Universitat Oberta de Catalunya

uoc.edu

Anàlisis i implementació d'un SIEM en l'àmbit empresarial

Alumne: Jordi Malla Esqué
Màster Universitari en Ciberseguretat i Privadesa
Seguretat empresarial

Director del TFM: Miguel Ángel Flores Terrón
Professor/a responsable de l'assignatura: Victor Garcia Font
Data de lliurament PEC1: 29/09/2020

FITXA DEL TREBALL FINAL

Títol del treball:	*Anàlisis i implementació d'un SIEM en l'àmbit empresarial*
Nom de l'autor:	*Jordi Malla Esqué*
Nom del consultor/a:	*Miguel Ángel Flores Terrón*
Nom del PRA:	*Victor Garcia Font*
Data de lliurament:	*12/2020*
Titulació o programa:	*Màster Universitari en Ciberseguretat i Privadesa*
Àrea del Treball Final:	*Seguretat empresarial*
Idioma del treball:	*Català*
Paraules clau	*SIEM, Wazuh, empresarial, Elastic*

Resum del Treball

Aquest TFM te com a objectiu explorar una eina molt concreta, com és el SIEM Wazuh, juntament amb la pila Elastic, per tal d'analitzar els logs generats en un sistema i evaluar-los mitjançant eines de Machine Learning per determinar si s'està produint un incident de seguretat concret com és un atac de Ransomware amb Cryptolocker.

La configuració de la solució s'ha realitzat en un entorn empresarial amb una configuració on premise, mitjançant Docker i utilitzant les solucions: Elastic Stack per emmagatzemar i gestionar els logs de manera centralitzada, Wazuh per recollir els logs i generar alertes de seguretat, la solució Machine Learning d'Elasticsearch per detectar i notificar incidents de seguretat, i, finalment, MS Teams per centralitzar la recepció de les alertes.

Les conclusions de la POC han estat satisfactòries en quant a la detecció de l'incident de seguretat, utilitzant la configuració de Machine Learning de Elasticsearch. Tot i això, s'insta a extendre la solució de seguretat amb més opcions per ampliar la protecció, ja què, aquest TFM està molt centrat en un tipus d'incident de seguretat molt concret, i, la seguretat empresarial és més complexa.

Abstract

This TFM explores the SIEM Wazuh with Elastic stack, so that to analyse the logs generated in a system and evaluate them with Machine Learning to detect a Ransomware attack with Cryptolocker.

The solution has been done in a business environment with an on premise Docker configuration and it use the platforms: Elastic stack to centralize storage and manage the logs, Wazuh to collect logs and generate security alerts, the Elasticsearch's machine learning to detect and inform security incidents, and finally MS Teams to centralize the alert's collections.

The findings of this POC have been satisfactory in terms of detecting this security incident with Elasticsearch's machine learning configuration, although it is recommended to extend the security solution with more options to increase protection, as this TFM is highly focused on a very specific security incident, and business security is more complex.

Índex de continguts

Índex d’il·lustracions

1. Introducció

1.1 Context i justificació del Treball

La seguretat informàtica s'està convertint en el principal cavall de batalla de les empreses, es considerin o no digitals; Per què hi ha alguna empresa que no sigui digital? al meu entendre no, i és que cada cop més les empreses necessiten digitalitzar-se més i protegir aquests actius per ser més eficients i competitives, sense oblidar el compliment de les normatives en matèria de protecció i privacitat de les dades.

Actualment estem patint una pandèmia sanitària que està influint, i molt, en la nostra manera de treballar, obligant a les empreses i treballadors/es a adaptar-se a gran velocitat a aspectes com el teletreball, l'ús massiu del correu electrònic, videoconferències, etc. Aquesta adaptació vertiginosa i obligada ha obert moltes portes als cybercriminals que no han dubtat ni un minut en explotar-les al màxim, com en els casos recents i tant recurrents d'atacs amb Cryptolocker.

Aquests atacs persegueixen encriptar la informació de la víctima i demanar-ne un rescat a canvi de recuperar-la. Degut al nivell d'afectació de la informació sensible aquest atacs poden arribar a ser molt perillosos, afectant la productivitat de l'empresa i en alguns casos obligar al tancament.

Per tal de fer front a tots aquest reptes de seguretat informàtica i complir amb les noves normatives de protecció i privacitat de les dades, les empreses s'han de dotar de coneixement, polítiques de seguretat i nombrosos sistemes de seguretat com: Còpies de seguretat, Firewall, Antivirus, IDS, IPS, SIEM, etc.

Degut a què l'àmbit de la seguretat empresarial és molt ampli, i dissenyar i implantar un sistema de seguretat complet a nivell global requereix molt de temps, aquest treball de final de màster, en endavant TFM, es centra en establir les bases d'un sistema de seguretat, duent a terme una configuració inicial que ens ajudi a detectar l'encriptació massiva de fitxers, mitjançant un agent HIDS i centralitzant-ne la gestió amb la pila ELK i el SIEM Wazuh.

1.2 Motivació

L'afectació d'un atac per Cryptolocker és molt crítica per una empresa si prèviament no s'han establert mesures per mitigar-ho i/o recursos per gestionar una resposta adequada.

La principal motivació del projecte és implantar les bases d'una eina que permeti a la meva empresa tenir una visió global de la seguretat i que l'equip de IT puguem reaccionar de manera proactiva als possibles incidents de seguretat. Per establir les bases s'ha decidit iniciar la implantació i centrar les proves en la detecció dels Cryptolockers, degut als recents atacs que hem patit directament en la nostra empresa.

1.3 Objectius del Treball

L'objectiu final del TFM és disposar d'una solució que ens permeti inicialment detectar atacs amb Cryptolocker però que alhora sigui escalable i en la qual sigui possible integrar-hi altres solucions de seguretat, i també que es pugui implementar en petites i mitjanes empreses amb pocs recursos econòmics.

Per assolir aquest objectiu final he definit 3 objectius que m'han d'ajudar a elaborar el TFM per parts:

- 1a Part: Aconseguir la màxima informació per decidir l'esquema a implantar per tal de:
    - Obtenir una visió global dels sistemes de seguretat, i en concret dels SIEM i IDS.
    - Conèixer l'evolució dels atacs per Cryptolocker i la seva afectació a les empreses.
    - Decidir quins sistemes i com s'implantaran per tal d'obtenir el resultat desitjat.
- 2a Part: Implantar les bases d'un sistema de seguretat:
    - Realitzar la implantació en un entorn Docker ja existent.
    - Implantar i configurar l'agent en el servidor a monitorar.
    - Implantar i configurar el SIEM.
    - Simular un atac.
    - Proposar i documentar millores.
- 3a Part: Avaluar i treure conclusions de la proposta de forma global
    - Valorar els resultats obtinguts.
    - Realitzar una valoració econòmica de la implantació del sistema de seguretat proposat.

1.4 Enfocament i mètode seguit

El TFM està enfocat dins un cas real en l'àmbit empresarial, per tal d'intentar donar solució a un problema que afecta a moltes empreses, i que actualment, degut a la pandèmia sanitària, ha crescut exponencialment, com son els atacs amb Cryptolockers.

Per dur a terme l'objectiu principal del TFM s'han valorat dues estratègies com son: la elaboració d'un sistema de seguretat propi ja integrat dins l'empresa, o aprofitar els productes open source amb llicències gratuïtes que ja existeixen i integrar-los dins l'esquema de l'empresa.

L'estratègia escollida és la d'aprofitar els productes ja disponibles al mercat i implantar el SIEM Wazuh i el seu agent HIDS, integrat dins la pila ELK aprofitant les llicències gratuïtes; i valorar els serveis de pagament com el de Machine Learning que ens ofereix la pila ELK. Per finalitzar, també configurar les alertes del SIEM perquè arribin al canal de Teams que ja utilitzem al departament de IT.

Aquesta decisió l'he pres basant-me en 4 premisses. Primer, per una qüestió d'integració, ja que el procediment descrit aquí pot ser exportable a qualsevol altra empresa. Segon, per una qüestió de temps, ja que el TFM està limitat en el temps i no dona per crear tot un sistema de seguretat. Tercer, per l'oferta que hi ha de productes, ja que les llicències gratuïtes dels productes open source ens ofereixen una funcionalitat molt bona si a l'empresa disposem de personal especialitzat. I finalment considero que aquests productes en concret s'integren molt bé en un entorn Docker facilitant molt tota la seva instal·lació, configuració i exportació.

1.5 Planificació del Treball

1.5.1 Descripció dels recursos necessaris

Per implantar el TFM necessitarem una infraestructura amb com a mínim 2 servidors, un servidor per monitorar i realitzar la instal·lació del SIEM i un segon servidor que serà monitorat amb la instal·lació de l'agent HIDS. Aquesta infraestructura ha de tenir accés a Internet per tal que els productes puguin obtenir tota la informació necessària per al seu funcionament.

Com que la implantació és realitza en un entorn amb Docker, també és requerirà que la infraestructura disposi d'un entorn d'aquestes característiques ja preinstal·lat, i un compte de Teams ja configurat per a la recepció de les alertes del SIEM.

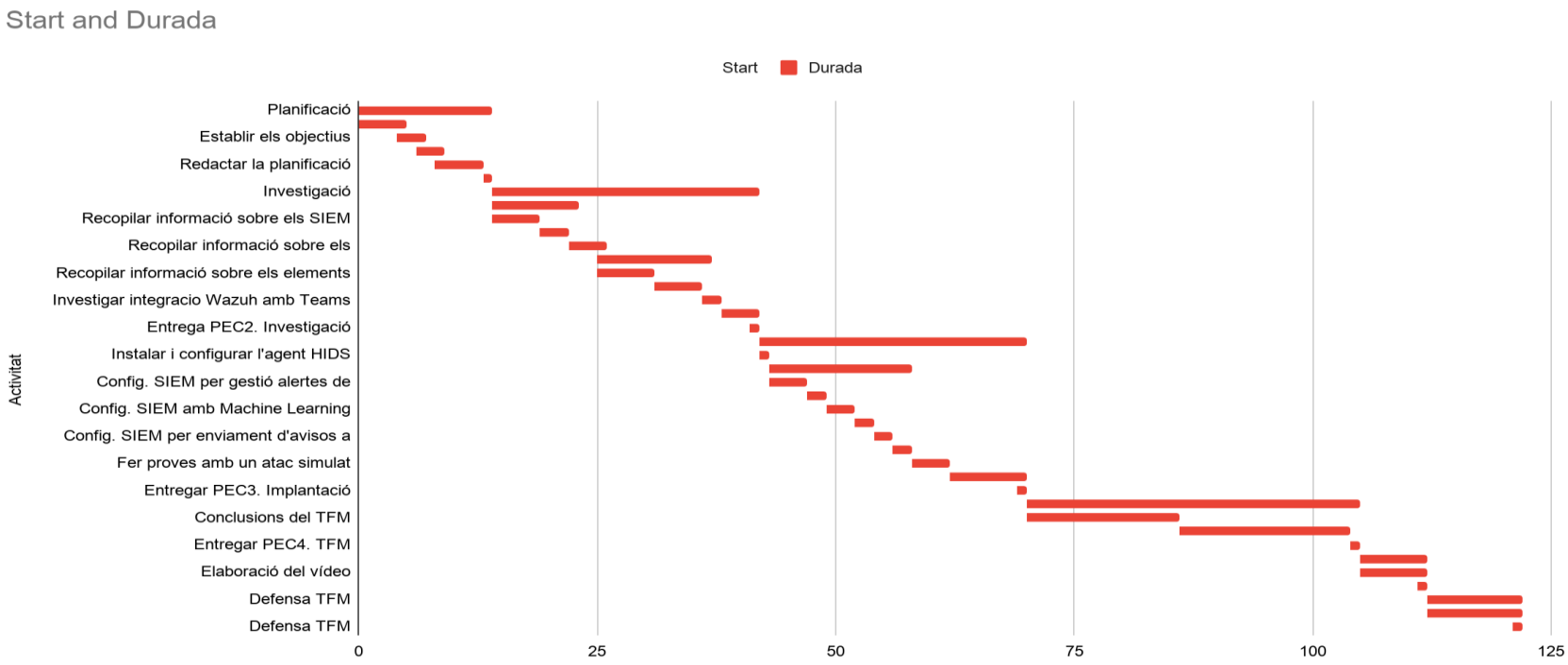
1.5.2 Llistat de les tasques a realitzar

	Tasca	Data Inici	Data fi	Dies
1	**Planificació**	9/16/2020	9/29/2020	14
1.1	Buscar i establir context del projecte	9/16/2020	9/20/2020	5
1.2	Establir els objectius	9/20/2020	9/22/2020	3
1.3	Plantejar la metodologia	9/22/2020	9/24/2020	3
1.4	Redactar la planificació	9/24/2020	9/28/2020	5
1.5	**Entregar PEC1. Planificació**	9/29/2020	9/29/2020	1
2	**Investigació**	9/30/2020	10/27/2020	28
2.1	Investigar Sistemes de seguretat	09/30/2020	10/08/2020	9
2.1.1	Recopilar informació sobre els SIEM	09/30/2020	10/04/2020	5
2.1.2	Recopilar informació sobre els IDS	10/05/2020	10/07/2020	3
2.2	Recopilar informació sobre els Cryptolocker	10/08/2020	10/11/2020	4
2.3	Recopilar informació sobre la pila ELK	10/11/2020	10/22/2020	12
2.3.1	Recopilar informació sobre els elements de la pila ELK	10/11/2020	10/16/2020	6
2.3.2	Recopilar informació sobre l'opció Machine Learnig de ELK	10/17/2020	10/21/2020	5
2.4	Investigar integració Wazuh amb Teams	10/22/2020	10/23/2020	2
2.5	Redactar l'esquema del sistema seguretat	10/24/2020	10/27/2020	4
2.6	**Entrega PEC2. Investigació**	10/27/2020	10/27/2020	1
3	**Implantació**	10/28/2020	11/24/2020	28
3.1	Instal·lar i configurar l'agent HIDS	10/28/2020	10/28/2020	1
3.2	Instal·lar el servidor SIEM Wazuh i ELK	10/29/2020	11/12/2020	15
3.2.1	Config. SIEM per gestió alertes de l'agent IDS	10/29/2020	11/01/2020	4
3.2.2	Realitzar proves de comunicació entre l'agent i el SIEM	11/02/2020	11/03/2020	2
3.2.3	Config. SIEM amb Machine Learning ELK	11/04/2020	11/6/2020	3
3.2.4	Realitzar proves amb l'opció Machine Learing	11/07/2020	11/8/2020	2
3.2.5	Config. SIEM per enviament d'avisos a Teams	11/9/2020	11/10/2020	2

3.2.6	Provar recepció d'avisos a Teams	11/11/2020	11/12/2020	2
3.3	Fer proves amb un atac simulat	11/13/2020	11/16/2020	4
3.4	Valorar integració opcions de millora al sistema	11/17/2020	11/24/2020	8
3.5	**Entregar PEC3. Implantació**	11/24/2020	11/24/2020	1
4	**Obtenció de resultats**	11/25/2020	12/29/2020	35
4.1	Conclusions del TFM	11/25/2020	12/10/2020	16
4.2	Redactar la memòria	12/11/2020	12/28/2020	18
4.3	**Entregar PEC4. TFM**	12/29/2020	12/29/2020	1
5	**Presentació**	12/30/2020	1/5/2021	7
5.1	Elaboració del vídeo	12/30/2020	01/05/2021	7
5.2	**Entregar vídeo**	01/05/2021	01/05/2021	1
6	**Defensa TFM**	01/06/2021	01/15/2021	10
6.1	Preparar defensa TFM	01/06/2021	01/15/2021	10
6.2	**Defensa TFM**	01/15/2021	01/15/2021	1

Il·lustració 1: Planificació

1.5.3 Diagrama de Gantt



Il·lustració 2: Diagrama de Gantt

1.6 Estat de l’art dels SIEM open source

La capacitat d’adaptació als canvis sempre ha estat un segell de garantia per a les empreses, però en l’actualitat aquest segell ha pujat la seva cotització fins a nivells molt elevats, degut a l’obligada acceleració dels canvis provocat per la pandèmia del COVID 19. Aquests canvis s’han focalitzat, en part, amb el teletreball i l’ús massius de les eines digitals, com podem observar per exemple en l’interès de Gartner en vers aquest tema amb alguna de les seves enquestes en referència al teletreball i la COVID19, “with coronavirus in mind are you ready for remote work”, publicat el 3 de març del 2020.

Una de les eines que tenen a l’abast les empreses, per mitigar els incidents de seguretat en aquesta vertiginosa implantació digital, son el SIEM, solució hibrida entre SIM (Security Information Management) i SEM (Security Event Management), que ens centralitza la gestió de tots els esdeveniments de la xarxa aportant una visió global de la seguretat. Per fer una petita valoració dels SIEM open source actuals més populars, amb llicència gratuïta, m’he basat en les cerques a Google i el quadrant màgic de Gartner.

El quadrant màgic de Gartner, “Magic Quadrant for Security Information and Event Management”, publicat el 18 de Febrer de 2020 posa el focus sobre un seguit d’eines molt interessants però que estan fora de l’abast d’aquest TFM degut al seu llicenciament, tot i això en podem extreure una informació força interessant en l’apartat que parla dels SIEM alternatius, on es destaca la solució “ELK Stack”.

Agafant com a referència aquest apunt de l’informe Gartner, he fet una cerca a Google buscant quines opcions hi ha amb la pila ELK i quins son els seus competidors.

Les solucions escollides per fer aquesta petita presentació son, ELK Stack + Wazuh, OSSIM, Apache Metron i Splunk.

1.6.1 ELK Stack + Wazuh

La unió d'aquestes dues solucions ens proporciona la funcionalitat i experiència en la gestió de logs de la pila ELK i una eina molt ben valorada per a la gestió de la seguretat i detecció d'anomalies com és Wazuh.

La solució ELK Stack consta de 4 productes Elasticsearch, Logstash, Beats i Kibana.

Elasticsearch, és un motor de cerca NoSQL basat en la llibreria Lucene molt popular en l'àmbit d'anàlisis de dades. Per realitzar les cerques utilitza un API amb l'esquema JSON.

Il·lustració 3: Logo Elasticsearch Font: Internet

Kibana, és la capa de visualització de dades mitjançant dashboards.

Il·lustració 4: Logo Kibana Font: Internet

Logstash, és el producte ubicat al servidor encarregat de rebre els logs de diferents orígens, processar-los i mitjançant un "pipeline" indexar-los normalment en la base de dades Elasticsearch.

Il·lustració 5: Logo Logstash Font: Internet

Beats, son agents lleugers que s'utilizen per recol·lectar logs de funcionalitats molt concretes i enviar-los a Logstash o Elasticsearch.

Il·lustració 6: Logo Beats Font: Internet

Wazuh, és un fork de OSSEC que va ser creat al 2008. Wazuh ha evolucionat incloent moltes més funcionalitats que el seu predecessor. El fork de Wazuh va treure la seva primera release al 2015.

Wazuh ens ofereix un mixt entre agent HIDS i SIEM. Per una part l'agent permet monitorar l'equip detectant anomalies i enviant tota aquesta informació al SIEM per a ser analitzada i correlacionada amb la resta d'informació del sistema, oferint detecció d'amenaces i resposta a incidents. Wazuh també permet la integració amb altres projectes com Suricata, que és un IDS per a la detecció d'anomalies en les comunicacions, Thehive, que és una plataforma per donar resposta als incidents de seguretat, entre molts altres.

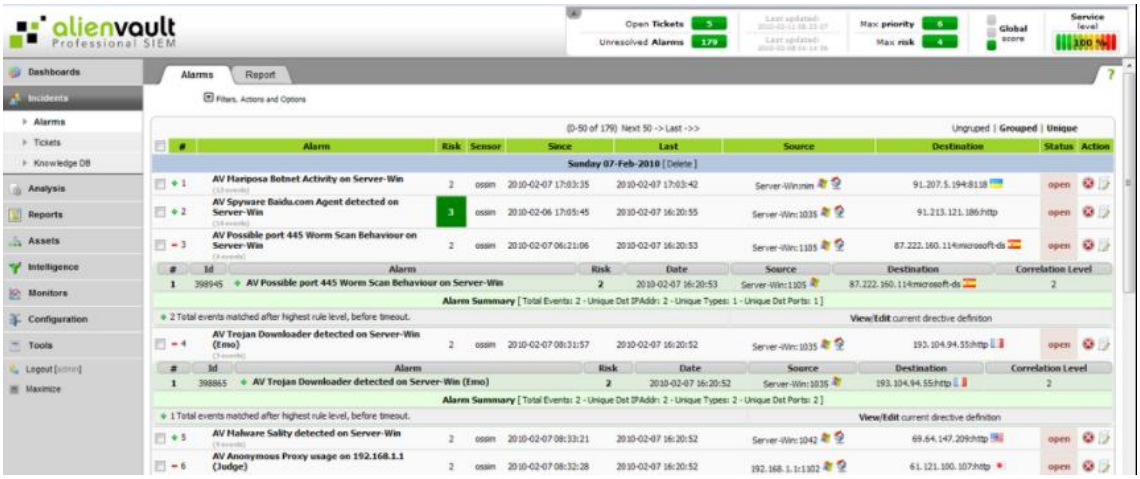
Il·lustració 7: Logo Wazuh Font: Internet

1.6.2 OSSIM

OSSIM, Open Source Security Information Management, aquest projecte es va iniciar al 2003 donant lloc al 2008 a l'empresa Alienvault i la seva actual solució de pagament Alienvault USM.

OSSIM és un conjunt d'eines per administrar la seguretat de la xarxa i per a la detecció i prevenció d'incidents.

OSSIM combina l'emmagatzematge de logs nativa i la seva capacitat de correlacionar-los, amb altres eines open source com Snort, que és un NIDS, Network Intrusion Detection System, Suricata, Munin, que és una eina de monitoratge, Nagios, per monitoritzar sistemes, OpenVas, solució que integra serveis per la gestió de vulnerabilitats, etc.



Il·lustració 8: Vista panell de control OSSIM Font: Wikipedia

1.6.3 Apache Metron

Apache Metron està desenvolupat dins el projecte CISCO OpenSOC, i ens proporciona funcionalitats per emmagatzemar, agregar i indexar logs a l'hora que també ens ofereix funcionalitats per analitzar i enriquir les dades, proporcionant-nos una eina per monitorar i analitzar la seguretat del nostre sistema. Apache Metron va treure la seva primera release el 2016.

Per emmagatzemar les dades utilitza Hadoop, Elasticsearch, o Solr, per a la visualització dels dashboards utilitza Kibana, i ofereix un API REST per interactuar-hi.

Il·lustració 9: Esquema Apache Metron Font: Wikimedia

1.6.4 Splunk

Splunk és un dels productes líders en l'àmbit dels SIEM tal i com indica el quadrant màgic dels SIEM 2020 de Gartner.
Al igual que Elastic Stack, Splunk ens ofereix un software per emmagatzemar, buscar, indexar, monitorar i analitzar dades generades per màquines, big data, en temps real, mitjançant una interface web amb dashboards personalitzables per l'usuari. Splunk a diferencia de Elastic Stack es presenta com un software integrat.
Splunk també disposa de l'opció SIEM amb el producte Splunk Enterprise Security amb llicència de pagament. Per altra banda Wazuh també és pot integrar amb Splunk, tot i que la versió gratuïta de Splunk te limitacions com la indexació de com a màxim 500MB diaris, entre altres.

Il·lustració 10: Logo Splunk Font: Wikimedia

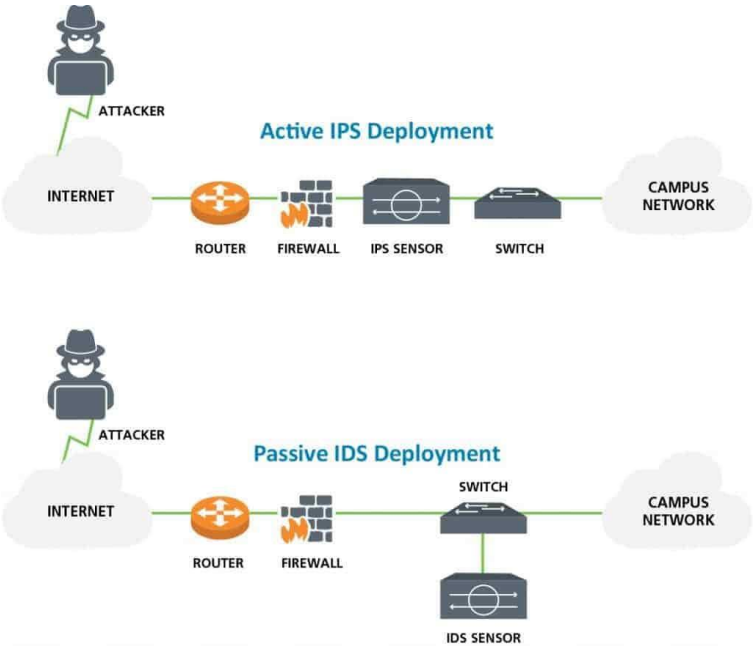
2. Descripcions

En aquest apartat s'exposen les descripcions dels principals elements de seguretat de gestió de logs que han de servir de base per tenir un millor control sobre la seguretat de la infraestructura TIC, Tecnologies de la Informació i les Comunicacions. Per fer-ho, es segueix el flux dels logs, des de que es generen i preprocesen al dispositiu mitjançant els agents, passant per la seva gestió i visualització al SIEM, fins a les alertes que permeten actuar en conseqüència. I per acabar s'exposa una petita descripció de l'amenaça amb la qual es prova el sistema de seguretat implantat, els Cryptolockers.

2.1 Generació de logs

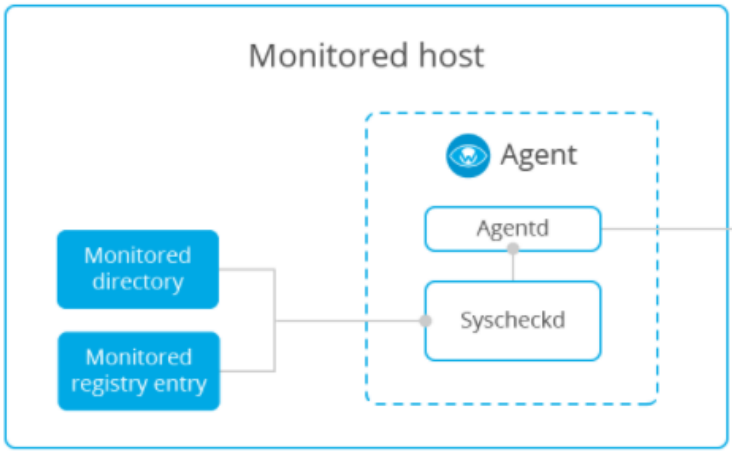
La generació de logs d'informació és un procés molt comú en qualsevol sistema d'una infraestructura TIC. Els logs permeten registrar informació dels esdeveniments que han ocorregut en un moment i dispositiu en concret per exemple: en un Firewall es pot registrar les comunicacions, amb l'origen, destí, tipus de protocol, etc., en un sistema operatiu es pot registrar l'usuari que ha fet login, l'equip on s'ha fet, si es correcte o no, etc, o en un servidor de fitxers també es pot registrar quan un fitxer s'ha modificat, quin usuari ho ha fet, etc. Tots aquests logs poden ser utilitzats per un sistema que els pugui interpretar i, a partir d'una base de dades de coneixement, determinar si s'està produint, o és possible que es produeixi, un incident de seguretat.

Els agents permeten recollir i preprocessar els logs, per tal d'enviar al SIEM només aquella informació que sigui rellevant per a la seguretat del sistema, d'aquesta manera s'evita un trànsit innecessari a la xarxa. En aquest punt es parla dels IDS (Intrusion Detection System) i IPS (Intrusión Prevention System) dispositius que permeten analitzar els logs en temps real en un determinat punt del sistema, i enviar la informació rellevant al SIEM i/o actuar en conseqüència.



Il·lustració 11: IDS vs IPS Font: https://www.digitalplanet.ie/ips-ids/

Els IDS, Intrusion Detection System, son sistemes que monitoritzen, en temps real, la xarxa buscant anomalies en un determinat punt de la infraestructura, comparen les dades monitorades amb bases de dades actualitzades d'atacs coneguts, i, en cas de trobar alguna coincidència, generen alarmes, però en cap cas actuen per parar l'atac. En aquest projecte s'utilitza un HIDS, Host Intrusion Detection System, que és un agent instal·lat en un equip per monitoritzar els esdeveniments que esdevenen en aquest, concretament es monitoritza els canvis en els fitxers d'un servidor mitjançant el component syscheckd de l'agent Wazuh.



Il·lustració 12:Agent Wazuh, File Integrity Monitoring (FIM) Font: https://www.programmersought.com/article/9734805292

Els IPS, Intrusion Prevention System, son sistemes que realitzen el mateix monitoratge que els IDS però en cas de detectar anomalies actuen en conseqüència bloquejant el trànsit. Un exemple de IDS es pot trobar en l'aplicació Suricata.

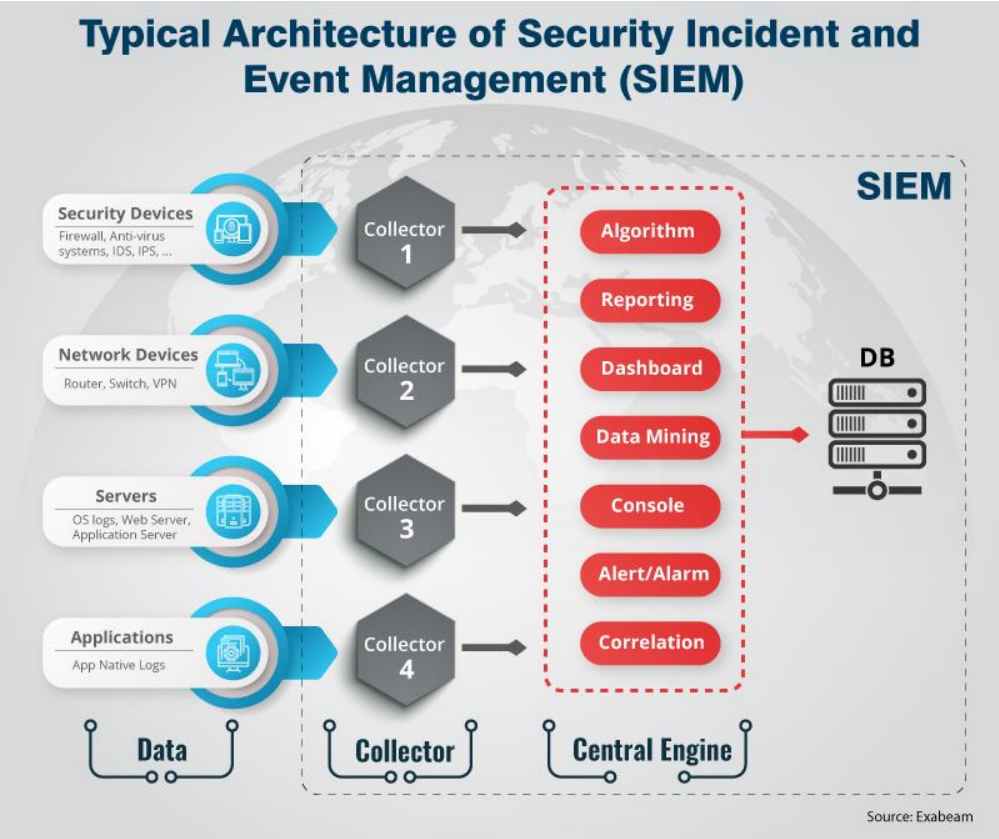
El principal avantatge dels IPS respecte als IDS és la seva ràpida actuació en cas d'incident bloquejant l'atac, tot i què, en el cas de falsos positius es poden produir bloquejos indeguts perjudicant el funcionament normal del sistema. També s'ha de tenir en compte que tant els IDS com els IPS son vulnerables a atacs DDoS[1], Distributed Denial of Service, i DoS, Denial of Service.

2.2 Gestió centralitzada dels esdeveniments de seguretat

El número d'esdeveniment de seguretat que es poden produir en un sistema per unitat de temps pot ser molt elevat i de diferents orígens, per tant, hi ha la necessitat de tenir un sistema d'emmagatzematge centralitzat que permeti normalitzar i correlacionar logs de diferents orígens, emmagatzemar un històric, etc., per tal de: limitar al màxim els falsos positius, tenir una capacitat de resposta ràpida d'avant dels incidents, oferir una visió global del compliment normatiu i permetre realitzar anàlisis forenses. En aquest apartat es comenta el funcionament del SIEM.

A principis de segle XX van començar a aparèixer les primeres versions comercials de SIEM; aquestes primeres versions combinaven el SIM (System Information Management) i el SEM (System Event Management) per oferir un producte unificat de gestió de logs i esdeveniments. En la segona generació de SIEM, que va arribar al voltant del 2011, es van millorar aspectes com: l'escalabilitat, correlació i enriquiment de la informació amb la utilització de tecnologia de Big Data centralitzada, també es van millorar els dashboards i els informes, i la configuració de les alertes. La introducció del Machine Learning per millorar la capacitat operativa és una de les principals millores que s'introdueixen en els SIEM a partir del 2015 i també tècniques com UEBA, User and Entity Behaviour Analytics, que estableix patrons de funcionaments base entre usuaris i entitats[2] i en monitoritza les variacions.
En definitiva un SIEM, recol·lecta molta informació de diferents tipus mitjançant agents, un cop rebuda, la correlaciona i la compara amb fonts d'amenaces conegudes i ens llança alarmes, per altra banda, també ens permet visualitzar tota aquesta informació en temps real gràcies als dashboards, i, a més a més, permet estudiar-ne els històrics i comprovar el compliment de la normativa vigent en quan a seguretat de la informació. Tota aquesta funcionalitat es complementa en els SIEM moderns amb: tecnologies de machine learning per millorar la detecció d'amenaces, monitorització continua del compliment normatiu, monitorització de l'usuari amb tècniques com UEBA, Threat Intelligence amb una base de dades molt més àmplia i actualitzada constantment, Incident response que intenta prioritzar els incidents utilitzant machine learning per reduir els falsos positius, i SOAR que promet millorar el temps de resposta als incidents automatitzant les respostes amb la mínima interacció humana.

[1] DoS: Aquest atac té la finalitat de bloquejar el sistema i/o servei al que va destinat enviant mes sol·licituds de peticions de les que pot resoldre. La principal diferència amb DDoS és l'origen de l'atac, amb DoS es produeix des d'un únic equip i amb l'atac DDoS es produeix des de múltiples equips simultàniament.
[2] entitat: servidors, aplicacions, etc.



Il·lustració 13: Esquema SIEM Font: Internet

Il·lustració 14: SIEM Modern Font: Internet

2.4 Cryptolocker

Cryptolocker és un Malware[3] de tipus Ransomware[4] que encripta els fitxers de l'equip infectat utilitzant criptografia de clau pública RSA. En aquest apartat escric algunes línies parlant del Ransomware i com afecta a les empreses.

El Ransomware busca accedir a l'equip de la víctima per mitjà d'atacs d'enginyeria social o buscant vulnerabilitats en el perímetre de l'empresa. Una vegada ha accededit a l'equip vulnerable encripta la informació i es propaga per la xarxa en busca de més equips vulnerables. L'atacant guarda la clau per a desencriptar els fitxers i demana un rescat econòmic, en anglès Ransom, en bitcoins a canvi d'aquesta.

La seva aparició data del anys 80 però, és ara quan està creixent el seu ús de manera exponencial per part dels delinqüents, i, és què, si tenim en compte: la gran quantitat de dispositius que utilitzem avui en dia, els avenços en criptografia, formes de pagament totalment anònimes, com els bitcoins, i l'acceleració tecnològica en detriment de la seguretat, degut a la pandemia del COVID19; es donen un conjunt de factors que fan que sigui molt rentable per als delinqüents la utilització d'aquest atacs.

Alguns dels Ransomware més popular son:

- AIDS info disk: al 1989 aquest ransomware va causar una pèrdua d'informació significativa en la comunitat científica després de ser enviat amb disquets a diverses associacions d'investigació contra la SIDA. Aquest ransomware s'instal·la al sistema modificant el fitxer AUTOEXEC.bat i demana un rescat per poder recuperar el control de l'equip.
- WannaCry: que al 2017 va aprofitar un forat de seguretat en el protocol SMB per infectar i encriptar molts servidors de moltes empreses, al voltant de 200.000 usuaris de diferents països van ser víctimes del seu atac. Va ser un dels primers Ransomwares a gran escala
- Cerber: Aquest Ransomware és un producte RaaS[5] què, mitjançant subscripció a canvi d'un percentatge dels beneficis, permet als delinqüents utilitzar-lo amb un campanya de phishing per correu electrònic amb un document adjunt, que un cop obert instal·la el virus i encripta la informació.

La defensa contra aquest tipus d'atacs és complexa i cal afrontar-la des de diferents punts de vista:

- Humà: Un dels factors més vulnerables són les persones i cal prevenir als treballadors sobre els atacs d'enginyeria social, formant i donant-los eines per identificar els atacs a temps.
- Del Sistema: Configurant els recursos necessaris per, tenir una bona protecció i una bona resposta davant d'un incident. I això ho podem aconseguir amb proteccions perimetrals,

[3] Malware: de l'anglès "**mal**icious soft**ware"**, és un software amb intencions malicioses.
[4] Ransomware: és una aplicació maliciosa que busca segrestar les dades de la víctima per demanar-ne un rescat a canvi de tornar-ne l'accés.
[5] RaaS: Ransom as a service

segmentació de la xarxa, actualitzacions dels sistemes, eines de backup, eines internes de monitoratge i detecció (IDS, IPS, SIEM, ...) i pla de contingència, entre altres.

3. Solució aplicada al cas d'ús

En aquest punt es descriu el cas d'ús i la solució escollida per afrontar la implantació del projecte, que és Elastic Stack, amb el motor de Machine Learning, el servidor Wazuh i el seu plugin per a Elastic Stack. I també, s'explica la integració de Wazuh amb Teams per a la gestió de les alertes.

3.1 Descripció del cas d'ús

L'empresa on estic treballant actualment disposa d'un CPD centralitzat amb diferents servidors que donen servei als usuaris. Un dels serveis que s'ofereix és el servidor de fitxers objecte d'estudi en aquest projecte, en el qual s'instal·larà l'agent HIDS. Al CPD també es disposa d'una plataforma de gestió de contenidors amb Docker en la que s'instal·larà tota la plataforma SIEM, per altra banda el departament TIC té un canal de Teams per a la gestió de les alertes de tota la infraestructura, i que també s'utilitzarà per rebre les alertes generades pel SIEM.

3.2 Elastic Stack

Elastic Stack, en aquest projecte, s'encarrega d'emmagatzemar i gestionar els logs i esdeveniments de seguretat generats per l'agent HIDS, i de mostrar la informació amb dashboards personalitzats. Amb l'ajuda del plugin de Machine Learning s'avaluarà com aquest pot millorar l'eficiència en la detecció de falsos positius.

Elastic Stack és l'acrònim de quatre productes Open Source de l'empresa Elastic NV: Elasticsearch, Logstash, Kibana i Beats. En aquesta pila els 4 components tenen una funció molt definida: Elasticsearch és el motor de cerca, indexació i análisis, Logstash s'encarrega de rebre els logs processar-los i enviar-los a Elasticsearch, Kibana ens ofereix la informació d'una forma visual, gràfica i amigable, i Beats és un client lleuger que captura els logs d'una tipologia concreta per enviar-los a Elasticsearch o Logstash.

Tot seguit es descriu el funcionament d'aquests quatre productes i el seu plugin de pagament Machine Learning.

3.2.1 Elasticsearch

Elasticsearch és el cor de Elastic Stack i s'encarrega d'emmagatzemar, indexar i analitzar les dades; amb un motor de cerca distribuït, NoSQL i basat en la llibreria Apache lucene; una llibreria escrita originalment per Doug Cutting amb el llenguatge Java l'any 1999.

Elasticsearch emmagatzema i indexa estructures de dades complexes serialitzades en documents JSON de manera distribuida en un clúster amb diferents nodes, i la interacció es realitza mitjançant un API Restful.

La unitat de cerca i indexació, és el document que a la vegada conté un o més fitxers, col·lecció de parells clau-valor, on hi ha continguda la informació. Cada camp de dades està indexat i té

una estructura de dades dedicada i optimitzada, per exemple, els camps de text s'indexen de forma invertida, és a dir, que s'enumera cada paraula única que apareix i en els documents que es troba, els camps numèrics i geogràfics amb estructures d'arbre BKD[6], etc.
Per interactuar amb Elasticsearch s'utilitza el seu API Restful, per exemple per afegir un document nou:

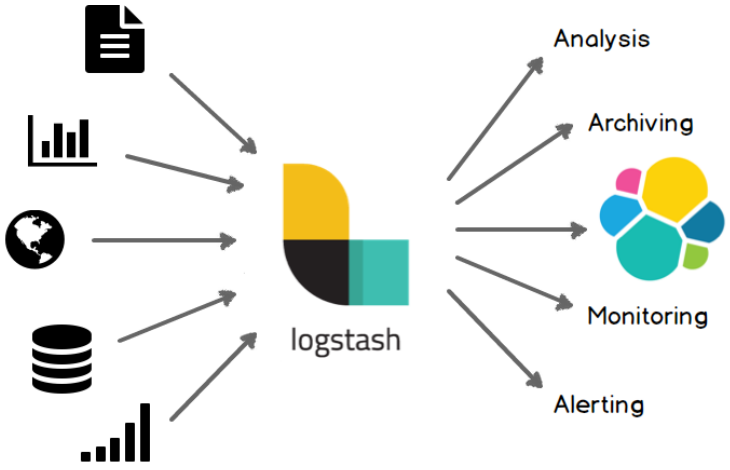
```
POST /<target>/_doc/<_id>
{
  "@timestamp": "2020-12-07T11:06:07.000Z",
  "user": {
    "id": "8a4f500d"
  },
  "message": "Login successful"
}
```

Exemple tret de la web de Elastic.co

on:
<target> és el nom del data stream o index on s'emmagatzema la informació
_doc o _create ens garanteix que només s'indexarà si no existeix el document.
<_id> és opcional i un identificador únic per aquest document. Si es deixa en blanc s'assigna automàticament. S'utilitza per modificacions o eliminacions futures del mateix.

3.2.2 Logstash

Logstash és la solució de Elastic Stack que s'encarrega de rebre els logs de diferents orígens, normalitzar-los i enviar-los a Elasticsearch o altres plataformes. Logstash ens ofereix un arquitectura de plugins oberta i extensible a la comunitat, que permet configurar diferents orígens de les dades, filtres i destins.



Il·lustració 15: Logstash Font: web de Elastic

[6] BKD: És un tipus d'arbre utilitzat per a cercar dades multidimensionals.

El funcionament de Logstash està estructurat en tres estats comunicats entre si de manera lineal: input -> filter -> output, i cada un d'aquests pot estar compost per diferents plugins segons les necessitats.

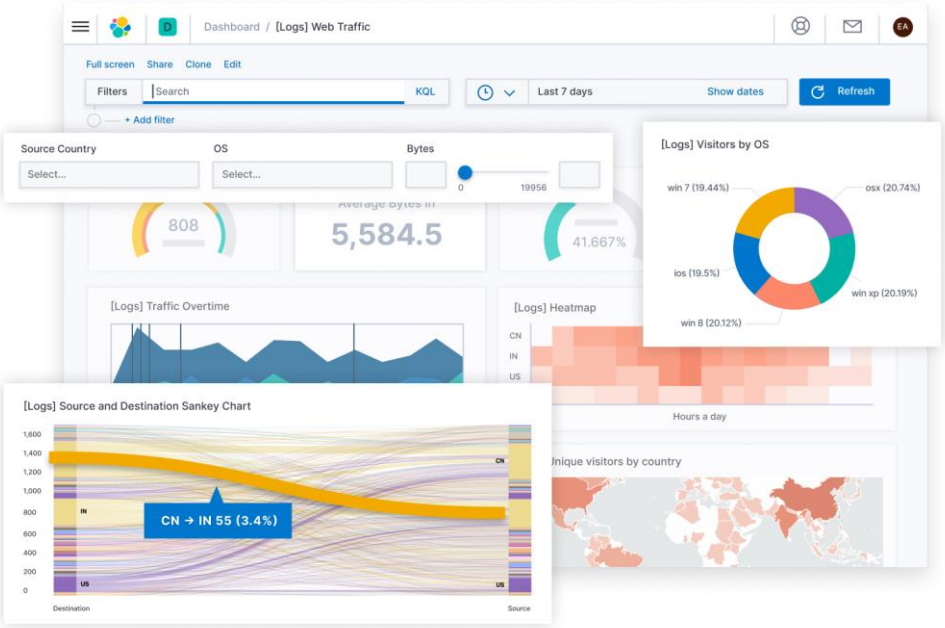
1. En l'estat input els plugins s'encarreguen d'obtenir la informació dels diferents orígens.
   Aquí es pot consultar el llistat dels plugins:
   https://www.elastic.co/guide/en/logstash/7.9/input-plugins.html
2. En l'estat filter els plugins s'encarreguen de tractar i processar les dades, aplicant un o diferents plugins segons els criteris establerts.
   Aquí es pot consultar el llistat dels plugins:
   https://www.elastic.co/guide/en/logstash/7.9/filter-plugins.html
3. I l'última fase del procés son els plugins de l'estat output, que envien la informació al destí escollit.
   Aquí es pot consultar el llistat dels plugins:
   https://www.elastic.co/guide/en/logstash/7.9/output-plugins.html

3.2.3 Kibana

Kibana és la eina què es troba al cap damunt de Elastic Stack, oferint la gestió gràfica de tota la solució.
Aquesta ofereix la oportunitat de visualitzar les dades mitjançant dashboards personalitzables per l'usuari, permet gestionar Elastic Stack amb un entorn gràfic i dona una eina on centralitzar la gestió de tots els productes de Elastic i els plugins externs.

Des de la pantalla gràfica de Kibana es pot:

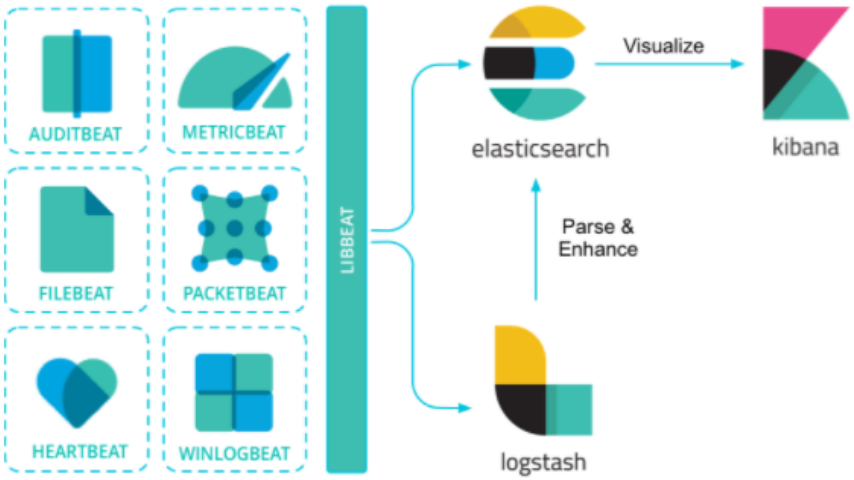
1. Entrar dades: permet l'entrada de dades, amb File Data Visualizer, a partir de fitxers de log i/o csv, i, indexar i crear flux de dades a Elasticsearch.
2. Explorar les dades: amb Discover es poden cercar i filtrar les dades indexades a Elasticsearch, per tal de, tenir un visió més detallada i examinar més a fons les dades.
3. Visualitzar i analitzar les dades: amb els Dashboards personalitzables es pot unificar la visualització de diferent informació i agilitzar-ne l'anàlisi. Per visualitzar-la tenim les opcions: Visualize que ofereix gràfiques, taules, mètriques, etc.; Canvas que permet personalitzar les visualitzacions amb colors, fonts, etc; Maps per mostrar dades geogràfiques a escala, etc; i TSVB per mostrar dades en una línia temporal.



Il·lustració 16: Kibana Font: web de Elastic

3.2.4 Beats

És una aplicació open source d'enviament de dades amb un propòsit molt concret. La solució Elastic Stack utilitza aquesta funcionalitat com a client lleuger per enviar logs amb un propòsit concret directament a Elasticsearch o mitjançant Logstash.



Il·lustració 17: Beats Font: web de Elastic

3.2.5 Machine Learning

El machine learning consisteix en automatitzar l'aprenentatge d'un sistema mitjançant algorismes per detectar patrons o tendències entre les dades. El seu objectiu és tenir un model que resol una tasca concreta i entrenar-lo amb una gran quantitat de dades, per tal de fer prediccions i detectar tendències.

Elastic ofereix la funcionalitat de machine learning amb llicència de pagament o una llicència de prova de 30 dies, i per poder utilitzar-la cal que el clúster de Elasticsearch tingui almenys un node amb el rol de machine learning activat que executi aquests treballs.

La configuració es defineix en 3 passos: càrrega de dades, creació dels treballs amb una i múltiples mètriques i interpretar els resultats per detectar anomalies.

- Càrrega de dades: Les dades es carreguen a partir de Elasticsearch o enviant-les directament fent un POST al API, i s'utilitza el concepte de Datafeed, que és un conjunt de dades recollides a partir d'unes propietats prefixades.
- Treballs o "jobs" de machine learning: un job conté la configuració i metadades per realitzar la tasca d'anàlisi. Alguns conceptes interessants de la configuració dels jobs són:
    - Bucket Span: Interval de temps que s'utilitza per modelar les dades.
    - Cardinality: Per definir comportaments tenint en compte agrupacions d'entitats relacionades.
    - Detectors: Aplica una funció d'anàlisi sobre un camp específic de les dades.
    - Influencers: habitualment es designen els usuaris o IP com a influencers per detectar el causant de l'anomalia.
    - Model memory limits: s'utilitza per establir un màxim de memòria a utilitzar per cada procés d'anàlisi.
- La visualització dels anàlisis es fa mitjançant l'entorn gràfic Kibana:
    - Explorador d'anomalies: Ens proporciona una vista del resultat de l'anàlisi amb diferents gràfiques.

Il·lustració 18: Kibana explorador d'analítiques Font: web Elastic

- Visor de mètriques: Només està disponible en jobs que analitzen una única sèrie de dades de temps, i, mostra les dades analitzades i les esperades.

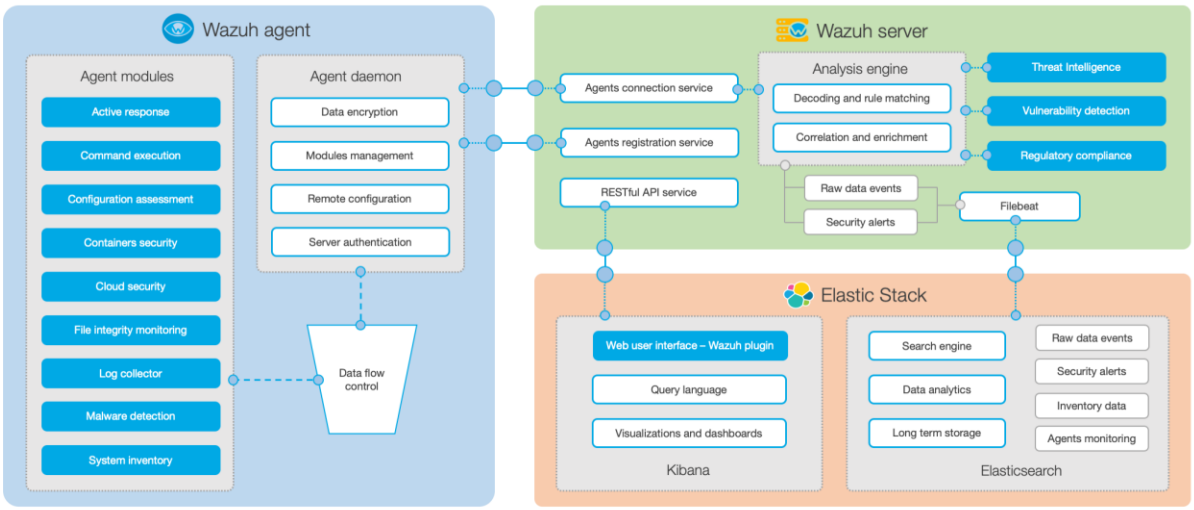
Il·lustració 19: Kibana visor de mètriques Font: web Elastic

3.3 Wazuh i Elastic Stack

La solució Elastic Stack integra d'una manera molt fàcil el software Wazuh i permet gestionar-lo des del mateix entorn gràfic Kibana, utilitzant Elasticsearch com a motor de cerca.

A continuació es fa una petita descripció del software Wazuh, la seva integració dins Elastic Stack i la integració de Wazuh amb Teams per a la gestió de les alertes.

3.3.1 Wazuh



Il·lustració 20: Esquema Wazuh Font: web Wazuh

Wazuh és un fork [7]del projecte open source OSSIM HIDS, que està format pels components:

- Agent Wazuh: És multi plataforma i modular. Mitjançant els seus components ofereix funcionalitats: d'inventari de dades, monitorització de logs, detecció de malware, monitorització del sistema de fitxers, etc.
- Wazuh server: És la part que analitza, correlaciona i enriqueix les dades rebudes dels agents. També, disposa d'un API Restful per interactuar-hi i de la funcionalitat Filebeat per exportar els esdeveniments i alertes a Elasticsearch.
- Elastic Stack: s'utilitza per interactuar amb Wazuh server i visualitzar les dades analitzades gràficament mitjançant un plugin, i també com a motor de cerca.

Les funcionalitat que ens ofereix Wazuh son les següents:

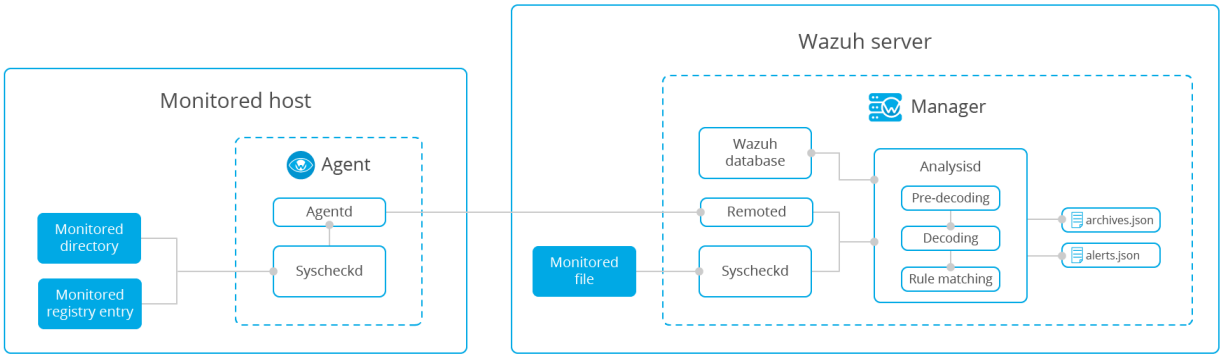
- Anàlisi de seguretat: El servidor Wazuh s'encarrega de recollir les dades dels agents, agregar-les, indexar-les i realitzar els anàlisis de seguretat per detectar possibles atacs i anomalies.
- Detecció d'intrusos: Els agents de Wazuh escanegen els equips on es troben instal·lats buscant anomalies sospitoses, a més a més, els components del servidor utilitzen bases de dades de patrons coneguts per detectar incidents de seguretat.
- Anàlisi de logs: els agents poden recollir els logs del sistema i enviar-los al servidor central per ser analitzats.
- Monitoratge de la integritat dels fitxers: Wazuh monitora els canvis que es produeixen en els fitxers, tant a nivell de contingut, com de permisos, els usuaris que realitzen els canvis, etc. Combinat amb la detecció d'intrusos ens pot ajudar a diagnosticar equips compromesos.

[7] Fork: En enginyeria de software un fork es produeix quan s'agafa un còpia d'un producte ja existent com a punt de partida d'una nova solució.

- Detecció de vulnerabilitats: Els agents recopilen el software dels equips i envien la informació al servidor que ho correlaciona amb les base de dades CVE, Common Vulnerabilities and Exposure, per detectar vulnerabilitats.
- Avaluació de la configuració: Wazuh pot monitoritzar sistemes i aplicacions, i determinar si compleixen les polítiques de seguretat de l'empresa.
- Resposta a incidents: Wazuh ofereix algunes funcionalitat preestablertes per actuar en cas d'incident per exemple: bloquejar un accés, executar scripts al host, etc.
- Avaluació compliment normatiu: Wazuh ofereix els controls necessaris per complir amb les regulacions i els estàndards de la industria com PCI DSS, Payment Card Industry Data Security Standard, o GDPR, General Data Protection Regulation.
- Monitorització de la seguretat al Cloud: Wazuh permet monitoritzar la infraestructura del cloud a nivell de API.
- Seguretat en contenidors: permet detectar incidents, anomalies i vulnerabilitats observant el comportament dels contenidors amb la integració nativa dels agents de Wazuh

3.3.2 Wazuh agent

L'agent de Wazuh és l'encarregat de recollir les dades dels diferents host i enviar-les al servidor Wazuh per a ser interpretades. Depenent dels plugins configurats en l'agent les dades enviades son: logs de sistema i aplicacions, vulnerabilitats, inventaris, integritat dels fitxers, etc. En aquest apartat revisarem la configuració de l'agent per al plugin File Integrity Monitoring, què es el que s'utilitzarà en la implementació. Aquest plugin permet monitoritzar les modificacions que es produeix als fitxers i les claus del registre seleccionats i enviar alertes.



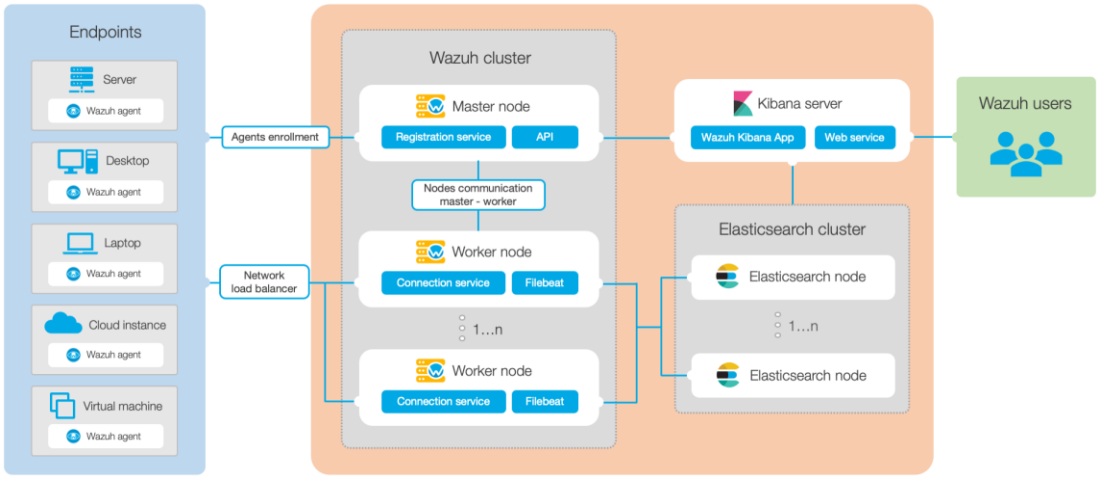
Il·lustració 21: Plugin File Integrity Monitoring Font: web Wazuh

Una vegada instal·lat l'agent s'ha de procedir a configurat el plugin File Integrity Monitoring editant el contingut de les etiquetes <Syscheck> del fitxer de configuració ossec.conf.
Aquest plugin ofereix les opcions d'indicar la freqüència, temps en segons de cada quan s'executarà l'escaneig, els directoris a escanejar, si volem ignorar algun fitxer en concret dins el directori seleccionat i alerta si es creen fitxers nous dins el directori, entre altres opcions.

En aquesta url es poden observar exemples de configuració:
https://documentation.wazuh.com/3.7/user-manual/capabilities/file-integrity/fim-configuration.html#basic-usage

3.3.3 Integració de Wazuh amb Elastic Stack

La integració del servidor Wazuh i Elastic Stack es fa mitjançant un plugin que interactua amb Wazuh mitjançant l'API Restful que ofereix aquest.
Aquesta integració permet utilitzar les potents eines de Elastic Stack per gestionar el servidor Wazuh, amb el seu entorn gràfic Kibana, el motor de cerca Elasticsearch, les propietats de machine learning, etc…



Il·lustració 22: Arquitectura Wazuh i Elastic Stack Font: http://www.wazuh.com

3.3.4 Integració de Wazuh amb Teams

Wazuh fins al moment no té cap integració específica amb Teams, tal i com s'indica en el seu repositori de github, https://github.com/wazuh/wazuh/issues/6349. Per altra banda, en aquest mateix fil s'informa que la integració amb Teams es pot fer utilitzant la funcionalitat de Wazuh d'integració amb APIs externes.

Per tal de realitzar la integració entre Wazuh i Teams s'han de seguir 2 passos:

1. Primer, crear un webhook sobre un canal de Teams ja existent, tal i com s'indica en aquesta url: https://docs.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook
2. Segon, customitzar Wazuh segons aquest 2 passos:
    1. Editar el fitxer de configuració ossec.conf:

```
<integration>
  <name>custom-integration</name>
  <hook_url>WEBHOOK</hook_url>
  <api_key>KEY</api_key>
  <level>10</level>
  <rule_id>ID</rule_id>
  <group>multiple_drops|authentication_failures</group>
  <event_location>LOCATION</event_location>
  <alert_format>json</alert_format>
</integration>
```

name: Fa referència al nom del script que realitzarà la integració, tenint en compte que sempre ha de començar per "custom-".
hook_url: És la url del del API externa. Aquesta opció és opcional, ja què, es pot incloure directament al script.

api_key: La clau del API extern. Aquesta opció també és opcional per la mateixa raó que el hook_url.
level: El nivell a partir del qual el script rebrà les alertes.
rule_id: Establir filtres segons identificadors d'alertes.
group: Establir filtres segons grups d'alertes.
event_location: Establir filtres segons l'origen de les alertes**.**
alert_format: Format amb el que rebrà les dades el script. Es recomana JSON, per defecte s'envia en format full_log.

2. I crear el script d'integració amb les consideracions següents:

```
#!/usr/bin/env python
import sys
import json
import requests
from requests.auth import HTTPBasicAuth

# Get parameters
alert_file = sys.argv[1]
api_key = sys.argv[2]
hook_url = sys.argv[3]

# Read the alert file
alert_json = json.loads(alert_file.read())
alert_file.close()

# Read the alert properties
alert_level = alert_json['rule']['level']
description = alert_json['rule']['description']

# Generate request
msg_data = {
  'summary': 'Wazuh Alert ALERT_NAME',
  'themeColor': 'ff0000',
  'sections': {
    'title': 'Wazuh alert',
    'activityImage': 'URL_IMAGE',
    'activityTitle': 'ALERT_NAME',
    'activitySubtitle': 'ALERT_DATE'
  },
  'facts': [
    {
      'name': alert_level,
      'value': alert_description
    }
  ]
}
```

```
# Generate header
headers = {
    'Content-Type': 'application/json'
}

# Send the request
requests.post(hook_url, headers=headers,
data=json.dumps(msg_data))

sys.exit(0)
```

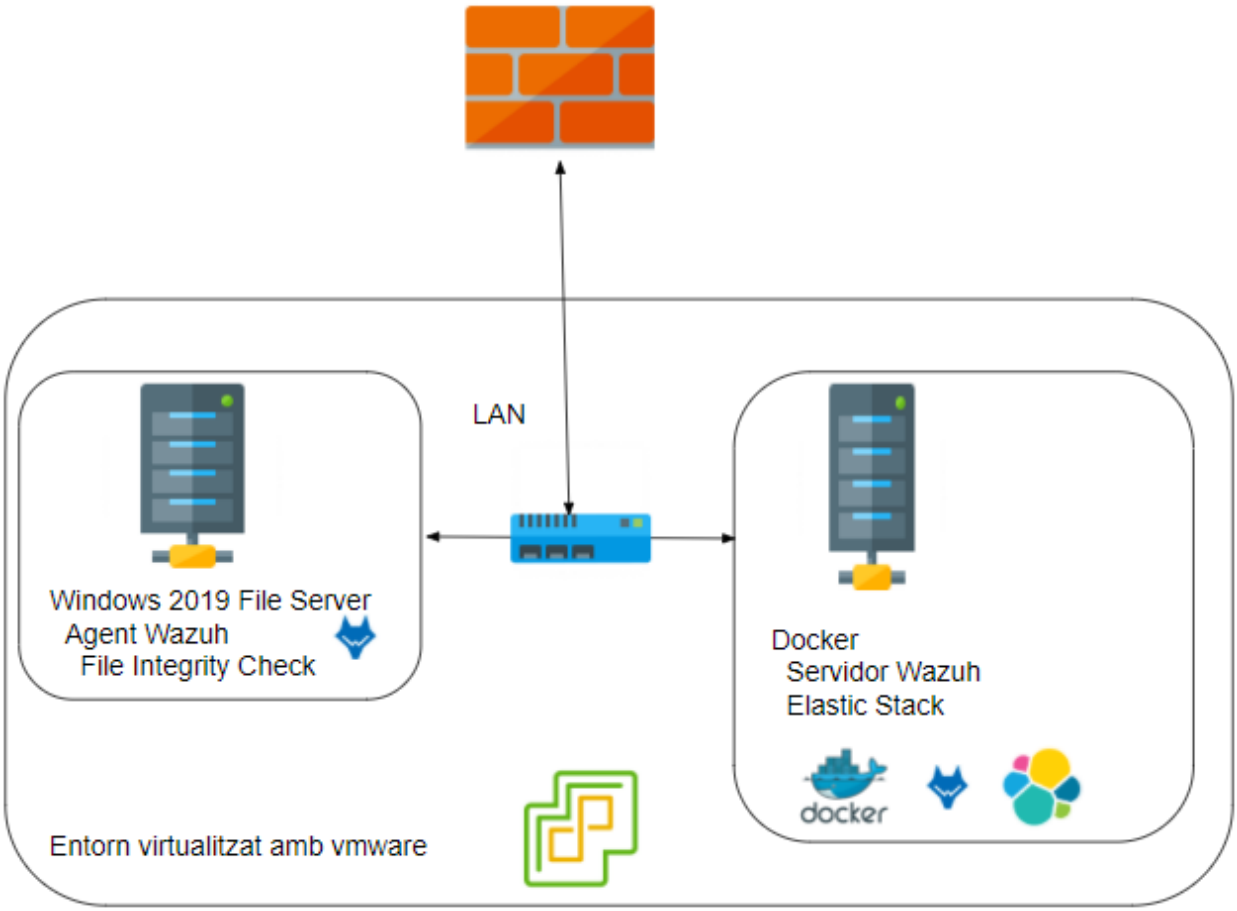
La primera línia del script descriu l'intèrpret que s'utilitzarà, en aquest cas Python. A continuació es recuperen les variables de configuració mitjançant els paràmetres. Tot seguit és recupera la informació de l'alerta del fitxer i es construeix el cos de la informació a enviar a Teams. I, per acabar, s'envia la informació de l'alerta al canal de Teams amb la url del webhook.

Tal i com s'indica en la documentació, es recomana visualitzar el fitxer /logs/alerts/alerts.json per veure l'esquema de les alertes.

Aquest no és un script funcional. En aquest apartat només es fa una referència al seu esquema, ja que en la part de la implementació és definirà la seva funcionalitat.

4. Esquema de la solució

L'esquema de la solució és un punt important del projecte, ja què, s'estableix un esquema gràfic de com s'estructuren totes les peces del trencaclosques adaptades al cas d'ús. En aquest apartat es presenta l'esquema gràfic de la implantació.



Il·lustració 23: Esquema de la solució

Els requisits per aquesta instal·lació, pel que fa a la part del SIEM, són tenir Docker i Docker Compose instal·lat en un equip amb com a mínim 6GB de memòria RAM. En la documentació de Wazuh s'indica també que cal incrementar el vm.max_map_count fins a 262144.

Per preparar la implantació de l'entorn primer cal descarregar el fitxer docker-compose.yml del repositori de github de wazuh-docker i modificar-lo segons la configuració desitjada, part què s'abordarà en els següents apartats.

En aquest enllaç es pot consultar la documentació de Wazuh per a realitzar la implantació amb Docker: https://documentation.wazuh.com/4.0/docker/wazuh-container.html

I en aquest altre enllaç, del repositori Github, podem trobar la implementació de Wazuh amb Docker: https://github.com/wazuh/wazuh-docker

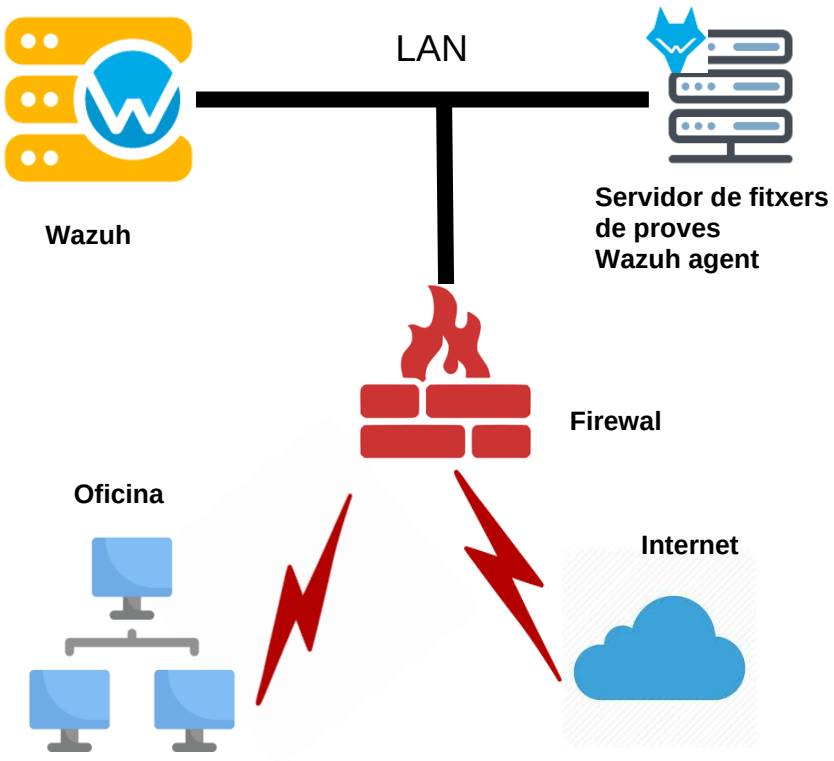
En la documentació de Wazuh-docker s'ha observat que recentment s'ha fet el canvi en la implantació de la solució Wazuh en Docker, de Elastic Stack a ODFE (Open Distro for Elasticsearch). En la següent part del projecte, la implantació, s'haurà de valorar quina opció es segueix, si ODFE o Elastic Stack.

5. Implantació

5.1 Descripció del cas d'ús

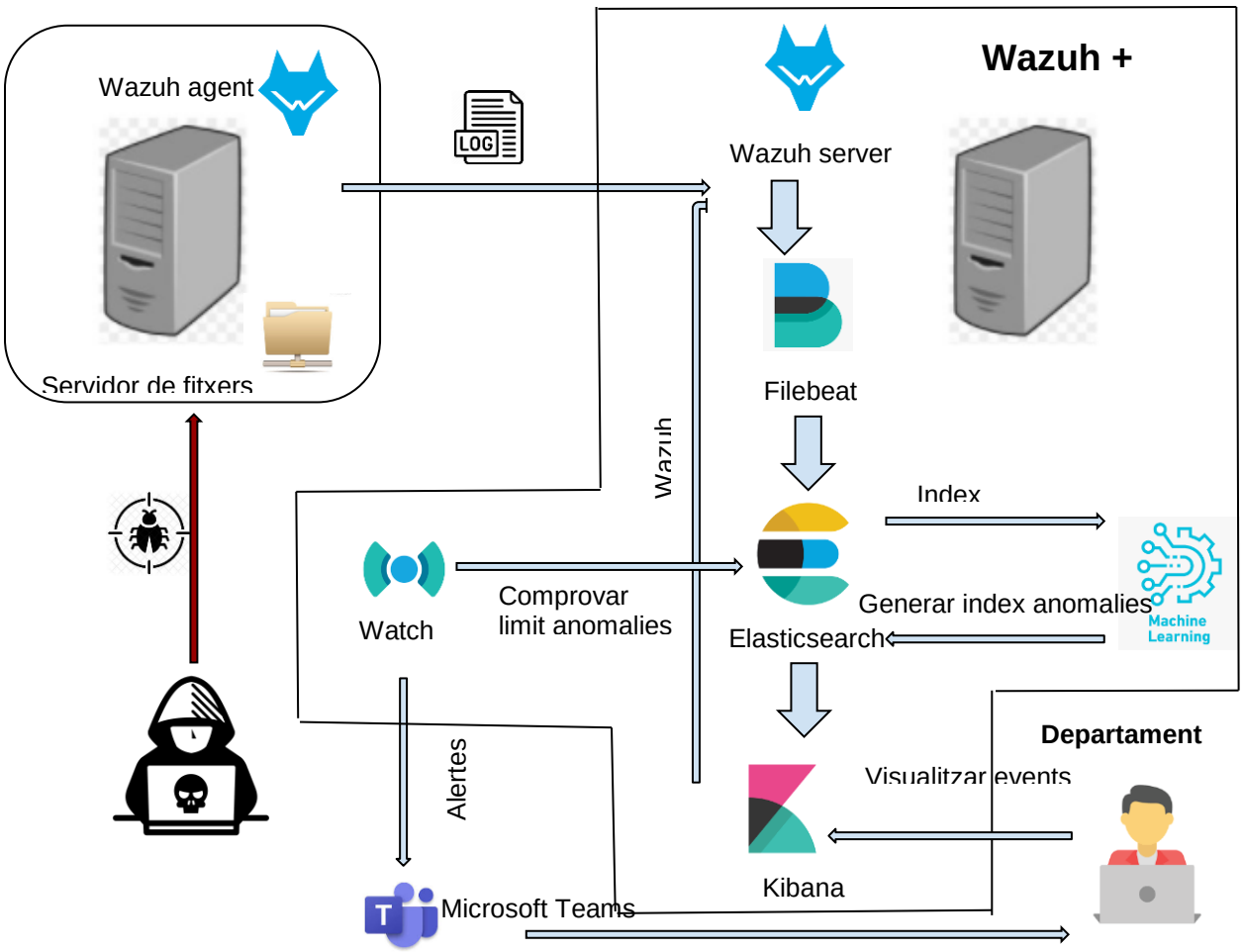
L'empresa on es realitza la POC disposa d'un CPD virtualitzat amb més de 30 servidors, 6 dels quals són servidors de fitxers. També disposa de connexió a Internet i connexió segura amb més de 20 oficines de la mateixa empresa mitjançant un firewall. L'objecte d'estudi d'aquesta POC és veure el comportament del SIEM amb un atac de Ransomware, i per dur-ho a terme s'ha utilitzat un servidor de fitxers de proves ubicat dins l'entorn virtual de l'empresa.

A continuació es presenta l'esquema de xarxa de l'empresa on es realitza la POC.



Il·lustració 24: Esquema de xarxa del cas d'ús

Per tal de tenir una visió generalista del funcionament de la POC a continuació es presenta l'esquema de tot el procés que realitza un log, des que es produeix l'atac fins que arriba l'alerta al departament IT.



Il·lustració 25: Esquema detallat del cas d'ús

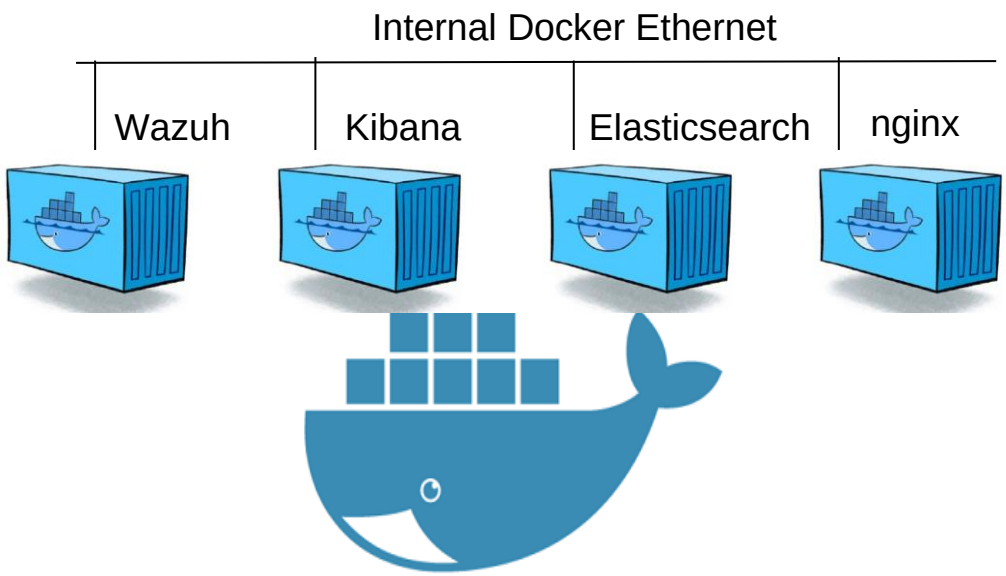
5.2 Instal·lació SIEM

En l'apartat de documentació d'aquest projecte s'ha detectat que la instal·lació de la solució Wazuh, recentment, i des de la web oficial de Wazuh, es recomana fer-la amb la solució Open Distro for Elasticsearch, una solució llançada des de AWS per preservar que Elasticsearch sigui un projecte Open Source, segons comenten en la seva nota informativa, https://aws.amazon.com/es/blogs/opensource/launching-open-distro-for-elasticsearch-security-features-on-amazon-elasticsearch-service/

A primera vista la solució Wazuh amb ODFE sembla que és una solució mes adaptada i més enfocada a agilitzar el funcionament de Wazuh, tot i això s'ha decidit què, per a la implantació de la POC, utilitzar la solució ELK per tal de poder avaluar la funcionalitat de Machine Learning.

5.2.1 Instal·lació Wazuh server i Elastic Stack

La instal·lació de Wazuh server i Elastick Stack es realitza en un entorn Docker ja preinstal·lat, situat en una xarxa visible des del servidor Windows on es realitza la instal·lació del HIDS Wazuh. A continuació es mostra l'esquema de contenidors Docker de la POC.



Ports públics:
Administrar Wazuh server amb Kibana:
HTTPS -> 443
HTTP -> 80
Connexió agents HIDS:
1514 -> Servei Recepció logs agents
1515 -> Servei Registre agents
514 -> Servei Recepció syslog

Il·lustració 26: Esquema contenidors Docker

La instal·lació s'ha realitzat mitjançant l'eina docker-compose amb el següent fitxer docker-compose.yml d'instal·lació:

docker-compose.yml

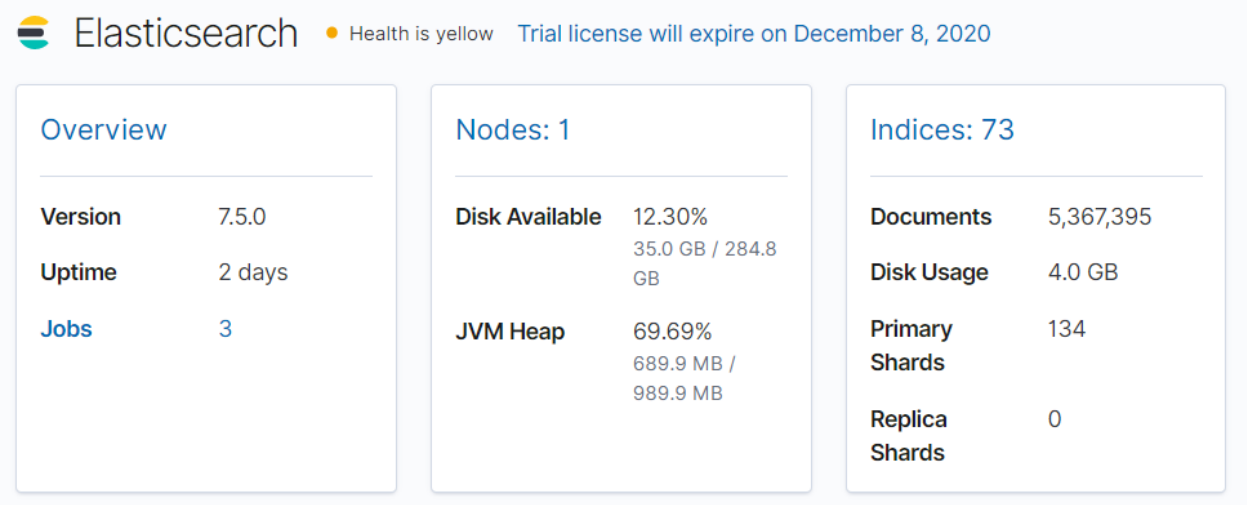
```
# Wazuh App Copyright (C) 2020 Wazuh Inc. (License GPLv2)
version: '2'

services:
  wazuh:
    image: wazuh/wazuh
    hostname: wazuh-manager
    restart: always
    ports:
      - "1514:1514/udp"
      - "1515:1515"
      - "514:514/udp"
      - "55000:55000"
```

```
elasticsearch:
  image: wazuh/wazuh-elasticsearch
  hostname: elasticsearch
  restart: always
  ports:
    - "9200:9200"
  environment:
    - "ES_JAVA_OPTS=-Xms1g -Xmx1g"
    - ELASTIC_CLUSTER=true
    - CLUSTER_NODE_MASTER=true
  ulimits:
    memlock:
      soft: -1
      hard: -1

kibana:
  image: wazuh/wazuh-kibana
  hostname: kibana
  restart: always
  depends_on:
    - elasticsearch
  links:
    - elasticsearch:elasticsearch
    - wazuh:wazuh

nginx:
  image: wazuh/wazuh-nginx
  hostname: nginx
  restart: always
  environment:
    - NGINX_PORT=443
    - NGINX_CREDENTIALS
  ports:
    - "80:80"
    - “443:443"
  depends_on:
    - kibana
  links:
    - kibana:kibana
```

El fitxer està dividit en 4 serveis/contenidors: wazuh, elasticsearch, kibana i nginx. La informació per elaborar aquest fitxer s’ha extret del compte oficial de Github de Wazuh, que malgrat haver

optat, per a les noves versions, per utilitzar la versió Elasticsearch ODFE, continua facilitant la configuració per fer la instal·lació amb Elasticsearch en entorns Docker.

La versió instal·lada pel que fa a Elasticsearch és la 7.5.0



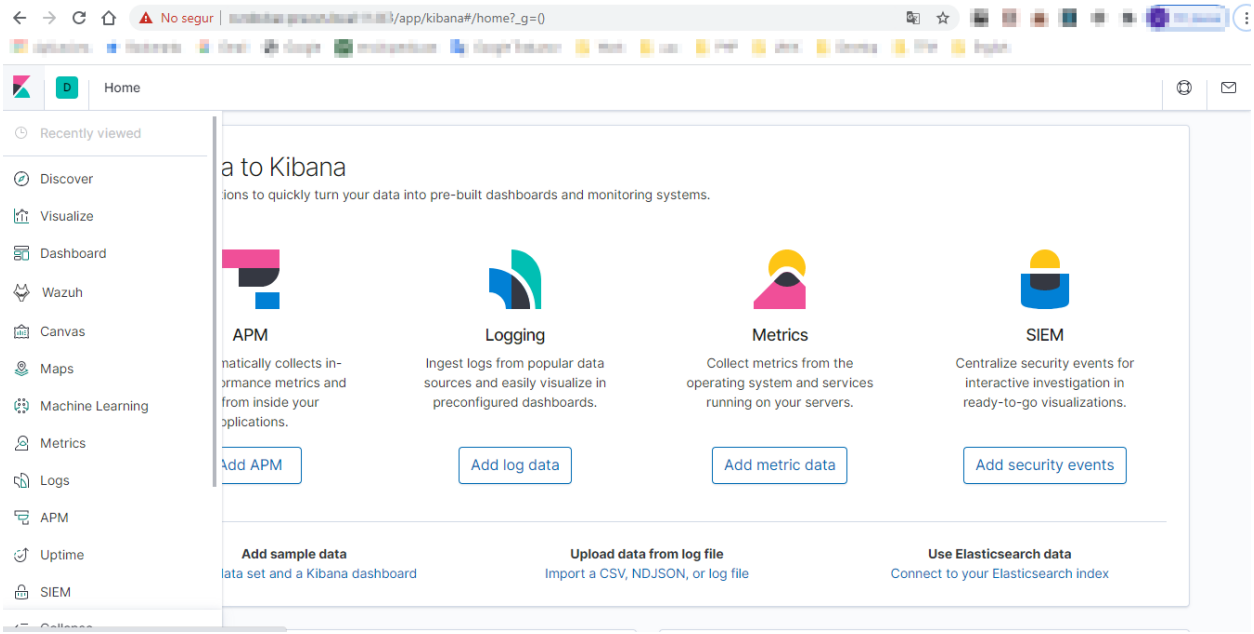
Il·lustració 27: Versió de Elasticsearch

Un vegada executada la següent ordre en el directori on tenim el fitxer de configuració, ja podem disposar de l'entorn Wazuh server i Elastic Stack.

```
docker-compose up -d
```

Per accedir a l'entorn ho podem fer mitjançant un navegador web amb la url del servidor Docker.

https://url_sevidor_wazuh



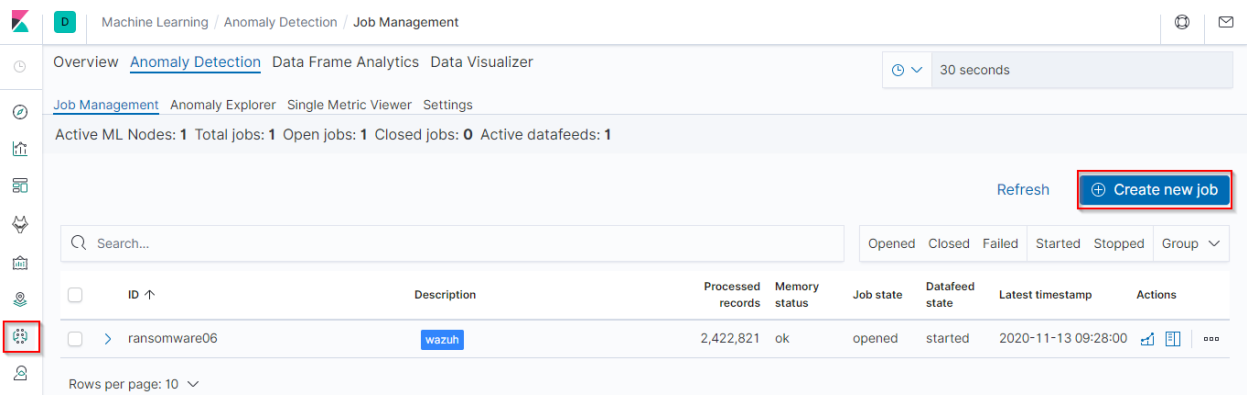
Il·lustració 28: Visió general Kibana

Al accedir a la web, el navegador ens mostra l'error de seguretat, indicant que no és una web segura degut a què el certificat està signat per una entitat certificadora no reconeguda, en aquest cas no suposa cap problema. Una vegada dins, podem observar a l'esquerra el menú amb les opcions: Discover, Wazuh, Management i Machine Learning, com a més rellevants en aquesta POC.

5.2.2 Configuració Machine Learning

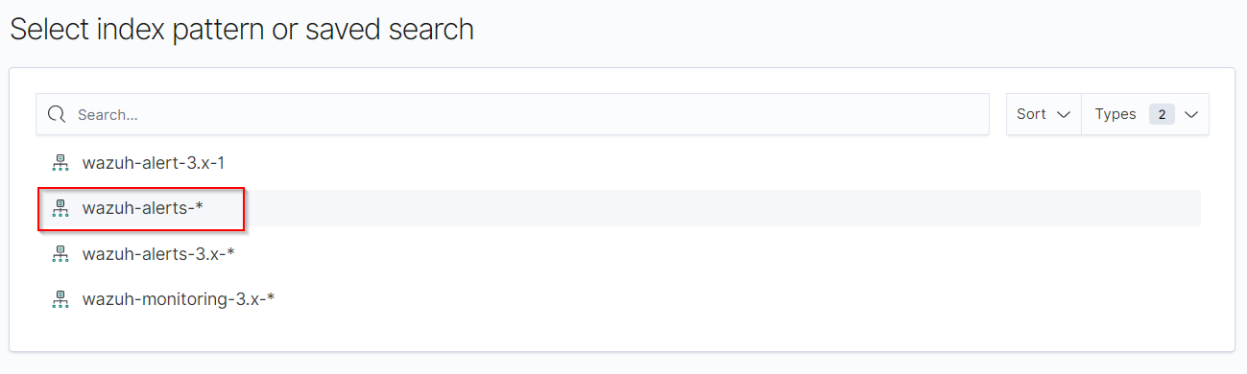
En aquest apartat s'aborda la configuració d'un treball de Machine Learning per intentar detectar l'atac simulat de Ransomware en un servidor en concret i es valora la seva efectivitat en aquesta POC. Tot seguit es mostra, primer, la configuració i després el resultat obtingut una vegada llançat l'atac explicat en l'apartat 5.4.

En primer lloc cal activar la llicència de prova de Machine Learning des del mateix menú de Kibana i a continuació es configura el treball des del mateix menú, tal i com es detalla en les següents imatges:



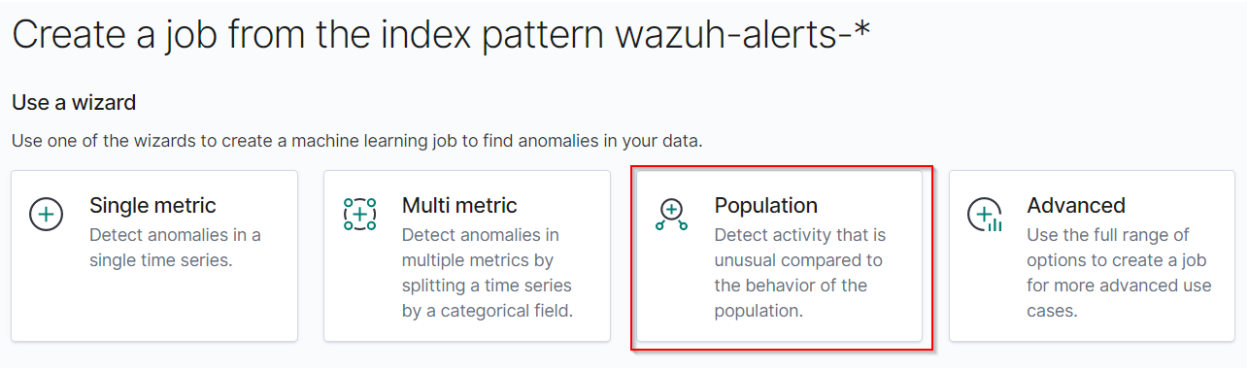
Il·lustració 29: Creació Job Machine Learning pas 1

Al clicar en l'opció "Create new job", s'obre una finestra on es selecciona l'índex a partir del qual es recolliran les dades, en aquest cas "wazuh-alerts*", ja què, volem analitzar les alertes dels agents Wazuh.



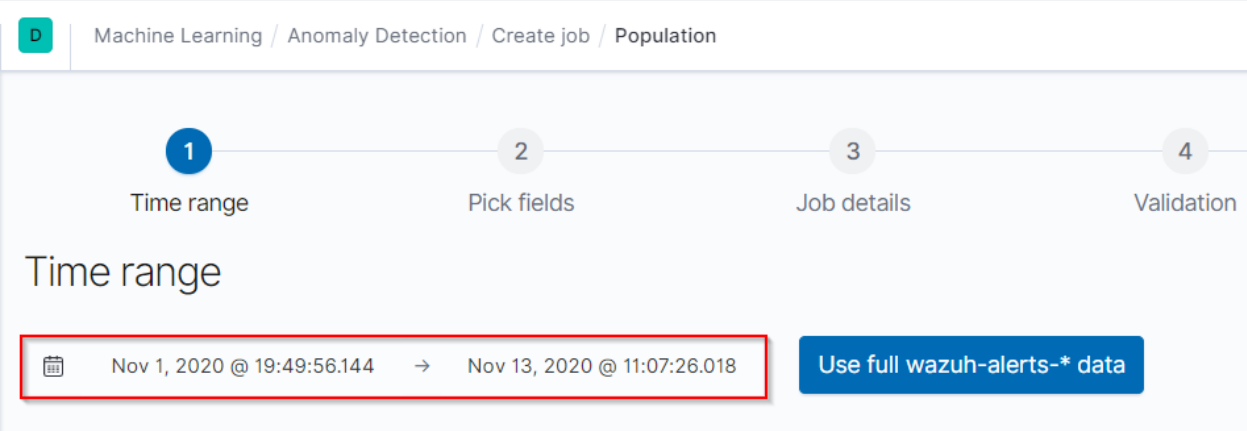
Il·lustració 30: Configuració Machine Learning, selecció de l'index

En el següent pas es tria l'assistent que ajuda en el procés de creació del treball. Aquí cliquem l'opció "Population", perquè es vol detectar comportaments irregulars d'un servidor en base al seu comportament habitual o comparant-lo amb d'altres servidors.



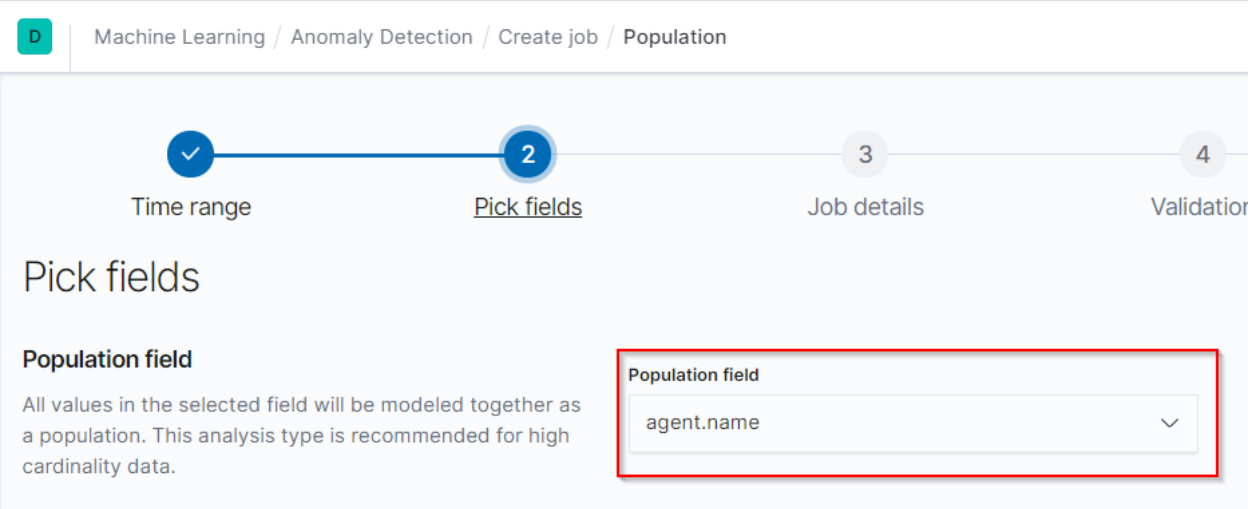
Il·lustració 31: Configuració Machine Learning, selecció wizard

A continuació es selecciona el temps d'exploració. Com que la instal·lació i recollida de dades s'ha iniciat el Novembre de 2020, es posa el rang de dades en aquest terme.



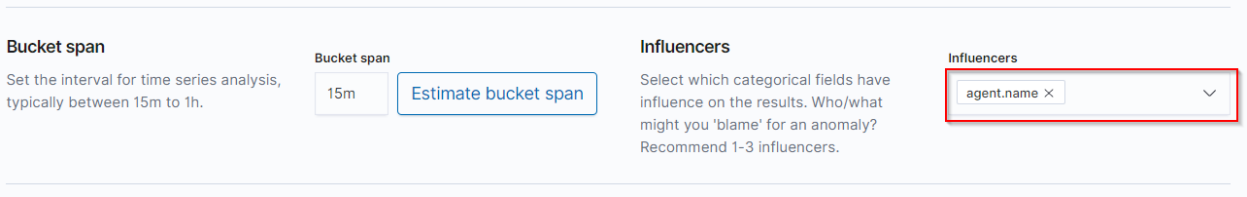
Il·lustració 32: Configuració Machine Learning, dates a explorar

En aquest punt es selecciona el paràmetre "Population", què és el nom de l'agent. Es selecciona aquesta opció perquè es creu interessant comparar el comportament d'un agent, servidor, vers la resta, ja què un atac de Ransomware es pot iniciar en un servidor i després propagar-se a la resta, per tant, la diferència de comportament d'un servidor en vers la resta pot ajudar a la detecció.



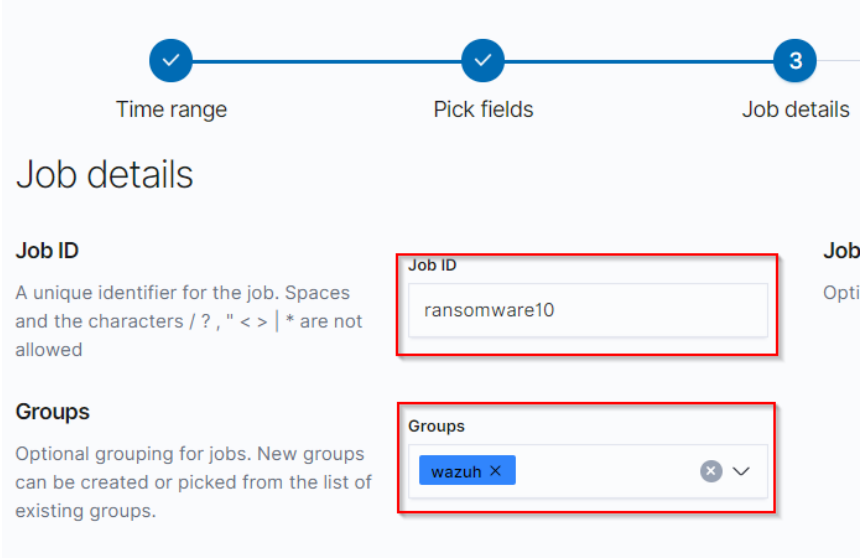
Il·lustració 33: Configuració Machine Learning, paràmetre Population

En aquesta mateixa pàgina de configuració també és important prestar atenció al paràmetre "Influencers", en aquest cas s'ha deixat el mateix que en el paràmetre Population, perquè ajuda a donar visibilitat a quin és el servidor on s'està duent a terme l'anomalia.



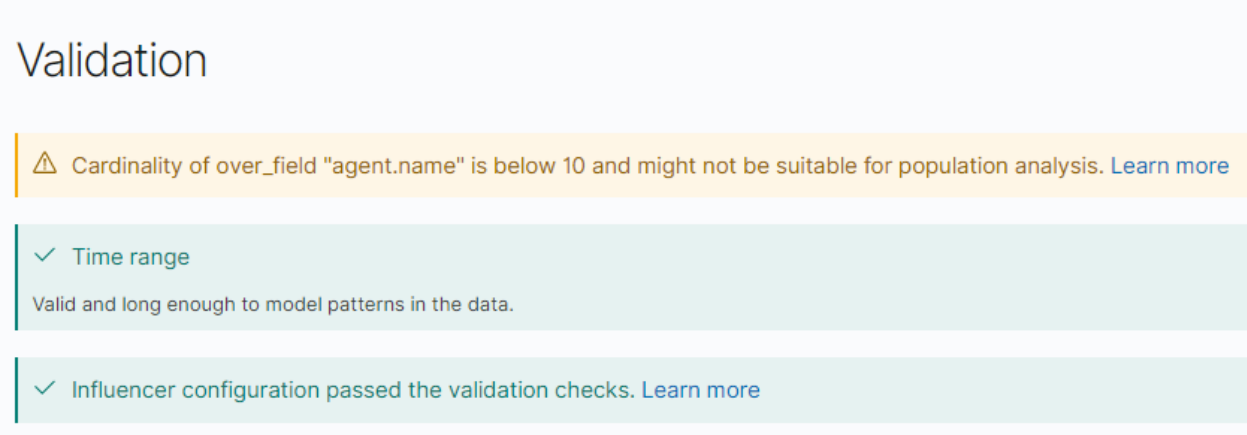
Il·lustració 34: Configuració Machine Learning, paràmetre Influencers

En el següent pas s'assigna un nom representatiu a la tasca i s'indica si es vol agrupar.



Il·lustració 35: Configuració Machine Learning, detalls

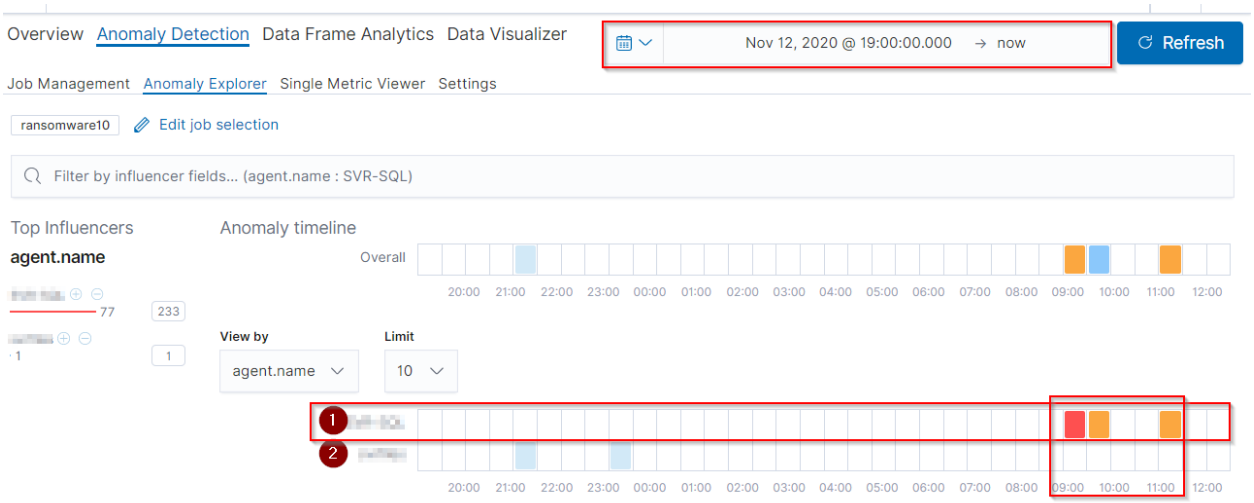
Tot seguit s'adverteix què no és recomanable utilitzar el paràmetre Population que s'ha seleccionat degut a què no hi ha prou elements diferenciadors. És correcta aquesta indicació perquè per realitzar la prova només s'ha instal·lat l'agent en 1 servidor, però com es té previst ampliar-ho a més servidors s'ha cregut convenient deixar-ho així.



Il·lustració 36: Configuració Machine Learning, missatge validació

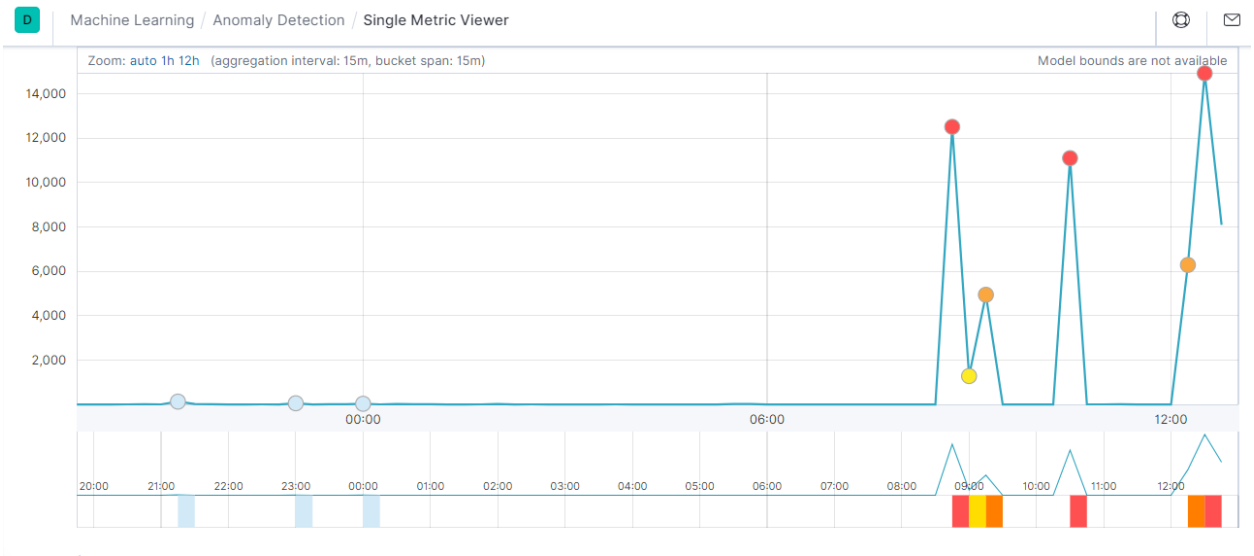
I per finalitzar, només queda clicar a "Create Job" i "Start Job running in real time".

Després de realitzar la simulació d'atac de l'apartat 5.3 en diferents hores del matí s'observa els següents resultats a l'explorador d'anomalies.
En la següent imatge es pot observar dos "Influencers", els punts vermells 1 i 2, que són els 2 servidors on s'ha instal·lat l'agent, i les anomalies detectades en un determinat interval de temps. Per tal què la visualització sigui més clara s'estableix el filtre de les dades en les darreres 24h i s'observa com en les hores en que s'ha realitzat la simulació de l'atac apareixen les marques vermella i taronja a l'hora dels atacs simulats.



Il·lustració 37: Configuració Machine Learning, visualització anomalies

En la vista "Single Metric Viewer" es pot visualitzar la gràfica més detallada, on es pot veure clarament els 3 atacs simulats.

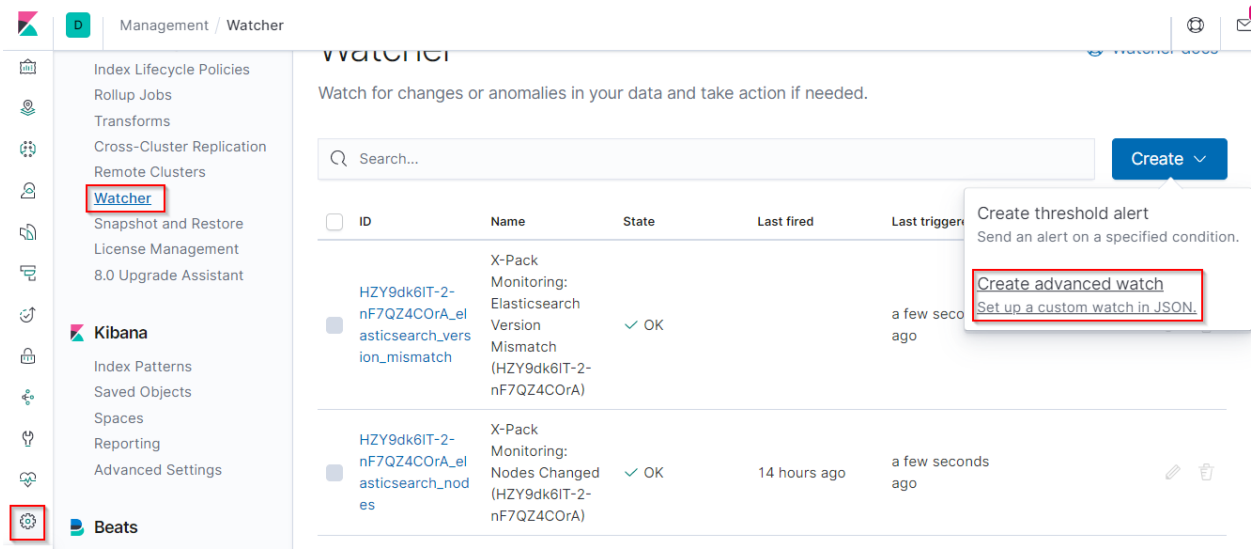


Il·lustració 38:Configuració Machine Learning, visualització anomalies amb Single Metric Viewer

5.2.3 Configuració alertes Kibana

En aquest apartat s'explica la configuració de l'entorn Kibana per a l'enviament d'una l'alerta a MS Teams.

La configuració de l'alerta s'ha realitzat des de l'opció Watcher que es pot trobar al menú de Kibana, Management - Watcher.
S'ha escollit l'opció de configuració avançada perquè en la versió instal·lada de Elasticsearch la opció "Create threshold alert" no funciona correctament amb l'enviament a Teams mitjançant webhook.



Il·lustració 39: Configuració Watcher, crear

A continuació s'assigna un nom al "Watcher" i al camp Watch JSON s'introdueix la configuració del Watcher, tal i com s'indica a continuació:

```
{
  "trigger": {
    "schedule": {
      "interval": "109s"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          ".ml-anomalies-*"
        ],
        "rest_total_hits_as_int": true,
        "body": {
```

```
"size": 0,
"query": {
  "bool": {
    "filter": [
      {
        "term": {
          "job_id": "ransomware10"
        }
      },
      {
        "range": {
          "timestamp": {
            "gte": "now-30m"
          }
        }
      },
      {
        "terms": {
          "result_type": [
            "bucket",
            "record",
            "influencer"
          ]
        }
      }
    ]
  }
},
"aggs": {
  "bucket_results": {
    "filter": {
      "range": {
        "anomaly_score": {
          "gte": 5
        }
      }
    },
    "aggs": {
      "top_bucket_hits": {
        "top_hits": {
          "sort": [
            {
              "anomaly_score": {
                "order": "desc"
              }
            }
          ],
          "_source": {
            "includes": [
              "job_id",
```

```
                "result_type",
                "timestamp",
                "anomaly_score",
                "is_interim"
              ]
            },
            "size": 1,
            "script_fields": {
              "start": {
                "script": {
                  "lang": "painless",
                  "source":
"LocalDateTime.ofEpochSecond((doc[\"timestamp\"].value.getMillis()-
((doc[\"bucket_span\"].value * 1000)\n * params.padding)) / 1000, 0,
ZoneOffset.UTC).toString()+\":00.000Z\"",
                  "params": {
                    "padding": 10
                  }
                }
              },
              "end": {
                "script": {
                  "lang": "painless",
                  "source":
"LocalDateTime.ofEpochSecond((doc[\"timestamp\"].value.getMillis()+((doc[\"bucket_span\"].v
alue * 1000)\n * params.padding)) / 1000, 0, ZoneOffset.UTC).toString()+\":00.000Z\"",
                  "params": {
                    "padding": 10
                  }
                }
              },
              "timestamp_epoch": {
                "script": {
                  "lang": "painless",
                  "source": "doc[\"timestamp\"].value.getMillis()/1000"
                }
              },
              "timestamp_iso8601": {
                "script": {
                  "lang": "painless",
                  "source": "doc[\"timestamp\"].value"
                }
              },
              "score": {
                "script": {
                  "lang": "painless",
                  "source": "Math.round(doc[\"anomaly_score\"].value)"
                }
              }
            }
```

```
        }
       }
      }
     },
     "influencer_results": {
      "filter": {
       "range": {
        "influencer_score": {
         "gte": 1
        }
       }
      },
      "aggs": {
       "top_influencer_hits": {
        "top_hits": {
         "sort": [
          {
           "influencer_score": {
            "order": "desc"
           }
          }
         ],
         "_source": {
          "includes": [
           "result_type",
           "timestamp",
           "influencer_field_name",
           "influencer_field_value",
           "influencer_score",
           "isInterim"
          ]
         },
         "size": 3,
         "script_fields": {
          "score": {
           "script": {
            "lang": "painless",
            "source": "Math.round(doc[\"influencer_score\"].value)"
           }
          }
         }
        }
       }
      }
     },
     "record_results": {
      "filter": {
       "range": {
        "record_score": {
         "gte": 3
```

```
            }
          }
        },
        "aggs": {
          "top_record_hits": {
            "top_hits": {
              "sort": [
                {
                  "record_score": {
                    "order": "desc"
                  }
                }
              ],
              "_source": {
                "includes": [
                  "result_type",
                  "timestamp",
                  "record_score",
                  "is_interim",
                  "function",
                  "field_name",
                  "by_field_value",
                  "over_field_value",
                  "partition_field_value"
                ]
              },
              "size": 3,
              "script_fields": {
                "score": {
                  "script": {
                    "lang": "painless",
                    "source": "Math.round(doc[\"record_score\"].value)"
                  }
                }
              }
            }
          }
        }
      }
    }
  }
},
"condition": {
  "compare": {
    "ctx.payload.aggregations.bucket_results.doc_count": {
      "gt": 0
    }
  }
```

```
  },
  "actions": {
    "log": {
      "logging": {
        "level": "info",
        "text": "Alert for job
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0._source.job_id}}] at
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0.fields.timestamp_iso860
1.0}}] score
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0.fields.score.0}}]"
      }
    },
    "webhook_1": {
      "webhook": {
        "scheme": "https",
        "host": "outlook.office.com",
        "port": 443,
        "method": "post",
        "path": "/webhook/**********",
        "params": {},
        "headers": {},
        "body": "{\"@type\": \"MessageCard\",\"@context\":
\"https://schema.org/extensions\",\"themeColor\": \"64a837\",\"title\": \"Ransomware
monitor\",\"summary\": \"{{ctx.watchid}} just entered alert status. Please investigate the issue
.\",\"sections\":[{\"activityTitle\": \"Job
{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.rce.j0._souob_id}}\",\"activi
tySubtitle\": \"Alert for job
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0._source.job_id}}] at
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0.fields.timestamp_iso860
1.0}}] score
[{{ctx.payload.aggregations.bucket_results.top_bucket_hits.hits.hits.0.fields.score.0}}]\",\"activi
tyImage\":
\"https://teamsnodesample.azurewebsites.net/static/img/image1.png\",\"facts\":[{\"name\":\"Infl
uencer:\",\"value\":
\"{{ctx.payload.aggregations.influencer_results.top_influencer_hits.hits.hits.0._source.influenc
er_field_value}}\"},{\"name\": \"Trigger time:\",\"value\": \"{{ctx.execution_time}}\"}]}]}"
      }
    }
  }
}
```

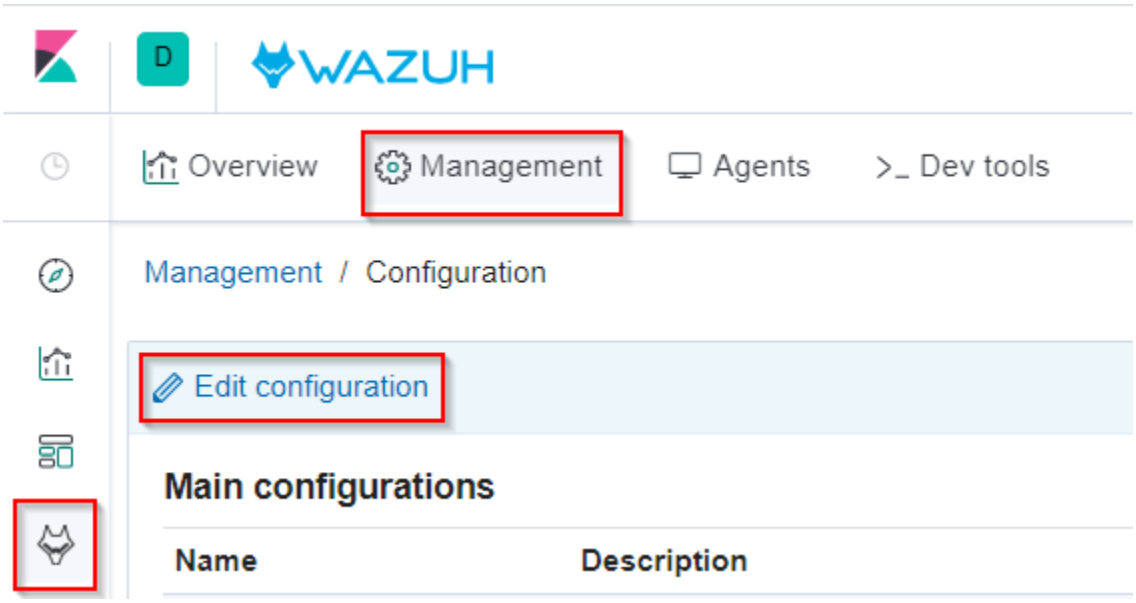
Al camp “indice” se li indica l'índex de l’anomalia generat pel treball de Machine Learning, que varia segon el nom del treball, en el camp “condition” es pot veure el llindar que activa l’alerta, i al camp “action” s'ha configurat 2 accions, la primer genera un log dins el mateix elasticsearch i la segona envia l’alerta a MS Teams.

D'aquesta manera un cop guardada la configuració del Watcher, només queda veure com reacciona l'alerta davant d'un intent d'atac.

5.2.4 Configuració alertes Wazuh

A continuació s'explica com configurar l'enviament de notificacions a MS Teams desde Wazuh per alertes d'un determinat nivell.

Aquesta configuració es realitza des del menú de Kibana - Wazuh - Management i clicant sobre l'opció "Edit cofiguration"



Il·lustració 40: Wazuh manager, configuració

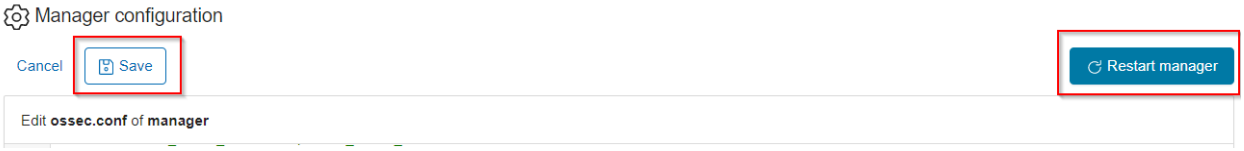
Al fitxer de configuració s'ha afegit els paràmetres d'integració de la següent manera:

```
<ossec_config>
……
        <integration>
                <name>custom-msteams</name>
                <hook_url>https://outlook.office.com/webhook/**********</hook_url>
                <level>10</level>
                <alert_format>json</alert_format>
        </integration>
……...
</ossec_config>
```

Cal prestar especial atenció en 2 punts. Primer el tag “name” de la integració, ja què si no és una integració de les preconfigurades per Wazuh, cal afegir el prefix “custom-”. I segon, el tag “level”, què és el valor que dispara l’alerta, inicialment per fer les proves s’ha fixat un valor baix de 3, i en el moment que s’ha vist què les alertes arribaven al canal de Teams s’ha establert el valor a 10, que és el què es recomana inicialment des de la documentació de Wazuh.

El següent pas és afegir a l’ubicació, /var/ossec/integrations/, els scripts, custom-msteams i custom-msteams.py, agafant com a referència els scripts per defecte que existeixen per a Slack.

Una vegada fetes les modificacions cal guardar la configuració i reiniciar el “manager”.



Il·lustració 41: Wazuh manager, guardar configuració

custom-msteams

```
#!/bin/sh
# Copyright (C) 2015-2019, Wazuh Inc.
# Created by Wazuh, Inc. <info@wazuh.com>.
# This program is free software; you can redistribute it and/or modify it under
the terms of GPLv2

WPYTHON_BIN="framework/python/bin/python3"

SCRIPT_PATH_NAME="$0"

DIR_NAME="$(cd $(dirname ${SCRIPT_PATH_NAME}); pwd -P)"
SCRIPT_NAME="$(basename ${SCRIPT_PATH_NAME})"

case ${DIR_NAME} in
    */active-response/bin | */wodles*)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/../..; pwd)"
        fi

        PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
    */bin)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
        fi

        PYTHON_SCRIPT="${WAZUH_PATH}/framework/scripts/${SCRIPT_NAME}.py"
    ;;
     */integrations)
```

```
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
        fi

        PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
esac


${WAZUH_PATH}/${WPYTHON_BIN} ${PYTHON_SCRIPT} $@
```

custom-msteams.py

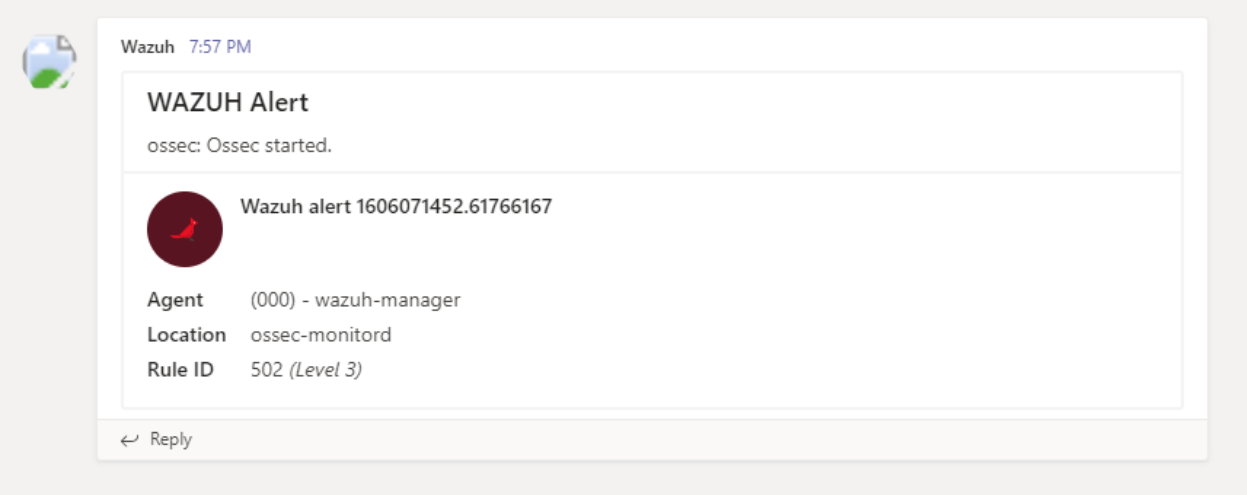
```
#!/usr/bin/env python
# Copyright (C) 2015-2019, Wazuh Inc.
# March 13, 2018.
#
# This program is free software; you can redistribute it
# and/or modify it under the terms of the GNU General Public
# License (version 2) as published by the FSF - Free Software
# Foundation.

import json
import sys
import time
import os

try:
    import requests
    from requests.auth import HTTPBasicAuth
except Exception as e:
    print("No module 'requests' found. Install: pip install requests")
    sys.exit(1)

# ossec.conf configuration:
#  <integration>
#      <name>msteams</name>
#      <hook_url>XXXXXX</hook_url>
#      <alert_format>json</alert_format>
#  </integration>

# Global vars

debug_enabled = False
pwd = os.path.dirname(os.path.dirname(os.path.realpath(__file__)))
json_alert = {}
now = time.strftime("%a %b %d %H:%M:%S %Z %Y")

# Set paths
log_file = '{0}/logs/integrations.log'.format(pwd)
```

```
def main(args):
    debug("# Starting")

    # Read args
    alert_file_location = args[1]
    webhook = args[2]

    debug("# Webhook")
    debug(webhook)

    debug("# File location")
    debug(alert_file_location)

    # Load alert. Parse JSON object.
    with open(alert_file_location) as alert_file:
        json_alert = json.load(alert_file)
    debug("# Processing alert")
    debug(json_alert)

    debug("# Generating message")
    msg = generate_msg(json_alert)
    debug(msg)

    debug("# Sending message")
    send_msg(msg,webhook)


def debug(msg):
    if debug_enabled:
        msg = "{0}: {1}\n".format(now, msg)
        print(msg)
        f = open(log_file,"a")
        f.write(msg)
        f.close()

def generate_msg(alert):

    level = alert['rule']['level']

    if ( level <= 4 ):
        color = "good";
    elif ( level >= 5 and level <= 7 ):
        color= "warning";
    else:
        color= "danger";

    msg = {}
    msg['@type'] = "MessageCard"
    msg['@context'] = "https://schema.org/extensions"
```

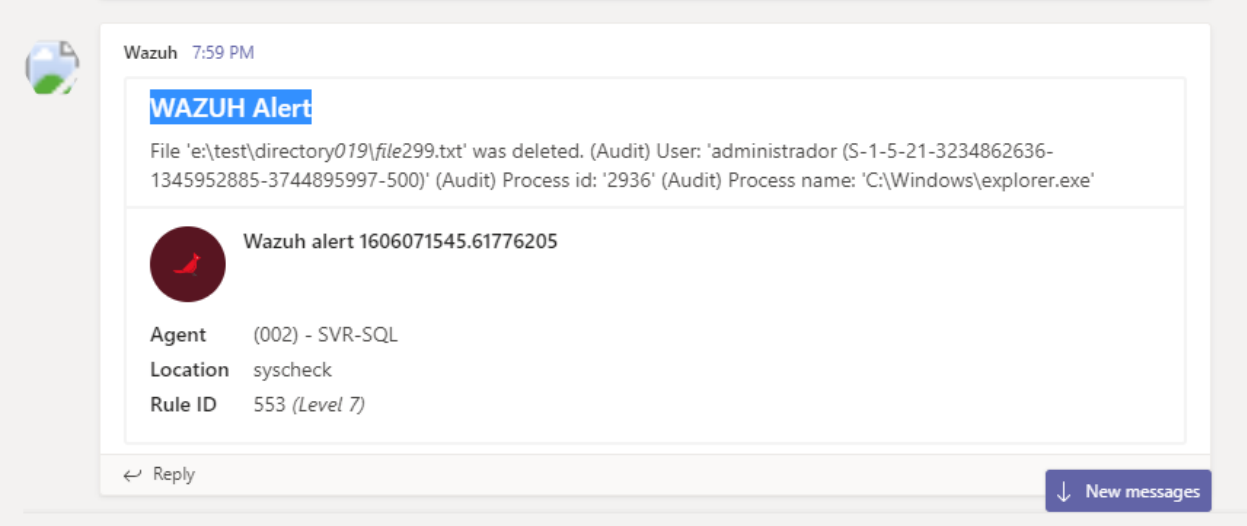
```
    msg['themeColor'] = color
    msg['title'] = "WAZUH Alert"
    msg['summary'] = alert['rule']['description']
    msg['text'] = alert.get('full_log')
    agent = { "name":"Agent", "value":"({0}) - {1}".format(alert['agent']['id'],alert['agent']['name']) }
    location = { "name":"Location", "value":alert['location'] }
    rule = { "name":"Rule ID", "value":"{0} _(Level {1})_".format(alert['rule']['id'],level) }
    section = {"activityTitle":"Wazuh alert {0}".format(alert['id']),
"activitySubtitle":"","activityImage":"https://teamsnodesample.azurewebsites.net/static/img/ima
ge1.png", "facts":[agent,location,rule]}
    msg['sections'] = [section]

    return json.dumps(msg)


def send_msg(msg,url):

    headers = {'content-type': 'application/json', 'Accept-Charset': 'UTF-8'}
    res = requests.post(url, data=msg, headers=headers)
    debug(res)

if __name__ == "__main__":
    try:
        # Read arguments
        bad_arguments = False
        if len(sys.argv) >= 4:
            msg = '{0} {1} {2} {3} {4}'.format(now, sys.argv[1], sys.argv[2], sys.argv[3], sys.argv[4] if
len(sys.argv) > 4 else '')
            debug_enabled = (len(sys.argv) > 4 and sys.argv[4] == 'debug')
        else:
            msg = '{0} Wrong arguments'.format(now)
            bad_arguments = True

        # Logging the call
        f = open(log_file, 'a')
        f.write(msg +'\n')
        f.close()

        if bad_arguments:
            debug("# Exiting: Bad arguments.")
            sys.exit(1)

        # Main function
        main(sys.argv)

    except Exception as e:
        debug(str(e))
        raise
```

Al script custom-msteams.py, que és el què definitivament executa el procés de notificació, es pot observar una primera part on s'omplen les dades a enviar dins la variable "msg" i la funció send_msg, què s'encarrega de fer l'enviament de la notificació en format json a MSTeams.

A continuació es poden veure 2 imatges amb les alertes que han arribat al canal de Teams, la primera de nivell 3 i la segona de nivell 7.



Il·lustració 42: MS Teams, notificació 1



Il·lustració 43: MS Teams, notificació 2

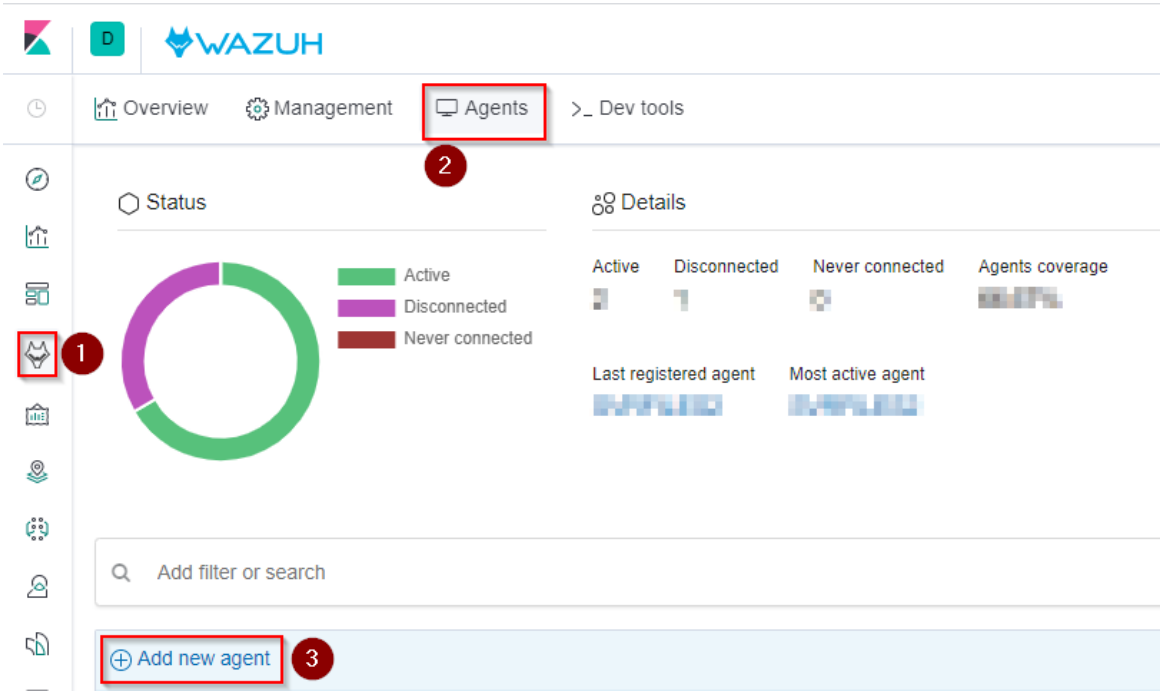
5.3 Instal·lació i configuració de l'agent HIDS

En aquest apartat s'explica el procediment seguit per a realitzar la instal·lació de l'agent HIDS al servidor de proves, les modificacions al fitxer de configuració de l'agent i, finalment, com comprovar des de Kibana que la configuració s'ha realitzat correctament.

Per instal·lar l'agent HIDS de Wazuh en un servidor Windows s'han seguit els següents passos:

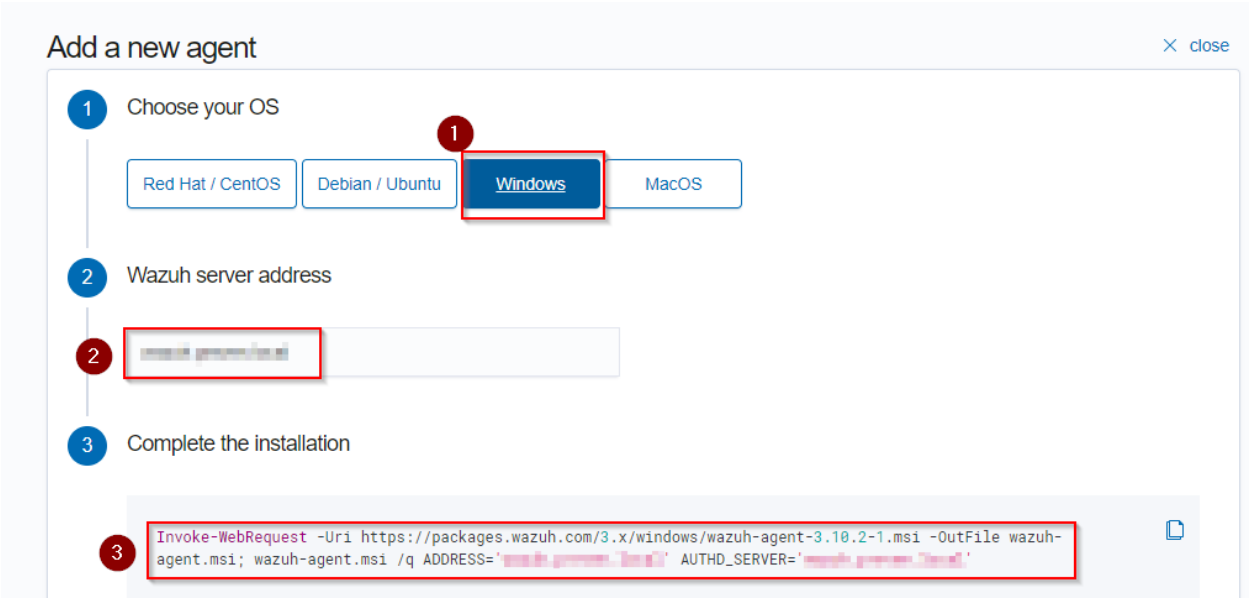
1. Accedir a la url del servidor SIEM amb les credencials que prèviament s'han introduït en la instal·lació i recollir l'ordre PowerShell que ens instal·larà i configurarà l'agent, tal i com es mostra en les següents imatges:

   En aquesta primera imatge es pot veure la pantalla de gestió dels agents Wazuh de Kibana, i els números de la imatge ens indiquen els passos a seguir per accedir a la pàgina d'instal·lació de l'agent.



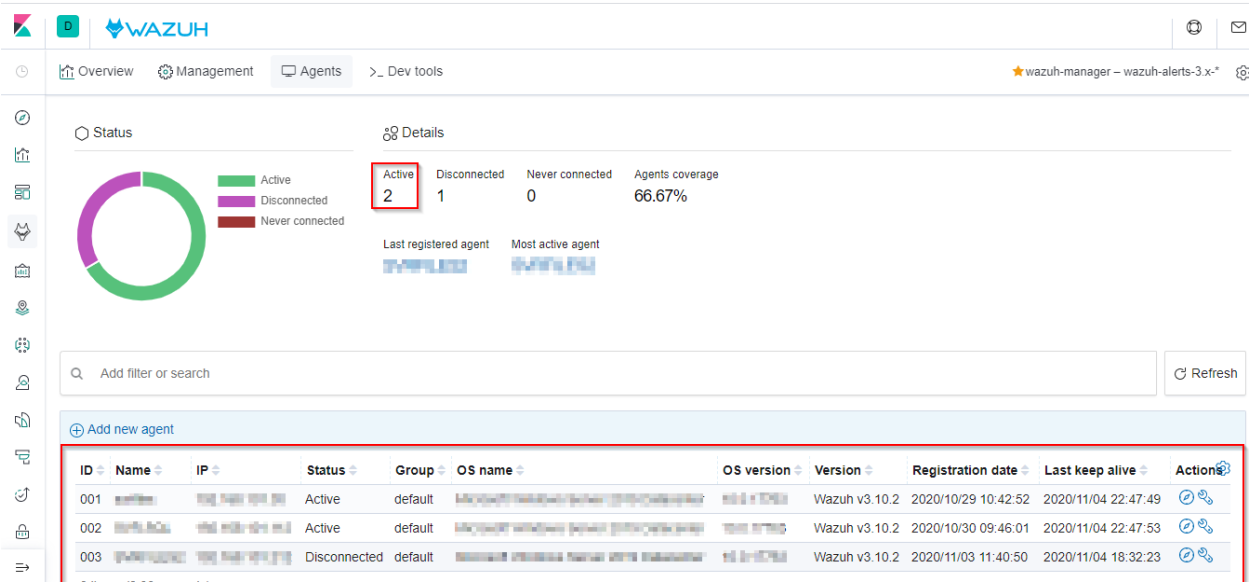
Il·lustració 44: Pantalla de gestió dels agents

En aquesta segona imatge es pot veure com després de seguir els passos indicats s'obté en el pas 3 l'ordre PowerShell per realitzar la instal·lació de l'agent en qualsevol equip que estigui dins la mateixa xarxa.



Il·lustració 45: Pantalla d'instal·lació dels agents

Una vegada executada l'ordre PowerShell es pot observar la connexió de l'agent HIDS amb el servidor Wazuh en aquesta pantalla de Kibana.



Il·lustració 46: Pantalla de gestió dels agents

Per tal d'obtenir els logs de la modificació de fitxers, cal modificar el fitxer de configuració de l'agent Wazuh i configurar els permisos de les carpetes de Windows adequadament, tal i com s'indica a continuació:

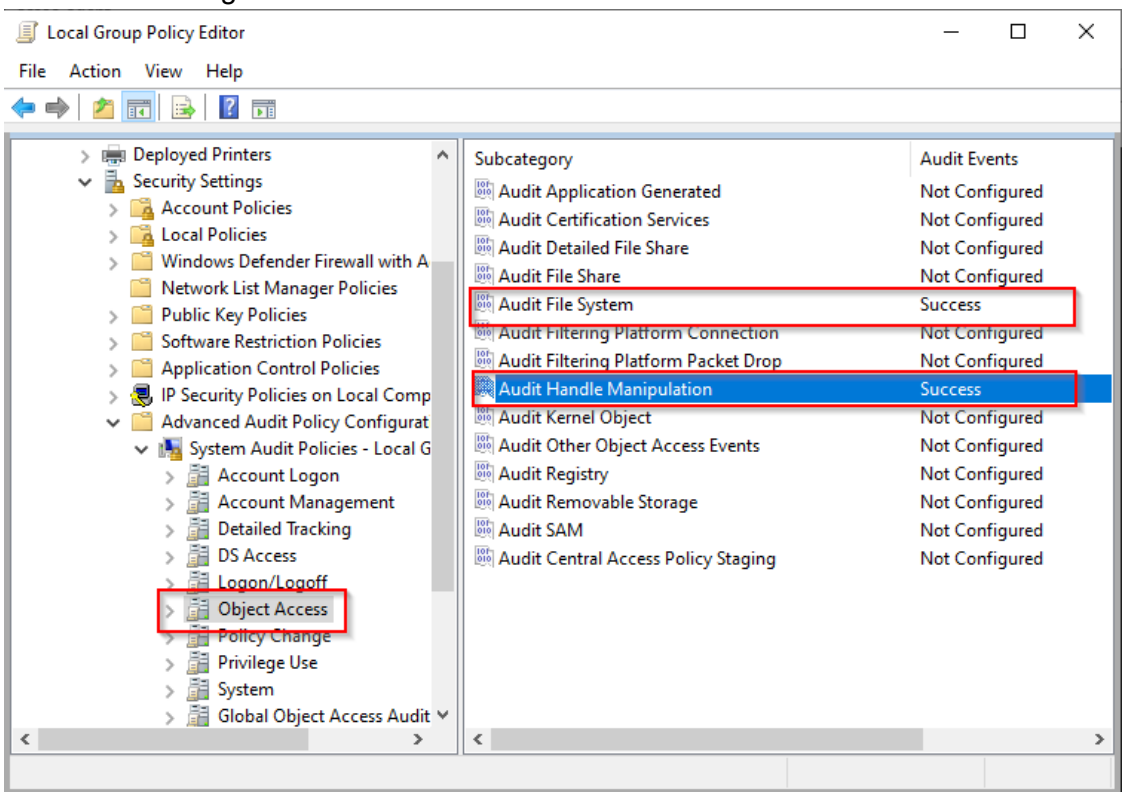
Arribats en aquest punt el servidor Windows on és vol realitzar les proves ja té l'agent instal·lat amb la configuració per defecte, el següent pas és configurar el mòdul "File Integrity monitoring" perquè monitoritzi els directoris i/o fitxers escollits.

1. En primer lloc es modifica el fitxer de configuració ossec.conf afegint les següents línies entre les etiquetes <syscheck> </syscheck>

```
<directories check_all="yes" whodata="yes">E:\Test</directories>
```

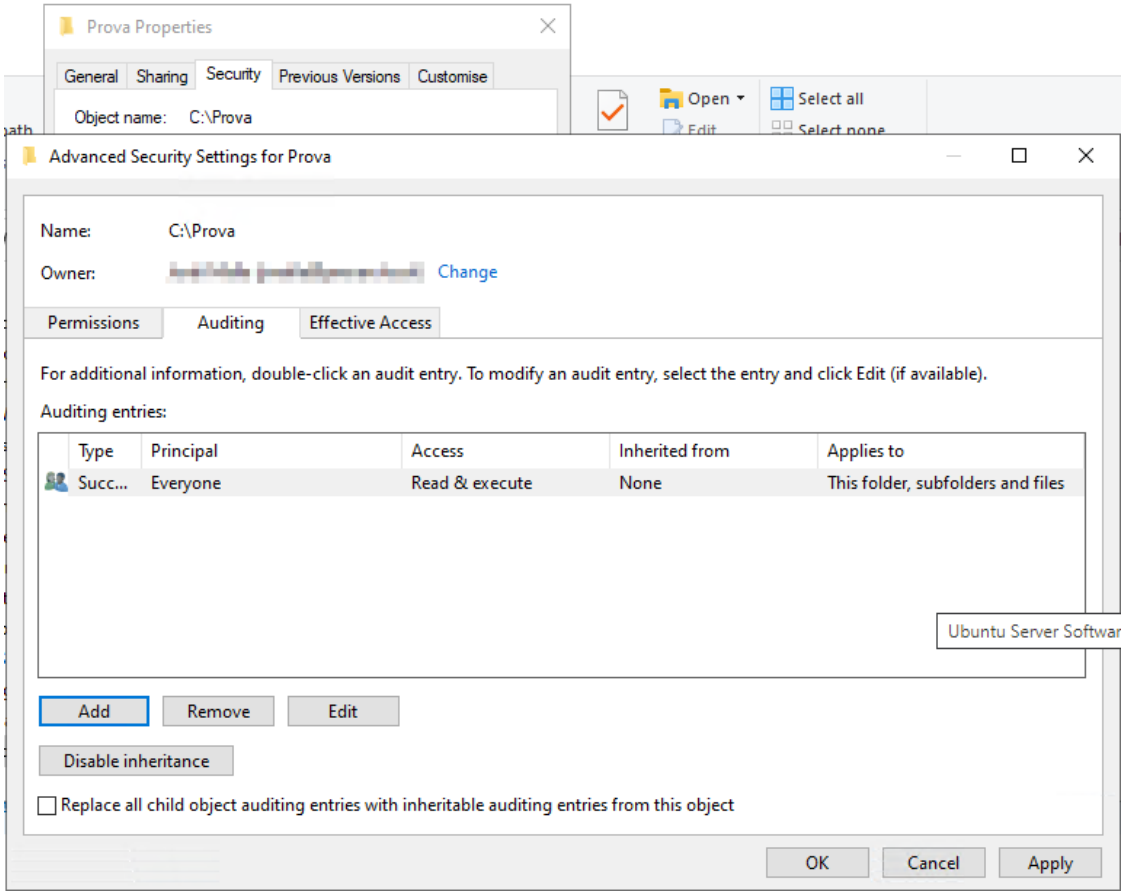
   Amb aquesta línia indiquem que volem monitoritzar els canvis que es produeixen dins la carpeta E:\Test i amb l'etiqueta "whodata" obtenim quin usuari està fent els canvis i amb quina aplicació ho està fent.

2. En segon lloc, i per a que l'etiqueta "whodata" tingui efecte, cal configurar el servidor Windows per tal què auditi les modificacions als fitxers i/o directoris desitjats seguint els següents passos:
   a. Primer s'executa el "Local Group Policy Editor" amb l'ordre "gpedit.msc" i es modifica les claus, "Audit File System" i "Audit Handle Manipulation", tal i com s'indica a la imatge.



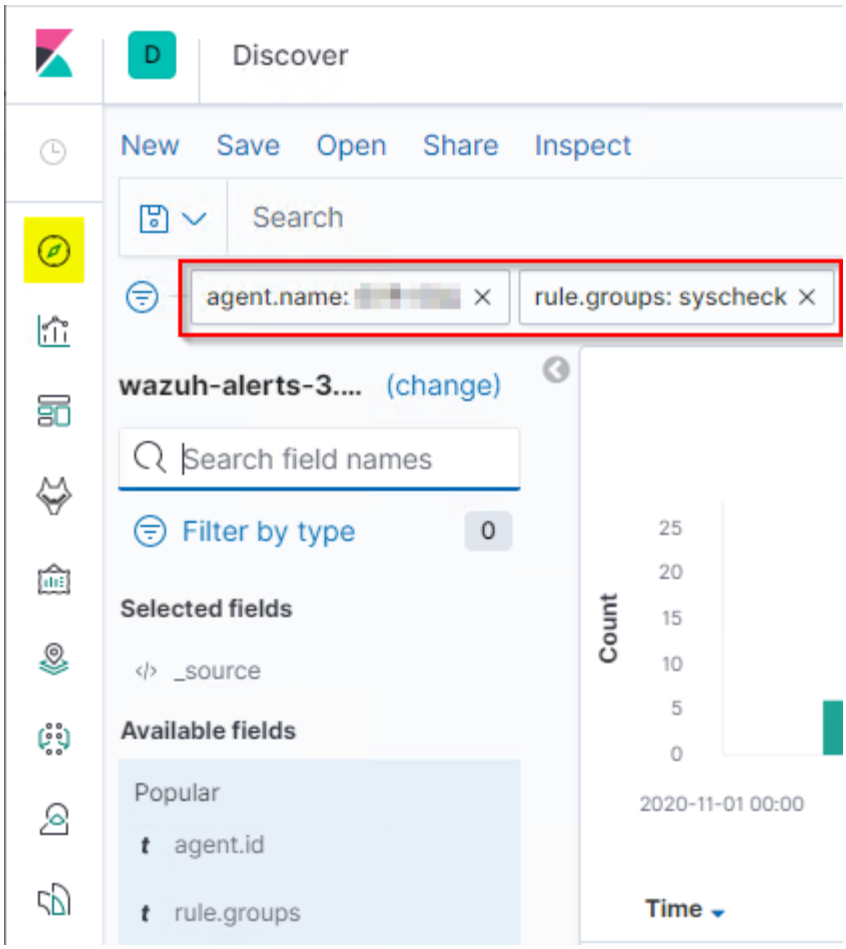
Il·lustració 47: Configuració polítiques de grups locals

   b. I en segon lloc cal configurar l'auditoria a la carpeta escollida. Per fer-ho cal situar-se a les propietats de la carpeta, pestanya seguretat, opcions avançades i a la pestanya auditoria afegir la auditoria, tal i com s'indica a la imatge.



Il·lustració 48: Configuració auditoria carpeta

Per donar com a finalitzada la instal·lació de l'agent HIDS s'ha comprovat la recepció de dades al servidor Wazuh. Per fer-ho, primer s'han creat i eliminat fitxers dins la carpeta monitoritzada i, tot seguit, s'ha visualitzat el resultat al menú Discover de Kibana. En aquest punt, i després d'aplicar els filtres pertinents, tals com "rule.grups=syscheck" i "agent.name=server", s'han visualitzat els esdeveniments de les modificacions amb l'usuari i l'aplicació que les ha fet, tal i com es mostra en les imatges següents.



Il·lustració 49: Filtres per visualitzar els events desitjats

Nov 4, 2020 @ 18:15:51.560 agent.name: rule.groups: ossec, syscheck input.type: log syscheck.path: e:\test\addd\sdf.txt syscheck.audit.process.name: C:\Windows\explorer.exe syscheck.audit.process.id: 13792 syscheck.audit.user.name: administrador syscheck.audit.user.id: S-1-5-21-3234862636-1345952885-3744895997-500 syscheck.event: deleted agent.ip: agent.id: 002 manager.name: wazuh-manager rule.firedtimes: 3 rule.mail: false rule.pci_dss: 11.5 rule.level: 7 rule.hipaa: 164.312.c.1, 164.312.c.2 rule.description: File

Nov 4, 2020 @ 18:15:45.773 agent.name: rule.groups: ossec, syscheck syscheck.path: e:\test\ddd\nuevo documento de texto.txt syscheck.audit.process.name: C:\Windows\explorer.exe syscheck.audit.process.id: 13792 syscheck.audit.user.name: administrador syscheck.audit.user.id: S-1-5-21-3234862636-1345952885-3744895997-500 syscheck.event: deleted input.type: log agent.ip: agent.id: 002 manager.name: wazuh-manager rule.firedtimes: 2 rule.mail: false rule.pci_dss: 11.5 rule.hipaa: 164.312.c.1, 164.312.c.2 rule.level: 7

Nov 4, 2020 @ 18:15:45.757 agent.name: rule.groups: ossec, syscheck syscheck.path: e:\test\ddd\dddd.txt syscheck.sha1_after: da39a3ee5e6b4b0d3255bfef95601890afd80709 syscheck.mtime_after: Nov 4, 2020 @ 18:15:42.000 syscheck.uname_after: Administradores syscheck.attrs_after: ARCHIVE syscheck.size_after: 0 syscheck.uid_after: S-1-5-32-544 syscheck.win_perm_after: { "allowed": ["DELETE", "READ_CONTROL", "WRITE_DAC", "WRITE_OWNER", "SYNCHRONIZE", "FILE_READ_DATA", "FILE_WRITE_DATA", "FILE_APPEND_DATA", "FILE_READ_EA",

Il·lustració 50: Alguns events obtinguts

I, a continuació es presenta el detall d'un esdeveniment en concret, en format JSON, on es pot observar com es presenten les dades de l'auditoria en el camp "audit".


```
{
  "_index": "wazuh-alerts-3.x-2020.11.04",
  "_type": "_doc",
  "_id": "LvpClHUBY__dQILDAvmf",
  "_version": 1,
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "syscheck": {
      "path": "e:\\test\\addd\\sdf.txt",
      "audit": {
        "process": {
          "name": "C:\\Windows\\explorer.exe",
          "id": "13792"
        },
        "user": {
          "name": "administrador",
          "id": "S-1-5-21-3234862636-1345952885-3744895997-500"
        }
      },
      "event": "deleted"
    },
    "agent": {
      "ip": "**********",
      "name": "*****",
      "id": "002"
    },
    "manager": {
      "name": "wazuh-manager"
    },
    "rule": {
      "firedtimes": 3,
      "mail": false,
      "pci_dss": [
        "11.5"
      ],
      "level": 7,
      "hipaa": [
        "164.312.c.1",
        "164.312.c.2"
      ],
      "description": "File deleted.",
      "groups": [
        "ossec",
        "syscheck"
      ],
```

```
      "id": "553",
      "nist_800_53": [
        "SI.7"
      ],
      "gpg13": [
        "4.11"
      ],
      "gdpr": [
        "II_5.1.f"
      ]
    },
    "location": "syscheck",
    "id": "1604510151.8139688",
    "decoder": {
      "name": "syscheck_integrity_changed"
    },
    "timestamp": "2020-11-04T17:15:51.560+0000",
    "full_log": "File 'e:\\test\\addd\\sdf.txt' was deleted.\n(Audit) User: 'administrador (S-1-5-21-3234862636-
1345952885-3744895997-500)'\n(Audit) Process id: '13792'\n(Audit) Process name: 'C:\\Windows\\explorer.exe'\n"
  },
  "fields": {
    "timestamp": [
      "2020-11-04T17:15:51.560Z"
    ]
  },
  "highlight": {
    "agent.name": [
      "@kibana-highlighted-field@***@/kibana-highlighted-field@"
    ],
    "rule.groups": [
      "@kibana-highlighted-field@syscheck@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1604510151560
  ]
}
```

5.4 Simular un atac de Ransomware

En aquest punt s'exposen els passos que s'han seguit per comprovar el funcionament de la solució SIEM configurada mitjançant la simulació d'un atac de Ransomware.

Per tal de simular un atac d'aquestes característiques, s'ha elaborat un petit script en Batch què simula en primera instància, amb l'opció "init", la creació de "x" directoris i de "y" fitxers en cada directori, i en segon lloc, amb l'opció "atack", simula l'encriptació dels fitxers.

Test_Rasnsomware.bat

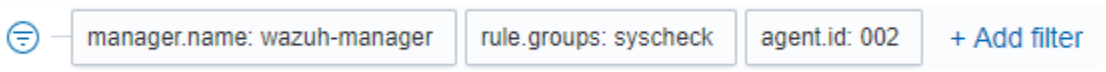
```
@echo off
:: add other test for the arguments here...
if not [%1]==[] goto main
goto showMainHelp

:exit
exit /B 1

:showMainHelp
echo Use this correct form.
echo.
echo %0 param%%1 param%%2
echo      param%%1 [init, atack]
echo      param%%2 -h Help about the command
goto exit

:main
if [%1] == [init] (
    goto checkInit
) else if [%1] == [atack] (
    goto atack
) else (
    echo Incorrect arguments.
    echo.
    goto showMainHelp
)
echo do something with all arguments (%%* == %*) here...
goto exit

:showInitHelp
echo Help for Init.
echo.
echo %0 init param%%2
echo    param%%2 a number of directories to create
echo    param%%3 a number of files into each directories
goto exit
```

```
:checkInit
if [%2] == [-h] (
    goto showInitHelp
) else if %2 EQU +%2 (
    if %3 EQU +%3 (
        goto initCreate
    )
) else (
    goto initErrorComands
)
goto exit

:initErrorComands
    echo Incorrect arguments.
    echo.
    goto showInitHelp
goto exit

:initCreate
setlocal
set /A num_dir=%2
set /A num_files=%3
for /L %%i IN (0,1,%num_dir%) DO (
    mkdir Directory_0%%i
    cd Directory_0%%i
    for /L %%e IN (0,1,%num_files%) DO (
        echo Text of test file. > File_%%e.txt
    )
    cd ..
)
endlocal
goto exit

:atack
echo START
date /T
time /T
for /R . %%G IN (*.txt) DO (
          del %%G
          echo T$e$x$t$ $o$f$ $t$e$s$t$ $f$i$l$e$.$ FILE ENCRYPTED SOS >
%%~pG\%%~nG.encryp
)
echo END
date /T
time /T
goto exit
```

Per executar l'atac, primer s'ha creat l'estructura de directoris amb la següent ordre:

```
E:\test\Test_Ransomware.bat Init 20 1000
```

En aquest moment des del menú Discover de Kibana i aplicant els següents filtres, es pot veure els logs recollits.



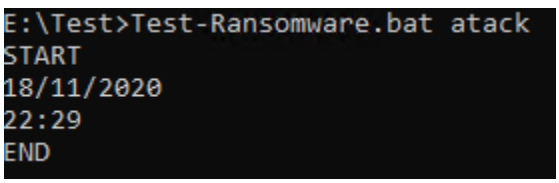
Il·lustració 51: Filtres aplicats al menú Discover de Kibana

Time	syscheck.path	syscheck.event	agent.name
Nov 11, 2020 @ 21:00:26.635	e:\test\directory_04\file_99.txt	added	
Nov 11, 2020 @ 21:00:26.619	e:\test\directory_04\file_98.txt	added	
Nov 11, 2020 @ 21:00:26.588	e:\test\directory_04\file_97.txt	added	
Nov 11, 2020 @ 21:00:26.572	e:\test\directory_04\file_96.txt	added	
Nov 11, 2020 @ 21:00:26.556	e:\test\directory_04\file_95.txt	added	
Nov 11, 2020 @ 21:00:26.541	e:\test\directory_04\file_94.txt	added	
Nov 11, 2020 @ 21:00:26.510	e:\test\directory_04\file_93.txt	added	
Nov 11, 2020 @ 21:00:26.494	e:\test\directory_04\file_92.txt	added	
Nov 11, 2020 @ 21:00:26.478	e:\test\directory_04\file_91.txt	added	
Nov 11, 2020 @ 21:00:25.446	e:\test\directory_04\file_90.txt	added	
Nov 11, 2020 @ 21:00:25.415	e:\test\directory_04\file_89.txt	added	
Nov 11, 2020 @ 21:00:20.788	e:\test\directory_04\file_298.txt	added	
Nov 11, 2020 @ 21:00:20.772	e:\test\directory_04\file_297.txt	added	

Il·lustració 52: Resultats obtinguts després de la creació de l'estructura de fitxers

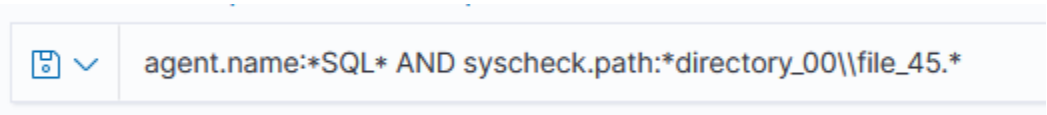
A continuació s'executa l'atac amb l'ordre següent:

```
E:\Test\Test_Ransomware.bat atack
```



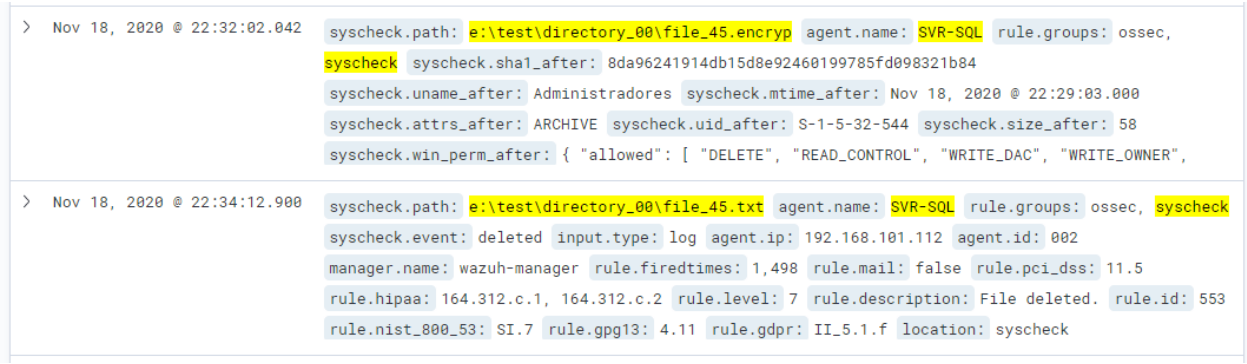
Il·lustració 53: Consola, execució atac simulat

Ara en el menú Discover es pot observar els registres de l'eliminació del fitxer .txt i d'afegir el fitxer .encryp, conseqüències de l'atac. Per visualitzar millor l'exemple a Kibana s'ha aplicat el filtre del nom de l'agent i el path del fitxer, tal i com s'indica a continuació.



Il·lustració 54: Discover, filtre visualitzar l'atac

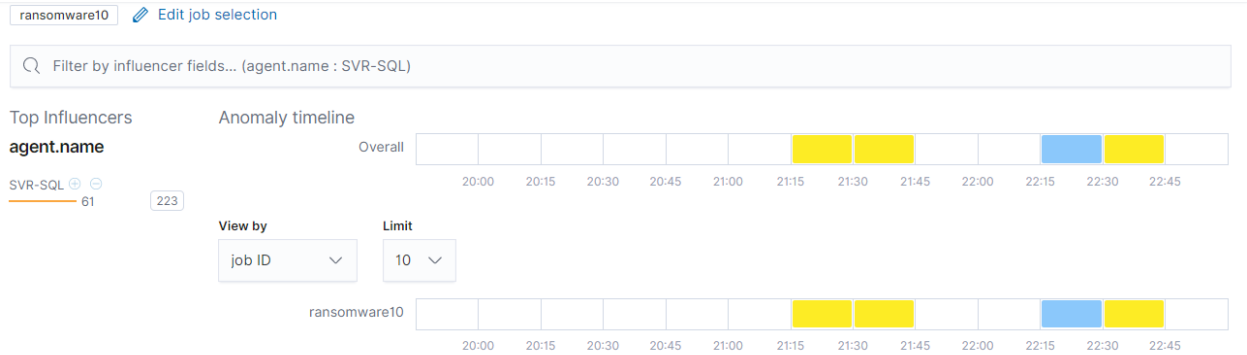
Una vegada aplicat el filtre, es poden visualitzar els registres següents:



Il·lustració 55: Discover, Registres de l'atac

En aquest cas s'ha afegit el filtre de la ruta d'un fitxer en concret per tenir una visió més localitzada i poder observar com mostra els resultat Discover en el cas de l'atac de Ransomware.

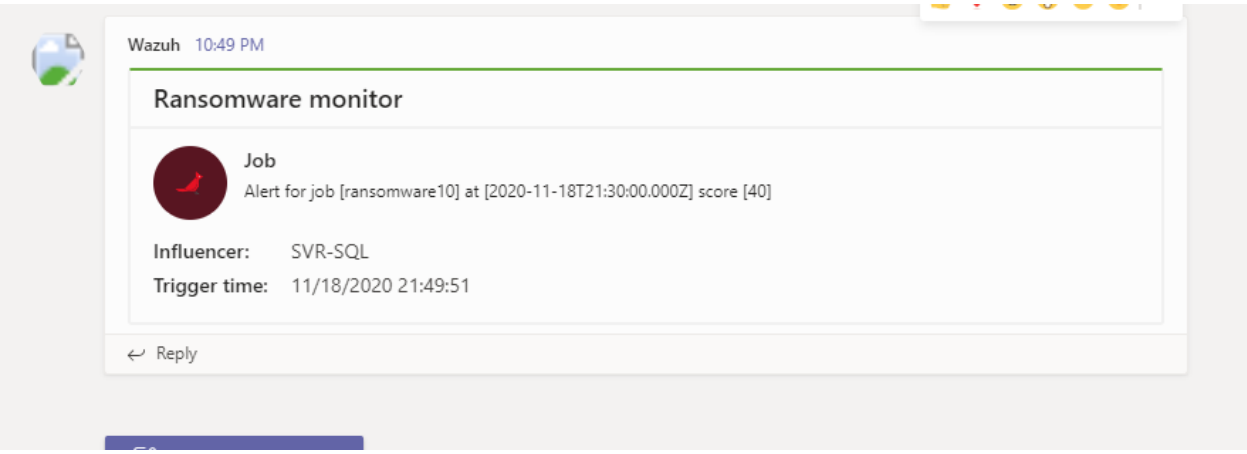
Per altra, banda també es pot observar com minuts després de produir-se l'atac, en l'apartat de Machine Learning, es visualitzen els indicadors.



Il·lustració 56: Machine Learning, anomaly timeline

I per últim, es pot observar en la següent imatge, com al canal de Teams arriba l'alerta de l'atac.

Il·lustració 57: MS Teams, alert 1



Il·lustració 58: MS Teams, alerta 2

En aquestes imatges es pot comprovar com augmenta la puntuació o score, que dona el treball de Machine Learning a l'incident, a mesura que avança l'atac.

Es pot apreciar també, com l'hora del trigger és inferior a l'hora de la recepció de l'alerta a Teams, això és degut a què el contenidor Docker de Elasticsearch està configurat amb la data i hora UTC.

Una altra de les apreciacions que s'han fet en aquest punt és que només arriba l'alerta generada pel treball de Machine Learning, configurada en l'apartat 5.2.3. En canvi, l'alerta configurada al Wazuh manager, en l'apartat 5.3.4, només genera alertes de nivell 7, supressió de fitxer i, al no ser superior a 10, no s'envia cap notificació.

6 Conclusions finals

La visualització que aporta Wazuh juntament amb Elastic Stack és una opció molt vàlida per la seva fàcil implementació, desplegament centralitzat, integració amb multitud d'eines i la seva interfície intuïtiva.

En el cas de la POC en qüestió no s'ha pogut analitzar tot el seu potencial degut a que s'ha centrat en el descobriment de la plataforma, la observació de la funcionalitat Machine Learning i la integració amb Teams, deixant de banda opcions molt interessants com la integració amb Virustotal, l'anàlisi de vulnerabilitats, GDPR, active responsive, etc.

Pel que fa a la valoració de l'opció Machine Learning i, degut a què s'ha executat en un servidor de proves on no hi ha activitat, no es pot afirmar que la detecció que s'observa de l'atac en el punt 5.4 sigui concloent. El següent pas seria provar-ho en un servidor en producció i veure com detecta Wazuh l'atac i amb quina severitat el notifica.

Pel que fa a les notificacions, s'ha observat que les què estan configurades directament a Wazuh manager, punt 5.3.4, no s'han disparat durant l'atac simulat, en canvi, les notificacions del job de Machine Learning, punt 5.3.3, si què han arribat a Teams. Les alertes de Wazuh manager no s'han disparat perquè el llindar esta establert en 10 i les alertes d'eliminació i creació de fitxers estan indicades amb el valor 7. Per visualitzar l'atac amb les notificacions configurades en el punt 5.3.4, es pot optar per baixar el nivell d'alerta que dispara la notificació fins a 7, com podem veure en la notificació de la imatge 43, tot i que no és gens recomanable degut al gran nombre de notificacions que es rebran de fitxers modificats, siguin, o no, un atac.

6.1 Valoració econòmica del projecte

En aquest apartat es fa una valoració econòmica de la gestió i la implantació del projecte, sense tenir en compte el cost de la infraestructura, ja què, es pressuposa que el projecte s'aplica a una infraestructura ja existent.
Per a la seva valoració econòmica es te en compte els següents criteris:

1. Es divideix el treball en dos rols, el gestor del projecte i l'enginyer de seguretat. Les tasques del gestor del projecte son les de valorar les necessitats del sistema, dissenyar l'entorn, elaborar la planificació i vetllar pel bon compliment del projecte. En canvi, l'enginyer de seguretat s'encarrega de la implantació i manteniment del sistema dissenyat, seguint la planificació establerta.

2. El càlcul de les hores de dedicació s'ha realitzat en base al nombre de crèdits del TFM, que són 12, i les hores de dedicació per crèdit segons la documentació de la UOC, que són 25h/crèdit. El resultat de les hores totals del projecte són: 12c x 25h/c = 300h

3. Per últim també s'ha valorat la subscripció de la llicència per a utilitzar l'opció de Machine Learning.

En base als criteris esmentats, s'ha realitzat la següent assignació pressupostària.

Cost total		**12.600 € 22€/mes**
Descripció	**Dedicació**	**Total**
Disseny de la solució, planificació i seguiment del projecte	100 h	5.000 €
Implantació de la solució	200 h	7.600 €
Llicència Machine Learning		22€/mes

6.2 Seguiment de la planificació

La planificació del TFM s'ha estructurat en 3 blocs molt diferenciats, el primer d'investigació, el segon d'implantació i l'últim amb les conclusions.

L'elaboració de la planificació inicial s'ha realitzat de manera molt realista amb uns objectius molt marcats, tenint en compte el temps de dedicació i les solucions a utilitzar. Sent conscient que la plataforma Wazuh i ELK Stack són unes plataformes amb molt potencial, tot i això, s'ha optat per establir uns objectius modestos per tenir temps d'analitzar, instal·lar i configurar la solució, i veure'n els resultats.

En general el compliment de la planificació ha estat correcte a excepció del bloc d'implantació on s'ha dedicat més temps del previst degut a les configuracions de Machine Learning i les notificacions que es deriven d'aquest.

6.3 Valoració dels objectius aconseguits

1a Part: Aconseguir la màxima informació per decidir l'esquema a implantar per tal de:

- **Obtenir una visió global dels sistemes de seguretat, i en concret dels SIEM i IDS.**
  S'ha trobat molta informació a les xarxes i s'ha pogut aprofundir en la historia i el funcionament d'aquestes solucions, observant com de valuosos son els logs.
- **Conèixer l'evolució dels atacs per Cryptolocker i la seva afectació a les empreses.**

Sens dubte és una de les amenaces més de moda tot i portar molts anys entre nosaltres.

- **Decidir quins sistemes i com s'implantaran per tal d'obtenir el resultat desitjat.**
  Gràcies a tota la investigació feta s'ha pogut valorar la implantació del SIEM open source Wazuh integrat amb la ELK Stack.

2a Part: Implantar les bases d'un sistema de seguretat:

- **Realitzar la implantació en un entorn Docker ja existent.**
  La plataforma Docker ha permès accelerar moltíssim la implantació del projecte, gràcies a les configuracions ja existents a la pàgina de github de Wazuh.
- **Implantar i configurar l'agent en el servidor a monitorar.**
  Gràcies a la configuració de l'agent Wazuh i les polítiques de Windows s'ha obtingut un resultat satisfactori de les incidències registrades amb la simulació d'atac.
- **Implantar i configurar el SIEM.**
  La visibilitat de la informació per part de la ELK Stack i la possibilitat de centralitzar la configuració dels agents agrupant-los, sense dubte fan de Wazuh una eina molt àgil.
- **Simular un atac.**
  S'ha realitzat una simulació d'atac molt senzilla per tal de veure el resultat de tot el cicle dels logs, des que es generen al servidor atacat fins que és rep la notificació a Teams.
- **Proposar i documentar millores.**
  Degut a que s'ha utilitzat molt temps en la implantació i documetació del projecte, les millores que s'han proposat son a nivell teòric.

3a Part: Avaluar i treure conclusions de la proposta de forma global

- **Valorar els resultats obtinguts.**
  Els resultats obtinguts han permès veure el funcionament global de la solució i la seva integració amb les eines existents del departament IT.
- **Realitzar una valoració econòmica de la implantació del sistema de seguretat proposat.**
  S'ha realitzat una valoració econòmica del disseny i implantació del projecte.

6.4 Treball futur

En aquest apartat es descriuen algunes de les possibles millores del projecte, que per falta de temps no s'han pogut dur a terme.

Com a millores i treballs a futurs s'observa que serien molt interessants els següents punts: comprovar el funcionament dels treballs de Machine Learning en un servidor en producció, respondre a l'atac amb la configuració d'un Active Responsive, ampliar la configuració del agent amb la funcionalitat "VirusTotal", millorar la implementació dels agents HIDS i estudiar la integració amb un SIRP[8].

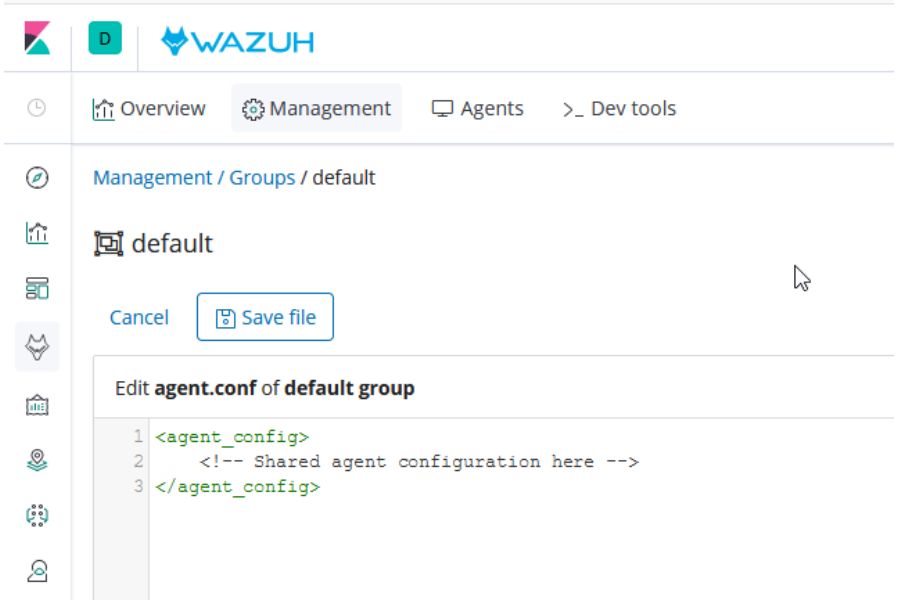
Pel que fa al treball de Machine Learning en la configuració actual, s'ha observat la detecció de l'atac en un servidor de proves amb molt poc trànsit d'informació, per tal de tenir una valoració més acurada del funcionament del treball configurat, seria molt interessant observar com mostra els resultats i els temps de resposta en un entorn en producció amb un flux de dades més pròxim a la realitat.

L'agent HIDS també permet la configuració de "active responsive" per tal d'executar un script en l'agent a partir d'un cert nivell d'alerta, o grups d'alertes. Aquesta opció permetria, per exemple, aïllar el servidor atacat afegint una regla al firewall de l'equip i minimitzar les conseqüències de l'atac.

La següent opció que s'ha contemplat és la integració que ofereix Wazuh amb el servei de VirusTotal, una opció Open Source què permet analitzar fitxers a partir d'una base dades de coneixement, detectar malware als fitxers del servidor i, mitjançant la configuració d'un "active responsive", realitzar accions com eliminar el virus. Aquest servei complementaria la detecció no només de Ransomware, si no d'altres opcions de Malware.

Com a opció de millora també s'ha contemplat la manera d'implementar els agents HIDS mitjançant polítiques de domini i modificar la configuració dels mateixos de manera centralitzada, mitjançant el menú Wazuh ubicada a Kibana i agrupan els agents per grups.

[8] Security Incident Response Platform o plataforma de resposta a incidents de seguretat.



Il·lustració 59: Kibana - Wazuh, configuració agent

I per últim també es considera com a treball molt interessant la creació d'un SIRP per tal de fer un seguiment dels incidents. Per dur-ho a terme s'ha contemplat la opció TheHive, Cortex i MISP com a plataformes que s'integren perfectament amb Wazuh i Elastic Stack, i són projectes Open Source.

Il·lustració 60: Logos de TheHive, MISP, Cortex

Glosari

- **Ransomware**: de l'anglès "**ransom**" segres i "soft**ware**", és un tipus de programa maliciós que busca capturar les dades per després demanar-ne un rescat a canvi d'alliberar-les
- **Cryptolocker:** és un tipus de Ransomware que encripta les dades segrestades i demana un rescat a canvi d'obtenir la clau per desencriptar-les.
- **HIDS:** de les seves sigles en anglès Host-based Intrusion Detection System, és un sistema de detecció d'intrusos en Host. Aquest sistema busca detecta anomalies que siguin un risc en un equip concret.
- **Pila ELK:** Les sigles ELK fan referència als productes Elasticsearch, Logstash i Kibana de l'empresa Elastic.
- **SIEM:** de les seves sigles en anglès, Security Information Event Management, és un sistema centralitzat de recollida d'esdeveniments i logs, que permet relacionar-los i tenir una visió global de la seguretat d'un sistema.
- **Wazuh:** és un sistema open source de detecció d'anomalies de seguretat basat en Host
- **IDS:** de les seves sigles en anglès, Intrusión Detection System, son sistemes de detecció d'intrusos i entre ells podem trobar els HIDS, NIDS, etc.
- **Docker:** plataforma open source per al desplegament de la virtualització de software amb contenidors en un sistema operatiu comú.
- **SEM:** de les seves sigles en anglès, Security Event Management, és un sistema que recol·lecta, monitoritza y analitza esdeveniment de seguretat de manera centralitzada.
- **SIM:** de les seves sigles en anglès, Security Information Management, és un sistema que recol·lecta, monitoritza y analitza logs de seguretat de manera centralitzada.
- **Fork:** en enginyeria de software un Fork és con s'agafa el codi d'un projecte existent i s'inicia un projecte independent agafant com a base aquest codi.
- **NIDS:** de les seves sigles en anglès, Network Intrusion Detection, és un sistema de detecció d'anomalies basat en la xarxa.
- **IPS:** de les seves sigles en anglès, Intrusion Prevention System, és un sistema que controla l'accés a la xarxa.
- **DoS:** Aquest atac té la finalitat de bloquejar el sistema i/o servei al que va destinat enviant, des d'un equip, més sol·licituds de peticions de les que pot resoldre el servei.
- **DDoS:** Aquest atac té la finalitat de bloquejar el sistema i/o servei al que va destinat enviant, des de múltiples equips, més sol·licituds de peticions de les que pot resoldre el servei.
- **UEBA:** de les seves sigles en anglès, User and Entity Behavior Analytics, s'utilitza en Machine Learning i anàlisis de dades per determinar models de comportaments dels humans i les màquines dins un entorn concret.
- **SOAR:** de les seves sigles en anglès, Security Orchestration Automation and Response. Aquestes solucions intenten automatitzar les tasques més rutinàries en seguretat mitjançant l'agregació i correlació de dades.
- **SIRP:** de les seves sigles en anglès, Security Incident Response Platform, és una plataforma per gestionar la resposta a incidents de seguretat.

- **RSA:** de les sigles dels seus creadors, Ron **R**ivest, Adi **S**hamir i Leonard **A**dleman, és un sistema criptogràfic de clau pública molt utilitzant, tant en xifratge de dades com en firma digital.
- **RaaS:** de les seves sigles en anglès, Ransomware As A Service, és un tipus de servei que ofereix un Malware com a servei a canvi d'un pagament per ús.
- **Malware:** és tot aquell software dissenyat per causar algun d'any a l'equip o equips als que va destinats.
- **Machine Learning:** és una aplicació de la intel·ligència artificial que busca d'aprendre del comportament de manera automàtica i sense cap programació específica.
- **LOG:** és informació guardada per un sistema d'un comportament determinat ocorregut en un determinat moment, per exemple el login d'un usuari, o l'eliminació d'un fitxer.
- **Base de dades CVE:** de les seves sigles en anglès, Common Vulnerabilities and Exposures. És una base dades que utilitza el sistema CVE per publicar vulnerabilitats.
- **GDPR:** de les seves sigles en anglès, General Data Protection Regulation, és una normativa europea que regula la protecció de les dades a partir del 25 de maig del 2018
- **ODFE:** de les seves sigles en anglès, Open Distro For Elasticsearch, és un fork de Elasticsearch creat per l'empresa Amazon.

Bibliografia

- **“IDS” 2020. [Web] Disponible: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips**
- **“Ransomware” 2020. [Web] Disponible: https://es.malwarebytes.com/ransomware/**
- **“SIEM” 2020. [Web] Disponible: https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage**
- **“Elasticsearch” 2020. [Web] Disponible: https://en.wikipedia.org/wiki/Elasticsearch**
- **“SIEM” 2020. [Web] Disponible: https://logz.io/blog/open-source-siem-tools/**
- **“Wazuh” 2020. [Web] Disponible: https://www.programmersought.com/article/9734805292/**
- **“App Wazuh en Splunk” 2020. [Web] Disponible: https://documentation.wazuh.com/3.7/installing-splunk/index.html**
- **INCIBE “DDos, DoS” 2020. [Web] Disponible: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos**
- **“Història dels SIEM” 2020. [Web] Disponible: https://cybersecurity-magazine.com/a-brief-history-of-siem/#:~:text=SIEM%201.0%20circa%202006%20%E2%80%93%20A,management%20for%20the%20first%20time.**
- **“SIEM, UEBA, SOAR” 2020. [Web] Disponible: https://www.technology.org/2019/04/30/siem-ueba-and-soar-whats-the-difference/**
- **“Cryptolocker” 2020. [Web] Disponible: https://en.wikipedia.org/wiki/CryptoLocker**
- **“Ransomware” 2020. [Web] Disponible: https://www.incibe.es/protege-tu-empresa/blog/el-ransomware-y-recupero-mi-informacion#:~:text=El%20ransomware%20es%20un%20tipo,que%20vuelva%20a%20ser%20accesible.**
- **INCIBE “Wannacry” 2020. [Web] Disponible: https://www.incibe.es/sites/default/files/contenidos/boletines/doc/boletin_informativo_19_de_mayo_de_2017.pdf**
- **Wikipedia “Splunk” 2020. [Web] Disponible: https://en.wikipedia.org/wiki/Splunk**
- **Wazhu “Splunk and Wazuh” 2020. [Web] Disponible: https://documentation.wazuh.com/3.13/installation-guide/installing-splunk/splunk-app.html**
- **Gartner “Magic quadrant SIEM 2020” 2020. [Web] Disponible: https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage**

- **Elastic “Elastic Stack and Wazuh” 2020. [Web] Disponible: https://www.elastic.co/es/blog/improve-security-analytics-with-the-elastic-stack-wazuh-and-ids**
- **Elastic “Elasticsearch” 2020. [Web] Disponible: https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html**
- **Elastic “Logstash” 2020. [Web] Disponible: https://www.elastic.co/guide/en/logstash/current/introduction.html**
- **Elastic “Kibana” 2020. [Web] Disponible: https://www.elastic.co/guide/en/kibana/7.9/index.html**
- **Elastic “Machine learning” 2020. [Web] Disponible: https://www.elastic.co/guide/en/machine-learning/current/index.html**
- **“Machine learning” 2020. [Web] Disponible: https://expertsystem.com/machine-learning-definition/#:~:text=Machine%20learning%20is%20an%20application,use%20it%20learn%20for%20themselves.**
- **“Wazuh” 2020. [Web] Disponible: https://documentation.wazuh.com/3.9/user-manual/index.html**
- **“Wazuh integració API externa” 2020. [Web] Disponible: https://wazuh.com/blog/how-to-integrate-external-software-using-integrator/**
- **“ODFE” 2020. [Web] Disponible: https://opendistro.github.io/for-elasticsearch/**
- **“Wazuh File Integrity Monitoring” 2020. [Web] Disponible: https://documentation.wazuh.com/3.10/user-manual/capabilities/auditing-whodata/who-windows.html**
- **“Opendistro for Elasticsearch” 2020. [Web] Disponible: https://aws.amazon.com/es/blogs/opensource/launching-open-distro-for-elasticsearch-security-features-on-amazon-elasticsearch-service/**
- **“Github Wazuh” 2020. [Web] Disponible: https://github.com/wazuh/wazuh/issues/3467**
- **“Active Responsive Wazuh” 2020. [Web] Disponible: https://documentation.wazuh.com/3.11/user-manual/capabilities/active-response/how-it-works.html**
- **“Wikipedia Virustotal” 2020. [Web] Disponible: https://en.wikipedia.org/wiki/VirusTotal**
- **“SIRP” 2020. [Web] Disponible: https://red-orbita.com/?p=8726**
- **“TheHive” 2020. [Web] Disponible: https://thehive-project.org/**
- **“Wikipedia CVE” 2020. [Web] Disponible: https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures**
- **“GDPR” 2020. [Web] Disponible: https://gdpr-info.eu/**