Universitat Oberta de Catalunya

uoc.edu

SIEMaaS adreçat a la PIME

Raül Martínez Díaz
Màster de Seguretat de les Tecnologies de la Informació i de les Comunicacions
Seguretat Empresarial

Jordi Guijarro Olivares
Victor Garcia Font

Tarragona, 31 de Maig de 2022


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

FITXA DEL TREBALL FINAL

Títol del treball:	SIEMaaS adreçat a la PIME
Nom de l'autor:	*Raül Martínez Díaz*
Nom del consultor/a:	*Victor Garcia Font*
Nom del PRA:	*Jordi Guijarro Olivares*
Data de lliurament (mm/aaaa):	*05/2022*
Titulació o programa:	Màster de Seguretat de les Tecnologies de la Informació i de les Comunicacions
Àrea del Treball Final:	*M1.749 - TFM-Seguretat empresarial*
Idioma del treball:	*Català*
Paraules clau	*Ciberseguretat, PIME, SIEM, EDR.*

Resum del Treball:

Els incidents de ciberseguretat van assolir un màxim històric a nivell mundial el quart trimestre del 2021 . Les PIME espanyoles no son alienes a aquesta tendència, exposades a un notable increment en el nombre i complexitat de les amenaces que han d'afrontar.

Davant el repte de protegir la seva activitat, les PIME estan abocades a fer un pas endavant en les seves estratègies de ciberseguretat mitjançant la implementació d'estratègies de protecció que requereixen el desplegament d'eines de vigilància de la seguretat avançades.

El present treball aborda el disseny i desplegament d'una solució SIEM as a Service orientada a la PIME basada en Elastic Stack i la plataforma de seguretat Wazuh. S'analitzen les característiques de la solució, funcionalitats i possibles models de servei, realitzant una sèrie de proves de concepte sobre la solució per tal de valorar la seva idoneïtat com a solució SIEM as a Service orientada a la PIME

Abstract:

Cybersecurity incidents reached an all-time high globally in the fourth quarter of 2021. Spanish SMEs are not exempt from this trend, exposed to a notable increase in the number and complexity of the threats that we must face.

Faced with the challenge of protecting their activity, SMEs are bound to take a step forward in their cybersecurity strategies by implementing protection strategies that require the deployment of advanced security monitoring tools.

This paper deals with the design and deployment of a SIEM as a Service solution oriented to SMEs based on the Elastic Stack and the Wazuh security platform. The characteristics of the solution, functionalities and possible service models are analyzed, carrying out a series of concept tests on the solution to assess its suitability as a SIEM as a Service solution oriented to SMEs.

Índex

Índex de figures

1. Introducció

1.1 Context i justificació del Treball

Els incidents de ciberseguretat van assolir un màxim històric el quart trimestre del 2021, una any que alguns dels principals proveïdors de solucions en ciberseguretat defineixen com a especialment complicat. En aquest sentit, Check Point Research constata fins a un 50% més d'intents d'atac per setmana a nivell mundial sobre les xarxes corporatives en comparació amb el 2020 [1].

Les organitzacions i PIME espanyoles no son alienes a aquesta tendència, així ho indica el creixent número d'incidents de seguretat gestionats per l'Institut Nacional de Ciberseguridad (INCIBE), fins a 133.155 incidents atesos l'any 2020, un 30% més de casos que l'any anterior [2].

Els experts coincideixen a indicar que no es tracta d'un fet conjuntural, i que gran, mitjana i petita empresa s'enfronten a un creixent nombre d'amenaces. Aquest increment en el número i complexitat de les amenaces suposa un repte per les empreses, abocades a fer pas endavant en les seves estratègies de ciberseguretat mitjançant la definició de plans i polítiques de seguretat, alhora que impulsen la implementació d'eines de vigilància de la seguretat avançades, com ara tallafocs de nova generació (NGFW), sistemes de detecció i prevenció d'intrusions (IDS, IPS), o sistemes de vigilància continua de la seguretat (SIEM, EDR, XDR). Son eines complexes, amb uns costos generalment elevats i que requereixen de professionals específics altament qualificats.

A Espanya, on les petites i mitjanes empreses (PIME) engloben el 99,8% de les empreses, els ciberatacs impliquen un elevat cost econòmic, algunes fonts el xifren en uns 35.000 euros per atac de mitjana, però també de

[1] CKECK POINT. *Check Point Research:Cyber Attacks Increased 50% Year over Year* [en línia]. Blog, 2021 [consulta: 27 de Febrer de 2022]. Disponible a https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

[2] INCIBE. *INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020* [en línia]. Nota de premsa, 2021 [consulta: 28 de Febrer de 2022]. Disponible a https://www.incibe.es/sala-prensa/notas-prensa/incibe-gestiono-mas-130000-incidentes-ciberseguridad-durante-el-ano-2020

reputació, especialment quan impacten directament sobre l'activitat de l'empresa.

L'informe "*Panorama actual de la Ciberseguretat a Espanya*"[3] indica que la cultura de ciberseguretat a l'empresa espanyola és encara molt reactiva i només un 36% de les empreses enquestades han establert alguna mena de principis bàsics de seguretat a la seves organitzacions. Tot i això, l'estudi constata una creixent preocupació de les empreses en matèria de ciberseguretat.

Tot plegat ens situa en un context en el qual les pimes tenen la necessitat de protegir el seu negoci consolidant la seva estratègia de ciberseguretat mitjançant eines de vigilància de la seguretat avançades que, generalment, no estan al seu abast, o bé perquè impliques uns costos elevats, o bé perquè requereixen de professionals altament qualificats dels quals no disposen.

El present treball explora les possibilitats per dotar a les PIME d'una solució SIEM as a Service integrada per un ecosistema de tecnologies de vigilància de la seguretat que, per la seva complexitat i costos, estan habitualment fora del seu abast.

1.2 Objectius del Treball

L'objectiu principal del present treball és l'estudi, anàlisi i desplegament d'una solució de SIEM as a Service (SIEMaaS) adreçada a la PIME.

Per tal d'assolir l'objectiu establert s'han definit tres etapes: una primera fase de recerca i anàlisi adreçada a recollir els requisits funcionals de la solució, una segona fase de integració i desenvolupament adreçada a desplegar un model funcional de SIEM as a Service en base als requisits obtinguts, i per últim, una darrera fase de síntesi i anàlisi de la viabilitat comercial de la solució.

Per a cada una d'aquestes fases s'han definit objectius específics, essencials per assolir l'objectiu final del treball:

[3] GOOGLE. Panorama actual de la Ciberseguridad en España [en línia]. Publicació en línea, Octubre de 2019 [consulta: 27 de Febrer de 2022]. Disponible a: https://drive.google.com/file/d/18TNjaDus-lrSl5gL5Wt-Z4DOsKXtQ46m/view

Fase recerca i anàlisi:

- Anàlisi de les característiques de la infraestructura IT en el context de la PIME a fi de determinar els requisits que hauria de tenir un sistema SIEM per al seu desplegament en aquest àmbit.
- Identificar les característiques i requisits específics d'un SIEM as a Service.
- A partir de l'estudi i anàlisi dels sistemes SIEM existents al mercat determinar la solució que més s'adeqüi tan a les característiques i necessitats especifiques de la PIME, com als requeriments funcionals d'un SIEM as a Service.
- Identificar els conjunt d'eines i serveis complementaris necessaris per al desplegament d'un ecosistema SIEM as a Service sobre la base del sistema SIEM seleccionat.

Fase d'integració i desenvolupament:

- Dissenyar un ecosistema de SIEM as a Service sobre la base del sistema SIEM seleccionat.
- Implementar un model funcional del ecosistema SIEM dissenyat, integrant el sistema base SIEM amb el conjunt d'eines i serveis necessaris per assolir les funcionalitats definides als requisit funcionals.
- Validar el model mitjançant la execució de conjunts de probes específicament dissenyats.

Síntesi i anàlisi de viabilitat:

- Valoració del ecosistema SIEM as a Service obtingut, identificació de fortaleses i mancances.
- Valoració de la viabilitat del ecosistema obtingut com a solució comercial, identificar i valorar models d'explotació i servei.

1.3 Enfocament i mètode seguit

El focus del present treball rau a l'estudi, anàlisi i desplegament d'una solució de SIEM as a Service (SIEMaaS) adreçada a la PIME. Per tal d'assolir l'objectiu definit, s'ha optat per afrontar el treball des de dues vessants, una primera vesant d'investigació o recerca adreçada principalment a la recollida dels requisits funcionals de la solució, i una segona vesant de integració, adreçada al desplegament d'una solució SIEM en base als requisits obtinguts.

Cada una d'aquestes vessants constitueix una fase *sine qua non* del present treball.

La fase de recerca i anàlisi està focalitzada sobre l'estudi de l'estat de l'art i de les solucions SIEM existents a fi de determinar aquella solució o solucions que s'adeqüin, d'una banda a les característiques i necessitats especifiques de la PIME, i d'altra banda als requeriments funcionals d'un SIEM as a Service. A partir d'aquesta tasca s'elaborarà una proposta de ecosistema SIEM as a Service, així com el conjunt de requisits funcionals que la solució ha de satisfer fer assolir l'objectiu principal del treball.

La fase d'integració i desenvolupament consisteix a desplegar un model funcional de la solució SIEM seleccionada, així com de l'ecosistema d'eines i serveis complementaris necessaris per a la paquetització de la solució com SIEM as a Service. Per tal de validar que el model desplegat s'ajusta als requisits funcionals definits a la fase d'investigació, s'integrarà la solució desenvolupada en un entorn de laboratori on s'hi desenvoluparan una sèrie de proves de concepte.

Donat que el temps disponible per assolir dels objectius definits és limitat, al treball hi tindran més rellevància l'estudi, anàlisi, disseny i viabilitat de la solució SIEM as a Service que no pas el desenvolupament funcional de la mateixa, que és limitarà al desplegament de les funcionalitats essencials per a la validació del model integrat.

Finalment, com a síntesi del treball, es destinarà un darrer apartat a valorar la solució obtinguda, fent èmfasi en les seves fortaleses i mancances, així com a determinar-ne la seva viabilitat com a producte comercial.

1.4 Planificació del Treball

La planificació del present treball s'estructura en quatre fites, corresponents a les entregues definides al calendari del Pla Docent. Cada una d'aquestes fites delimita una etapa necessària del treball . Al següent quadre, es detallen cada una d'aquestes fites així com les tasques necessàries per assolir-les:

Tasques	Inici	Fi	
Pla de Treball	16/02/2022	1/03/2022	14 dies
Anàlisis previ i recollida d'objectius	16/02/2022	25/02/2022	9 dies
Redacció Entrega 1 - Pla de Treball	26/02/2022	1/03/2022	5 dies
Entrega 1 - Pla de Treball		**1/03/2022**	**FITA**

Recerca i anàlisi		2/03/2022	29/03/2022	28 dies
	Recerca, estudi i anàlisi de la infraestructura IT de la Pime	2/03/2022	8/03/2022	7 dies
	Recerca, estudi i anàlisi SIEM as a Service	9/03/2022	28/03/2022	20 dies
	Estudi de l'estat de l'art	9/03/2022	15/03/2022	7 dies
	Recerca i estudi ecosistema SIEM	16/03/2022	19/03/2022	4 dies
	Elecció de sistema SIEM	20/03/2022	20/03/2022	1 dia
	Estudi detallat sistema SIEM seleccionat	20/03/2022	28/03/2022	9 dies
	Definició formal dels requisits funcionals de la solució	25/03/2022	29/03/2022	5 dies
	Redacció Entrega 2 – Recerca	22/03/2022	29/03/2022	8 dies
	Entrega 2 - Recerca		**29/03/2022**	**FITA**
Integració i desenvolupament		30/03/2022	26/04/2022	28 dies
	Documentació i preparació de recursos	30/03/2022	2/04/2022	4 dies
	Disseny i prototipatge de la solució	30/03/2022	06/04/2022	8 dies
	Integració	07/04/2022	26/04/0222	20 dies
	Integració SIEM seleccionat	07/04/2022	16/04/2022	10 dies
	Integració SOAR	17/04/2022	21/04/2022	5 dies
	Integració d'altres eines i serveis segons requisits funcionals SIEM as a Service.	22/04/2022	24/04/2022	2 dies
	Redacció Entrega 3 – Integració	20/04/2022	26/04/2022	7 dies
	Entrega 3 - Integració		**26/04/2022**	**FITA**
Jocs de probes, validació i lliurament final		27/04/2022	31/05/2022	35 dies
	Jocs de Probes	27/04/2022	15/05/2022	19 dies
	Preparació entorn de probes	27/04/2022	30/04/2022	4 dies
	Disseny e implementació joc de probes	1/05/2022	10/05/2022	10 dies
	Anàlisi de resultats	11/05/2022	15/05/022	5 dies
	Síntesi i anàlisi de viabilitat	15/05/2022	21/05/2022	7 dies
	Redacció Memòria Final	15/05/2022	31/05/2022	17 dies
	Entrega 4 – Memòria Final		**31/05/2022**	**FITA**
	Elaboració vídeo presentació Memòria Final	1/07/2022	07/06/2022	7 dies
Durada del treball		16/02/2022	31/05/2022	105 dies

1.5 Descripció de la memòria del treball

El present document conté la memòria del treball final del Màster de Seguretat de les Tecnologies de la Informació i de les Comunicacions, treball desenvolupat en l'àrea de Seguretat empresarial i al qual s'aborda l'estudi i desenvolupament d'una solució SIEM as a Service orientada a la PIME.

La memòria del treball s'estructura en una sèrie de capítols, corresponents a cada una de les fases del treball:

- Introducció i pla del treball (Capítol 1) En aquest apartat s'introdueix el context, objectius i l'enfocament del treball.
- Recerca i anàlisi (Capítol 2) El capítol de recerca i anàlisi s'hi desenvolupa, d'una banda, l'estudi de les característiques de la ciberseguretat a la PIME espanyola, i de l'altra, l'estudi de l'estat de l'art i de les solucions SIEM existents a fi de determinar aquella solució que s'adeqüi, d'una banda a les característiques i necessitats especifiques de la PIME, i de l'altra als requeriments funcionals d'un SIEM as a Service.
- Elastic Stack i les solucions Open Source (Capítols 3 i 4) En aquests capítols es descriuen i analitzen les característiques i funcionalitats dels productes i solucions escollits per al desenvolupament de la solució SIEMaaS, Elastic Stack i Wazuh.
- Desplegament d'una solució SIEMaaS (Capítols 5) Aquest capítol està dedicat a l'estudi, disseny i desplegament d'un model funcional de SIEM as a Service a partir de Elastic Stack i Wazuh. S'hi descriuen les funcionalitat, l'arquitectura general de la solució, així com possibles models de servei.
- Conclusions (Capítols 6) Capítol destinat a exposar les conclusions de la memòria, valorar l'ecosistema SIEM as a Service obtingut, així com identificar-ne fortaleses i mancances. El capítol conclou amb una síntesi de les línies de treball futur que no s'han pogut explorar en aquest treball i han quedat pendents.

Als darrers capítols del document s'hi recull un glossari amb el termes més destacats, així com un llistat amb bibliografia consultada per a la realització del present treball.

Finalment, als annexes s'inclouen una sèrie de guies d'instal·lació i configuració de la solució SIEM as a Service desplegada a les proves de concepte.

2. Recerca i anàlisi

Aquesta secció recull els resultats de l'estudi realitzat sobre les necessitats especifiques de la PIME en l'àmbit de la ciberseguretat, per després centrar-se en l'estudi de l'estat de l'art i les característiques, funcionalitats i beneficis d'una solució SIEM.

2.1 Ciberseguretat a la PIME

2.1.1 Panorama de la ciberseguretat a la PIME

La digitalització d'empreses i organitzacions és un fet des de fa alguns anys, però amb l'arribada de la pandèmia de la Covid-19 aquest procés sembla haver-se accelerat per la necessitat d'adaptar-se a la nova realitat. La introducció massiva del teletreball ha impulsat notablement la digitalització del processos empresarials, estimulant la innovació i la transformació digital, però alhora també ha generat una sèrie de riscos i amenaces de ciberseguretat.

Segons dades de *Check Point Research* l'any 2021 es van produir un 50% més d'intents d'atac per setmana a nivell mundial sobre les xarxes corporatives en comparació amb el 2020.

Les PIME i empreses espanyoles no son alienes a aquesta tendència, així ho indica el creixent número d'incidents de seguretat gestionats per l'Institut Nacional de Ciberseguridad (INCIBE), fins a 133.155 incidents atesos l'any 2020, un 30% més de casos que l'any anterior.

Els ciberatacs impliquen per les PIMES un elevat cost econòmic, que algunes fonts xifren en uns 35.000 euros per atac de mitjana, i de reputació, especialment quan impacten directament sobre l'activitat de l'empresa, paralitzant total o parcialment. Tot i això, l'informe "*Panorama actual de la Ciberseguretat a Espanya*" indica que la cultura de ciberseguretat Espanyola és encara molt reactiva i només un 36% de les empreses enquestades han establert alguna mena de principis bàsics de seguretat a la seves organitzacions.

Al mateix informe s'apunta també indiquen cert desconeixement dels riscos al quals s'enfronten. Kaspersky, en el seu informe "*Economía de la seguridad*

de TI en el 2019"[4] indica que més de la meitat (el 55%) de les empreses confien plenament que la seva xarxa no ha estat hackejada, encara que més d'un terç (el 38%) reconeixen que no compten amb prou informació sobre les amenaces a les quals s'enfronten.

En general les dades indiquen que les PIMES i empreses espanyoles tenen un grau de maduresa en el camp de la ciberseguretat inferior a la mitjana europea, i per tant molt marge de millora.

Tot i que les dades puguin semblar pessimistes, hi ha una creixent preocupació sobre la problemàtica de la ciberseguretat dins la PIME. Sigui perquè han estat víctimes d'un atac, per compliments normatius, o per requisits de clients i proveïdors, els gestors i equips directius estan cada cop més conscienciats dels riscos que els ciberatacs comporten a les seves organitzacions. Aquesta preocupació ha impulsant, i ho continuarà fent de manera notable durant propers anys, la demanda de solucions i productes adreçats a la PIME en l'àmbit de la ciberseguretat.

Un altre fet rellevant és el constant increment en l'ús per part de la PIME de serveis, aplicacions i recursos ubicats al núvol, ja que veuen en aquestes tecnologies una oportunitat per modernitzar les seves infraestructures d'una manera més rentable, flexible i eficient. Segons dades de Karpersky[5] el 73% de les pimes i el 56% de les micro-pimes asseguren utilitzar com a mínim un servei al núvol. Entre les solucions al núvol més implementades es troben les plataformes de correu electrònic, les eines de col·laboració i emmagatzemament de documents o les aplicacions de gestió i finances.

Aquesta consolidació en l'ús d'aplicacions i serveis ubicats al núvol introdueix nous escenaris en la gestió de la seguretat. La dispersió de dades i serveis entre múltiples plataformes de les quals en moltes ocasions no s'arriben a tenir els nivells de control i visibilitat adequats obliga a les PIMES revisar les seves polítiques i protocols de seguretat. En moltes ocasions els departament de IT corresponents no disposen de la formació necessària per a la correcta gestió d'aquestes plataformes o aquesta és incompleta, generant que es puguin produir errors a la configuració del servei o en la seva gestió. Errors que poden comprometre la seguretat del servei i de les dades que conté.

[5] KARPERSKY. *Economía de la seguridad de TI en el 2019* [en línia]. Publicació, 2019 [consulta: 27 de Febrer de 2022]. Disponible a https://go.kaspersky.com/rs/802-IJN-240/images/SP%20Brochure_A4_Report-IT-Security-Economics-SP.pdf

2.1.2 Principals amenaces de seguretat a la PIME

Les empreses i PIMES s'enfronten cada dia a un ampli i creixent ventall d'amenaces de seguretat. Cada una d'aquestes amenaces exigeix la implementació d'unes mesures de control i prevenció especifiques.

A la següent taula es recull una relació de les principals amenaces de ciberseguretat així com les seves respectives mesures de prevenció:

AMENAÇA	**MESURA**
Configuracions errònies i males pràctiques	Auditories de Sistemes i seguretat Formació TIC
Phishing	Filtres anti-spam Conscienciació d'usuaris
Atacs de denegació de servei i intrusions	Tallafocs Sistema de Prevenció d'intrusions (IPS)
Programari maliciós (Malware)	Antivirus Sistema de Detecció d'Intrusions (SDI)
Programari de rescat (Ransomware)	Antivirus Sistema de Detecció d'Intrusions (SDI) Segmentació de xarxes
Vulnerabilitats de dia zero	Sistemes de detecció avançada Auditories i anàlisis de vulnerabilitats
Fuita de dades	Sistemes de prevenció de fuita de dades (Data Lake Prevention)

Com es pot apreciar a la taula anterior, si el ventall d'amenaces és ampli, també ho son el conjunt de mesures de control i prevenció que aquestes exigeixen.

Cada una d'aquestes mesures genera de forma contínua alertes i esdeveniments de seguretat que els professionals de la seguretat han de revisar i gestionar el més àgil i ràpidament possible per tal de prendre les mesures de contenció i mitigació oportunes.

Per facilitar aquesta tasca els professionals de la seguretat disposen d'un potent instrument, els SIEM (Security Information and Event Management) o Sistema de Gestió de Esdeveniments i Informació de Seguretat, que permeten recopilar, normalitzar i analitzar els esdeveniments de seguretat provinents de múltiples fonts proporcionant una visió global de la seguretat. Al següent apartats s'analitzarà aquest eina i avaluarem quins beneficis pot aportar el seu ús a la gestió i supervisió de la seguretat a la PIME.

2.2 SIEM

En aquest apartat s'estudia què és un SIEM, quines són les seves funcionalitats principals i quins beneficis aporta en el context de la gestió de la informació de seguretat.

2.2.1 Què és un SIEM ?

Un **SIEM** (*Security Information and Event Management*) o Sistema de Gestió de Esdeveniments i Informació de Seguretat, és una solució orientada a la vigilància de la seguretat. Integrada per ampli ventall d'eines i serveis, és caracteritza per la seva capacitat per detectar, respondre i neutralitzar les amenaces informàtiques. El seu objectiu principal és el proporcionar una visió global de la seguretat en l'àmbit de les tecnologies de la informació.

Els SIEM combinen en una única solució les eines i serveis necessaris per recopilar esdeveniments i alertes de seguretat de totes les tecnologies que intervenen en una xarxa (aplicacions, tallafocs, solucions de prevenció d'intrusions com IDS/HIDS, registres..). El SIEM ingesta, emmagatzema, normalitza i analitza les dades recopilades d'aquestes fonts, permetent una visió completa de la seguretat de la informació, alhora que ofereix als analistes de seguretat un potent instrument per descobrir, en temps real, tendències i patrons anòmals que evidenciïn amenaces de seguretat i atacs presents a la infraestructura.

La tecnologia SIEM neix a partir de la combinació la gestió de la informació de seguretat (SIM) i la gestió de esdeveniments de seguretat (SEM) per proporcionar una anàlisi en temps real de les alertes de seguretat generades per les aplicacions i el maquinari de la xarxa.

- SEM s'utilitza per detectar patrons anormals i analitzar, pràcticament en temps real, tot el que passa en la gestió de seguretat.

- SIM recopila i agrupa les dades en un repositori central per posteriorment analitzar-les, proporcionant informes automatitzats content informació molt valuosa per als professionals de la seguretat responsables de la infraestructura.

La combinació de ambdues funcionalitats en una única solució permet que es pugui actuar més ràpidament sobre els atacs, ja que d'una banda ofereixen més visibilitat i de l'altra permeten utilitzar les dades per a la supervisió i l'anàlisi de la seguretat en temps real.

2.2.2 Quines funcionalitats té un SIEM ?

En aquest apartat es descriuen breument les funcionalitats principals d'un SIEM:

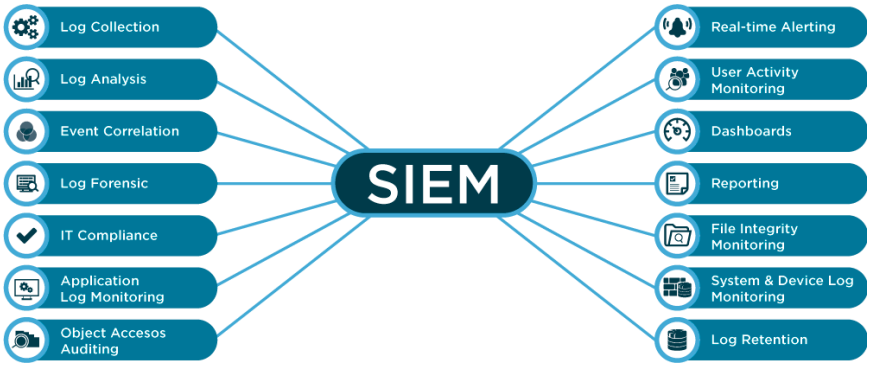


Figura 1- Funcionalitat d'un SIEM

- Agregació de dades: Les solucions SIEM tenen la capacitat de ingerir dades provinents de múltiples fonts, traslladant la informació a un repositori central. Aquestes dades poden recopilar-se directament a partir de col·lector dissenyats per obtenir dades de tota mena de dispositius, equips i aplicacions de la xarxa o a través de d'agents que recullen la informació als equips i la reenvien cap la solució SIEM.
- Correlació d'esdeveniments de seguretat: La correlació d'esdeveniments de seguretat es basa en el tractament de la informació recopilada a fi de detectar patrons i identificar indicis d'activitat maliciosa.
- Gestió d'alertes: Partint de l'anàlisi dels esdeveniments correlacionats els SIEM tenen la capacitat de generar avisos de seguretat automatitzats que s'envien als responsables de seguretat pel seu tractament.
- Taulell de comandament: Els SIEM disposen d'una sèrie d'eines que els permeten transformar la informació i mostrar-la en taulells de comandament que mitjançant taules, gràfiques i altres recursos visuals, faciliten la tasca de interpretació de la informació.
- Compliment: Els SIEM tenen la capacitat de valorar el nivell de compliment de les normatives de seguretat existent a partir de les dades recopilades.
- Retenció. Redundància i escalabilitat: Els SIEM tenen la capacitat d'emmagatzemar gran quantitat de dades i esdeveniments i preservar-los al llarg del temps. Per facilitat aquesta tasca, les solucions SIEM son redundables, per tal d'evitar la pèrdua de dades, i altament escalables de manera que poden adaptar-se les necessitats de l'entorn a cada moment.

- Anàlisi forense: Per la seva capacitat d'emmagatzemar gran quantitat de dades i preservar-les al llarg del temps, els SIEM son una eina molt útil en els anàlisis forenses. L'anàlisi forense permet analitzar les dades recollides durant un període de temps i intentar determinar la gravetat dels esdeveniments que van conduir a la violació, des del moment inicial de l'atac, fins a la sèrie d'activitats realitzades després d'entrar als sistemes de l'organització.

2.2.3 Quins beneficis aporta un SIEM ?

A partir de les característiques i funcionalitats de les solucions SIEM podem determinar els beneficis que aporta per a la seguretat de la informació d'una entitat o organització la implementació d'aquesta mena de solucions.

Entre les beneficis, destacaríem:

- Reducció del temps de resposta i millora en la eficiència de la gestió d'incidents.
- Recol·lecció centralitzada d'esdeveniments i registres de seguretat, mitjançant el processament i normalització de dades recopilades a partir de múltiples fonts i formats.
- Detecció i gestió d'anomalies i amenaces automatitzades a partir de la correlació d'esdeveniments i el seu anàlisi.
- Detecció d'amenaces a partir de la correlació d'esdeveniments amb fonts d'informació externes.
- Gestió d'alertes automatitzada.
- Protecció de les dades i registres per evitar-ne alteracions, i garantir la seva disponibilitat per a tasques d'anàlisi forense.
- Visió completa i unificada de la seguretat de la informació, alhora que ofereix als analistes de seguretat un potent instrument per descobrir, en temps real, tendències i patrons anòmals que evidenciïn amenaces de seguretat i atacs presents a la infraestructura.

2.3 Solucions SIEM a la PIME

Les solucions SIEM son complexes i requereixen una forta inversió en recursos tècnics especialitzats per a la seva configuració i manteniment continu. La majoria de les PIMES no tenen al seu abast aquest recursos, però alhora, tenen cada cop més la necessitat de protegir el seu negoci consolidant la seva estratègia de ciberseguretat mitjançant eines de vigilància de la seguretat avançades com són precisament les solucions SIEM que

aporten notables avantatges en l'àmbit de la vigilància i analítica de la seguretat.

Per superar aquestes limitacions i poder desplegar aquesta mena de solucions avançades a la seva organització, la PIME recorre habitualment a proveïdors de serveis externs (MSP) amb més experiència i solvència tècnica en l'ús d'aquesta mena de solucions.

2.4 SIEM as a Service (SIEMaaS)

L'objectiu principal del present treball és l'estudi, anàlisi i desplegament d'una solució de SIEM as a Service (SIEMaaS) adreçada a la Pime. Aquesta objectiu es fonamenta en dues realitats, d'una banda la necessitat de disposar a la PIME d'eines de vigilància de la seguretat avançades, i de l'altra, la dificultat que tenen aquestes organitzacions per disposar d'equips interns de professionals de la seguretat, el que les motiva a contractar aquest tipus de serveis a proveïdors externs.

En aquest apartat s'analitzen les característiques d'un model de servei SIEM as a Service, fent èmfasi en les seves característiques i models de desplegament.

2.4.1 Què és un SIEM as a Service ?

Les solucions SIEM aporten notables avantatges en l'àmbit de la vigilància i analítica de la seguretat a les organitzacions, però alhora son solucions complexes que requereixen d'una considerable inversió en recursos tècnics especialitzats.

La implementació d'un SIEM as a Service proporciona a les organitzacions tots els beneficis d'una solució SIEM, però sense la necessitat de destinar les altes inversions de recursos i capital necessàries per a mantenir els recursos tècnics especialitzats encarregats de la seva configuració i manteniment continu. En el model SIEM as a Service, és un proveïdor extern qui s'encarrega d'administrar la solució i qui es responsabilitza de la implementació i el manteniment de la plataforma.

Tot plegat, implica una notable reducció de costos i possibilita l'accés a un conjunt de tecnologies de la vigilància i analítica de la seguretat que per la seva complexitat i costos estan fora de l'abast de les organitzacions que no disposen d'equips de professionals de la seguretat especialitzats.

2.4.2 Quins beneficis aporta un SIEM as a Service ?

La implementació d'una solució SIEM as a Service aporta a les organitzacions tots els beneficis per a la gestió de la seguretat que ofereixen les eines SIEM, més una sèrie de beneficis addicionals que es descriuen a continuació:

- Accelera la implementació de tecnologies de vigilància de la seguretat a la organització ja que gran part de les tasques necessàries per a la implementació d'un SIEM en mans dels professionals extens que ofereixen el servei.
- No es necessari operar sistemes i solucions complexes, ni formar o contractar personal altament qualificat.
- La solució contractada evoluciona i es manté actualitzada, sense necessitat de noves inversions en personal o formació.
- Possibilita establir nivells de servei i SLAs sota contracte.
- Es redueix la complexitat de la solució i el seu desplegament
- Permet una notable reducció de costos i possibilita l'accés a tecnologies de la vigilància de la seguretat que per la seva complexitat i costos estan fora de l'abast de les organitzacions que no disposen d'equips de professionals de la seguretat qualificats.

2.4.3 Models de servei

Definim el model de servei com el model de despelgament utilitzat per implementar un servei SIEM as a Service en una organització.

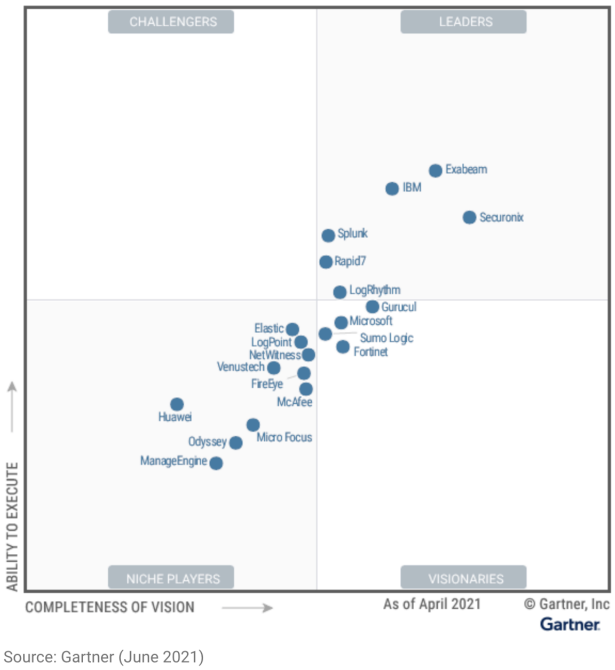
- SIEM as a Service hostatjat a la infraestructura client. Determinades organitzacions poden exigir per polítiques de seguretat internes o compliment normatiu que totes les dades recopilades al seus sistemes es trobin dins de l'organització. Aquest model preveu el desplegament de la solució SIEM as Service a la infraestructura de client sota un model de servei gestionat (*managed service)*.
- SIEM as a Service hostatjat a infraestructura del proveïdor. En aquest model la solució SIEM as Service s'allotja en una infrastructura gestionada pel proveïdor de servei, desplegant únicament a la infraestructura client els agent necessaris per a la recol·lecció i enviament de registres.

- SIEM as a Service hostatjat en infraestructura compartida. En aquest model la solució SIEM as Service s'allotja en una infraestructura compartida per varies organitzacions client i gestionada pel proveïdor de servei. A cada un dels client es despleguen els clients necessaris per a la recol·lecció i enviament de registres. Els client comparteixen la infraestructura, però únicament tenen visibilitat sobre les seves dades i en cap cas sobre les dades de la resta de clients hostatjats.

2.5 Comparativa de solucions SIEM

En aquest apartat s'estudien breument les principals solucions SIEM existents des del punt de vista de les seves funcionalitats, costos i models de desplegament. La relació de solucions no pretén ésser exhaustiva, únicament es busca il·lustrar mitjançant una petita mostra l'amplia varietat de solucions existents al mercat i les divergències existent entre unes i altres.

Per a la mostra, s'han tingut en compte els resultats del darrer informe Gartner "*Magic Quadrant Security Information and Event Management (SIEM)*"[6]



Source: Gartner (June 2021)

Figura 2 - Gartner - Magic Quadrant Security Information and Event Management (SIEM)

[6] GARTNER - *Magic Quadrant Security Information and Event Management (SIEM)* [en línia]. Web , 2021 [consulta: 18 de Març de 2022].
Disponible a: https://www.gartner.com/en/documents/4003080

2.5.1 IBM Security® QRadar® Information and Event Management

IBM Security® QRadar® Information and Event Management (SIEM) ajuda els equips de seguretat a detectar, prioritzar i respondre a les amenaces a tota l'empresa. Com a part integral de la seva estratègia de confiança zero, analitza i agrupa automàticament les dades de registre i flux de milers de dispositius, punts finals i aplicacions de tota la xarxa, i proporciona alertes úniques per agilitzar la correcció i l'anàlisi d'incidents. QRadar SIEM està disponible per a entorns en cloud i local.

Avantatges:

- Es tracta d'un SIEM líder al mercat, amb moltes funcionalitat i multitud d'opcions de desplegament i caso d'us.
- Tot i tractar-se d'un producte sofisticat és considera relativament senzill d'utilitzar.
- Excel·lent per entorns d'alta seguretat.

Inconvenients:

- La alguns serveis com la gestió d'incidències i la investigació d'esdeveniments comporten càrrecs addicionals.
- El model i la gestió de llicències resulta complex.
- La solució no disposa d'un EDR natiu.

Els client habituals de la solució IBM Security QRadar SIEM són empreses grans o mitjanes.

2.5.2 LogRhythm NextGen SIEM Platform

La plataforma LogRhythm NextGen SIEM utilitza intel·ligència artificial (IA) per correlacionar els esdeveniments de seguretat de l'entorn. La solució permet automatitzar tasques repetitives, permetent als professionals de la ciberseguretat treure el màxim profit dels seus fluxos de treball.

Avantatges:

- La solució ofereix múltiples opcions de granuralitat, permetent als usauris personalitzar les alertes i funcionalitats de la solució.
- S'actualitza constantment, incorporant constantment noves funcionalitats i alhora millorant les existents.

Inconvenients:

- L’entorn d’usuari pot ser en alguns casos d’us complex, requerint masses accions per tasques relativament senzilles.
- Algunes funcionalitats tenen costos addicionals
- El cost del producte és lleugerament superior a altres solucions similars.

2.5.3 Splunk Enterprise Security

Splunk Enterprise Security que sovint ocupa un lloc destacat a les llistes de les millors eines SIEM. Les funcions d'alertes basades en el risc redueixen les falses alarmes i ajuden la gent a determinar quins problemes val la pena tractar immediatament. La plataforma també inclou eines d'investigació integrades per accelerar les respostes dels equips de ciberseguretat.

Avantatges:

- Es un solució molt potent, que cobreix totes les funcionalitats d’una solució SIEM amb una ampli ventall de casos d’us.
- L’entorn d’usuari es altament personalitzable i la informació es mostra de manera clara i fàcilment interpretable.

Inconvenients:

- El preu és el principal inconvenient que esmenten els usuaris, ja que la despesa global depèn de la mida dels registres indexats.

La solució s’orienta a grans i mitjanes empreses, tot i que també pot implementar-se en petites empreses si es dimensiona i parametritza correctament reduint la ingesta i indexació de registres.

2.5.4 Elastic Stack: Elastic Security

Elastic Security és la solució de seguretat que ofereix Elastic per prevenir, detectar i respondre a possibles amenaces oferint una visió unificada de tota la infraestructura. Alhora, combina les funcionalitats de detecció d'amenaces d’una eina SIEM amb les capacitats de prevenció i resposta de punt final que proporciona Enpoint Security.

Avantatges:

- Elastic Security té un entorn intuïtiu i relativament senzill de gestionar.
- Kibana li proporciona una ampli ventall de possibilitats per a la gestió i visualització de la informació.
- Ofereix una distribució oberta i gratuïta que proporciona accés a una part significativa de les funcionalitat de la plataforma

- Ofereix un model de llicenciament molt flexible basat en subscripcions anuals que proporcionen que proporcionen accés a funcionalitats i característiques addicionals.
- Els seus orígens com a projecte de codi obert han propiciat que es generin al seu voltant múltiples eines i complements basats en codi obert.
- Integra en una única solució les funcionalitats d'un SIEM i les capacitats de prevenció i resposta d'un Endpoint.

Inconvenients:

- Algunes funcionalitats natives son poc madures comparades amb solucions similars.
- Alguns casos disposen de poca documentació i requereixen de molta formació i pràctica per treure'ls partit.

La flexibilitat del model de negoci de Elastic Security fan que sigui una solució molt adaptable, apta per organitzacions petites, mitjanes i grans.

2.5.5 Conclusions

Al mercat existeixen una amplia varietat de solucions SIEM a banda de les esmentades, cada una d'elles amb els seus avantatges i inconvenient, però totes tenen en comú una certa complexitat, tan en la seva implementació com en la gestió diària, que requereix de professionals de la seguretat altament qualificats.

Un altra factor comú es que acostumen a ser solucions costoses, tan a nivell de llicenciament com a nivell de recursos de còmput i emmagatzemament necessaris per la seva implementació.

Actualment, gran part d'aquestes solucions ofereixen la possibilitat de contractar el producte com a servei hostatjat en plataformes de Cloud públic o privat. Aquesta model de servei simplifica el desplegament i configuració inicials de la solució a banda que proporciona una alta escalabilitat i un model de costos flexible, alhora que previsible.

Pràcticament totes les solucions estudiades ofereixen un model de negoci per a proveïdors de serveis (Managed Service Providers), tot i que amb certes exigència en quan a nombre de sistemes gestionats i volum de facturació.

2.6 Elecció i justificació de la solució SIEM

La solució SIEM seleccionada com a base per al desenvolupament del present treball ha estat la solució basada en Elastic Stack.

S'ha optat per aquesta solució principalment per dos motius, d'una banda perquè proporciona un ampli ventall de funcionalitats en l'àmbit de la gestió de la seguretat a través de Elastic Security i Elastic Endpoint Security, i de l'altra perquè els seus orígens com a codi obert han propiciat el desenvolupament d'un ampli ecosistema de projectes i solucions de codi obert en l'àmbit de la analítica i vigilància de la seguretat En aquest sentit, destaca Wazuh, un projecte gratuït i de codi obert que proporciona una plataforma de seguretat que proporciona protecció XDR i SIEM unificada per a punts finals i càrregues de treball al núvol.

Un altre factor determinant ha estat que Elastic Stack disposa d'una llicència oberta i gratuïta, que proporciona accés a una important nombre de funcionalitats de la solució, oferint la possibilitat d'adquirir plans de subscripció flexibles que entre d'altres avantatges, proporcionen accés a funcionalitats avançades com Machine learning o gestió i enviament d'alertes. Finalment, també és remarcable l'existència d'un ampli ventall de projectes basats en codi obert desenvolupats sobre la base de Elastic Stack que possibilita que es puguin integrar per suplir part de les funcionalitats únicament disponibles mitjançant subscripció.

Al següent apartat s'estudia detalladament l'eina Elastic Stack, així com les seves funcionalitats en l'àmbit de l'analítica de la seguretat.

3. Elastic Stack

Elastic Stack és el nom donat per la companyia Elastic al conjunt de productes integrat per Elasticsearch, Kibama, Logstash i una sèrie d'agents agrupats sota la denominació Beats.

Si bé les eines que integren Elastic Stack poden utilitzar-se com a eines independents, combinades constitueixen una potent solució que permet recopilar informació, esdeveniments i registres de tota mena d'aplicacions i dispositius, per posteriorment analitzar, agregar, enriquir o consultar aquestes dades.

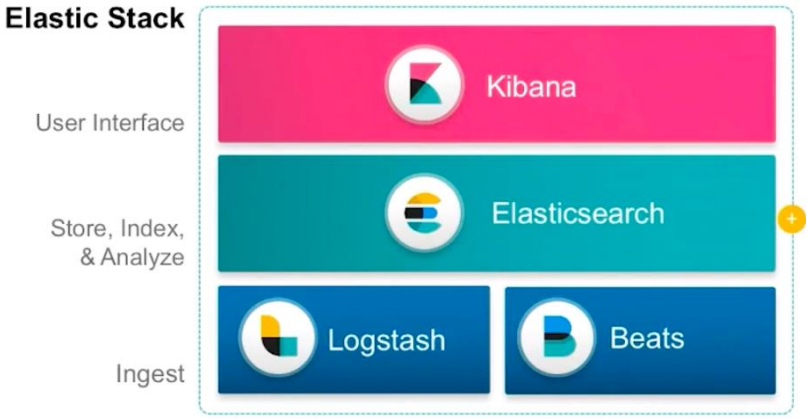


Figura 3 - Pila de serveis de Elastic Stack

3.1 Components d'Elastic Stack

Elastic Stack es la nova nomenclatura de la solució ELK, conjunt de productes integrat per Elasticsearch, Kibama, Logstash als quals se li han afegit una sèrie d'agents agrupats sota la denominació Beats, així com un ampli ventall de components addicionals. En aquest apartat es descriuen breument el components més destacats de l'Elastic Stack.

3.1.1 Elasticsearch

Elasticsearch és el component principal de Elastic stack. La companyia Elastic el defineix com un motor d'analítica i anàlisi distribuït, gratuït i obert per a tots els tipus de dades, incloent-hi dades textuals, numèriques, geoespacials, estructurades i no estructurades.

Elasticsearch és caracteritza per ser escalable i distribuït, el que permet el seu creixement horitzontal emmagatzemant grans quantitats de dades no estructurades mitjançant documents JSON. Alhora, és notablement més ràpid que altres solucions similars, oferint un excel·lent rendiment alhora de cercar i visualitzar informació en temps real.

Elasticsearch està desenvolupat a partir d'Apache Lucene i va ser presentat per primera vegada el 2010 per Elasticsearch N.V. (ara conegut com Elastic).

3.1.2 Logstash

Elastic defineix Logstash com un motor de recollida de dades de codi obert amb capacitats de canalització (*pipeline*) en temps real. Logstash pot unificar dinàmicament dades de fonts dispars i normalitzar-les cap una destinació de sortida.

Dins Elastic Stack, la funció de Logtash és la de alimentar en temps reals Elasticsearch amb dades normalitzades provinents de tota mena de fonts i disparitat de formats.

3.1.3 Kibana

Dins Elastic Stack, Kibana té dues funcions concretes, d'una banda, és la interfície gràfica que permet administrar totes les eines de la solució i de l'altra, l'eina d'usuari que permet la visualització de la informació mitjançant un ampli ventall de recursos com ara taulers de control, mapes, informes, grafs, entre d'altres.

3.1.4 Beats

Elastic defineix els Beats com a enviadors de dades (*shippers*) que s'instal·len com a agents a servidors, equips i dispositius, permetent enviar dades operatives a Elasticsearch. Els agents poden enviar les dades directament a Elasticsearch o fer-ho mitjançant Logstash, on son processades i enriquides abans de visualitzar-les a Kibana.

3.2 Casos d'us

Per la seva versatilitat, el conjunt d'eines que integren Elastic Stack proporcionen un ampli ventall de casos d'us, entre els quals destaquen:

- Cerca d'aplicacions, web i empresarial
- Recol·lecció de registres i analítiques de registres

- Mètriques d'infraestructura i monitorització de contenidors
- Monitorització de rendiment d'aplicacions
- Anàlisi i visualització de dades geoespacials
- Analítica de seguretat
- Analítica de negocis

Al present treball centrarem l'estudi de Elastic Stack en l'àmbit de l'analítica de seguretat i les seves capacitats en relació a la Informació de seguretat i gestió d'esdeveniments (SIEM - Security Information and Event Management)

3.3 Elastic Security

Elastic Security és la solució de seguretat que ofereix Elastic per prevenir, detectar i respondre a possibles amenaces oferint una visió unificada de tota la infraestructura. Alhora, combina les funcionalitats de detecció d'amenaces d'una eina SIEM amb les capacitats de prevenció i resposta de punt final que proporciona Enpoint Security.

Elastic defineix Elastic Security com XDR (detecció i resposta esteses) i l'emmarca en una nova generació de solucions SIEM enfocada a oferir seguretat intel·ligent, automatitzada i integrada en tots els dominis per ajudar els defensors a connectar alertes aparentment dispars i avançar-se als atacants.
Elastic Security ofereix, entre d'altres, els següents avantatges i funcionalitats en l'àmbit de la seguretat:

- Un potent motor de detecció que aprofita la velocitat i extensibilitat d'Elasticsearch, per identificar atacs i configuracions incorrectes del sistema
- Un espai de treball per al triatge i la investigació d'esdeveniments.
- Un entorn de visualització interactiu basat en Kibana que permet investigar les relacions de processos.
- Gestió de casos integrada amb accions automatitzades.
- Prevenció contra codi maliciós (malware), ransomware i phishing mitjançant Endpoint Security

3.4 Models de desplegament i llicenciament

Un dels aspectes més rellevants alhora de valorar l'adquisició d'una solució de software qualsevol són els models de desplegament que ofereix i el seu llicenciament.

Actualment Elastic Stack disposa d'una distribució autogestionada, oberta i gratuïta que proporciona accés a una part significativa de les funcionalitat de la plataforma. Alhora ofereix la possibilitat d'adquirir subscripcions comercials que proporcionen accés a funcionalitats i característiques addicionals.

A banda, Elastic proporciona Elastic Stack com a servei gestionat oferint la possibilitat de desplegar la solució gestionada sobre Amazon Web Services, Microsoft Azure o Google Cloud. Actualment el servei gestionat s'ofereix en quatre possibles models de subscripció, cada un d'ells proporciona accés a funcionalitats i característiques addicionals.

3.4.1 Restriccions de llicenciament en el model autogestionat

Històricament s'ha considerat Elasticsearch una solució de codi obert, doncs va ésser originàriament. ElasticSearch va ser distribuït per primer cop l'any 2010 per Shay Banon sota una llicència estàndard d'Apache 2.0[7]. Des d'aquella primera distribució la plataforma ha evolucionat notablement, incorporant constantment noves eines i funcionalitats, fins a convertir-se el conjunt de productes que coneixem com Elastic Stack. Part d'aquestes noves funcionalitats es van continuar distribuint sota llicència Apache 2, mentre per d'altres es va optar per utilitzar una llicència propietària més restrictiva anomenada Elastic License.

A principis de l'any 2021, Elastic, la companyia comercial darrera Elastic Stack anuncia un canvi estratègic en el seu model de llicenciament a fi de protegir el seu model de negoci[8]. Totes les noves versions dels seus productes passaran a publicar-se sota una llicència dual, integrada per una llicència SSPL 1.0[9] i una nova llicència denominada Elastic 2.0 (ELv2)[10], que com tret principal limita el desplegament de la solució a tercers com a servei allotjat o gestionat.

Per tant, actualment Elastic Stack, així com els components que la integren, no poden considerar-se solucions de codi obert. Elastic continua oferint de

[7] APACHE - *APACHE LICENSE, VERSION 2.0* [en línia]. Web , 2018 [consulta: 21 de Març de 2022]. Disponible a: https://www.apache.org/licenses/LICENSE-2.0

[8] ELASTIC - *Preguntas frecuentes sobre el cambio de licencia 2021* [en línia]. Web , 2018 [consulta: 25 de Març de 2022]. Disponible a: https://www.elastic.co/es/pricing/faq/licensing

[9] SPDX. *Server Side Public License, v1* [en línia]. Web [consulta: 25 de Març de 2022]. Disponible a: https://spdx.org/licenses/SSPL-1.0.html

[10] ELASTIC - Elastic License 2.0 (ELv2) [en línia]. Web 2022 [consulta: 10 de Març de 2022]. Disponible a: https://www.elastic.co/es/licensing/elastic-license

manera oberta i gratuïta la seva solució, però sota les restriccions imposades per la llicència propietària Elastic 2.0 (ELv2).

La llicència Elastic 2.0 (ELv2) limita el desplegament de la solució a tercers com a servei allotjat o gestionat, indicant que no es podran proporcionar aquest tipus de serveis, quan el servei ofereix als usuaris accés a qualsevol conjunt substancial de les característiques o funcionalitats del programari:

> *"You may not provide the software to third parties as a hosted or managed service, where the service provides users with access to any substantial set of the features or functionality of the software."*

A efectes del present treball les restriccions de la llicència Elastic 2.0 (ELv2) limiten model de serveis de la solució SIEMaaS a implementar, doncs únicament és podrà oferir i desplegar a tercers com a servei allotjat o gestionat, sempre i quan, no se'ls proporcioni accés substancial a les característiques o funcionalitats del programari.

4. ELK i l'ecosistema Open Source

Als objectius del treball es definia una segona fase de integració i desenvolupament adreçada a desplegar un model funcional de SIEMaaS en base als requisits específics de la PIME.

Donats els costos de les subscripcions comercials de Elastic Stack i el fet que part de les funcionalitats que aquestes proporcionen es puguin reemplaçar mitjançant eines i projectes basats en codi obert s'ha optat per implementar un model basat en Elastic Stack autogestionat complementat amb eines de codi obert o Open Souce.

El model seleccionat està integrat sobre la base de la solució Elastic Stack, en la seva versió autogestionada, gratuïta i oberta, sense descartar l'adquisició puntual de llicències comercials en aquells entorns en els quals es desitgi disposar de les funcionalitats addicionals que les llicències comercials proporcionen. Sobre aquesta base, es proposar integrar la solució EDR de Wazuh que proporciona funcionalitats per a la monitorització de la seguretat com son la detecció d'amenaces, el control de la integritat, la resposta a incidents i el compliment. El model es completa amb la implementació de la plataforma de resposta a incidents de seguretat (SIRP) TheHive.

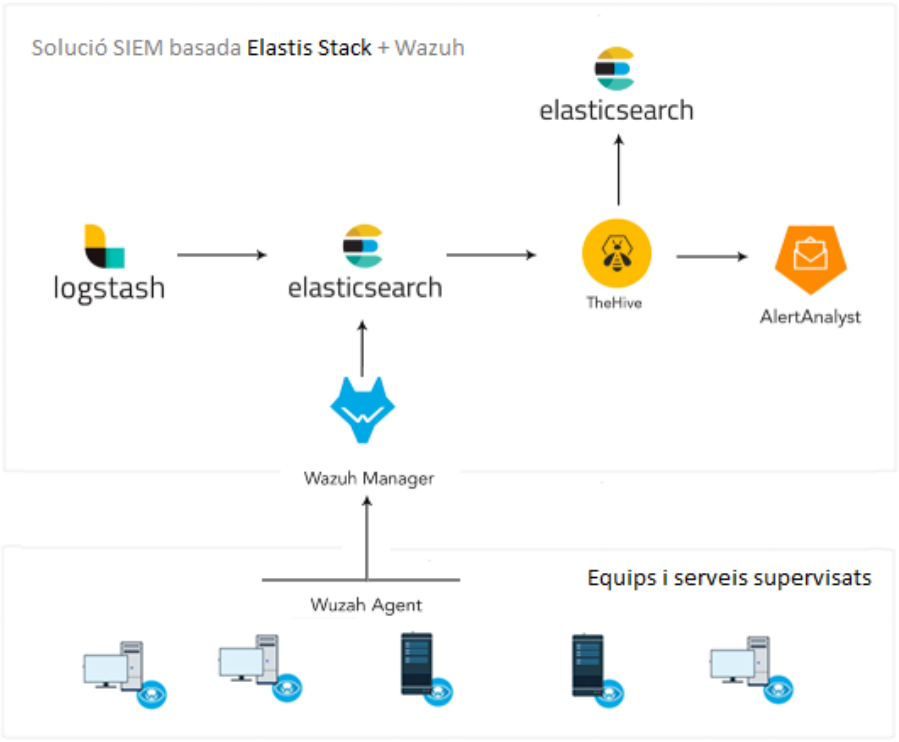


Figura 4 - Plataforma SIEM basada en Elastic Stack + Wazuh

4.1 Wazuh

Wazuh és un projecte gratuït i de codi obert que proporciona una plataforma de seguretat que proporciona protecció XDR i SIEM unificada per a punts finals i càrregues de treball al núvol. La plataforma integra serveis relacionats amb la seguretat com ara detecció d'amenaces, monitorització d'integritat, resposta d'incidents i compliment o detecció d'intrusions. La solució permet protegir les càrregues de treball en entorns locals, virtualitzats, en contenidors i basats en núvol.

Wazuh s'integra de dos components: un agent de seguretat modular i multiplataforma desplegat als sistemes supervisats, i un servidor de gestió que recull i analitza les dades recopilades pels agents. A banda, Wazuh integra amb Elastic Stack, proporcionant als usuaris un potent motor de cerca i una eina de visualització de dades i alertes de seguretat.

4.1.1 Serveis i funcionalitats de Wazuh

La solució de Wazuh proporciona una amplia varietat de serveis i funcionalitats en l'àmbit de la monitorització de la seguretat. En aquest apartat es descriuen breument els servei i funcionalitat més rellevants per a la execució del present treball:

- Anàlisi de seguretat: La funcionalitat principal de Wazuh és la de recol·lectar, agregar, indexar i analitzar informació de seguretat, ajudant les organitzacions a detectar intrusos, amenaces i anomalies.
- Detecció d'intrusos: els agents de Wazuh permeten monitoritzar els sistemes cercant malware, rootkits i anomalies sospitoses.
- Anàlisi d'Informació de Logs: Els agents de Wazuh recullen els registres del sistema operatiu i de les aplicacions, i els envien de manera segura a al servidors per ser emmagatzemats i analitzats en base a unes pautes establertes.
- Monitorització d'integritat d'arxius: Wazuh permet monitoritzar el sistema de fitxers identificar canvis en el contingut, permisos, propietat, etc ..
- Detecció de vulnerabilitats: La informació enviada pels agents de Wazuh cap al servidor és correlacionada amb les bases de dades de vulnerabilitats CVE (Common Vulnerabilities and Exposure), per tal d'identificar serveis i programari vulnerable.
- Resposta a incidents: Wazuh proporciona funcionalitats de resposta a incidents en forma de respostes actives que permeten prendre contramesures enfront les amenaces existents.
- Compliment Normatiu: Wazuh proveeix alguns dels controls de seguretat necessaris per complir amb els estàndards i regulacions de la indústria.

4.1.2 Arquitectura general de Wazuh

La arquitectura de Wazuh es basa en un agent modular i multiplataforma, que s'executa sobre els equips i serveis a supervisar, i en tres components centrals: el servidor o manager Wazuh, l'indexador i el tauler de control de Wazuh.

- El servidor de Wazuh analitza les dades rebudes dels agents i les processa mitjançant descodificadors i regles per buscar indicadors de compromís (IOC) coneguts. Alhora, el servidor de Wazuh també permet la gestió els agents, configurant-los i actualitzant-los de forma remota quan sigui necessari.
- L'indexador Wazuh és un motor d'anàlisi i cerca de text altament escalable encarregat de indexar i emmagatzemar les alertes generades pel servidor Wazuh.
- El tauler de control de Wazuh és la interfície d'usuari web per a la visualització i l'anàlisi de dades. Inclou quadres de comandament detallats per a cada una de les funcionalitats que ofereix la solució, inclosa la gestió de la pròpia plataforma.
- Els agents de Wazuh s'executen als equips i sistemes que es desitja supervisar, recollint i enviant contínuament dades de seguretat al servidor central a través de comunicacions autenticades i xifrades.

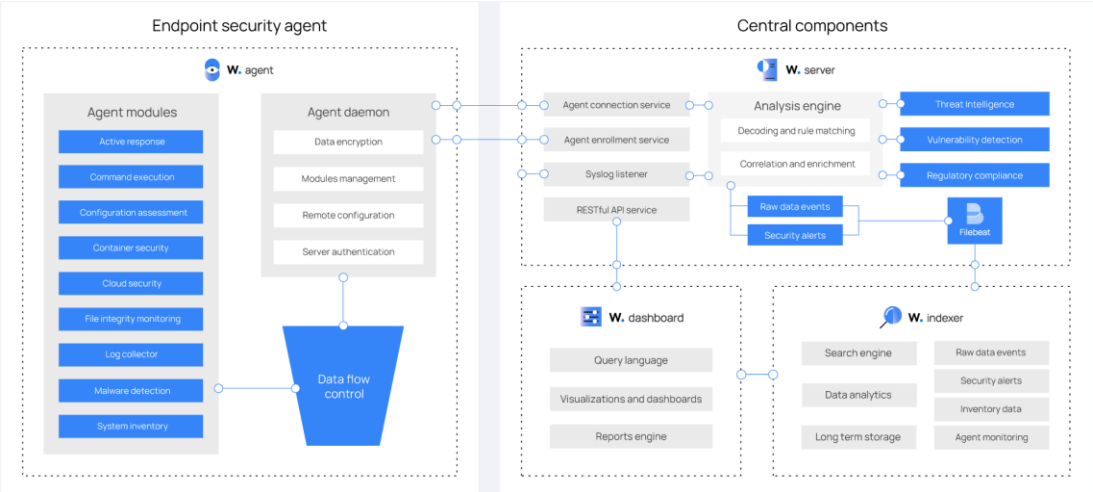


Figura 5 - Arquitectura general de Wazuh

Actualment Wazuh pot desplegar-se sobre la base de OpenSearch, Splunk, o Elastic Stack. Per al desenvolupament d'aquest treball s'ha optat per desplegar la plataforma sobre la base de Elastic Stack. Tot i això, no es descarta que en determinats escenaris on no es contempli l'ús de les característiques de seguretat avançades que proporciona Elastic Stack, es pugui desplegar sobre la base de OpenSeach.

El diagrama següent representa un model d'arquitectura escalable de Wazuh desplegada sobre la base de Elastic Stack. Al diagrama ho podem observar els diferents components de la solució i com, tan el servidor de Wazuh com els indexadors es poden configurar com a clústers, dotant d'equilibri de càrrega i alta disponibilitat a la plataforma.

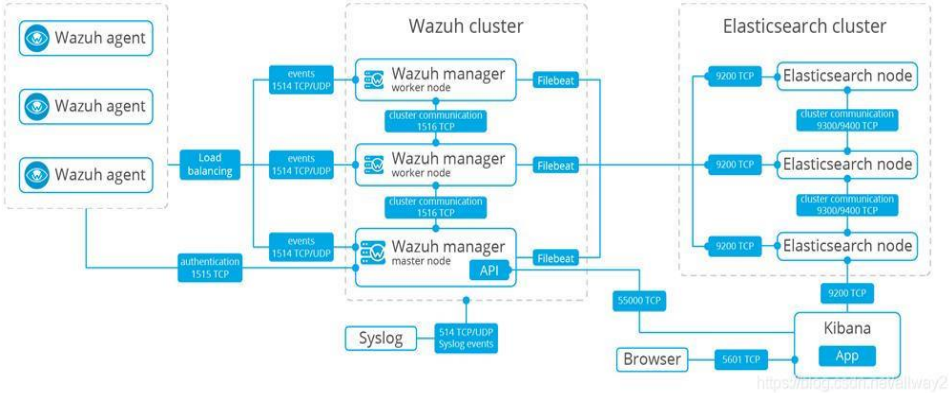


Figura 6 - Arquitectura de Wazuh en entorns clusteritzats

Tot plegat fa que l'arquitectura de Wazuh sigui extraordinàriament versàtil, permetent el seu desplegament des de entorns petits intregrats per unes dotzenes d'agents finals, fins a escalar a entorns amb milers d'agents desplegats.

4.1.3 Agents i integracions

L'arquitectura Wazuh es basa en agents multiplataforma, que s'executen als equips i sistemes que es desitja supervisar, i que recullen i envien contínuament dades de seguretat a un servidor central a través de comunicacions autenticades i xifrades.

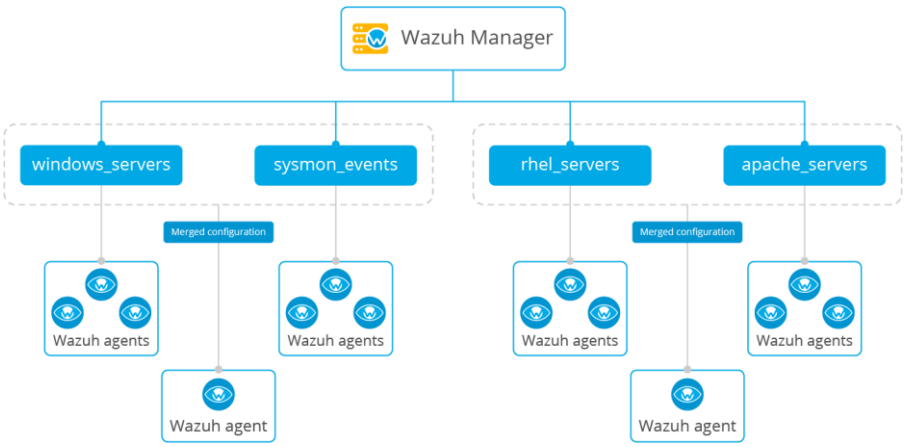


Figura 7- Distribució dels agents de Wazuh

Els agents es basen en una arquitectura modular basada en múltiples components que proporcionen funcionalitats clau per a la gestió i supervisió de la seguretat dels equips supervisats. A continuació es descriuen breument les principals funcionalitats que proporcionen els agents de Wazuh son:

- Recol·lecció de registres i esdeveniments de seguretat: Aquest component de l'agent pot llegir fitxers de registre i esdeveniments de Windows, recopilant registres d'aplicacions i sistemes operatius.
- Inventari de sistema: Aquest mòdul executa periòdicament exploracions del sistema, recopilant dades d'inventari com ara la versió del sistema operatiu, interfícies de xarxa, processos en execució, aplicacions instal·lades, etc ...
- Avaluacions de la configuració de seguretat (SCA): Aquest component proporciona una avaluació contínua de la configuració de seguretat dels sistemes supervisats en base a les recomanacions de seguretat definides pel Center of Internet Security (CIS). D'altra banda, els agent també poden executat avaluacions de seguretat personalitzats.
- Detecció de programari maliciós: Aquest component pot detectar la presencia d'activitat anòmala que pugui indicar la presencia de rootkits als sistemes supervisats
- Resposta activa a amenaces de seguretat: Aquest mòdul té la capacitat d'executar accions automàtiques quan es detecten amenaces al equips supervisats, activant respostes per bloquejar una connexió de xarxa, aturar un procés en execució o suprimir un fitxer maliciós.
- Supervisió de la integritat dels fitxers (FIM): Aquest mòdul supervisa el sistema de fitxers i informa quan es creen, s'eliminen o es modifiquen fitxers.
- Seguretat al núvol: Aquest components permet la integració amb les API de diferents proveïdors de serveis al núvol com ara Amazon AWS, Microsoft Azure o Google GCP, recollint esdeveniments de seguretat i dades del registre i detectant possibles canvis i anomalies a la infraestructura del núvol.

Destacar que l'arquitectura modular dels agents permet personalitzar i adaptar les funcionalitats per a cada un dels agents desplegats, habilitant o deshabilitant els mòduls en funció dels requisits de cada sistema supervisat.

Els agents de Wazuh s'instal·len en equips i sistemes finals com ara ordinadors portàtils, ordinadors de sobretaula, servidors, instàncies al núvol o màquines virtuals, proporcionant capacitats de prevenció, detecció i resposta d'amenaces. Els agents estan disponibles per a múltiples plataformes i sistemes operatius, com ara Linux, Windows, macOS, Solaris, AIX i HP-UX.

En entorn petits el desplegament dels agents es pot realitzar de manera manual, als annexos del present treball s'hi recullen alguns exemples. En entorn grans, amb centenars d'equips a supervisar, es pot recórrer al desplegament dels agents mitjançant diferents eines d'automatització com ara Puppet, Chef, SCCM, or Ansible.

D'altra banda, ens entorns basats en Active Directory, l'ús de les polítiques de grup (GPO) permet el desplegament i configuració dels agents al sistemes Windows supervisats.

Finalment, els dispositius sense agent com ara tallafocs, commutadors, encaminadors i punts d'accés poden enviar al servidor esdeveniments de seguretat de manera activa mitjançant Syslog, SSH o mitjançant la seva API. El servidor central descodifica i analitza la informació entrant i passa els resultats a l'indexador Wazuh per a la indexació i l'emmagatzematge.

4.2 TheHive

TheHive és una plataforma de resposta a incidents de seguretat, gratuïta i basada en codi obert, dissenyada per facilitar la tasca dels equips de SOC, CSIRT, CERT i en general a qualsevol professional de la seguretat encarregat de la gestió d'incidents de seguretat.

TheHive és altament automatitzable i està especialment dissenyada per integrar-se amb altres tecnologies, com ara els projectes Cortex o MISP, per tal de millorar la seva eficàcia i funcionalitat.

4.3 Idoneïtat d'un SIEMaaS basat en Open Source

Definim el model de SIEMaaS basat en Open Source com la solució SIEM integrada per la base oberta i gratuïta de Elastic Stack i la plataforma de monitorització i gestió de la seguretat Wazuh.

Com hem vist als punts anteriors la plataforma basada en la combinació de solucions Elastic Stack + Wazuh proporciona totes les funcionalitats i serveis bàsics que integra un SIEM sense els punt de partida dels costos de llicenciament habituals en aquest tipus de solucions. A banda, la seva arquitectura és extraordinàriament versàtil i adaptable a qualsevol model de servei.

A continuació es descriuen breument les principals característiques i funcionalitats que fan de la plataforma Elastic Stack + Wazuh una excel·lent

opció per a la implementació d'un servei de SIEM as a Service orientat a la PIME.

- La plataforma integrada per Elastic Stack + Wazuh proporciona un ampli ventall de funcionalitats en l'àmbit de la seguretat. D'una banda la plataforma proporciona les funcionalitats principals d'una solució SIEM (agregació de dades, correlació d'esdeveniments, gestió d'alertes, retenció i escalabilitat...), de l'altra, els agents de Wazuh i Elastic Security proporcionen a la plataforma les funcionalitats addicionals dels sistemes EDR/XDR.

- L'arquitectura de Wazuh és extraordinàriament versàtil, permetent el seu desplegament tan en entorns petits integrats per unes dotzenes d'agents finals, com escalar la solució per donar servei a entorns amb milers d'agents desplegats. D'altra banda, la flexibilitat de la solució SIEM basada en Elastic Stack + Wazuh proporciona un ampli ventall d'opcions per al seu desplegament, oferint la possibilitat implementar diferents models de servei en funció dels requisits de cada infraestructura.

- L'arquitectura modular dels agents de Wazuh permet personalitzar i adaptar les funcionalitats per a cada un dels agents desplegats, habilitant o deshabilitant els mòduls en funció dels requisits de cada sistema supervisat.

- A banda dels agents i la possibilitat de recopilar registres directament dels dispositius mitjançant syslog, Elastic Stack i Wazuh disposen d'un bon nombre Integracions amb serveis de tercers, com ara plataformes de proveïdors de serveis al núvol, Osquery, detecció de vulnerabilitats, etc ...

- Un dels aspectes més rellevant alhora de implementar un SIEM és el seu cost, tan en relació al llicenciament de la solució, com en relació als professionals qualificats necessaris per al seu desplegament i gestió. En molts casos els elevats costos de llicenciament situen les solucions SIEM existents al mercat fora de l'abast de la majoria de pimes. En aquest sentit, la plataforma integrada per Elastic Stack + Wazuh parteix d'un model de llicenciament gratuït, al qual es poden afegir les subscripcions de pagament que ofereix Elastic Stack per dotar-lo de funcionalitats addicionals, com Machine learning, detecció de malware/ransomware mitjançant els agent finals, etc ...

4.4 Models de servei d'un SIEMaaS basat en Open Source

Definim el model de servei com el model utilitzat per implementar un servei SIEM as a Service en una organització. En aquest sentit, la flexibilitat de la solució SIEM basada en Elastic Stack + Wazuh proporciona un ampli ventall d'opcions per al seu desplegament, oferint la possibilitat implementar diferents models de servei en funció dels requisits de cada infraestructura.

S'han definit tres models de servei que encaixen perfectament amb les característiques i funcionalitats de la solució:

- SIEMaaS On-Premises (SIEM as a Service hostatjat a la infraestructura client). Aquest model preveu el desplegament de la solució SIEM as Service a la infraestructura de client sota un model de servei gestionat (*managed service)*. Per aquest model es preveu la instal·lació de tots els components de la solució en un únic equip, amb capacitat per donar servei a un màxim de 80-100 equips client.

- SIEMaaS Cloud (SIEM as a Service hostatjat en infraestructura compartida). En aquest model la solució SIEM as Service s'allotja en una infraestructura gestionada pel proveïdor de servei, desplegant únicament a la infraestructura client els agent necessaris per a la recol·lecció i enviament de registres. La infraestructura es compartida per varies organitzacions client i gestionada pel proveïdor de servei. Els client comparteixen la infraestructura, però únicament tenen visibilitat sobre les seves dades i en cap cas sobre les dades de la resta de clients hostatjats. Per aquest model es preveu la instal·lació en clúster dels components de la solució, escalant en recursos segons demanda.

- SIEMaaS Híbrid (SIEM as a Service hostatjat a infraestructura del proveïdor). En aquest model la solució SIEM as Service s'allotja en una infraestructura gestionada pel proveïdor de servei, desplegant únicament a la infraestructura client els agent necessaris per a la recol·lecció i enviament de registres. Per a desplegaments amb pocs equips client es contempla la instal·lació de tots els components en una única màquina virtual, mentre per desplegaments més grans es contempla el desplegament de clústers dedicats.

5. Desplegament d'un SIEMaaS

En aquest apartat es descriu el disseny i desplegament d'un model funcional de la solució SIEM seleccionada, així com de l'ecosistema d'eines i serveis complementaris necessaris per a la paquetització de la solució com SIEM as a Service. Per tal de validar que el model desplegat s'ajusta als requisits funcionals definits a la fase d'investigació, s'integrarà la solució desenvolupada en un entorn de laboratori on s'hi desenvoluparan una sèrie de proves de concepte.

5.1 Estructura de la solució desplegada

A partir de la comparativa de diferents solucions SIEM, tan comercials com *open source*, s'ha optat per desplegar una prova de concepte de SIEMaaS sobre la base, oberta i gratuïta, de Elastic Stack i la plataforma de codi obert Wazuh, proporcionant protecció XDR i SIEM unificada per a punts finals i càrregues de treball al núvol.

Figura 8 - Arquitectura general de la solució desplegada

Tot i que Wazuh permet el seu desplegament sobre la base de OpenSearch, s'ha optat per implementar-lo sobre Elastic Stack ja que aquest disposa de les funcionalitats i integracions addicionals de Elastic Security. L'estudi detallat de les funcionalitats i integracions de Elastic Security i els beneficis que pot aportar a la solució dissenyada queden fora de l'abast del present treball i s'abordaran en treballs futurs.

Com s'ha vist anteriorment, la flexibilitat de la solució SIEM basada en Elastic Stack + Wazuh proporciona un ampli ventall d'opcions per al seu desplegament, oferint la possibilitat implementar diferents models de servei en funció dels requisits de cada infraestructura. En aquest sentit, l'estrucutura modular dels agents permet adaptar-los als requisits de cada un dels sistemes auditats, i per tant a les característiques i requisits específics de cada PIME.

5.2 Instal·lació la solució

Per tal de avaluar adequadament el model seleccionat s'ha desplegat una prova de concepte de la solució exposada al punt anterior en un entorn de laboratori. El model de servei implementat ha estat un SIEMaaS *Híbrid*, amb una instancia dedicada per un hipotètic client amb múltiples seus. Tots els components de la solució SIEMaaS s'ha desplegat sobre una única màquina virtual ubicada a la Azure. Per la part client, s'ha simulat una infraestructura de client distribuïda en varies seus, integrada per un ventall de servidors i estacions de treball equipats amb sistemes Windows o Linux segons el cas.

Cada un dels components que integren la solució SIEMaaS s'ha instal·lat seguint la respectiva documentació del producte. Als annexos del treball s'hi recull una completa guia de instal·lació de la solució dissenyada, elaborada a partir d'aquestes documentacions.

5.3 Desplegament d'agents

Com hem vist anteriorment, l'arquitectura Wazuh es basa principalment en l'activitat dels agents, que s'executen als equips i sistemes que es desitja supervisar, recollint i enviant contínuament dades de seguretat al servidor central.

Per aquells dispositius client que no sigui possible desplegar el corresponent agent, com ara tallafocs, commutadors, encaminadors, punts d'accés i d'altres, es contempla l'ús dels mecanismes alternatius que proporciona la plataforma Wazuh com ara l'esdeveniment de registres de seguretat de manera activa mitjançant Syslog, SSH o mitjançant la seva API.

Per tal d'avaluar adequadament el model de SIEM as a Service dissenyat, s'ha simulat una infraestructura de client distribuïda en varies seus, integrada per un ventall de servidors i estacions de treball equipats amb sistemes Windows o Linux segons el cas. Sobre cada un d'aquest sistemes a supervisar s'hi han desplegat els corresponents agents de Wazuh, que connecten al servidor central ubicat a Azure. La comunicació entre els agents i el servidor ubicat al núvol es realitza mitjançant una VPN site-to-site sobre la qual s'ha habilitat únicament el tràfic de xarxa imprescindible per la comunicació i gestió dels agents amb la infraestructura de Wazuh.

A l'annex del present document s'hi recull una guia per la instal·lació manual dels agents en sistemes Windows i Linux.

5.4 Ús de la solució

Un cop desplegada la solució al nostre sistema podem realitzar la gestió i seguiment de la plataforma Elastic Stack amb la integració de Wazuh a través del seu taulell de control.

El tauler de control de Wazuh és una interfície d'usuari web flexible i intuïtiva basada en Kibana que permet la gestió de la plataforma, i alhora, extreure, analitzar i visualitzar esdeveniments de seguretat i dades d'alertes.

Accedim a la plataforma a través de la seva URL e introduïm les credencials d'accés. Wazuh incorpora funcions per al control d'accés basat en rols (RBAC) així com integració amb inici de sessió únic (SSO).

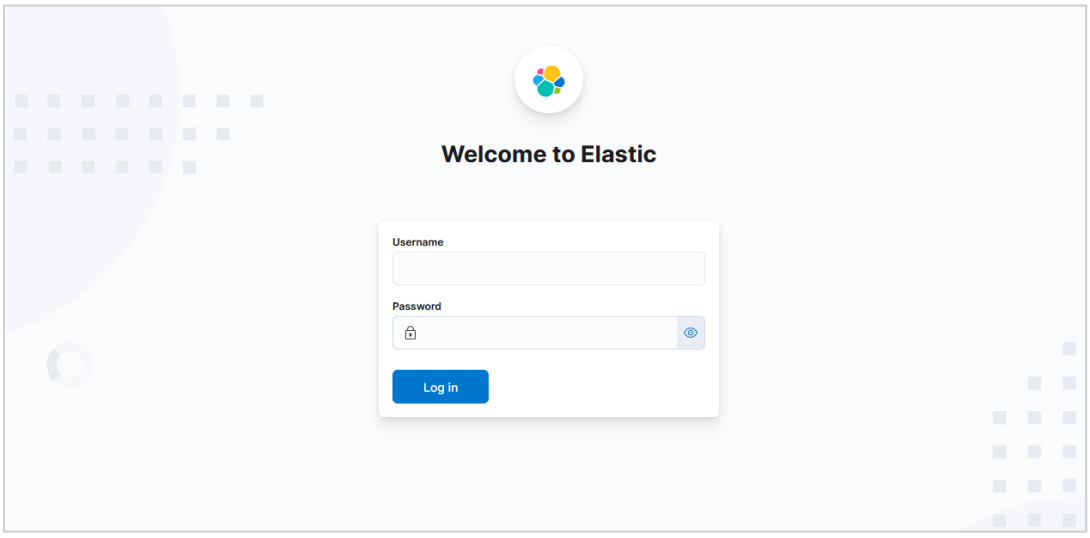


Figura 9 - Finestra d'identificació de Elastic Stack

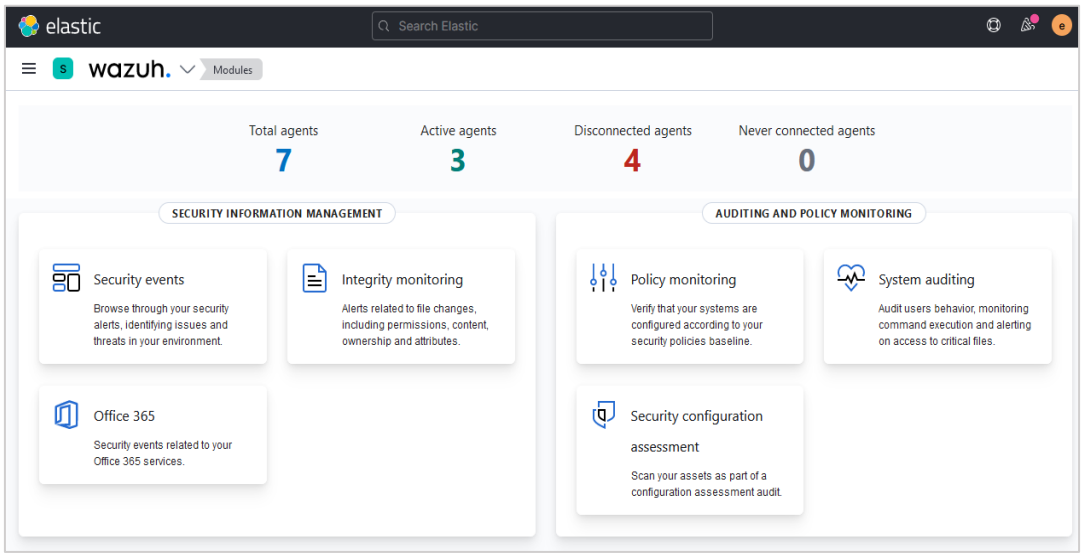


Figura 10 - Taulell de control de Wazuh

El mòdul de Wahuh permet accedir de forma àgil i ràpida a una sèrie de vistes preconfigurades que proporcionen informació sobre les diferent funcionalitats habilitades a la solució. Les vistes s'agrupen en quatre categories principals:

- Security information management
- Threat detection and response
- Auditing and policy monitoring
- Regulatory compliance

Les diferents vistes ajuden als usuaris a navegar pels diferents tipus de dades recollides pels agents de Wazuh, així com a visualitzar les alertes de seguretat generades pel servidor de Wazuh. Els usuaris també poden generar informes i crear visualitzacions i taulers personalitzats.

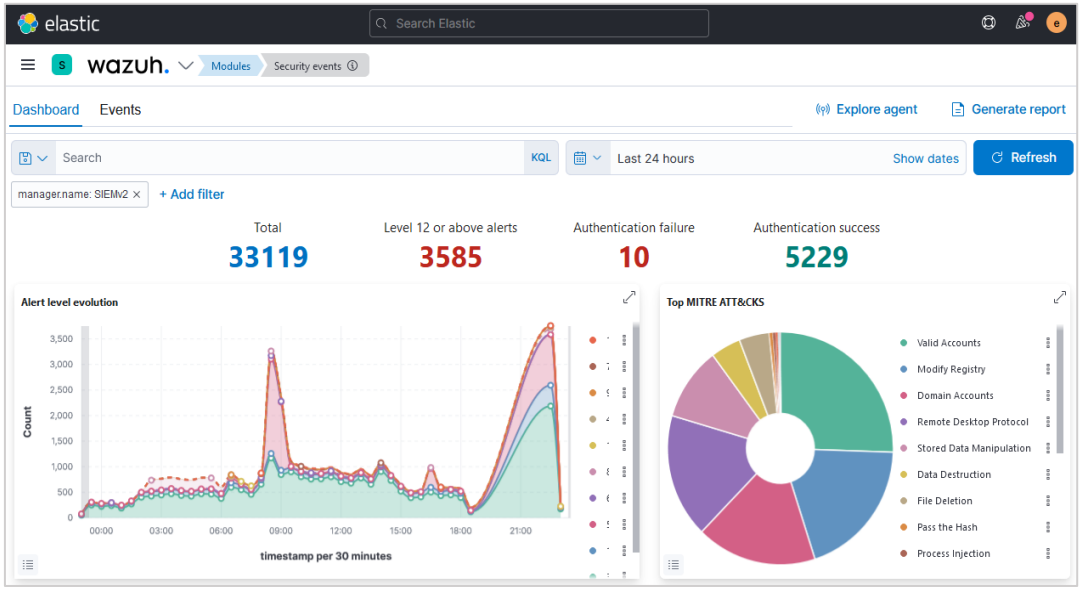


Figura 11- Vista general dels esdeveniments de seguretat a Wazuh

Una vegada desplegats els agents de Wazuh, aquest comencen a recopilar esdeveniments al equips client transferir-los al servidor de Wazuh per a la seva ingesta.

Els agents de Wazuh tenen una arquitectura modular. Cada component s'encarrega de les seves pròpies tasques, inclosa la supervisió del sistema de fitxers, la lectura de missatges de registre, la recollida de dades d'inventari, l'escaneig de la configuració del sistema i la recerca de programari maliciós. Els mòduls de l'agent es poden gestionar mitjançant els paràmetres de configuració, adaptant la solució a cada ús particular.

Wazuh proporciona una vista predeterminada per a gestió dels agents desplegats. La vista proporciona una visió tàctica dels agent, proporcionant dades rellevants sobre el seu estat, darrera connexió, sistema base, versió de l'agent...

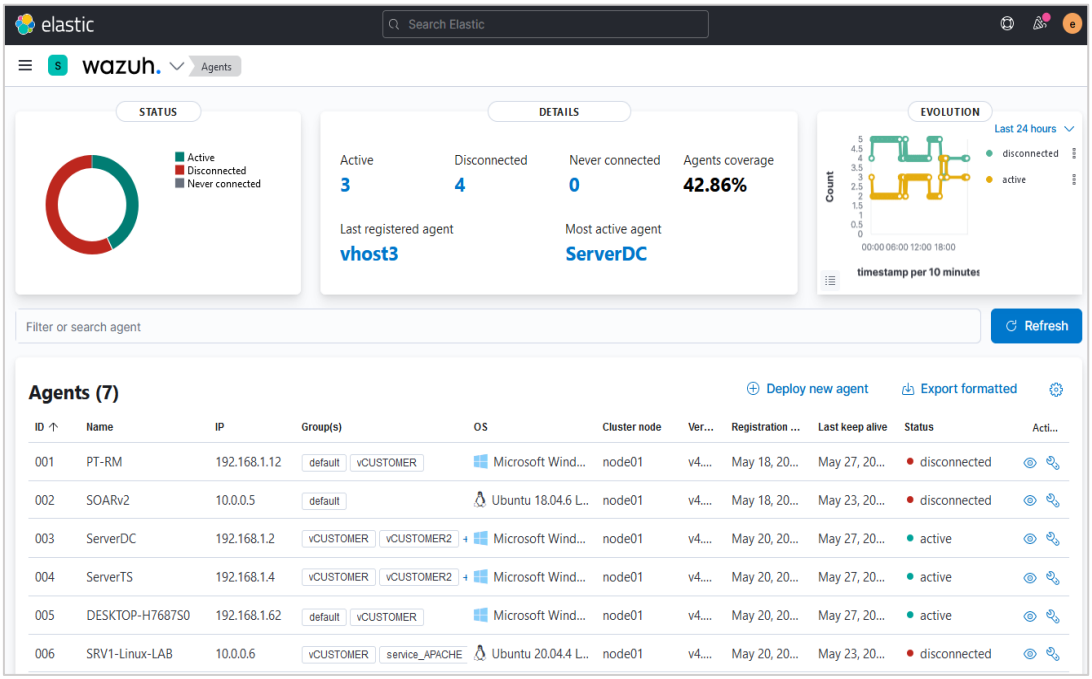


Figura 12 - Vista general dels agents a Wazuh

El tauler de control de Wazuh permet als usuaris gestionar la configuració dels agents i controlar-ne el seu estat. Com a exemple, per a cada punt final supervisat, els usuaris poden definir quins mòduls d'agent s'habilitaran, quins fitxers de registre es llegiran, quins fitxers es controlaran per als canvis d'integritat o quines comprovacions de configuració es realitzaran.

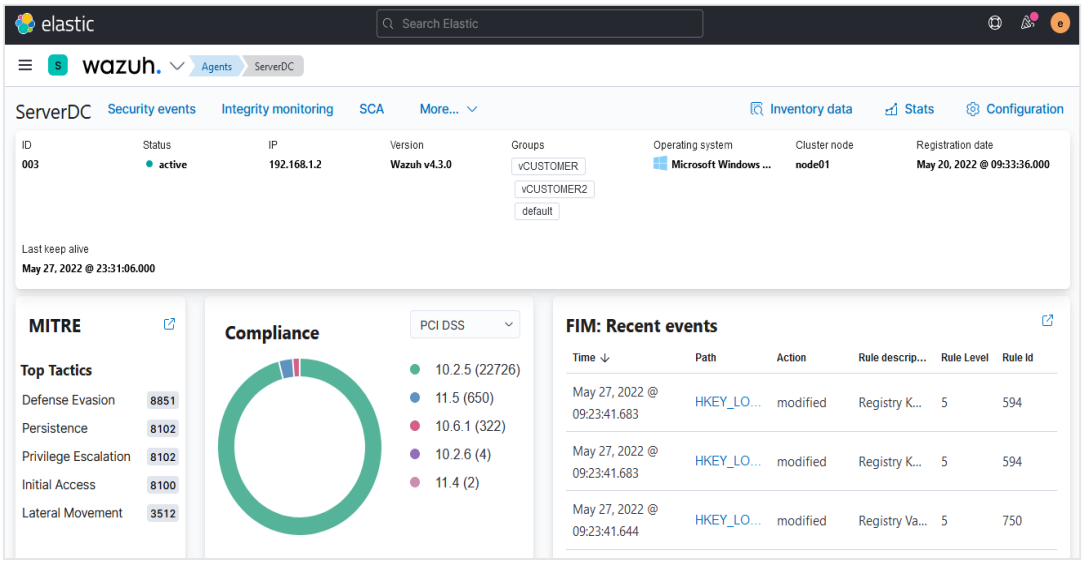


Figura 13 - Vista detallada d'un agent a Wazuh

La interfície de Wazuh basada en Kibana proporciona una vista detallada dels esdeveniments, permet fer consultes molt detallades sobre les dades en un llenguatge similar a SQL, denominat KQL.

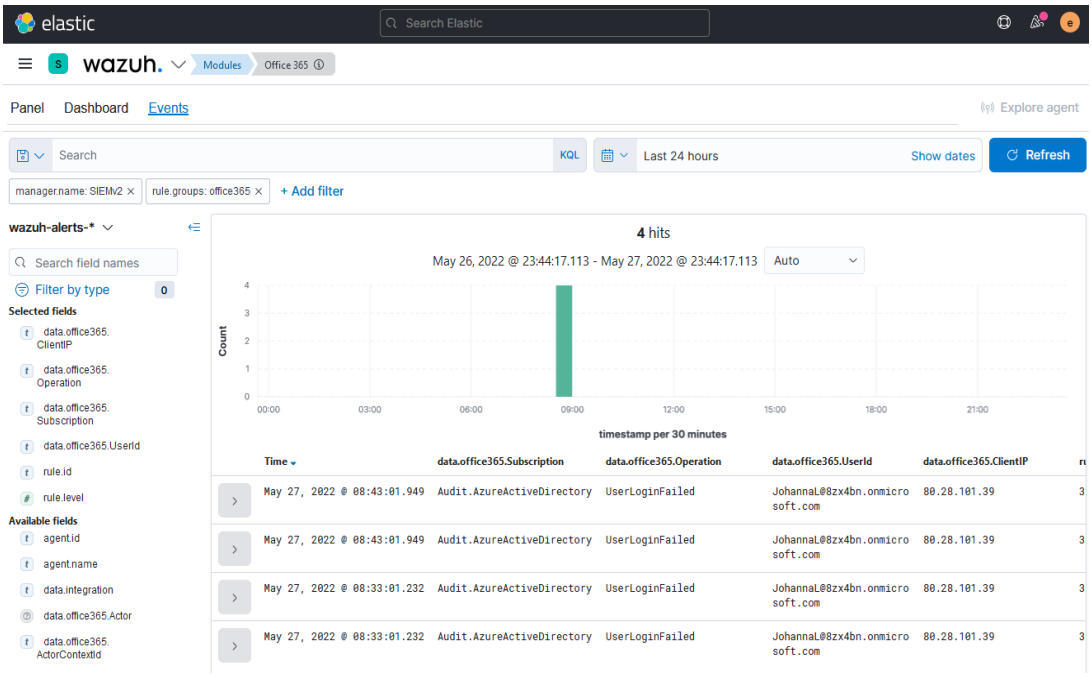


Figura 14 - Vista d'una taula d'esdeveniments a Wazuh

Alhora, la interfície de Kibana permet la creació de taulells personalitzats basats en aquestes consultes. Kibana disposa d'un ampli ventat de recursos gràfics per a la visualització de dades i la creació de taulells de control.

El taulell de control de Wazuh també proporciona una interfície gràfica per a la supervisió i edició de les regles existents, així com per la creació de noves.

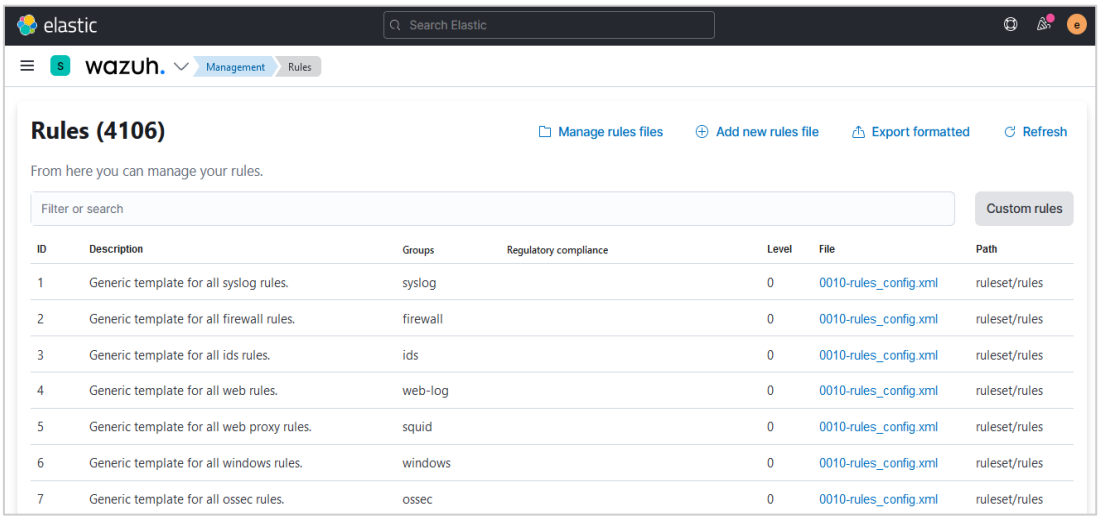


Figura 15 - Vista del editor de regles a Wazuh

5.5 Validació de la solució. Proof on Concept (PoC)

En aquest apartat es descriuen una sèrie de proves de concepte realitzades sobre la solució SIEM as a Service dissenyada per tal validar que el model desplegat s'ajusta als requisits funcionals definits a la fase d'investigació, a fi de determinar-ne la viabilitat de la solució i verificar que funcionarà tal com s'ha previst.

Per tal de dur a terme les proves de concepte s'ha desplegat la solució en un entorn de laboratori. El model de servei implementat a l'entorn de laboratori ha estat un SIEMaaS Híbrid, amb una instancia dedicada per un hipotètic client amb múltiples seus. Tots els components de la solució SIEMaaS s'ha desplegat sobre una única màquina virtual ubicada a la Azure. Per la part client, s'ha simulat una infraestructura distribuïda en varies seus, integrada per un ventall de servidors i estacions de treball equipats amb sistemes Windows o Linux, sobre els quals s'hi ha desplegat els corresponents agents de Wazuh.

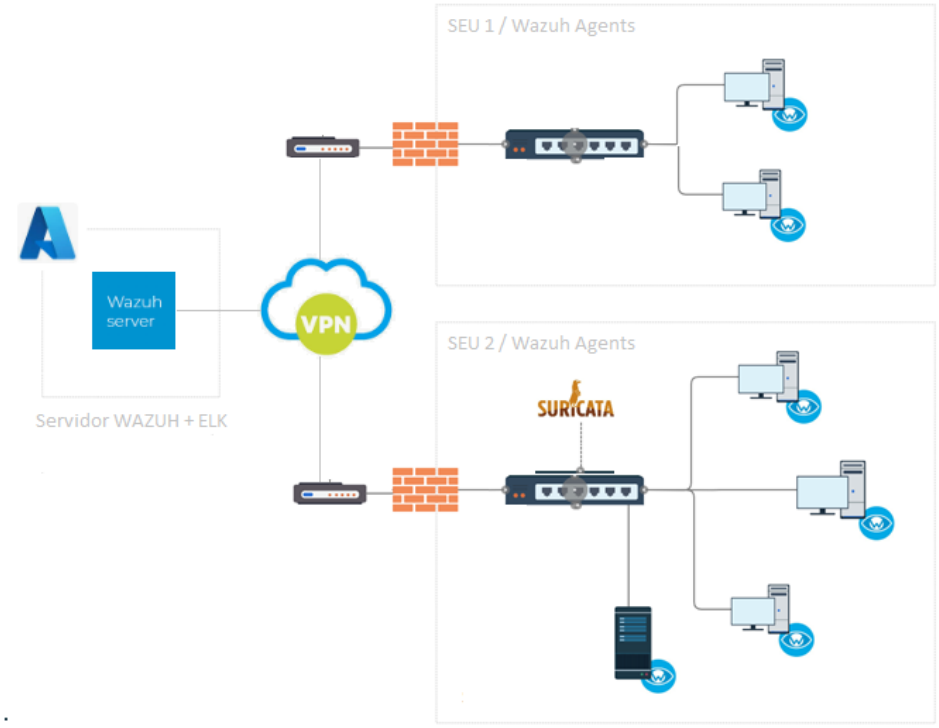


Figura 16 - Diagrama de la solució desplegada a l'entorn de laboratori

Les proves de concepte realitzades s'han formulat a partir de les principals amenaces de ciberseguretat a les quals s'enfronten les PIME. L'objectiu es valorar les capacitat de detecció i resposta de la solució enfront aquestes amenaces.

5.6.1 Detecció d'atacs de força bruta

Els atacants utilitzen les tècniques de força bruta per accedir i comprometre sistemes i serveis mitjançant comptes d'usuaris de les quals desconeix la contrasenya. En un atac de força bruta es busca, mitjançant mecanismes iteratius o repetitius, esbrinar una contrasenya a partir de provar totes les combinacions possibles fins a trobar la combinació correcta.

Els atacs de força bruta, atès que utilitzen el mètode de prova i error, poden dilatar-se notablement en el temps, per aquesta raó solen combinar-se amb atacs de diccionari.

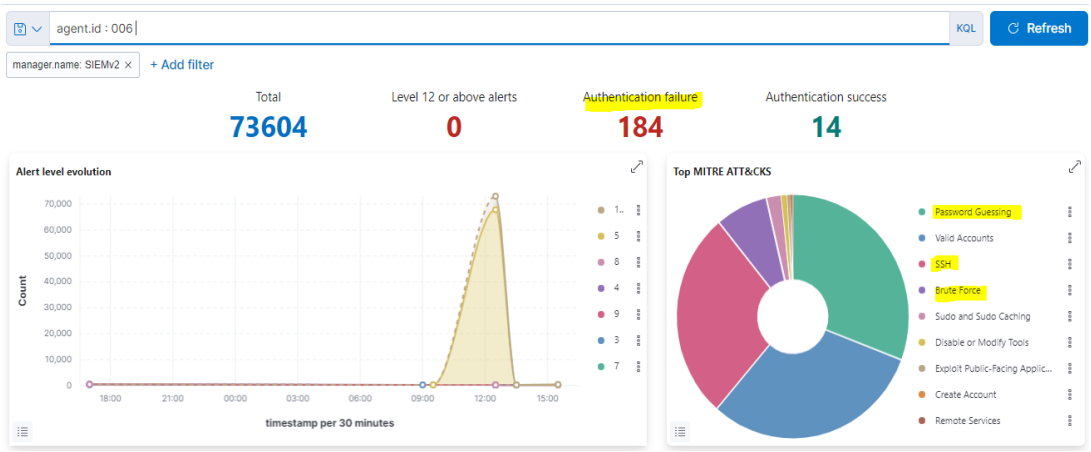
En aquesta prova de concepte simularem un atac de força bruta sobre el servei SSH d'un dels servidors Linux que hem desplegat al laboratori.

Per a realitzar l'atac de força bruta utilitzarem l'eina Hybra:

```
hydra -f -L wordlist/ssh/user -P wordlist/ssh/password -t 4
ssh://10.0.0.6
```

Aquest eina utilitza un atac de diccionari sobre el servei SSH especificat, amb l'objectiu de trobar una combinació d'usuari i contrasenya que proporcioni accés a l'equip atacat.

Un cop llençat l'atac podem comprovar com Wazuh comença a recollir els esdeveniments d'autenticació fallida generats.



Podem comprovar com les regles de Wazuh no només recopilen i generen alertes dels esdeveniments d'autenticació fallida, sinó els agreguen i correlacionen amb el framework MITRE ATT&CK, generant les corresponent alertes.

	Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
›	May 21, 2022 @ 15:55:24.170	SRV1-Linux-LAB	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
›	May 21, 2022 @ 15:55:24.167	SRV1-Linux-LAB	T1110	Credential Access	Maximum authentication attempts exceeded.	8	5758
›	May 21, 2022 @ 15:55:22.307	SRV1-Linux-LAB	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
›	May 21, 2022 @ 15:55:22.302	SRV1-Linux-LAB	T1110	Credential Access	Maximum authentication attempts exceeded.	8	5758
›	May 21, 2022 @ 15:55:22.298	SRV1-Linux-LAB	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
›	May 21, 2022 @ 15:55:22.294	SRV1-Linux-LAB	T1110	Credential Access	Maximum authentication attempts exceeded.	8	5758
›	May 21, 2022 @ 15:55:22.290	SRV1-Linux-LAB	T1110	Credential Access	syslog: User missed the password more than one time	10	2502

A la captura anterior podem apreciar les alertes generades per les regles 2502 i 5758 de Wazuh, ambdues relacionades amb atacs de força bruta segons el framework MITRE ATT&CK.

D'altra banda, podem apreciar com les alertes generades per l'atac de força bruta son enviades a la plataforma de resposta a incidents de seguretat TheHive per a la seva gestió.

	Severity	Read	Title	# Case	Type	Source	Reference	Observables	Dates O. C. U.
☐	M	Unread	PAM: Multiple failed logins in a small period of time. agent_name=SRV1-Linux-LAB rule=5551 agent_id=006 agent_ip=10.0.0.6 wazuh	None	wazuh_alert	wazuh	f0fb67	2	O. 05/21/22 17:05 C. 05/21/22 17:05
☐	M	Unread	PAM: Multiple failed logins in a small period of time. agent_name=SRV1-Linux-LAB rule=5551 agent_id=006 agent_ip=10.0.0.6 wazuh	None	wazuh_alert	wazuh	70c5f4	2	O. 05/21/22 17:05 C. 05/21/22 17:05
☐	M	Unread	sshd: brute force trying to get access to the system. Non existent user.	None	wazuh_alert	wazuh	0bc60b	2	O. 05/21/22 17:05 C. 05/21/22 17:05

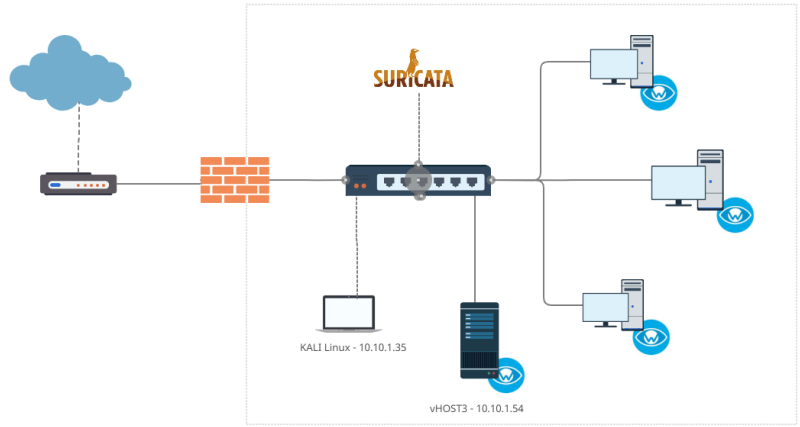
5.6.2 Detecció d'escaneig de ports – Integració amb IDS/IPS Suricata

L'escaneig de ports és una tècnica utilitzada per un potencial atacant per tal de verificar els ports d'una màquina connectada a la xarxa amb la finalitat de d'obtenir i identificar els serveis que s'hi executen. El resultat d'aquesta exploració permetrà a l'atacant obtenir informació sobre la composició de la infraestructura de xarxa i la seva arquitectura, el sistema operatiu dels equips i dispositius, així com els potencials forats de seguretat que després seran explotats pels atacants.

La detecció d'un escaneig de ports dins la xarxa pot indicar la presencia d'un actor no autoritzat a la nostra infraestructura.

Per a la realització d'aquesta prova de concepte s'ha implementat a la xarxa de laboratori el sistema de prevenció d'intrusions (IPS) basat en codi obert Suricata. Aquesta eina de seguretat monitoritza contínuament l'activitat de la xarxa, cercant activitat maliciosa o anòmala, i prenent les accions de prevenció i alerta que es considerin oportunes.

A l'annex del present document es detalla el procés d'instal·lació i integració amb Wazuh.



Per aquesta prova de concepte simularem un escaneig de ports realitzat des d'un equip compromès present a la nostra xarxa, i observarem com l'activitat detectada per Suricata es recollida al nostre SIEM. A banda, també comprovarem les característiques d'edició i personalització de regles de detecció a Wazuh, creant una alerta personalitzada per a la detecció de l'escaneig de ports.

Per realitzar l'escaneig de ports, utilitzarem l'eina *nmap*

```
nmap -sC -sV -Pn 10.10.1.54
```

Un cop iniciat l'escaneig de ports podem comprovar com el IPS Suricata ha detectat l'activitat anòmala a la xarxa, generant les corresponent alertes al nostre SIEM

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 25, 2022 @ 11:20:43.652			Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	86601
May 25, 2022 @ 11:20:43.652			Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	86601
May 25, 2022 @ 11:20:43.638			Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	86601
May 25, 2022 @ 11:20:43.638			Suricata: Alert - ET SCAN Potential SSH Scan	3	86601

Wazuh integra per defecte una sèrie de regles per a la ingesta i gestió d'alertes provinents de Suricata, aquestes regles bàsiques es recullen a l'arxiu *0475-suricata_rules.xml.* Per defecte, totes les alertes de Suricata es categoritzen amb *rule.level* = 3. Volem crear una regla personalitzada i assignar a les alertes de detecció d'escaneig de ports un *rule.level* superior per a diferencia-les de la resta d'alertes generades per Suricata.

Per realitzar aquesta modificació, editarem el fitxer de regles *local_rules.xml* afegint-hi una regla personalitzada per a la detecció de l'escaneig de ports. A la nova regla es recategoritza l'alerta, es modifica la descripció afegint-hi les adreces IP dels equips origen i destí, finalment s'afegeixen a l'alerta l'identificador i la categoria corresponents dins el framework MITRE ATT&CK.

```
<group name="ids,suricata,">
   <rule id="100002" level="10">
      <if_sid>86600</if_sid>
      <field name="event_type">^alert$</field>
      <field name="alert.signature">^ET SCAN</field>
      <description>Suricata Potential SCAN: Alert - $(alert.signature)
from $(src_ip) to $(dest_ip)</description>
      <mitre>
            <id>T1046</id>
      </mitre>
      <group>discovery</group>
    </rule>
</group>
```

Apliquem el nou fitxer de regles i executem de nou l'escaneig de ports. Observem com les alertes recollides al nostre SIEM es generen segons la regla que acabem de definir:

›	May 26, 2022 @ 10:20:28.088	T1046	Discovery	Suricata Potential SCAN: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 from 192.168.1.100 to 192.168.1.62	10	100002
›	May 26, 2022 @ 10:20:26.087	T1046	Discovery	Suricata Potential SCAN: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 from 192.168.1.100 to 192.168.1.62	10	100002
›	May 26, 2022 @ 10:20:26.087	T1046	Discovery	Suricata Potential SCAN: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 from 192.168.1.100 to 192.168.1.62	10	100002

5.6.3 Detecció d'anomalies en la gestió d'usuaris

La detecció d'anomalies en la gestió del usuaris o en els seus hàbits d'activitat pot revelar la possible existència d'un incident de seguretat. En aquest apartat avaluarem les capacitats de la solució dissenyada per a detectar patrons o comportament anòmals en la gestió d'usuaris

La detecció al sistema d'activitats fora de l'horari habitual dels usuaris o d'activitat a l'organització, pot ser indicador de la presencia a la infraestructura d'un atacant o sistema compromès.

Per aquesta proba de concepte s'ha creat una regla personalitzada que alerta de la creació o modificació de comptes d'usuari fora de l'horari habitual de l'organització:

```
<rule id="100004" level="12">
    <if_sid>60103</if_sid>
    <time>10 pm - 6:30 am</time>
    <field name="win.system.eventID">^4720$|^4722$</field>
    <description>User account enabled or created during non-business
hours.</description>
    <mitre>
      <id>T1098</id>
    </mitre>
    <group>account_changed,adduser</group>
</rule>
```

Podem comprovar com, un cop aplicada la nova regla, al SIEM es genera la corresponent alerta d'activitat anòmala al crear un nou usuari fora de l'horari habitual de l'organització:

›	May 26, 2022 @ 19:08:24.549	T1098	Persistence	User account enabled or created during non-business hours.	12	100004
›	May 26, 2022 @ 19:08:24.549	T1098	Persistence	User account enabled or created during non-business hours.	12	100004

Un altre indicador que pot revelar un incident de seguretat és la modificació dels permisos o rols d'un usuari al sistema, especialment quan aquesta modificació es realitza des d'un origen desconegut o en unes franges horàries poc habituals.

En aquest cas, s'ha creat una nova regla que alerta quan es produeixen modificacions al grup d'administradors del domini. Al la captura següent podem comprovar com el SIEM ha generat la corresponent alerta a afegir un nou usuaris al grup d'administradors del sistema supervisat.

›	May 26, 2022 @ 11:52:49.222	T1484	Defense Evasion, Privilege Escalation	User added to administrators group.	12	100003
›	May 26, 2022 @ 11:40:55.651	T1484	Defense Evasion, Privilege Escalation	User added to administrators group.	12	100003
›	May 26, 2022 @ 11:36:15.307	T1484	Defense Evasion, Privilege Escalation	User added to administrators group.	12	100003

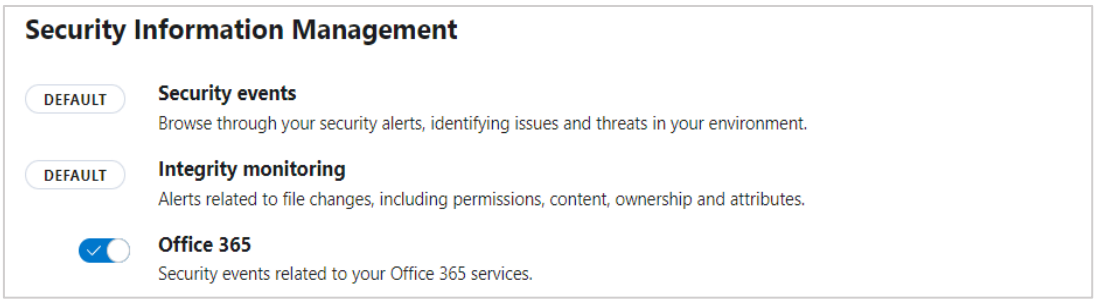
5.6.4 Seguretat al núvol – Integració amb Office 365

Les pimes no son alienes a la tendència consolidada de migrar càrregues de treball cap al núvol. Des del punt de vista de la seguretat, les plataformes i proveïdors de serveis al núvol ha redefinit el concepte tradicional de gestió de la seguretat cap a un nou model basat en responsabilitats compartides. Tot i que pot haver petites diferencies segons el proveïdor i la tipologia de servei contractat, en general, la seguretat dels accessos i de les dades correspon al client final i per tant ha de ser considerats dins l'estratègia de seguretat de qualsevol empresa.

En aquesta prova de concepte comprovarem com la solució SIEM proposada proporciona integracions per a supervisar la seguretat de les càrregues de treball ubicades als principals proveïdors de serveis al núvol.

En aquesta prova de concepte avaluarem la integració de la solució amb els serveis de Office 365 per a la obtenció dels esdeveniments de seguretat generats per la plataforma.

Per fer ús de la integració d'Office 365 amb Wazuh cal, en primer lloc, habilitar el component. Podem fer-ho de forma ràpida des de la interfície web de Wazuh.

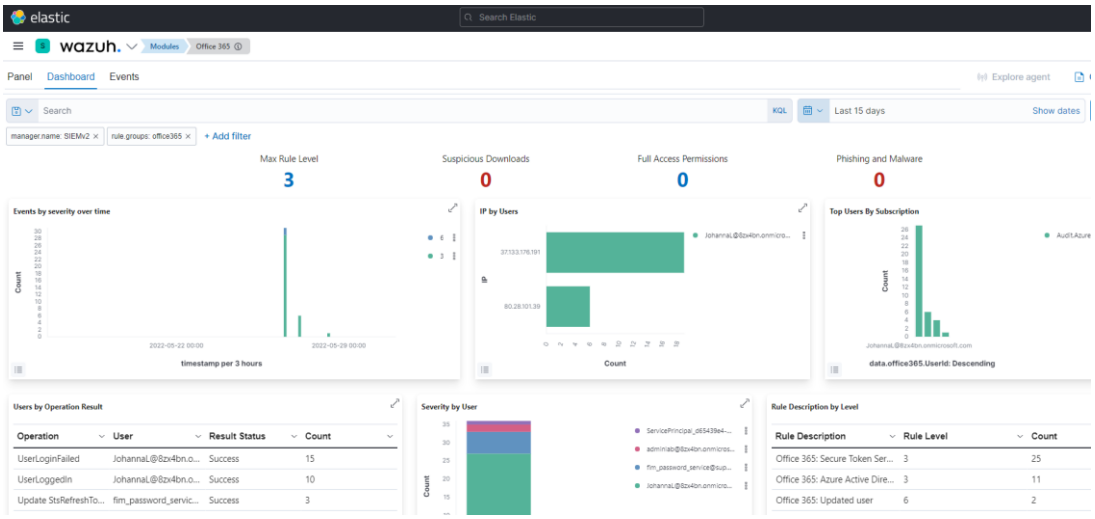


Aquest mòdul de Wazuh permet recollir tots els registres d'Office 365 mitjançant la seva API. Perquè Wazuh es connecti correctament a l'API d'Office365, cal un procés d'autenticació. Per fer-ho, hem de proporcionar els *tenant_id*, *client_id* i *client_secret* de l'aplicació que autoritzem a l'organització.

Un cop habilitat el mòdul, cal que el configurem perquè es connecti al nostre t*enant* o *tenants* de Office 365. En aquest cas, configurem Wazuh perquè reculli els esdeveniments del tipus Audit. Audit.AzureActiveDirectory en un interval de 10 minuts.

```
<office365>
    <enabled>yes</enabled>
    <interval>10m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
        <tenant_id>4ac1c52f-aaf8-4087-ac19-...</tenant_id>
        <client_id>ca42ee78-1026-4943-a5ec-...</client_id>
        <client_secret>x-
I8Q~gUGIuKkvK8ON1K4S9I23H4aMRm38....</client_secret>
    </api_auth>
    <subscriptions>
        <subscription>Audit.AzureActiveDirectory</subscription>
    </subscriptions>
  </office365>
```

Wazuh disposa d'un panell específic a la interfície web per a la gestió i visualització dels esdeveniments de seguretat generats per la integració amb Office 365.



A la següent captura podem apreciar alguns esdeveniments de seguretat registrats. En aquest cas podem observa errors de validació d'una de les comptes d'usuari.

›	May 28, 2022 @ 13:07:45.376	Audit.AzureActiveDirectory	Update device.	ServicePrincipal_d65439e4-5401-43d0-b81a-940915ee7840	-
›	May 27, 2022 @ 08:43:01.949	Audit.AzureActiveDirectory	UserLoginFailed	JohannaL@8zx4bn.onmicrosoft.com	80.28.101.39
›	May 27, 2022 @ 08:43:01.949	Audit.AzureActiveDirectory	UserLoginFailed	JohannaL@8zx4bn.onmicrosoft.com	80.28.101.39
›	May 27, 2022 @ 08:43:01.949	Audit.AzureActiveDirectory	UserLoginFailed	JohannaL@8zx4bn.onmicrosoft.com	80.28.101.39

6. Conclusions

El present treball es desenvolupa al voltant del panorama actual de la ciberseguretat a la PIME, les quals motivades per una creixent exposició en el nombre i la complexitat d'amenaces i atacs, han hagut de fer un pas endavant en les seves estratègies de ciberseguretat mitjançant la definició de plans i polítiques de seguretat, així com la implementació d'estratègies de protecció que requereixen el desplegament d'eines de vigilància de la seguretat avançades.

A partir de l'estudi de diferents solucions de SIEM disponibles al mercat, el treball aborda la possibilitat de desenvolupar una solució SIEM as a Service integrada per un ecosistema de tecnologies de vigilància de la seguretat que pugui donar resposta a les necessitats de la PIME.

A partir del desenvolupament del treball, es poden extreure les següent conclusions clau:

- Els SIEM proporcionen una visió completa i unificada de la seguretat de la informació, alhora que ofereix als analistes de seguretat un potent instrument per descobrir, en temps real, tendències i patrons anòmals que evidenciïn amenaces de seguretat i atacs presents a la infraestructura.
- Un dels aspectes més rellevant alhora de implementar un SIEM és el seu cost, tan en relació al llicenciament de la solució, com en relació als professionals qualificats necessaris per al seu desplegament i gestió. Gran part de les solucions SIEM estudiades al treball tenien uns costos de llicenciament considerablement elevats que les situen fora de l'abast de la majoria de pimes.
- Mitjançant l'ús de solucions basades en codi obert es poden obtenir totes les funcionalitats i serveis bàsics que integra un SIEM sense els punt de partida dels costos de llicenciament habituals en aquest tipus de solucions.
- La solució estudiada al present treball, integrada per Elastic Stack + Wazuh proporciona un ampli ventall de funcionalitats en l'àmbit de la seguretat, a banda d'una arquitectura molt versàtil capaç d'adaptar-se a múltiples models de servei.
- Les proves de concepte realitzades han revelat que la solució dissenyada pot adaptar-se perfectament a les necessitats en matèria de vigilància de la seguretat d'un gran nombre de pimes.

6.1 Seguiment de la planificació i metodologia de treball

La principal motivació per a desenvolupar el treball de final de màster al voltant de la PIME i les eines de vigilància de la seguretat avançades va ser professional. El present treball ha estat una bona oportunitat de consolidar els coneixements adquirits durant el màster i alhora aprofundir en una sèrie de tecnologies de les quals només tenia alguns coneixements teòrics, i que tindran aplicació directa en el meu dia a dia professional.

Crec que la metodologia seguida era la més indicada, amb una part important del treball dedicada a estudiar els sistemes SIEM, tot i que he trobat un camp molt més extens i complexa del que inicialment esperava.

El principal inconvenient que he trobat en el seguiment de la planificació del treball és una planificació inicial errònia. Tot i que com he comentat, considero que la par de investigació era essencial, el temps disponible per a l'estudi de Elastic Stack i Wazuh ha estat del tot insuficient.

A nivell formatiu ha estat una experiència molt enriquidora i que de ven segur ha establert les bases sobre les que s'assentarà la meva activitat professional els propers anys.

6.2 Línies de treball futur

Si bé part dels objectius que es van definir a l'inici el treball s'han assolit, considero que encara resta feina per fer.

El desenvolupament del treball ha permès definir l'estructura, funcionalitats i models de servei d'una hipotètica solució *SIEM as a Service* basada en Elastic Stack + Wazuh capaç cobrir les necessitats en matèria de vigilància de la seguretat de tota mena de pimes. Tot i això, ha quedat pendent aprofundir en l'estudi de cada una d'aquestes funcionalitats i serveis, avaluar-ne els punt forts i especialment les limitacions.

D'altra banda, el desenvolupament del treball s'ha centrat principalment sobre les funcionalitats i serveis que ofereix Wazuh, deixant per a treballs futurs l'estudi detallat de les funcionalitats i integracions dels components de Elastic Security i els beneficis que pot aportar a la solució dissenyada.

Una possible línia de treball futur podria abordar el desenvolupament d'un servei de SOC (Security Operations Center) orientat a la PIME i construït al voltant de la solució SIEM as a Service plantejada al present treball.

7. Glossari

EDR *(Endpoint Detection Response)* - Un sistema EDR es caracteritza per unir funcionalitats d'un antivirus tradicional amb la detecció d'amenaces avançades mitjançant intel·ligència artificial.

Endpoint - Un endpoint és qualsevol dispositiu que sigui físicament la part final duna xarxa. Els ordinadors de sobretaula, els portàtils, les tablets, i els smatphones son considerats endpoints.

IDS (*Intrusion Detection System*) - Un Sistema de Detecció d'Intrusos és un programa de detecció d'accessos no autoritzats a un computador o a una xarxa.

IPS (*Intrusion Prevention System*) – Un sistema de prevenció d'intrusions és un dispositiu de seguretat de xarxa que monitoritza el tràfic de xarxa i les activitats d'un sistema, a la recerca d'activitat maliciosa.

Malware (Malicious Sofware) - El programari maliciós o programari nociu és el programari o arxiu nociu per a l'ordinador que està dissenyat per a inserir virus, cucs, troians, programari espia o bots, intentant aconseguir algun objectiu, com ara recollir informació sobre l'usuari o sobre l'ordinador en si.

NGFW (Next Generation Firewalls) o tallafoc de nova generació – Són tallafocs que han evolucionat incorporant moltes altres funcionalitats de seguretat que a través d'una anàlisi exhaustiva del tràfic de xarxa permeten detectar i minimitzar riscos actius, problemes de seguretat, activitats sospitoses, fuites de dades, etc.

PoC (Proof of Concept) - Una prova de concepte és una implementació d'un mètode o d'una idea realitzada amb el propòsit de verificar que el concepte o la teoria en qüestió és susceptible de ser explotada d'una manera útil.

SIEM (Security information and event management) - Un sistema de informació de seguretat i gestió d'esdeveniments combina la gestió de la informació de seguretat (SIM) amb la gestió d'esdeveniments de seguretat (SEM). roporcionen anàlisis en temps real de les alertes de seguretat generades per aplicacions i maquinari de xarxa.

SOAR (security orchestration, automation and response) – Conjunt de programes i utilitats que permeten recopilar dades sobre amenaces de seguretat i respondre als esdeveniments de seguretat sense intervenció humana. L'objectiu d'utilitzar una plataforma SOAR és millorar l'eficiència de les operacions de seguretat física i digital.

XDR (Extended Detection and Response) - Permet la detecció i resposta a incidents de seguretat en totes les capes de l'entorn de TI. La tecnologia XDR recopila i vincula automàticament les dades de diverses fonts, que poden incloure punts finals, xarxes i usuaris.

8. Bibliografia

[1] CKECK POINT. *Check Point Research:Cyber Attacks Increased 50% Year over Year* [en línia]. Blog, 2021 [consulta: 27 de Febrer de 2022]. Disponible a https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

[2] GOOGLE. Panorama actual de la Ciberseguridad en España [en línia]. Publicació en línea, Octubre de 2019 [consulta: 27 de Febrer de 2022]. Disponible a: https://drive.google.com/file/d/18TNjaDus-lrSl5gL5Wt-Z4DOsKXtQ46m/view

[3] INCIBE. *INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020* [en línia]. Nota de premsa, 2021 [consulta: 28 de Febrer de 2022]. Disponible a https://www.incibe.es/sala-prensa/notas-prensa/incibe-gestiono-mas-130000-incidentes-ciberseguridad-durante-el-ano-2020

[4] INCIBE. *Tendencias en Ciberseguridad – Gestión de información de Eventos de Seguridad (SIEM)* [en línia]. Ficha, 2019 [consulta: 25 de Febrer de 2022]. Disponible a: https://www.incibe.es/sites/default/files/estudios/gestion_de_informacion_de_eventos_de_seguridad-siem.pdf

[5] INCIBE – Empresas – ¿Qué te interesa? – Buenas prácticas en el área de informática – [en línia]. Web , 2022 [consulta: 20 de Abril de 2022]. Disponible a: https://www.incibe.es/protege-tu-empresa/que-te-interesa/buenas-practicas-area-informatica

[6] INCIBE – Empresas – ¿Qué te interesa? – Plan director de seguridad [en línia]. Web , 2022 [consulta: 20 de Maig de 2022]. Disponible a: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[7] INCIBE – Empresas – ¿Qué te interesa? – Plan de contingencia y continuidad de negocio [en línia]. Web , 2022 [consulta: 20 de Maig de 2022]. Disponible a: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingenciacontinuidad-negocio

[8] INCIBE – Empresas – ¿Qué te interesa? – Desarrollar cultura de seguridad [en línia]. Web , 2022 [consulta: 20 de Maig de 2022]. Disponible a: https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-enseguridad

[9] KASPERSKY. *Economía de la seguridad de TI en el 2019* [en línia]. Informe, 2019 [consulta: 25 de Febrer de 2022]. Disponible a: https://go.kaspersky.com/rs/802-IJN-240/images/SP%20Brochure_A4_Report-IT-Security-Economics-SP.pdf

[10] DELOITTE. *El estado de la ciberseguridad en España. Post pandemia: un camino inexplorado* - [en línia]. Informe, 2022 *[consulta: 10 d'Abril de 2022]. Disponible a: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html*

[11] GARTNER - *Magic Quadrant Security Information and Event Management (SIEM)* [en línia]. Web , 2021 [consulta: 18 de Març de 2022]. Disponible a: https://www.gartner.com/en/documents/4003080

[12] ELASTIC SECURITY - *SIEM basado en el cloud y analíticas de seguridad [*en línia]. Web, 2022 [consulta: 21 de Març de 2022]. Disponible a: https://www.elastic.co/es/siem/

[13] *BITLYFT – What is SIEM-as-a-Service (A Guide to managed SIEM service)* [en línia]. Article en línea, 2022 [consulta: 28 de Març de 2022]. Disponible a: https://www.bitlyft.com/resources/what-is-managed-siem-as-a-service

[14] DAVINCI GROUP - *Elastic Security: Qué es, ECS, SIEM*.. [en línia]. Article en línia, 2022 [consulta: 22 de Març de 2022]. Disponible a: https://www.davincigroup.es/que-es-elastic-security/

[15] ELASTIC - *Preguntas frecuentes sobre el cambio de licencia 2021* [en línia]. Web , 2018 [consulta: 25 de Març de 2022]. Disponible a: https://www.elastic.co/es/pricing/faq/licensing

[16] ELASTIC - Elastic License 2.0 (ELv2) [en línia]. Web 2022 [consulta: 10 de Març de 2022]. Disponible a: https://www.elastic.co/es/licensing/elastic-license

[17] WAZUH - *The Open Source Security Platform* [en línia]. Web , 2022 [consulta: 22 de Març de 2022]. Disponible a: https://wazuh.com/

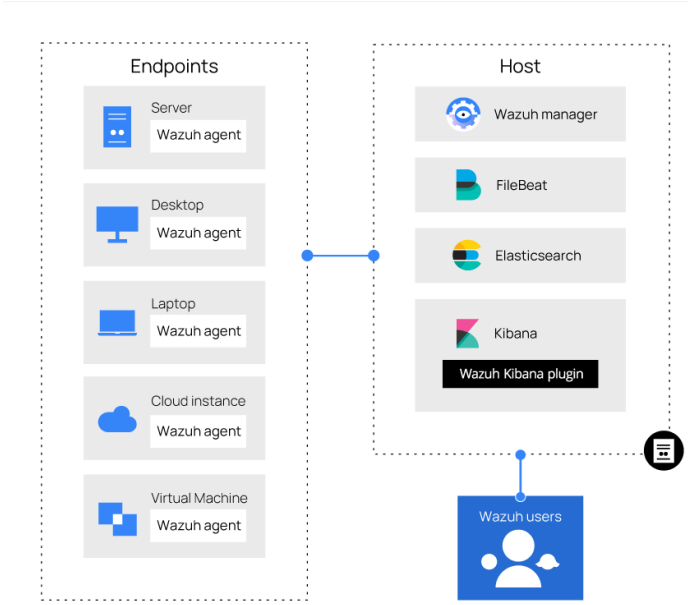
[18] TheHive - *SECURITY INCIDENT RESPONSE FOR THE MASSES* [en línia]. Web , 2022 [consulta: 22 de Març de 2022]. Disponible a: https://thehive-project.org/

[19] SURICATA – [en línia]. Web , 2022 [consulta: 20 de Maig de 2022]. Disponible a: https://suricata.io/

9. Annex I – Guies d'instal·lació

Al present annex es recull la guia de instal·lació de la solució SIEMaaS seleccionada, basada en un desplegament de Elastic Stack autogestionat complementat amb les eines de monitorització i gestió de la seguretat Wazuh i TheHive.

La present guia es basa en el model de desplegament i servei SIEMaaS On-Premises (SIEM as a Service hostatjat a la infraestructura client). Per aquest model es preveu la instal·lació de tots els components de la solució en un únic equip o màquina virtual, amb capacitat per donar servei a un màxim de 80-100 equips client.



Per al desplegament de la solució, s'ha seleccionat el sistema operatiu base Ubuntu Server 20.04.

La present guia es basa en la documentació oficial de Wazuh, específicament en la documentació per la instal·lació de Wazuh en un entorn All-in-one basat en Elastic Stack bàsic license.

Per tal de mantenir la compatibilitat entre tots els components de la solució les versions implementades a la següent guia son:

- Elastic Stack 7.17.3 (ElasticSearch, LogStash, Kibana, Filebeats)
- Wazuh Server 4.3
- TheHive 4.1.19
- Suricata 6.0.5

9.1 Instal·lació d'Elasticsearch

1) Afegim el repositori de Elastic Stack a la nostre servidor Ubuntu 20.04

Importem la clau GPG:

```
rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Afegim el repositori:

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

2) Instal·lació i configuració d'ElasticSearch

Instal·lem el paquet Elasticsearch:

```
yum install elasticsearch-7.17.3
```

Baixem el fitxer /etc/elasticsearch/elasticsearch.yml de configuració de la següent manera:

```
curl -so /etc/elasticsearch/elasticsearch.yml
https://packages.wazuh.com/4.3/tpl/elastic-
basic/elasticsearch_all_in_one.yml
```

3) Creació i desplegament de certificats

Descarrega el fitxer de configuració per crear els certificats:

```
curl -so /usr/share/elasticsearch/instances.yml
https://packages.wazuh.com/4.3/tpl/elastic-
basic/instances_aio.yml
```

Els certificats es poden crear mitjançant l'eina elasticsearch-certutil:

```
/usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem
--in instances.yml --keep-ca-key --out ~/certs.zip
```

Extraieu el fitxer */usr/share/elasticsearch/certs.zip* generat al pas anterior:

```
unzip ~/certs.zip -d ~/certs
```

Crear el directori */etc/elasticsearch/certs*. Copiar-hi el fitxer CA, el certificat i la clau:

```
mkdir /etc/elasticsearch/certs/ca -p
cp -R ~/certs/ca/ ~/certs/elasticsearch/*
/etc/elasticsearch/certs/
chown -R elasticsearch: /etc/elasticsearch/certs
chmod -R 500 /etc/elasticsearch/certs
chmod 400 /etc/elasticsearch/certs/ca/ca.*
/etc/elasticsearch/certs/elasticsearch.*
rm -rf ~/certs/ ~/certs.zip
```

4) Activar i iniciar el servei Elasticsearch:

```
systemctl daemon-reload
systemctl enable elasticsearch
systemctl start elasticsearch
```

5) Generem les credencials per a tots els rols i usuaris predefinits d'Elastic Stack:

```
/usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```

L'ordre anterior mostrarà una sortida com la següent, que conté el les contrasenyes generades pels usuaris predefinits:

```
Changed password for user apm_system
PASSWORD apm_system = lLPZhZkB6oUOzzCrkLSF

Changed password for user kibana_system
PASSWORD kibana_system = TaLqVOnSoqKTYLIU0vDn

Changed password for user kibana
PASSWORD kibana = TaLqVOvXoqKTYLIU0vDn

Changed password for user logstash_system
PASSWORD logstash_system = UtuDv2tWkXGYL83v9kWA

Changed password for user beats_system
PASSWORD beats_system = qZcbvCslafMpoEOrE9Ob

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = LzJpQiSylncmCU2GLBTS

Changed password for user elastic
PASSWORD elastic = AN4UeQGA7HGl5iHpMla7
```

6) Comprovar que la instal·lació s'ha completat correctament:

Per comprovar que la instal·lació s'ha fet correctament, executem l'ordre següent substituint <*elastic_password*> per la contrasenya generada al pas anterior per a l'usuari *elastic*:

```
curl -XGET https://localhost:9200 -u elastic:<elastic_password> -
k
```

Si tot és correcte, aquesta comanda hauria de generar una sortida com la següent:

```
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "upF9h1afQN2TfHtt0h3Kuw",
  "version" : {
    "number" : "7.17.3",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "6bc13727ce758c0e943c3c21653b3da82f627f75",
    "build_date" : "2021-09-15T10:18:09.722761972Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

9.2 Instal·lació del servidor Wazuh

El servidor Wazuh recopila i analitza dades dels agents desplegats. Executa el gestor de Wazuh, l'API de Wazuh i Filebeat.

1) Afegim el repositori de Wazuh a la nostre servidor Ubuntu 20.04

Importem la clau GPG:

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

Afegim el repositori:

```
cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-\$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF
```

2) Instal·leu el paquet del gestor de Wazuh

```
yum install wazuh-manager
```

3) Activar i iniciar el servei de gestor de Wazuh:

```
systemctl daemon-reload
systemctl enable wazuh-manager
systemctl start wazuh-manager
```

Un cop iniciat el servei, executeu l'ordre següent per comprovar si el gestor de Wazuh està actiu:

```
systemctl status wazuh-manager
```

9.3 Instal·lació de Filebeat

1) Instal·lació i configuració de Filebeat

Instal·lem el paquet Filebeat:

```
yum install filebeat-7.17.3
```

Baixem el fitxer de configuració de Filebeat utilitzat per reenviar alertes de Wazuh a Elasticsearch:

```
curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.3/tpl/elastic-
basic/filebeat_all_in_one.yml
```

Descarreguem la plantilla d'alertes per a Elasticsearch:

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/4.3/extensions/elas
ticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json
```

Descarreguem el mòdul Wazuh per a Filebeat:

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-
0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Editem, el fitxer */etc/filebeat/filebeat.yml*:

```
output.elasticsearch.password: <elasticsearch_password>
```

Substituït *elasticsearch_password* amb la contrasenya generada anteriorment per a l'usuari elastic.

Copiem els certificats a */etc/filebeat/certs/*

```
cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/
cp /etc/elasticsearch/certs/elasticsearch.crt
/etc/filebeat/certs/filebeat.crt
cp /etc/elasticsearch/certs/elasticsearch.key
/etc/filebeat/certs/filebeat.key
```

2) Activar i iniciar el servei de Filebeat:

```
systemctl daemon-reload
systemctl enable filebeat
systemctl start filebeat
```

Per assegurar-nos que Filebeat s'ha instal·lat correctament, executem l'ordre següent:

```
filebeat test output
```

9.4 Instal·lació i configuració de Kibana

Kibana és una interfície web flexible i intuïtiva per extreure i visualitzar els esdeveniments i arxius emmagatzemats a Elasticsearch.

1) Instal·lació i configuració de Kibana

Instal·lem el paquet Kibana:

```
yum install kibana-7.17.3
```

Copiem els certificats d'Elasticsearch a la carpeta de configuració de Kibana:

```
mkdir /etc/kibana/certs/ca -p
cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/
cp /etc/elasticsearch/certs/elasticsearch.key
/etc/kibana/certs/kibana.key
cp /etc/elasticsearch/certs/elasticsearch.crt
/etc/kibana/certs/kibana.crt
chown -R kibana:kibana /etc/kibana/
chmod -R 500 /etc/kibana/certs
chmod 440 /etc/kibana/certs/ca/ca.* /etc/kibana/certs/kibana.*
```

Descarreguem els fitxers de configuració de Kibana:

```
curl -so /etc/kibana/kibana.yml
https://packages.wazuh.com/4.3/tpl/elastic-
basic/kibana_all_in_one.yml
```

Editem el fitxer */etc/kibana/kibana.yml*:

```
elasticsearch.password: <elasticsearch_password>
```

Substituït *elasticsearch_password* amb la contrasenya generada anteriorment per a l'usuari elastic.

Creem el directori */usr/share/kibana/data*:

```
mkdir /usr/share/kibana/data
chown -R kibana:kibana /usr/share/kibana
```

Instal·lem el connector Wazuh Kibana. La instal·lació del connector s'ha de fer des del directori inicial de Kibana de la següent manera:

```
cd /usr/share/kibana
 sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-
4.3.1_7.17.3-1.zip
```

Enllacem el socket de Kibana al port 443:

```
setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node
```

2) Activar i iniciar el servei de Kibana:

```
systemctl daemon-reload
systemctl enable kibana
systemctl start kibana
```

9.5 Instal·lació i configuració de TheHive

TheHive és una plataforma de resposta a incidents de seguretat, basada en codi obert i gratuïta, dissenyada per facilitar la tasca dels equips de SOC, CSIRT, CERT i a qualsevol professional de la seguretat de la informació responsable d'investigar i gestionar incidents de seguretat.

1) Instal·lació de dependències

Instal·lem JVM (Java Virtual Machine):

```
apt-get install -y openjdk-8-jre-headless
echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" >>
/etc/environment
export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"
```

2) Instal·lació i configuració de Apache Cassandra:

Afegim el repositori:

```
curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-
key add -
echo "deb http://www.apache.org/dist/cassandra/debian 311x main"
| sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list
```

Instal·lem Cassandra des del seu repositori:

```
sudo apt update
sudo apt install cassandra
```

Iniciem la configuració de Cassandra modificant el nom predeterminat del clúster:

```
cqlsh localhost 9042

cqlsh> UPDATE system.local SET cluster_name = 'thp' where
key='local';
```

Configurem Cassandra editant el fitxer */etc/cassandra/cassandra.yaml* :

```
# content from /etc/cassandra/cassandra.yaml

cluster_name: 'thp'
listen_address: 'xx.xx.xx.xx' # address for nodes
rpc_address: 'xx.xx.xx.xx' # address for clients
seed_provider:
    - class_name: org.apache.cassandra.locator.SimpleSeedProvider
      parameters:
          # Ex: "<ip1>,<ip2>,<ip3>"
          - seeds: 'xx.xx.xx.xx' # self for the first node
data_file_directories:
  - '/var/lib/cassandra/data'
commitlog_directory: '/var/lib/cassandra/commitlog'
saved_caches_directory: '/var/lib/cassandra/saved_caches'
hints_directory:
  - '/var/lib/cassandra/hints'
```

Finalment reiniciem el servei per aplicar la nova configuració:

```
service cassandra restart
```

3) Instal·lació i configuració de TheHive:

Importem la clau GPG:

```
curl https://raw.githubusercontent.com/TheHive-
Project/TheHive/master/PGP-PUBLIC-KEY | sudo apt-key add -
```

Afegim el repositori i instal·lem la darrera versió estable de TheHive4:

```
echo 'deb https://deb.thehive-project.org release main' | sudo
tee -a /etc/apt/sources.list.d/thehive-project.list
sudo apt-get update
sudo apt-get install thehive4
```

Un cop instal·lat, configurarem TheHive per a que utiltzi les bases de dades de Cassandra. Per fer-ho editem el fitxer */etc/thehive/application.conf* :

```
db {
  provider: janusgraph
  janusgraph {
    storage {
      backend: cql
      hostname: ["127.0.0.1"] # seed node ip addresses
      #username: "<cassandra_username>"       # login to connect
to database (if configured in Cassandra)
      #password: "<cassandra_passowrd"
      cql {
        cluster-name: thp       # cluster name
        keyspace: thehive           # name of the keyspace
        local-datacenter: datacenter1   # name of the datacenter
where TheHive runs (relevant only on multi datacenter setup)
        # replication-factor: 2 # number of replica
        read-consistency-level: ONE
        write-consistency-level: ONE
      }
    }
  }
}
```

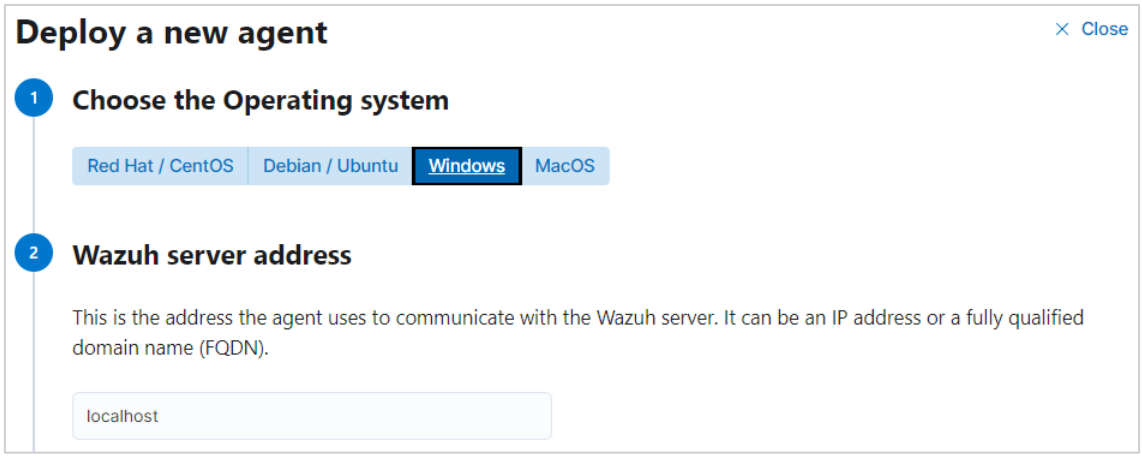
Finalment iniciem el servei:

```
service thehive start
```

9.6 Desplegament d'agents de Wazuh

Els agents de Wazuh s'executa a Linux, Windows, macOS, Solaris, AIX i altres sistemes operatius. Es pot implementar a ordinadors portàtils, ordinadors de sobretaula, servidors, instàncies al núvol, contenidors o màquines virtuals. L'agent ajuda a protegir el vostre sistema proporcionant capacitats de prevenció, detecció i resposta d'amenaces. També s'utilitza per recollir diferents tipus de dades del sistema i de l'aplicació que reenvia al servidor Wazuh a través d'un canal encriptat i autenticat.

El taulell de control de Wazuh proporciona un assistent pas a pas per a la instal·lació dels agents de del repositori en línia. Per fer-ho cal definir el sistema operatiu, l'adreça del servidor de Wazuh i el grup al qual s'assignarà l'agent un cop es connecti al servidor.



1) Desplegament manual dels agents en sistemes Windows:

   Per implementar l'agent descarreguem la darrera versió des del repositori online i editem la variable WAZUH_MANAGER perquè contingui l'adreça IP o el nom d'amfitrió del gestor de Wazuh.

   Despleguem mitjançant l'intèrpret de comandes:

   ```
   wazuh-agent-4.3.1-1.msi /q WAZUH_MANAGER="10.0.0.2"
   ```

   O bé, mitjançant Powershell:

   ```
   .\wazuh-agent-4.3.1-1.msi /q WAZUH_MANAGER="10.0.0.2"
   ```

   Un cop instal·lat l'agent, iniciem el servei:

   ```
   NET START WazuhSvc
   ```

9.7 Instal·lació i integració de Suricata

Suricata és un motor de detecció d'amenaces de codi obert que integra les funcionalitats de detecció d'intrusions (IDS), prevenció d'intrusions (IPS), i seguiment de la seguretat a la xarxa (NSM) por identificar, bloquejar i avaluar ràpidament un ampli ventall d'atacs.

1) Instal·lació de Suricata

Instal·lem dependències i afegim el repositori:

```
yum -y install epel-release wget jq

curl -O
https://copr.fedorainfracloud.org/coprs/jasonish/suricata-
6.0/repo/epel-7/jasonish-suricata-6.0-epel-7.repo
```

Instal·lem Suricata des del repositori:

```
yum -y install suricata
```

Descarreguem i instal·lem el conjunt de regles Emerging Threats Open ruleset

```
wget https://rules.emergingthreats.net/open/suricata-
6.0.3/emerging.rules.tar.gz

tar zxvf emerging.rules.tar.gz
rm /etc/suricata/rules/* -f
mv rules/*.rules /etc/suricata/rules/
```

Descarreguem i instal·lem el fitxer de configuració de Suricata personalitzar i optimitzat pel conjunt de regles del Emerging Threats Pro Team

```
rm -f /etc/suricata/suricata.yaml

wget -O /etc/suricata/suricata.yaml
http://www.branchnetconsulting.com/wazuh/suricata.yaml
```

Ens caldrà editar el fitxer de configuració descarregat i configurar-hi les dades especifiques de la nostra instal·lació, com ara l'identificador de xarxa

```
vi /etc/suricata/suricata.yaml

# Linux high speed capture support
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets
based on flow.
    cluster-id: 99
```

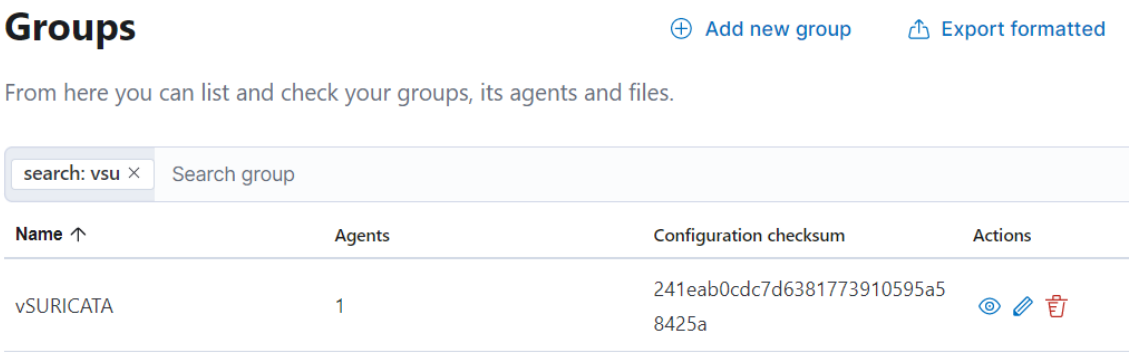
Finalment habilitem i iniciem el servei:

```
systemctl daemon-reload
systemctl enable suricata
systemctl start suricata
```

2) Integració de Suricata a Wazuh

Suricata desa les alertes de seguretat generades al fitxer */var/log/suricata/eve.json* Per defecte Wazuh no monitoritza aquest fitxer, pel que haurem d'afegir-lo a la configuració de l'agent corresponent.

Creem a Wazuh un nou grup:



Editem la configuració local del grup, afegint el fitxer a monitoritzar:

Finalment afegim l'agent al nou grup, i verifiquem a Wazuh que s'estan rebent les alertes provinents de Suricata.