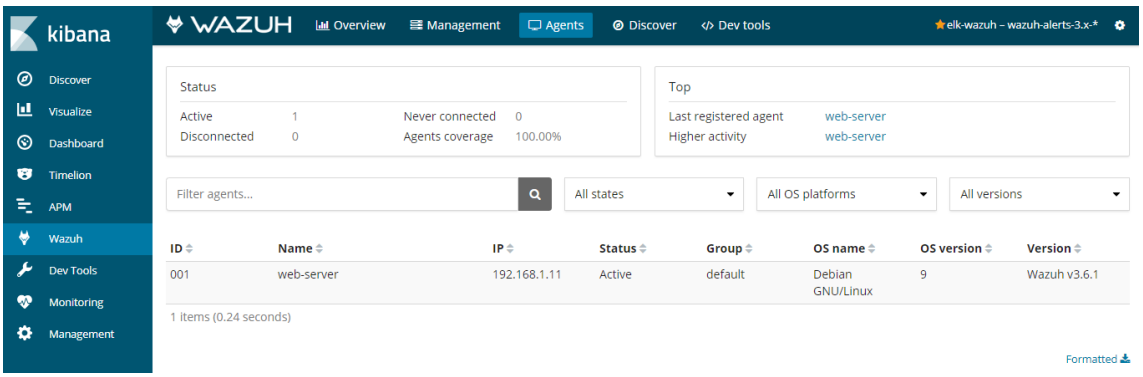
Ara només ens queda extraure la key generada per importar-la al servidor web:

```
root@web-server:~# /var/ossec/bin/manage_agents

****************************************
* Wazuh v3.6.1 Agent manager.          *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHdlYi1zZXJ2ZXIgMTkyLjE2OC4xLjExIGM3NDY3YTc0NzBkY2Y3NzE1NTU0
ZmE3ZjllMmVlN2ZmNWI1YjZkOTBhNmRiMWRlM2MxMTBjODhkMGQ5ZGYyZjk=

Agent information:
   ID:001
   Name:web-server
   IP Address:192.168.1.11

Confirm adding it?(y/n): y
Added.
```

Per últim editarem la configuració d'Ossec per indicar-li quina es la IP de Wazuh manager i reiniciarem el servei:

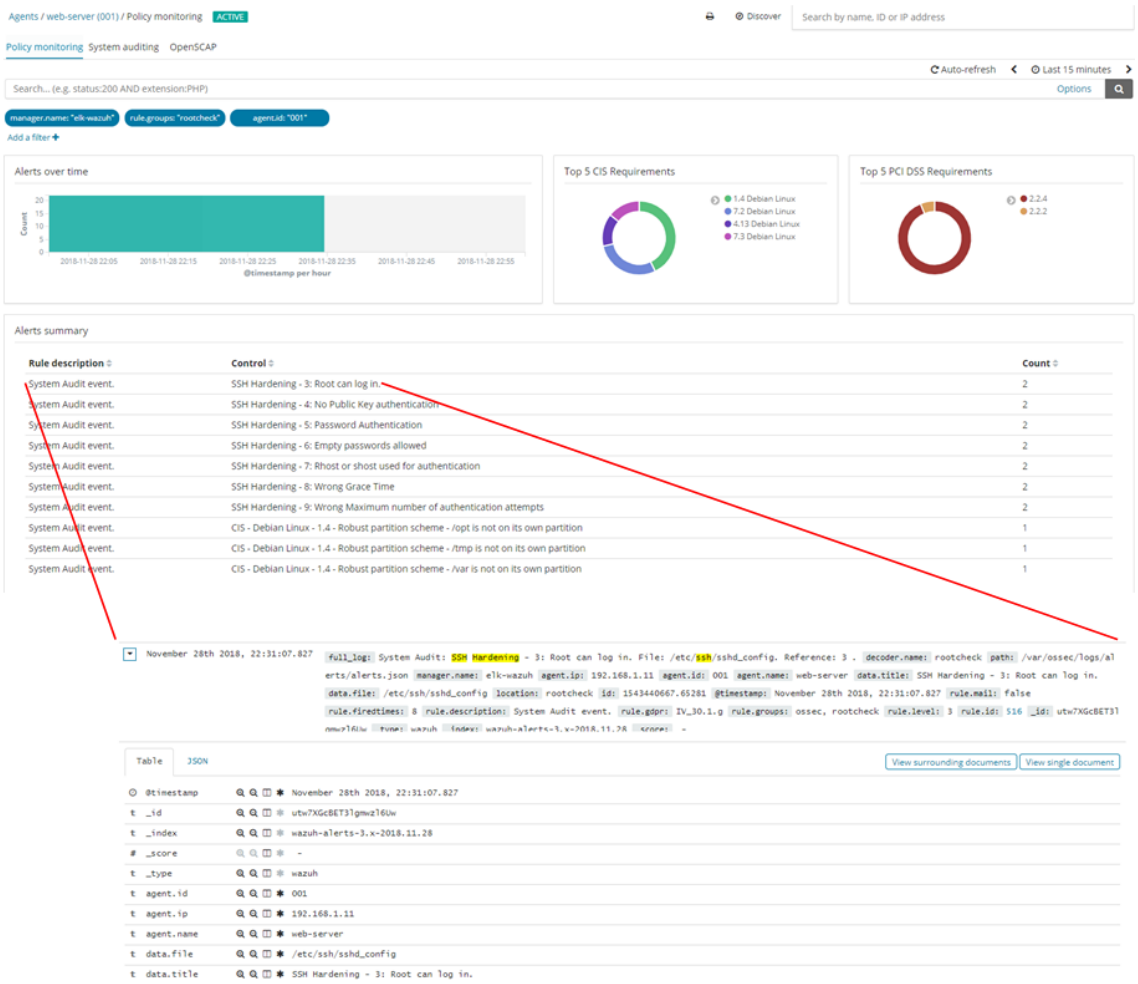
```
root@web-server:~# nano /var/ossec/etc/ossec.conf

<client>
      <server-ip>192.168.1.10</server-ip>
</client>

root@web-server:~# /var/ossec/bin/ossec-control restart
```

Podem veure com ja ens apareix el servidor web al nostre panell d'administració.



Il·lustració 21 - Agent

Si accedim a 'Policy monitoring' podem observar els diferents controls que no ha passat satisfactòriament el servidor, com la possibilitat de validar amb l'usuari root, configuració incorrecte d'intents d'accés per SSH, o les recomanacions del CIS per configurar el directoris /opt, /tmp i /var en particions diferents per tindre més robustesa. Les alertes queden registrades en ElasticSearch per consultar-les en qualsevol moment en el format de la resta de logs.



Il·lustració 22 - Policy monitoring

3.2.2 Elastic Stack

Ens disposem a instal·lar el paquet Elastic Stack composat per Logstash, Elasticsearch i Kivana, un requisit per poder fer-ho és tindre el paquet d'Oracle Java JRE 8, per tant afegirem els repositoris i procedirem a la instal·lació.

**Per la versió Debian 9 haurem d'instal·lar el paquet 'dirmngr' per a que ens funcioni tot el procés.*

Afegim repositoris:

```
root@elk-wazuh:~# echo  "deb
http://ppa.launchpad.net/webupd8team/java/ubuntu xenial main"  |
tee /etc/apt/sources.list.d/webupd8team-java.list

root@elk-wazuh:~# echo  "deb-src
http://ppa.launchpad.net/webupd8team/java/ubuntu xenial main"  |
tee -a /etc/apt/sources.list.d/webupd8team-java.list

root@elk-wazuh:~# apt-key adv --keyserver
hkp://keyserver.ubuntu.com:80 --recv-keys EEA14886
```

Procedim a la instal·lació:

```
root@elk-wazuh:~# apt-get update
root@elk-wazuh:~# apt-get install oracle-java8-installer
```

3.2.2.1 Elasticsearch

El primer que instal·larem del paquet ELK Stack és el motor de cerca i anàlisi de text Elasticsearch, per fer-ho afegirem el repositori i la seva clau GPG, després ja podrem procedir a la instal·lació.

```
root@elk-wazuh:~# curl -s https://artifacts.elastic.co/GPG-KEY-
elasticsearch | apt-key add -

root@elk-wazuh:~# echo  "deb
https://artifacts.elastic.co/packages/6.x/apt estable main"  |
tee /etc/apt/sources.list.d/elastic-6.x.list

root@elk-wazuh:~# apt-get update
```

Instal·lem Elasticsearch a la versió 6.4.2 (la més recent en el moment de la instal·lació):

```
root@elk-wazuh:~# apt-get install elasticsearch=6.4.2
```

Activem e iniciem el servei:

```
root@elk-wazuh:~# systemctl daemon-reload
root@elk-wazuh:~# systemctl enable elasticsearch.service
root@elk-wazuh:~# systemctl start elasticsearch.service
```

Per comprovar sempre que el servei s'està executant correctament ho farem amb la comanda 'curl "localhost:9200/?pretty"' que ens retornarà la sortida.

```
root@elk-wazuh:~# curl "localhost:9200/?pretty"
{
  "name" : "o43BkCZ",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "17sTzEdhRjuTuaYYXcZJ8Q",
  "version" : {
    "number" : "6.4.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "04711c2",
    "build_date" : "2018-09-26T13:34:09.098244Z",
    "build_snapshot" : false,
    "lucene_version" : "7.4.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Carreguem el template Wazuh per Elasticsearch:

```
root@elk-wazuh:~# curl
https://raw.githubusercontent.com/wazuh/wazuh/3.6/extensions/ela
sticsearch/wazuh-elastic6-template-alerts.json | curl -XPUT
'http://localhost:9200/_template/wazuh' -H 'Content-Type:
application/json' -d @-
```

Desactivem les actualitzacions automàtiques de Elasticsearch per estalviar possibles errors i tindre les actualitzacions totalment controlades i planificades.

```
root@elk-wazuh:~# sed -i "s/^deb/#deb/"
/etc/apt/sources.list.d/elastic-6.x.list
root@elk-wazuh:~# apt-get update
```

3.2.2.2 Instal·lació Logstash

El següent pas seria la instal·lació de Logstash, l'encarregat de recopilar, analitzar i reenviar les dades rebudes per tots els actius monitoritzats (tan per agent Wazuh com per beats) a Elasticsearch, que indexarà i emmagatzemarà tots els registres.

```
root@elk-wazuh:~# apt-get install logstash=1:6.4.2-1
```

Ara ens descarreguem l'arxiu de configuració per rebre les alertes de Wazuh a Logstash.

```
root@elk-wazuh:~# curl -so /etc/logstash/conf.d/01-wazuh.conf
https://raw.githubusercontent.com/wazuh/wazuh/3.6/extensions/log
stash/01-wazuh-local.conf
```

Afegim l'usuari de logstash al grup OSSEC per a que pugui llegir l'arxiu alerts.json:

```
root@elk-wazuh:~# usermod -a -G ossec logstash
```

Activem e iniciem el servei:

```
root@elk-wazuh:~# systemctl daemon-reload
root@elk-wazuh:~# systemctl enable logstash.service
root@elk-wazuh:~# systemctl start logstash.service
```

3.2.2.3 Kibana

Com a últim pas per tindre la versió completa d'Elastic Stack és instal·lar Kivana, l'encarregat de mostrar els esdeveniments i arxius emmagatzemats a Elasticsearch mitjançant una plana web on també tindrem el mòdul Wazuh integrat completament.

Instal·lem Kibana:

```
root@elk-wazuh:~# apt-get install kibana=6.4.2
```

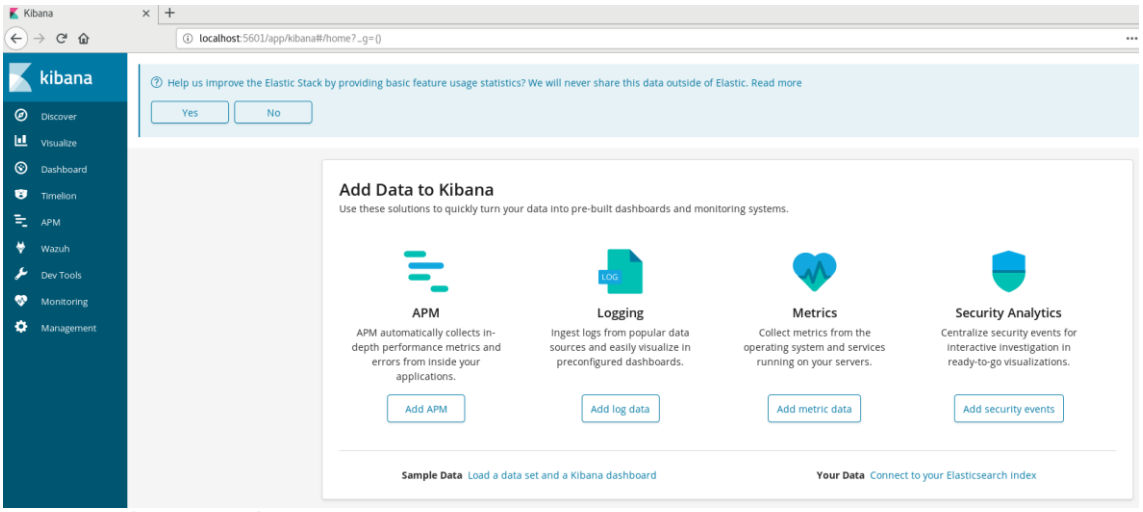
Ara instal·lem l'aplicació Wazuh que estarà integrada a Kibana, però abans necessitem establir un límit de memòria del node.js ja que pot ocasionar error en l'execució.

```
root@elk-wazuh:~# export NODE_OPTIONS="--max-old-space-
size=3072"
root@elk-wazuh:~# /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/wazuhapp/wazuhapp-3.6.1_6.4.2.zip
```

Activem e iniciem el servei:

```
root@elk-wazuh:~# systemctl daemon-reload
root@elk-wazuh:~# systemctl enable kibana.service
root@elk-wazuh:~# systemctl start kibana.service
```

Per comprovar que s'ha instal·lat tot correctament entrem al explorador del servidor i carreguem http://localhost:5601, podem veure que s'ha iniciat correctament i s'ha instal·lat el complement Wazuh.



Il·lustració 23 - Accés Kibana

3.2.2.3.1 Autenticació i Xifratge

Per defecte Kibana no proporciona un portal de validació amb el que qualsevol podria accedir-hi i consultar dades confidencials. Al mercat existeixen diferents plugins que ens donen solució per aquesta problemàtica, com el mòdul X-Pack d'Elastic o Search Guard, amb el que et donen moltes possibilitats com validació LDAP, Active Directory, xifratge de dades, etc.

Nosaltres optarem per un altre solució diferent, ja que les anteriors depenent la solució s'ha de realitzar una subscripció de pagament i encara que amb 'Search Guard' podríem obtenir el mateix resultat de manera gratuïta, escollirem el mètode d'instal·lar un servidor web 'nginx' que faci de Proxy i redirigeixi les peticions, i amb el paquet apache2-utils afegirem la validació.

Instal·lem NGINX:

```
root@elk-wazuh:~# apt-get install nginx
```

Com no tenim un certificat signat vàlid, ens generarem els nostres propis certificats per presentar al portal web, ja que farem la redirecció del protocol http a https:

```
root@elk-wazuh:~# mkdir -p /etc/ssl/certs /etc/ssl/private
root@elk-wazuh:~# openssl req -x509 -batch -nodes -days 365 -
newkey rsa:2048 -keyout /etc/ssl/private/kibana-access.key -out
/etc/ssl/certs/kibana-access.pem
```

Editem l'arxiu default de sites-available del servidor web (nginx) per a que quan escolti per el port 80 (http) ens faci una redirecció al port 443 (https) i ens faci de Proxy apuntant al port 5601 on està l'aplicació Kibana escoltant.

```
root@elk-wazuh:~# nano /etc/nginx/sites-available/default

server {
    listen 80;
    listen [::]:80;
    return 301 https://$host$request_uri;
}

server {
    listen 443 default_server;
    listen            [::]:443;
    ssl on;
    ssl_certificate /etc/ssl/certs/kibana-access.pem;
    ssl_certificate_key /etc/ssl/private/kibana-access.key;
    access_log            /var/log/nginx/nginx.access.log;
    error_log            /var/log/nginx/nginx.error.log;
    location / {
        auth_basic "Restricted";
        auth_basic_user_file /etc/nginx/conf.d/kibana.htpasswd;
        proxy_pass http://localhost:5601/;
    }
}
```

Instal·lem el paquet 'apache2-utils' per tindre validació:

```
root@elk-wazuh:~# apt-get install apache2-utils
```

Creem l'usuari per la validació:

```
root@elk-wazuh:~# htpasswd -c /etc/nginx/conf.d/kibana.htpasswd
mcama
```

Finalment reiniciem el servei:

```
root@elk-wazuh:~# systemctl restart nginx
```

3.2.2.4 Netflow

3.2.2.4.1 Logstash

Per poder monitoritzar els fluxos de xarxa s'activarà un mòdul a Logstash on ens permetrà recollir la informació enviada per el servidor web, i es crearan dashboards de monitorització per recollir estadístiques.

```
root@elk-wazuh:~#/usr/share/logstash/bin/logstash --modules
netflow --setup --path.settings=/etc/logstash -M
"netflow.var.kibana.ssl.enabled=false" -M
"netflow.var.input.udp.port=12001"
```

Configurem logstash.yml perquè escolti per el port UDP/12001 on rebrà tota la informació.

```
modules:
  - name: netflow
    var.input.udp.port: 12001
```

3.2.2.4.2 Servidor web

Ara es configurarà el servidor web per a que enviï els fluxos de xarxa, per fer-ho ens caldrà instal·lar IPT-Netflow que mitjançant l'iptables instal·lat al servidor ens enviarà tot el tràfic que després es processarà a Logstash.

**Enllaç de descarrega 'github.com/aabc/ipt-netflow.git ipt-netflow'*

Configurem IPT-Netflow per enviar les dades a Logstash.

```
root@web-server:~# echo options ipt_NETFLOW
destination=192.168.1.10:12001protocol=9
 > /etc/modprobe.d/netflow.conf
```

Configurem l'iptables per a que enviï el tràfic al mòdul de netflow instal·lat.

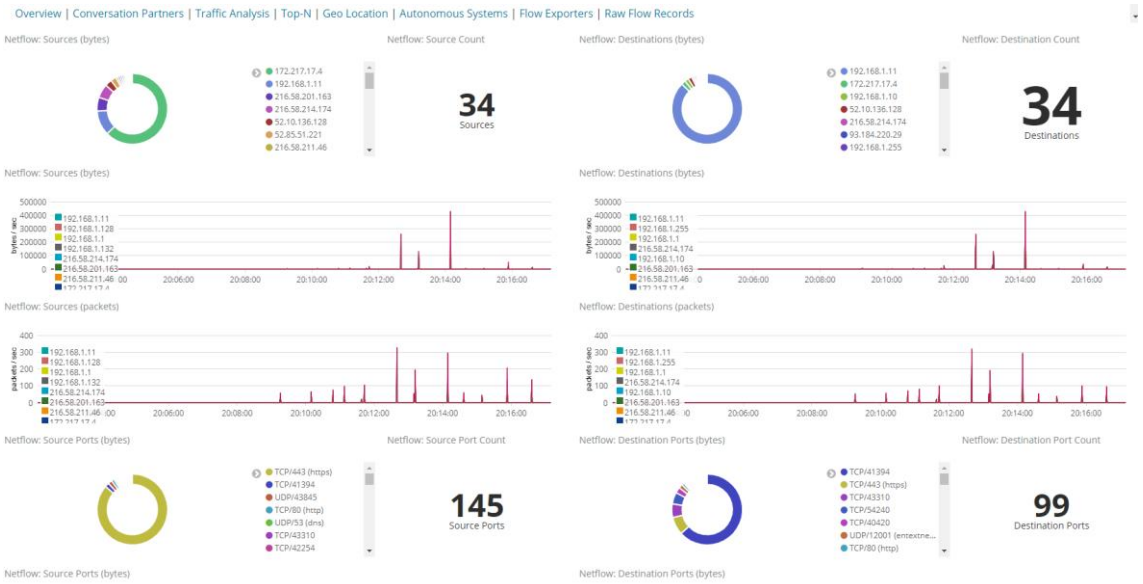
```
root@web-server:~# iptables -I FORWARD -j NETFLOW
```

Com podem veure en les següents captures el tràfic del servidor es mostra amb diferents menús depenent de la informació que necessitem extreure.

A '**Overview'** podem veure un resum de les dades capturades com quin protocol s'utilitza, destinació dels paquets (localització, IPs, dominis), tipus de connexió, etc.

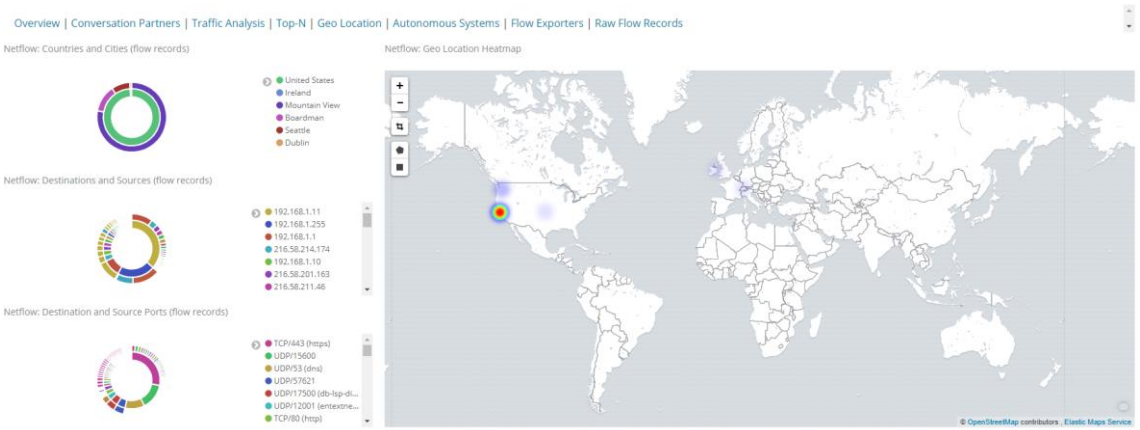
Il·lustració 24 - Overview

Un manera visual de veure esdeveniments destacables és mitjançant '**Traffic Analysis**' amb el que tindrem gràfiques per bytes per segon i paquets per segon de les IPs en les transaccions, per tant podrem veure molt ràpidament si alguna d'elles està destacant amb algun dels dos paràmetres i sortint dels límits habituals.



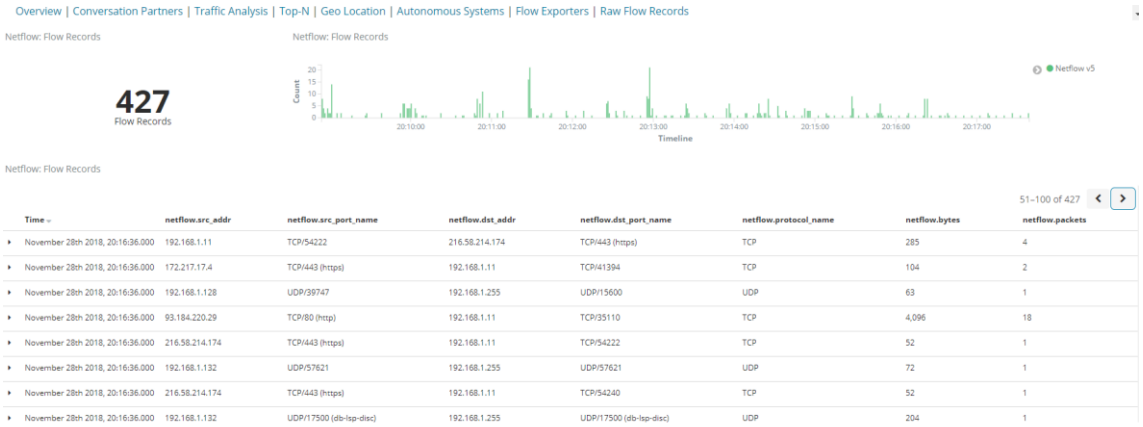
Il·lustració 25 - Traffic Analysis

El menú '**Geo Location**' és més visual i la seva utilitat pot ser més a nivell informatiu per veure d'una manera rapida i gràfica on s'està dirigint el tràfic de la teva xarxa, com veiem la major part del tràfic prové d'Estats Units ja que la majoria de serveis que fem servir estan allotjats allà, amb el que si aquest puts el tinguéssim a una regió com per exemple Xina i nosaltres ja sabem que no hauria d'haver-hi un volum tan gran doncs seria motiu d'alerta.



Il·lustració 26 - Geo Location

Un altre de les funcions interesants d'aquest mòdul és '**Raw Flow**' on podem veure en detall cada paquet que creua el Firewall i poder fer anàlisi forense dels successos que ens interessin.



Il·lustració 27 - Raw Flow

3.2.2.5 FileBeat

Per poder recopilar els logs dels servidors ens caldrà la utilització de Beats que enviarà els logs que vulguem registrar d'un servidor a ELK així podrem consultar-los quan vulguem.

3.2.2.5.1 Servidor web

Primer de tot descarregarem e instal·lem la clau publica GPG per poder descarregar els paquets via repositori.

```
root@web-server:~# wget -qO - https://artifacts.elastic.co/GPG-
KEY-elasticsearch | apt-key add -
OK
```

Afegim el repositori, instal·lem i habilitem el servei per a que arranqui sol.

```
root@serverlinux:~# apt-get update && apt-get install apt-
transport-https

root@serverlinux:~# echo "deb
https://artifacts.elastic.co/packages/6.x/apt stable main" | tee
-a /etc/apt/sources.list.d/elastic-6.x.list
deb https://artifacts.elastic.co/packages/6.x/apt stable main

root@serverlinux:~# apt-get update && apt-get install filebeat

root@serverlinux:~# systemctl enable filebeat
```

Modifiquem el fitxer /etc/filebeat/filebeat.yml i configurem el servidor logstash que rebrà els logs i el arxius a enviar.

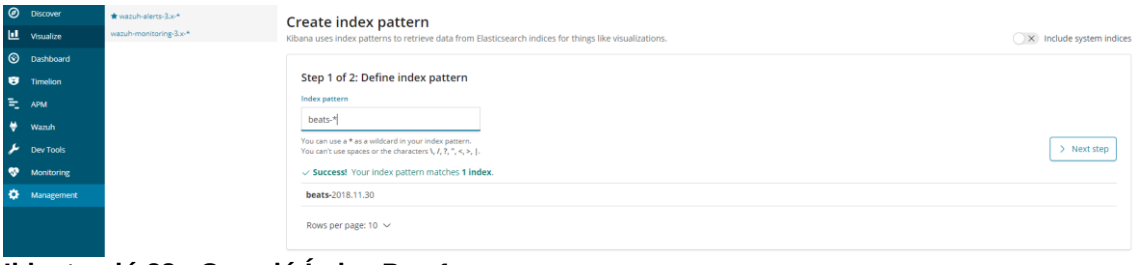
```
#==================== Filebeat inputs=============================
- /var/log/*.log
#------------------------ Logstash output ----------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.10:5044"]
```

3.2.2.5.2 ELK

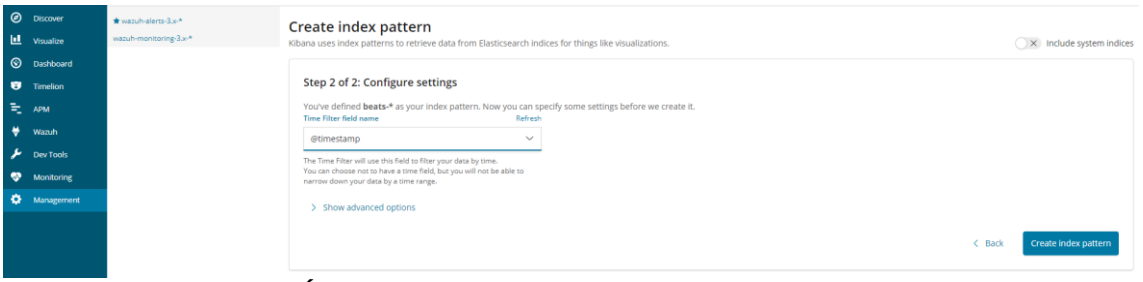
Ara ens caldrà crear una entrada a logstash (/etc/logstash/conf.d/logstash-beats.conf) per a que escolti per el port 5044 formati els logs i els enviï a elàstic per a que els emmagatzemi.

```
input {
  beats {
    port => 5044
 }
}

output {
  elasticsearch {
    hosts => "localhost:9200"
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-
%{+YYYY.MM.dd}"
  }
}
```

Per últim entrarem a Kibana i crearem el nou índex per a que tot el que arribi amb el nom beats ho inclogui en aquesta nova categoria.

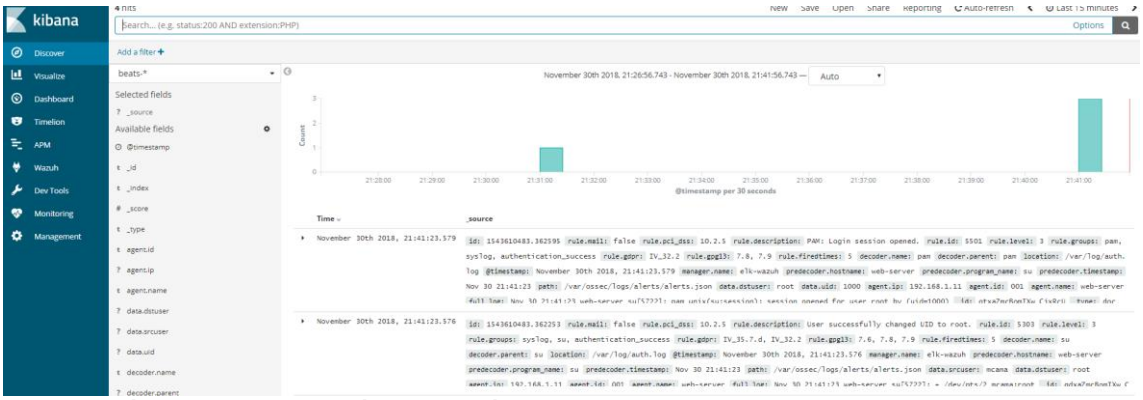


Il·lustració 28 - Creació Índex Pas 1



Il·lustració 29 - Creació Índex Pas 2

Una vegada configura ja podem veure els logs de sistema:



Il·lustració 30 - Comprovació indexació

3.3 Entorn real

En aquestes seccions explicarem les particularitats de la configuració d'una arquitectura distribuïda, perquè són necessàries, i quines possibilitats tenim en cas de que la infraestructura vagi escalant amb diferents nodes. Aquest entorn aniria destinat a una organització de més de 50 servidors amb una tassa d'indexació de més de 1000 shards per segon.

3.3.1 Elasticsearch

Per configurar els paràmetres necessaris per que els nodes formin part d'un cluster necessitarem editar l'arxiu /etc/elasticsearch/elasticsearch.yml. Per l'arquitectura exposada on tindrem un clúster de tres nodes es configuraran els tres com a màster de dades, per tant la configuració serà la mateixa en els tres.

En cas de que necessitéssim més nodes perquè la nostra infraestructura a crescut o estem monitoritzant moltes més dades ens caldrà configurar nodes diferenciats entre màsters i dedicats a dades, d'aquesta manera el flux de les operacions serà molt més àgil i no tindrem problemes d'alentiment amb el que la experiència de l'usuari no es veurà afectada.

```
# ---------------------------------- Cluster -----------------------
----------------
#
# Use a descriptive name for your cluster:
#
cluster.name: elk-elastic
#
# ------------------------------------ Node ------------------------
----------------
#
# Use a descriptive name for the node:
#
node.name: elk-elastic1
```

```
#
# Add custom attributes to the node:
#
#node.attr.rack: r1

#define node 1 as master-eligible:
node.master: true

#define nodes 2 and 3 as data nodes:
node.data: true
…
…
network.host: 10.168.64.10
#
# Set a custom port for HTTP:
#
http.port: 9200
```

Quan tenim més nodes en un mateix clúster haurem de configurar altres paràmetres necessaris per a que el comportament entre els nodes sigui el correcte.

- **discovery.zen.ping.unicast.host**: Necessitarem indicar-li les IP's dels nodes dels clúster, incloent el node en el que estem configurant, així quan es posin en marxa tots els nodes es pugin descobrir entre ells per a que no hi hagi conflictes.

- **discovery.zen.minimum_master_nodes:** En el cas de que la comunicació dels nodes en el clúster falli per un tall de xarxa o perquè un dels nodes s'ha caigut, haurem d'evitar que més d'un node cregui que és el màster provocant inconsistències en les dades. Aquesta variable ens indica quants nodes màster han d'estar en sincronia per escollir un d'ells. Per tant s'haurà de modificar en funció dels nodes màster que hi hagi en el clúster de dades. La millor practica per decidir el numero es utilitzar la fórmula N/2+1 on N és el número de nodes màster del clúster. Si es dones el cas d'un clúster amb 3 màster, posaríem com a valor 2.

```
discovery.zen.ping.unicast.hosts: ["10.168.64.10”,
“10.168.64.14", "10.168.64.15"]
discovery.zen.minimum_master_nodes: 2
```

Un altre punt important és quan ajustem la memòria Heap de Java, per tant s'han de tindre les següents consideracions.

- S'ha de definir com a memòria RAM del servidor un 50% sense sobrepassar mai els 32GB, degut a que JAVA amb quantitats superior a 32GB és totalment ineficaç.

- Alhora de configura el valor de la memòria màxima i mínima s'ha de tindre en compte que han d'estar parells, per tant hauran de tindre sempre el mateix valor.

Si posem en pràctica aquestes consideracions, quan configurem un servidor en el que la memòria RAM sigui de 8GB haurem de definir els següents valors en el fitxer /etc/elasticsearch/jvm.options.

```
# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

-Xms4g
-Xmx4g
```

Un dels problemes que ens trobem amb Elastichsearch és que la utilització del swap provoca de tant en quan una sèrie de desconnexions. En una arquitectura distribuïda on les dades que s'emmagatzemen poden ser crítiques i on les avantatges que ens aporta aquest tipus de configuració és que tots els sistemes estan redundats, i si hi ha algun problema en algun node sempre tenim una via de backup per on no perdrem disponibilitat ni pèrdua de dades. No podem deixar que el clúster presenti inestabilitat en el seu funcionament, per tant s'hauran de fer les següents accions.

- Eliminar el swap del servidor, aquesta acció es farà únicament en aquest tipus d'arquitectura on en el servidor nomes esta instal·lat Elasticsearch.
- Utilitzar mlockall per bloquejar l'accés a la swap per Elasticsearch. Una manera molt efectiva ja que s'estalvien problemes que podem ocorre amb altres serveis.

Per aplicar correctament les configuracions esmentades haurem d'editar l'arxiu /etc/elasticsearch/elasticsearch.yml amb el que habilitarem memory_lock.

```
# ---------------------- Memory -----------------------------
#
# Lock the memory on startup:
#
bootstrap.memory_lock: true
```

Configurarem l'inici d'Elasticsearch en systemd per a permetre el bloqueig de la memòria.

```
root@elk-elastic1:~# systemctl edit elasticsearch
```

Aquesta comanda crea el fitxer /etc/systemd/system/elasticsearch.service.d/override.conf per a modificar els paràmetres d'inici del servei. Afegim el següent contingut al fitxer.

```
[Service]
LimitMEMLOCK=infinity
```

I ja podem recarregar systemd

```
root@elk-elastic1:~# systemctl daemon-reload
```

Una de les modificacions de tuning que s'han fet també en aquesta arquitectura és a /etc/default/elasticsearch, ja que si es vol monitoritzar la memòria de java del servidor al ser una aplicació que funciona amb Tomcat, ens caldrà afegir opcions personalitzades a la variable ES_JAVA_OPTS.

```
# Additional Java OPTS
#ES_JAVA_OPTS=
ES_JAVA_OPTS="-Dcom.sun.management.jmxremote -
Dcom.sun.management.jmxremote.port=9999 -
Dcom.sun.management.jmxremote.rmi.port=9999 -
Dcom.sun.management.jmxremote.ssl=false -
Dcom.sun.management.jmxremote.authenticate=false"
```

Ara que tenim la configuració d'un node del clúster necessitarem configurar el node que balancejarà la carrega entre la resta, per això editarem elasticsearch.yml i afegirem la següent configuració. S'ha de puntualitzar que el transport de dades es configuri amb TCP ja que encara que el fluxe de dades pugui tindre un petit desfasament en el temps serà inapreciable i ens assegurarem que les dades arribin correctament.

```
# ------------------------ Cluster -----------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: elk-elastic
#
# --------------------------- Node -----------------------------

node.name: elk-elasticbal

node.master: false
node.data: false
node.ingest: false
…
…
network.host: 10.168.64.21
#
# Set a custom port for HTTP:
#
http.port: 9200

transport.host: 10.168.64.21
transport.tcp.port: 9300 – 9400
```

```
discovery.zen.ping.unicast.hosts: ["10.168.64.10",
"10.168.64.14", "10.168.64.15"]
discovery.zen.minimum_master_nodes: 2
```

3.3.2 Logstash

Els servidors Logstash que tenim distribuïts per les diferents zones de xarxa ens permeten la recol·lecció de logs de tots els servidors a traves dels agents Beats instal·lats en cadascun d'ells, per permetre que aquest puguin enviar correctament els logs haurem de crear fitxers de configuració on s'especificaran els plugins que volem utilitzar, fitxers d'entrada, ports, destinació de la informació, etc.

El primer pas seria crear el fitxer logstash-beats.conf al directori /etc/logstash/conf.d per configurar la recollida de logs des de Beats per el port 5251, amb el que s'enviaran les dades als nodes master de elasticsearch.

```
input {
  beats {
    port => 5251
 }
}

output {
  elasticsearch {
    hosts =>
["10.168.64.10:9200","10.168.64.14:9200","10.168.64.15:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-
%{+YYYY.MM.dd}"
  }
}
```

Ara ens caldrà crear filtres per tractar les dades que rebrem a traves de Beats, això ens crearà una sèrie d'instàncies que depenent les fonts d'origen ens ho dividirà, per tant en el nostre panell d'administració (Kibana) podrem distingir cada log per aplicació i fer les cerques molt més acurades.

Per el nostre cas crearem diferents filtres primer un per els logs d'Apache.

```
filter {
  if [fileset][module] == "apache2" {
    mutate{
       replace => { "type" => "apache2" }
    }
    if [fileset][name] == "access" {
      grok {
```

```
        match => { "message" =>
["%{IPORHOST:[apache2][access][remote_ip]} -
%{DATA:[apache2][access][user_name]}
\[%{HTTPDATE:[apache2][access][time]}\]
\"%{WORD:[apache2][access][method]}
%{DATA:[apache2][access][url]}
HTTP/%{NUMBER:[apache2][access][http_version]}\"
%{NUMBER:[apache2][access][response_code]}
%{NUMBER:[apache2][access][body_sent][bytes]}(
\"%{DATA:[apache2][access][referrer]}\")?(
\"%{DATA:[apache2][access][agent]}\")?",
          "%{IPORHOST:[apache2][access][remote_ip]} -
%{DATA:[apache2][access][user_name]}
\\[%{HTTPDATE:[apache2][access][time]}\\] \"-\"
%{NUMBER:[apache2][access][response_code]} -" ] }
        remove_field => "message"
      }
      mutate {
        add_field => { "read_timestamp" => "%{@timestamp}" }
      }
      date {
        match => [ "[apache2][access][time]", "dd/MMM/YYYY:H:m:s
Z" ]
        remove_field => "[apache2][access][time]"
      }
      useragent {
        source => "[apache2][access][agent]"
        target => "[apache2][access][user_agent]"
        remove_field => "[apache2][access][agent]"
      }
      geoip {
        source => "[apache2][access][remote_ip]"
        target => "[apache2][access][geoip]"
      }
    }
    else if [fileset][name] == "error" {
      grok {
        match => { "message" =>
["\[%{APACHE_TIME:[apache2][error][timestamp]}\]
\[%{LOGLEVEL:[apache2][error][level]}\]( \[client
%{IPORHOST:[apache2][error][client]}\])?
%{GREEDYDATA:[apache2][error][message]}",
          "\[%{APACHE_TIME:[apache2][error][timestamp]}\]
\[%{DATA:[apache2][error][module]}:%{LOGLEVEL:[apache2][error][l
evel]}\] \[pid %{NUMBER:[apache2][error][pid]}(:tid
%{NUMBER:[apache2][error][tid]})?\]( \[client
%{IPORHOST:[apache2][error][client]}\])?
%{GREEDYDATA:[apache2][error][message1]}" ] }
        pattern_definitions => {
```

```
          "APACHE_TIME" => "%{DAY} %{MONTH} %{MONTHDAY} %{TIME}
%{YEAR}"
        }
        remove_field => "message"
      }
      mutate {
        rename => { "[apache2][error][message1]" =>
"[apache2][error][message]" }
      }
      date {
        match => [ "[apache2][error][timestamp]", "EEE MMM dd
H:m:s YYYY", "EEE MMM dd H:m:s.SSSSSS YYYY" ]
        remove_field => "[apache2][error][timestamp]"
      }
    }
  }
}
```

Filtre per MySQL:

```
filter {
  if [fileset][module] == "mysql" {
    mutate{
       replace => { "type" => "mysql" }
    }
    if [fileset][name] == "error" {
      grok {
        match => { "message" =>
["%{LOCALDATETIME:[mysql][error][timestamp]}
(\[%{DATA:[mysql][error][level]}\]
)?%{GREEDYDATA:[mysql][error][message]}",
          "%{TIMESTAMP_ISO8601:[mysql][error][timestamp]}
%{NUMBER:[mysql][error][thread_id]}
\[%{DATA:[mysql][error][level]}\]
%{GREEDYDATA:[mysql][error][message1]}",
          "%{GREEDYDATA:[mysql][error][message2]}"] }
        pattern_definitions => {
          "LOCALDATETIME" => "[0-9]+ %{TIME}"
        }
        remove_field => "message"
      }
      mutate {
        rename => { "[mysql][error][message1]" =>
"[mysql][error][message]" }
      }
      mutate {
        rename => { "[mysql][error][message2]" =>
"[mysql][error][message]" }
      }
```

```
      date {
        match => [ "[mysql][error][timestamp]", "ISO8601",
"YYMMdd H:m:s" ]
        remove_field => "[mysql][error][time]"
      }
    }
    else if [fileset][name] == "slowlog" {
      grok {
        match => { "message" => ["^# User@Host:
%{USER:[mysql][slowlog][user]}(\[[^\]]+\])? @
%{HOSTNAME:[mysql][slowlog][host]}
\[(IP:[mysql][slowlog][ip])?\](\s*Id:\s*
%{NUMBER:[mysql][slowlog][id]})?\n# Query_time:
%{NUMBER:[mysql][slowlog][query_time][sec]}\s* Lock_time:
%{NUMBER:[mysql][slowlog][lock_time][sec]}\s* Rows_sent:
%{NUMBER:[mysql][slowlog][rows_sent]}\s* Rows_examined:
%{NUMBER:[mysql][slowlog][rows_examined]}\n(SET
timestamp=%{NUMBER:[mysql][slowlog][timestamp]};\n)?%{GREEDYMULT
ILINE:[mysql][slowlog][query]}"] }
        pattern_definitions => {
          "GREEDYMULTILINE" => "(.|\n)*"
        }
        remove_field => "message"
      }
      date {
        match => [ "[mysql][slowlog][timestamp]", "UNIX" ]
      }
      mutate {
        gsub => ["[mysql][slowlog][query]", "\n# Time: [0-9]+
[0-9][0-9]:[0-9][0-9]:[0-9][0-9](\\.[0-9]+)?$", ""]
      }
    }
  }
}
```

Filtre per nginx:

```
filter {
  if [fileset][module] == "nginx" {
    mutate{
       replace => { "type" => "nginx" }
    }
      if [fileset][name] == "access" {
      grok {
        match => { "message" =>
["%{IPORHOST:[nginx][access][remote_ip]} -
%{DATA:[nginx][access][user_name]}
\[%{HTTPDATE:[nginx][access][time]}\]
\"%{WORD:[nginx][access][method]} %{DATA:[nginx][access][url]}
```

```
HTTP/%{NUMBER:[nginx][access][http_version]}\"
%{NUMBER:[nginx][access][response_code]}
%{NUMBER:[nginx][access][body_sent][bytes]}
\"%{DATA:[nginx][access][referrer]}\"
\"%{DATA:[nginx][access][agent]}\""] }
        remove_field => "message"
      }
      mutate {
        add_field => { "read_timestamp" => "%{@timestamp}" }
      }
      date {
        match => [ "[nginx][access][time]", "dd/MMM/YYYY:H:m:s
Z" ]
        remove_field => "[nginx][access][time]"
      }
      useragent {
        source => "[nginx][access][agent]"
        target => "[nginx][access][user_agent]"
        remove_field => "[nginx][access][agent]"
      }
      geoip {
        source => "[nginx][access][remote_ip]"
        target => "[nginx][access][geoip]"
      }
    }
    else if [fileset][name] == "error" {
      grok {
        match => { "message" => ["%{DATA:[nginx][error][time]}
\[%{DATA:[nginx][error][level]}\]
%{NUMBER:[nginx][error][pid]}#%{NUMBER:[nginx][error][tid]}:
(\*%{NUMBER:[nginx][error][connection_id]}
)?%{GREEDYDATA:[nginx][error][message]}"] }
        remove_field => "message"
      }
      mutate {
        rename => { "@timestamp" => "read_timestamp" }
      }
      date {
        match => [ "[nginx][error][time]", "YYYY/MM/dd H:m:s" ]
        remove_field => "[nginx][error][time]"
      }
    }
  }
}
```

Filtre per els logs de sistema:

```
filter {
  if [fileset][module] == "system" {
```

```
    mutate{
       replace => { "type" => "syslog" }
    }
      if [fileset][name] == "auth" {
      grok {
        match => { "message" =>
["%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?:
%{DATA:[system][auth][ssh][event]}
%{DATA:[system][auth][ssh][method]} for (invalid user
)?%{DATA:[system][auth][user]} from
%{IPORHOST:[system][auth][ssh][ip]} port
%{NUMBER:[system][auth][ssh][port]} ssh2(:
%{GREEDYDATA:[system][auth][ssh][signature]})?",
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?:
%{DATA:[system][auth][ssh][event]} user
%{DATA:[system][auth][user]} from
%{IPORHOST:[system][auth][ssh][ip]}",
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
sshd(?:\[%{POSINT:[system][auth][pid]}\])?: Did not receive
identification string from
%{IPORHOST:[system][auth][ssh][dropped_ip]}",
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
sudo(?:\[%{POSINT:[system][auth][pid]}\])?:
\s*%{DATA:[system][auth][user]} :(
%{DATA:[system][auth][sudo][error]} ;)?
TTY=%{DATA:[system][auth][sudo][tty]} ;
PWD=%{DATA:[system][auth][sudo][pwd]} ;
USER=%{DATA:[system][auth][sudo][user]} ;
COMMAND=%{GREEDYDATA:[system][auth][sudo][command]}",
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
groupadd(?:\[%{POSINT:[system][auth][pid]}\])?: new group:
name=%{DATA:system.auth.groupadd.name},
GID=%{NUMBER:system.auth.groupadd.gid}",
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
useradd(?:\[%{POSINT:[system][auth][pid]}\])?: new user:
name=%{DATA:[system][auth][user][add][name]},
UID=%{NUMBER:[system][auth][user][add][uid]},
GID=%{NUMBER:[system][auth][user][add][gid]},
home=%{DATA:[system][auth][user][add][home]},
shell=%{DATA:[system][auth][user][add][shell]}$",
```

```
                  "%{SYSLOGTIMESTAMP:[system][auth][timestamp]}
%{SYSLOGHOST:[system][auth][hostname]}
%{DATA:[system][auth][program]}(?:\[%{POSINT:[system][auth][pid]
}\])?: %{GREEDYMULTILINE:[system][auth][message]}"] }
        pattern_definitions => {
          "GREEDYMULTILINE"=> "(.|\n)*"
        }
        remove_field => "message"
      }
      date {
        match => [ "[system][auth][timestamp]", "MMM  d
HH:mm:ss", "MMM dd HH:mm:ss" ]
      }
      geoip {
        source => "[system][auth][ssh][ip]"
        target => "[system][auth][ssh][geoip]"
      }
    }
    else if [fileset][name] == "syslog" {
      grok {
        match => { "message" =>
["%{SYSLOGTIMESTAMP:[system][syslog][timestamp]}
%{SYSLOGHOST:[system][syslog][hostname]}
%{DATA:[system][syslog][program]}(?:\[%{POSINT:[system][syslog][
pid]}\])?: %{GREEDYMULTILINE:[system][syslog][message]}"] }
        pattern_definitions => { "GREEDYMULTILINE" => "(.|\n)*"
}
        remove_field => "message"
      }
      date {
        match => [ "[system][syslog][timestamp]", "MMM  d
HH:mm:ss", "MMM dd HH:mm:ss" ]
      }
    }
  }
}
```

Aquest casos anteriors han sigut quatre exemples de com filtrar els logs de les aplicacions més populars d'un servidor, però també ens podem trobar que vulguem monitoritzar els logs d'un sistema on no puguem instal·lar un agent Beats que ens redirigeixi els logs que vulguem analitzar, per tant tal i com hem fet amb el fitxer anterior, que s'ha creat una entrada per rebre tota la informació de beats, crearem un altre entrada per rebre els logs de per exemple el dispositius de xarxa de les facultats, per això es crearà un nou fitxer anomenat logstash-cores.conf on editarem el port per on escoltarà i rebrà tot el tràfic de syslog i després es configurarà el filtre corresponent amb la sortida de dades cap el servidor logstash.

```
input {
    udp {
        port => 5252
        type => inputType
        codec => plain {
                charset => "ISO-8859-1"
        }
    }
}

filter {
  if [type] == "core" {
    grok {
      match => { "message" =>
"%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?:
%{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd
HH:mm:ss" ]
    }
  }
}

output {
  elasticsearch {
    hosts =>
["10.168.64.10:9200","10.168.64.14:9200","10.168.64.15:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-
%{+YYYY.MM.dd}"
  }
}
```

Un dels problemes que ens em trobat amb aquest mètode és alhora de enviar els logs dels sistemes solaris amb la versió Spark, ja que no són compatibles amb l'agent Beats, per tant s'ha hagut de recorre a una solució alternativa.

Primer de tot tenim que el servidor solaris utilitza el port 514 per enviar el syslog a logstash, però logstash no permet configurar aquest port per un altre fi, ja que te reservat per a sistema del port 1 al 1024. Per tant el que farem serà reenviar tot el tràfic que entri per aquest port cap al UPD/5253 amb una política del FW.

```
#LOGSTASH
LOGSTASH(ACCEPT)    net      $FW
REDIRECT        net     5253    udp     514
```

Una vegada tinguem això configurat ja podrem crear un nou input que escolti per el port 5253 i que permeti rebre aquests logs.

Crearem el fitxer /etc/logstash/conf.d/logstash-solaris.conf i posarem la següent informació, com a detall de la configuració ens em trobat que al rebre els logs solaris envia la IP del host però no el nom, amb el que s'ha afegit una funció 'mutate' que ens resol la IP i en fa el canvi per el nom DNS, amb això guanyarem que si estem revisant els logs podem identificar ràpidament de quin servidor estem observant el log.

```
input {
    udp {
        port => 5253
        type => "apache-solaris"
    }
}

filter {
  if [type] in [ "apache" , "apache_access" , "apache-access",
"apache-solaris" ]  {
    mutate {
      add_field => { "hostname" => "%{host}" }
    }
    dns {
      action => "replace"
      reverse => [ "hostname" ]
    }
    if [message] =~ "httpd" {
     grok {
         match => [
         "message" ,
"%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra_fields}",
         "message" ,
"%{COMMONAPACHELOG}+%{GREEDYDATA:extra_fields}"
         ]
         overwrite => [ "message" ]
      }
      mutate {
         convert => ["response", "integer"]
         convert => ["bytes", "integer"]
         convert => ["responsetime", "float"]
      }
      geoip {
```

```
         source => "clientip"
         target => "geoip"
         add_tag => [ "apache-geoip" ]
      }
      date {
         match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]
         remove_field => [ "timestamp" ]
      }
      useragent {
         source => "agent"
      }
   }
   if [message] =~ "syslog" {
        mutate{
                replace => { "type" => "syslog-solaris" }
        }
        grok {
        match => { "message" =>
["%{SYSLOGTIMESTAMP:[system][syslog][timestamp]}
%{SYSLOGHOST:[system][syslog][hostname]}
%{DATA:[system][syslog][program]}(?:\[%{POSINT:[system][syslog][
pid]}\])?: %{GREEDYMULTILINE:[system][syslog][message]}"] }
        pattern_definitions => { "GREEDYMULTILINE" => "(.|\n)*"
}
        remove_field => "message"
      }
      date {
        match => [ "[system][syslog][timestamp]", "MMM  d
HH:mm:ss", "MMM dd HH:mm:ss" ]
      }
   }
 }
 if [type] in ["apache_error","apache-error"] {
      grok {
         match => ["message", "\[%{WORD:dayname} %{WORD:month}
%{DATA:day} %{DATA:hour}:%{DATA:minute}:%{DATA:second}
%{YEAR:year}\] \[%{NOTSPACE:loglevel}\] (?:\[client
%{IPORHOST:clientip}\] ){0,1}%{GREEDYDATA:message}"]
         overwrite => [ "message" ]
      }
      mutate
      {
         add_field =>
         {
            "time_stamp" =>
"%{day}/%{month}/%{year}:%{hour}:%{minute}:%{second}"
         }
      }
      date {
```

```
        match => ["time_stamp", "dd/MMM/YYYY:HH:mm:ss"]
        remove_field => [
"time_stamp","day","dayname","month","hour","minute","second","y
ear"]
      }
   }
}
```

Per últim i donat aquesta configuració també s'ha observat que les consultes DNS dels servidors creixia força amb el que s'ha instal·lat el paquet dnsmasq per a que resolgui localment aquest noms sense fer peticions al DNS i satura-ho.

3.3.3 Kibana

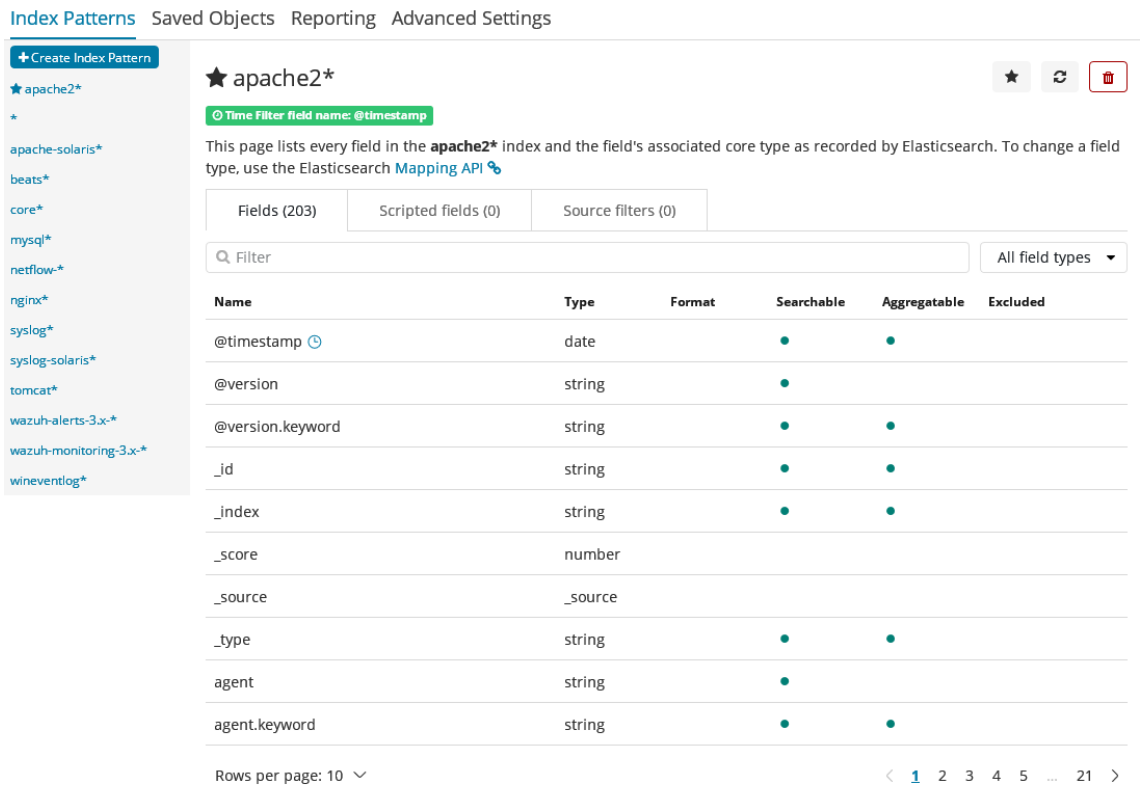
Una de les problemàtiques que sorgeixen alhora de tindre una configuració distribuïda, es que si tenim un clúster de nodes d'Elasticsearch que gestionen totes les dades ells es distribueixen aquestes d'una manera aleatòria segons ho consideren amb el que quan realitzem cerques amb Kibana no podem apuntar nomes a un d'ells, ni tampoc apuntar als tres alhora, per aquest casos s'ha d'introduir un nou element que pugui gestionar aquesta circumstancia, es a dir un node balancejador que estigui sincronitzat amb els nodes màster de dades i pugi extreure dita informació. Per tant en la configuració de kibana.yml haurem d'especificat el servidor encarregat de balancejar la carrega.

```
elasticsearch.url: "http://10.168.64.21:9200"
```

Una vegada configurat això també podem observar com encara que un dels nodes produeixi una caiguda la informació segueix sent accessible ja que el node balancejador s'encarrega de tota la gestió.

**A l'apartat 3.4.4.3 podrem veure les conseqüències de la caiguda d'un dels nodes.*

Una vegada es rebin tots els logs dels diferents softwares s'hauran de classificar per a mostra-ho al panell d'administració d'una manera ordenada per això ens dirigirem a Management → Kibana → Index Patterns → Create Index Patterns. En aquest apartat veurem com buscant les paraules claus del software a monitoritzar ja ens apareixerà perquè s'ha fet un filtratge previ en el servidor de Logstash amb el que simplement hauríem de posar un asterisc en substitució de la data del log ja que anirà variant en el transcurs del temps.



Il·lustració 31 - Index Patterns

D3.4 Exemple d'ús

En aquest apartat s'explicarà la part operacional en la utilització de la plataforma SIEM muntada i totes les tasques operatives de la que s'encarrega un equip de seguretat.

3.4.1 Procés de Detecció, Anàlisi i Monitorització d'incidents

Per la monitorització, detecció i anàlisi dels incidents de seguretat generats per la plataforma SEIM s'encarregarà el centre d'operacions de seguretat (SOC), aquets són un conjunt d'equips de persones format per diferents perfils de professionals, les seves tasques són descartar fals positius de les alertes generades, detecció de vulnerabilitats, intrusions als sistemes, desfasaments, o qualsevol altre tipus d'incident que pugi suposar un problema de seguretat per la organització.

En el nostre cas estem parlant de tres nivells per on passarà una alerta abans de passar a estat resolt o ser descartada.

El primer nivell tenim els operadors que revisaran les alertes creades automàticament, aquí es seguiran una sèrie de pautes ja definides on segons si la alerta és coneguda o els patrons són els indicats es descartarà la alerta i es tancarà el tiquet generat o per el contrari s'ha d'escalar al següent nivell.

Quan un cas arriba al nivell dos del organigrama, els analistes s'encarreguen de revisar exactament perquè s'ha produït quin ha sigut el motiu del origen i

quines son les possibles causes, per fer aquest anàlisi es recolzen en les diferents eines de seguretat, el propi SIEM on es pot fer anàlisi forense gracies a que s'emmagatzemen tots els logs dels sistemes, analitzadors de xarxa, IDS, etc. Una vegada tretes les conclusions, hi ha tres possibilitats:

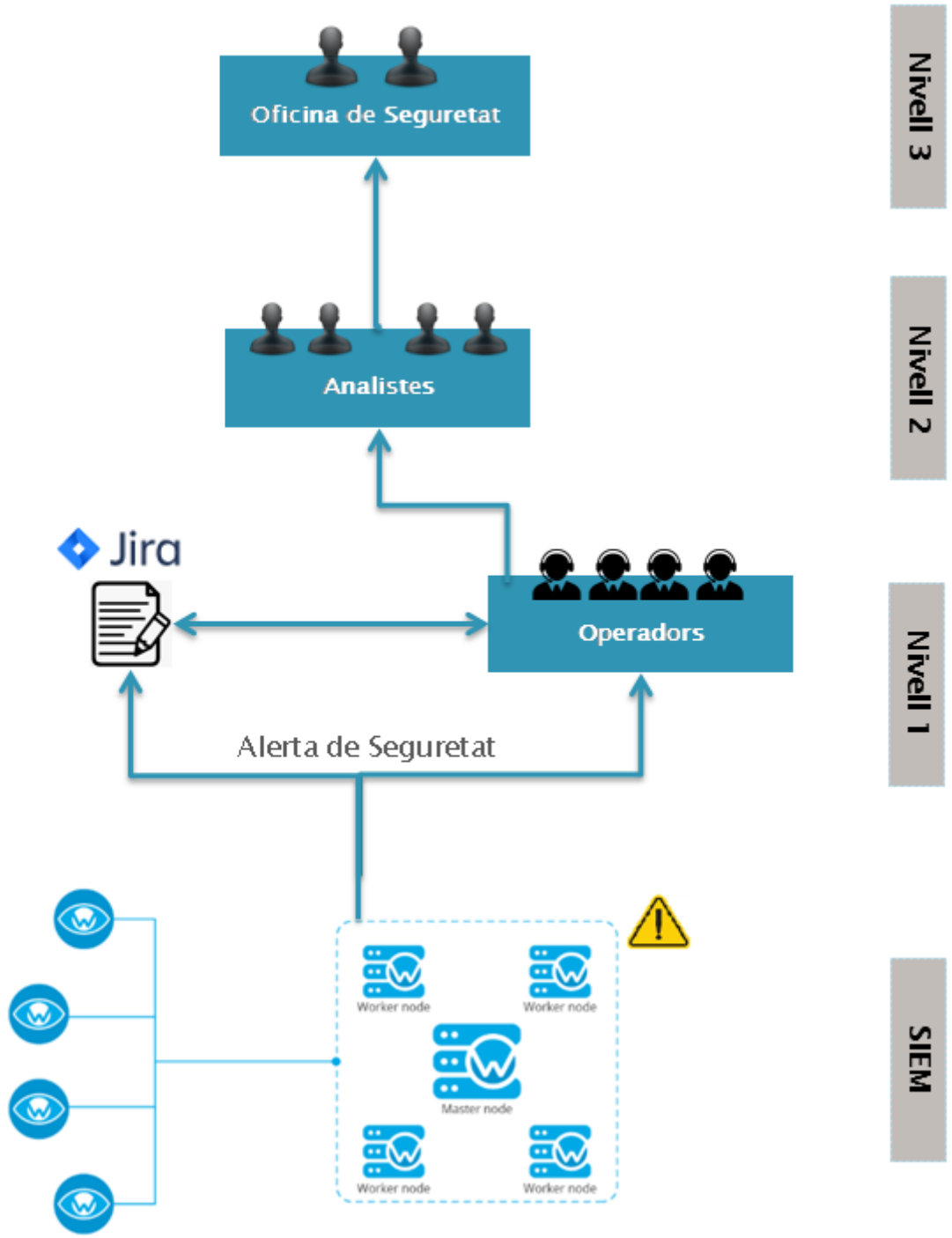
- L'incident pot ser descartat, per tant es tornaria el tiquet obert als operadors amb la resolució del incident i es donaria per tancat.

- L'incident s'ha produït i s'han detectat les causes, per tant es faria un estudi del impacte que ha tingut per la organització i quin alcans podria haver tingut. A més s'identificarà la alerta i es documentarà amb el que es traslladarà tota la informació als operadors per agilitzar les futures alertes i determinar les possibles accions.

- No s'ha pogut determinar l'origen del incident, en aquest cas s'escalarà a la oficina de seguretat.

Per últim tenim el nivell tres del organigrama, les funcions que fa l'oficina de seguretat són coordinació de les accions que s'han de prendre quan es produeix un incident, establiment de les polítiques de seguretat, detectar amenaces que el SIEM no sigui capaç de detectar automàticament, parlar amb altres organismes de seguretat per fer col·laboracions conjuntes i coordinar-se amb els analistes de nivell dos per realitzar anàlisis de gestió e riscos per la organització. Per tant quan un dels tiquets arriba a la oficina de seguretat es dedicaran a treballar conjuntament amb els analistes de nivell dos per veure el procediment de detecció quin ha estat el problema i com solucionar-ho, una vegada tretes totes les conclusions i tindre clares les accions a prendre es documentarà tot el procés i es tornarà als operadors perquè es tanqui el cas.

Una de les particularitats del SOC de la universitat és que al ser un organisme públic també te una part del SOC externalitat, ja que està sota del paraigües de la administració i la xarxa està constantment monitoritzada per INCIBE, CESICAT i CESUC amb el que els operadors de nivell 1 també reben notificacions d'aquest organismes què s'hauran de tractar per igual. A més anualment s'ha de passar una auditoria de la organització (esquema nacional de seguretat) establert per el CCN-CERT.



Il·lustració 32 - Flux de detecció d'incident

3.4.2 Gestió de riscos

A l'apartat anterior s'ha explicat el procés que segueix una alerta de seguretat des del moment que es genera fins que es tanca, en aquest procés hi ha una part de gestió de riscos on es comptabilitza l'impacte que tenen les amenaces que es produeixen per a una organització. Tot seguit detallarem en que consisteix una gestió de riscos i que s'ha de tindre en compte per realitzar-la correctament.

Per el disseny i la implantació del procés de gestió de riscos, s'han utilitzat diverses metodologies de l'àmbit de seguretat TI. Concretament s'ha utilitzat RiskIT per la gestió de riscos, i la ISO 27001/COBIT per la identificació de les amenaces i controls de seguretat.

3.4.2.1 Definició del risc i l'abast de la gestió de riscos

El primer pas per la correcta gestió de riscos és la identificació del risc el qual s'engloba en:

- Processos de negoci a analitzar.
- Activitats que componen cada un dels processos de negoci.
- Dependències i relacions entre activitats i processos.
- Aplicacions i infraestructura de suport als processos de negoci mitjançant la prestació de serveis de TI. Cal destacar que la gestió dels riscos TI ha de ser vist des de la perspectiva de l'activitat extrem a extrem, tenint especial èmfasi en les funcions TI (operacions de TI, gestió de projectes d'infraestructura, desenvolupament d'aplicacions, recuperació davant desastres, seguretat , etc.)

Per a la identificació dels processos i activitats s'ha de partir de l'anàlisi inicial de l'àmbit d'aplicació de la Gestió de Riscos, en aquest cas per als serveis d'Administració de Sistemes i Aplicacions i els processos de negoci als quals donen suport. Aquest anàlisi s'ha de realitzar durant la fase de Transició.

Per cadascuna de les amenaces s'ha d'emplenar la següent fitxa, tenint en compte els impactes i les probabilitats que apareguin.

❖ Valoració de la freqüència /probabilitat

Per valorar la freqüència del risc (probabilitat que sigui efectiva una amenaça) es proposa tenir en compte l'historial d'incidències anteriors. La valoració per amenaça es realitza en funció de les vegades/any:

Freqüència (vegades/any)	1	2	3	4	5
	0<I≤2 ☐	2<I≤4 ☐	4<I≤6 ☐	6<I≤8 ☐	8<I ☐

En el cas que no hi hagi possibilitat de mesurament en base a evidències reals, es tindrà en compte un factor de probabilitat d'ocurrència basat en estimacions subjectives.

❖ Valoració del impacte

Per la valoració de l'impacte, la metodologia proposada serà d'un model basat en subcriteris d'impactes, aquests mesuren l'impacte d'un risc a partir dels serveis de la organització.

En aquest sentit és imprescindible tenir alineades les activitats de gestió de riscos amb:

- La **criticitat de les aplicacions** donant més rellevància a aquelles amb major valor per a la organització. En el cas d'una universitat seria el servei de matrícula i campus virtual.
- La **criticitat de cada implantació** en producció de nous elements d'infraestructura, productes, actualitzacions de sistema o redimensionament d'elements ja existents, raó per la qual es realitzarà una anàlisi de riscos per cada pujada a producció, avaluant dependències, precisió de la documentació, recursos necessaris en base als riscos detectats, etc.

La pèrdua de disponibilitat dels serveis més crítics en termes de negoci, el cost associat a l'impacte legal de la no disponibilitat o el cost de les mesures necessàries per posar en marxa accions pal·liatives són part dels subcriteris a considerar.

Els cinc criteris per calcular l'impacte en cas de materialitzar un risc, es basen en la classificació següent:

Tecnologia	Mida	Complexitat	Criticitat	Horari

- Pèrdua de Disponibilitat:

Disponibilitat	1	2	3	4	5
Valoració del impacte	0<I≤2h ☐	2h<I≤8h ☐	8h<I≤12h ☐	12h<I≤24h ☐	24h<N ☐

On L és el temps que pot deixar sense servei una amenaça activa. Es basa en l'horari d'atenció requerit per a aquesta aplicació o servei.

- Cost de la resposta/contramesures:

Cost de la resposta	1	2	3	4	5
Valoració del impacte	0<I≤1K€ ☐	1K€<I≤6K€ ☐	6K€<I≤15K€ ☐	15K€<I≤25K€ ☐	25K€<N ☐

On L és la suma del cost d'implantar les contramesures per eliminar l'amenaça. Per a això s'ha de tenir en compte els possibles costos de la no disponibilitat del servei que es podran calcular tenint en compte els costos per la pèrdua de productivitat de l'usuari, pèrdua de productivitat informàtica pèrdua d'ingressos o impactes sobre el servei als clients. Cost dels plans d'acció a posar en marxa per mitigar o reaccionar davant els riscos.

- Criticitat del servei:

Satisfacció del client	1	2	3	4	5
Valoració del impacte	Nul·la ☐	Mínima ☐	Mitja ☐	Alta ☐	Molt Alta ☐

En aquest punt es tindrà en compte la criticitat pel que fa al destinatari del servei i del negoci.

- Impacte legal y penalitzacions:

Impacte legal i penalitzacions	1	2	3	4	5
Valoració del impacte	0<I≤600€ ☐	600€<I≤6K€ ☐	6K€<I≤25K€ ☐	25K€<I≤100K€ ☐	100K€<N ☐

Aquest subcriteri té especial rellevància amb les aplicacions que poden suposar variació dels ingressos o fins i tot devolucions d'ingressos previs.

- Impacte total:

Aquest impacte es calcula segons la formual I=(I1+I2+I3+I4)/4 ponderant la escala segons la següent taula:

	0<I≤5	5<I≤10	10<I≤15	15<I≤20	20<I≤25
Valoració del impacte	Insignificant (1)	Baix (2)	Mitja (3)	Alt (4)	Crític (5)

Amb la incorporació d'aquest criteri en la valoració dels riscos, es completa l'objectivitat del seu càlcul al poder, sobre la base de lliçons apreses, estimacions per volums d'activitat, etc.

❖ Mapa de riscos

Per poder determinar si els riscos detectats són importants o no, i poder ordenar l'actuació preventiva, cal poder classificar aquests riscos en funció de la seva magnitud. Per a això, es procedirà determinant el valor del risc (R) com el producte resultant d'analitzar la seva probabilitat d'aparició o freqüència (N) per l'impacte que aquest provocaria en el projecte (S). Per obtenir un valor homogeni al llarg del servei es seguirà la taula següent:

Valor del risc R=SxN		Probabilitat del Risc (N)				
		Molt Baix (1)	Baix (2)	Mitja (3)	Alt (4)	Molt Alt (5)
Impacte / risc del severitat (S)	Insignificant (1)	1	2	3	4	5
	Baix (2)	2	4	6	8	10
	Mitjà (3)	3	6	9	12	15
	Alt (4)	4	8	12	16	20
	Crític (5)	5	10	15	20	25

Per tal que el tractament del risc sigui adequat, tota amenaça que estigui dins dels quadres verds (valor del risc <10) serà acceptat per l'organització. Les marcades en groc (10<R<15) i les tractades en vermell hauran de tractar (acceptació, transferència, mitigació o eliminació).

En finalitzar l'avaluació de cada amenaça es disposarà d'un mapa de risc que permetrà veure de forma ràpida, la situació de risc de cada procés.

- Tractament del risc

  Un cop identificades les amenaces i l'impacte de cadascuna d'elles, en cada procés s'identificarà què fer amb i quins controls / contramesures s'hauran d'aplicar per eliminar el risc o mitigar-lo.

Aquelles amenaces que estiguin dins dels paràmetres acceptables no es tractaran ja que l'organització els accepta. Per a aquells que estiguin fora del rang d'acceptació es realitzarà alguna de les accions següents: transferència del risc, mitigació o eliminació. Per a això es seleccionaran els controls oportuns i la seva justificació.

3.4.2.2 Flux de treball en la gestió de riscos

El flux de treball de la gestió de riscos es descriu esquemàticament en els següents punts:

1. Definir l'abast de l'anàlisi de risc. Definir els objectius i les limitacions de l'anàlisi, tenint en compte les aportacions de diverses qüestions estratègiques per a la investigació dels fets freqüents. Aquest pas es realitza amb la participació dels diferents responsables de cada servei, ja que han de participar en la decisió sobre els actius i àrees a tenir en compte.

2. Recollida de dades. Assegurar-se que s'utilitzen totes les fonts possibles de recopilació de dades rellevants en relació amb esdeveniments que van donar lloc a un resultat positiu i / o impacte negatiu sobre el negoci. Això inclou les eines de gestió d'incidents TI, informes d'auditoria i de registre de canvis, així com els informes de risc, com les tecnologies d'anàlisi de tendències i canvis regulatoris.

3. Identificar els factors comuns de risc. Assegurar-se que els esdeveniments que estan relacionats entre si estan agrupats al voltant dels factors de risc comuns. Aquests factors poden influir en la freqüència i magnitud dels esdeveniments que tenen un impacte significatiu en el negoci.

4. Estimació de riscos de TI. Efectuar l'anàlisi real per estimar la freqüència i magnitud dels escenaris, tenint en compte els factors de risc.

5. La tolerància al risc definida. Això servirà de base per a la determinació de la resposta al risc. S'ha d'identificar les opcions de resposta de risc. Aquest pas s'ha de realitzar en cooperació amb els propietaris rellevants dels processos empresarials que depenen de les àrees d'IT que estan sent avaluats.

6. Selecció dels controls per mitigar / eliminar / transferir el risc.

7. Procés d'aprovació per part del responsable de cada servei per aprovar els controls proposats i del risc residual.

8. Implantació de les contramesures propostes en els entorns de producció afectats.

9. Revisió de la implantació de les contramesures, analitzant si l'efectivitat dels controls és l'adequat.

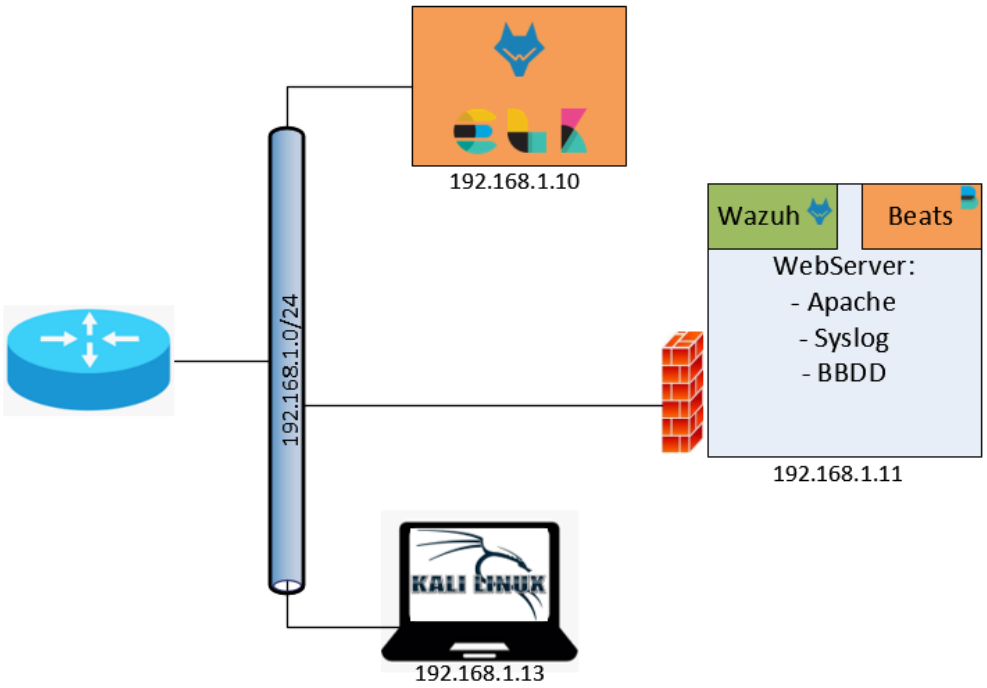
3.4.3 Test d'intrusió

En aquest apartat veurem el tipus d'alarmes que genera aquest sistema referent a intrusions, perquè passen i com solucionar-les. Com s'estan comparant els dos entorns es faran unes petites simulacions al entorn de laboratori per veure com es generen les alarmes, i després es mostraran alarmes reals en el sistema distribuït.

3.4.3.1 Entorn laboratori

Per generar les alarmes del agent wazuh instal·lat al servidor web instal·larem en una nova màquina virtual amb la distribució Kali Linux on farem les proves de simulació d'atacs, les característiques per aquesta màquina són les següents:

	Kali-Linux
IP	192.168.1.13
Memòria	2GB
CPU's	2 cores
Disc	15GB
S.O.	Kali 2018.4 x64
Memòria de Vídeo	32MB



Il·lustració 33 - Arquitectura test

3.4.3.1.1 Força bruta

Mitjançant aplicacions com Hydra o Burp suite podem realitzar proves d'accés a diferents serveis mitjançant diccionari, si fem la prova amb el servei de SSH del servidor web-server (192.168.1.11) podem veure que ens surt el següent missatge a Wazuh indicant-nos que s'està fallant la paraula de pas.

Els atacs per força bruta per regla general son relativament fàcils d'evitar, a no ser que siguis un objectiu fitxat i que et vulguin treure informació dels teus sistemes sigui com sigui. Normalment un atac de força bruta s'inicia perquè amb anterioritat han fet un escaneig de la teva xarxa (fase de descobriment) i han localitzat que hi ha un servei obert. Aquests tipus d'escaneigs no es fan a tots els ports TCP ja que un escaneig massiu a tots els ports TCP trigaria dies en realitzar-se. Per tant es cerquen una sèrie de protocols determinats per després poder fer la fase d'atac. Per tant una manera bastant efectiva i senzilla és canviar el port del servei i no utilitzar el port per defecte, és a dir el servei SSH l'obrirem per el port TCP/2244 que no és un port estàndard de cap servei.

Tot i que tinguem canviat el port per defecte del servei, aquest seguirà escoltant i estant desprotegit, per tant sempre que configurem un servei que està exposat a possibles atacants s'ha de revisar les configuracions addicionals e intentar protegir-lo. Amb OpenSSH tenim moltes possibilitats de configuracions com limitar el número d'intents fallits amb el que després bloquejarem la IP per a que no ho seguis intentant o la utilització de la tècnica (knocking), que el servei nomes s'obrirà si abans s'ha intentat establir la connexió amb altres serveis en un ordre determinat.

Table JSON View surrounding documents View single document

@timestamp		November 30th 2018, 17:45:23.269
t _id		zx5CZWcBZypW9-N-s2MU
t _index		wazuh-alerts-3.x-2018.11.30
# _score		-
t _type		wazuh
t agent.id		001
t agent.ip		192.168.1.11
t agent.name		web-server
t data.dstuser		root
t data.srcip		192.168.1.13
t decoder.name		sshd
t decoder.parent		sshd
t full_log		Nov 30 17:45:21 web-server sshd[4177]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.13 user=root
t id		1543596323.72769
t location		/var/log/auth.log
t manager.name		elk-wazuh
t path		/var/ossec/logs/alerts/alerts.json
t predecoder.hostname		web-server
t predecoder.program_name		sshd
t predecoder.timestamp		Nov 30 17:45:21
t rule.description		syslog: User missed the password more than one time
# rule.firedtimes		2
t rule.gdpr		IV_35.7.d, IV_32.2
t rule.gpg13		7.8
t rule.groups		syslog, access_control, authentication_failed
t rule.id		2502
# rule.level		10
rule.mail		false
t rule.pci_dss		10.2.4, 10.2.5

Il·lustració 34 - Log força bruta

3.4.3.1.2 Escalat de privilegis

En la següent captura podem observar la monitorització de fitxers i com un atacant utilitzant una vulnerabilitat del servidor per escalar privilegis i modificar el fitxer passwd.

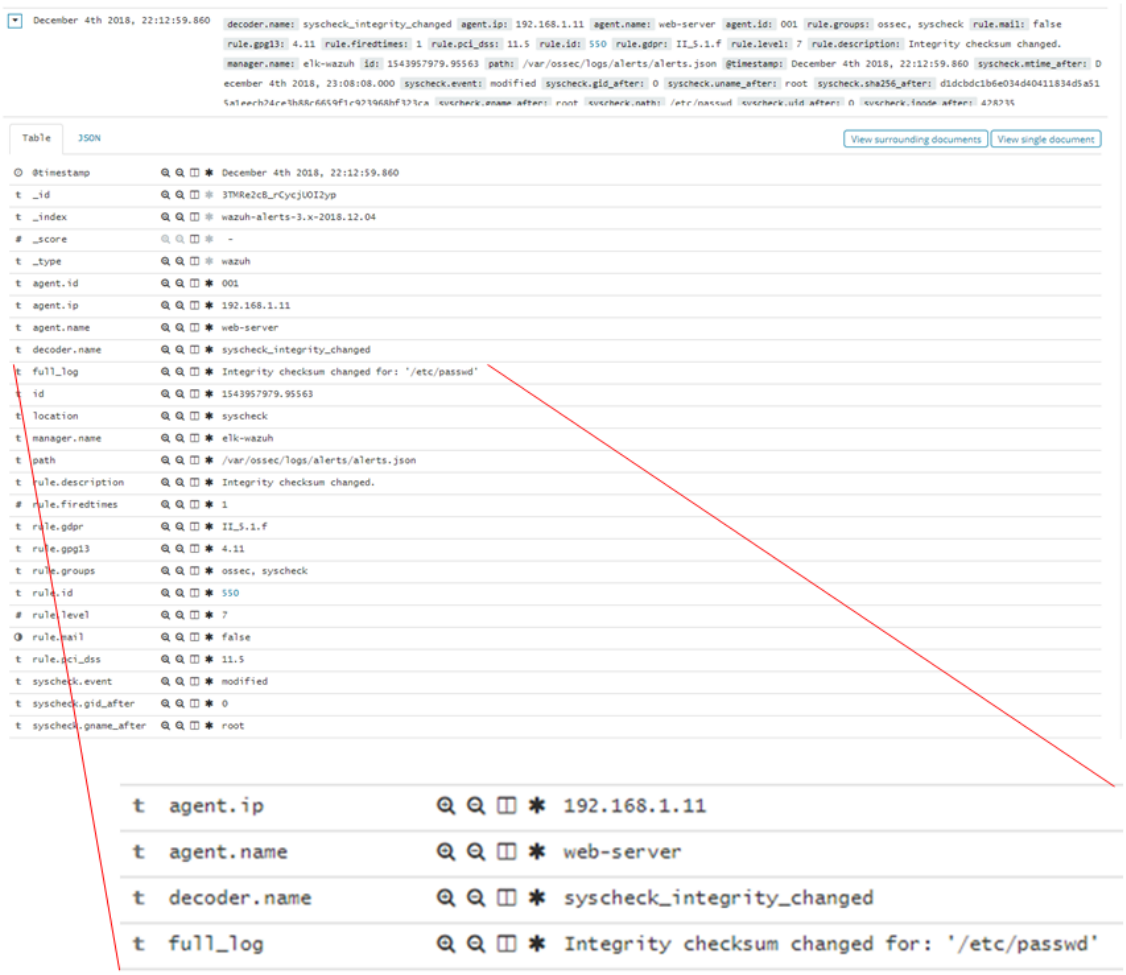
Principalment un escalat de privilegis ve donat per paraules de pas dèbils, vulnerabilitats en la aplicació o vulnerabilitats en el propi sistema operatiu.

Les polítiques de seguretat referent a les paraules de pas indiquen que la majoria de les vulneracions venen degudes a filtració de paraules de pas per vulnerabilitats en les bases de dades com per exemple MongoDB, que ha sigut víctima de diversos atacs gracies a les vulnerabilitats presentades. Per tant la manera per evitar aquests tipus d'atacs són utilitzar paraules de pas amb un requisits mínims de seguretat (majúscules, caràcters especials, números, etc.), utilitzar paraules de pas diferents en cada aplicació que s'utilitzi i canviar-les periòdicament. Una manera senzilla de gestionar això és la utilització d'un gestor de paraules de pas multiplataforma.

Un altre del casos és les vulnerabilitats de les aplicacions que s'utilitzen en els webs, normalment això es produeix en formularis o camps de text on es pugui utilitzar el verb POST i fent diferents tipus de proves trobis la manera que el servidor es retorni informació confidencial i acabis accedint a ell. Per tant s'ha de tindre molta cura i validar les dades que es poden introduir en els formularis d'una plana web.

Finalment tenim les pròpies vulnerabilitats del sistema operatiu, en aquest cas és la que te menys afectació te normalment, ja que els fabricants alliberen pegats de seguretat ràpidament i la difusió que es pugi tindre és molt més gran

que una aplicació que utilitzis en el teu servidor o una que hagis programat tu mateix, que en aquest cas no es tindria cap tipus de difusió externa.



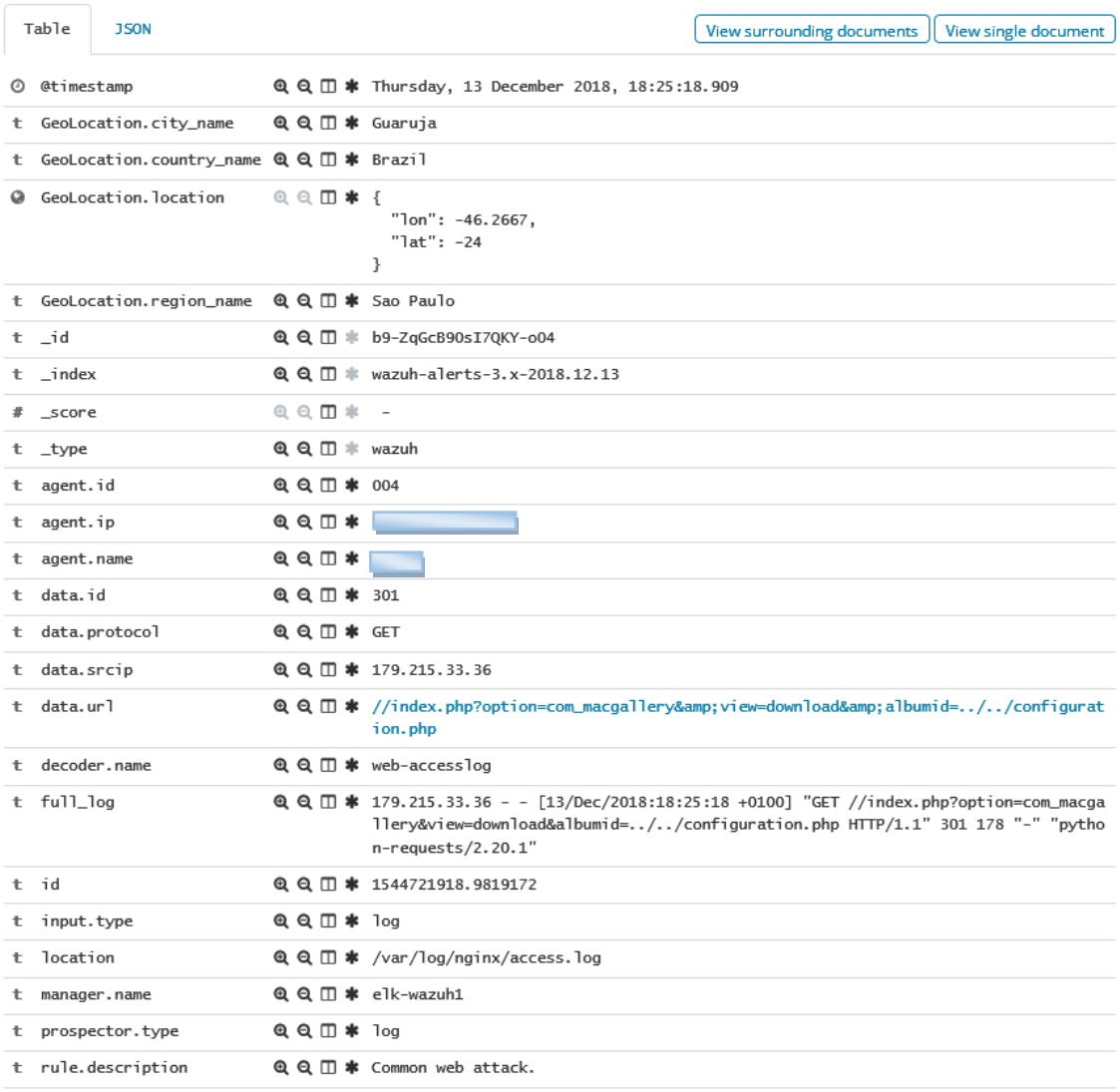
Il·lustració 35 - Log escalat de privilegis

3.4.3.2 Entorn real

3.4.3.2.1 Directory Traversal

Aquesta vulnerabilitat és una de les més conegudes, si mirem a OWASP la consideren la cinquena en el seu TOP10 de vulnerabilitats més perilloses i de més afectació. Si revisem les explicacions de OWASP i determinem els motius per el qual pot succeir una vulnerabilitat de 'path tranversal' podem deduir que el principal motiu és quan no es fa una gestió correcta dels paràmetres que rebem del client que realitza les peticions, exactament es produiria alhora de demanar un recurs específic amb un accés determinat es a dir la incorrecta autorització en els arxius i directoris de la nostra aplicació.

Per tant si un atacant modificant les entrades de les peticions construís un path que coincidís amb el directori del servidor podria saltar-se la restricció i navegar a traves seu arribant al sistema d'arxius del propi sistema, aquesta construcció de path es realitzaria mitjançant "../" amb el que aniria retrocedint directoris. Amb la següent figura viem un exemple d'atac.



Il·lustració 36 - Log directory traversal

Per a que aquests atacs no es duguin a terme la validació en l'esquema d'autorització no ha de permetre accessos als recursos no autoritzats, amb el que s'ha d'iniciar reconeixement o enumeracions en tots el punts de les entrades, si tot s'ha validat correctament el servidor retornarà una resposta indicant que no es te permisos per accedir aquest recurs.

Amb la informació explicada podem concloure que les accions més importants per evitar aquest tipus d'atac és que alhora de crear el servei donar el mínim privilegi possible, evitar entrades de l'usuari amb caràcters tal com '../' o '..\', utilitzar mapes de referencia indirectes a objectes i comprovar els noms dels arxius que pugui entrar per el client.

3.4.3.2.1 Injecció SQL

Els atacs d'injecció SQL són els atacs reis per definició, si mirem a OWASP els tenen com a número 1 en el seu top ten. Aquests atacs estan definits en tres grups, posarem un exemple de cada un per veure com es declararien.

- Per errors: Són quan realitzes consultes y els errors que produeix l'aplicació es mostra per pantalla, i no es queda a nivell intern en el servidor.

- Bassat en Unió: Es realitza mitjançant consultes a taules lligades, així s'aconsegueix extreure més informació.

  Ex.: .php?colors=blau' union select * from sys.tables--

- Blind: El tipus d'atac on et trobes completament a cegues i s'ha d'esbrinar les sentencies vulnerables fent suposicions.

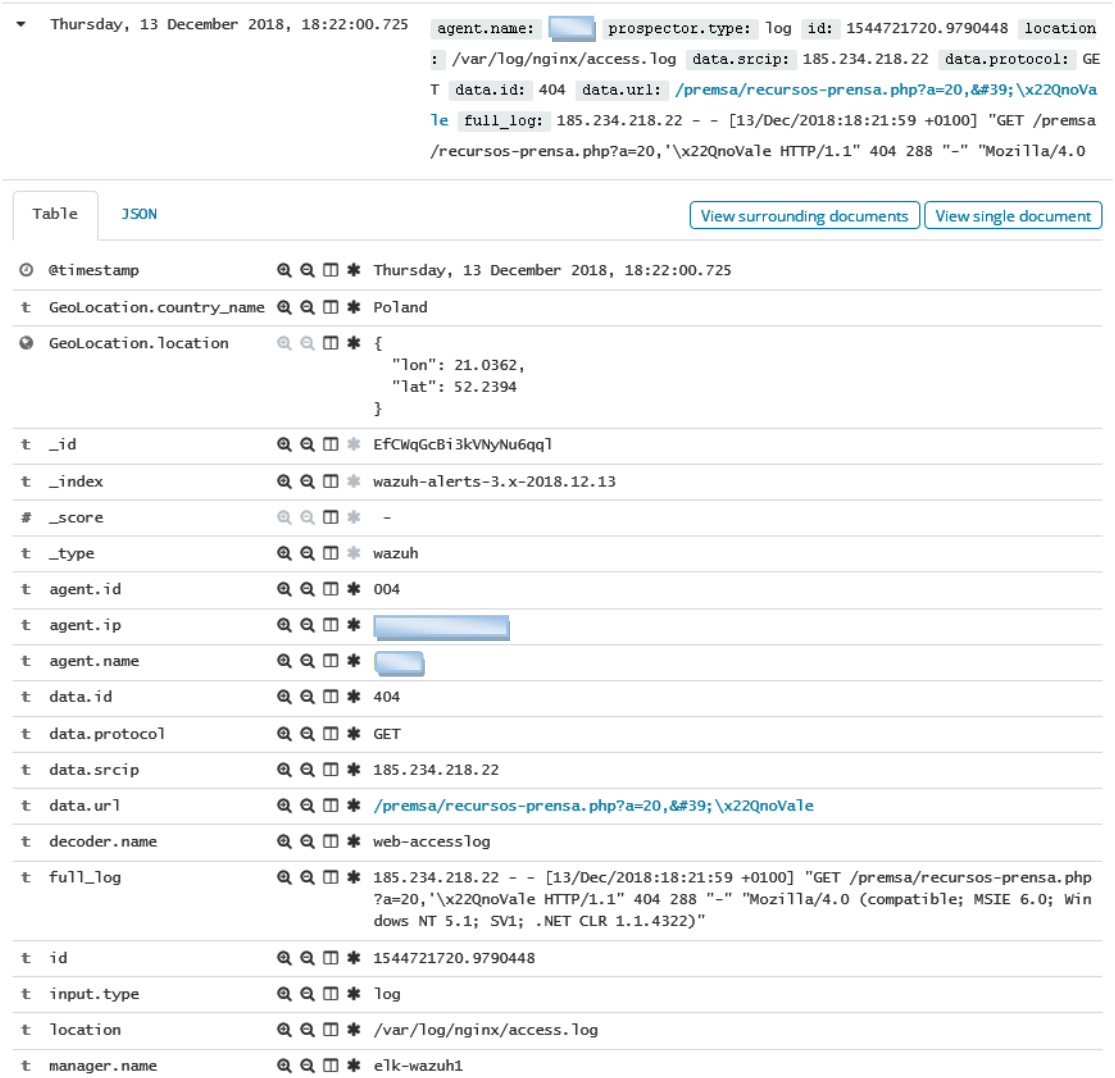
  Ex.: .php?colors=blau' and 1=(select top 1 name from sys.tables)--

**S'afegeix -- al final de cada sentencia per comentar qualsevol error SQL que es pugui ocasionar després.*

La recomanació més bàsica alhora d'evitar aquest tipus d'atacs és saber quin tipus de dades s'introduiran a la nostre aplicació i una vegada sabut programar la neteja de les entrades, els caràcters que s'han d'evitar són els següents.

```
', ", *, /, \, -, --, =, %, #, @, @@, ;, +, ?, |, ., :
```

Si ens fixem en el nostre cas s'està intentant tancar la sentencia, això tal com acabem d'esmentar s'aconsegueix amb un dels caràcters anteriors, a la nostre alarma això surt codificat en la URL però si ens fixem la part de la sentencia després de la coma la podem passar a un apòstrof ' → ' amb el que tancaríem la sentencia i després es podem afegir consultes extres. En aquest cas el que s'està intentant l'atac Blind amb el que amb una sèrie de cheats declarats es van provant sentencies fins trobar o un error (primer tipus d'atac) que ens mostri alguna informació rellevant per poder aprofundir en el servidor



Il·lustració 37 - Log injecció SQL

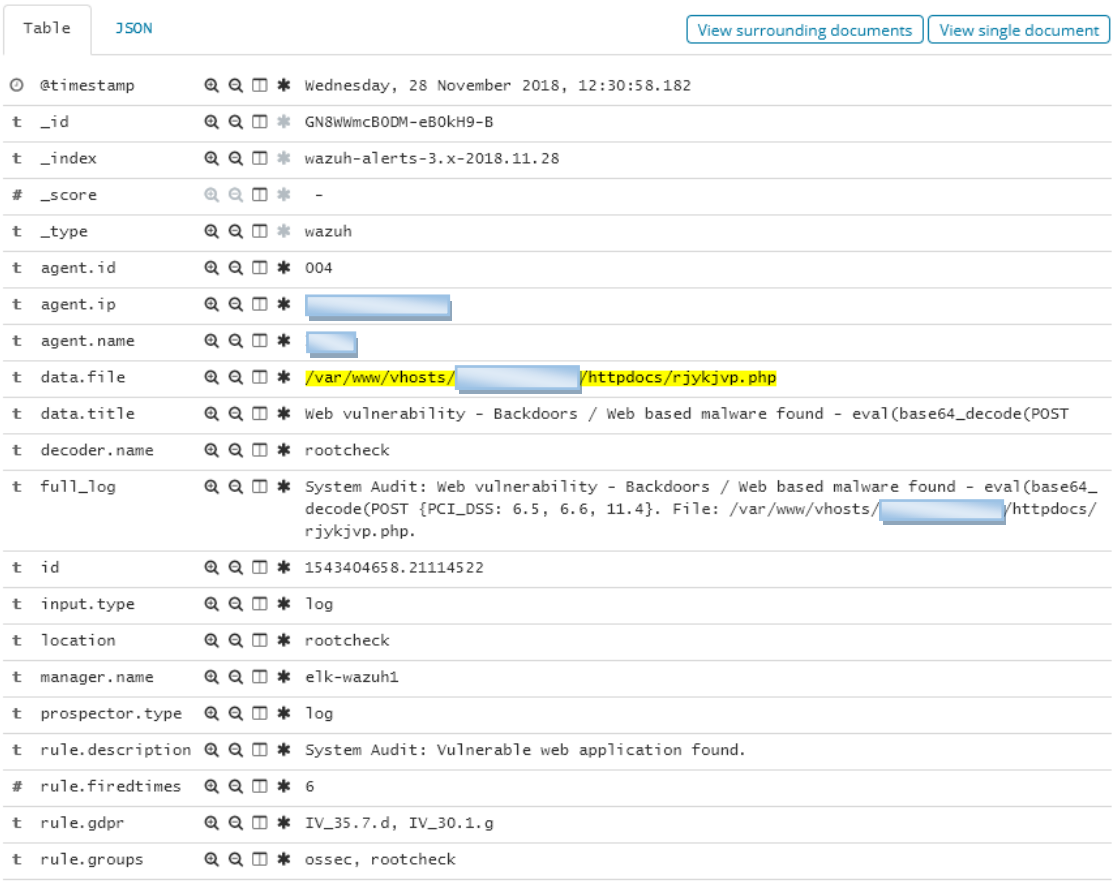
3.4.3.2.1 Malware detectat

Si revisem el codi de l'aplicació podem trobar la utilització de funcions com fsockopen(s'utilitza per la creació de Shell remotes) eval (constructor de llenguatge que ens permet la execució de codi php arbitrari i evadir errors en l'execució de codi) entre d'altres sentencies que permetrien a un atacant poder connectar-se remotament i injectar codi maliciós per els usuaris que entrin a la web o realitzar un desfasament per introduir missatges de terrorisme o d'altres connotacions.

Per aquest motiu quan es planteja la obertura d'una plana web s'ha de tindre en compte una sèrie de polítiques i condicions, aquestes poden ser tals com la actualització continua de tot l'entorn (servidor web, codi web, CMS, etc.). Tindre copies de seguretat de tot el que es pugi perdre, fer canvi de paraules de pas, aplicació de la llei menor millor, on els permisos d'usuari han de ser els mínims, els serveis exposats (ftp, ssh, http, etc.) han de ser just els necessaris i els permisos dels arxius del servidor han de ser els menors possibles. A més

també es recomanable la inclusió de regles de protecció en els arxius .web.config, .htaccess o nginx.conf.

Seguint aquestes premisses casos com el següent no haurien de succeir, un clar exemple és la programació de la plana web infectada, podem veure que s'ha creat amb Microsoft FrontPage un editor de pagines web HTML de l'any 2003, considerat poc adequat per les incongruències en la programació que conté.



Il·lustració 38 - Log detecció de Malware

3.4.4 Gestió e Investigació

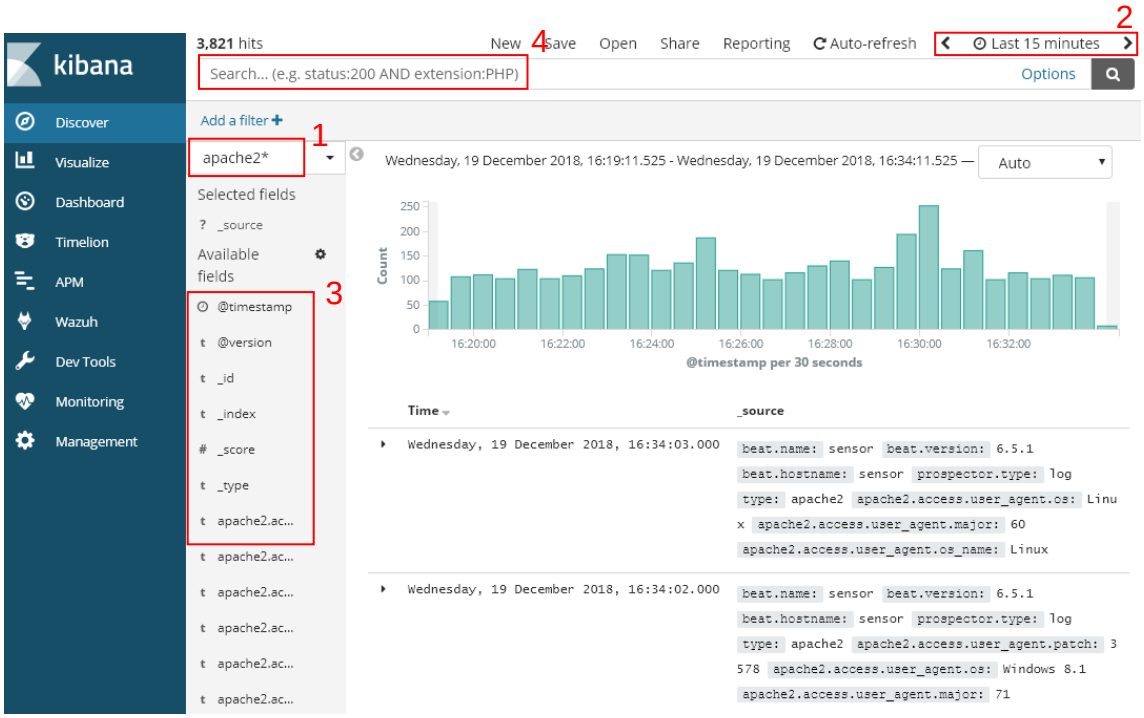
En aquest apartat s'explicarà tot l'entorn d'us diari de la aplicació, con explorar els logs i fer investigació d'alertes, gestió d'emmagatzematge, i alta disponibilitat de la plataforma.

3.4.4.1 Exploració

En el panell d'administració Kibana tenim dos menús claus que són el que s'utilitzen dia a dia per fer cerques i veure el resum de les alarmes generades, ordenar-les per criticitat, etc.

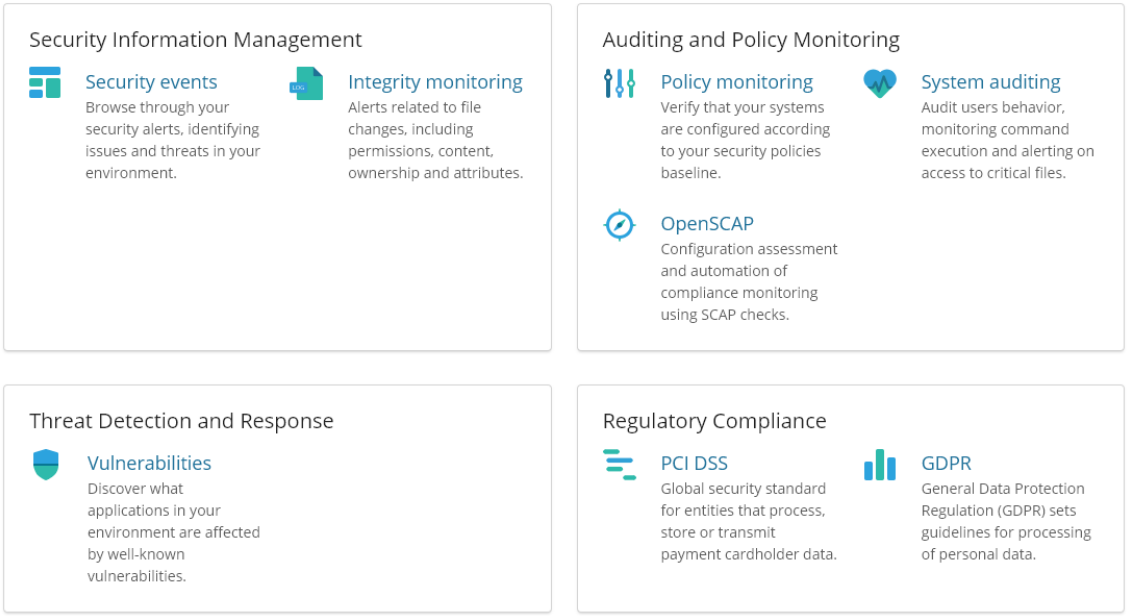
E primer menú és Discover que conté tots els logs categoritzats per tecnologia (1) on podem realitzar cerques en el temps (2) i filtratge per els 'fields' (3) disponibles que t'indica la plataforma o directament amb un cercador (4) on es pot buscar el contingut directament.

Si sabem que volem cercar el més senzill és utilitzar el buscador amb les paraules clau que vulguem i afegiríem asterisc davant i darrera la consulta per si a la sentencia hi ha altres paraules que ens impedís fer la cerca correctament. Com em explicat en anterior apartats la gran virtut d'Elasticsearch és la potencia de cerca, si busquem una paraula en un rang de temps de 7 dies (55,606,392 hits) triga entre 3-4 segons en trobar i mostrar-nos tots el resultats això ens permet poder realitzar cerques molt acurades en molt poc temps.



Il·lustració 39 - Discover Kibana

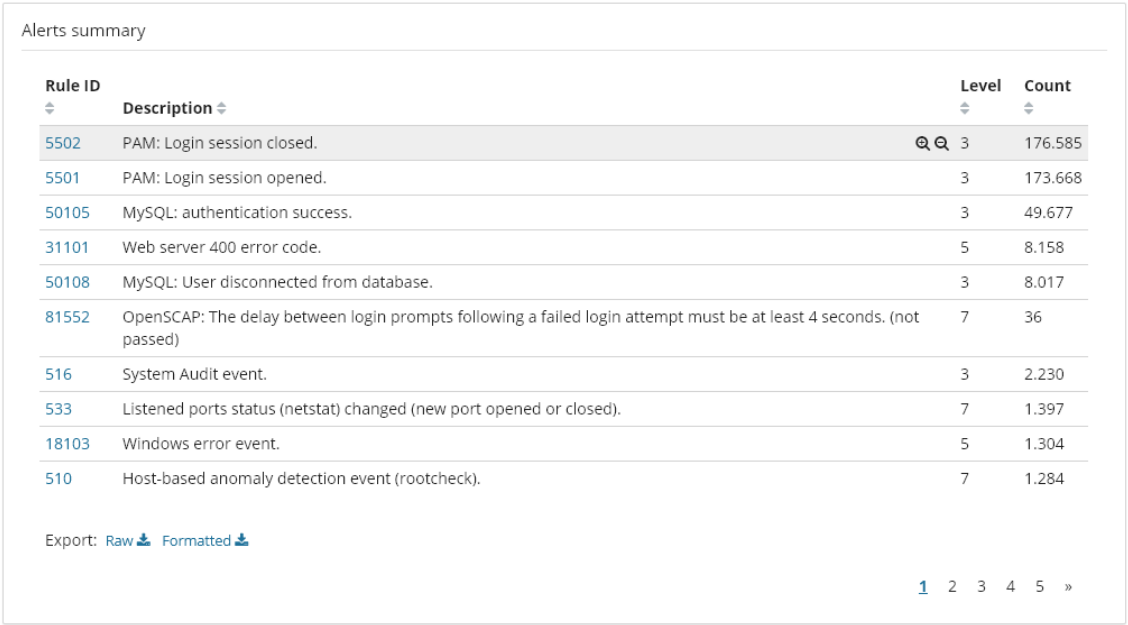
La part de Discover com hem vist és la base de la aplicació ja que ens permet indagar en totes les dades indexades, però per poder aprofundir en les dades ens cal saber que s'ha de buscar, per això tenim l'apartat de Wazuh, on tenim els agents monitoritzant els logs, arxius i aplicacions dels servidors per poder avisar-nos si sorgeix qualsevol anomalia. A l'apartat Overview podem trobar els següents quatre grans grups.



Il·lustració 40 - Wazuh Kibana

Security Information Management

En aquest apartat es on trobarem el resum de les alertes que s'han generat a traves de les rules disponibles, com vam indicar en la configuració de l'arxiu ossec.conf es redirigeixen els logs de cada aplicació i s'indiquen una sèrie de file-name on es diu quin tipus de log es (syslog, iis, apache, etc.) amb aquesta informació wazuh correla les traces de dades i les converteix en alarmes com poden ser els inicis de sessió, canvis en bases de dades, errors en les aplicacions etc.



Alerts summary

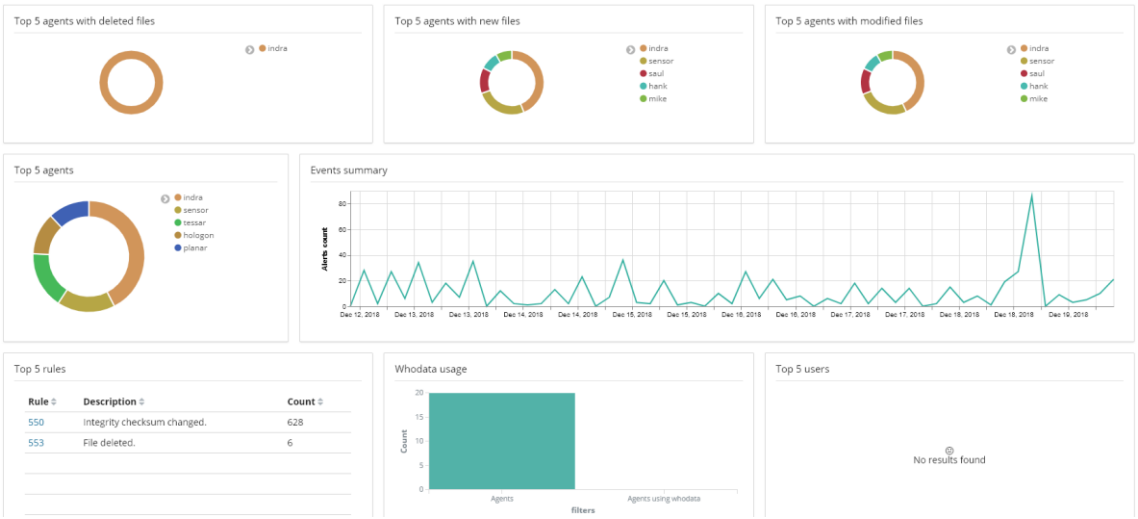
Rule ID	Description	Level	Count
5502	PAM: Login session closed.	3	176.585
5501	PAM: Login session opened.	3	173.668
50105	MySQL: authentication success.	3	49.677
31101	Web server 400 error code.	5	8.158
50108	MySQL: User disconnected from database.	3	8.017
81552	OpenSCAP: The delay between login prompts following a failed login attempt must be at least 4 seconds. (not passed)	7	36
516	System Audit event.	3	2.230
533	Listened ports status (netstat) changed (new port opened or closed).	7	1.397
18103	Windows error event.	5	1.304
510	Host-based anomaly detection event (rootcheck).	7	1.284

Export: Raw Formatted

1 2 3 4 5 »

Il·lustració 41 - SIM

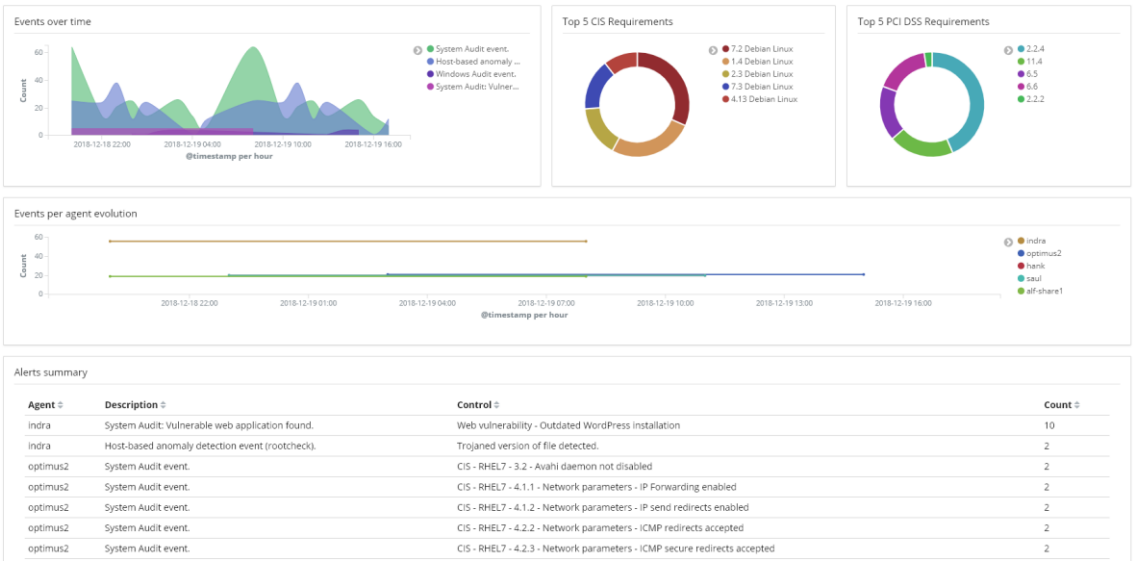
També podem trobar la monitorització dels arxius on tenim indicats la quantitat de canvis que hi ha en el servidor això es realitza monitoritzant els hash de cada arxiu.



Il·lustració 42 - Monitorització d'arxius

Auditing and Policy Monitoring

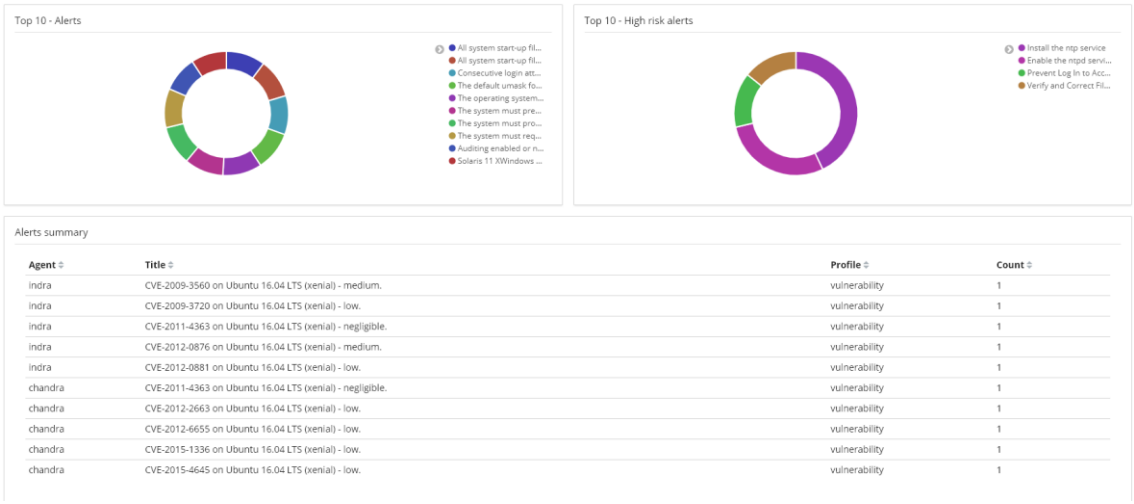
Aquest apartat és molt interesant, primerament tenim Policy monitoring on ens fan les recomanacions de seguretat que hauríem de tindre en el nostre servidors per complir amb l'estàndard del CIS com no permetre autenticar-se amb l'usuari root, establir un màxim d'intents a quatre, separar particions, etc. A més també ens monitoritza el servidor indicant-nos la possible inclusió d'exploits, o vulnerabilitats en aplicacions.



Il·lustració 43 - Policy Monitoring

Per últim tenim la part OpenScap on segon l'esquema oval tenim indicades totes les vulnerabilitats declarades en el servidor per a que les corregim, això és una gran ventatge ja que gestionar totes les versions de servidors i veure si

tenen una vulnerabilitat és bastant costosa de mantenir, i més a una empresa on el pool de servidors és tan gran.

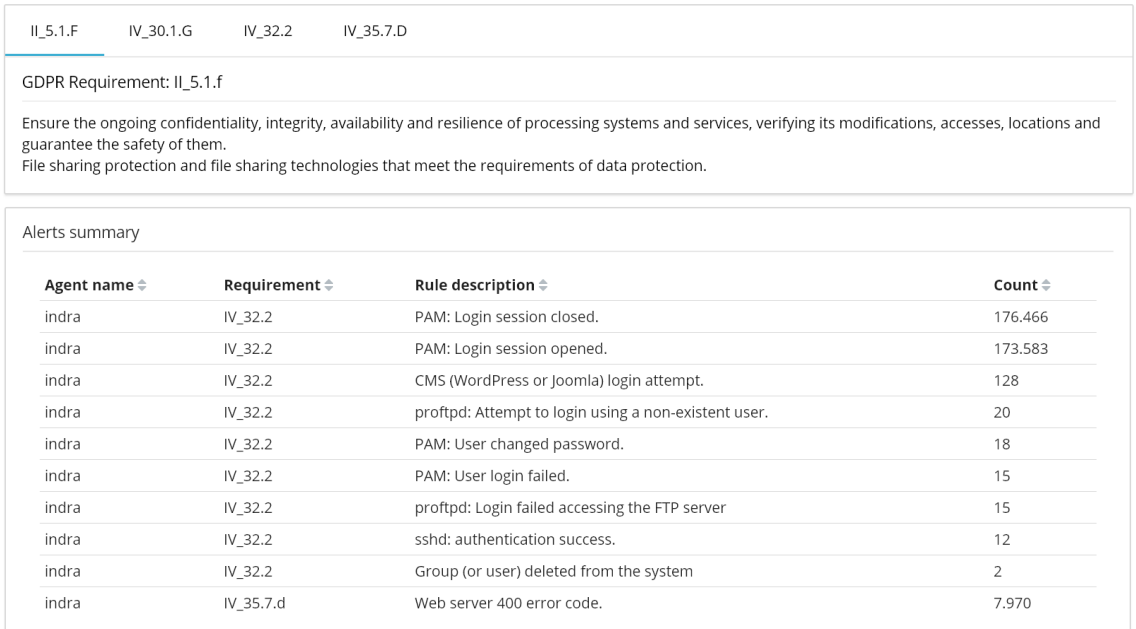


Il·lustració 44 - OpenScap

Regulatory compliance

Un altre de les característiques que tenim disponible és saber si complim amb els ordres regulatoris com PCI DSS que s'hauria de tindre en compte en cas de que es guardin dades de targetes de crèdit o del nou reglament de protecció de dades (GDPR) que en aquest cas si que és d'obligatori compliment tant per les empreses de la administració publica com la empresa privada.

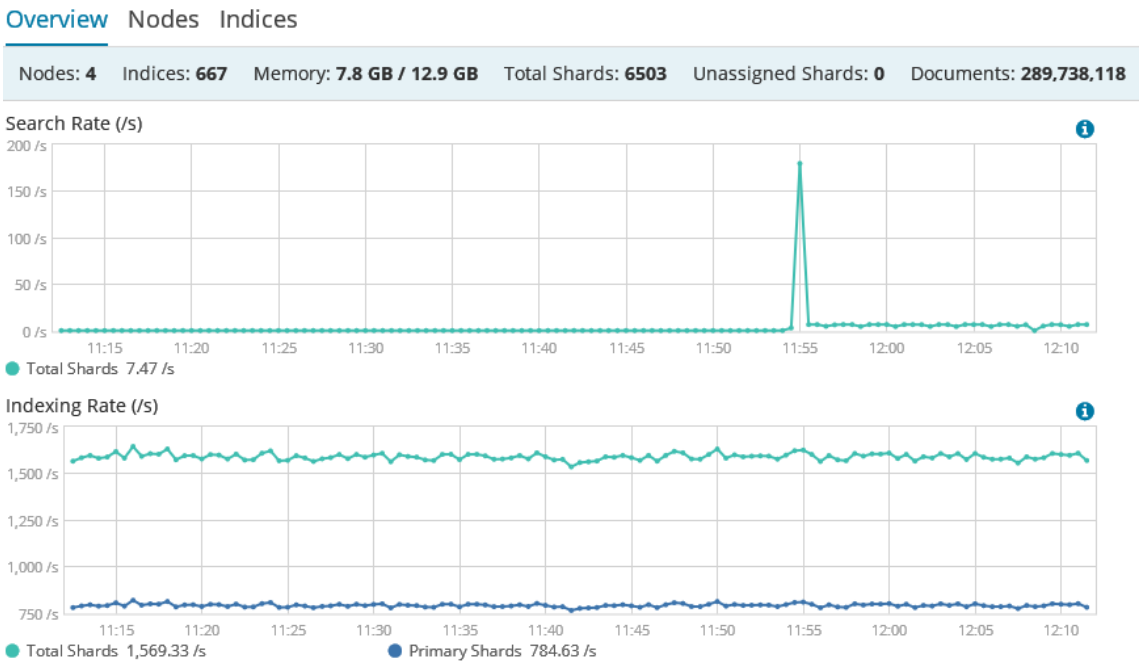
En el cas de GDPR ens indicaria les polítiques que s'estan incomplint juntament i el perquè s'està incomplint.



Il·lustració 45 - GDPR

3.4.4.2 Estadístiques i Gestió de logs

Com podem veure en la següent captura actualment es disposa de 289.738 documents indexats en el clúster d'Elasticsearch això pot arribar a ser una problemàtica si es continuen acumulant aquests documents ja que alhora de fer cerca de dades el rendiment del servidors pot veure bastant afectat.



Il·lustració 46 - Monitorització d'índex

Quan veiem que tenim aquest creixement en el nostre sistema s'ha d'establir unes polítiques d'emmagatzematge que ens permeti tancar els índex guardats per a que no afecti a les cerques, això ens permetrà no perdre els logs però que no afecti al rendiment. Una bona política es establir una tasca que tanqui els índex deixant els últims tres mesos de dades, per tancar-ho primer hauríem de fer un flush de les dades que vulguem tancar ja que si ens doni cap error per estar utilitzant aquests índex.

Il·lustració 47 - Tancament d'índex

Un altre possibilitat quan el espai en el nostre servidor no sigui suficient es emportar-nos els índex a un servidor NAS amb això s'aconseguirà guardar per

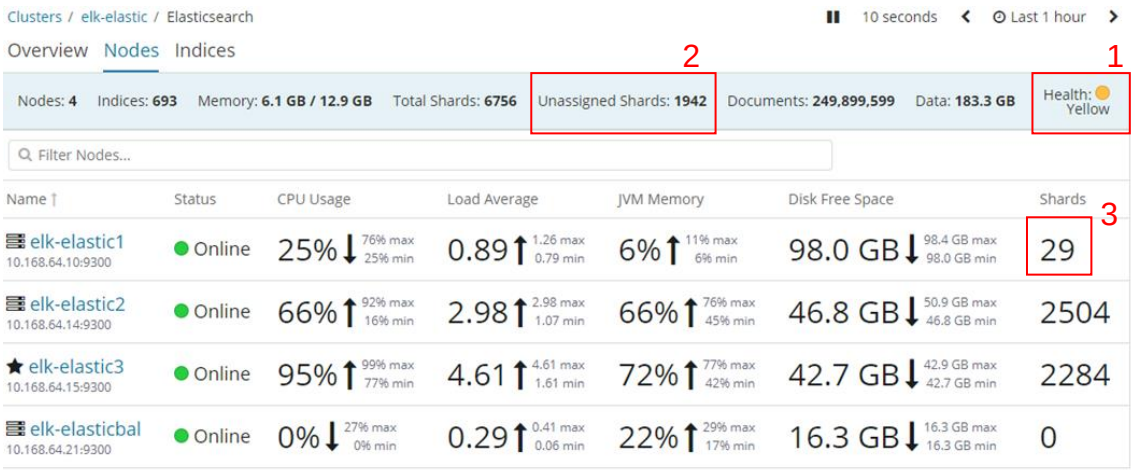
exemple logs d'alta sensibilitat que tinguin períodes d'emmagatzematge molt alts.

3.4.4.3 Alta disponibilitat

Un sistema d'aquest calatge normalment és molt crític per les organitzacions ja que te emmagatzemats tots els logs dels sistemes, necessaris per quan es produeixen incidents on intervenen requeriments judicials i s'ha d'entregar la informació sol·licitada, a més amb la nova normativa GDPR aquest sistemes agafen molt més protagonisme.

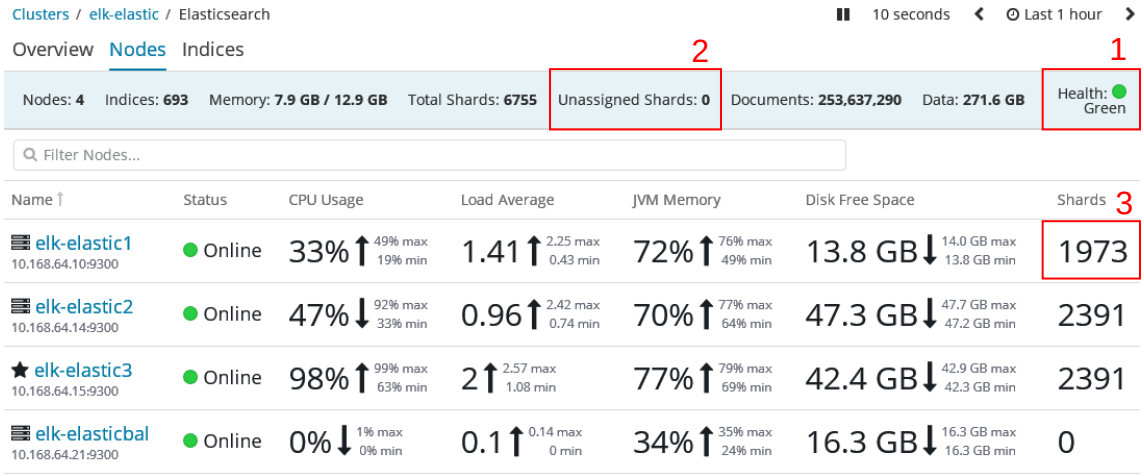
Com hem vist durant la documentació de la memòria la part clau de tota l'arquitectura és el clúster Elasticsearch ja que és on s'emmagatzemen totes les dades i els encarregats d'indexar tota la informació, per tant això fa que aquests elements siguin els que han de tindre un pla contra desastres, tot seguit mostrarem que passa si un dels nodes se li corrompés totes les dades emmagatzemades i no pogués consultar la informació.

Com veiem en la següent captura tenim que l'estat de 'salut' no està en verd sinó que esta en taronja, amb el que ens indica que en el sistema hi ha alguna cosa que esta fallant, si mirem el camp 'Unassigned Shards' veiem com tenim pendent 1942 shards pendents d'assignar quan hauria d'estar a 0, i efectivament podem observar com el node elk-elastic1 te molts pocs shards assignats.



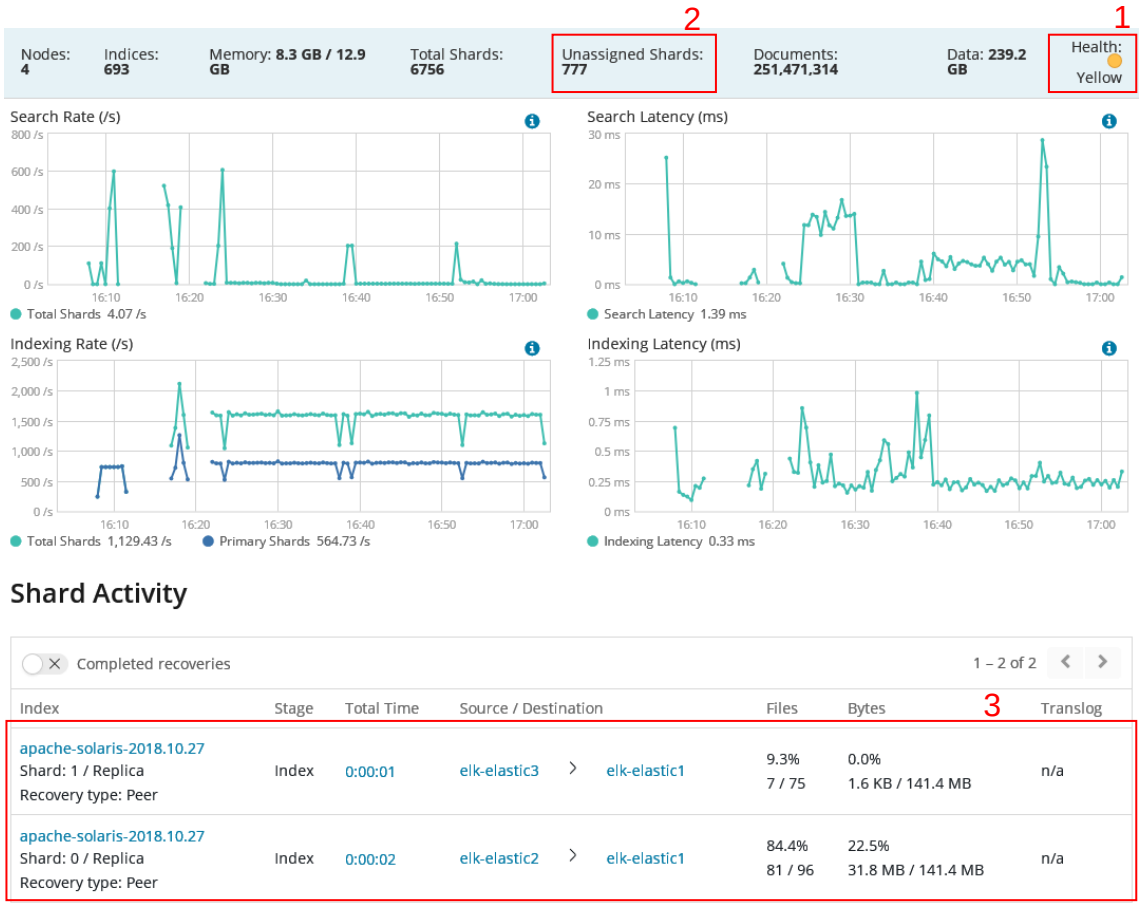
Il·lustració 48 – Reconstrucció d'índex

A la captura següent veiem quin seria l'estat normal del cluster quan totes les dades estan indexades correctament.



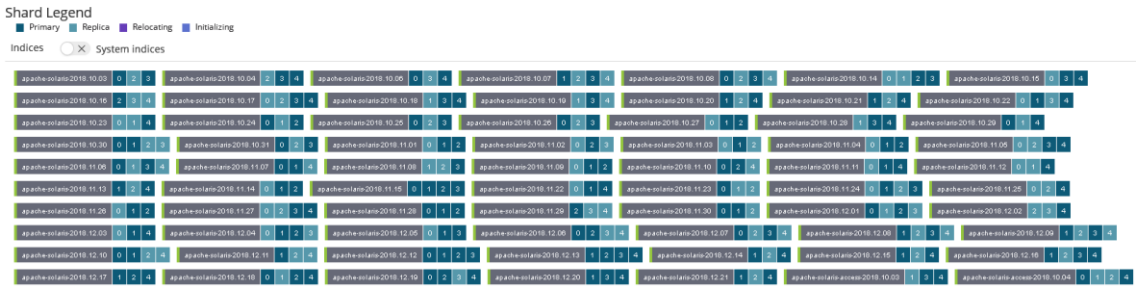
Il·lustració 49 - Índex reconstruïts

Per altre banda si ens dirigim al panell Overview d'Elasticsearch veiem com la reorganització del índex i les copies de les dades s'estan restablint gracies als altres dos nodes que no han sofert cap pèrdua de dades, per tant quan el procés finalitzi el cluster quedarà normalitzat.



Il·lustració 50 - Replica d'índex entre nodes

En la següent captura tenim com esta distribuïts els índex en el node1 del clúster, veiem com per exemple l'índex apache-solaris-2018.10.03 està guardat com a primari en el node 1 i 3 en el 2 simplement te una replica.

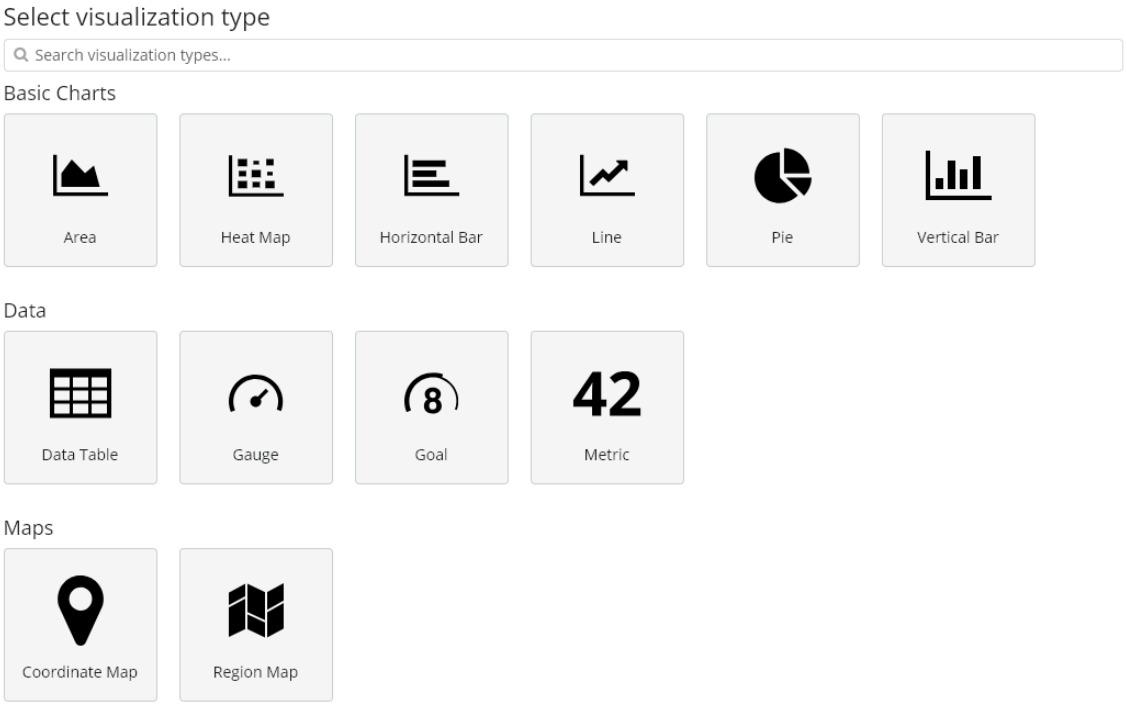


Il·lustració 51 - Organització d'índexs

3.4.4.3 Monitorització

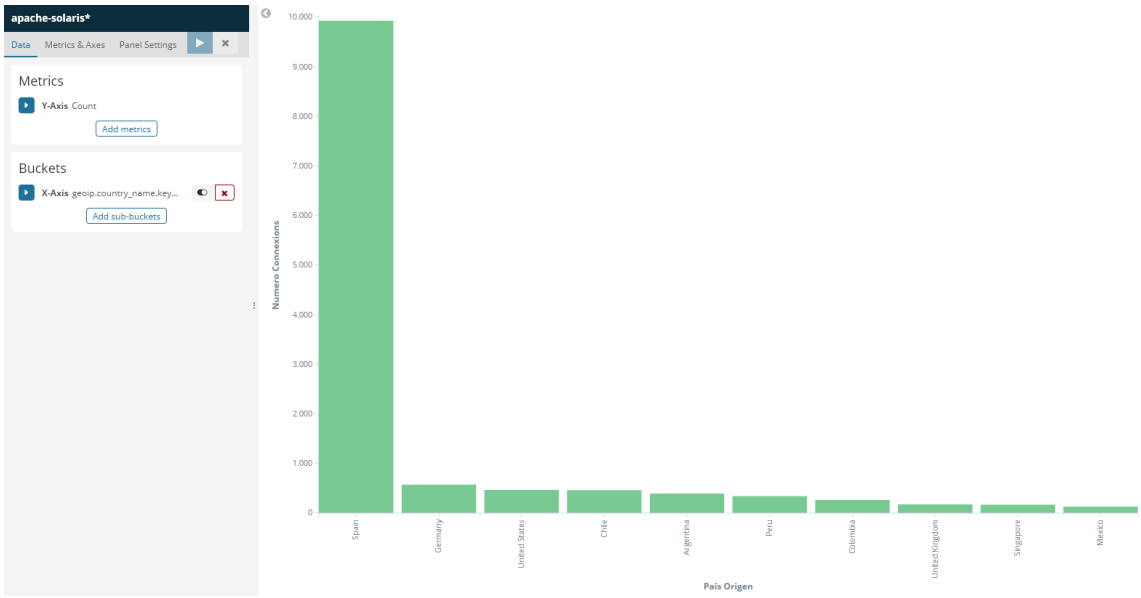
Amb la plataforma ELK també tenim la possibilitat de crear Dashboards, aquests son visualitzacions personalitzats amb les que podem graficar els paràmetres que creiem necessaris, i un cop creades anar-les afegint al Dashboard que vulguem.

Un exemple seria crear un Dashboard d'un servei com per exemple el portal de la universitat on monitoritzarem el número de connexions i la provinença d'aquestes. Per tant ens dirigirem a 'Visualize' on ens preguntarà el tipus de gràfic que volem crear.



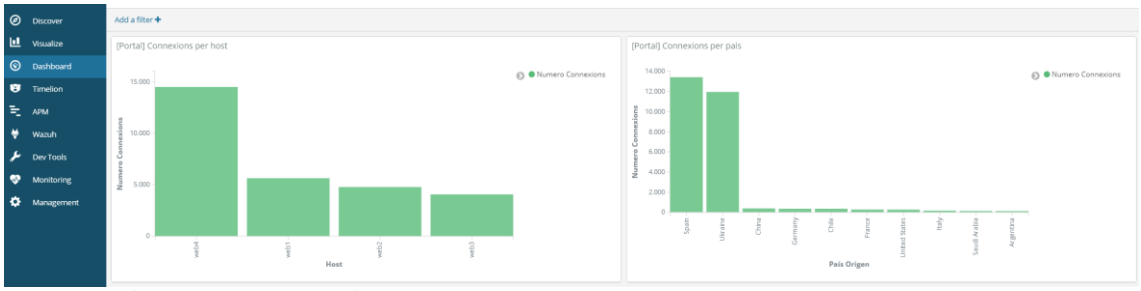
Il·lustració 52 - Selecció de gràfic

Tot seguit s'indicarà de quin log s'han de recollir les dades i quin parametres és el que s'ha de monitoritzar, en aquest cas serà el de la geolocalització.



Il·lustració 53 - Mètrica a monitoritzar

Finalment totes les visualitzacions d'un servei les podem agrupar en un mateix 'Dashboard' per poder-les monitoritzar.



Il·lustració 54 - Visualització del Dashboard

3.5 Valoració econòmica

Per la valoració econòmica es tindrà en compte diferents aspectes en el flux del projecte, des del moment inicial en el que la organització es planteja la integració d'un sistema de gestió d'esdeveniments i seguretat, fins la finalització del projecte amb tot l'entorn estable i funcionant. No es tindrà en compte el dia a dia que suposa la gestió dels incidents de seguretat i la millora continua.

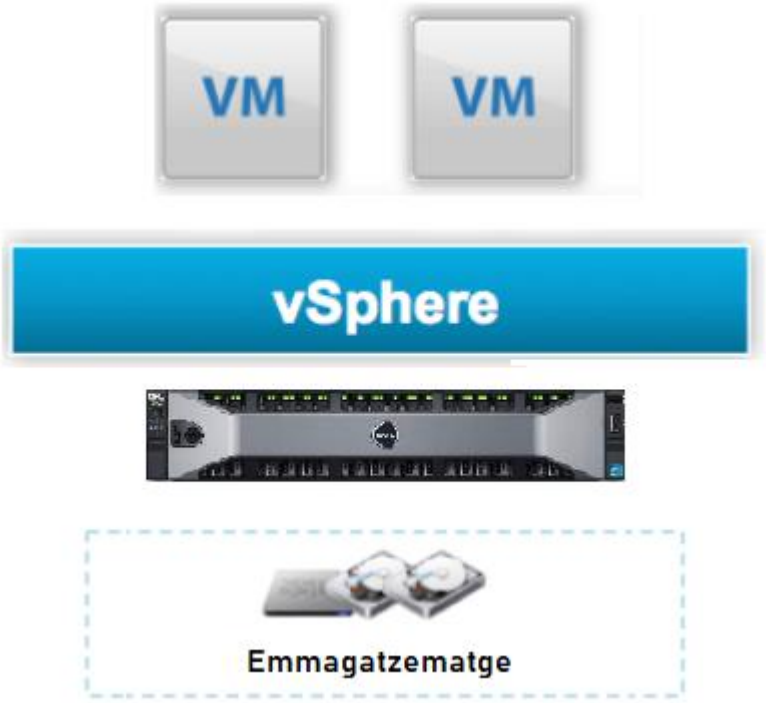
**Els costos d'aquest projecte són aproximats al seu valor real*

Els punts concrets que es tindran en compte són:

- ✓ Temps per el muntatge de cada arquitectura.
- ✓ Hardware de l'arquitectura.
- ✓ Software de l'arquitectura.
- ✓ Manteniment i Suport.

3.5.1 Arquitectura unificada

Per l'arquitectura unificada únicament contarà d'un servidor físic on estarà instal·lada tota la plataforma, els requisits d'aquest seran proporcionals a una arquitectura amb 10-20 servidors i 1 Firewall perimetral que tingui un throughput de 100-300 Megabits.



Il·lustració 55 - Arquitectura unificada física

Característiques Dell PowerEdge R610

- Dual (2) Intel Xeon X5650 6-Core 2.66GHz 12MB CPUs
- 64GB (8 x 8GB) DDR3 PC3-10600 1333MHz Registered Memory
- 6TB (6 x 1TB) 7.2K 6Gb/s SATA 2.5" HDDs
- PERC 6i RAID Controller with 256MB and Battery
- iDRAC6 Express
- Redundant Power Supplies

Llicències i suport

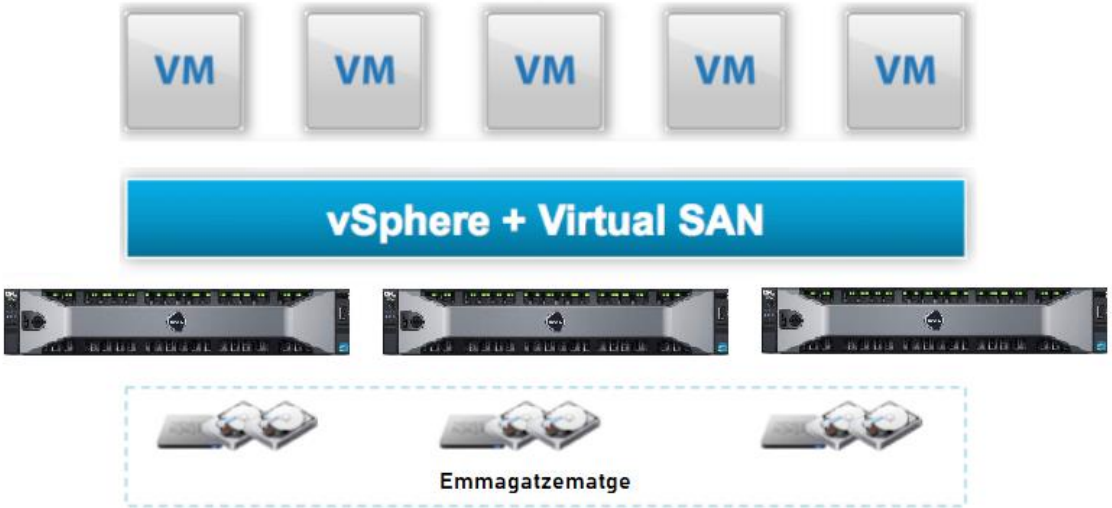
Suport onsite de Hardware

**Al no tindre un clúster no necessitem llicencies de virtualització.*

Valoració econòmica muntatge SIEM				
DESCRIPCIÓ	PREU	UNITATS	DTO.	TOTAL
Hardware				
Dell PowerEdge R610	1.312,36	1		1.312,36 €
Software & Llicències				
Suport onsite de Hardware R610	346,81	1		346,81 €
Muntatge				
Estudi i Disseny	60,00	5		300,00 €
Instal·lació màquines físiques	60,00	15		900,00 €
Preparació e Instal·lació entorn SIEM	60,00	23		1.380,00 €
Configuració SIEM	60,00	48		2.880,00 €
Revisió, Monitorització i Posada en producció	60,00	17		1.020,00 €
		Total Brut		**8.139,17 €**
	I.V.A. %		**21%**	**9.848,40 €**
Total				**9.848,40 €**

3.5.2 Arquitectura distribuïda

Per l'arquitectura distribuïda s'ha optat per un muntatge en clúster de vSAN, que implementarà una instancia vCenter Server Appliance (VCSA) i Platform Service Controller (PSC), una vegada instal·lat ens serà possible administrar un clúster vSAN d'un sol host i fer crides als discos. Aquesta arquitectura de clúster te dos possibilitats o en un mateix clúster de vSAN o amb clúster diferents, nosaltres optarem per un mateix clúster que constarà de tres màquines físiques DELL PowerEdge R830.



Il·lustració 56 - Arquitectura real física

Característiques Dell PowerEdge R830

- Quad (4) Intel Xeon E5-4610 v4 10-Core 1.8GHz 25MB CPU
- 64GB (4 x 16GB) DDR4 PC4-19200 2400MHz
- 4TB (8 x 500GB) 7.2K 3Gb/s SATA 2.5" HDDs
- PERC H330 12Gb/s RAID Controller
- iDRAC8 Express
- Redundant Power Supplies

Llicencies i suport

VMware vCenter Server 6 Foundation

VMware vSphere 6 Enterprise Plus Acceleration

Suport onsite de Hardware

Valoració econòmica muntatge SIEM				
DESCRIPCIÓ	PREU	UNITATS	DTO.	TOTAL
Hardware				
Dell PowerEdge R830	7.937,90	3		23.813,70 €
Software & Llicències				
VMware vCenter Server 6 Foundation	1.498,11	1		1.498,11 €
VMware vSphere 6 Enterprise Plus Acceleration	20.971,55	1		20.971,55 €
Suport onsite de Hardware R830	346,81	3		1.040,43 €
Muntatge				
Estudi i Disseny	60,00	8		480,00 €
Instal·lació màquines físiques	60,00	24		1.440,00 €
Preparació e Instal·lació entorn SIEM	60,00	40		2.400,00 €
Configuració SIEM	60,00	100		6.000,00 €
Revisió, Monitorització i Posada en producció	60,00	40		2.400,00 €
		Total Brut		**60.043,79 €**
	I.V.A. %		**21%**	**72.652,99 €**
Total				**72.652,99 €**

4. Conclusions

Aquest projecte es basa en la problemàtica actual alhora d'implementar un gestor de logs i esdeveniments de seguretat, tant per una organització amb pocs recursos, com per una gran empresa que vol tindre un bon gestor per monitoritzar la seguretat i logs de sistema sense tindre costos afegits de llicenciament de software.

Al implementar la plataforma s'ha pogut determinar la complexitat que comporta aquest tipus de muntatge, ja que sorgeixen diferent tipus de problemes en la configuració que has d'anar solucionant poc a poc. Un projecte d'aquesta embergadura en el que pots arribar a tindre grans volums de dades que tractar i gestionar, pot arribar a comportar força dificultat i hores de treball, però una vegada muntada la plataforma et retorna molts beneficis, ja que et permet tindre la teva infraestructura totalment controlada.

Respecte l'assoliment d'objectius, podem determinar que s'han assolit amb satisfacció, encara que han hagut punts del projecte que es podrien haver definit amb més detall o aprofundir una mica més, però per falta de temps no s'han pogut portar a terme.

Si ens enfoquem en l'objectiu principal de configurar la plataforma per les dues arquitectures i determinar quina és la millor solució per cada organització, podem concloure que per una empresa on el seu valor d'indexació sigui menor a 1000 shards per segon s'hauria d'optar per una arquitectura unificada ja que els costos associats a aquesta arquitectura són 7 vegades menors que una arquitectura distribuïda, a més de que el rendiment de les cerques de dades serà molt similar sempre que els índex oberts es mantinguin al voltant dels dos mesos.

Per altre banda un dels objectius principals era aconseguir els fonaments necessaris per obtenir una plataforma de gestió de logs i esdeveniments de seguretat funcionant, amb el que poder fer us de l'explotació de les dades per detectar i resoldre incidents, aquesta part també s'ha assolit satisfactòriament, ja que s'ha aconseguit que les dues arquitectures funcionin correctament i s'han posat exemples reals de la detecció dels incidents de seguretat, detecció de malware i auditoria dels sistemes.

Per tant un dels objectius que ens a quedat una mica incomplet és la part de prevenció, on ens a faltat aprofundir una mica més en les diferents alertes i en la millorar el servei.

Per el seguiment de la planificació podem dir que la base del projecte s'ha portat a terme correctament tot i que en alguns punts concrets s'ha tingut que desplaçar una mica en el temps ja que un projecte d'aquest tipus és difícil de determinar exactament quins temps requereixen les tasques associades, a més dels problemes que han sorgit durant la configuració i que s'han tingut que solucionar poc a poc.

Pel que fa a les línies de futur faltaria entrar en aspectes com la millora continua, creació d'alertes automàtiques amb resposta activa, on mitjançant scripts es generaria una alerta que ens crearia una regla al FW per denegar accessos a determinades IPs, reiniciar el procés d'algun servei, etc. També estaria interesant la creació d'alertes personalitzades mitjançant la auditoria de directoris específics o línies de log que la plataforma no contempla, però són d'importància per la organització.

5. Glossari

Actiu	Servidor, dispositiu de xarxa o element propietat de la empresa que es pot monitoritzar.
Agent	Programari que s'instal·la en un actiu i s'encarrega de monitoritzar-lo i enviar els logs de sistema.
API	Application Programming Interface. Interfície encarregada d'enllaçar dues plataformes diferents per a que pugin treballar entre elles.
CIS	Center for Internet Security. Organització sense ànim de lucre que promou i desenvolupa bones pràctiques per la seguretat dels sistemes.
Cluster	Conjunt de servidors interconnectats que treballen conjuntament per oferir un rendiment millorat.
Correlador	Procés que s'encarrega de comparar diferents dades i crear un nou esdeveniment a partir d'aquests.
Escalabilitat	Capacitat que te un sistema per ampliar els recursos i fer-lo més potent.
Esdeveniment	Alerta que es crea al sistema quan es produeixen certs patrons.
Firewall	Encarregat de bloquejar els accessos no autoritzats a un sistema o xarxa.
HTTPS	Protocol segur per les comunicacions webs.
Indexació	Mètode per incloure els diferents continguts dels logs.
Log	Esdeveniments que succeeixen al sistema que afecten als diferents processos.
Malware	Software dissenyat per infectar un sistema amb l'objectiu d'infiltrar-se o danyar-lo.
Match	Procés d'emparellar diferents resultats.
Open Source	Model de desenvolupament de software basat en col·laboració.
OWASP	Open Web Application Security Project. Organisme dedicat a combatre les causes que fan el software insegur.
Repositoris	Espai centralitzat on s'emmagatzema i distribueix arxius informàtics.
Shards	Instancia d'un índex de Lucene, cada índex esta compost per un o més shards.
SIEM	Sistema de gestió d'esdeveniments i informació de seguretat.
Software	Component lógic escrit en llenguatge de programació format per diferents aplicacions informàtiques que realitzen una funció concreta.
TCP	Transmission Control Protocol. És un dels protocols fundamentals en l'Internet d'avui en dia, s'utilitza per crear connexions i engloba protocols com HTTP, SSH o FTP.
URL	Uniform Resource Locator. Es tracta d'un identificador de recursos designats a una xarxa local o externa.
Vulnerabilitat	Error en el sistema que permet a un atacant la vulneració del mateix.

6. Bibliografia

[1] Tony Hsu, *Hands-On Security in DevOps: Ensure continuous security, Deployment*, and delivery with DevSecOps, Packt Publishing Ltd, Birmingham, 2018.

[2] Vinod Vasudevan, Anoop Mangla, Firosh Ummer, Sachin Shetty, Sangita Pakala, Siddharth Anbalahan, *Application Security in the ISO 27001:2013 Environment*, Second edition, IT Governance Publishing, Cambridgeshire, 2015.

[3] David R. Miller, Shon Harris, Allen A. Harper, Stephen VanDyke, Chris Blask, *Security Information and Event Management (SIEM) Implementation*, The McGraw-Hill Companies, New York, 2011.

[4] ISACA, *COBIT: A Business Framework for the Governance and Management of Enterprise IT*, ISACA, Rolling Meadows, 2012.

[5] ISACA, *The Risk IT Framework, ISACA,* Rolling Meadows, 2009.

[6] Ester Chicano Tejada, *MF0488_3: Gestión de incidentes de Seguridad informàtica, IC Editorial, Málaga, 2014.*

[7] https://www.elastic.co/guide/index.html [Últim accés 24/11/2018]

[8] https://documentation.wazuh.com/current/index.html [Últim accés 26/11/2018]

[9] https://www.owasp.org/ [Últim accés 11/12/2018]

[10] https://virtualizadesdezero.com/ [Últim accés 9/12/2018]

[11] https://www.vmware.com [Últim accés 9/12/2018]

[12] http://www.vmstore.es/ [Últim accés 13/12/2018]

[13] https://www.aventissystems.com [Últim accés 13/12/2018]

[14] www.isaca.org/ [Últim accés 4/12/2018]

[15] https://github.com/aabc/ipt-netflow [Últim accés 26/10/2018]

[16] https://www.alienvault.com/ [Últim accés 8/10/2018]

[17] https://www.prelude-siem.org/ [Últim accés 10/10/2018]

[18] https://www.splunk.com/es_es [Últim accés 11/10/2018]