Implementació d'un sistema de SIEM a l'administració pública local

Cas pràctic d'implementació a l'Ajuntament del Masnou

Lucas Maicas Molins

Anàlisi de dades

Tutor de TF
Joan Caparrós Ramírez
Professora responsable de l'assignatura
Andreu Pere Isern Deyà

Data Lliurament
10 de gener de 2023

Universitat Oberta de Catalunya

Agraïments

- A la meva estimada Natàlia, sobretot per caminar agafats de la ma en el camí de la vida, també per haver incentivat que em matriculés en aquest màster i al suport que m'ha donat, en els moments en què tot era complicat i costava tindre el temps necessari per a portar aquest projecte a bon port.

- A la meva filla Emma, que tot i que només té dos mesos i ella no n'és conscient, ha estat molt present en aquest projecte.

- A l'Ajuntament del Masnou, i en concret al meu cap Manu, per permetre que desenvolupi aquest projecte dins de la infraestructura de l'Ajuntament.

- Al Joan Caparrós Ramírez, per l'acompanyament constant durant el transcurs d'aquest semestre, per la ràpida resposta a les consultes i la predisposició a atendre'm.

FITXA DEL TREBALL FINAL

Títol del treball:	*Implementació d'un sistema de SIEM a l'administració pública local*
Nom de l'autor:	*Lucas Maicas Molins*
Nom del consultor/a:	*Joan Caparrós Ramírez*
Nom del PRA:	*Andreu Pere Isern Deyà*
Data de lliurament (mm/aaaa):	*01/2023*
Titulació o programa:	*Màster Universitari en Ciberseguretat i Privadesa*
Àrea del Treball Final:	*Anàlisi de dades*
Idioma del treball:	*Català*
Paraules clau	*SIEM, Administració local, Ciberseguretat*

Resum del Treball

En els últims temps, els incidents d'atacs per cibercriminals s'han multiplicat exponencialment, les administracions públiques no n'han quedat excentes. És per això que ja no son vàlids els sistemes clàssics de protegir els actius digitals, sinó que s'ha d'estar a l'última per evitar ser víctima d'aquests atacs. És per això que l'ús d'eines de recopilació, correlació i actuació d'avant d'esdeveniments com és un SIEM, són de vital importància per els tècnics, que a la vegada han d'estar formats i qualificats per afrontar tots els reptes que se'ls hi plantegen.

El present treball, és centra en l'estudi de les diferents eines SIEM existents al mercat i en concret, en el desplegament de l'eina Wazuh en l'entorn de l'Ajuntament i la seva integració amb les eines ja existents, incorporant el SIEM com a una pota més de la seguretat informàtica.

Abstract

In recent times, incidents of attacks by cybercriminals have increased, and specifically in civil service. This is why the classic systems of protecting digital assets are no longer valid, but you must be up to date to avoid being a victim of these attacks. This is why use apps for collection and correlation and pre-event action such as a SIEM, are of vital importance for technicians, who at the same time must be trained and qualified to face all the challenges posed to them.

The present project is focused on the study of the different SIEM tools existing on the market and specifically on the deployment of the Wazuh tool in the environment of the City Council and its integration with the existing tools, incorporating the SIEM on IT security.

Índex

Llista de figures

1. Introducció

1.1. Context i justificació del Treball

A les acaballes del 2022, vivim en plena era de les TIC. La informació i comunicació, és vital per el dia a dia de les persones i les empreses que la gestionen. Les organitzacions no poden funcionar sense accés a dita informació i sense les facilitats que ofereixen els sistemes informàtics. És per això que cada vegada, som més dependents d'aquests sistemes i de les dades que gestionen. Aquesta realitat és així tant en les organitzacions de caràcter públic, com privat.

Les màfies de ciberdelinqüents son conscients de lo valuoses que son les dades per les organitzacions i la dependència que en tenen, tan mateix, dites màfies s'han professionalitzat, crescut i millorat dins les seves estructures per a realitzar atacs cada vegada més sofisticats.

En l'actualitat, les noticies sobre atacs informàtics, infeccions per programari maliciós (ransomware i d'altres), segrest i robatori de dades, son el dia a dia i ja no ens sorprenen.

Tant l'any 2020, amb la sobrevinguda pandèmia de la covid i l'augment forçat del teletreball, com el passat 2021, els incidents per atacs informàtics han anat en augment i no sembla que el 2022 la tendència es capgiri.

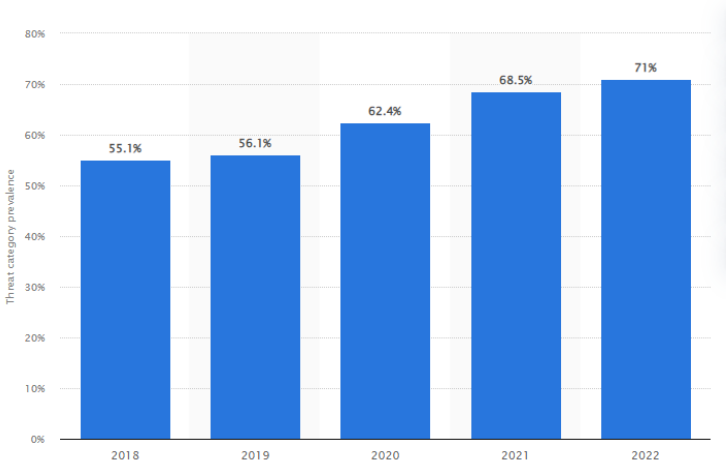


Figura 1[1]: Percentatge d'organitzacions que han estat víctimes d'atacs per ransomware a nivell mundial des del 2018 al 2022

[1] STATISTA. *Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022.* [Web] 16-9-2022. [Consultat el 1 d'octubre de 2022] Disponible a: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Com indica el informe de riscos globals de l'any 2022 de la WEF (Weforum.org), on es valoren diferents riscos, la ciberseguretat n'és el principal, amb un creixement del 5% envers el 2021.

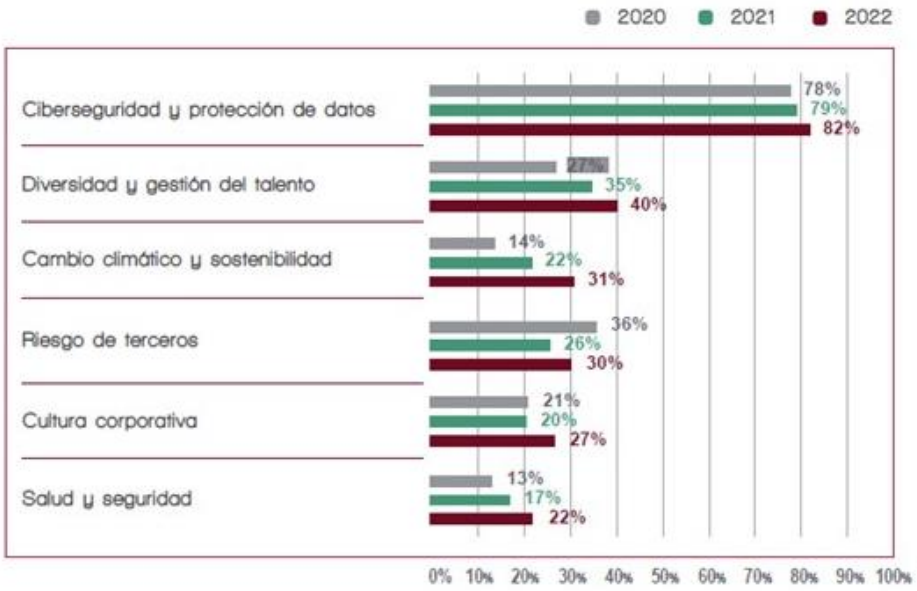


Figura 2[2]: Tendència dels principals riscos, segons els principals líders polítics, comercials, culturals i d'altres actors socials.

És clar, que les administracions, tant d'àmbit estatal com local, com serveis públics en general, no han estat absents de ser el focus aquests incidents i patir-ne les conseqüències. Exemples en són l'ajuntament de Gijón [3]el passat 19 d'abril del 2022, o el de Leganés[4] el 7 de desembre del 2021 o el de Getxo[5] el 17 de gener del 2022. O en l'àmbit estatal, amb l'atac del Servicio Público Estatal de Empleo (SEPE[6]), que va fer que el servei estigués més de 2 setmanes en funcionament parcial i que va causar endarreriments en totes les seves gestions.

---

[2] WE FORUM / INFORDISA. *The Global Risks Report 2022: la Ciberseguridad y la protección de datos destaca como riesgo principal.* [Blog] 8-2-2022. [Consultat el 1 d'octubre de 2022] Disponible a: https://soc.infordisa.com/la-ciberseguridad-desafio-global-2022/ / https://www.weforum.org/reports/global-risks-report-2022

[3] LA VANGUARDIA. *El Ayuntamiento de Gijón sufre un ataque informático.* [Diari en línea] 19-04-2022. [Consultat el 3 d'octubre de 2022] Disponible a: https://www.lavanguardia.com/local/asturias/20220419/8205917/ayuntamiento-gijon-sufre-ataque-informatico.html

[4] EUROPAPRESS. *El Ayuntamiento de Leganés sufre un "ataque informático" que afecta a todo su sistema.* [Diari en línea] 7-12-2021. [Consultat el 3 d'octubre de 2022] Disponible a: *https://www.europapress.es/madrid/noticia-ayuntamiento-leganes-sufre-ataque-informatico-afecta-todo-sistema-20211207144222.html*

[5] DEIA. *El Ayuntamiento de Getxo sufre un ciberataque.* [Diari en línea] 18-01-2022. . [Consultat el 3 d'octubre de 2022] Disponible a: https://www.deia.eus/bizkaia/2022/01/18/ayuntamiento-getxo-sufre-ciberataque-1748041.html

[6] XATAKA. *El SEPE sufre un ciberataque: el Servicio de Empleo deja de estar disponible y se retrasan gestiones como los ERTES o el paro.* [Diari en línea] 9-3-2021. [Consultat el 3 d'octubre de 2022] Disponible a: https://www.xataka.com/seguridad/sepe-sufre-ciberataque-servicio-empleo-deja-estar-disponible-se-retrasan-gestiones-como-ertes-paro

En l'àmbit d'altres tipus d'administracions com son l'educació, amb l'atac a la Universitat Autònoma de Barcelona (UAB[7]), el passat 11 d'octubre del 2021, que va afectar milers de fitxers i gairebé a la totalitat dels seues serveis, tant a nivell d'estudiantils, com a nivell d'equips de recerca i investigació, on els atacants demanaven 3 milions d'euros per alliberar la informació segrestada.

O el més recent atac en l'àmbit sanitari que ha afectat els serveis de tres hospitals [8]i d'altres centres, aquest 7 d'octubre de 2022.

Tant és així, que és necessari que les organitzacions, tant privades com públiques de totes les mides i àmbits, puguin garantir uns estàndards en seguretat, i professionalitzin els seus sistemes i equips de TIC, per lluitar contra aquestes màfies de ciberdelinqüents.

Si en centrem en l'àmbit que pertany l'Ajuntament del Masnou, la majoria d'ens locals de municipis amb el mateix nombre d'habitants i recursos semblants, veiem que disposen d'infraestructures clàssiques, on s'implementa una xarxa local, on hi ha els equips dels treballadors, els servidors dels diferents serveis/aplicacions de les quals es disposa i en aquesta xarxa s'implementa una seguretat perimetral basada en un tallafoc, que moltes vegades no consta ni de funcionalitats avançades com seria un IDS o IPS o filtratge en nivell d'aplicacions.

Tanmateix, totes les administracions, tenen l'obligació d'adaptar-se a l'Esquema Nacional de Seguretat (ENS)[9], aprovat en el real decret de 2010 RD 3/2010 [10]i desenvolupat en les posteriors modificacions de RD 951/2015 [11]i RD 311/2022[12]. Dit esquema, permet garantir que es compleixen la política de seguretat per la protecció adequada de la informació que es tracta i dels serveis que s'ofereixen,

---

[7] ARA. *El ataque informático a la UAB habría afectado a más de 650.000 archivos y los delincuentes reclaman 3 M€.* [Diari en línea] 15-10-2021. [Consultat el 3 d'octubre de 2022] Disponible a:https://es.ara.cat/sociedad/ataque-informatico-uab-habria-afectado-650-000-archivos-delincuentes-reclaman-3-m_1_4149340.html

[8] EL PAIS. *Un ciberataque prácticamente paraliza el servicio de al menos tres hospitales catalanes: Moisès Broggi, Dos de Maig y Creu Roja de L'Hospitalet.* [Diari en línea] 7-10-2022. [Consultat el 7 d'octubre de 2022] Disponible a: https://elpais.com/espana/catalunya/2022-10-07/un-ciberataque-afecta-el-servicio-de-al-menos-tres-hospitales-catalanes-moises-broggi-dos-de-maig-y-creu-roja-de-lhospitalet.html

[9] CCN. Esquema Nacional de Seguridad. [Web] [Consultat el 6 d'octubre de 2022] Disponible a: https://ens.ccn.cni.es/es/esquema-nacional-de-seguridad-ens

[10] BOE. *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* [Document en línia] 29-1-2010 [Consultat el 6 d'octubre de 2022] Disponible a: https://boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

[11] BOE. *Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* [Document en línia] 4-11-2015 [Consultat el 6 d'octubre de 2022] Disponible a: https://www.boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

[12] BOE. *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* [Document en línia] 4-5-2022 [Consultat el 6 d'octubre de 2022] Disponible a: https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

a través del plantejament comú de principis bàsics, requisits mínims, mesures de protecció i mecanismes de conformitat i monitorització.

Tot plegat, situa a l'Ajuntament del Masnou, en una necessitat de protegir els seus actius digitals, millorant la seva estratègia en ciberseguretat, a la vegada que, començar a dotar a l'Ajuntament de les eines necessàries per en un futur pròxim, poder-se adequar a l'ENS i obtenir la certificació corresponent.

Per a dotar l'Ajuntament d'aquestes característiques, aquest treball és centrarà en implementar les mesures de conformitat, i monitorització a través d'un programari del tipus SIEM i totes aquelles eines complementaries que siguin necessàries.

D'aquesta forma es dotarà a l'Ajuntament d'una eina que permetrà la realització de les següents tasques:

- Preventiva/correctiva: Mitjançant el bastionat dels equips i la correcta configuració dels sistemes verificant el compliment de les normatives existents. A la vegada que realitzant periòdicament anàlisis de vulnerabilitats conegudes en els sistemes per la seva posterior correcció.

- Proactiva: Mitjançant la recol·lecció de logs i anàlisi dels sistemes en temps reals per identificar comportaments anòmals. El sistema ha de permetre reaccionar de forma automatitzada a esdeveniments que siguin coneguts com a incidents de seguretat.

- Informativa: Notificant i mostrant tota la informació obtinguda de forma gràfica i comprensible per a poder realitzar el seu estudi i prendre les decisions pertinents.

1.2. Objectius del Treball

El principal objectiu del treball, és dotar a l'Ajuntament de major seguretat davant les creixents amenaces en l'ús de les TIC.

Per a fer-ho, s'han definit quatre etapes: La primera fase, en que es redacta i es planteja el pla de treball referent a la resta de fases, la segona de recerca i anàlisi, per tal de recollir els requisits funcionals de la solució, la tercera, encarregada en la integració i desenvolupament, adreçada a desplegar la solució de SIEM escollida i aquelles eines necessàries, per a complir els objectius proposats segons els requisits establerts, i la quarta i última etapa, de conclusions i treballs futurs, on es revisarà si s'ha aconseguit els objectius establerts, i es realitzarà una síntesi de possibles treballs a efectuar en un futur per a millorar o complementar les solucions proposades.

1. Fase de redacció del Pla de treball

- Es tracta de realitzar l'esquelet estructural del treball i assentar-ne les bases sobre on es construirà la resta de fases.

2. Fase de recerca i anàlisi:
    - Analitzar tant els serveis que ofereix actualment l'Ajuntament a la ciutadania, com les eines necessàries per a que els empleats realitzin la seva feina.
    - Estudiar les principals amenaces d'aquests actius i mesures per a mitigar-les
    - Identificar els requisits específics de cara a determinar la solució SIEM que més s'adeqüi a dites necessitats.
    - Identificar les necessitats complementaries per a complir amb el model d'infraestructura desitjat, format pels següents components:
        - Firewall + IDS com a seguretat perimetral.
        - HIDS en cada actiu essencial de la xarxa.
        - SIEM que permeti la correlació d'esdeveniments en temps real i la posterior explotació de dades.

3. Integració i desenvolupament:
    - Dissenyar un ecosistema, que integri el SIEM escollit amb els diferents actius de l'Ajuntament i d'altres eines vinculades.
    - Implementar totes les eines i configuracions necessàries pel seu desplegament en l'ecosistema.
    - Integració de les eines ja existents.

4. Conclusions i treballs futurs:
    - Verificar les diferents funcionalitats del SIEM mitjançant un conjunt de probes
    - Estudi del camí a recórrer en un futur per a millorar i enfortir tot el sistema de seguretat
    - Valoració de si s'han complert els objectius fixats en un inici.

De forma inherent a l'objectiu principal, se'n desglossen un seguit d'objectius derivats com ara:

- Millorar la seguretat i resiliència general de l'empresa.
- Desenvolupar la capacitat de detecció i resposta davant dels incidents en la seguretat informàtica.
- Ser capaços de generar intel·ligència en les eines de seguretat que permetin gestions automatitzades.

Dels que n'obtenim una sèrie d'objectius secundaris:

- Analitzar les diferents tipologies i tecnologies d'eines SIEM en el mercat
- Seleccionar-ne una per a la implantació en l'Ajuntament que compleixi amb els requisits de les seves infraestructures.
- Implantar l'eina escollida, estudi de les seves possibilitats i de la forma d'ús i configuració.

- Planificar i portar a terme un seguit de proves per verificar el funcionament del sistema.

1.3. Impacte en sostenibilitat, ètic-social i de diversitat

De cara a l'execució d'aquest treball, s'ha de tenir en compte que una eina SIEM, es basa en l'anàlisi profund dels registres que li subministren els diferents equips de la xarxa. És per això, que la gran majoria d'aquests registres, contindran dades dels usuaris que utilitzin els serveis que ofereix l'Ajuntament i, en molts casos, poden contenir dades de caràcter personal. És per això que és important garantir que l'ús d'aquestes dades només correspondrà a la cerca d'activitats anòmales dins dels sistemes i a l'estudi de possibles atacs informàtics i, en cap cas, se'n farà cap altre tipus d'ús.

De cara a garantir la transparència del servei, és important que els treballadors interns de l'Ajuntament, firmin un document de consentiment, envers a l'ús de la xarxa i a que son coneixedors del fet que es realitzarà inspecció del esdeveniments que succeeixin en els seus equips de treball i en el trànsit que generin cap a la xarxa i, en concret, cap a Internet.

Pel que fa als ciutadans que utilitzin els serveis electrònics de l'Ajuntament, han d'estar informats del fet que per la seguretat del sistema es realitzaran aquestes tasques d'inspecció, a la vegada que sempre que es treballi o es demanin dades personals, segons els RGPD, han de donar el seu consentiment explícit i autoritzar l'ús de dites dades personals únicament per la finalitat que n'han donat el consentiment.

Pel que fa als tècnics encarregats de realitzar les feines de gestió i anàlisi de l'eina SIEM i de tots els components que integren els sistemes de l'Ajuntament, han de tenir una vinculació amb l'ajuntament, que garanteixi la confidencialitat de totes les dades i el comportament ètic en totes les seves actuacions.

1.4. Enfocament i mètode seguit

La planificació i desenvolupament d'aquest projectes, es realitzarà de forma seqüencial seguin el clàssic model Waterfall o en cascada. Aquest treball s'estructura en 4 fases on es realitzaran tasques de forma seqüencial, una darrera l'altre i que culminaran en fites, corresponents a les diferents entregues indicades al pla docent.

Aquestes tasques comencen en la fase inicial de planificació del pla de treball, on s'ha definit el context i l'objectiu del treball, planificat el temps per a cada tasca i realitzat l'estudi de l'estat de l'art.
La fase 2 que consisteix en la recerca i anàlisi per identificar les necessitats i requisits, i escollir les solucions més adients.
La fase 3 que serà el disseny i implementació de les eines escollides dins del sistema.

I finalment la Fase 4 que consta de la fase de probes de la solució, la valoració dels objectius, l'estudi del futur de la implementació i l'elaboració de la memòria final.

Finalment també es realitzarà la vídeo presentació del treball i la posterior defensa del TFM.

1.5. Planificació del Treball

Per la realització d'aquest treball, s'haurà de contar amb la pròpia infraestructura de l'Ajuntament, per la instal·lació dels diferents sistemes necessaris per la solució SIEM escollida, a la vagada que s'haurà de contar amb un configuració que contingui els següents elements.

- Firewall + IDS com a seguretat perimetral.
- HIDS en cada actiu essencial de la xarxa.
- SIEM que permeti la correlació d'esdeveniments en temps real i la posterior explotació de dades.

En cas de que algun dels components ja hi consti a l'Ajuntament s'integrarà amb el nou sistema SIEM, i en cas de que no hi sigui es buscarà la millor solució per incorporar-ho a la implementació.

El conjunt de tasques a desenvolupar per la realització del projecte, s'engloben en 4 grans fases, totes elles indispensables entre sí. La finalització de cada una d'aquests grans tasques es conclou amb l'entrega de la prova d'avaluació continuada (PEC) corresponent.

Segons el pla d'estudis, l'assignació de crèdits de l'assignatura del Treball final de màster, correspon a un esforç de 12 crèdits, que segons la correspondència d'hores crèdit a l'any 2022, de 25 hores per crèdit, li correspon un esforç de 300 hores lectives.

Per a la comptabilització d'aquests esforç, s'ha calculat que les jornades de treball son de dilluns a divendres, respectant els descansos setmanals de 2 dies aplicats en dissabte i diumenge, i tots els festius corresponents al calendari laboral 2022/2023 de la comunitat autònoma de Catalunya. A la vegada, s'ha de tenir en compte que la dedicació del personal al projecte serà de mitja jornada, és a dir 4 hores per jornada.
Com que els recursos assignats al conjunt del projecte, és de només d'una persona, per a saber el còmput d'hores de cadascuna de les 4 fases que corresponen el projecte o de les seves subtasques, s'haurà d'aplicar la formula següent:

Cost total = Jornades * 4hores

Les tasques per a dur a terme el projecte seran les següents:

1. Pla de treball - Fase Inicial (12 jornades - 48h): És la fase inicial on es planteja quin son els objectius del projecte i serveix per dotar d'estructura i planificació a la resta d'apartats, a la vegada que ens permet elaborar una primera aproximació a la temàtica de l'estudi que s'efectuarà.

    1.1. Context i justificació del Treball (5 jornades - 20h):
    Descripció de la situació en que s'engloba el projecte i el perquè de la seva necessitat.

    1.2. Objectius del Treball, Enfocament i mètode seguit (3 jornades - 12h): Explicació dels diferents objectius, primaris i secundaris i de la metodologia que es seguirà per a complir dits objectius.

    1.3. Planificació del Treball (1 jornada - 4h):
    Descripció de les diferents tasques i cronograma de l'esforça a dedicar per cada una d'elles.

    1.4. Estudi de l'estat de l'art (3 jornades - 12h): Breu estudi de l'objecte del treball i el marc en que s'engloba.

2. Fase de recerca i anàlisi - Fase 2 (18 jornades - 72h): En aquest apartat, es realitzarà un estudi extens de la situació actual de l'Ajuntament, tant dels seus actius com de les principals amenaces i s'avaluarà les diferents eines SIEM disponibles en el mercat per a escollir-ne una per a la implementació.

    2.1. Estudi dels actius de l'Ajuntament (7 jornades - 28h):
    Descripció i estudi dels diferents actius de l'Ajuntament.

    2.2. Estudi de les principals amenaces i mesures de mitigació (3 jornades - 12h):
    Identificació de les principals amenaces a nivell tecnològic que existeixen actualment.

    2.3. Identificar els requisits específics de la solució (3 jornades - 12h):
    Enumerar les diferents característiques imprescindibles a complir per part de l'eina SIEM escollida.

    2.4. Elecció del sistema SIEM i solucions complementaries (5 jornades - 20h):
    Estudi de les diferents eines SIEM que hi ha disponibles al mercat, les seves característiques i elecció de l'eina a implementar a l'Ajuntament.

3. Integració i desenvolupament - Fase 3 (19 jornades - 76h): En la tercera fase, es dissenyarà la integració de l'ecosistema actual de l'Ajuntament, amb l'eina escollida. Un cop realitzat el disseny, es procedirà a la seva implementació i integració amb el Firewall i altres eines preexistents.

    3.1. Disseny de l'ecosistema d'integració (5 jornades - 20h):
    Segons l'estudi de l'ecosistema de l'Ajuntament, es realitzarà les modificacions pertinents per a la integració de la solució SIEM.

3.2. Implementació de les diferents eines (8 jornades - 32h):
Realització de les tasques d'instal·lació i implementació de l'eina.

3.3. Integració de les eines ja existents a l'Ajuntament (6 jornades - 24h):
Configuració i modificació de l'eina SIEM i els equips de l'Ajuntament per a la seva integració.

4. Validació del funcionament del sistema - Fase 4 Part1 (15 jornades – 60h)
   4.1. Preparació i execució del joc de proves (12 jornades – 48h)
   Disseny de les proves i realització d'elles per avaluar el funcionament de l'eina.

   4.2. Anàlisi dels resultats(3 jornades – 12h)
   Breu descripció dels resultats obtinguts.

5. Conclusions i treballs futurs - Fase 4 Part2 (6 jornades – 24h)
   5.1. Redacció de les conclusions finals (3 jornades – 12h)

   5.2. Identificació dels treballs a futur de la implementació (3 jornades – 12h)
   Breu descripció dels treballs que no s'han pogut implementar en aquest projecte, o que serien una bona forma de continuar per seguir millorant la seguretat, però que no formen part de l'actual projecte.

6. Vídeo presentació (4 jornades – 16h):
   Realització d'un vídeo amb la presentació tant del concepte com de la part pràctica del projecte.

7. Defensa del TFM

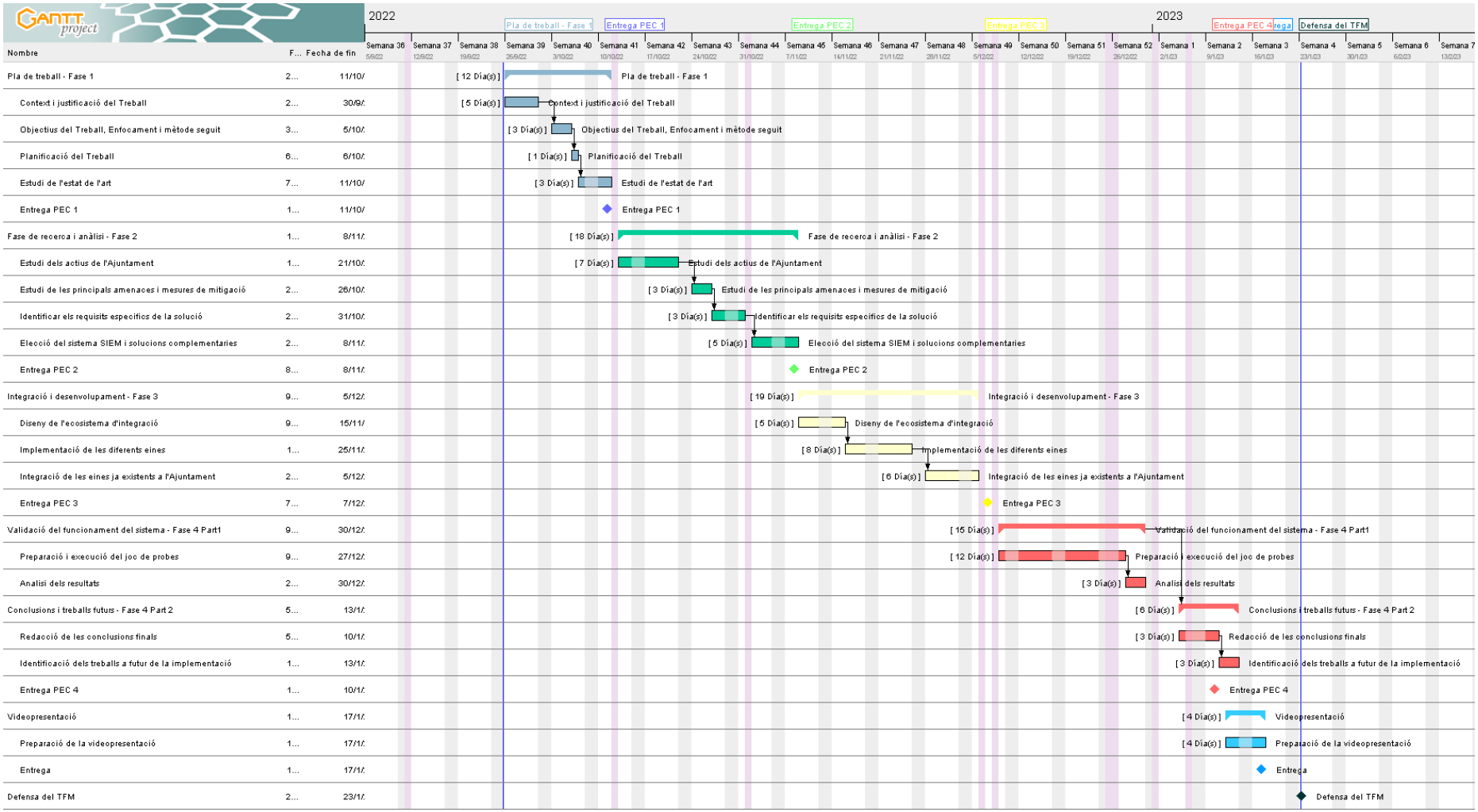


Figura 3: Cronograma de les tasques a realitzar en el projecte

1.6. Breu sumari de productes obtinguts i costos associats

Aquest treball estarà composat per els següents continguts:

- Memòria (aquest document).
- Annex amb les guies d'instal·lació dels diferents productes escollits.
- Vídeo presentació.

Tanmateix de l'elaboració d'aquest TFM, se'n derivaran un seguit de costos associats:

- La instal·lació del programari escollit, es realitzarà en una o més màquines virtuals, que s'implementaran dins de les infraestructures actuals de l'Ajuntament del Masnou. És per això, que el cost associat d'aquests equips, és difícil de ser calculat, ja que queda com a una part proporcional segons els recursos (us de CPU, RAM i espai d'emmagatzematge) que els elements que englobin aquest projecte necessitin. És per això que el més important és saber d'on partim, el conjunt global de recursos i el seu cost. Aquests recursos, van ser adquirits mitjançant una licitació pública el març del 2021 i el seu cost en va ser el següent:

Marca	Descripció	Funció	Valor contable
HP	Proliant DL360 G10	Host VM	10.087,37 €
HP	Proliant DL360 G10	Host VM	10.087,37 €
HP	HPE Nimble Storage AF20 All Flash	Cabina emmagatzematge	49.514,47 €
HP	HP 1950 12XGT 4SFP+	Switch iSCSI	1.285,83 €
HP	HP 1950 12XGT 4SFP+	Switch iSCSI	1.285,83 €
ZENITH	SAI 6000VA	Sistema d'Alimentació	2.652,26 €
Synology	NAS RackStation RS2416RP+	Backups	1.960,53 €
		Total	**76.873,66 €**

A més del cost d'adquisició, se n'hauria de calcular el cost proporcional del consum energètic i de manteniment dins del conjunt de costos del propi CPD.

- Cost del llicenciament del programari, en cas de que no sigui Opensource. (Com que el programari escollit ha estat Wazuh, el cost en llicenciament ha estat de 0€ i el sistema operatiu sobre el que funciona ha estat Ubuntu Server que també és de llicenciament opensource i per tant a cost 0).

1.7. Estudi de l'art

Com que la finalitat d'aquest treball, és la implantació d'un sistema SIEM en l'Ajuntament del Masnou. En aquest apartat, es realitzarà un estudi del que és i quines funcionalitats té, una eina del tipus SIEM.

1.7.1. Que és un SIEM?

Començant per el seu nom, SIEM, son les sigles de Security Information and Event Management, és a dir, Informació de la Seguretat i Gestió d'Esdeveniments i, la seva finalitat, és proporcionar una eina de resposta ràpida i precisa per detectar i respondre davant qualsevol amenaça dels sistemes informàtics que gestioni.

Com el seu nom indica, en realitat combina dos tipus de solucions de seguretat diferents, per una banda un sistema SIM (Security Information Managment) i per l'altra un sistema SEM (Security Event Managment). El sistema SIM s'encarrega de la recollida i emmagatzematge de dades, i el seu posterior processament per a ser analitzades i generar informes automatitzats. En canvi el SEM, utilitza les dades recollides per a establir correlacions d'esdeveniments entre elles, per detectar, i reaccionar de forma automatitzada a activitats inusuals en el sistema.

1.7.2. Quins funcionalitats té?

La funcionalitat principal d'un SIEM, és la recol·lecció i emmagatzematge de registres de tot tipus de dispositius i/o subsistemes que intervinguin en el sistema informàtic. Tots aquests registres, un cop processats, s'emmagatzemen de forma centralitzada en una base de dades per a poder realitzar una anàlisi profunda, i així detectar tendències i patrons de comportament, que permetin diferenciar d'aquells que no siguin habituals.

Les principals característiques que disposa un bon sistema SIEM, per a la seguretat i resposta ràpida d'una empresa són:

- Identificar entre amenaces reals i falsos incidents.
- Monitoritzar de forma centralitzada totes les amenaces potencials.
- Redirigir l'actuació al personal qualificat per a resoldre-la.
- Aportar un major grau de coneixement sobre els incidents per a facilitar la seva resolució.
- Documentar tot el procés de detecció, actuació i resolució.
- Complir amb les normes i legislacions vigents en qüestió de protecció de dades i seguretat.

1.7.3. Quins beneficis aporta el seu ús?

Permet detectar les amenaces i respondre davant elles en temps real, fins i tot, atacs que poden escapar a les mesures de seguretat més convencionals, ja que estem davant un sistema de seguretat proactiu, basat en machine learning.

Una altra dels avantatges del sistema SIEM, és que permet reduir la càrrega de treball dels responsables de seguretat informàtica, ja que produeix informes de manera automatitzada, que poden interpretar-se molt més ràpidament, sense necessitat d'haver d'analitzar tota la informació que genera cada sistema, equip o dispositiu de xarxa.

A més, el sistema SIEM guarda la informació durant llargs períodes de temps, la qual cosa permet, en cas necessari, analitzar tot el procés d'un atac: abans que ocorri, quan està ocorrent i després d'haver ocorregut, la qual cosa ajuda, d'una banda, a millorar el sistema de detecció, i per un altre, serveix com a eina per a l'anàlisi forense informàtic d'un incident de seguretat.

2. Estudi, recerca i anàlisis

Per poder decidir quina eina de SIEM és la que més encaixa en els requisits actuals de l'Ajuntament i, poder implementar una solució integrada i adaptada a les infraestructures actuals, es farà un detall dels actius que disposa l'Ajuntament, quins d'aquests són el puntal del model de negoci, i identificar-ne les principals amenaces a què estan exposats, en l'àmbit de la seguretat de les TIC i quines mesures podríem efectuar per mitigar-les.

Tot aquest estudi ens ajudarà a identificar els requisits concrets de la implementació que s'efectuarà i es dissenyarà en els apartats posteriors.

2.1. Actius de l'ajuntament i infraestructura que els subministra.

- <u>Actius del model de negoci:</u>

L'administració pública, i en concret l'administració local, com és l'Ajuntament de Masnou, es basen en oferir una sèrie de serveis a la ciutadania, a la vegada que reben constantment peticions i comunicacions referents a temes molt variats i que l'Ajuntament gestiona amb la dedicació del seu personal, i el lideratge de l'estructura política.

Totes aquestes peticions, són canalitzades pel servei de l'Oficina d'Atenció al Ciutadà, que utilitza l'eina del Registre d'Entrada com a numeració única per a identificar-les, i que dites peticions poden ser introduïdes per un gestor, en format presencial o pel ciutadà mateix, a través del web de tramitació de la Seu Electrònica.

És, per tant, el canal principal d'entrada del ciutadà amb l'Ajuntament, però a la vegada també és una de les eines principals de comunicació oficial, amb l'eina de Registre de Sortida i la seva notificació (tant sigui en paper com electrònica).

Totes aquestes peticions/tramitacions que l'Ajuntament gestiona, es basen en la utilització d'un gestor d'expedients, eina que vincula i engloba, tant les entrades pel Registre d'Entrada, com la seva tramitació, segons si s'efectuen els informes corresponents per cada tècnic gestor, o les aprovacions per Decret, propostes de la Junta de Govern Local, o a l'òrgan superior com és el PLE, i les posteriors sortides pel Registre de Sortida per la comunicació amb el ciutadà.

Un altre dels canals més necessaris per al dia a dia del treballador de l'Ajuntament, per poder realitzar la seva feina, és l'ús del correu electrònic.

Actualment, l'Ajuntament utilitza un servidor de correu Exchange 2010, que està configurat en les instal·lacions de l'edifici principal d'aquest. Com que la versió que s'utilitza és una versió molt antiga, que ja està discontinuada per Microsoft, hi ha programada una migració al núvol per utilitzar els serveis d'Exchange 365, la qual cosa, serà un punt important a l'hora d'escollir l'eina SIEM a implementar i que ha de poder gestionar, tant serveis "On-premise" com serveis al núvol.

A més de les comunicacions amb el ciutadà, la infraestructura TIC de l'Ajuntament, ha d'oferir, diferents eines per a cada departament per a poder realitzar les seves tasques de la forma més eficient possible.

Cada treballador disposa d'un equip de treball, connectat a la xarxa local i registrat al domini, amb les eines necessàries d'un punt de treball, com són les eines ofimàtiques, un client d'antivirus corporatiu i accés a la unitat de fitxers compartits, a més, depenent de les necessitats de cada departament, disposaran d'accés a les diferents eines ofertes pels servidors d'aplicacions.

La granja de servidors que disposa l'Ajuntament, es basen en un sistema de virtualització de la marca VMWare, que consta de redundància per a evitar tindre cap punt de fallada únic, i que ofereix flexibilitat i recursos per a poder ampliar i granularitzar les necessitats en servidors, tant d'aplicacions com d'altres serveis.

Per altra banda, els treballadors disposen de l'opció de treballar des de fora de les instal·lacions que formen la xarxa local, mitjançant la connexió per VPN i l'ús del doble factor d'autentificació.

- Infraestructura, equipament i logística actual:

Pel que fa a instal·lacions, l'Ajuntament es basa en un edifici principal, que seria la Casa de la Vila, i un seguit d'edificis de diferents mides. Tots ells units per una xarxa de fibra òptica propietària de l'Ajuntament.

En l'edifici principal, és on s'ubica el centre de processament de dades (CPD), que consta de diverses connexions a internet amb FTTH per als diferents serveis, unides a un tallafocs de la marca Sonicwall i al sistema de teletreball també de Sonicwall. A la vegada disposa d'un armari de telecomunicacions, que consta d'un repartidor principal que uneix totes les instal·lacions en fibra i les comunica amb el tallafocs i la resta de serveis i un repartidor de la xarxa del propi edifici que reparteix entre cada planta de l'edifici i aquests a la vegada connecten amb cada estació de treball.

Pel que fa a l'armari de servidors, es basa en un sistema de virtualització de servidors, amb el programa de gestió de VMWare versió 7 i compost per 2 servidors host HP ProLiant DL360 Gen10 amb doble processador Intel(R) Xeon(R) Silver 4215R CPU @ 3.20GHz i 380 GB de memòria RAM, cabina d'emmagatzematge Nimble amb 20TB d'espai net i connectivitat mitjançant switchos HP 1950 12XGT 4SFP+ apilats en stack per oferir la màxima redundància.

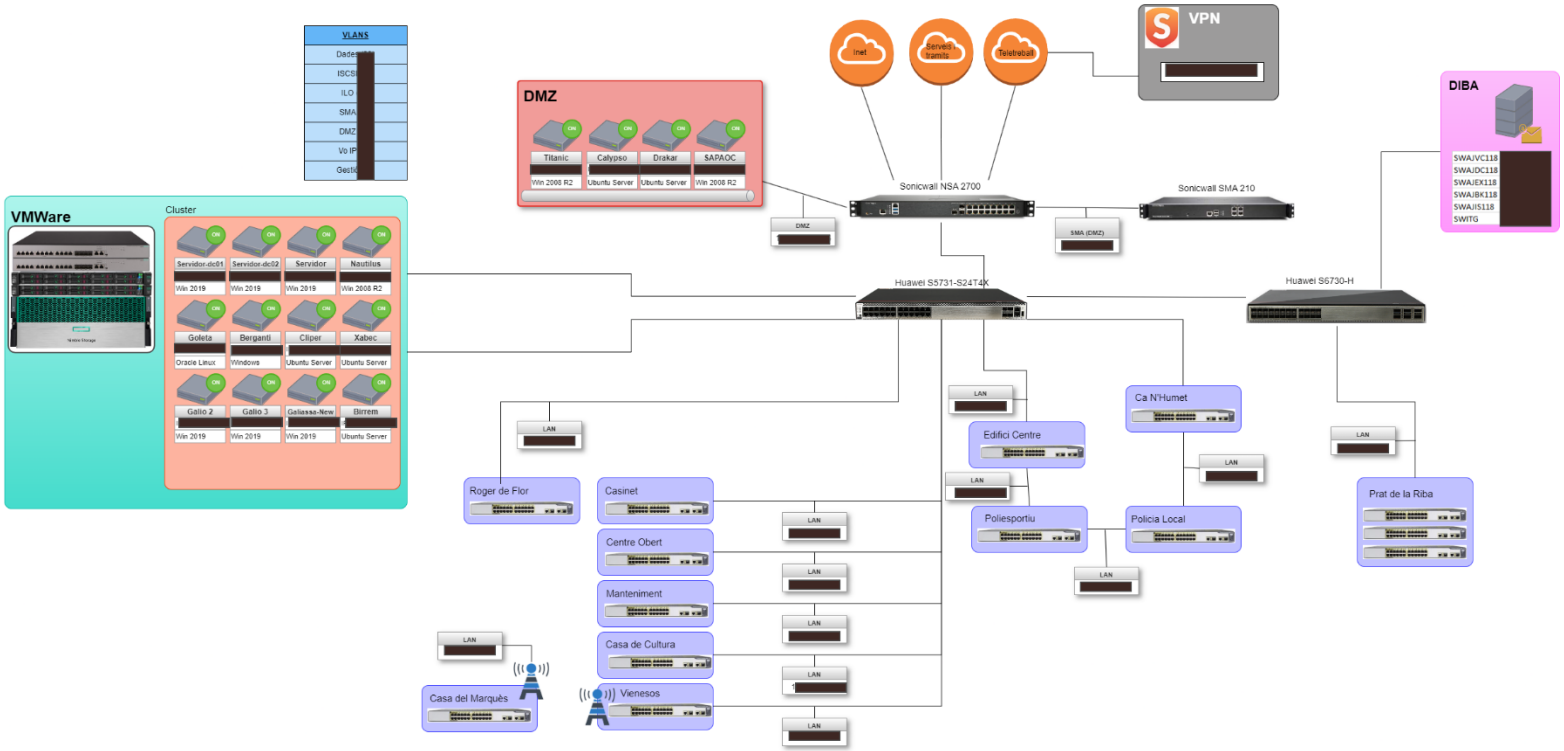


Figura 5: Diagrama de l'arquitectura de xarxa de l'organització

Per seguretat, s'han anònimitzat tots els adreçaments en el TFM.

2.2. Principals amenaces i mesures de mitigació

Vist els principals actius de que disposa l'Ajuntament, (Web Municipal, Servei de correu electrònic, Servei de tramitació electrònica, Gestió d'expedients, Servidor d'emmagatzematge de fitxers, Equips clients, Altres servidors d'aplicacions), que a la vegada, tots ells se sustenten sobre uns equips de virtualització que ofereixen tota la infraestructura de servidors, uns intercomunicadors de xarxa que uneixen tots els equips clients i un tallafoc amb connexió a Internet per una FTTH que permet la comunicació amb l'exterior i permet l'ús de la tramitació per part del ciutadà.

Podem passem a tenir en compte el que serien els principals factors d'atac i amenaces a què estan exposats els actius informàtics, tant els que estan a disposició de la ciutadania, publicats a Internet, com les eines dels mateixos treballadors de l'Ajuntament.

Podem desglossar les amenaces segons el diferents àmbits d'actuació:

L'àmbit de la xarxa local, en els equips dels usuaris, el principal factor d'atac és:

- Correu electrònic: Mitjançant el correu, els atacants envien fitxers maliciosos per infectar els equips i aconseguir el control d'aquests. Un cop en tenen el control, miren de dur a terme desplaçaments laterals i/o desplaçaments verticals per augmentar els privilegis i així poder accedir a les parts del sistema que contenen més dades i poder abastir el màxim possible en el seu atac.

  També s'utilitza el correu per a realitzar tècniques de Phising on poder redirigir a l'usuari cap a un web maliciós i poder robar-li les seves credencials.

  Les formes de mitigar aquests riscos, són la implementació d'eines anti SPAM que eviti que l'usuari rebi aquests correus.

  Eina d'anàlisi del correu i els fitxers del sistema local, ja sigui un sistema d'antivirus del lloc de treball o alguna eina més sofisticada que analitzi el tràfic de dades.

  I el filtrat, per evitar l'accés, a tots aquells dominis i IPs que estiguin identificats com a maliciosos.

  Tot i aquestes eines automatitzades, l'eina més efectiva és la formació dels usuaris i la conscienciació per tal que evitin caure en els paranys que li puguin fer.

- Internet: De la mateixa forma que amb el correu electrònic, quan els usuaris estan navegant per planes web, moltes vegades poden estar donant informació o permeten que s'executin procediments de webs malicioses. La forma de mitigar aquests atacs, és amb una eina d'anàlisi del tràfic de xarxa, ja sigui a nivell de l'equip local o en l'accés a Internet del tallafocs corporatiu, que permeti limitar l'accés a les planes malicioses

i evitar l'execució del codi que contenen. Tot i això, la millor eina és la conscienciació i formació dels usuaris.

Dins d'aquest àmbit, i utilitzant els factors d'atac que s'han comentat, podem trobar molt tipus de programari maliciós diferent:

- Virus: Són el programari típic per infectar un dispositiu i fer que aquest funcioni malament.

- Cucs: Són programes que permeten infectar dispositius dins d'una xarxa, sense la intervenció de l'usuari, i en molts casos, son els precursors d'altres tipus de programari maliciós, com el ransomware.

- Troians: Són programes que s'instal·len en els equips, però estan dissenyats per obrir ports, i permetre l'accés al dispositiu per algun altre programari i així aconseguir el control d'aquest. Tot això passant desapercebuts per l'usuari.

- Ransomware: El programa més actual i més temut per totes les organitzacions i usuaris en general. És un programa que xifra tota la informació a la qual té accés, i posteriorment en demana un rescat per a subministrar la clau de desxifrat.

- Keyloggers: Solen ser programes que van acompanyats o a correlació d'altres dels programes maliciosos que s'ha comentat. Serveixen per registrar la informació que s'introdueix per teclat i així obtenir usuaris, contrasenyes i informació confidencial.

L'àmbit dels serveis que s'ofereixen als ciutadans, on els principals atacs són:

- DDoS: L'atac per denegació de serveis distribuïts, es produeix quan un servidor rep moltes peticions d'accés, se sobrecarrega el sistema i fa que el servei deixi de funcionar correctament. Per tal de mitigar aquest atac, és important que existeixi un sistema de gestió de les peticions malicioses i les filtri de les peticions correctes, per evitar que col·lapsi el sistema.

- Vulnerabilitat de contrasenyes: Tant amb la implementació del teletreball, com amb l'accés a qualsevol servei mitjançant usuari i contrasenya, és susceptible que l'atacant esbrini aquesta contrasenya i, per tant, aconsegueixi l'accés no desitjat als sistemes. A més si aquesta contrasenya no és prou complexa, es pot patir un atac per força bruta o per diccionari de contrasenyes habituals i que el sistema quedi exposat. Per mitigar aquest risc, la millor forma és evitar l'accés mitjançant usuari i contrasenya, utilitzant algun altre sistema més segur, o en tot cas, habilitar l'autentificació amb doble factor (2FA), que permet verificar en cada accés que l'usuari és qui diu ser.

- Vulnerabilitat dels sistemes: Els sistemes i aplicacions, sempre tenen algun error en el disseny, estructura o codi, que generen alguna vulnerabilitat. Ja sigui per errròrs en la configuració, o en la gestió dels

recursos i l'accés que en fan, errors en els sistemes de validació, que permeten saltar-se la seguretat, errors en els accessos als fitxers o permisos dels usuaris, etc ... Els atacants, disposen de bases de dades, on consta les versions dels sistemes o aplicacions que són vulnerables, i les fan servir per explotar aquestes vulnerabilitats. Per tal de mitigar aquest risc, és molt important verificar constantment si els sistemes disposen d'actualitzacions per evitar vulnerabilitats conegudes, a la vegada que és molt útil consultar les bases de dades de vulnerabilitats per si existeix alguna, que encara no té actualització que la resolgui, però es pot mitigar el problema variant la configuració.

- Mal ús del programari: A més de les ja comentades, també existeix la possibilitat dels atacs directament amb un mal ús de les aplicacions. És a dir, l'ús de l'eina, però per una tasca que no és per la que ha estat dissenyada. Dins d'aquests atacs, podem trobar les injeccions SQL, que permeten accedir a parts del sistema de base de dades o a fitxers que en cap cas haurien de ser d'accés per l'ús de l'aplicació. O un altre tipus de mal ús seria l'execució de comandes de llocs creuats (Cross-site scripting o XSS), que permet l'execució de codi directament en l'aplicació web i obtenir resultats i/o accessos inesperats.

2.3. Identificar els requisits específics de la solució

Per poder escollir la solució de SIEM més adequada per l'Ajuntament del Masnou, s'hauran de complir els requisits següents:

- Que permeti la implantació en els sistemes de l'Ajuntament, suportant la tecnologia de virtualització VMWare.
- Que permeti monitorar la majoria dels dispositius de xarxa i dels sistemes operatius que hi ha actualment en ús (Windows server edicions 2008/2019, Ubuntu Server 20 o superior, Firewall Sonicwall, etc.).
- Que permeti securitzar el tràfic entre els dispositius recol·lectors de la informació i l'eina de gestió central. A la vegada que aquesta eina eviti els accessos anònims o comptes genèrics en el seu ús.
- A la vegada ha de permetre la monitorització de recursos en el cloud de Microsoft, per securitzar la futura migració del sistema de correu electrònic al núvol.
- Que ajudi a complir amb la normativa reguladora vigent, com és el RGPD o el ENS.
- Que pugui detectar vulnerabilitats en els diferents sistemes.
- Que s'integri amb l'eina de monitoratge de l'Ajuntament (Zabbix).
- Que permeti la detecció de malware, atacs o integritat de fitxers.
- Que permeti l'actuació en diferents supòsits davant d'atacs, de forma desatesa i automatitzada, tot generant les corresponents notificacions als gestors.
- Que permeti l'ús de l'eina i el seu desplegament per l'equip actual d'informàtics en plantilla de l'Ajuntament, i que en cap cas obligui a la modificació del pressupost del 2022, que ja està aprovat i compromès en la seva totalitat.

2.4. Quines eines SIEM existeixen en el mercat?

En l'actualitat existeixen moltes eines catalogades com a SIEM, tot i que no totes actuen de la mateixa manera o ofereixen les mateixes funcionalitats. Si ens fixem en la classificació que en fa Gartner per l'any 2022, n'estudiarem els que segons ells estan millor posicionats al mercat, a la vegada que també tindrem en compte les opcions de llicència Open Source, i els nous models de processament al núvol, que en el quadrant no hi son contemplats.

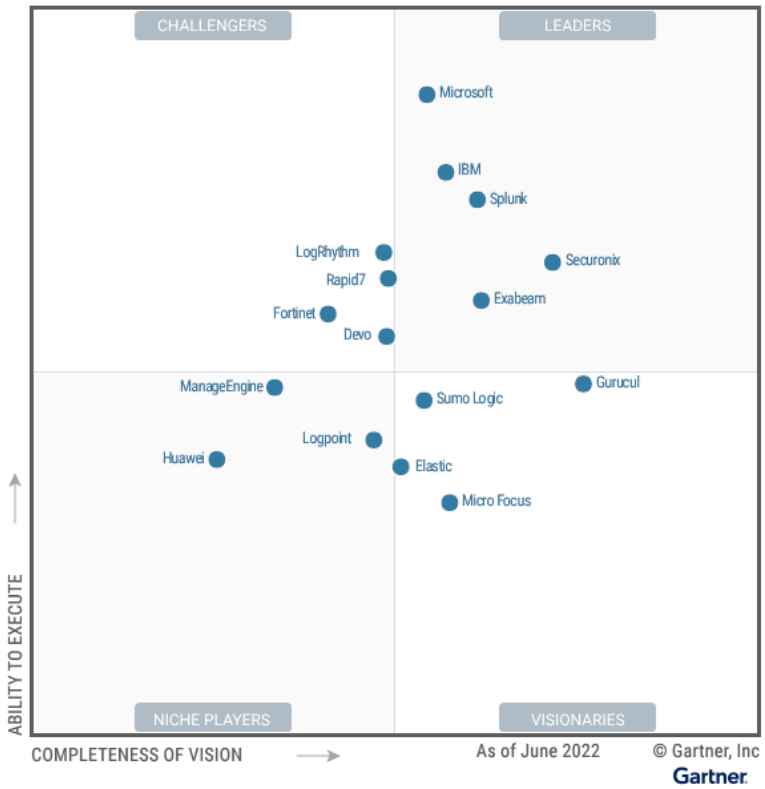


Figura 4:[13] Quadrant màgic de Gartner per a solucions SIEM (Juny 2022)

- **Devo:** Aquesta eina que funciona en el núvol, ha estat desenvolupada per una petita "startup", i ha resultat la gran novetat del 2022, quedant com la més valorada per part de Gartner.

  Avantatges: No és necessària disposar de la infraestructura pròpia per el seu funcionament, i permet que sempre es disposi de l'eina en la seva última versió i funcionalitats. Està molt ben valorada per Gartner i segons la pròpia empresa disposen de la millor eina de cara a optimitzar el funcionament del SOC.

  Desaventatges: És una empresa molt petita i de nova creació, que no disposa del mercat ni l'experiència de les grans companyies del sector.

[13] **GARTNER**: *Magic Quadrant for Security Information and Event Management*. Octubre de 2022 [Web] [Consultat el 13 d'octubre de 2022] Disponible a: https://www.gartner.com/doc/reprints?id=1-2BDC4CDW&ct=221010&st=sb

- **IBM Security QRadar:**
  Es tracta d'un dels sistemes SIEM més complets que existeixen. Compta amb més de 400 mòduls que són capaços de suportar una gran quantitat de càrrega, podent gestionar milions d'esdeveniments al dia. Aquest sistema aporta solucions intel·ligents perquè els equips de seguretat puguin actuar de manera immediata i evitar o reduir l'abast dels incidents. Seria l'equivalent a l'eina SAP en sistema SIEM.

  Avantatges: És una eina molt implantada, amb anys d'experiència i amb una de les empreses més grans del sector darrera. El fet de que tantes empreses la utilitzin fa que l'eina cada vegada sigui millor.

  Inconvenients: És una eina molt potent però pensada per a empreses grans, que tenen un alt pressupost destinat a la seguretat de les seves infraestructures i el seu preu així ho denota.

  https://www.ibm.com/uk-en/qradar?utm_content=SRCWW&p1=Search&p4=43700068018089518&p5=e&gclsrc=ds

- **LogRhythm:**
  Es un dels SIEM per excel·lència, que va començar en una empresa StartUp i que s'ha posicionat com un dels principals actors en el sector. Han sabut evolucionar els últims anys, passant el seu model com a servei al núvol i oferint plans de tractament de dades il·limitades, i adquirint empreses per dotar al seu programa de funcionalitats extres.

  Avantatges: És un dels grans SIEM del mercat que ha quedat guanyador del quadrant màgic de Gartner els últims 9 anys.

  Inconvenients: S'haurà de veure si en els pròxims anys és capaç de lluitar contra els grans del processament de dades al núvol, com són, Microsoft, Amazon o Google.
  Tot i que ofereix plans de processament de dades il·limitats, el seu preu no està a l'abast de tots els pressupostos.

  https://logrhythm.com/

- **Splunk Enterprise Security:**
  Splunk proporciona operacions de seguretat millorades com panells de control personalitzables, descobriment d'actius, anàlisi estadística i revisió, classificació i recerca d'incidents. Té característiques de gestió d'alertes, puntuació del risc, etc.

  Avantatges:
  - És una eina molt potent, i pot treballar amb qualsevol tipus de dada, tan en local com en el núvol.
  - Utilitza la intel·ligència artificial per a automatitzar les taques i facilitar la detecció d'incidents.

  Inconvenients:

- És una eina que no està pensada per entorns petits o poc tecnificats i necessita de formació especifica per la seva posta en marxa.
- L'elevat cost que té i el fet de ser una eina pensada per a grans empreses.

https://www.splunk.com/

- **Elastic Security:**

  És una evolució del que va començar essent un programa de software lliure, que es basava en la ràpida indexació de milers en el seu sistema de base de dades i la generació flexible de quadres de control que explotaven aquestes dades. Aquest programa se l'anomenava ELK i estava composat per Elastic search, Logstash i Kibana.
  En l'actualitat, el model ja no és software lliure i ofereix una evolució dels quadres de control de Kibana per a la gestió de la seguretat i la resposta a incidents.

  Avantatges: És una eina que ha anat evolucionant amb el temps per guanyar especialització.

  Inconvenients: No disposa de les eines que poden tenir els grans actors del mercat.

  https://www.elastic.co/es/security/siem

- **Wazuh:**

  Wazuh és un sistema de detecció d'intrusos basat en host de codi obert i lliure. Es basa en una bifurcació del programa OSSEC, però ha evolucionat molt, oferint tot tipus d'extres i de quadres de control, a la vegada que implementant la integració amb tot tipus de fonts de generació de registres, i integra tecnologia XDR. En versions anteriors utilitzava les eines de Elastic search + Kibana, però des de la versió 4 utilitza els seus propis indexadors i monitors de control.

  Tot i ser opensource, si es necessiten serveis professionals, l'empresa que hi ha al darrera del seu desenvolupament, ofereix tant formació, com hores d'un tècnic especialitzat. També s'ofereix el model al núvol.

  Avantatges: El cost del llicenciament, a la vegada de tota la comunitat que hi ha al darrera que és de més de 10000 usuaris.

  La flexibilitat del funcionament tant en un servidor únic com en un sistema de clústers per a major processament i velocitat.

  Inconvenients: Tot i tindre una empresa que ofereix els seus serveis d'implantació i configuració, és una eina pensada per a tècnics amb coneixements i no disposa del múscul que pot tindre les solucions de pagament com ara IBM, Google o Microsoft.

https://wazuh.com/

- **Google Chronicle:**

  Chronicle és la plataforma SIEM nativa del núvol de Google, que es basa en la potència de la infraestructura i la informació valuosa d'intel·ligència sobre amenaces de Google.

  Avantatges: Una capacitat de processament i velocitat de detecció més elevada que la resta.
  Retenció de les dades recopilades d'un any sense cost addicional

  Inconvenients: Tot i que no hi ha una taula de costos pública, el cost d'ús deu ser semblant al d'altres plataformes al núvol, i per tant un cost força elevat, que la majoria de petites i mitjanes empreses no poden assumir.

  https://cloud.google.com/solutions/security-information-event-management?hl=es-419

- **Azure Sentinel:**

  Sentinel és l'eina nativa del núvol de Microsoft. Permet l'enviament dels fitxers a analitzar i els serveis de processament i tot el coneixement i IA de l'eina fa la resta.

  Avantatges: Permet un escalat de recursos i velocitat molt altes gràcies al múscul que disposa Microsoft a Azure.

  Inconvenients: El preu és força elevat. Es factura segons la quantitat de dades a analitzar, començant per 2,5€ el GB analitzat, i amb tarifes més reduïdes a mida que s'augmenta el volum de dades, obtenint un preu de 1€ si s'envia 500GB diaris.

  https://azure.microsoft.com/es-es/products/microsoft-sentinel/

- **Mónica:**

  Mónica és el SIEM del Centre Criptològico Nacional (CCN-CERT). Actualment el subministren de forma gratuïta a les administracions públiques, tant per a facilitat la seguretat informàtica, com per integrar-ho amb altres eines de gestió d'incidents de que disposen.
  Té funcionalitats de detecció, emmagatzematge d'evidències, resposta automàtica a esdeveniments, etc.
  Avantatges: És la millor eina de cara a la integració amb les eines del CCN i la gestió de l'adaptació a l'ENS.

  Inconvenients: Tot i que el llicenciament és gratuït per les administracions, s'han de contractar els serveis d'implantació i formació de l'eina. En l'actualitat només hi ha tres empreses que ofereixin aquest servei.

https://www.ccn-cert.cni.es/soluciones-seguridad/monica.html

2.5. Elecció del sistema SIEM i solucions complementàries

Un cop efectuat un estudi del mercat, desglossat en l'apartat anterior i els requisits enumerats en el punt 2.3, la solució seleccionada ha estat l'eina de Wasuh.

Compleix el principal requisit, és de programari lliure i, per tant, permet la seva implementació sense afectar al pressupost de l'Ajuntament. A la vegada, al disposar d'una comunitat que en desenvolupa els complements i millores, el seu potencial i integració és infinit. Tot i això, permet que la mateixa empresa que hi ha al darrere de Wasuh, ofereixi serveis d'implementació, configuració, suport i formació, en cas de necessitar-ho.

L'eina permet desplegar el programari client (agent), que fa les funcions de HIDS i envia la informació a la consola de gestió centralitzada de forma segura encriptant-la i comprimint-la. Aquest agent és compatible amb els sistemes Windows des de Windows XP fins a l'actual Windows 11 o Windows Server 2022. També ho és amb equips Linux, MacOS i d'altres.

L'eina permet entorns híbrids, on es gestionen equips en la xarxa local i serveis o dispositius en el núvol.

L'eina permet verificar el compliment del RGPD [14], seguint el sistema de compliment de que disposa.

Permet verificar si existeix alguna vulnerabilitat coneguda en el sistema i t'indica com arrengar-la.

Permet la detecció de malware i la monitorització de la integritat [15]de fitxers.

És compatible amb la implementació dins d'un sistema de virtualització com VMWare, i de fet permet el seu desplegament de forma desatesa amb un fitxer preconfigurat del tipus OVA.

[14] Wazuh: *Wazuh's support for GDPR* [PDF en línia] [Consultat el 7-11-2022] Disponible a: https://wazuh.com/resources/Wazuh_GDPR_White_Paper.pdf

[15] CPO Magazine: *Implementing File Integrity Monitoring With Wazuh* Octubre de 2022 [Web] [Consultat el 7-11-2022] Disponible a: https://www.cpomagazine.com/insights/implementing-file-integrity-monitoring-with-wazuh/

3. Integració i Desenvolupament

Un cop escollida la solució que s'ajusta a les necessitats de l'Ajuntament, procedirem a dissenyar l'ecosistema d'integració tot basant-nos en els requisits dels diferents components que integren la solució de Wasuh.

3.1. Disseny de l'ecosistema d'integració

Com podem veure indicat en la documentació de la solució, l'arquitectura de Wasuh, es basa en la part dels clients (Endpoints), que realitzen la captura dels registres de successos i funciona com un agent resident en cada dispositiu que vulguem monitoritzar, i la part del servidor que rep i processa aquests registres.

Tanmateix, la part del servidor està composada per tres elements diferenciats que interaccionen entre si, que son el motor d'indexació (W. Indexer), el motor central de processament de dades i accions de resposta (W. Server) i l'eina de configuració i monitorització de forma visual per part dels operadors (W. Dashboard).

En el següent diagrama es pot observar amb claredat els diferents components, i la possibilitats de ser instal·lats de forma independent o en format de granja de treball en paral·lel (clúster).

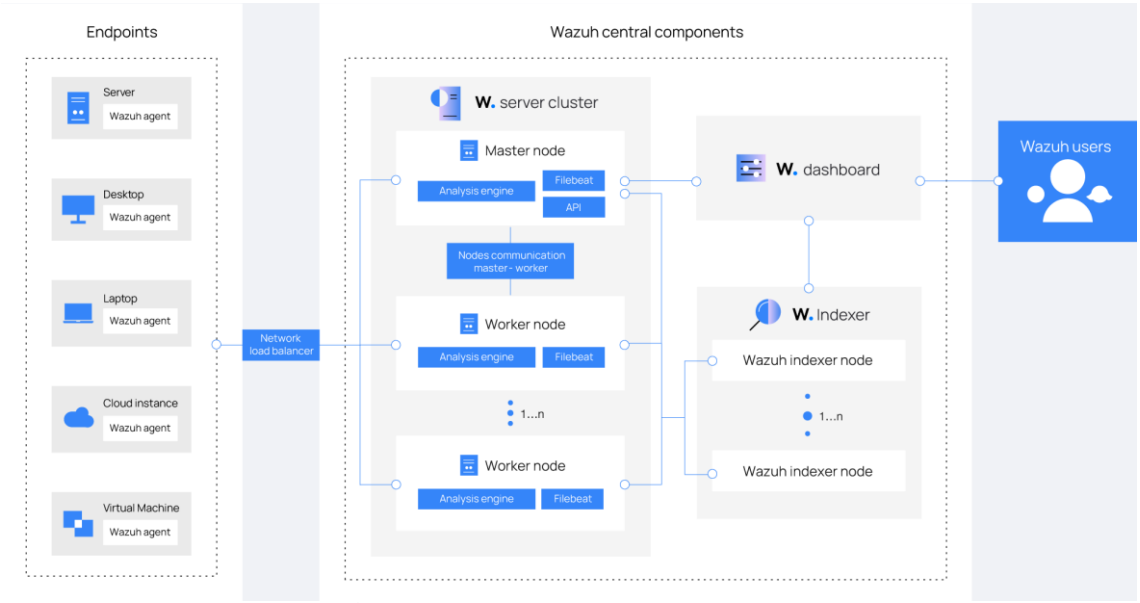


Figura 6[16]: Arquitectura d'implementació de Wasuh.

Seguint les indicacions dels desenvolupadors, per poder implementar els diferents components en la xarxa de l'Ajuntament, s'haurà de complir els següents requisits estimats, segons el nombre d'agents a monitoritzar:

[16] Wasuh. *Architecture.* [Web] [Consultat el 17 de novembre de 2022] Disponible a: https://documentation.wazuh.com/current/getting-started/architecture.html

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

Figura 7[17]: Requisits servidor Wasuh.

A banda dels requisits exposats, es podrà desplegar la solució en diferents entorns i de diferents formes. Com es pot observar en el següent llistat, l'eina es pot instal·lar en diferents distribucions Linux, com son Red Hat, CentOS, Ubuntu o Amazon Linux. A la vegada, es plantejant diferents escenaris d'implementació com pot ser el desplegament dins de contenidors amb Docker o Kubernetes, a través d'una màquina virtual preconfigurada i empaquetada com a fitxer OVA o la descàrrega dels diferents components a través de repositoris d'aplicacions.

Es pot aprofundir en les diferents opcions en el següent enllaç: Opcions d'instal·lació Wasuh.[18]

Per tal d'implementar la solució, s'ha escollit fer-ho pas per pas sobre un servidor Ubuntu. A la vegada, inicialment es realitzarà la instal·lació dels diferents components en mode individual, ja que en principi no serà necessari monitoritzar més de 25 servidors, tot i que si en un futur es volgués realitzar el desplegament a tots els equips de la xarxa, s'implementaria la instal·lació en clúster per repartir la càrrega de treball i augmentar el rendiment.

Així el diagrama amb l'arquitectura de xarxa passaria a quedar així:

[17] Wasuh. *Quickstart - Requirements.* [Web] [Consultat el 17 de novembre de 2022] Disponible a: https://documentation.wazuh.com/current/quickstart.html
[18] Wasuh. *Installation alternatives.* [Web] [Consultat el 17 de novembre de 2022] Disponible a: https://documentation.wazuh.com/current/deployment-options/index.html

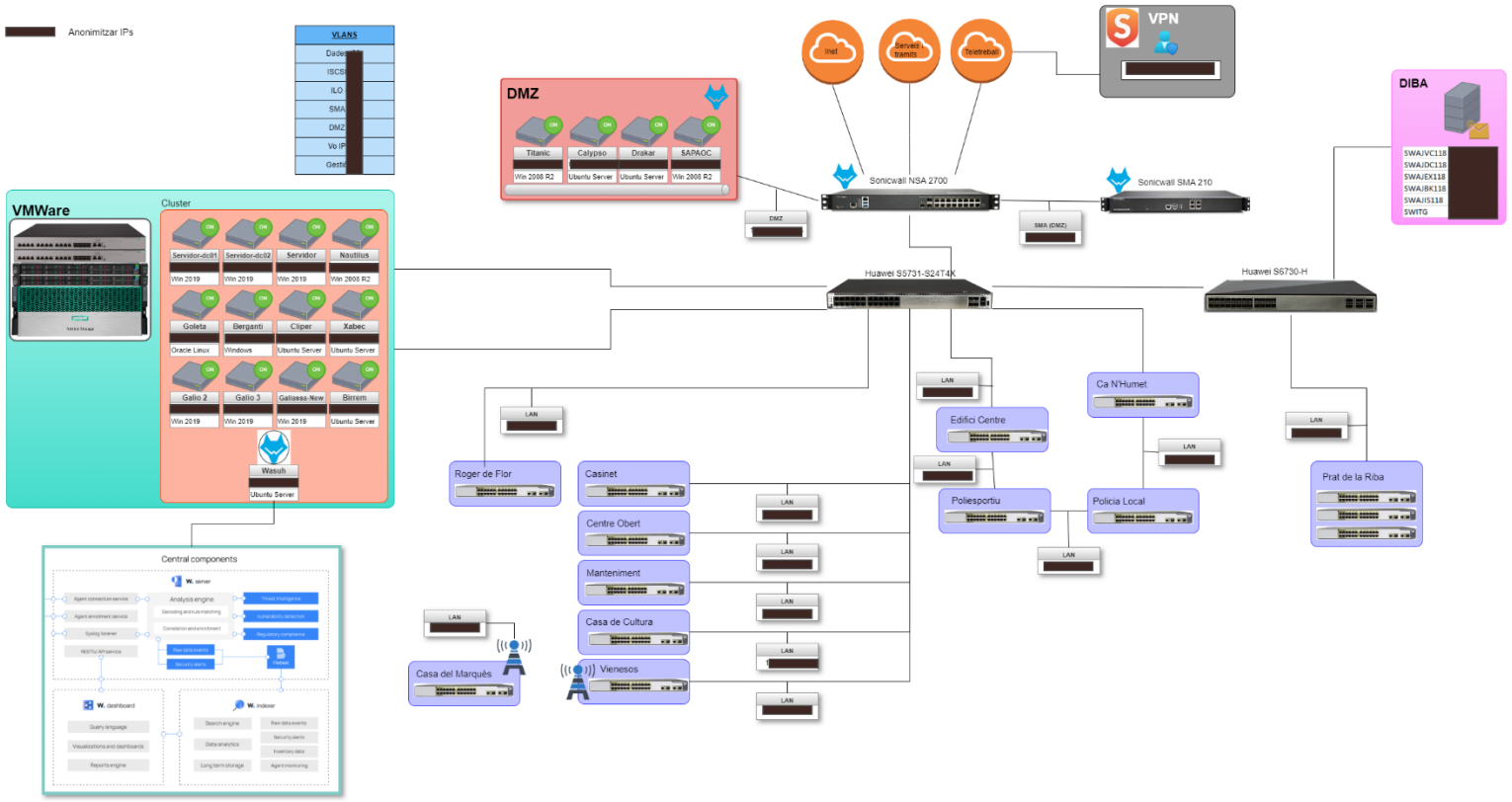


Figura 8: Diagrama de l'arquitectura de xarxa de l'organització un cop incorporat el servidor de Wasuh

Per seguretat, s'han anonimitzat tots els adreçaments en el TFM.

En el diagrama podem veure el nou servidor com a màquina virtual en l'entorn de virtualització VMWare, a la vegada que es desglossa l'estructura de components que formen el servidor Wazuh al complet.

També es marca amb el logotip de Wazuh, aquells equips que tot i no disposar d'un agent de monitorització pròpiament, es procedirà a integrar els registres del seu funcionament, per a que l'eina pugui monitoritzar i procedir segons els esdeveniments que vagin succeint.

3.2. Implementació de les diferents eines

Per realitzar la implementació del servidor i tots els seus components, s'ha desplegat una màquina virtual amb els següents paràmetres de configuració:

8 CPU + 8GB Memoria RAM + 500GB de disc dur

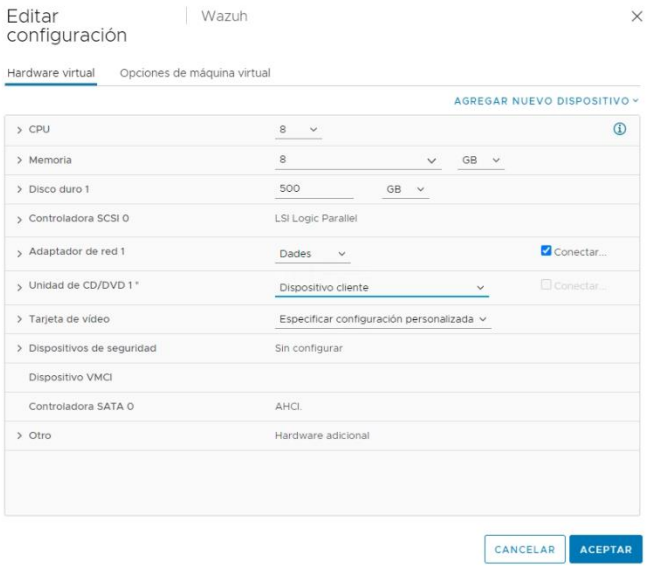


Figura 9: Dades de configuració de la VM creada en l'entorn de virtualització.

En aquest servidor s'hi ha fet la instal·lació del sistema operatiu Ubuntu server 20.04 LTS.

Un cop el sistema ha estat configurat i actualitzat, s'ha procedit amb la instal·lació del components de l'entorn de Wazuh segons les guies d'instal·lació incloses en l'apartat d'annexos.

Un cop tenim el servidor operatiu, ens trobem amb els diferents apartats de que consta el quadre de control de Wazuh, que són:

L'apartat de "home", que mostra la pantalla inicial amb l'estat dels agents i els diferents apartats de seguretat que ens ofereix Wazuh.

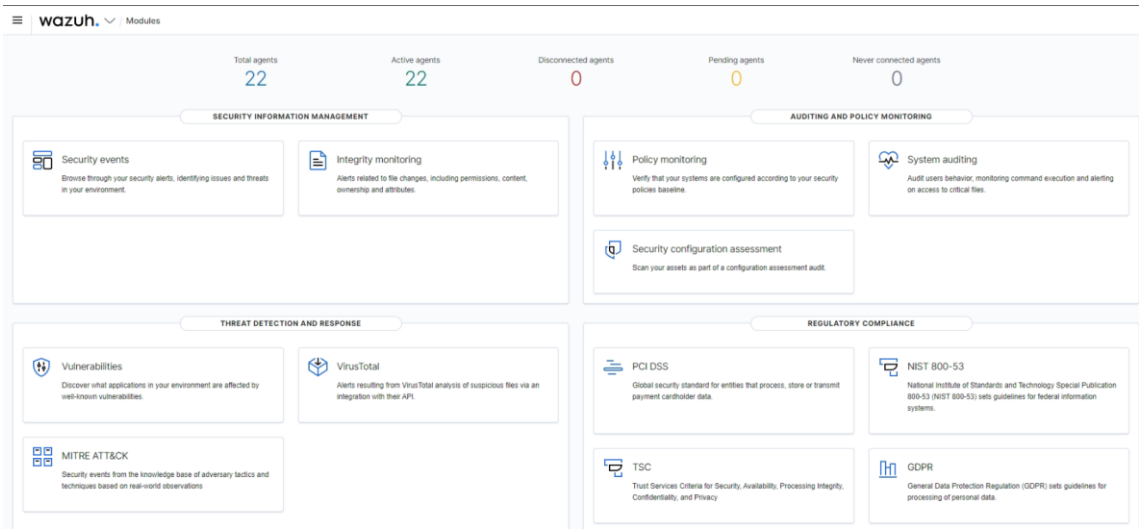


Figura 10: Panell de control del Wazuh.

A més tenim el menú de Wazuh, que ens mostra els diferents apartats de gestió i configuració

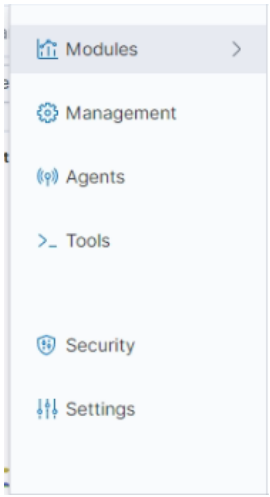


Figura 11: Panell d'opcions disponibles del Wazuh.

En el primer apartat, els **"Modules"**, hi tenim la monitorització de totes les eines de control i seguretat que tenim per controlar l'estat dels agents, i que correspondria amb la pantalla de "**Home**". Dins d'aquests mòduls i tenim els següents apartats:

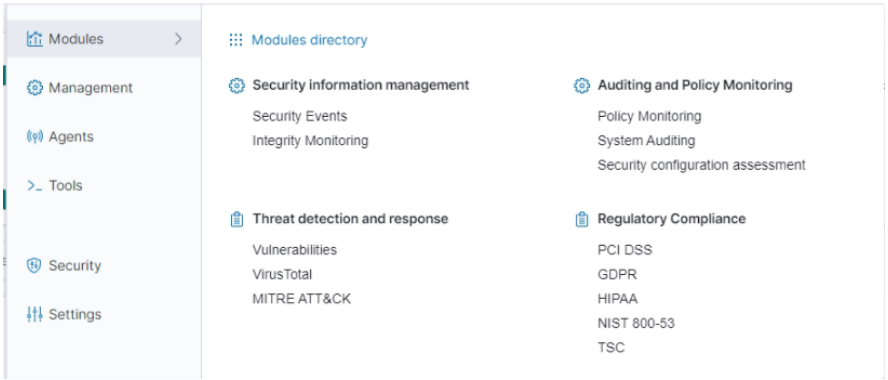


Figura 12: Mòduls disponibles per a implementar.

Sense entrar en el detall de tots els mòduls, si que en fixarem en els principals responsables de la verificació dels sistemes, que ens permeten actuar sobre les configuracions dels diferents agents a nivell de sistema operatiu i així poder aplicar correccions prèvies a que hi hagi cap incident de seguretat.

En concret son:

- L'apartat de "**Vulnerabilities**". Aquest mòdul, no està activat per defecte, sinó que l'haurem d'activar des de la configuració. Un cop fet els passos que es detallen a la guia d'instal·lació, podrem veure per cada agent, si existeix algun programari, que presenti alguna vulnerabilitat coneguda i que coincideixi amb la base de dades de vulnerabilitats. Segons si el sistema és un Windows o un Linux, aquesta comprovació es farà en la seva base de dades corresponent.

  Si ens fixem en el nostre sistema, veiem com un dels servidors Windows, li consta que té vulnerabilitats conegudes, ens mostrarà la gravetat d'aquestes i ens facilitarà la informació sobre tots els detalls necessaris per a saber l'afectació de dita vulnerabilitat i si existeix forma de solucionar-la.

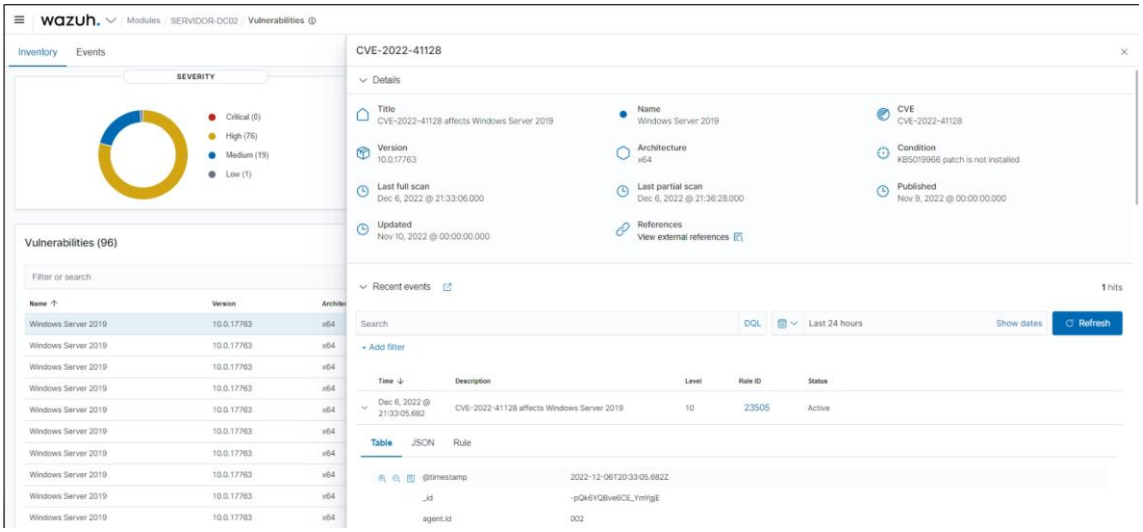


Figura 13: Mòdul de vulnerabilitats aplicat a un agent Windows.

Així podrem anar comprovant cada agent i aplicant els pegats de seguretat, per evitar que un atacant pugui explotar aquestes vulnerabilitat aconseguint escalar en privilegis o realitzar moviments laterals de servidor a servidor.

- Un altre dels apartats, que ens permet prevenir atacs segons el control de la configuració, és el mòdul de "**Security configuration assessment**".
  Aquest apartat, ens permet verificar si els nostres sistemes estan ben bastionats. El propi Wazuh, disposa d'una llista de paràmetres a comprovar, segons cada perfil de sistema operatiu, que permeten verificar si hem realitzat una configuració correcta a nivell de securitzar i minimitzar el risc de vulnerabilitats i atacs als nostres equips. El sistema aplica aquesta comprovació als diferents agents i ens llista si hem passat la comprovació, si l'hem fallat o si no ens aplica.

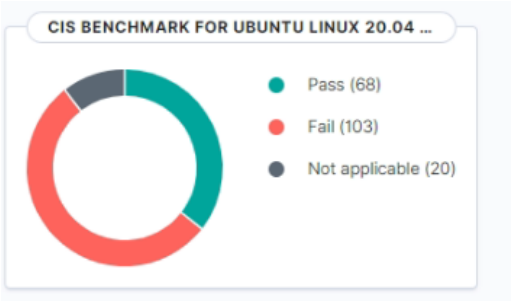


Figura 14: Nivell d'acompliment dels punts de configuració revisats

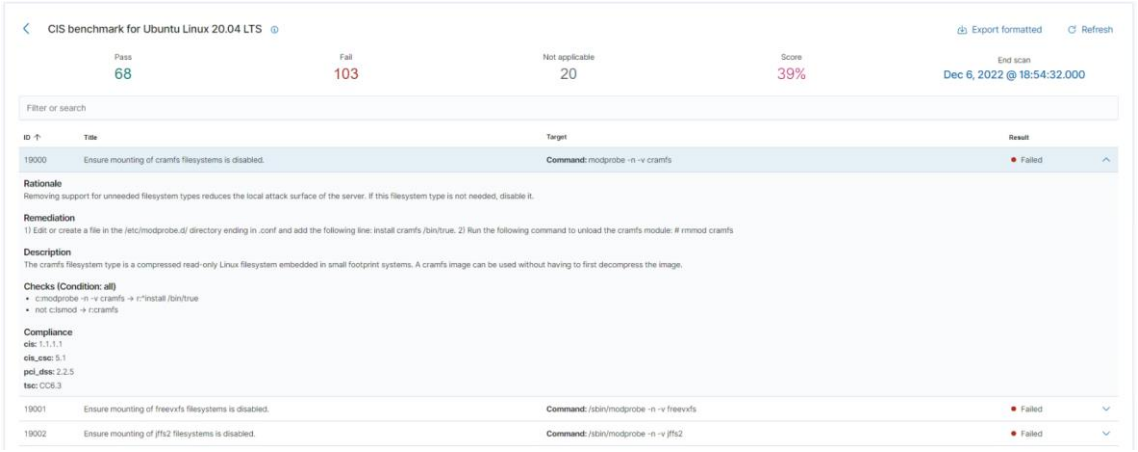


Figura 15: Detall del nivell d'acompliment dels punts de configuració revisats

- I finalment l'apartat de "**MITRE ATT&CK**". Aquest apartat, com el seu nom indica, es basa en la matrius del tipus ATT&CK que desenvolupa l'empresa MITRE, i que serveixen per verificar les accions que els atacants realitzen en atacs reals i ho classifica perquè es pugui verificar si aquestes accions i situacions prèvies que podrien resultar un atac, estan passant en els nostres sistemes.

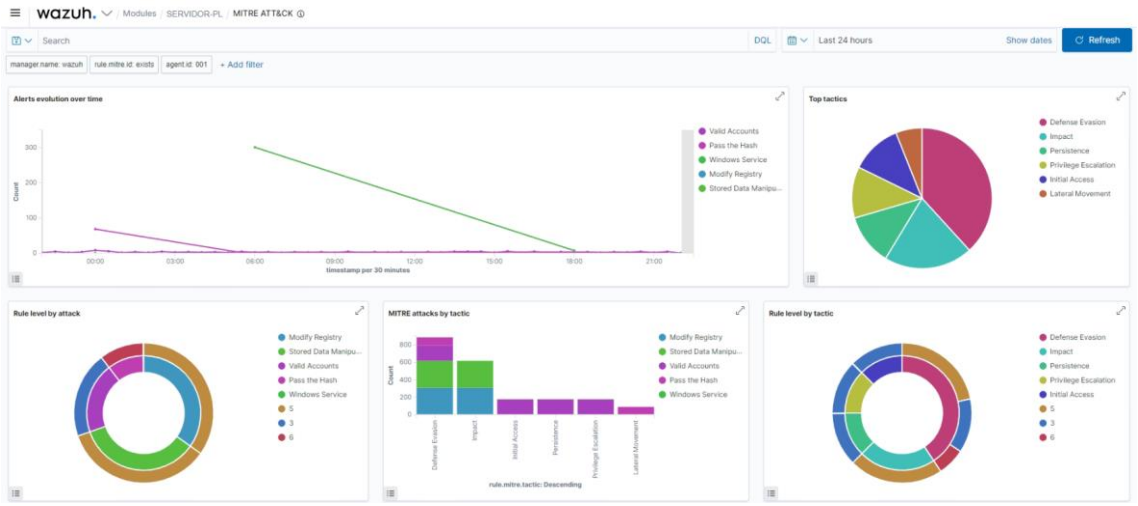


Figura 16: Estadístiques de la Matriu d'Atack de MITRE aplicades a un agent Windows

Per altra banda, un dels altres mòduls a tenir en compte indistintament de si succeix algun event de seguretat o no, és l'apartat de "Regulatory Compliance".

Aquest apartat, ens mostra diferents normatives de seguretat, com són, la guia del NIST SP 800-53 o el compliment del Reglament en Protecció de Dades (GDPR) i d'altres. Aquestes guies, consten d'un seguit de paràmetres a configurar en els nostres equips per tal de complir amb la normativa, i el Wazuh, el que fa és comprar les guies amb els nostres sistemes i verificar quin és el nivell d'acompliment que en tenim i si hi ha hagut esdeveniments que incompleixin aquesta normativa.

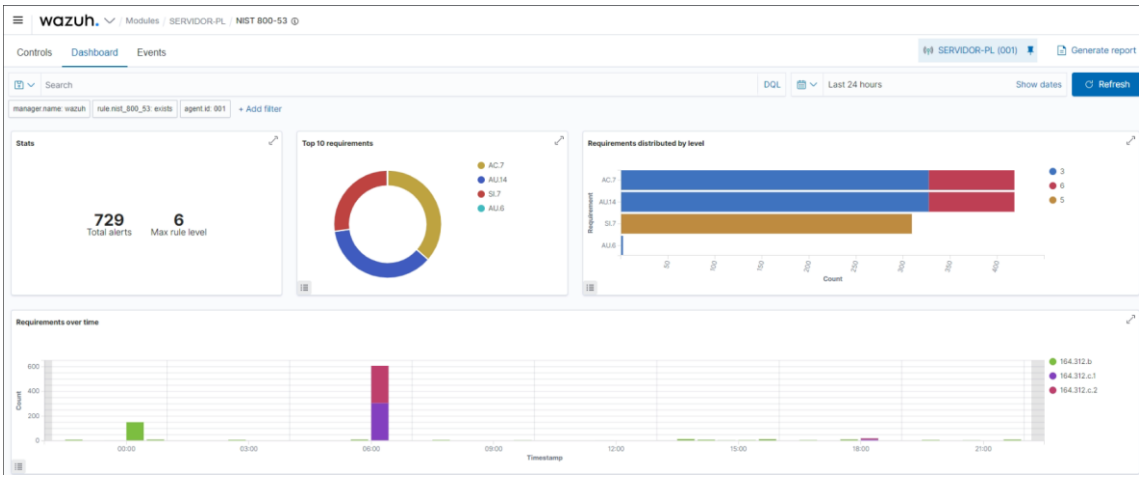


Figura 17: Acompliment de la normativa NIST 800 en un agent Windows.

Sí seguim explorant el menú del sistema, i ens fixem en el segon apartat, veurem l'apartat de **"Managment"**, on tindrem accés a la configuració del les regles de detecció, els descodificadors de missatges de log, la creació de grups per classificar els agents i la configuració general del servidor.

A més també hi podem veure l'estat dels diferents serveis i del clúster a més d'estadístiques d'ús i el registre general de funcionament del servidor.

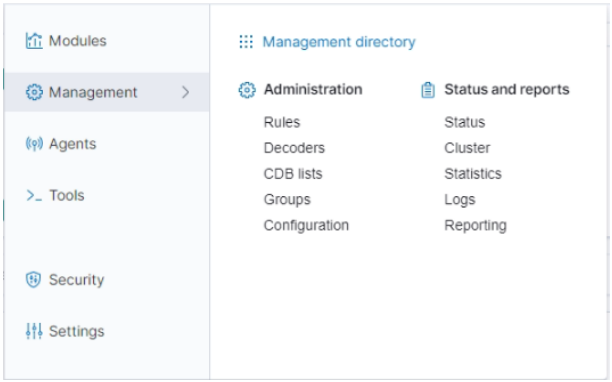


Figura 18: Opcions del menú Managment del Wazuh.

Dins de l'opció **"Agents",** i obtindrem el panell de control amb informació dels diferents agents que hi tinguem configurats.

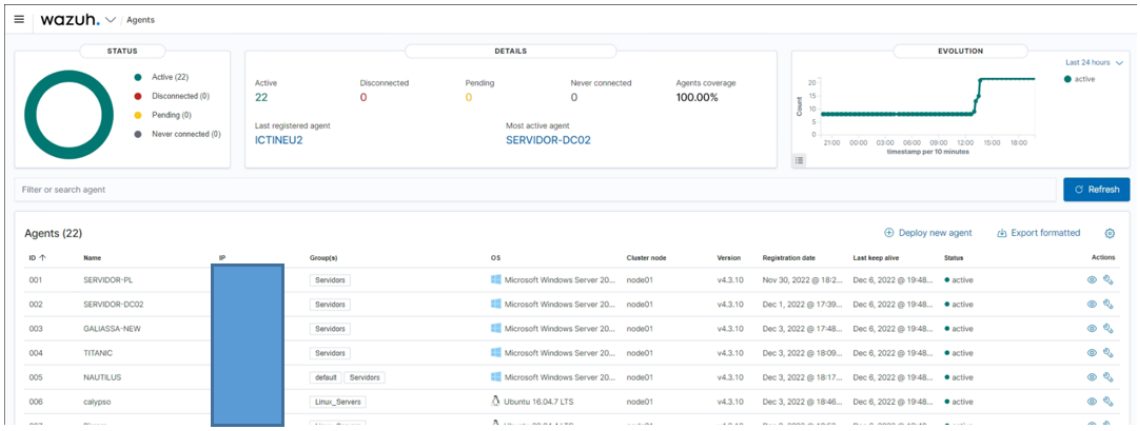


Figura 19: Vista del llistats d'agents i el seu estat

En l'apartat de **"Tools"**, tenim accés a configurar la nostre pròpia API i a realitzar proves amb regles de nova creació, per a veure el resultat que donarien si les implementem.

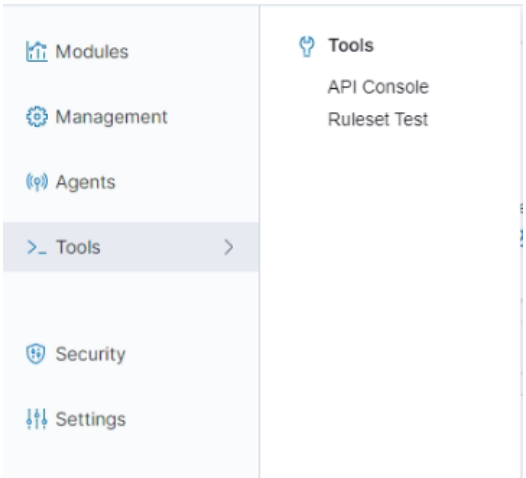


Figura 20: Eines disponibles

A l'apartat de "**Security**", hi podrem configurar els diferents usuaris amb accés a l'aplicació, a més dels rols d'aquests usuaris i les polítiques d'accés de l'aplicació.

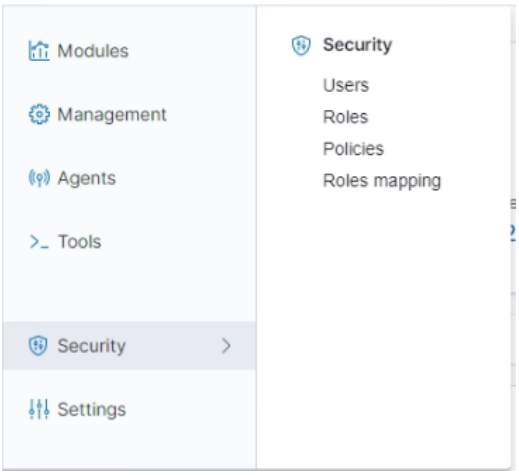


Figura 21: Configuració d'usuaris i roles de l'aplicació

Finalment en l'apartat de **"Settings"**, i podem configurar totes les propietats referents al Dashboard. Com per exemple quins mòduls es mostraran a l'apartat de "Modules", o si volem utilitzar dades d'exemple per a veure el comportament de l'aplicació, configuracions de la connexió i obtenció de dades dels diferents quadres de control, etc.

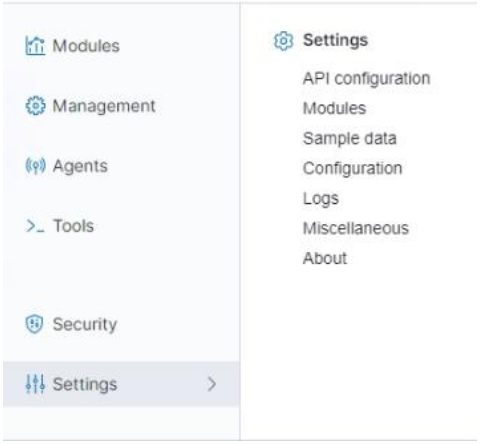


Figura 22: Opcions de parametrització del funcionament de Wazuh.

3.3. Integració de les eines ja existents a l'Ajuntament

Un dels requisits a l'hora de seleccionar l'eina SIEM que s'adaptés a les necessitats de l'Ajuntament, era la necessitat de poder integrar dita eina amb els sistemes existent. Aquests sistemes son el Firewall perimetral que controla l'accés als serveis publicats a la DMZ i que dona servei de sortida a Internet a tots els equips de la xarxa. A la vegada s'encarrega de realitzar l'encaminament dels diferents dispositius entre les xarxes VLAN que estan configurades a la xarxa de treball de l'Ajuntament per separar el tràfic dels diferents dispositius i serveis.

Aquest Firewall és un equip de la marca Sonicwall, que realitza les funcions de Firewall pròpiament dites i altres funcions de seguretat avançades com ara funcions d'IDS, APPControl, Geo-IP Filtering, Bootnet filtre, etc.

Es per tant l'equip que protegeix tot el perímetre i que ha de garantir que els atacants no passen de la porta i frustrar els seus intents de trencar la seguretat.

Així, el que farem és configurar la recepció dels esdeveniments de seguretat que el propi Firewall va enregistrant, i s'enviaran al servidor de Wazuh per a avaluar si la seguretat ha estat compromesa.

Seguint la guia de configuració, activarem la recepció d'aquests esdeveniments. La pròpia base de dades de Wazuh, a nivell de decodificadors i regles, ja disposa d'un apartat exprés per a gestionar esdeveniments dels equips de la marca Sonicwall.

Com que aquest equip no és un agent, sinó que envia la informació directament al recol·lector del servidor, veurem que el nom de l'agent que enregistra els esdeveniments, és el propi servidor wazuh, però dins de la informació de cada registre, si que ens identificarà quin equip és el que l'ha generat.

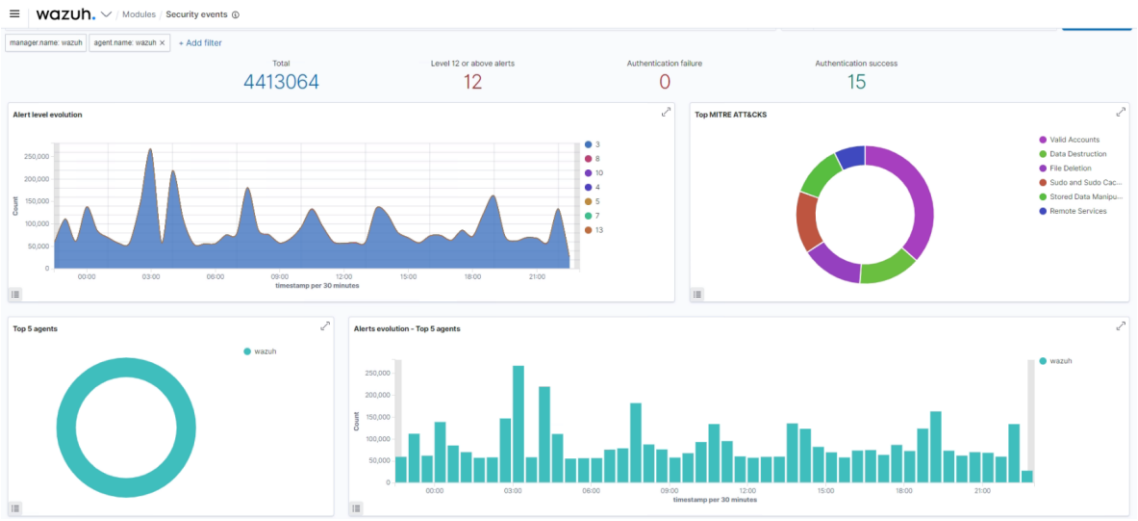


Figura 23: Panell de control de les alertes detectades per syslog.

Com és d'esperar, el Firewall és l'element que més esdeveniments genera amb diferència, i molts d'ells son de cert nivell de criticitat, tot i que el propi Firewall els ha gestionat correctament, com ara pot ser el filtrat de connexions per IPs que no son del propi país i que per tant es descarten pel filtrat de Geo-IP .

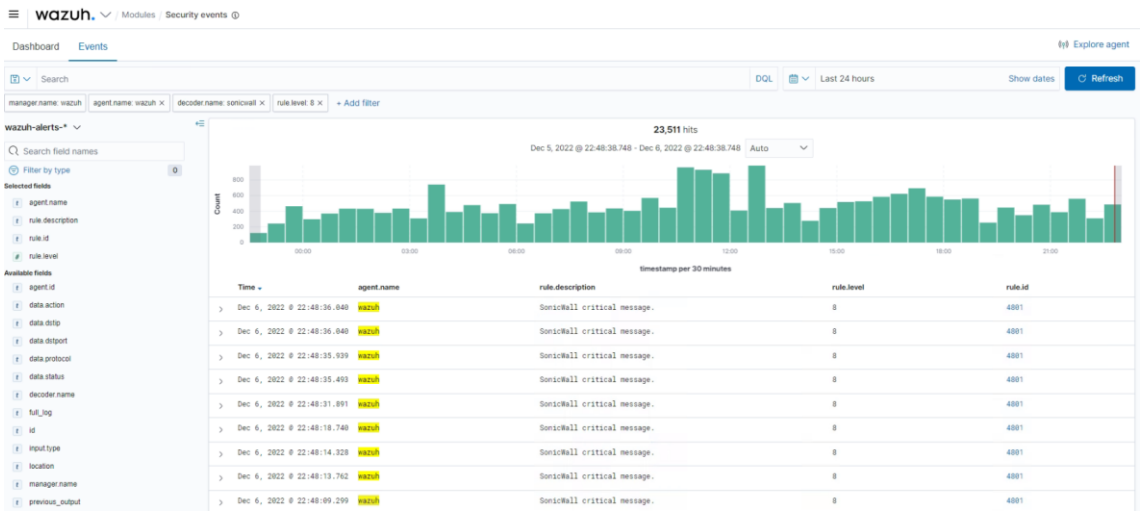


Figura 24: Llistat d'alertes detectades per l'agent Wazuh.

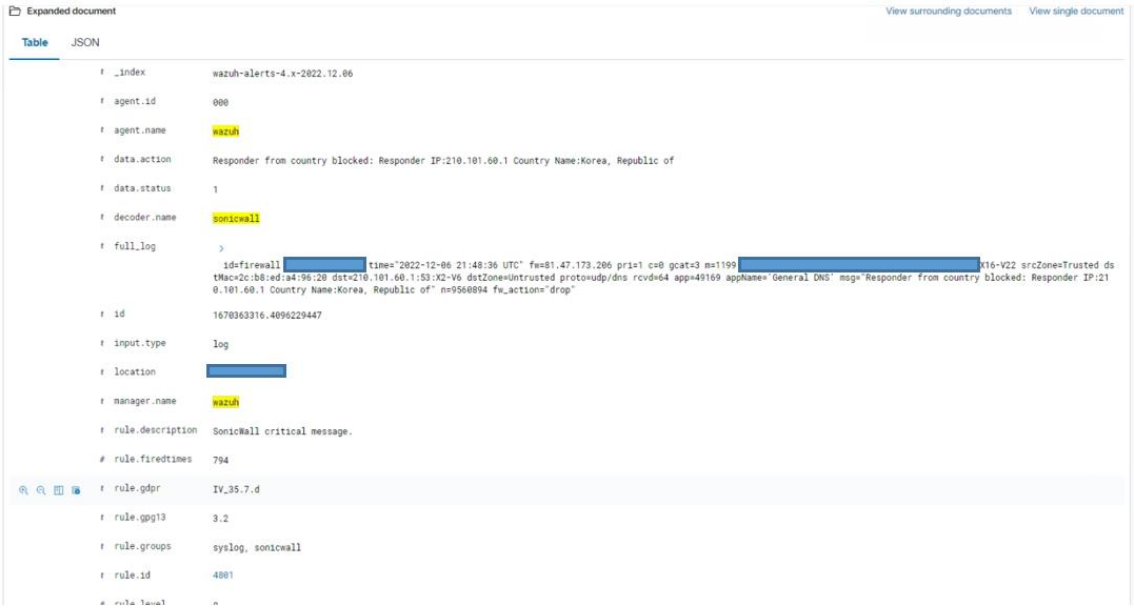


Figura 24: Detall alerta detectada per l'agent Wazuh, com a sonicwall.

4. Validació del funcionament de l'eina

Un cop el sistema està funcionant, i s'ha desplegat els diferents agents i realitzat les configuracions pertinents, procedirem a validar el funcionament del Wazuh com a eina SIEM. Per a fer-ho, realitzarem les següents simulacions del que serien possibles atacs als sistemes de l'Ajuntament.

4.1. Atac per força bruta

Un atac per força brut, es refereix a l'intentat d'accedir als sistemes amb un usuari conegut, i l'intent reiteratiu de la seva paraula de pas, utilitzant la generació de totes les possibles opcions amb els diferents caràcters de l'alfabet escollit. Per a escurçar el temps d'execució, se sol fer ús d'un llistat com a diccionari amb possibles contrasenyes ja calculades.
Per a fer-ho, existeix l'eina Hydra, que genera aquests intents i ens retorna si ha aconseguit fer el login.

Des de un equip Linux amb aquesta eina instal·lada, intentem accedir al sistema atacat (un equip amb Ubuntu Server) per a observar el resultat.

Per a fer-ho primer hem generat un fitxer amb alguns password possibles per a que hydra els utilitzi a mode de diccionari.

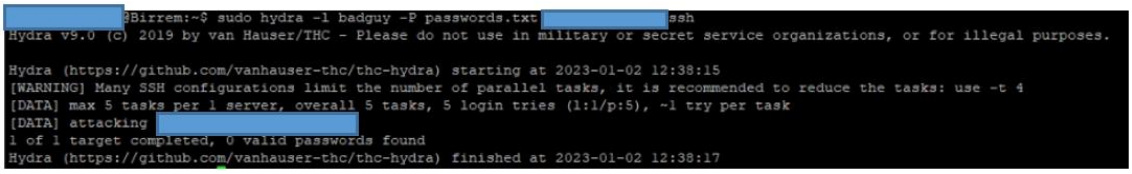


Figura 25: Execució de l'eina hydra

Un cop hem executat l'eina, si visualitzem el monitor del Wazuh de l'agent en concret, veiem que ha detectat els intents de login

Time	rule.description	rule.level	rule.id
Jan 2, 2023 @ 13:38:17.813	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:17.807	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:17.805	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:17.801	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Jan 2, 2023 @ 13:38:17.799	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.874	PAM: User login failed.	5	5503
Jan 2, 2023 @ 13:38:15.874	PAM: User login failed.	5	5503
Jan 2, 2023 @ 13:38:15.874	PAM: User login failed.	5	5503
Jan 2, 2023 @ 13:38:15.832	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.832	PAM: User login failed.	5	5503
Jan 2, 2023 @ 13:38:15.832	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.813	PAM: User login failed.	5	5503
Jan 2, 2023 @ 13:38:15.813	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.813	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.813	sshd: Attempt to login using a non-existent user	5	5710
Jan 2, 2023 @ 13:38:15.796	sshd: Attempt to login using a non-existent user	5	5710

Figura 26: Alertes del Wazuh per atac de força bruta

Per un costat ens indica que l'usuari no existeix, i que el login ha fallat.

4.2. Monitorització de la integritat d'un fitxer

És de molta utilitat, posar especial control en aquells fitxers que continguin informació delicada, ja siguin usuaris i contrasenyes, com informació confidencial de l'empresa i que vulguem vigilar les modificacions que hagi pogut patir.

Per això, afegirem el monitoreig de la integritat dels fitxers o carpetes que ens interessi en cada agent. Per a fer-ho, editarem el fitxer de configuració i afegirem la ruta que ens interessi. En el cas d'exemple s'ha configurat l'escriptori d'un usuari, on s'ha creat un fitxer que suposadament conté dades importants.

```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

 <!-- Llista de fitxers personalitzats a monitoritzar -->
 <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\LucasMAD\Desktop</directories>
```

Un cop afegit el control, hem procedit a crear el fitxer i veiem que el Wazuh, en detecta la creació i l'afegeix a la monitorització.

Figura 27: Inclusió d'un fitxer a la monitorització d'integritat

Després l'hem modificat afegint dades

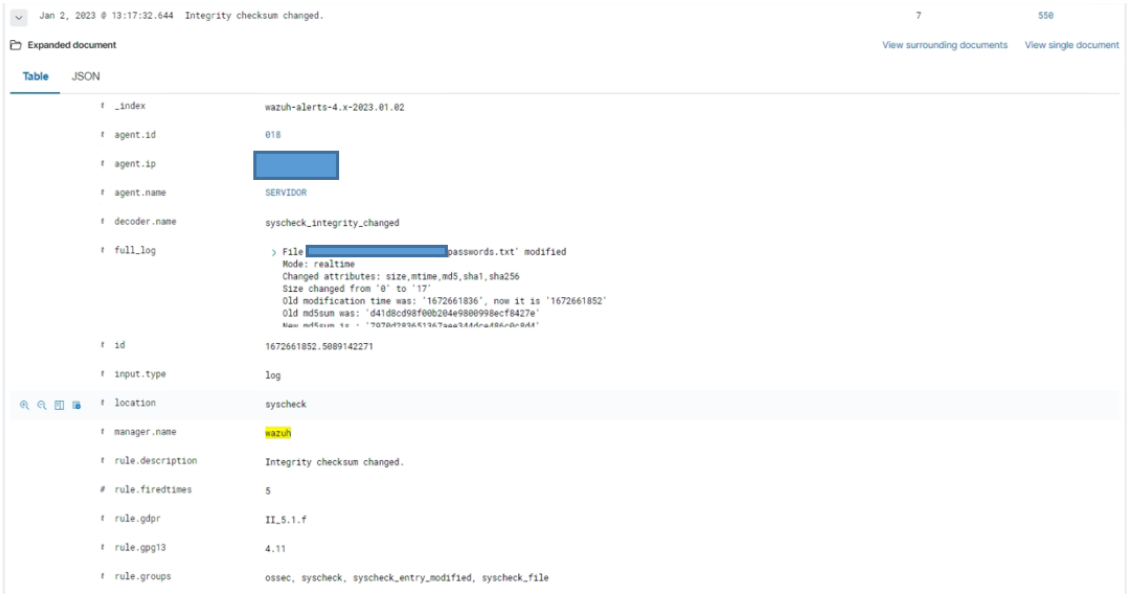


Figura 28: Alerta de modificació d'un fitxer

I finalment l'hem esborrat

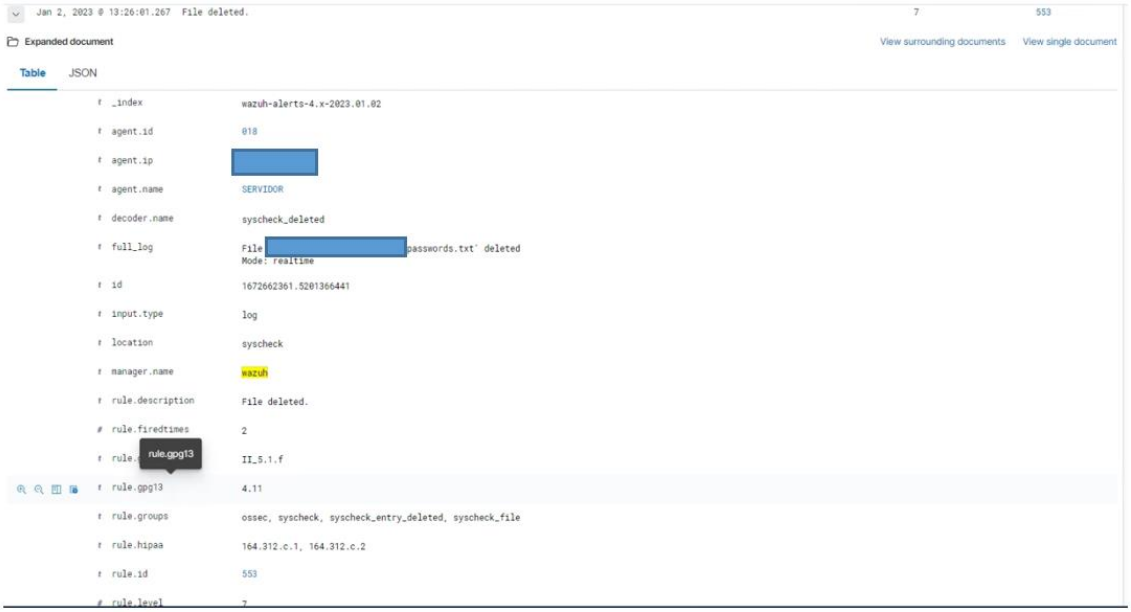


Figura 29: Alerta d'esborrat d'un fitxer

4.3. Verificació de l'escaneig de fitxers per part de VirusTotal

Una de les accions que s'han fet a les guies d'instal·lació, i que consta com a part important de la integració per part de Wazuh amb una eina d'un tercer, és la integració de l'escaneig de fitxers amb l'API de VirusTotal.

Per a fer-ho ens hem donat d'alta i aconseguit una clau que ens dona accés a dita API.

Un cop amb la clau, i afegida al fitxer de configuració del servidor de Wazuh, en el moment que afegim alguna carpeta com a monitoratge de la integritat de fitxers, el servei efectua un escaneig per part de l'antivirus VirusTotal, i en cas de ser positiu en registra la incidència.

Es podria configurar l'actuació proactiva per part del servei i que elimines el fitxer, però de moment, i tenint en compte que la solució està en un entorn de producció, s'ha preferit que només fos informatiu.

Per a fer la prova, descarreguem un fitxer que detectarà l'antivirus, tot i que no realitzarà cap acció maliciosa, en la carpeta "/home/**********", que prèviament hem configurat com a carpeta inspeccionada.

A l'observar el Wazuh, veiem que n'ha detectat la perillositat.

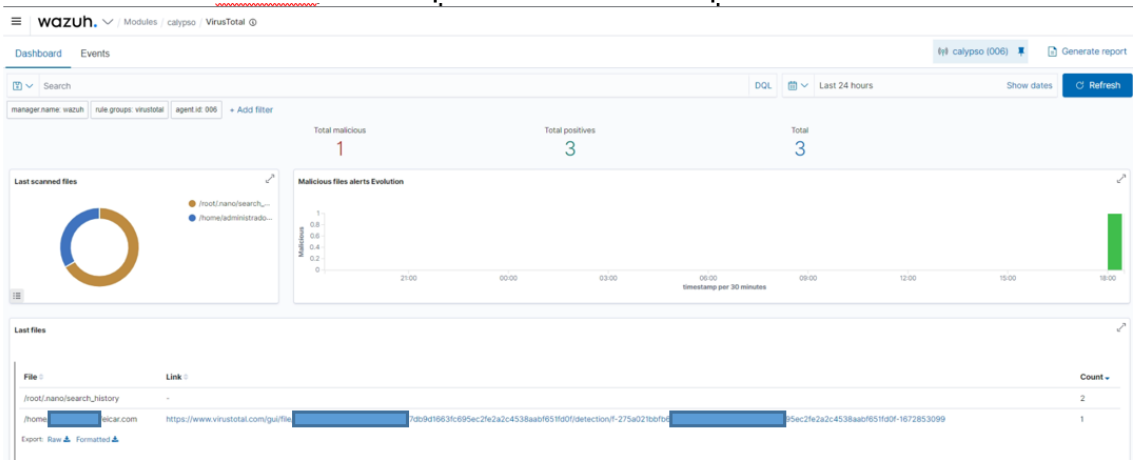


Figura 30: Alerta VirusTotal

4.4. Vigilància de la creació d'usuaris i l'escalat de privilegis

Per defecte, els agents de wazuh ja tenen activat l'auditoria de creació d'usuaris i sobretot de modificació dels grups especials que atorguen més privilegis, com ara els administradors locals o de domini, per notificar en cas que algú estigui aconseguint elevar els privilegis del seu usuari.

Per això, en el moment que afegim o traíem un usuari d'aquests grups, queda registrat amb el codi d'alerta del nivell 5.

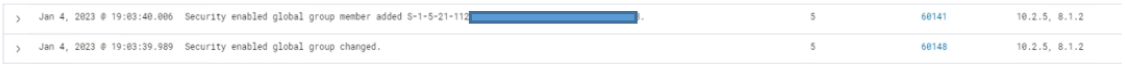


Figura 31: Alerta per modificacions del grup "admin domini"

Tot i això, seria bona idea modificar l'alerta perquè fos de més alt nivell en cas que la pràctica d'afegir i treure usuaris d'aquests grups no sigui una cosa habitual, ja que només les alertes de nivell 12 queden registrades com a greus, i possiblement, amb l'actual configuració se'ns podria passar per alt.

5. Conclusions

En el transcurs d'aquest projecte, s'ha pogut constatar, que la ciberdelinqüència i els atacs informàtics han vingut per quedar-se i cada vegada en seran més i més elaborats. Les grans xarxes de delinqüents, cada vegada més, són professionals amb grans estructures organitzatives i infinitat de branques, igual que funcionen les grans multinacionals del sector. És per això que l'única forma d'estar preparats davant d'ells és professionalitzar el perfil del tècnic en ciberseguretat, i dotar aquest tècnic/tècnics de les millors eines per a defensar-se.

Per tal d'iniciar aquest camí en la protecció dels actius, el principal és obtenir visibilitat del que succeeix i correlació amb els esdeveniments, que normalment, en entorns de producció, solen ser d'una gran magnitud i, per tant, és impossible realitzar-ho de forma individualitzada. És per això que entren en joc les eines SIEM, que permeten unificar el tractament d'esdeveniments d'infinitat d'equips i dispositius de diferents marques i fabricants, a la vegada que permeten correlacionar diferents esdeveniments per extreure conclusions i alertes més avançades que si es fes de forma independent.

Els tècnics encarregats han de tenir un perfil dedicat, a la vegada que una formació constant i especifica en les diferents formes i eines que van apareixent tant per part poder preveure quines formes utilitzaran els atacants, fent del que se sol anomenar com a Red Team, o com per part dels encarregats de la vigilància i resposta als incidents, com a Blue Team.

És per això, que segurament la millor i quasi única opció que hi ha per a petites i mitjanes empreses, on no es disposa d'un gran equip de tècnics en plantilla, és la contractació dels serveis d'un SOC externalitzat, que a la vegada disposarà de les llicències dels programes més potents i actualitzats per a treballar.

Dit això, no totes les empreses disposen de pressupost, ni recursos necessaris per a la contractació d'un SOC extern, o de les eines de pagament necessàries, i és aquí on entra el programari de software lliure Wazuh. És una eina molt versàtil, que amb pocs recursos, permet obtenir molta informació, correlacionar-la i reaccionar de forma activa. A la vegada permet verificar l'estat dels sistemes a nivell d'actualitzacions, vulnerabilitats i diferents normatives.

Dites característiques són molt útils per a la justificació, dels tècnics davant la direcció i sobretot, per a l'hora d'efectuar el pressupost poder avaluar amb dades contrastades, la necessitat d'adjudicar part del pressupost a la protecció d'atacs.

Per desenvolupar aquest projecte s'ha seguit la metodologia en cascada, i considero que ha estat l'adequada, ja que cada apartat donava les eines i consideracions necessàries per afrontar el següent.

L'objectiu principal d'aquest projecte, s'ha assolit amb creixes, s'havia de dotar d'eines per a millorar la seguretat de l'Ajuntament, i amb la implementació del SIEM Wazuh, s'ha aconseguit. A la vegada, un dels altres objectius, era l'estudi

del mercat per identificar i avaluar les diferents eines en aquest sentit que existeixen i aquest també s'ha aconseguit satisfactòriament.
També es volia poder integrar els registres que s'obtenen del Firewall, i s'ha pogut fer de forma molt senzilla i funcional.

Un dels requisits indicats en les funcionalitats de l'eina SIEM, però que a l'inici d'aquest projecte ja se sabia que no es podria complir, per estar fora de la l'ambit temporal d'aquest projecte, és la integració del Wazuh amb la monitorització del servidor de correu en el núvol de Microsoft 365, però l'eina disposa de la funcionalitat i quedarà com a treball a futur.

Per altra banda, és cert que és una eina amb una potència molt elevada, però que requereix invertir molt temps per ajustar i personalitzar el comportament de cada servei que es vol integrar, per tant, queda molta feina a fer, que no s'ha pogut implementar en aquest projecte, i es plantejarà de cara a treballs de futur.

6. Treballs futurs

Com ja s'ha exposat, la guerra de la ciberdelinqüència, no es guanya en una batalla, i per tant aquest projecte ha deixat moltes accions i implementacions pendents per al futur.

L'eina de Wazuh ens mostra els esdeveniments i els classifica per gravetat amb una numeració, però en cas que l'incident sigui de caràcter greu, no se'n realitza l'inici d'un seguiment concret i adequat. És per això que seria bo, la integració del Wazuh amb una eina d'obertura de tiquets per al seu tractament i estudi com ara podria ser l'eina "The Hive".

Per altra banda, s'ha efectuat la integració amb els registres d'esdeveniments que envia el tallafoc Sonicwall, però s'hauria d'aprofundir en la utilització de l'API que posa a disposició el mateix tallafoc per a realitzar respostes actives davant d'atacs, i que per falta de temps no s'ha pogut treballar.

Tanmateix, també es podria perfeccionar la identificació de Malware, amb la integració de l'eina Yara, que n'identifica els patrons textuals o binaris i n'identifica les famílies.

Com ja s'ha indicat en les conclusions, faltarà la integració amb Office 365, utilitzant el mòdul concret que disposa Wazuh per a la monitorització en el núvol.

Finalment, s'hauria de treballar en com fer que l'eina fos tan automàtica com sigui possible, per evitar la necessitat d'estar revisant i estudiant els esdeveniments que es mostra de forma diària. Per a fer-ho s'hauria d'integrar les eines 'un sistema SOAR que permetis aquesta automatització, però tal tasca podria significar un projecte de les mateixes dimensions que l'actual.

7. Glossari

TIC: Són les sigles de Tecnologies de la Informació i Comunicació.

SIEM: És la combinació de dues sigles angleses entre elles. Per una banda SIM, “Security Information Management”, i per l’altra SEM, “Security Event Management” quedant en “Security Information and Event Management”, administrador d’informació i events de seguretat.

CPD: Sigles de Centre de Processament de Dades.

ENS: Sigles del Esquema Nacional de Seguretat, document normatiu que regula i assegura l'accés, la integritat, la disponibilitat i la veracitat de la informació emprada en mitjans electrònics relacionats amb les administracions públiques (estatals, autonòmiques i locals).

2FA: Acrònim que identifica el doble factor d’autentificació en un sistema informàtic.

XSS: Es refereix a una forma d’atac, anomenat Cross-Site Scripting.

Blue Team: Forma d’anomenar a l’equip que s’encarrega de la resposta a incidents de seguretat informàtica.

Red Team: Forma d’anomenar a l’equip que s’encarrega de testejar quan de segura és una organització o infraestructura, per detectar-ne els punts febles.

SOAR: Sigles de l’anglès “Security Orchestration, Automation, and Response” que vol dir Orquestració de Seguretat, Automatització i Resposta.

Dashboard: Paraula anglesa, que serveix per referir-nos al panell de control de qualsevol aplicació, que ens indica diferents valors, gràfics i informacions de forma gràfica i visual per la seva ràpida comprensió.

IDS: Sigles de l’anglès “Intrusion Detection System”, és a dir un sistema de detecció d’intrusions.

APPControl: Us del filtrat i informació de les diferents aplicacions que contenen els paquets de la xarxa segons la capa d’aplicació de la torre OSI.

OSI: Sigles de l’anglès “Open Systems Interconnection”, és un model de referència per els protocols de comunicació que està format amb diferents capes, de menys a més abstracció.

Geo-IP: Filtre de contingut segons la localització de la seva IP

Bootnet: Detecció de les xarxes zombis conegudes per a filtrar-ne el seu accés.

8. Bibliografia

- **STATISTA**. *Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022.* [Web] 16-9-2022. [Consultat el 1 d'octubre de 2022] Disponible a: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

- **WE FORUM / INFORDISA**. *The Global Risks Report 2022: la Ciberseguridad y la protección de datos destaca como riesgo principal.* [Blog] 8-2-2022. [Consultat el 1 d'octubre de 2022] Disponible a: https://soc.infordisa.com/la-ciberseguridad-desafio-global-2022/ / https://www.weforum.org/reports/global-risks-report-2022

- **LA VANGUARDIA**. *El Ayuntamiento de Gijón sufre un ataque informático.* [Diari en línea] 19-04-2022. [Consultat el 3 d'octubre de 2022] Disponible a: https://www.lavanguardia.com/local/asturias/20220419/8205917/ayuntamiento-gijon-sufre-ataque-informatico.html

- **EUROPAPRESS**. *El Ayuntamiento de Leganés sufre un "ataque informático" que afecta a todo su sistema.* [Diari en línea] 7-12-2021. [Consultat el 3 d'octubre de 2022] Disponible a: *https://www.europapress.es/madrid/noticia-ayuntamiento-leganes-sufre-ataque-informatico-afecta-todo-sistema-20211207144222.html*

- **DEIA**. *El Ayuntamiento de Getxo sufre un ciberataque.* [Diari en línea] 18-01-2022. . [Consultat el 3 d'octubre de 2022] Disponible a: https://www.deia.eus/bizkaia/2022/01/18/ayuntamiento-getxo-sufre-ciberataque-1748041.html

- **XATAKA**. *El SEPE sufre un ciberataque: el Servicio de Empleo deja de estar disponible y se retrasan gestiones como los ERTES o el paro.* [Diari en línea] 9-3-2021. [Consultat el 3 d'octubre de 2022] Disponible a: https://www.xataka.com/seguridad/sepe-sufre-ciberataque-servicio-empleo-deja-estar-disponible-se-retrasan-gestiones-como-ertes-paro

- **ARA**. *El ataque informático a la UAB habría afectado a más de 650.000 archivos y los delincuentes reclaman 3 M€.* [Diari en línea] 15-10-2021. [Consultat el 3 d'octubre de 2022] Disponible a:https://es.ara.cat/sociedad/ataque-informatico-uab-habria-afectado-650-000-archivos-delincuentes-reclaman-3-m_1_4149340.html

- **EL PAIS**. *Un ciberataque prácticamente paraliza el servicio de al menos tres hospitales catalanes: Moisès Broggi, Dos de Maig y Creu Roja de L'Hospitalet.* [Diari en línea] 7-10-2022. [Consultat el 7 d'octubre de 2022] Disponible a: https://elpais.com/espana/catalunya/2022-10-07/un-ciberataque-afecta-el-servicio-de-al-menos-tres-hospitales-catalanes-moises-broggi-dos-de-maig-y-creu-roja-de-lhospitalet.html

- **CCN.** Esquema Nacional de Seguridad. [Web] [Consultat el 6 d'octubre de 2022] Disponible a: https://ens.ccn.cni.es/es/esquema-nacional-de-seguridad-ens

- **BOE**. *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* [Document en línia] 29-1-2010 [Consultat el 6 d'octubre de 2022] Disponible a: https://boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

- **BOE**. *Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* [Document en línia] 4-11-2015 [Consultat el 6 d'octubre de 2022] Disponible a: https://www.boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

- **BOE.** *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* [Document en línia] 4-5-2022 [Consultat el 6 d'octubre de 2022] Disponible a: https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

- **GARTNER**. *Magic Quadrant for Security Information and Event Management*. Juny 2021 [Web] [Consultat el 9 d'octubre de 2022] Disponible a: https://www.elastic.co/es/campaigns/2021-gartner-magic-quadrant-siem

- **PAE**. *MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Octubre 2012 [Web] [Consultat el 5 de novembre de 2022] Disponible a: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- **Wazuh**. *Wazuh's support for GDPR* [PDF en línia] [Consultat el 7-11-2022] Disponible a: https://wazuh.com/resources/Wazuh_GDPR_White_Paper.pdf

9. Annexos – Guies d'instal·lació

9.1. Instal·lació dels components del servidor Wazuh.

Per tal de realitzar la instal·lació de tots els components del servidor de Wazuh, s'ha seguit la guia de la documentació oficial.[19]

Wazuh Indexer:

Descarreguem els fitxers necessaris des de el repositori propi de Wazuh.

```
@wazuh:/tmp$ cd wazuh-install/
@wazuh:/tmp/wazuh-install$ curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
@wazuh:/tmp/wazuh-install$ curl -sO https://packages.wazuh.com/4.3/config.yml
```

Editem el fitxer de configuració, on afegim la ip dels nostres servidors (Indexer, un o mes segons si tenim el sistema en standalone o en cluster, el servidor pròpiament dit i el dashboard) :

```
  GNU nano 4.8
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: wazuh
      ip: [redacted]
    #- name: node-2
    #  ip: <indexer-node-ip>
    #- name: node-3
    #  ip: <indexer-node-ip>

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh
      ip: [redacted]
    #  node_type: master
    #- name: wazuh-2
    #  ip: <wazuh-manager-ip>
    #  node_type: worker
    #- name: wazuh-3
    #  ip: <wazuh-manager-ip>
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: wazuh
      ip: [redacted]
```

Generem un fitxer comprimit tar, amb els certificats per a realitzar les autentificacions i encriptació de les comunicacions.

[19] WAZUH. *Installation guide* [Web] [Consultat el 1 d'octubre de 2022] Disponible a: https://documentation.wazuh.com/current/installation-guide/index.html

```
@wazuh:/tmp/wazuh-install$ sudo bash wazuh-install.sh --generate-config-files
:04:13 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.10
:04:13 INFO: Verbose logging redirected to /var/log/wazuh-install.log
:04:14 INFO: --- Configuration files ---
:04:14 INFO: Generating configuration files.
:04:15 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
```

Executem el script d'instal·lació del servei d'indexer

```
@wazuh:/tmp/wazuh-install$ sudo bash wazuh-install.sh --wazuh-indexer wazuh
:08:09 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.10
:08:09 INFO: Verbose logging redirected to /var/log/wazuh-install.log
:08:23 INFO: --- Dependencies ----
:08:23 INFO: Installing apt-transport-https.
:08:29 INFO: Wazuh repository added.
:08:29 INFO: --- Wazuh indexer ---
:08:29 INFO: Starting Wazuh indexer installation.
:09:12 INFO: Wazuh indexer installation finished.
:09:12 INFO: Wazuh indexer post-install configuration finished.
:09:12 INFO: Starting service wazuh-indexer.
:09:24 INFO: wazuh-indexer service started.
:09:24 INFO: Initializing Wazuh indexer cluster security settings.
:09:26 INFO: Wazuh indexer cluster initialized.
:09:26 INFO: Installation finished.
```

Inicialitzem el cluster, en el nostre cas només d'un servidor.

```
@wazuh:/tmp/wazuh-install$ sudo bash wazuh-install.sh --start-cluster
:15:14 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.10
:15:14 INFO: Verbose logging redirected to /var/log/wazuh-install.log
:15:21 INFO: Wazuh indexer cluster security configuration initialized.
:15:34 INFO: Wazuh indexer cluster started.
```

Recuperem password admin autogenerat en la instal·lació.

Verifiquem la configuració del cluster.

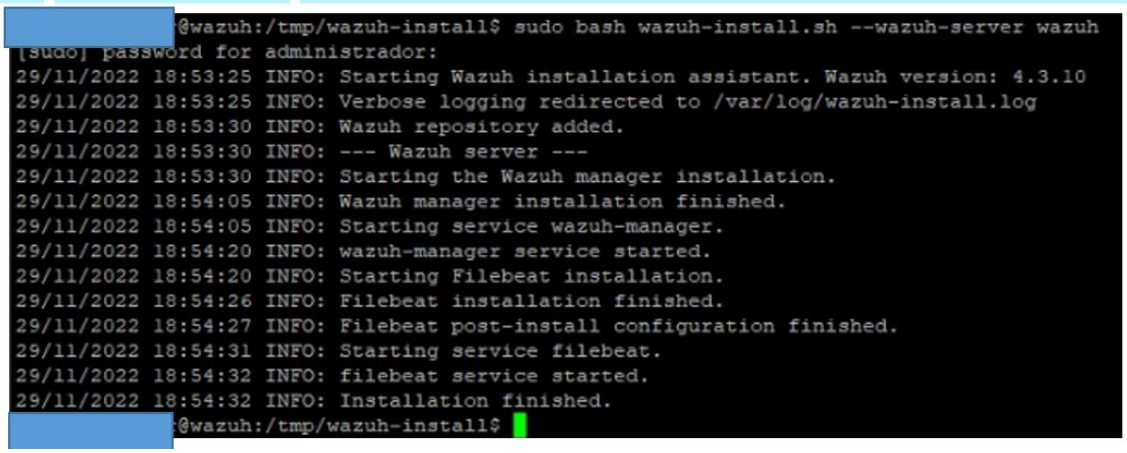
```
[redacted]@wazuh:/tmp/wazuh-install$ curl -k -u [redacted]
{
  "name" : "wazuh",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : [redacted]
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "e505b10357c03ae8d26d675172402f2f2144ef0f",
    "build_date" : "2022-01-14T03:38:06.881862Z",
    "build_snapshot" : false,
    "lucene_version" : "8.10.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

I el seu funcionament.

```
[redacted]@wazuh:/tmp/wazuh-install$ curl -k -u [redacted]_cat/nodes?v
ip         heap.percent ram.percent cpu load_1m load_5m load_15m node.role master name
[redacted]           28          81   0    0.00    0.09     0.09 dimr      *      wazuh
```

Wazuh server:

Un cop tenim l'Indexer instal·lat, passem a instal·lar el servidor pròpiament dit executant el script d'instal·lació amb l'opció –wazuh-server.



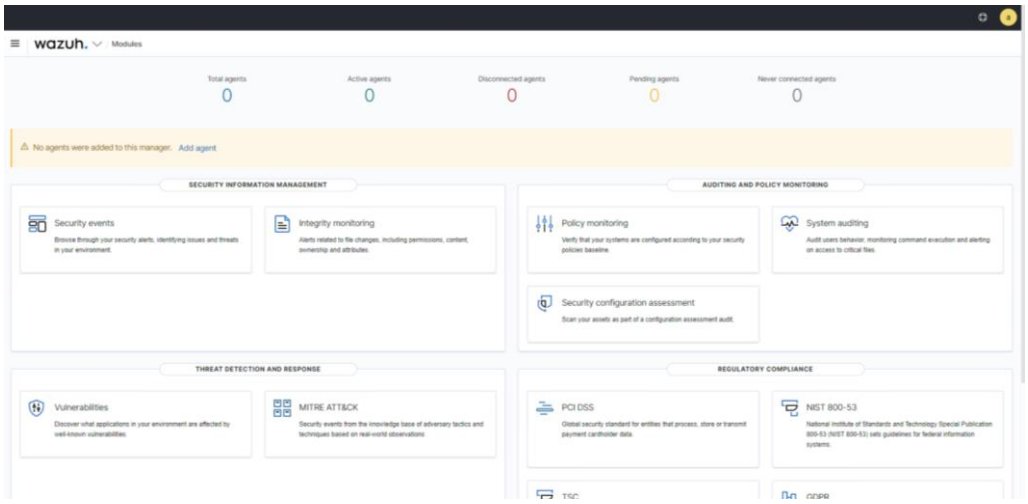
Wazuh Dashboard:

I finalment el mateix script amb l'opció –wazuh-dashboard per a instal·lar el Dashboard.

El propi script d'instal·lació, genera tot un seguit d'usuaris i passwords per a poder accedir als diferents apartats i segmentar els permisos de cada servei. Al llistar el fitxer txt que està dins del fitxer comprimit tar, els podem veure.

Finalment si accedim a la URL del nostre servidor, podem veure com el serveis de wazuh està operatiu i tots els seus components funcionen.

Un cop ens hem identificat podem veure la pantalla de gestió.



9.2. Afegir el servidor a la monitorització Zabbix

Per tal de verificar el rendiment dels serveis de wazuh i el seu correcte funcionament, afegirem el client de Zabbix per a poder monitoritzar-ho des de la consola central i anar veient el rendiment a mida que s'afegeixen agents.

Primerament s'ha d'afegir el repositori i actualitzar llista de paquets disponibles.

```
[redacted]@wazuh:~$ wget https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/
z/zabbix-release/zabbix-release_6.2-2+ubuntu20.04_all.deb
--2022-11-30 17:55:11--  https://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/z
abbix-release/zabbix-release_6.2-2+ubuntu20.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::20
62:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3700 (3.6K) [application/octet-stream]
Saving to: 'zabbix-release_6.2-2+ubuntu20.04_all.deb'

zabbix-release_6.2- 100%[===================>]   3.61K  --.-KB/s    in 0s

2022-11-30 17:55:12 (1.02 GB/s) - 'zabbix-release_6.2-2+ubuntu20.04_all.deb' sav
ed [3700/3700]

[redacted]@wazuh:~$ sudo dpkg -i zabbix-release_6.2-2+ubuntu20.04_all.deb
[sudo] password for [redacted]
Selecting previously unselected package zabbix-release.
(Reading database ... 186678 files and directories currently installed.)
Preparing to unpack zabbix-release_6.2-2+ubuntu20.04_all.deb ...
Unpacking zabbix-release (1:6.2-2+ubuntu20.04) ...
Setting up zabbix-release (1:6.2-2+ubuntu20.04) ...
[redacted]@wazuh:~$
```

Un cop actualitzat, es pot procedir a fer la instal·lació de l'agent.

```
[redacted]@wazuh:~$ sudo apt install zabbix-agent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libmodbus5
The following NEW packages will be installed:
  libmodbus5 zabbix-agent
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 264 kB of archives.
After this operation, 1051 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 libmodbus5 amd64 3.1.6-2 [23.5 kB]
Get:2 https://repo.zabbix.com/zabbix/6.2/ubuntu focal/main amd64 zabbix-agent amd64 1:6.2.5-1+ubuntu20.04 [240 kB]
Fetched 264 kB in 1s (179 kB/s)
Selecting previously unselected package libmodbus5:amd64.
(Reading database ... 186685 files and directories currently installed.)
Preparing to unpack .../libmodbus5_3.1.6-2_amd64.deb ...
Unpacking libmodbus5:amd64 (3.1.6-2) ...
Selecting previously unselected package zabbix-agent.
Preparing to unpack .../zabbix-agent_1%3a6.2.5-1+ubuntu20.04_amd64.deb ...
Unpacking zabbix-agent (1:6.2.5-1+ubuntu20.04) ...
Setting up libmodbus5:amd64 (3.1.6-2) ...
Setting up zabbix-agent (1:6.2.5-1+ubuntu20.04) ...
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Processing triggers for systemd (245.4-4ubuntu3.19) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
```

Per tal de securitzar les comunicacions de l'agent amb el servidor Zabbix, generarem una clau psk predefinida, y l'afegirem en la configuració del client i del servidor.

Primer haurem de crear la clau psk amb la llibreria openssl amb la següent comanda:

```
@wazuh:/etc/zabbix$ sudo openssl rand -out psk.key -hex 32
```

I posteriorment editar el fitxer de configuració de l'agent de zabbix per a que utilitzi aquesta clau.

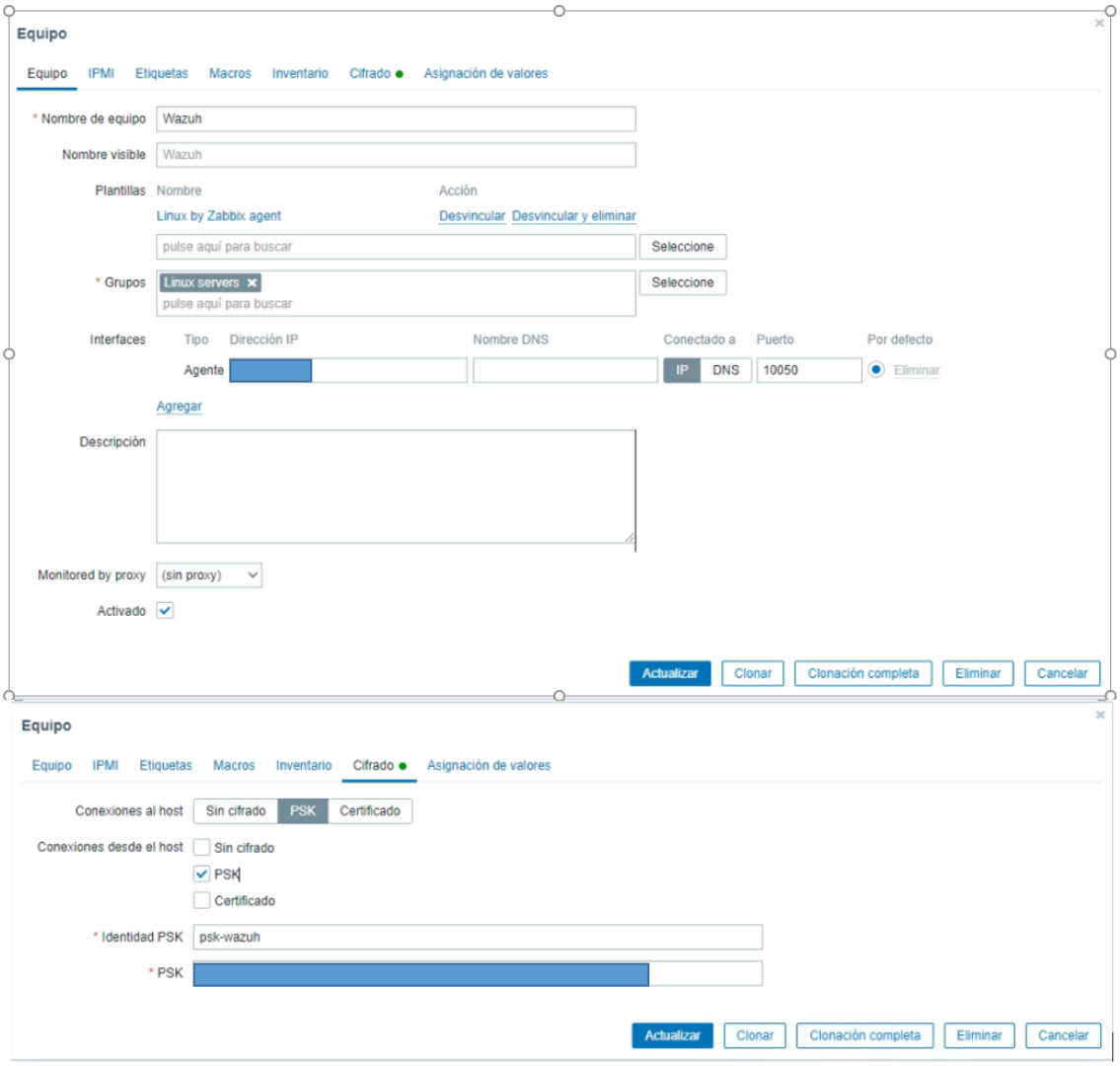
sudo nano /etc/zabbix/zabbix_agentd.conf

```
####### TLS-RELATED PARAMETERS #######

### Option: TLSConnect
#       How the agent should connect to server or proxy. Used for active checks.
#       Only one value can be specified:
#               unencrypted - connect without encryption
#               psk         - connect using TLS and a pre-shared key
#               cert        - connect using TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'unencrypted' connection)
# Default:
# TLSConnect=unencrypted
TLSConnect=psk

### Option: TLSAccept
#       What incoming connections to accept.
#       Multiple values can be specified, separated by comma:
#               unencrypted - accept connections without encryption
#               psk         - accept connections secured with TLS and a pre-shared key
#               cert        - accept connections secured with TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'unencrypted' connection)
# Default:
# TLSAccept=unencrypted
TLSAccept=psk

### Option: TLSPSKIdentity
#       Unique, case sensitive string used to identify the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKIdentity=
TLSPSKIdentity=psk-wazuh

### Option: TLSPSKFile
#       Full pathname of a file containing the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKFile=
TLSPSKFile=/etc/zabbix/psk.key
```

Un cop editat el fitxer reiniciem els serveis.

```
@wazuh:/etc/zabbix$ sudo systemctl restart zabbix-agent
@wazuh:/etc/zabbix$ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
```

Finalment ja podem afegir el servidor Wazuh al monitor de Zabbix:



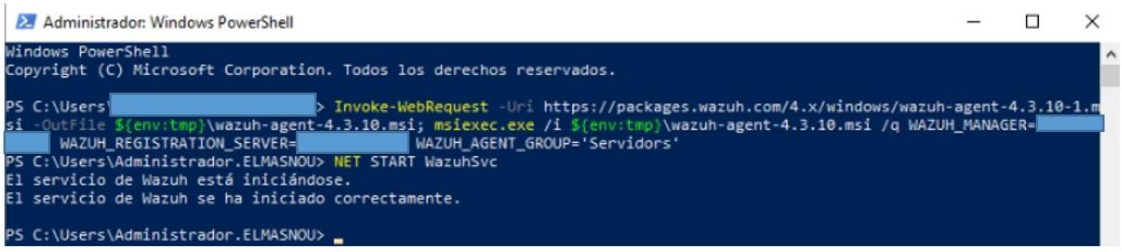
Podem veure el seus rendiments a nivell de CPU o espai en disc i si existeixen problemes detectats per Zabbix.

9.3. Afegir agents Wazuh

Per tal de fer la instal·lació dels diferents agents que gestionaran la informació que els servidors generen i li enviarà al servidor de Wazuh, haurem de diferenciar segons si el sistema operatiu és Windows, Linux o algun altre dels sistemes compatibles.

Agent Windows

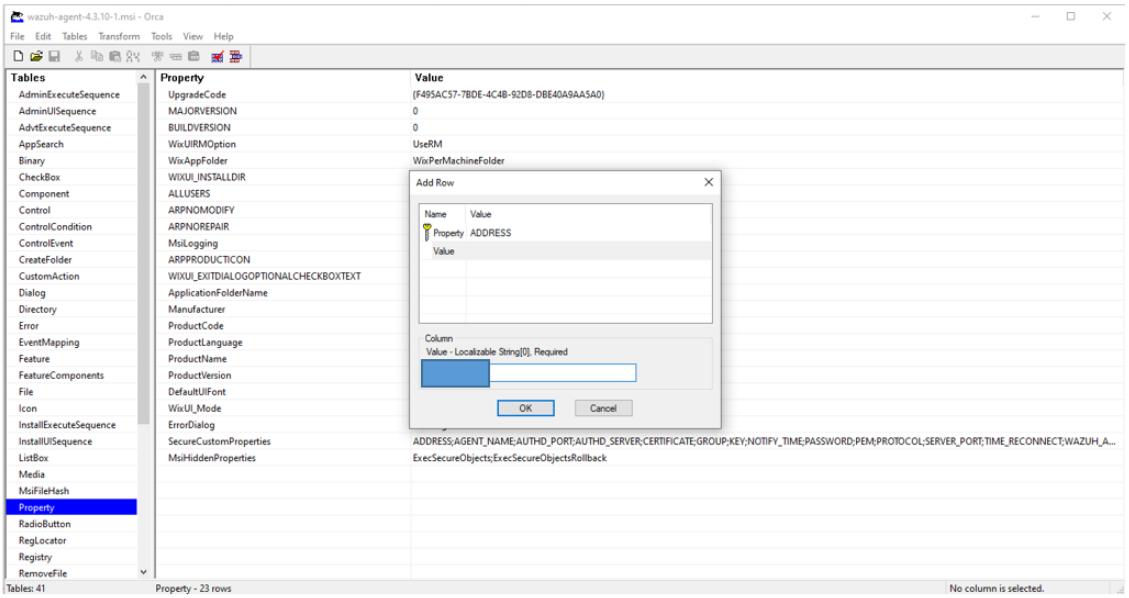
Pel que fa als clients Windows tindrem 2 opcions per desplegar els agents de monitorització.
La primera opció és la instal·lació manual seguint les comandes de powershell que la guia d'instal·lació ens proposa.
Obrim una sessió amb l'equip i executem la descarrega i instal·lació del fitxer msi i posteriorment l'inici del servei que activa l'agent.

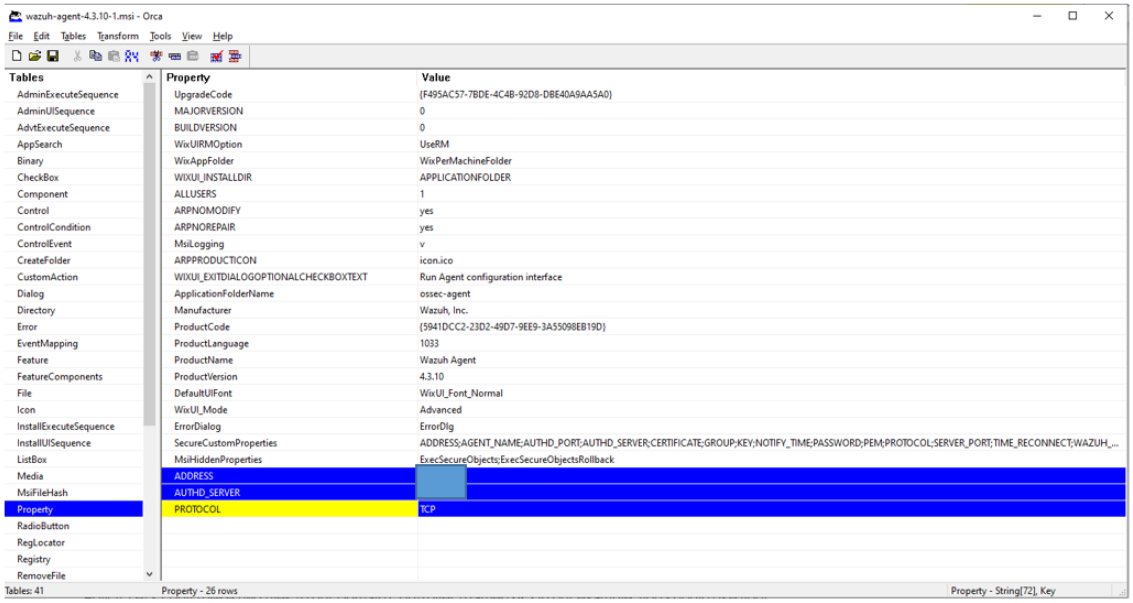


La segona opció serà fer el desplegament per GPO, que tot i que comportarà més feina inicialment, ens ajudarà a desplegar el client de Wazuh per xarxes on hi ha molts equips a monitoritzar i aquests equips estiguin en domini.

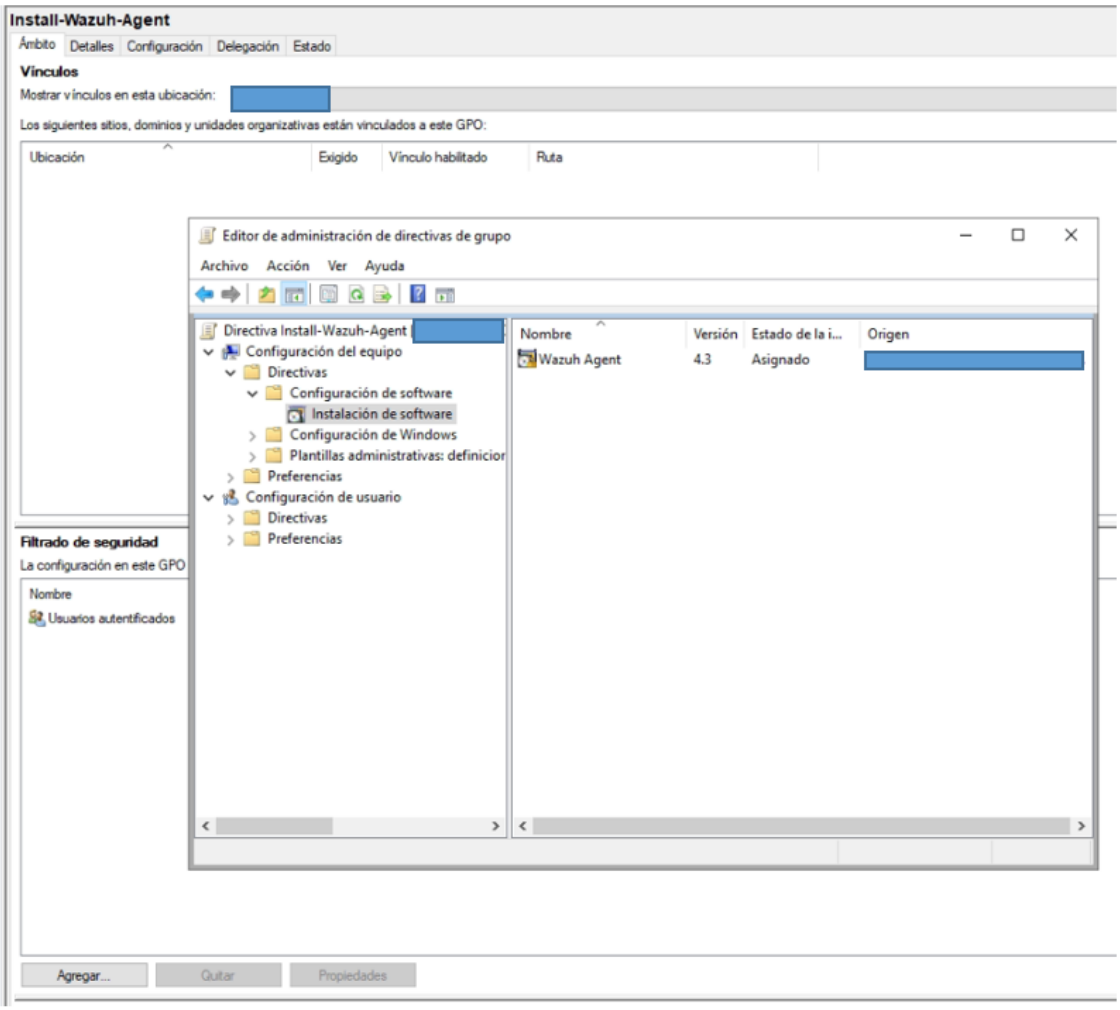
Per poder desplegar el instal·lador, primerament haurem de modificar el fitxer msi per a afegir la ip del nostre servidor, el protocol de comunicacions i el servidor que realitzarà la encriptació de les comunicacions. Per a fer-ho, utilitzarem una eina que ens subministra Microsoft dins del paquet d'eines per a desenvolupadors que s'anomena Orca, i justament permet fer la modificació dels fitxers MSI.

Obrim el fitxer i afegim els paràmetres en l'apartat "Property"

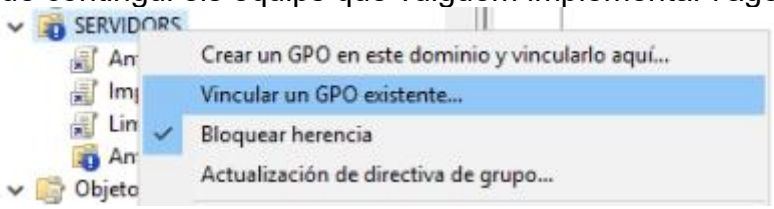




Un cop tenim el msi i la modificació, passem a crear una nova política, on en l'apartat de "Directivas" + "Configuración de software", afegirem el fitxer d'instal·lació.

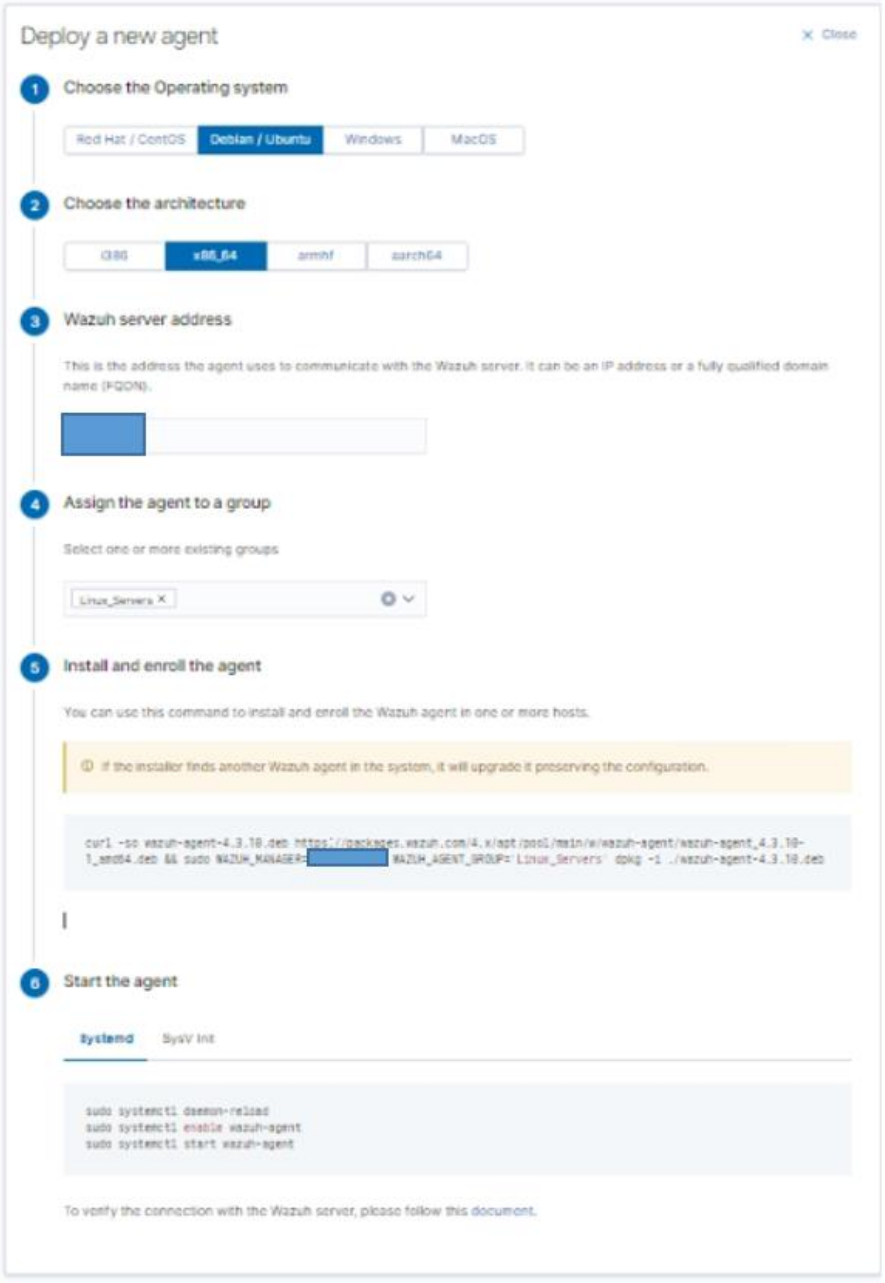


Un cop creada la política, ja la podem assignar a qualsevol unitat organitzativa que contingui els equips que vulguem implementar l'agent de Wazuh.



Agent Linux

Pel que fa als equips amb sistema operatiu Linux, haurem de seguir les instruccions que ens indica el propi servidor en l'apartat d'afegir agent. Escollirem segons la distribució de Linux adequada al nostre servidor, i executarem les comandes que ens proposa.



*curl -so wazuh-agent-4.3.10.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.3.10-1_amd64.deb && sudo WAZUH_MANAGER=***.***.***.*** WAZUH_AGENT_GROUP='Linux_Servers' dpkg -i ./wazuh-agent-4.3.10.deb*

Un cop descarregat el client del repositoris de Wazuh, i realitzada la instal·lació, ja podem passar a afegir-lo perquè s'iniciï de forma automàtica a cada reinici.

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

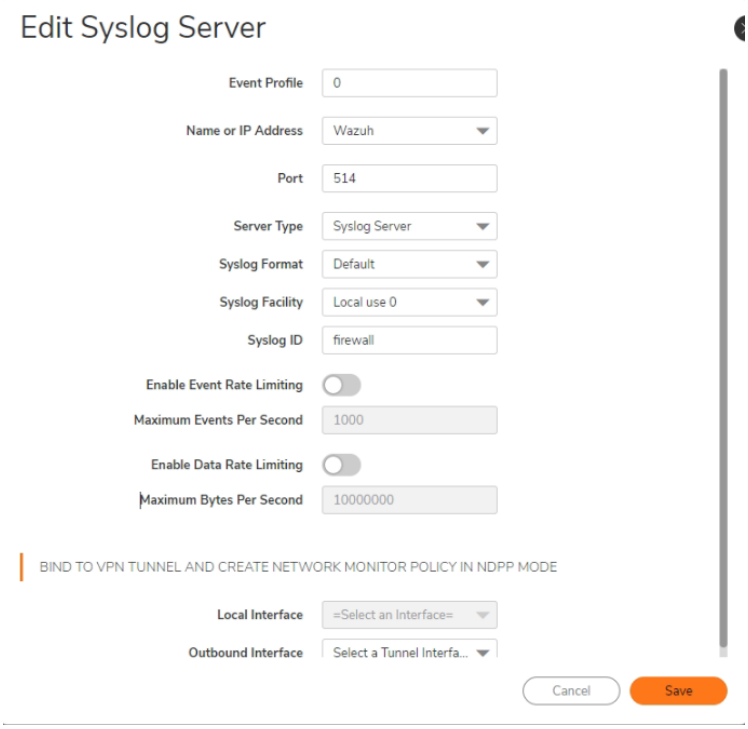
9.4. Integració d'equips que no disposen d'agent (Firewall Sonicwall).

Per tal de monitoritzar equips que no disposen d'agent propi, haurem d'utilitzar algun dels mètodes alternatius que ens proposa Wazuh.

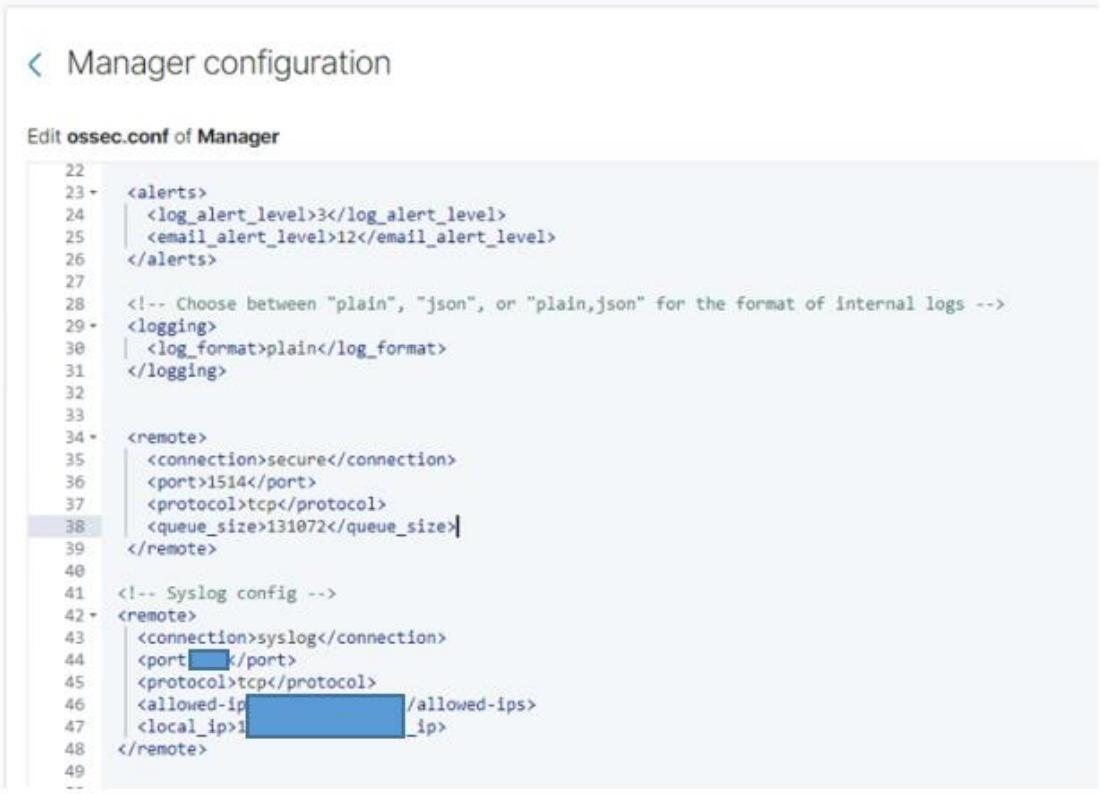
El primera opció, és la recol·lecció de missatges d'un servidor de Syslog. Com que el propi sistema de Sonicwall, disposa de l'opció d'enviar els esdeveniments a un servidor de el format de Syslog, serà l'opció escollida.

Primer de tot afegirem el servidor de Wazuh com a objecte dins de la configuració del Sonicwall.

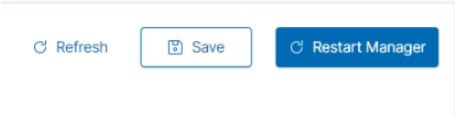
Un cop tenim el servidor, ja podem anar a l'apartat de configuració del servidor de syslog, on afegirem el servidor, el port y el format dels missatges.



Un cop configurat l'enviament des de el dispositiu, en quedarà configurar la recepció d'aquests missatges per part del "Indexer" de Wazuh.
Per fer-ho, haurem d'anar a l'aparta de "Manager" + "Configuration" i escollir l'opció d'"edit configuration".
Aquí obtindrem accés al fitxer de configuracions "ossec.conf", d'una forma més amigable que directament des d'un editor en consola Linux.
Per activar la funcionalitat d'escolta de missatges via Syslog, haurem d'afegir en l'apartat de "remote", l'opció de syslog, on indicarem el port i protocol d'escolta, a més del filtre de quines IPs seran les permeses en enviar missatges al nostre servidor.



Un cop s'ha editat la configuració, ja podem guardar i reiniciar el Manager perquè s'activin les modificacions.



9.5. Activar la verificació de vulnerabilitats:

Per tal d'obtenir les dades de quines vulnerabilitats existeixen en els nostres sistemes, el servidor Wazuh disposa de la comprovació del programari dels agents amb les bases de dades de vulnerabilitats conegudes. El problema és que aquesta funcionalitat no està activada per defecte, sinó que s'ha d'activar[20] en la configuració. Per fer-ho, primer modificarem el fitxer que permet modificar la configuració dels agents de forma centralitzada des de el servidor.

```
@wazuh:~$ sudo nano /var/ossec/etc/shared/default/agent.conf
```

On afegirem el següent codi:

[20] WAZUH. *Scanning unsupported systems* [WEB] [Consultat el 1 de desembre de 2022] Disponible a: https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/allow-os.html

```
<agent_config>

  <!-- Shared agent configuration he

<wodle name="syscollector">
   <disabled>no</disabled>
   <interval>1h</interval>
   <os>yes</os>
   <packages>yes</packages>
   <hotfixes>yes</hotfixes>
</wodle>



</agent_config>
```

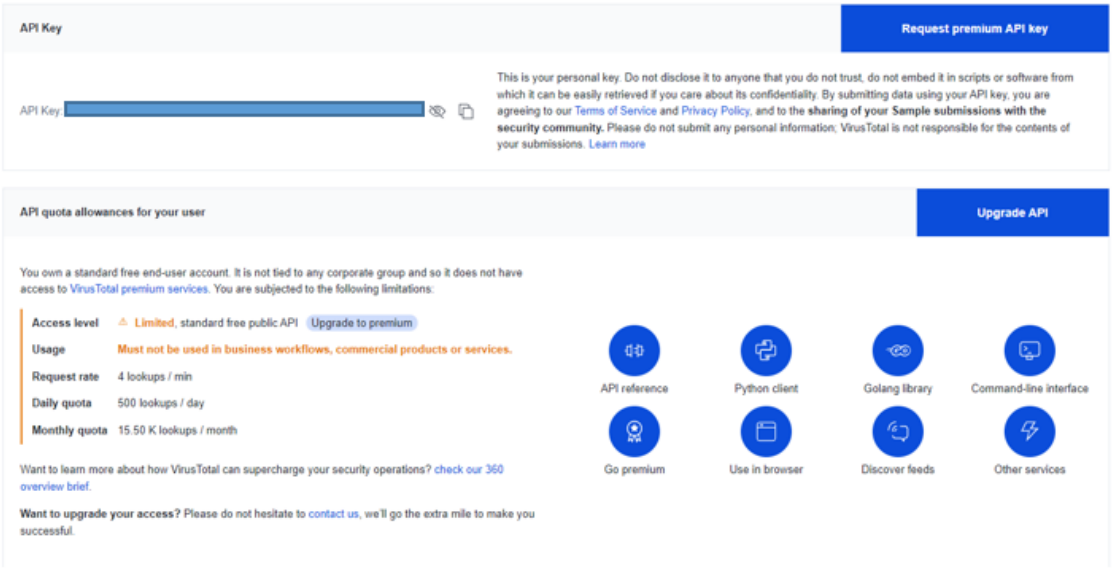
Un cop reconfigurats els agents, ja només haurem d'activar el mòdul en la configuració del servidor i esperar el temps necessari perquè es realitzi la sincronització.

```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>stretch</os>
    <os>buster</os>
    <os>bullseye</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- RedHat OS vulnerabilities -->
  <provider name="redhat">
    <enabled>yes</enabled>
    <os>5</os>
    <os>6</os>
    <os>7</os>
    <os>8</os>
    <os>9</os>
    <update_interval>1h</update_interval>
  </provider>
```

Activarem el mòdul i cada sistema operatiu que consti com agent i vulguem que es realitzi la verificació. Finalment guardarem i reiniciarem el servidor perquè els canvis entrin en funcionament.

9.6. Afegir funcionalitat d'escaneig de fitxers amb l'API de Virus Total:

Per tal d'afegir la integració de l'eina d'escaneig del web Virus Total, primer de tot ens haurem de donar d'alta per obtenir un codi únic d'accés a la seva API. En cas de ser un usuari d'ús gratuït, ens oferirà el servei amb certes limitacions com ara 4 cerques per minut, 500 per dia i 15,500 per més.
Pel cas concret d'ús de l'Ajuntament del Masnou, al ser una corporació, s'hauria de contractar el servei d'una API de pagament, sinó estaríem incomplint els requisits del seu llicenciament, però de moment pel cas d'aquest treball i a mode de prova de concepte, ho realitzarem amb l'API gratuïta.



Un cop ens hem registrat, ja podem obtenir el codi de la nostre API personalitzada, i passarem a la configuració del servei en el Wazuh, segons la guia oficial[21].

En l'apartat de configuracions, afegirem el codi següent:

```
<!-- External integration -->
  <integration>
    <name>virustotal</name>
    <api_key>[redacted]</api_key> <!-- Replace with your VirusTotal API key -->
    <group>syscheck</group>
    <alert_format>json</alert_format>
</integration>
```

Un cop aplicat i reiniciat el servidor ja podríem utilitzar el servei.

[21] WAZUH. *User manual – Capabilities - VirusTotal – integration - How it works* [Web] [Consultat el 1 de desembre de 2022] Disponible a: https://documentation.wazuh.com/current/user-manual/capabilities/virustotal-scan/integration.html#use-case-scanning-a-file