UNIVERSITAT DE BARCELONA

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

MALWARE SCAN
Cortex i la Centralització del Coneixement en Seguretat

Autor: Alicia Carrasco Guardiola

Director: Dr. Raul Roca
Realitzat a: Departament d'Informàtica

Barcelona, 17 de gener de 2024

Resum

En el context actual de la ciberseguretat, la detecció i resposta a amenaces cibernètiques són fonamentals per a protegir la integritat de la informació i els sistemes. Com a Treball de Fi de Grau (TFG), he desenvolupat una aplicació anomenada "Malware Scan". Aquesta plataforma web s'ha dissenyat per a analitzar els registres generats pel sistema Cortex XDR i proporcionar informació addicional, recomanacions i un marc col.laboratiu per a la gestió d'amenaces.

"Malware Scan" no sols examinen els registres a la recerca d'amenaces, sinó que també enriqueix les alertes amb context addicional, facilitant la col.laboració entre organitzacions i equips de seguretat. A través d'aquesta investigació, es pretén avaluar a fons aquesta eina que he desenvolupat i la seva capacitat per a millorar la ciberseguretat en un entorn digital en constant canvi.

Paraules clau: ciberseguretat, anàlisi d'amenaces, incidents de seguretat, alertes, resposta a incidents.

Abstract

In the current context of cybersecurity, detection and response to cyber threats are essential to protect the integrity of information and systems. As a Final Degree Project (TFG), I have developed an application called "Malware Scan". This web platform is designed to analyze the logs generated by the Cortex XDR system and provide additional information, recommendations and a collaborative framework for threat management.

"Malware Scan" not only examines logs for threats, but also enriches alerts with additional context, facilitating collaboration between organizations and security teams. Through this research, I intend to thoroughly evaluate this tool that I have developed and its ability to improve cybersecurity in an ever-changing digital environment.

Keywords: cybersecurity, threat analysis, security incidents, alerts, incident response.

Índex

1 Introducció

La ciberseguretat esdevé un pilar fonamental de l'era digital actual. La capacitat de detectar i respondre eficaç i ràpidament a les amenaces cibernètiques és necessària per a protegir la integritat de la informació, així com els sistemes. En aquest context, he desenvolupat l'aplicació "Malware Scan" com a part del meu Treball de Fi de Grau (TFG). Aquesta plataforma web té l'objectiu d'analitzar els registres generats per l'eina Cortex XDR i proporcionar informació addicional, recomanacions i un entorn col.laboratiu per a la gestió d'amenaces.

"Malware Scan" tracta de centralitzar la visió i el coneixement en la detecció d'amenaces. L'aplicació no sols examina els registres a la recerca de possibles riscos, sinó que també enriqueix les alertes amb recomanacions addicionals i, en aquest mateix apartat, facilita la col.laboració entre organitzacions i analistes de seguretat.

Aquest projecte tracta també de ser una contribució a la comunitat de seguretat informàtica. A través d'aquesta recerca, s'aspira a proporcionar una solució original per a poder abordar les amenaces cibernètiques amb més facilitat i millorar la seguretat en un entorn digital, cada vegada més interconnectat.

1.1 Elecció de làmbit i tema de treball

L'elecció d'aquest tema i el seu àmbit de recerca troba el seu fonament en una sèrie d'experiències i motivacions, tant personals com professionals, que han modelat el meu interès i compromís amb el camp de la ciberseguretat.

Fa aproximadament un any, vaig tenir l'oportunitat de realitzar les meves pràctiques en el camp de la ciberseguretat en una consultoria. Durant aquest període, vaig ser introduïda en un món molt dinàmic i en constant evolució, on vaig rebre les primeres directrius i experiències pràctiques. Més tard, vaig iniciar la feina en la que actualment continuo, del sector públic, també en el departament específic de la seguretat de la informació.

L'àmbit de la ciberseguretat sempre havia estat una de les meves passions des de ben jove. Fins i tot en els meus anys d'adolescència, mostrava un gran interès per protegir els meus comptes en línia (majoritàriament xarxes socials), implementant contrasenyes úniques per a cada plataforma. Aquesta precaució, que podria semblar obsessiva, es un principi fonamental de la seguretat informàtica: la gestió adequada de les contrasenyes.

Amb aquesta base d'experiència i passió per la seguretat informàtica, justifico l'elecció del meu Treball de Fi de Grau en aquest àmbit. El meu objectiu és aprofundir en la base dels meus coneixements i comprendre a fons les complexitats i desafiaments que involucra la ciberseguretat, aplicant les meves habilitats i experiències en un context de recerca acadèmica.

D'altra banda, considerant el meu historial acadèmic, on les assignatures relacionades amb el desenvolupament de software van representar un gran desafiament, em va semblar interessant enfrontar aquest repte i submergir-me en l'àmbit de l'enginyeria de *software*. L'elaboració d'una pàgina web, amb totes les seves fases de desenvolupament que comporta, es presenta com una oportunitat d'aprenentatge significativa en el qual puc aplicar i millorar les meves habilitats tècniques.

Aquest treball de recerca, aleshores, representa una convergència dels meus interessos personals i professionals en el camp de la ciberseguretat, així com una oportunitat per a expandir els meus coneixements i habilitats en enginyeria de *software*. A través d'aquest projecte, tinc intenció de contribuir a l'enteniment i millora de la seguretat informàtica, a la vegada que afronto un repte en el desenvolupament de programari.

1.2 Objectius del treball

A continuació es llisten els objectius d'aquest treball:

- Contribuir a la Pràctica Professional:

Proporcionar recomanacions i millors pràctiques en funció dels resultats de la recerca que puguin ser aplicades en l'entorn professional de la ciberseguretat i el desenvolupament de programari.

- Comprendre el *MITRE ATT&CK*:

Aprofundir en l'enteniment del *MITRE ATT&CK*, especialment en les tàctiques i tècniques utilitzades per actors maliciosos, per a aplicar aquest coneixement en l'anàlisi de les alertes de seguretat.

- Avaluar la Seguretat de l'Aplicació:

Identificar i abordar possibles vulnerabilitats de seguretat en l'aplicació "Malware Scan", amb l'objectiu de millorar la seva robustesa.

- Desenvolupar Competències en Desenvolupament Web:

Adquirir habilitats en el desenvolupament web a través de la creació completa d'una pàgina web, incloent el seu disseny, implementació, gestió de bases de dades i desplegament.

- Millorar la presa de decisions en Seguretat:

Avaluar la utilitat de la informació extreta per l'aplicació creada en la optimització de la presa de decisions de seguretat en l'àmbit de la resposta a incidents.

- Fomentar la col.laboració interorganitzacional:

Promoure la col.laboració entre equips de ciberseguretat en l'anàlisi previ i posterior resposta als incidents.

1.3 Estructura del treball

Abans d'iniciar amb el contingut d'aquest treball, he considerat fonamental justificar l'estructura que s'ha aplicat en aquest.

En el pròxim capítol, es presenta una revisió literària, destinada a abordar els coneixements de l'àmbit de la seguretat cibernètica que són essencials per a comprendre tant el propòsit com les funcionalitats d'aquest projecte des d'una visió de ciberseguretat.

A continuació, es desenvolupa el Capítol 3, on s'ha dividit el marc teòric en quatre parts clau, corresponents a les quatre eines fonamentals utilitzades en el projecte. En primer lloc, es troba Cortex XDR, que serveix com a referència i base en l'àmbit de la ciberseguretat. Seguidament, es detallen dos elements centrals del projecte, Nuxt.js i Supabase, que aborden respectivament el frontend i la base de dades. Finalment, l'eina de desplegament Vercel.

El quart apartat es concentra en la part de disseny i desenvolupament web, incloent tots els aspectes relacionats amb l'enginyeria de programari, que, encara que no sigui la part central del TFG, ha estat un component molt necessari en el desenvolupament del projecte.

A continuació, el cinquè apartat aborda les funcionalitats de seguretat implementades en l'aplicació. Això abasta des de la selecció inicial de dades, passant per la informació addicional incorporada, fins a la relació amb les recomanacions de seguretat.

A mesura que avancem, ens trobem amb els apartats de Resultats i Discussió, Conclusió, Desenvolupament Futur, Contribucions i Bibliografia. Cadascun d'aquests apartats compleix un rol específic en l'estructura del treball, i els seus noms indiquen clarament el seu contingut i enfocament.

2 Revisió de la literatura

2.1 Conceptes fonamentals de ciberseguretat

En l'era digital actual, la ciberseguretat es manifesta com un pilar essencial per a salvaguardar la integritat i confidencialitat de la informació. Tal com va dir Bruce Schneier, "En ciberseguretat, entendre els conceptes fonamentals és com tenir un mapa en un territori desconegut. Sense aquest coneixement, és difícil navegar i prendre decisions informades." Amb la creixent interconnexió de sistemes i l'omnipresència de dades digitals, les organitzacions es veuen desafiades per amenaces cada vegada més sofisticades. En aquest apartat es busca explorar els fonaments de la ciberseguretat, específicament en el context de l'anàlisi d'amenaces, establint una connexió coherent entre els principis bàsics, la identificació d'amenaces, la gestió de riscos i l'evolució de les estratègies de seguretat, amb aquests conceptes fonamentals ens introduirem en l'entorn de Cortex XDR, l'eina clau d'aquest treball.

Els principis bàsics de la ciberseguretat, encapsulats en la triangle de seguretat anomenat CIA, Confidencialitat, Integritat i Accessibilitat, són el punt de partida essencial.

Figura 1: Triangle de Seguretat CIA

La confidencialitat garanteix que només aquells autoritzats accedeixin a la informació, la integritat vetlla per la consistència i precisió de les dades, i la accessibilitat assegura que els recursos estiguin disponibles quan es necessitin. Aquests principis proporcionen el marc conceptual necessari per a abordar els desafiaments dinàmics de l'anàlisi d'amenaces. En paraules d'Eugene Spafford, "Els conceptes fonamentals de ciberseguretat, com la gestió d'identitats i la privacitat, són els fonaments sobre els quals construïm una defensa sòlida contra les amenaces digitals."

l'anàlisi d'amenaces implica la identificació i comprensió dels riscos potencials que poden afectar a la seguretat dels sistemes. En reconèixer amenaces específiques i les vulnerabilitats susceptibles de ser explotades, les organitzacions poden dissenyar contramesures efectives. Aquest procés d'identificació estableix un vincle crucial amb els principis bàsics, ja que la protecció contra amenaces es basa en la preservació de la confidencialitat, integritat i accessibilitat.

La gestió de riscos en ciberseguretat implica un enfocament proactiu i continu per a adaptar-se a un panorama d'amenaces en constant evolució. Avaluar, mitigar i monitorar els riscos identificats es converteix en un procès dinàmic que busca preservar la seguretat de la informació. Aquest enfocament continu reflecteix la necessitat d'alinear l'estratègia de ciberseguretat amb els principis bàsics i la identificació d'amenaces.

l'evolució de la seguretat, des de les solucions antivirus tradicionals fins a enfocaments més avançats com XDR, reflecteix l'adaptació contínua a amenaces emergents. Aquest procés evolutiu no sols implica adoptar noves tecnologies, sinó també canviar paradigmes en la resposta a amenaces. La flexibilitat i capacitat de resposta són essencials per a mantenir la integritat, confidencialitat i accessibilitat en un entorn d'anàlisi d'amenaces.

2.2 Eines i tecnologies en ciberseguretat

En làmbit específic de l'anàlisi d'amenaces, es requereix una combinació estratègica d'eines i tecnologies especialitzades per a garantir l'eficàcia del procés i la protecció dels actius digitals involucrats.

Les plataformes d'anàlisi d'amenaces es beneficien enormement d'eines d'intel.ligència d'amenaces que recopilen, analitzen i correlacionen informació sobre les amenaces actuals. Aquestes eines permeten una presa de decisions informada sobre les possibles amenaces que podrien afectar la plataforma.

Aquestes eines avançades d'anàlisis de comportament són essencials per a detectar patrons anómals dins de l'activitat dels sistemes, ja que utilitzen algorismes avançats per a identificar comportaments fora del comú que podrien indicar possibles amenaces o activitats malicioses i, les eines que permeten la resposta ràpida i automàtica a esdeveniments de seguretat, com la quarantena de sistemes compromesos o l'actualització de regles de seguretat, són fonamentals per a mitigar riscos de manera eficient.

Pel que fa a l'anàlisi forense digital, l'ús d'aquestes eines específiques faciliten la reconstrucció d'esdeveniments després d'una amenaça o incident. Aquestes eines permeten una recerca profunda per a comprendre la naturalesa de l'amenaça i millorar les estratègies de seguretat. Un altre punt a destacar és la combinació de tecnologies de detecció basada en signatures i comportament, la qual ofereix una defensa integral. La detecció basada en signatures identifica amenaces conegudes, mentre que la detecció basada en comportament revela activitats anòmales que podrien indicar noves amenaces. Tal com diu Mikko Hyppönen, 'Les amenaces evolucionen constantment, i les nostres eines d'anàlisis han d'evolucionar amb elles. La tecnologia exerceix un paper fonamental en la nostra capacitat per a comprendre i combatre les amenaces digitals en constant canvi.'

Durant aquest treball tractarem de treure el màxim profit de la integració de totes aquestes funcionalitats específiques en l'anàlisi d'amenaces a partir de la plataforma Cortex XDR.

2.3 Evolució de la Seguretat: d'Antivirus a XDR

L'evolució de les solucions de seguretat, des dels antivirus tradicionals fins a la detecció i resposta estesa (XDR, per les seves sigles en anglès), reflecteix la creixent complexitat de les amenaces cibernètiques i la necessitat d'enfocaments més avançats per a protegir els sistemes. A continuació, i per a contextualitzar l'evolució i arribada a les eines XDR, com Cortex XDR, s'explica un resum de la seva evolució:

2.3.1 Antivirus Tradicional

Els antivirus tradicionals són programes dissenyats per a identificar, prevenir i eliminar programari maliciós, conegut com *malware*, dels sistemes informàtics. El seu criteri principal es basa en la identificació de patrons específics de codi, anomenats signatures.

Aquests antivirus mantenen una base de dades de signatures que correspon als patrons especfícs associats als *malware*s coneguts. Quan un arxiu o programa és escanejat, l'antivirus compara el seu contingut amb les signatures de la base de dades per a identificar amenaces potencials. A més, utilitzen tècniques heurístiques per a analitzar el comportament dels programes a la recerca d'activitats sospitoses, permetent la detecció d'amenaces fins i tot si no coincideixen amb signatures conegudes.

Els escanejos exhaustius d'arxius i directoris són una característica comuna dels antivirus tradicionals. Aquestes anílisis poden ser programades o iniciades manualment per l'usuari, i busquen identificar i eliminar qualsevol *malware* present en el sistema.

L'actualització periòdica de les bases de dades de signatures és imprescindible per a l'efectivitat dels antivirus tradicionals, ja que aquestes actualitzacions permeten als programes abordar les noves amenaces que sorgeixen constantment en el panorama cibernètic. Malgrat la seva importància històrica en la seguretat informàtica, els antivirus tradicionals tenen limitacions, ja que poden ser menys efectius contra amenaces desconegudes per a les quals no tenen signatures i poden ser vulnerables a tàctiques d'evasió avançades utilitzades per uns certs tipus de *malware*. Amb l'augment de la sofisticació de les ciberamenaces, han sorgit enfocaments més avançats, per a proporcionar una protecció més integral i adaptativa contra les amenaces cibernètiques modernes. A continuació es mostra una imatge que tracta de resumir el procés anteriorment explicat:

Figura 2: Resum funcionament antivirus

2.3.2 Evolució d'Antivirus a Solucions EDR

La transició des dels enfocaments tradicionals d'antivirus cap a les solucions d'*Endpoint Detection and Response* (EDR) representa una resposta necessària a la constant evolució de les amenaces cibernètiques. Brian Dye, president de Symantec, conegut per l'antivirus Norton va dir el següent: "Els antivirus són una part important de l'estratègia de seguretat, però han de combinar-se amb enfocaments més avançats, com la detecció d'amenaces basada en comportaments". Mentre que els antivirus tradicionals han estat fonamentals en la identificació de *malware* conegut mitjançant signatures i heurístiques, les solucions EDR han emergit per a abordar les limitacions inherents a aquest model.

En el context de la seguretat informàtica, les solucions EDR es centren en el monitoratge constant d'esdeveniments i activitats en els *endpoints*, els quals són els dispositius finals dins d'una xarxa (ordinadors, servidors, dispositius mòbils, en d'altres). Aquest enfocament proactiu implica la detecció de possibles amenaces en temps real i la capacitat de respondre de manera immediata davant d'esdeveniments de seguretat.

Una de les característiques principals de les solucions EDR és la visibilitat avançada que proporcionen. En analitzar exhaustivament l'activitat en els *endpoints*, aquestes solucions ofereixen una comprensió detallada dels comportaments i activitats que podrien indicar la presència d'amenaces cibernètiques. Aquesta visibilitat més profunda permet a les organitzacions identificar de manera primerenca comportaments anòmals, una capacitat crucial en la detecció i mitigació proactiva d'amenaces avançades i persistents.

La capacitat de resposta activa és una altra part distintiva de les solucions EDR. En lloc de dependre únicament de la identificació de signatures, aquestes solucions permeten als equips de seguretat actuar immediatament davant esdeveniments sospitosos, contenint i mitigant les amenaces abans que puguin causar un mal significatiu. Aquesta capacitat de resposta ràpida és necessària en un panorama d'amenaces on la velocitat de reacció pot marcar la diferència entre una intrusió menor i un incident de seguretat greu.

No obstant això, és important reconèixer que les solucions EDR també presenten

desafiaments, donat que la quantitat substancial de dades generades pel monitoratge constant requereix una anàlisi eficient per a identificar amenaces de manera efectiva. A més, la interpretació i l'acció sobre aquestes dades demanden un personal amb coneixements en l'àmbit d'anàlisi d'amenaces.

En la figura que tenim a continuacó podem veure un petit resum que mostre l'abast dels EDR, en comparació amb l'antivirus.

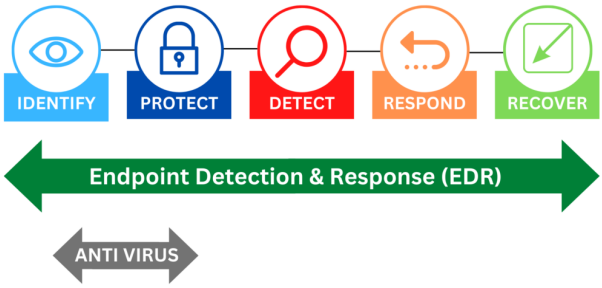

Figura 3: EDR vs Antivirus

Veiem que l'evolució cap a solucions EDR representa un pas endavant en la seguretat cibernètica, superant les limitacions dels enfocaments dels antivirus tradicionals. Aquestes solucions no sols ofereixen una visibilitat més profunda i una capacitat de resposta activa, sinó que també reflecteixen la alta necessitat d'estratègies més proactives i àgils per a fer front a les amenaces cibernètiques en constant evolució.

2.3.3 Transició a XDR

La transició des de les anteriorment explicades solucions d'*Endpoint Detection and Response* (EDR) cap a un paradigma més integral conegut com a *eXtended Detection and Response* (XDR) representa una evolució significativa en la resposta a les amenaces cibernètiques. A mesura que les tàctiques dels ciberdelinqüents segueixen tornant-se més complexes, les organitzacions busquen enfocaments encara més avançats i holístics per a enfortir la seva postura de seguretat.

En el context d'EDR, l'enfocament se centra principalment en el monitoratge i resposta a esdeveniments de seguretat en *endpoints*, com a ordinadors i servidors. Aquesta solució ofereix una visió detallada i activa de les amenaces, però es limita a l'àmbit específic dels dispositius finals.

La transició cap a Detecció i Resposta Estesa (XDR) implica una expansió de l'abast. XDR va més enllà dels *endpoints* i incorpora la detecció i resposta a amenaces en múltiples punts de la infraestructura d'IT, unificant la informació de diverses fonts, incloses xarxes, *endpoints* i sistemes en el núvol.

Una característica clau de XDR és la seva capacitat avançada de correlació de

dades. Pot identificar patrons i amenaces a través de diferents capes de seguretat, proporcionant un context integral per a entendre la naturalesa i l'abast de les amenaces. Això permet una visió més completa de les activitats malicioses i millora la capacitat de detecció i resposta.

A més, XDR ofereix un context global més ampli, permetent una comprensió més profunda de les tàctiques, tècniques i procediments utilitzats pels atacants. Facilita una resposta més eficient en proporcionar informació contextual que ajuda a prioritzar accions i millora la coordinació de respostes en tota la infraestructura de IT.

2.4 El Model MITRE ATT&CK en la Seguretat Cibernètica

El Model MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) s'ha convertit en un marc de referència essencial en el camp de la seguretat cibernètica. Desenvolupat per MITRE Corporation, aquest model proporciona una àmplia matriu que descriu tàctiques i tècniques utilitzades pels actors d'amenaces cibernètiques per a comprometre sistemes i xarxes. El MITRE ATT&CK s'ha convertit en una eina inavaluable per a la comprensió, detecció i resposta a amenaces cibernètiques, i la seva influència en la comunitat de seguretat és notable.

El model ATT&CK es basa en una matriu que enumera les tàctiques dels adversaris (per exemple, "Execució" o "Persistència") i les tècniques específiques que utilitzen dins de cada tàctica (per exemple, "Execució de codi en procés en memòria" o "Injecció de DLL"). Aquesta matriu s'ha convertit en una guia exhaustiva que ajuda els professionals de seguretat a comprendre com els atacants poden dur a terme les seves accions i com es poden detectar i prevenir.

A continuació, es mostra una imatge d'una part de la taula MITRE ATTCK. No obstant això, és important tenir en clar que aquesta taula està en constant evolució. Per tant, per a obtenir la informació més fiable i actualitzada, el més recomanable és consultar-la en el lloc oficial de MITRE.

Figura 4: Matriu MITRE ATT&CK

Una dels avantatges clau del Model MITRE ATT&CK és el seu enfocament en l'adversitat. En lloc de centrar-se únicament en les vulnerabilitats i les amenaces conegudes, el model es concentra en les tàctiques i tècniques que els actors d'amenaces poden utilitzar. Això permet als equips de seguretat anticipar i respondre a amenaces desconegudes i avançades de manera més efectiva.

El Model MITRE ATT&CK s'ha convertit en un recurs àmpliament utilitzat per organitzacions de tot el món per a millorar les seves estratègies de seguretat cibernètica. Les empreses ho empren per a avaluar les seves postures de seguretat, identificar àrees de risc i enfortir els seus sistemes de detecció i resposta. A més, la comunitat de seguretat cibernètica comparteix constantment informació sobre noves tècniques i tàctiques observades en el camp, la qual cosa enriqueix encara més la matriu del MITRE ATT&CK.

3 Marc teòric

En el marc teòric d'aquest treball, es presenten les quatre eines principals del meu treball, cadascuna de les quals es relaciona amb un aspecte fonamental del desenvolupament d'aquest projecte. A continuació trobem un petit resum sobre l'eina de seguretat: Cortex, l'eina de desenvolupament frontend: Nuxt, l'eina de gestió de bases de dades: Supabase i l'encarregat del *hosting*: Vercel.

3.1 Cortex XDR

3.1.1 Introducció a Cortex XDR

Dins del marc teòric del meu treball, l'eina central i de major rellevància és Cortex XDR, desenvolupada per Palo Alto Networks. Cortex XDR destaca per la seva capacitat avançada de correlació de dades, unificant informació de diversos punts de la infraestructura de IT, incloent *endpoints*, xarxes i entorns en el núvol. Aquesta capacitat facilita la identificació de patrons i amenaces de manera efectiva, proporcionant un context integral per a comprendre les tàctiques i tècniques dels atacants. A més, destaca per la seva eficiència en la resposta a incidents, oferint eines per a una resposta ràpida i coordinada.

En el panorama actual de seguretat, on les amenaces cibernètiques evolucionen constantment, Cortex XDR es posiciona com una de les eines més utilitzades per a enfortir la postura de seguretat de les organitzacions.

3.1.2 Funcions principals de Cortex XDR

La capacitat distintiva de Cortex XDR recau en la seva habilitat per a correlacionar dades en temps real. Aquesta funció, en unificar informació provinent de diversos punts de la infraestructura, incloent *endpoints*, xarxes i entorns en el núvol, permet una identificació més eficient de patrons i amenaces. La correlació de dades proporciona un context integral que facilita la comprensió profunda de les tàctiques i les tècniques utilitzades pels atacants, permetent a les organitzacions anticipar i respondre proactivament a possibles riscos.

Més enllà de la mera detecció, Cortex XDR s'enfoca en la resposta ràpida i coordinada davant incidents de seguretat. La plataforma no sols identifica amenaces, sinó que també proporciona les eines necessàries per a una resposta àgil. La informació contextual, derivada de la correlació de dades, potència la presa de decisions informada, millorant significativament la capacitat de mitigar i contenir amenaces de manera eficient, minimitzant així l'impacte dels incidents. Sobre aquest tema, David Boone, Vicepresident de Serveis de Seguretat i CISO de Palo Alto Networks, destaca que "Cortex XDR utilitza intel.ligència artificial per a prevenir amenaces abans que afectin".

Un altre aspecte clau de Cortex XDR és la seva capacitat per a oferir una visió completa de la infraestructura de IT. Això permet a les organitzacions comprendre les activitats malicioses en tota la seva extensió, una visibilitat integral que resulta essencial per a anticipar i contrarestar amenaces que utilitzen múltiples vectors i tàctiques per a eludir les defenses tradicionals.

En resum, les funcions clau de Cortex XDR dins del marc teòric de la seguretat cibernètica no sols reforcen la capacitat de detecció precoç d'amenaces, sinó que també proporcionen eines pràctiques per a una gestió eficient i coordinada d'incidents. Aquestes capacitats són crucials per a enfortir la postura de seguretat de les organitzacions en un entorn digital dinàmic i desafiador.

3.1.3 Integració de Cortex XDR en l'Arquitectura de Seguretat

Cortex XDR no opera en aillament; en canvi, s'integra de manera holística en l'arquitectura de seguretat. La plataforma s'adapta a les solucions de seguretat existents, es personalitza segons les necessitats i polítiques de cada organització, automatitza fluxos de treball i s'integra amb fonts externes d'intel.ligència d'amenaces. Aquesta integració assegura una resposta coordinada i efectiva a les amenaces i garanteix l'escalabilitat i adaptabilitat a mesura que les necessitats de seguretat evolucionen.

3.2 Nuxt.js

Introducció a Nuxt.js Nuxt.js és un marc de desenvolupament web de codi obert que es basa en Vue.js, un *framework* JavaScript àmpliament utilitzat en la creació d'aplicacions web. El que distingeix a Nuxt.js és el seu enfocament a simplificar el procés de desenvolupament d'aplicacions web, proporcionant una estructura sòlida i convencions predefinides que ajuden els desenvolupadors a crear aplicacions més ràpidament i de manera més eficient. Característiques principals de Nuxt.js Una de les característiques més destacades de Nuxt.js és el seu enfocament en la renderització del costat del servidor (SSR) i la generació estàtica (SSG). La renderització del costat del servidor implica que les pàgines web generades per Nuxt.js es processen en el servidor abans de ser enviades al client. Això té diversos avantatges, com millorar la velocitat de càrrega de les pàgines, optimitzar la indexació en els motors de cerca i proporcionar una experiència d'usuari més ràpida i fluida.

A més del SSR, Nuxt.js també ofereix la generació estàtica (SSG). Això permet que les pàgines web es pre-renderitzin completament durant el procés de compilació. Aquesta funcionalitat és especialment útil per a contingut estàtic que no canvia amb freqüència, ja que permet lliurar contingut de manera ultraràpida als usuaris, millorant encara més l'eficiència i la velocitat de càrrega de l'aplicació.

Un altre avantatge clau de Nuxt.js és el seu sistema d'encaminament automàtic. En lloc de requerir una configuració manual tediosa de rutes, Nuxt.js genera au-

tomàticament les rutes de l'aplicació en funció de l'estructura d'arxius del projecte. Això estalvia temps i evita possibles errors humans en la configuració de rutes, la qual cosa facilita encara més el procés de desenvolupament.

Nuxt.js també s'integra de manera nativa amb Vuex, una biblioteca de gestió d'estats per a Vue.js. Això simplifica la gestió de dades en l'aplicació i garanteix la coherència en tot el projecte, la qual cosa és essencial per a aplicacions web complexes i dinàmiques.

A més d'aquestes característiques, Nuxt.js compta amb una comunitat activa i un ecosistema de complements i mòduls que faciliten l'expansió de les funcionalitats d'una aplicació web. Això redueix la necessitat de desenvolupar components personalitzats des de zero i accelera significativament el procés de desenvolupament.

3.3 Supabase

3.3.1 Introducció a Supabase

Quant a la gestió de dades, Supabase ha estat l'elecció per a la capa de *backend* de l'aplicació. Supabase és una plataforma de codi obert que ofereix una alternativa versàtil per a la gestió de bases de dades en aplicacions web i mòbils. Es basa en *PostgreSQL*, un sistema de gestió de bases de dades àmpliament reconegut per la seva robustesa i rendiment.

3.3.2 Característiques principals de Supabase

La plataforma Supabase proporciona una sèrie d'avantatges i característiques, entre els quals trobem la facilitat d'ús i l'experiència del desenvolupador. Ofereix, aleshores, una interfície d'usuari intuïtiva que simplifica la creació i administració de bases de dades. A més, proporciona eines de desenvolupament i APIs que faciliten la integració amb diverses aplicacions ja existents.

La plataforma incorpora també característiques d'autenticació i seguretat avançades per a protegir les dades emmagatzemades en la base de dades. Això inclou autenticació amb proveïdors d'identitat externs, com Google o Github, la qual cosa amplia les possibilitats de la gestió d'usuaris.

Supabase ofereix APIs en temps real que permeten la transmissió de dades en temps real entre aplicacions i bases de dades. Aquest punt és útil per a les funcionalitats de l'aplicació que requereixen actualitzacions instantànies. La plataforma també permet l'automatització de tasques rutinàries d'administració de bases de dades, com a còpies de seguretat i escalabilitat. Això allibera temps i recursos perquè els equips se centrin en el desenvolupament de característiques i millores.

Finalment, cal destacar com a característica el fet que Supabase està dissenyat per

a ser altament escalable i proporcionar un rendiment òptim, fins i tot en aplicacions amb alt trànsit, sent, aleshores, adequat per a projectes de qualsevol grandària.

3.4 Vercel

3.4.1 Introducció a Vercel

Vercel és una plataforma d'allotjament i desplegament d'aplicacions web que s'ha guanyat una reputació per la seva facilitat d'ús i el seu enfocament en l'automatització de tasques. Està dissenyada perquè els desenvolupadors puguin llançar i escalar aplicacions web de manera ràpida i senzilla, permetent un lliurament de contingut d'una forma més ràpida i eficient.

3.4.2 Característiques principals de Vercel

Una de les característiques més notables de Vercel és la seva capacitat per al desplegament ràpid i senzill d'aplicacions web. La plataforma automatitza gran part del procés d'implementació, la qual cosa permet als desenvolupadors llançar les seves aplicacions amb rapidesa i sense complicacions. Això és fonamental per a mantenir un cicle de desenvolupament àgil i per a oferir actualitzacions i noves característiques de manera eficient.

Vercel ofereix suport per a una àmplia varietat de piles tecnològiques, fet que significa que és compatible amb una àmplia gamma de llenguatges de programació i frameworks. Això brinda als desenvolupadors la flexibilitat de treballar amb les eines que millor s'adaptin a les seves necessitats, la qual cosa és especialment útil en un entorn on l'elecció de tecnologies és clau. També cal destacar que la plataforma incorpora capacitats d'automatització de tasques i un procés d'Integració Contínua / Lliurament Continu (CI/CD) integrat. Això permet als equips de desenvolupament automatitzar tasques com a proves, compilacions i desplegaments, la qual cosa garanteix la qualitat i la coherència del codi implementat. Com a última característica a mencionar, Vercel està dissenyat per a escalar automàticament en funció de la demanda de trànsit d'una aplicació. Això garanteix que les aplicacions es mantinguin disponibles i amb un rendiment òptim fins i tot en moments d'alt trànsit, la qual cosa és essencial per a oferir una experiència d'usuari sense interrupcions.

4 Disseny i desenvolupament de l'aplicació web

En la implementació de l'aplicació web dissenyada per a analitzar dades provinents de Cortex XDR, s'han aprofitat les característiques distintives de Nuxt.js, Supabase i Vercel per a aconseguir un sistema eficient, escalable i d'alt rendiment.

4.1 Arquitectura i disseny de l'aplicació

Quant a l'arquitectura de l'aplicació, s'ha decidit desactivar el renderitzat per SSR (Server Side Rendering) pel fet que, per als requisits, no existeixen suficients avantatges que justifiquin la complexitat afegida de tenir una aplicació renderitzada pel servidor. Si bé SSR ofereix importants beneficis, com la millora en el posicionament SEU (ja que els rastrejadors de Google indexen la pàgina de manera més efectiva en ser SSR i que proporcionar contingut més ràpid) o millores en el "*startup times*" de l'aplicació, aquests aspectes no són crítics per a una aplicació interna d'una empresa o un particular. Per tant, es pren la decisió, a meitat del projecte, de deshabilitar-lo a través de la configuració de Nuxt.

```
export default defineNuxtConfig( input: {
  ssr: false,
  spaLoadingTemplate: true,
```

Figura 5: Fragment arxiu nuxt.config.ts

En desactivar-ho, tot el projecte es renderitza en el costat del client, és a dir, fa una sol.licitud al servidor per a obtenir els arxius font, i és el navegador el que ha de processar els arxius i generar la pàgina web. Això implica, com s'esmenta anteriorment, un "*startup time*" més baix, per la qual cosa Nuxt ens ofereix l'opció de proporcionar un arxiu HTML amb un carregador que es mostrarà mentre el client prepara la pàgina (*spaLoadingTemplate: true*). Aquesta opció prendrà l'arxiu que col.loquis dins de "app/spa-loading-template" i mostrarà el seu contingut mentre es carrega la pàgina.

A pesar que no utilitzem la característica de Nuxt de renderitzat per SSR, aprofitem molts altres avantatges de Nuxt, ja que facilita molt el desenvolupament àgil. Per exemple, ofereix importacions automàtiques de components/utilitats/*composables*, encaminament basat en directoris i altres característiques que fan que utilitzar Nuxt sigui la millor opció.

Com a biblioteca de gestió d'estat compartit en l'aplicació, utilitzem Pinia, ja que és l'opció recomanada per Nuxt. Utilitzem aquesta biblioteca per a gestionar l'estat global de les alertes que es mostren per sobre de l'aplicació i també per a la barra de càrrega en realitzar accions en el servidor. Atès que els components que renderitzen les alertes i la barra de càrrega es troben en un sol lloc (layouts/default.vue) i han de poder ser anomenats des de qualsevol part de l'aplicació sense inconsistències de

dades.

Quant a la biblioteca d'estils, no utilitzem cap biblioteca de components Vue, ja que, encara que hauria simplificat el desenvolupament, el desenvolupament hauria d'adaptar-se a la API que proporcionen i aprendre coneixements que no són transferibles fora del domini de la biblioteca de components. Per tant, s'opta per utilitzar components de baix nivell de Nuxt/HTML. No obstant això, utilitzem una biblioteca d'estils, Tailwind, que proporciona propietats bàsiques de CSS a través de classes, simplificant en gran manera el codi i el nombre de propietats que han d'ingressar-se. és similar a Bootstrap però sense una estètica predefinida, la qual cosa brinda un gran potencial per a dissenyar qualsevol tipus d'interfície sense restriccions. També utilitzem biblioteques per a components més complexos, com Headless UI (per exemple, per a modals o diàlegs) o Tanstack Table (per a taules), ja que implementar-los des de zero seria tediós. No obstant això, cap d'aquests components inclou estils predeterminats.

Quant al backend de l'aplicació, utilitzem Supabase, del qual es proporcionaran més detalls en els punts següents.

Finalment, pel que fa als tipus, es va aplicar TypeScript en llocs específics, com la visualització de taules, però no es va anar estricte en la tipificació, ja que es buscava agilitat en el desenvolupament.

4.2 Interfície d'usuari i experiència de l'usuari

Per a dissenyar la interfície d'usuari, es va optar per un enfocament minimalista, atès que no es compta amb experiència en disseny i no és un punt fort en els objectius d'aquest projecte. Tots els estils es van crear utilitzant Tailwind CSS, aprofitant les classes predefinides, i es va prendre inspiració d'una biblioteca anomenada "Flowbite" que proporciona exemples d'HTML bàsic amb classes de Tailwind que es poden utilitzar sense cap dependència.

Malgrat aquest enfocament minimalista, es va buscar constantment aconseguir un disseny intuïtiu i fàcil d'usar, fins i tot si això implicava realitzar modificacions per a fer-ho més amigable des del punt de vista de l'experiència de l'usuari (UX). Es va posar un èmfasi especial en elements com a taules, modals i pàgines que mostren text de diverses maneres per a garantir una experiència d'usuari satisfactòria.

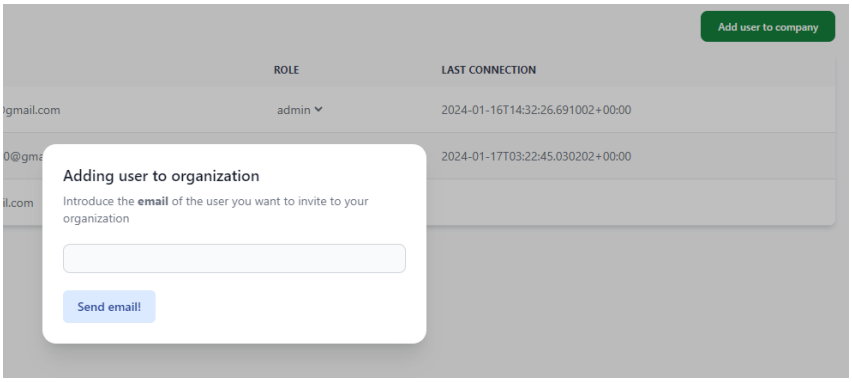

Figura 6: Exemple ús de dialegs

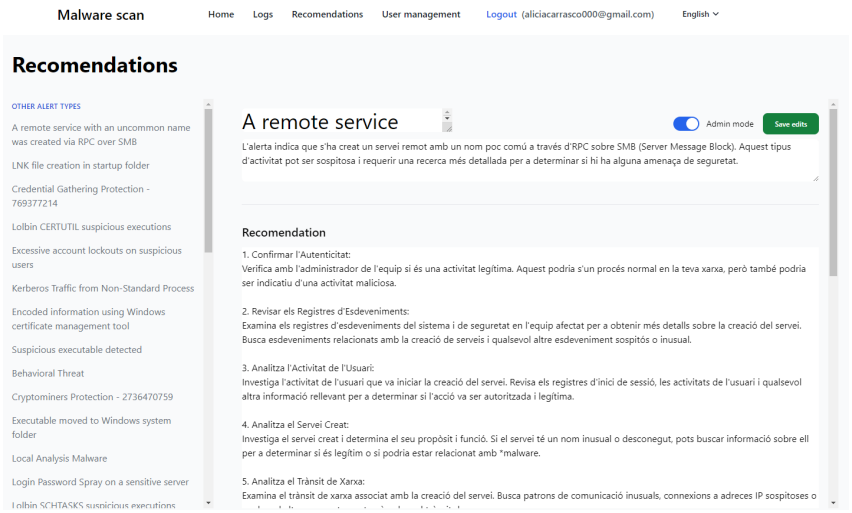

Figura 7: Exemple ús de modals

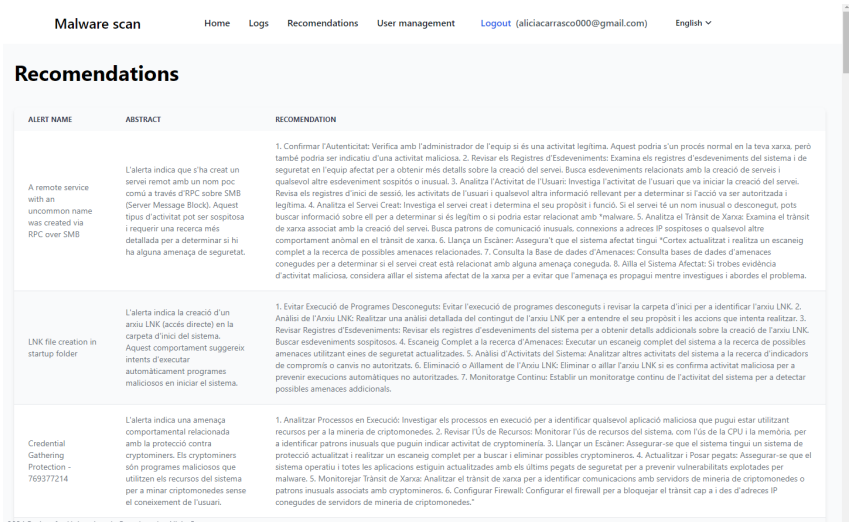

Figura 9: Exemple ús de taules

4.3 Integració amb Supabase

Com es va esmentar anteriorment, Supabase constitueix la base del backend de l'aplicació. Atès que no s'inclou en el projecte lliurat, ja que és una plataforma allotjada en el núvol, s'adjunten captures de les taules.

Figura 10: Taula scans

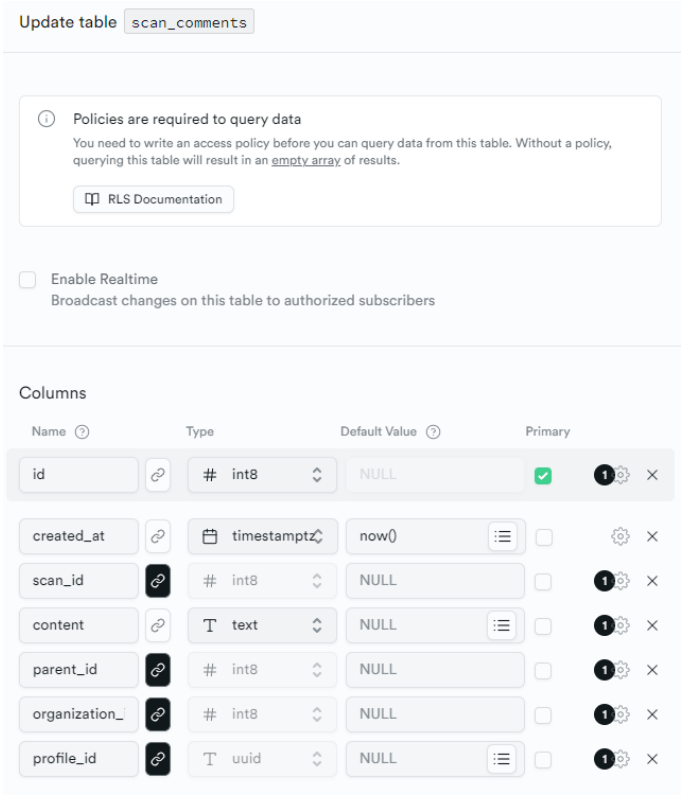

Figura 11: Taula dels comentaris dels scans

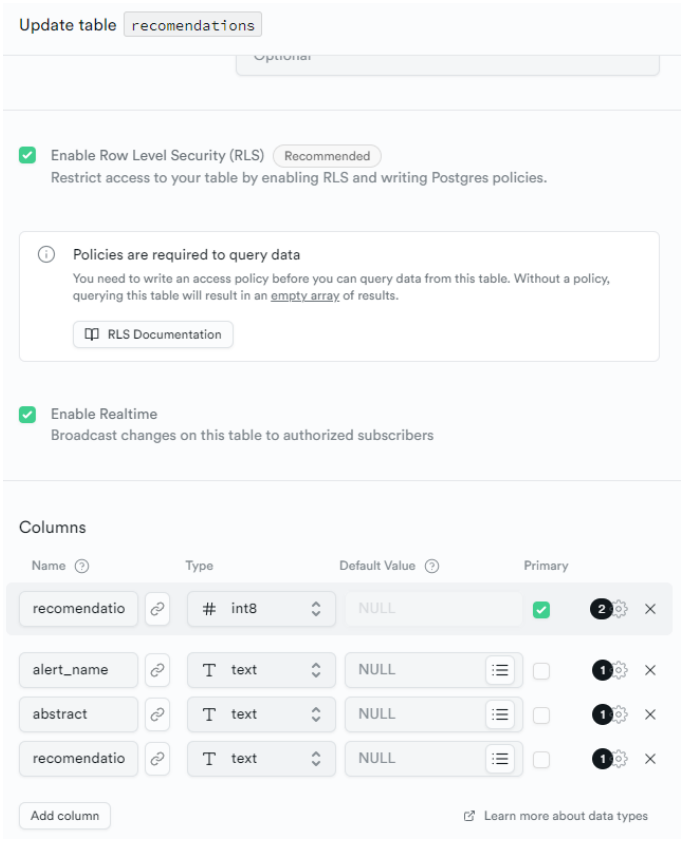

Figura 12: Taula recomanacions

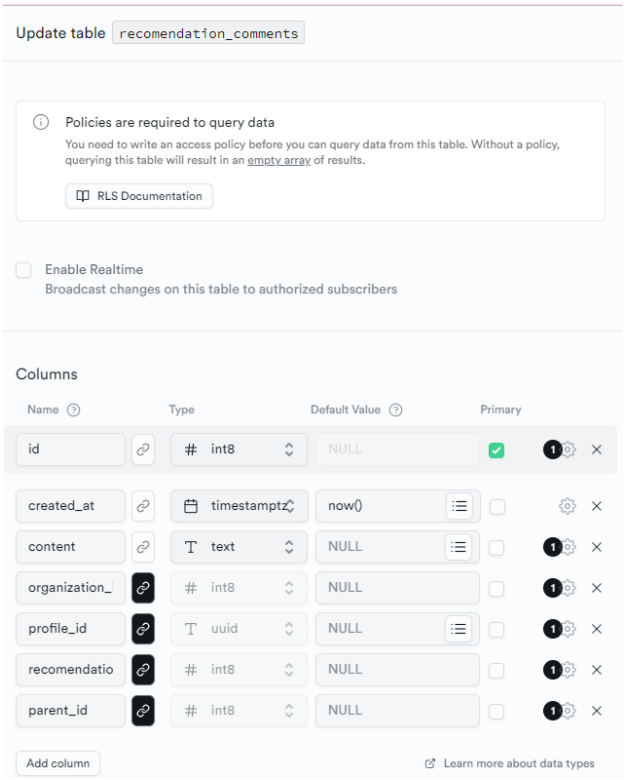

Figura 13: Taula dels comentaris de les recomanacions

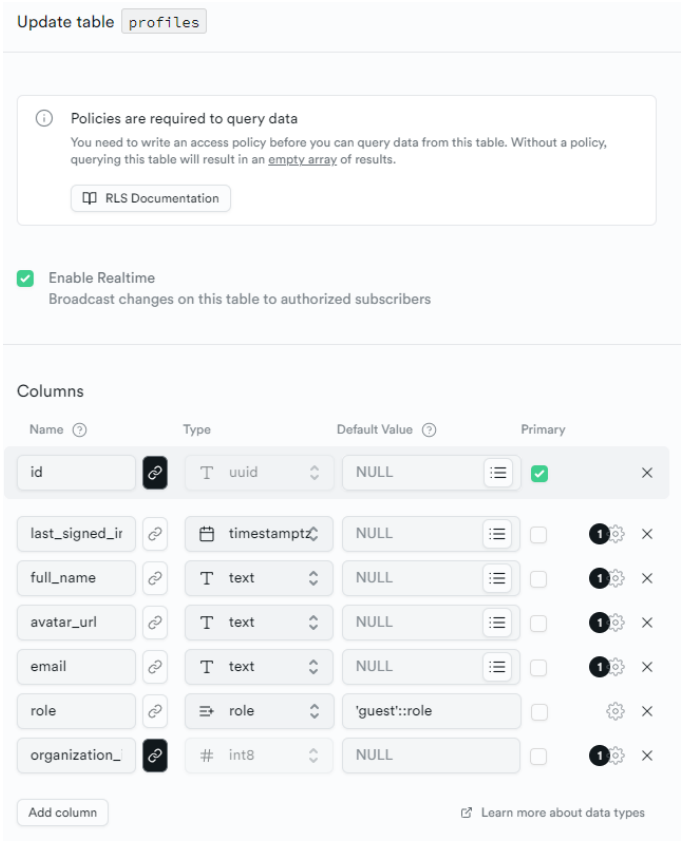

Figura 14: Taula perfils

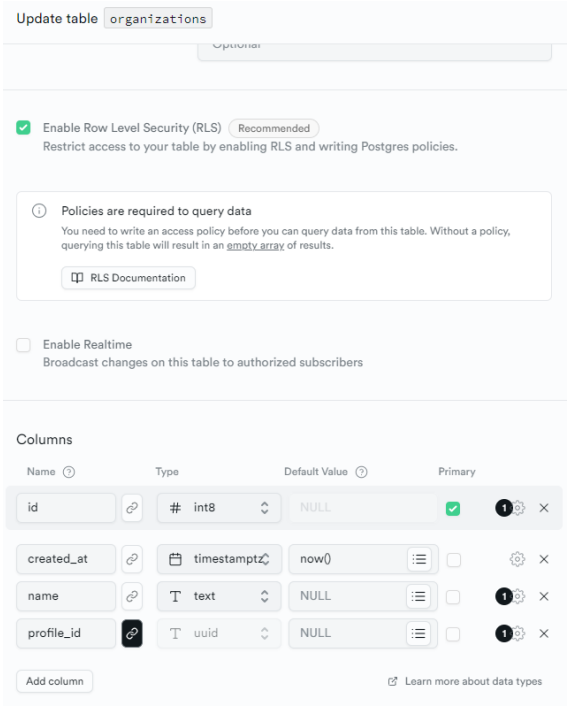

Figura 15: Taula de les organitzacions

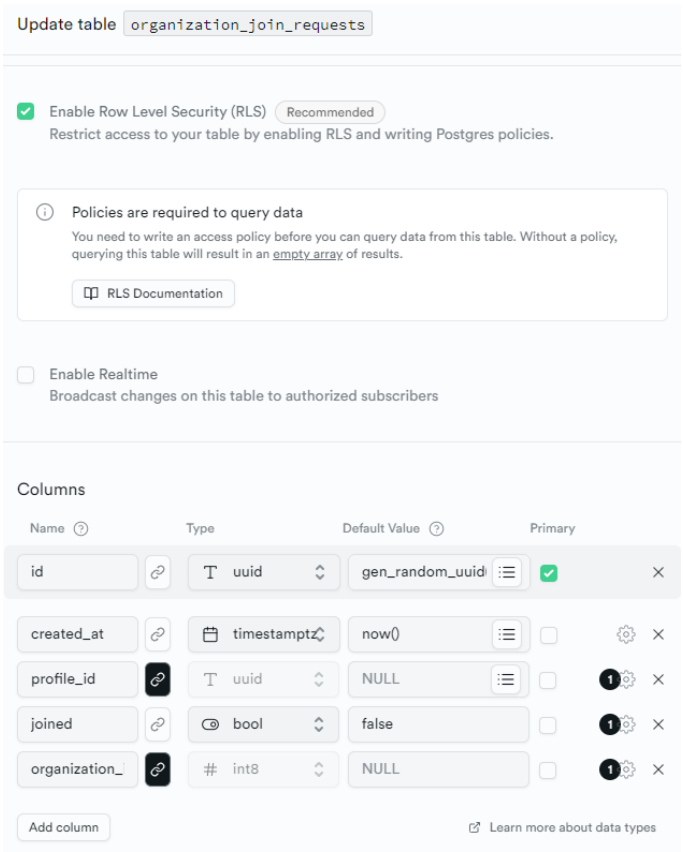

Figura 16: Taula validació de registres

4.4 Consideracions de seguretat durant el desenvolupament

Durant el desenvolupament d'aquest projecte, s'ha mantingut un compromís amb els principis de seguretat de la plataforma i s'han implementat mesures per a garantir la seguretat en diverses àrees clau. A continuació, s'expliquen els punts implementats en el desenvolupament:

4.4.1 Seguretat en el registre

Amb la finalitat de prevenir la suplantació d'identitat durant el procés de registre, s'ha implementat un pas intermedi entre la sol.licitud de registre i l'activació completa del compte.

En primer lloc, l'usuari completa el procés de registre. Una vegada completat, s'envia un correu electrònic de confirmació. Paral.lelament, en la base de dades s'ha creat una taula amb les sol.licituds de registre, i per defecte, els usuaris no estan validats. Quan l'usuari fa clic en l'enllaç del correu electrònic, el seu registre es valguda i se li permet accedir al sistema.

4.4.2 Classificació segons organitzacins

El segon punt es refereix a la gestió d'usuaris i rols. Inicialment, s'ha optat per tenir usuaris individuals amb l'opció de crear organitzacions. Una vegada que es crea una organització, només els usuaris amb rols d'administrador poden agregar nous membres. Perquè un usuari sigui part d'una organització, primer ha d'estar registrat. Després, un administrador li enviarà una sol.licitud i això generarà un correu de confirmació similar al cas del registre.

4.4.3 Permissos i privilegis

En l'apartat anterior es va esmentar el concepte de "administrador", que és un dels rols implementats en el sistema. L'administrador és l'usuari amb majors privilegis i té la capacitat de realitzar una àmplia gamma d'accions, que inclouen agregar usuaris a organitzacions, analitzar dades i canviar recomanacions, entre altres.

A continuació, es detallen els rols de "usuari" i "convidat", que actualment no es distingeixen entre si en termes de permisos.

Aquests permisos s'han implementat en conjunt amb el "PermissionChecker", el qual avalua els rols especificats en relació amb l'acció concreta que s'està sol.licitant. Si l'usuari té els rols requerits pel "PermissionChecker" per a aquesta acció en particular, se li permetrà realitzar-la. En cas contrari, no se li donarà accés. A continuació s'adjunta una imatge de l'esmentat.

Figura 17: Implementació de PermissionChecker

4.5 Desplegament en Vercel

Tot i que aquesta secció es troba al final, s'ha estat duent a terme durant tot el projecte, seguint la metodologia d'Integració i Desplegament Continu (CI/CD). El treball es troba en un repositori de GitHub i consta de dues branques: "main" i "develop". Com el seu nom indica, els canvis es realitzen sempre en la branca "develop", i una vegada que es té una versió estable, es fusiona amb la branca "main".

Tot això s'esmenta perquè Vercel realitza el desplegament basat en la branca "main". Per tant, cada vegada que es fusiona amb "main", simplement en iniciar sessió en la plataforma Vercel i fer clic en un botó, s'inicia automàticament el procés de desplegament.

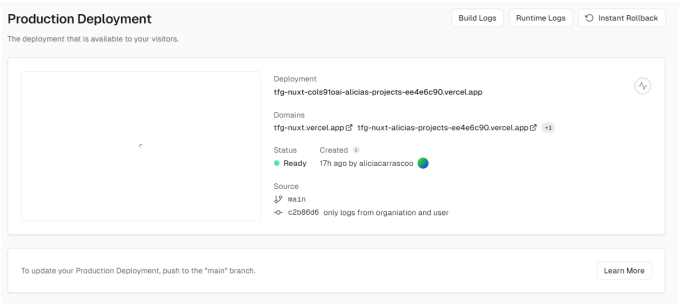

Figura 18: Deploy a Vercel

Podeu consultar la web: tfg-nuxt.vercel.app

5 Funcionalitats de seguretat clau

5.1 Selecció i extracció de les dades del JSON

La primera funcionalitat de l'àmbit de seguretat que trobem està situada en l'apartat de "Logs" anomenat "Scan a new log". Aquesta consisteix en l'extracció de característiques que s'han considerat més rellevants, partint dels logs proporcionats per l'eina Cortex XDR. Aquelles característiques seleccionades es consideren necessàries per a l'anàlisi i la gestió efectiva de les alertes de seguretat. A continuació, es llisten les característiques extretes.

- SHA (Secure Hash Algorithm)

El valor SHA representa una firma digital única per a cada arxiu i és bàsica per a la identificació precisa d'amenaces. Permet rastrejar i correlacionar arxius maliciosos i potencialment perillosos en diverses alertes i esdeveniments. Després de veure el SHA, se'ns mostra un botó que ens enllaça a VirusTotal, una eina que analitzarà aquest codi i ens mostrarà la reputació que té registrada per part de diferents venedors d'antivirus.

- Mitre Tactics i Techniques:

La matriu de tàctiques i tècniques mitre (*Adversarial Tactics, Techniques, and Common Knowledge*) proporciona una classificació estandarditzada de tàctiques i tècniques utilitzades per actors maliciosos. L'extracció d'aquesta informació permet una contextualització completa de les amenaces i ajuda als analistes a comprendre millor la naturalesa de les accions dels atacants. A més a més, s'inclou la funcionaliltat "Check Tactic" i "Check Technique", que ens enllaça a la pàgina oficial de MITTRE ATT&CK on està registrada la tàctica o tècnica concreta.

- Usuari

El nom d'usuari vinculat a una alerta és imprescindible per a l'atribució de responsabilitat i la identificació de possibles comptes o credencials compromeses. Saber el lloc de treball de l'usuari també facilita la resposta i el seguiment d'incidents, així com la presa de decisions de seguretat.

- Nom de l'equip

El nom del *host* afectat és essencial per a localitzar i saber el possible impacte, així com aïllar els sistemes compromesos. Permet una resposta més ràpida i eficaç, minimitzant l'impacte de l'amenaça en la resta de la xarxa.

- Nom de l'alerta

El nom de l'alerta proporciona una descripció concreta del tipus d'amenaça o activitat maliciosa detectada. Ajuda als analistes a prioritzar les alertes i a entendre ràpidament la naturalesa de l'incident. Aquesta característica serà bàsica per la implementació de les posteriors "recomanacions".

- Categoria de l'alerta

La categorització de l'alerta indica el tipus d'amenaça, com *malware, phishing* o filtració de dades. Facilita l'assignació de recursos i la implementació de mesures de seguretat adequades a realitzar.

- Descripció de l'alerta

La descripció d'aquesta proporciona informació contextual sobre l'amenaça concreta, les seves característiques específiques, així com possibles indicadors de compromís (IoC). De la mateixa forma que les anteriors, facilita la presa de decisions informades i la resposta ràpida i efectiva.

Totes aquestes dades tenen un paper principal en la identificació, avaluació i mitigació d'amenaces de seguretat. L'extracció d'aquestes característiques permet una comprensió més concreta dels incidents, la correlació de dades, la presa de decisions fonamentades i la resposta oportuna. A més, facilita la col.laboració entre diferents equips de seguretat en proporcionar informació clara, coherent i igual, fet que és essencial per a una resposta eficaç i una defensa proactiva contra les amenaces cibernètiques.

En la següent figura es mostra un exemple de l'extracció de dades d'una alerta.

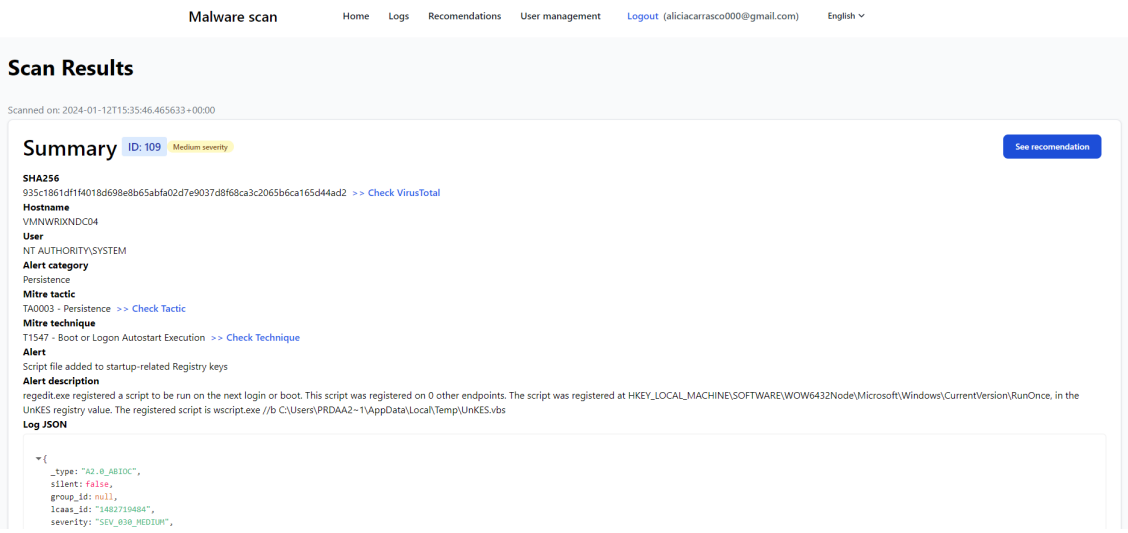

Figura 19: Exemple d'anàlisi de logs

5.2 Consulta d'informació en altres fonts

Un cop extretes les característiques clau dels logs de Cortex, l'aplicació mostra en la mateixa pantalla unes funcionalitats addicionals, les quals s'han mencionat anteriorment i afegeixen un valor significatiu a la gestió d'alertes de seguretat, ja que permeten accedir a informació addicional rellevant.

5.2.1 Enllaç a VirusTotal

L'aplicació ofereix una connexió directa a l'anàlisi de VirusTotal, la qual és l'eina d'anàlisi de firmes més utilitzada, donat que inclou la reputació registrada per múltiples venedors d'eines de detecció de *malware*. D'aquesta forma, es proporciona als analistes de seguretat informació addicional sobre l'arxiu, com la seva reputació, comportament i deteccions anteriors.

De la mateixa forma, agilitza la presa de decisions sobre la resposta a l'amenaça, incloent la quarantena o l'eliminació de l'arxiu concret.

La següent figura mostra un exemple d'una firma que ha donat un resultat no favorable:

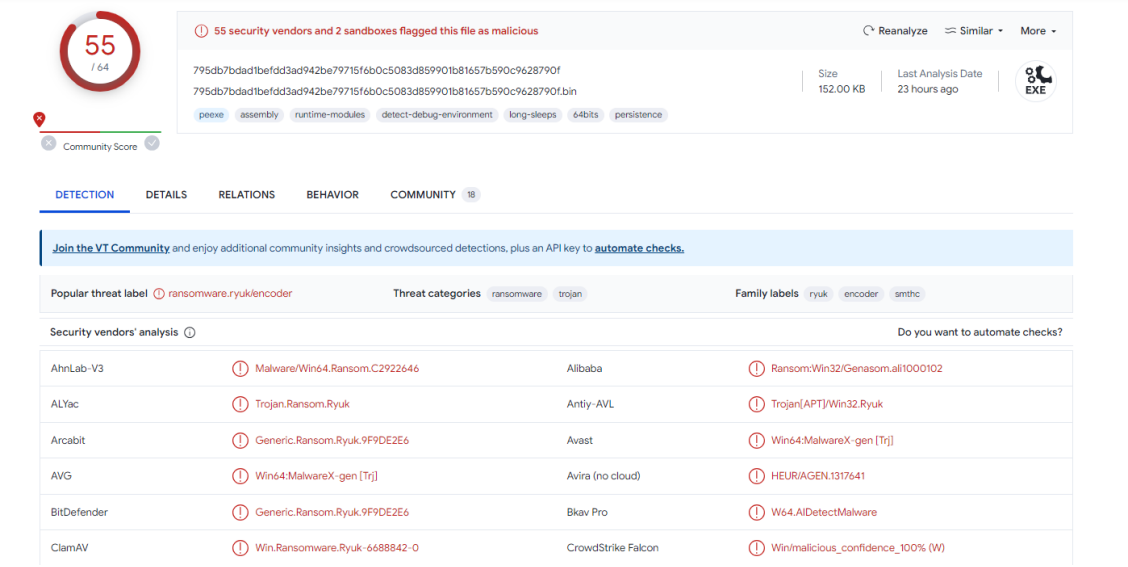

Figura 20: Exemple de VirusTotal

5.2.2 Enllaç a MITRE ATT&CK

Aquesta funcionalitat ofereix als usuaris l'oportunitat d'accedir a una explicació detallada de la tàctica o tècnica en la pàgina de MITRE ATT&CK. Tenir aquest informació addicional facilita la comprensió sobre com els actors maliciosos duen a terme les seves accions, la qual cosa és essencial per a un anàlisi més profund i detallat de l'amenaça, així com és de gran ajuda per dissenyar estratègies de defensa i contramesures per a mitigar l'amenaça específica de manera efectiva. De

la mateixa manera que anteriorment, es mostra un exemple de dues pantalles, de tàctiques i tècniques, respectivament, que podria mostrar-se com a resultat en un enllaç.

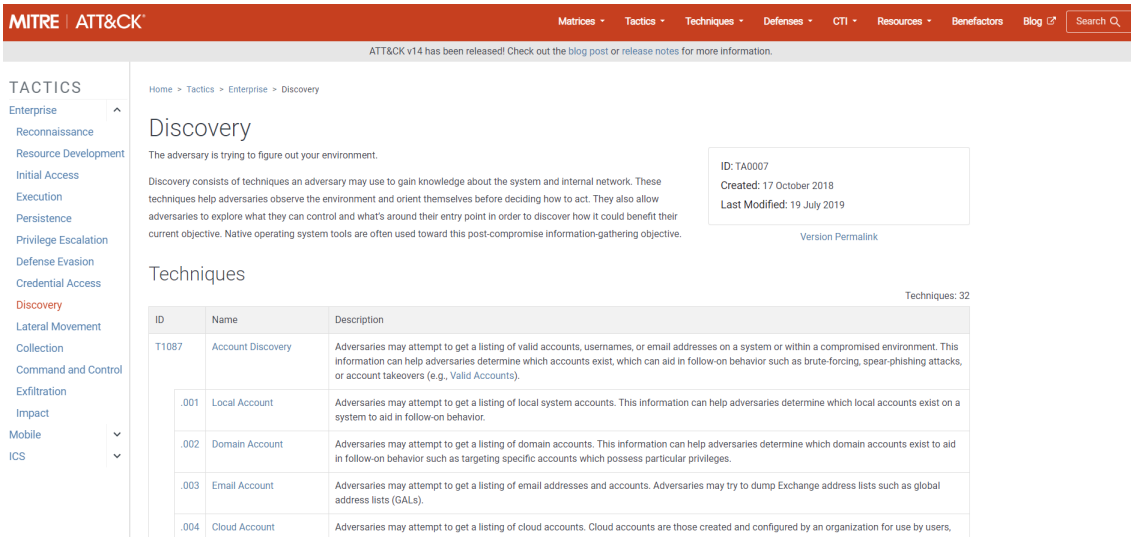

Figura 21: Exemple de Tàctica

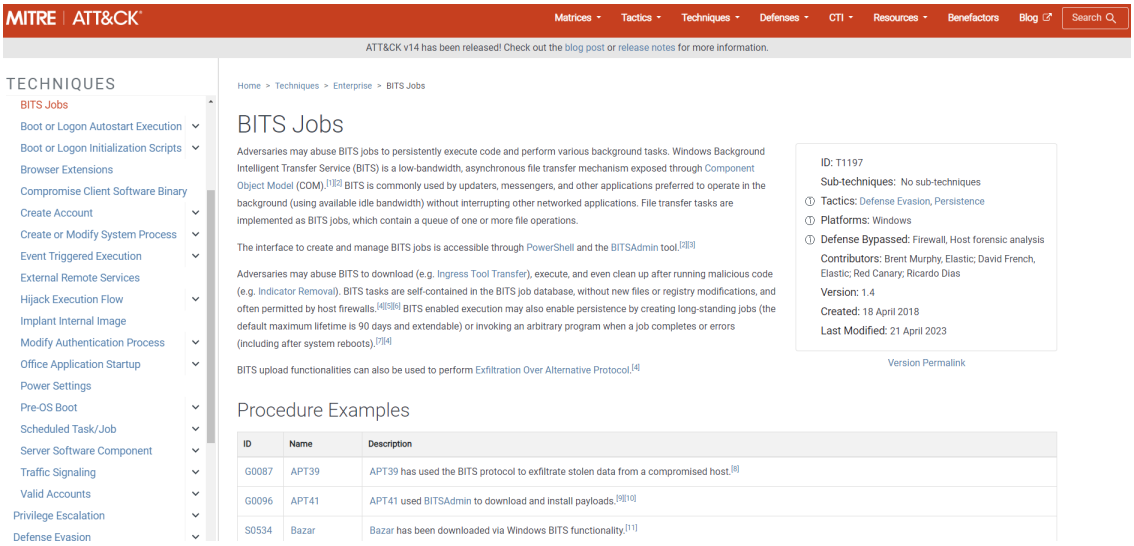

Figura 22: Exemple de Tècnica

Finalment, afegir que l'ús d'aquestes eines fomenta l'intercanvi d'informació col.laboratiu entre equips de seguretat, la qual cosa és necessària a l'entorn de ciberseguretat en constant evolució.

5.3 Apartat Recomanacions

L'apartat de recomanacions s'ha explicat anteriorment en termes de desenvolupament web. Pel que fa al propòsit com a tal, és essencial destacar que el que fa que la funcionalitat sigui especial és l'opció d'editar les recomanacions, la qual cosa la converteix en una eina col.laborativa entre organitzacions.

Per a emplenar la taula, s'han recopilat, analitzat i consolidat un total de 40 recomanacions procedents de diferents fonts i experiències pròpies. Aquestes recomanacions estan unificades i adaptades en el context de Cortex. Donat que la taula és molt extensa, s'adjunten a continuació dues recomanacions, la resta de la taula es troba a l'apartat annex.

Nom alerta	Anàlisi	Recomanació
A remote service with an uncommon name was created via RPC over SMB	L'alerta indica que s'ha creat un servei remot amb un nom poc comú a través d'RPC sobre SMB (Server Message Block). Aquest tipus d'activitat pot ser sospitosa i requerir una recerca més detallada per a determinar si hi ha alguna amenaça de seguretat.	1. Confirmar l'Autenticitat: Verifica amb l'administrador de l'equip si és una activitat legítima. Aquest podria s'un procés normal en la teva xarxa, però també podria ser indicatiu d'una activitat maliciosa. 2. Revisar els Registres d'Esdeveniments: Examina els registres d'esdeveniments del sistema i de seguretat en l'equip afectat per a obtenir més detalls sobre la creació del servei. Busca esdeveniments relacionats amb la creació de serveis i qualsevol altre esdeveniment sospitós o inusual. 3. Analitza l'Activitat de l'Usuari: Investiga l'activitat de l'usuari que va iniciar la creació del servei. Revisa els registres d'inici de sessió, les activitats de l'usuari i qualsevol altra informació rellevant per a determinar si l'acció va ser autoritzada i legítima. 4. Analitza el Servei Creat: Investiga el servei creat i determina el seu propòsit i funció. Si el servei té un nom inusual o desconegut, pots buscar informació sobre ell per a determinar si és legítim o si podria estar relacionat amb malware. 5. Analitza el Trànsit de Xarxa: Examina el trànsit de xarxa associat amb la creació del servei. Busca patrons de comunicació inusuals, connexions a adreces IP sospitoses o qualsevol altre comportament anòmal en el trànsit de xarxa. 6. Llança un Escàner: Assegura't que el sistema afectat tingui Cortex actualitzat i realitza un escaneig complet a la recerca de possibles amenaces relacionades. 7. Consulta la Base de dades d'Amenaces: Consulta bases de dades d'amenaces conegudes per a determinar si el servei creat està relacionat amb alguna amenaça coneguda. 8. Aïlla el Sistema Afectat: Si trobes evidència d'activitat maliciosa, considera aïllar el sistema afectat de la xarxa per a evitar que l'amenaça es propagui mentre investigues i abordes el problema.

Autorun.inf created in root C drive	L'alerta proporcionada indica que s'ha creat un arxiu Autorun.inf en l'arrel de la unitat C. La presència d'aquest arxiu podria ser un senyal d'activitat maliciosa, ja que els arxius Autorun.inf s'han utilitzat històricament per a executar automàticament programes en connectar unitats extraïbles a un sistema.	1. Revisa que no hi hagi connectades Unitats Extraïbles: Evita connectar qualsevol unitat extraïble (com a memòries USB) al sistema afectat fins que hagis investigat i abordat el problema i, en cas que hi hagi, desconnecta-les. Els arxius Autorun.inf solen estar associats amb l'execució automàtica de programes des de mitjans extraïbles. 2. Investiga el Contingut de Autorun.inf: Examina el contingut de l'arxiu Autorun.inf per a determinar quin programa o acció intenta executar. Pots obrir l'arxiu amb un editor de text per a revisar el seu contingut. Para esment als comandos i rutes especificades. 3. Analitza Registres d'Esdeveniments del Sistema: Revisa els registres d'esdeveniments del sistema per a obtenir més informació sobre la creació de l'arxiu Autorun.inf. Busca esdeveniments relacionats amb la creació d'arxius en la unitat C i qualsevol altre esdeveniment sospitós. 4. Llança un EscÃ¡neo: Assegura't que el sistema afectat tingui Cortex actualitzat i realitza un escaneig complet a la recerca de possibles amenaces relacionades. 5. Cerca Altres Indicadors de Compromís: Investiga si hi ha altres indicadors de compromís en el sistema. Busca arxius, processos o activitats inusuals. Els canvis no autoritzats en arxius del sistema o en la configuració poden ser senyals d'una intrusió. 6. Actualitza el Sistema: Assegura't que el sistema operatiu i totes les aplicacions estiguin actualitzades amb els últims pegats de seguretat. Les vulnerabilitats no posades pegats podrien ser explotades per malware. 7. Revisa la Política de Grups: Examina la configuració de la Política de Grups (Group Policy) per a assegurar-te que no hi hagi configuracions inusuals que permetin l'execució automàtica de programes des d'unitats extraïbles. 8. Elimina o Aïlla l'Arxiu Autorun.inf: Si es determina que l'arxiu Autorun.inf és maliciós, elimina-ho del sistema. Aïlla qualsevol sistema o dispositiu afectat per a evitar la propagació d'amenaces. 9. Analitza el Trànsit de Xarxa: Si és possible, analitza el trànsit de xarxa a la recerca de patrons inusuals o comunicacions amb adreces IP sospitoses.

6 Resultats i Comparacions

6.1 Resultats dels objectius

En aquesta secció, es presenten els resultats relacionats amb els objectius establerts a l'inici del treball de recerca:

- Contribuir en la Pràctica Professional:

L'aplicació demostra que pot ser útil en la pràctica professional, donat que proporciona un entorn col.laboratiu per a la gestió d'alertes de seguretat. Quants més usuaris la utilitzin, més registres d'esdeveniments es generaran, la qual cosa al seu torn augmentarà la quantitat d'alertes i, en conseqüència, de recomanacions, millorant així l'eficàcia d'aquesta eina.

- Comprendre el *MITRE ATT&CK*:

Comprendre el *MITRE ATT&CK*: S'ha aconseguit una aprofundir en la comprensió de *MITRE ATT&CK* en proporcionar enllaços directes a la pàgina oficial. Encara que no es contemplen accions directes sobre la matriu ATT&CK, s'estableixen les bases per a futures millores d'aquest recurs.

- Avaluar la Seguretat de l'Aplicació:

Malgrat la falta de coneixements previs, s'han implementat tècniques de seguretat en la web. Encara que no seria correcte afirmar que garanteix una seguretat absoluta, s'han aplicat mesures per a protegir alguns processos sensibles i dades, de la mateixa forma, les eines utilitzades s'han sel.leccionat tenint com a un dels principals requisit la seguretat de les dades.

- Desenvolupar Competències en el Desenvolupament Web:

L'objectiu referent al desenvolupament web considero que s'ha aconseguit. Encara que existeix un gran marge per a millorar i agregar noves funcionalitats, s'ha creat una aplicació web funcional.

- Millorar la presa de decisions de Seguretat:

L'aplicació centralitza gran quantitat d'informació rellevant per a la tria de decisions. L'efectivitat de les recomanacions depèn en gran mesura dels usuaris que la utilitzin, fet que augmenta el seu valor amb el temps.

- Fomentar la col.laboració interorganitzacional:

S'han afegit diverses funcionalitats col.laboratives en la funció de recomanacions per a promoure la col.laboració entre organitzacions mentre es protegeixen les dades sensibles. Aquesta característica recolça la capacitat dels equips de seguretat per a treballar junts en la resposta d'amenaces.

6.2 Comparativa amb solucions existents

A continuació, es presenta una comparació entre l'aplicació "Malware Scan" i dues solucions, "*TheHive Project*" i "*Splunk*", ambdues àmpliament conegudes.

- Enfoc Principal:

"Malware Scan" es centra en la gestió d'alertes de seguretat i l'enriquiment de dades a partir de llocs externs, així com dels propis usuaris.

TheHive Project s'especialitza en la gestió d'incidents de seguretat i la col.laboració entre equips de seguretat.

Splunk és una plataforma d'anàlisi de dades versàtil que s'utilitza per a una varietat d'àmbits, inclosa la seguretat.

- Col.laboració i Comunicació:

"Malware Scan" facilita la col.laboració tant dins d'una mateixa organització, així com entre vàries, a través de comentaris i recomanacions.

TheHive Project es centra en la col.laboració en la gestió d'incidents i la comunicació en temps real.

Splunk ofereix capacitat de col.laboració entre usuaris, tot i que no està específicament desenvolupat per a la gestió d'incidents.

- Usabilitat i Experiència d'Usuari:

"Malware Scan" tracta de proporcionar una experiència d'usuari minimalista, intuïtiva i enfocada en l'aprenentatge i la gestió d'alertes.

TheHive Project ofereix una interfície específicament dissenyada per a la gestió d'incidents i la col.laboració d'equips.

Splunk pot requerir una corba d'aprenentatge, ja que la plataforma a la seva versatilitat i ampli abast.

- Enriquiment d'alertes:

"Malware Scan" enriqueix les alertes amb context addicional i redirigeix a la pàgina oficial de *MITRE ATT&CK* per a obtenir informació detallada.

TheHive Project s'enfoca en la gestió d'incidents, amb menys èmfasi en l'enriquiment d'alertes específiques.

Splunk proporciona capacitats de cerca i anàlisi de dades, però requereix una configuració extra per a enriquir alertes específiques.

- Costos i Complexitat:

"Malware Scan" pot tenir costos variables segons la implementació i la grandària de l'organització.

TheHive Project és de codi obert i, en general, més assequible, en termes de costos.

Splunk pot ser molt costós i complex, depenent de la quantitat de dades i la personalització que es requereixi.

- Aplicabilitat Específica:

"Malware Scan" està dissenyat per a la gestió d'alertes de seguretat i l'enriquiment de les dades dels registres de Cortex XDR.

TheHive Project està específicament orientat a la gestió d'incidents i la resposta a amenaces.

Splunk és versàtil i s'utilitza en una varietat d'aplicacions, inclosa la ciberseguretat, però requereix configuració addicional per a casos específics.

Podriem concloure, aleshores, que "Malware Scan" destaca més pel seu enfocament específic en la gestió d'alertes de seguretat i la col.laboració, mentre que *Splunk* és versàtil però requereix configuració addicional, i , finalment, *TheHive Project* s'especialitza en la gestió d'incidents.

7 Conclusions

El desenvolupament de l'aplicació "Malware Scan" ha donat com a resultat una sèrie de conclusions i assoliments en diverses àrees:

- Gestió d'Usuaris:

La utilització de rols i la pertinença a organitzacions ha permès una gestió d'usuaris eficaç i escalable. Fet que assegura que els equips de seguretat puguin col.laborar de manera eficient, accedint només a la informació rellevant per a les seves responsabilitats, la qual cosa millora la seguretat i l'organització de les dades.

- Comentaris i Col.laboració:

La implementació de comentaris en l'aplicació ha fomentat la col.laboració entre usuaris i equips de seguretat. Això ha contribuït a la creació d'un ambient de treball col.laboratiu, tant dintre de la organització, podent comentar els logs interns, com entre organitzacions, referent a les recomanacions, fet que impulsa el seguiment d'amenaces de manera més efectiva.

- Assoliment d'Objectius:

Els objectius establerts a al principi del projecte s'han complert en la seva majoria. L'aplicació mostra una utilitat en la pràctica professional, ha millorat la comprensió de *MITRE ATT&CK* i ha aprofundit en l'àmbit de la seguretat.

- Seguretat de l'aplicació:

Malgrat no poder garantir una seguretat absoluta, s'han implementat varies tècniques per a protegir determinats processos i dades sensibles. Aquesta característica contribueix a la confiabilitat de l'aplicació i a la protecció de la informació.

- Comoditat de l'Usuari:

Durant el desenvolupament de la part visual, s'ha donat importància a l'experiència de l'usuari en proporcionar una interfície intuïtiva i centrada en la gestió d'alertes. A més, l'estat de càrrega de dades s'informa mitjançant un component, i la navegació simplificada ajuda a tenir una experiència d'usuari més agradable i eficient.

8 Millores futures

Com s'ha esmentat en anteriors apartats, aquest treball ofereix nombrosos àmbits que poden ser objecte d'un major desenvolupament i millora. D'una banda, la secció de recomanacions podria ser significativament millorada, permetent la possibilitat de generar múltiples recomanacions per a una mateixa alerta o implementant un sistema de gestió més sofisticat.

Pel que fa als rols d'usuaris, si bé s'han implementat els rols bàsics, existeix marge per a una gestió més refinada i segmentada que podria millorar la seguretat.

En relació al desenvolupament web, tant en el frontend com en el backend, existeixen àrees que poden ser optimitzades. Això inclou l'adaptació de l'aplicació per a dispositius mòbils, una estilització més personalitzada i una millora en la traducció, entre altres aspectes.

A més d'aquestes millores esmentades, l'aplicació presenta un potencial considerable per a la incorporació d'una àmplia gamma de funcionalitats addicionals. Per exemple, podria automatitzar-se l'entrada de dades des de Cortex, la qual cosa ampliaria encara més la seva utilitat i versatilitat.

9 Contribucions

En primer lloc, vull expressar el meu sincer agraïment al meu tutor, Raül Roca, per la seva tutela durant el desenvolupament d'aquest treball. En les nostres reunions, va demostrar una gran disposició per a escoltar les meves explicacions i proporcionar consells que no sols van beneficiar aquest projecte, sinó que també van resultar útils en algunes tasques de la meva feina.

En segon lloc, desitjo mostrar el meu profund agraïment a Alex Dickson pels seus valuosos consells i suport continu durant el desenvolupament d'aquest projecte. La seva experiència en la resolució d'errors, tant en el frontend com en el backend, va resultar fonamental. A més, em va brindar valuosos consells sobre les millors pràctiques en el desenvolupament.

En tercer lloc, vull expressar la meva gratitud cap als meus companys de treball. A Eric, agrair tots els coneixements que m'ha ensenyat, va ser el meu primer company de treball. A Oscar, el meu segon company de feina, li agraeixo la seva paciència durant els processos de d'aprenentatge. A més, vull estendre el meu agraïment a tots els meus companys actuals, els qui continuen ensenyant-me i col.laborant amb mi dia a dia en el nostre treball conjunt. El seu suport ha estat fonamental en el meu creixement professional.

10 Referències bibliogràfiques

Referències

[1] Documentació oficial de Vercel, *Vercel Documentation*, `https://vercel.com/docs`, 2023.

[2] Documentació oficial de Supabase, *Supabase Documentation*, `https://supabase.com/docs`, 2023.

[3] Supabase Beta December 2023, *Supabase Documentation*, `https://supabase.com/docs`, December 2023.

[4] Supabase Beta September 2023, *Supabase Documentation*, `https://supabase.com/docs`, September 2023.

[5] New Supabase Docs, built with Next.js, *Supabase Documentation*, `https://supabase.com/docs`, December 2022.

[6] "From EDR to XDR and Beyond: The Evolution of Endpoint Security," *Cisco Newsroom*, `https://newsroom.cisco.com`, 2022. *[Cisco Newsroom - EDR to XDR]*8203;“ãoaicite:1ã“8203;.

[7] "The Journey to Extended Detection and Response - XDR," *Palo Alto Networks*, `https://www.paloaltonetworks.com`, 2022. *[Palo Alto Networks - XDR Journey]*8203;“ãoaicite:0ã“8203;.

[8] Documentació oficial de Tailwind CSS, *Tailwind CSS Documentation*, `https://tailwindcss.com/docs`, 2023.

[9] Documentació oficial de Nuxt.js, *Nuxt.js Documentation*, `https://nuxtjs.org/docs`, 2023.

[10] Documentació oficial de Vue.js, *Vue.js Documentation*, `https://vuejs.org/v2/guide/`, 2023.

[11] Documentació oficial de Cortex XDR, *Cortex XDR Documentation*, `https://www.paloaltonetworks.com/cortex/cortex-xdr`, 2023.

[12] Evolució d'Antivirus a XDR, *From Antivirus to XDR: The Evolution of Cybersecurity*, 2022.

[13] Triangle CIA en Ciberseguretat, *The CIA Triangle in Cybersecurity*, 2022.

[14] Documentació de Flowbite, *Flowbite Documentation*, `https://flowbite.com/docs/`, 2023.

[15] AnÃ lisi d'amenaces amb Cortex, *Threat Analysis with Cortex*, 2022.

[16] Matriu MITRE ATTCK, *MITRE ATTCK*, `https://attack.mitre.org/`, 2023.

11 Annex

Behavioral Threat	L'alerta indica una amenaça comportamental relacionada amb la recopilació de credencials. Aquest tipus d'activitat és preocupant, ja que podria indicar intents de comprometre la seguretat del sistema mitjançant l'obtenció no autoritzada de credencials.	1. Analitzar el Comportament de l'Usuari: Investigar el comportament de l'usuari associat amb l'alerta. Revisar els registres d'inici de sessió, activitats de l'usuari i qualsevol altra informació rellevant per a determinar si es tracta d'una activitat legítima o maliciosa. 2. Revisar Registres d'Esdeveniments: Examinar els registres d'esdeveniments del sistema i de seguretat per a obtenir més detalls sobre l'amenaça. Buscar esdeveniments relacionats amb la recopilació de credencials i qualsevol altre esdeveniment sospitós. 3. Analitzar Trànsit de Xarxa: Examinar el trànsit de xarxa a la recerca de patrons inusuals o comunicacions amb adreces IP sospitoses. La recopilació de credencials sovint implica la comunicació amb servidors maliciosos. 4. Llançar un Escàner: Assegurar-se que el sistema tingui un sistema de protecció actualitzat i realitzar un escaneig complet per a buscar possibles amenaces. 5. Canviar Credencials Compromeses: Si es confirma l'amenaça, canviar les credencials associades amb els comptes compromesos per a evitar l'accés no autoritzat. 6. Aplicar Polítiques de Contrasenyes Fortes: Reforçar les polítiques de contrasenyes per a garantir que els usuaris utilitzin contrasenyes fortes i complexes. 7. Monitorejar Activitats Sospitoses: Implementar un monitoratge continu per a detectar qualsevol activitat sospitosa en el sistema.

Credential Gathering Protection - 769377214	L'alerta indica una amenaça comportamental relacionada amb la protecció contra cryptominers. Els cryptominers són programes maliciosos que utilitzen els recursos del sistema per a minar criptomonedes sense el coneixement de l'usuari.	1. Analitzar Processos en Execució: Investigar els processos en execució per a identificar qualsevol aplicació maliciosa que pugui estar utilitzant recursos per a la mineria de criptomonedes. 2. Revisar l'ús de Recursos: Monitorar l'ús de recursos del sistema, com l'ús de la CPU i la memòria, per a identificar patrons inusuals que puguin indicar activitat de cryptominería. 3. Llançar un Escàner: Assegurar-se que el sistema tingui un sistema de protecció actualitzat i realitzar un escaneig complet per a buscar i eliminar possibles cryptomineros. 4. Actualitzar i Posar pegats: Assegurar-se que el sistema operatiu i totes les aplicacions estiguin actualitzades amb els últims pegats de seguretat per a prevenir vulnerabilitats explotades per malware. 5. Monitorejar Trànsit de Xarxa: Analitzar el trànsit de xarxa per a identificar comunicacions amb servidors de mineria de criptomonedes o patrons inusuals associats amb cryptomineros. 6. Configurar Firewall: Configurar el firewall per a bloquejar el trànsit cap a i des d'adreces IP conegudes de servidors de mineria de criptomonedes.

Cryptominers Protection - 2736470759	L'alerta indica una amenaça comportamental relacionada amb la recopilació de credencials. Aquest tipus d'activitat és preocupant, ja que podria indicar intents de comprometre la seguretat del sistema mitjançant l'obtenció no autoritzada de credencials.	1. Analitzar el comportament de l'usuari Investigar el comportament de l'usuari associat amb l'alerta. Revisar els registres d'inici de sessió, activitats de l'usuari i qualsevol altra informació rellevant per a determinar si es tracta d'una activitat legítima o maliciosa. 2. Revisar Registres d'Esdeveniments: Examinar els registres d'esdeveniments del sistema i de seguretat per a obtenir més detalls sobre l'amenaça. Buscar esdeveniments relacionats amb la recopilació de credencials i qualsevol altre esdeveniment sospitós. 3. Analitzar Trànsit de Xarxa: Examinar el trànsit de xarxa a la recerca de patrons inusuals o comunicacions amb adreces IP sospitoses. La recopilació de credencials sovint implica la comunicació amb servidors maliciosos. 4. Llançar un Escàner: Assegurar-se que el sistema tingui un sistema de protecció actualitzat i realitzar un escaneig complet per a buscar possibles amenaces. 5. Canviar Credencials Compromeses: Si es confirma l'amenaça, canviar les credencials associades amb els comptes compromesos per a evitar l'accés no autoritzat. 6. Aplicar Polítiques de Contrasenyes Fortes: Reforçar les polítiques de contrasenyes per a garantir que els usuaris utilitzin contrasenyes fortes i complexes. 7. Monitorar Activitats Sospitoses: Implementar un monitoratge continu per a detectar qualsevol activitat sospitosa en el sistema.

Encoded information using Windows certificate management tool	L'alerta indica que s'ha codificat informació utilitzant l'eina de gestió de certificats de Windows. Aquest comportament pot ser una tècnica utilitzada per a ocultar informació sensible.	1. Descodificar la Informació: Analitzar i descodificar la informació codificada per a entendre el seu contingut. Pot ser necessari utilitzar eines especialitzades o consultar amb experts en seguretat. 2. Revisar Certificats: Revisar els certificats instal.lats en el sistema per a identificar qualsevol certificat sospitós o no autoritzat. 3. Monitorar Activitats de Certificats: Establir un monitoratge continu d'activitats relacionades amb certificats per a detectar comportaments anòmals. 4. Revisar Polítiques de Certificats: Verificar i reforçar les polítiques de gestió de certificats per a evitar l'ús indegut. 5. Actualitzar Sistemes: Assegurar-se que el sistema operatiu i les aplicacions estiguin actualitzats per a mitigar vulnerabilitats conegudes.
Excessive account lockouts on suspicious users	L'alerta indica un nombre excessiu de bloquejos de compte en usuaris sospitosos. Això podria indicar intents d'accés no autoritzat.	1. Analitzar Comptes Bloquejats: Investigar els comptes bloquejats per a identificar el motiu darrere dels intents fallits d'accés. 2. Revisar Registres de Seguretat: Examinar els registres d'esdeveniments de seguretat per a obtenir més detalls sobre els intents d'accés no autoritzat i qualsevol altre esdeveniment sospitós. 3. Canviar Credencials: En cas de confirmar activitat maliciosa, canviar les credencials dels comptes bloquejats per a prevenir l'accés no autoritzat. 4. Aplicar Polítiques de Bloqueig de Comptes: Reforçar les polítiques de bloqueig de comptes per a prevenir intents repetits d'accés no autoritzat. 5. Implementar Autenticació de Dos Factors (2FA): Considerar la implementació d'autenticació de dos factors per a agregar una capa addicional de seguretat. 6. Monitorar Activitats d'Usuari: Establir un monitoratge continu de les activitats d'usuari per a detectar comportaments sospitosos. 7. Actualitzar Sistemes: Assegurar-se que el sistema operatiu i les aplicacions estiguin actualitzats per a mitigar vulnerabilitats conegudes. Aquestes recomanacions estan dissenyades per a abordar cada alerta específica i ajudar a mitigar possibles riscos per a la seguretat del sistema.

Executable moved to Windows system folder	L'alerta indica que s'ha detectat l'acció de moure un executable a la carpeta del sistema de Windows. Aquest comportament és potencialment perillós, ja que uns certs tipus de malware intenten ocultar-se en ubicacions crítiques del sistema per a evadir detecció.	1. Verificar Autenticitat: Confirmar l'autenticitat de l'acció amb l'administrador del sistema. Determinar si l'acció és legítima o potencialment maliciosa. 2. Revisar Registres d'Esdeveniments: Analitzar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'acció de moure l'executable. Buscar esdeveniments relacionats que puguin proporcionar més context. 3. Anàlisi de l'Executable: Realitzar una anàlisi detallada de l'executable mogut per a determinar la seva legitimitat i funció. Utilitzar eines de seguretat per a escanejar l'arxiu a la recerca de possibles amenaces. 4. Escaneig Complet del Sistema: Executar un escaneig complet del sistema amb eines de seguretat actualitzades per a identificar possibles amenaces addicionals. 5. Consulta Bases de dades d'Amenaces: Consultar bases de dades d'amenaces conegudes per a identificar possibles connexions malicioses o patrons associats amb l'executable. 6. Aïllament del Sistema: En cas de confirmar-se activitat maliciosa, considerar aïllar el sistema afectat per a prevenir la propagació de l'amenaça. 7. Monitoratge del Trànsit de Xarxa: Establir un monitoratge continu del trànsit de xarxa per a identificar patrons inusuals o comunicacions amb adreces IP sospitoses.

Kerberos Traffic from Non-Standard Process	L'alerta assenyala la detecció de trànsit Kerberos provinent d'un procés no estàndard. Aquesta activitat és sospitosa, ja que els atacants sovint utilitzen tècniques Kerberos per a comprometre l'autenticació en un sistema.	1. Investigar el Procés no Estàndard: Investigar el procés no estàndard que està generant trànsit Kerberos. Determinar la seva legitimitat i funció en el sistema. 2. Revisar Registres d'Esdeveniments: Revisar els registres d'esdeveniments per a obtenir informació detallada sobre l'activitat de trànsit Kerberos. Buscar esdeveniments relacionats que puguin llançar llum sobre la situació. 3. Anàlisi del Trànsit de Xarxa: Analitzar el trànsit de xarxa a la recerca de patrons inusuals o connexions sospitoses associades amb el trànsit Kerberos no estàndard. 4. Escaneig de Seguretat: Realitzar un escaneig de seguretat complet del sistema per a identificar possibles amenaces i vulnerabilitats. 5. Canvi de Credencials: Canviar les credencials si es confirma activitat maliciosa per a prevenir accessos no autoritzats. 6. Reforçar Polítiques de Seguretat Kerberos: Reforçar les polítiques de seguretat relacionades amb l'autenticació Kerberos per a prevenir futurs incidents.

LNK file creation in startup folder	L'alerta indica la creació d'un arxiu LNK (accés directe) en la carpeta d'inici del sistema. Aquest comportament suggereix intents d'executar automàticament programes maliciosos en iniciar el sistema.	1. Evitar Execució de Programes Desconeguts: Evitar l'execució de programes desconeguts i revisar la carpeta d'inici per a identificar l'arxiu LNK. 2. Anàlisi de l'Arxiu LNK: Realitzar una anàlisi detallada del contingut de l'arxiu LNK per a entendre el seu propòsit i les accions que intenta realitzar. 3. Revisar Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la creació de l'arxiu LNK. Buscar esdeveniments sospitosos. 4. Escaneig Complet a la recerca d'Amenaces: Executar un escaneig complet del sistema a la recerca de possibles amenaces utilitzant eines de seguretat actualitzades. 5. Anàlisi d'Activitats del Sistema: Analitzar altres activitats del sistema a la recerca d'indicadors de compromís o canvis no autoritzats. 6. Eliminació o Aïllament de l'Arxiu LNK: Eliminar o aïllar l'arxiu LNK si es confirma activitat maliciosa per a prevenir execucions automàtiques no autoritzades. 7. Monitoratge Continu: Establir un monitoratge continu de l'activitat del sistema per a detectar possibles amenaces addicionals.
Local Analysis Malware	L'alerta indica la detecció de malware mitjançant anàlisi local. Això podria ser el resultat d'un escaneig de seguretat que va identificar un arxiu o activitat sospitosa en el sistema.	1. Investigar l'Arxiu o Activitat Maliciosa: Realitzar una recerca detallada de l'arxiu o activitat identificada com malware. 2. Escaneig Complet del Sistema: Executar un escaneig complet del sistema amb eines de seguretat actualitzades per a identificar i eliminar possibles amenaces. 3. Actualització de Definicions de Malware: Assegurar-se que les definicions de malware estiguin actualitzades per a detectar noves variants d'amenaces. 4. Aïllament del Sistema: Aïllar el sistema afectat per a prevenir la propagació del malware a altres sistemes de la xarxa. 5. Consulta amb l'Equip de Seguretat: Consultar amb l'administrador de seguretat o l'equip de resposta a incidents per a obtenir orientació addicional. 6. Monitoratge Continu: Establir un monitoratge continu de l'activitat del sistema per a identificar possibles amenaces addicionals.

Login Password Spray on a sensitive server	L'alerta indica un intent d'atac conegut com L-Login Password Esprai"en un servidor sensible. Aquest tipus d'atac implica provar un conjunt limitat de contrasenyes contra múltiples comptes d'usuari per a evitar la detecció automàtica.	1. Monitoratge de Comptes: Monitorar els comptes d'usuari per a detectar qualsevol activitat inusual, bloqueig de comptes o intents repetits d'inici de sessió. 2. Enfortir Polítiques de Contrasenyes: Reforçar les polítiques de contrasenyes i educar als usuaris sobre la importància d'utilitzar contrasenyes fortes. 3. Bloqueig de IPs: Bloquejar les adreces IP d'origen associades amb els intents de "L-Login Password Esprai"". 4. Anàlisi de Registres: Analitzar els registres d'esdeveniments per a obtenir detalls sobre els intents d'inici de sessió. Buscar patrons i correlacions. 5. Notificació d'Incidents: Notificar a l'equip de seguretat sobre l'incident perquè pugui prendre mesures addicionals, com canviar contrasenyes o revisar configuracions de seguretat.
Lolbin CERTUTIL suspicious executions	L'alerta indica execucions sospitoses de CERTUTIL, que és una utilitat de línia de comandos de Windows per a treballar amb certificats. Els atacants sovint abusen d'utilitats legítimes com Lolbins per a executar codi maliciós.	1. Anàlisi de l'ús de CERTUTIL: Investigar l'ús legítim de CERTUTIL en el sistema i comparar-lo amb l'execució sospitosa identificada. 2. Revisar Registres d'Esdeveniments: Revisar els registres d'esdeveniments per a obtenir detalls addicionals sobre les execucions de CERTUTIL. Buscar esdeveniments sospitosos. 3. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats anòmales que involucrin utilitats del sistema. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles malware associats amb execucions de CERTUTIL. 5. Restringir Execució de Lolbins: Implementar restriccions en l'execució de Lolbins com CERTUTIL per a prevenir abusos.

Lolbin SCHTASKS suspicious executions	L'alerta indica execucions sospitoses de SCHTASKS, que és una eina de línia de comandos de Windows utilitzada per a programar tasques. Els atacants poden abusar de Lolbins com SCHTASKS per a executar comandos maliciosos de manera encoberta.	1. Anàlisi de l'ús de SCHTASKS: Investigar l'ús legítim de SCHTASKS en el sistema i comparar-lo amb l'execució sospitosa identificada. 2. Revisar Registres d'Esdeveniments: Revisar els registres d'esdeveniments per a obtenir detalls addicionals sobre les execucions de SCHTASKS. Buscar esdeveniments sospitosos. 3. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats anòmales que involucrin utilitats del sistema. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles malware associats amb execucions de SCHTASKS. 5. Restringir Execució de Lolbins: Implementar restriccions en l'execució de Lolbins com SCHTASKS per a prevenir abusos.
LSASS memory dump file created	L'alerta indica la creació d'un arxiu de bolcat de memòria (memory dump) de LSASS (Local Security Authority Subsystem Service). Aquest comportament pot ser indicatiu d'intents de robatori de credencials i activitats malicioses.	1. Anàlisi del Bolcat de Memòria: Analitzar el contingut de l'arxiu de bolcat de memòria per a identificar possibles dades sensibles i determinar si es tracta d'un esdeveniment maliciós. 2. Revisar Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir informació sobre la creació de l'arxiu de bolcat de memòria. Buscar esdeveniments relacionats. 3. Monitoratge de Credencials: Monitorar les credencials i comptes d'usuari per a detectar possibles compromisos. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles malware que puguin haver causat la creació de l'arxiu de bolcat de memòria. 5. Actualitzacions de Seguretat: Assegurar-se que el sistema i les aplicacions estiguin actualitzades amb els últims pegats de seguretat. 6. Implementar Proteccions Addicionals: Implementar proteccions addicionals, com a solucions de detecció d'amenaces avançades, per a prevenir i detectar activitats malicioses. 7. Revisió de Polítiques de Seguretat: Revisar i enfortir les polítiques de seguretat per a mitigar riscos associats amb atacs a LSASS i robatori de credencials.

New Administrative Behavior	L'alerta indica la detecció d'un nou comportament administratiu en el sistema. Aquest tipus d'alerta sol generar-se quan un usuari o procés realitza accions que són inusuals o no coincideixen amb el comportament típic en la xarxa.	1. Recerca del Comportament: Investigar el nou comportament administratiu per a determinar la seva legitimitat i autorització. 2. Revisió d'Accessos: Revisar els registres d'accés i esdeveniments del sistema per a obtenir més detalls sobre les accions realitzades. 3. Validació amb Administradors: Validar l'activitat amb els administradors autoritzats per a assegurar que l'acció sigui legítima. 4. Monitoratge Continu: Establir un monitoratge continu per a detectar qualsevol activitat administrativa inusual en el futur. 5. Notificació a Equips de Seguretat: Notificar als equips de seguretat sobre l'activitat per a la seva anàlisi i seguiment.

Office process creates a scheduled task via file access	L'alerta indica que un procés d'Office ha creat una tasca programada mitjançant accés a arxius. Aquest comportament podria ser utilitzat de manera maliciosa per a executar tasques automatitzades no autoritzades.	1. Anàlisi del Procés d'Office: Analitzar el procés d'Office que ha creat la tasca programada per a determinar la seva legitimitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la creació de la tasca programada. 3. Validació amb Usuaris: Validar amb els usuaris afectats per a confirmar si l'acció va ser intencional i autoritzada. 4. Monitoratge Continu: Establir un monitoratge continu per a detectar accions similars en el futur. 5. Restriccions de Tasques Programades: Considerar restringir la capacitat de processos d'Office per a crear tasques programades, especialment si no és una funció necessària per a les operacions normals.

Possible DLL Side Loading by a Known Actor in the Organization	L'alerta suggereix la possibilitat de "DLL Side Loading"per part d'un actor conegut en l'organització. Aquest terme es refereix a la càrrega lateral d'una biblioteca dinàmica (DLL) maliciosa per un procés legítim.	1. Anàlisi de l'Actor Conegut: Investigar l'actor conegut en l'organització per a entendre les seves intencions i motivacions. 2. Anàlisi de DLL Side Loading: Realitzar una anàlisi detallada de la possible DLL Side Loading per a determinar la legitimitat i riscos associats. 3. Revisió d'Activitats de l'Actor: Revisar les activitats recents de l'actor conegut per a identificar patrons o comportaments sospitosos. 4. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb la DLL Side Loading. 5. Enfortiment de Seguretat: Enfortir les mesures de seguretat per a prevenir futurs incidents de DLL Side Loading. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats sospitoses relacionades amb l'actor conegut.
Possible LDAP enumeration by unsigned process	L'alerta indica la possibilitat d'enumeració LDAP (Lightweight Directory Access Protocol) per part d'un procés no signat digitalment. L'enumeració LDAP podria ser utilitzada per a recopilar informació sobre usuaris i recursos en el directori actiu.	1. Anàlisi del Procés No Signat: Investigar el procés no signat per a determinar el seu origen i legitimitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls sobre l'activitat d'enumeració LDAP. 3. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb el procés no signat. 4. Restricció d'Execució: Considerar la implementació de polítiques que restringeixin l'execució de processos no signats digitalment. 5. Actualització de Signatures de Seguretat: Assegurar-se que les signatures de seguretat estiguin actualitzades per a detectar noves amenaces relacionades amb l'enumeració LDAP. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars en el futur.

ProcDump usage detection	L'alerta indica la detecció de l'ús de ProcDump, una eina de línia de comandos utilitzada per a generar bolcats de memòria de processos en sistemes Windows. La utilització d'eines de bolcat de memòria pot ser indicativa d'intents d'anàlisis forense o compromís del sistema.	1. Anàlisi de l'ús de ProcDump: Investigar el motiu de l'ús de ProcDump per a determinar si és una activitat legítima o potencialment maliciosa. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'ús de ProcDump. Buscar esdeveniments relacionats i patrons sospitosos. 3. Anàlisi de Memòria Dump: Analitzar el contingut dels bolcats de memòria generats per ProcDump per a identificar possibles amenaces o activitats malicioses. 4. Monitoratge Continu: Establir un monitoratge continu per a detectar futurs usos d'eines de bolcat de memòria i activitats similars. 5. Implementar Restriccions: Considerar la implementació de polítiques que restringeixin l'ús d'eines de bolcat de memòria en entorns no autoritzats."
Recurring rare domain access from an unsigned process	L'alerta assenyala l'accés recurrent a un domini rar des d'un procés no signat digitalment. Accessos inusuals a dominis, especialment des de processos no de confiança, poden ser indicatius d'activitats malicioses.	1. Anàlisi del Domini i Procés: Investigar el domini rar i el procés no signat per a determinar la legitimitat de l'activitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'accés al domini i l'execució del procés no signat. 3. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb l'accés al domini i el procés no signat. 4. Restricció d'Accessos: Considerar la implementació de polítiques que restringeixin l'accés a dominis rars des de processos no de confiança. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i accessoris a dominis rars en el futur.

Remote account enumeration	L'alerta indica la possibilitat d'enumeració remota de comptes, un comportament que pot ser utilitzat per atacants per a recopilar informació sobre usuaris i comptes en el sistema.	1. Anàlisi d'Activitat d'Enumeració: Investigar l'activitat d'enumeració remota per a determinar el seu origen i naturalesa. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'activitat d'enumeració remota. 3. Canviar Credencials: Considerar el canvi de credencials si es confirma activitat maliciosa per a prevenir accessos no autoritzats. 4. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb l'enumeració remota. 5. Enfortiment de Seguretat: Reforçar les mesures de seguretat per a prevenir futures activitats d'enumeració remota. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.
Remote command execution via wmic.exe	L'alerta indica l'execució remota de comandos a través de wmic.exe, una eina legítima de Windows Management Instrumentation (WMI) que també pot ser utilitzada de manera maliciosa per a executar comandos a distància.	1. Anàlisi de Comandos Executats: Investigar els comandos executats a través de wmic.exe per a determinar la seva intenció i legitimitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'execució remota de comandos. 3. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb l'execució remota de comandos. 4. Restricció d'Execució: Considerar la implementació de polítiques que restringeixin l'execució remota de comandos a través de wmic.exe en entorns no autoritzats. 5. Enfortiment de Seguretat: Reforçar les mesures de seguretat per a prevenir futures execucions remotes de comandos no autoritzades. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.

Remote WMI process execution	L'alerta indica l'execució remota de processos a través de Windows Management Instrumentation (WMI). Aquesta activitat podria ser indicativa d'un intent de controlar sistemes a distància o realitzar accions malicioses en la xarxa.	1. Anàlisi de Processos Executats: Investigar els processos executats remotament a través de WMI per a determinar la seva legitimitat i autorització. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'execució remota de processos a través de WMI. 3. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb l'execució remota de processos. 4. Restricció d'Accés WMI: Considerar la implementació de polítiques que restringeixin l'accés remot a WMI i evitin el seu ús no autoritzat. 5. Enfortiment de Seguretat: Reforçar les mesures de seguretat per a prevenir futures execucions remotes de processos no autoritzades. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.
Rundll32 execution without parameters	L'alerta assenyala l'execució de Rundll32 sense paràmetres. Rundll32 és una utilitat de Windows que permet l'execució de funcions en arxius DLL. L'execució sense paràmetres pot ser indicativa d'un intent d'abús o execució maliciosa	1. Anàlisi d'Execució de Rundll32: Investigar l'execució de Rundll32 sense paràmetres per a determinar la seva intenció i legitimitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'execució de Rundll32. 3. Anàlisi de DLLs Invocades: Analitzar les DLLs invocades per Rundll32 per a identificar possibles amenaces o comportaments maliciosos. 4. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb l'execució de Rundll32. 5. Restricció d'Execució: Considerar la implementació de polítiques que restringeixin l'execució de Rundll32 sense paràmetres. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar execucions inusuals de Rundll32 i reforçar les polítiques de seguretat.

Script file added to startup-related Registry keys	L'alerta indica l'addició d'un arxiu de script a les claus del Registre relacionades amb l'inici del sistema. Aquest comportament podria indicar intents d'executar scripts maliciosos en iniciar el sistema.	1. Anàlisi del Script Agregat: Investigar el contingut del script agregat per a entendre el seu propòsit i avaluar la seva legitimitat. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre l'addició del script a les claus del Registre. 3. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb el script agregat a l'inici del sistema. 4. Eliminació o Aïllament del Script: Eliminar o aïllar el script si es confirma activitat maliciosa per a prevenir execucions automàtiques no autoritzades. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i enfortir les polítiques de seguretat relacionades amb l'inici del sistema.
Suspicious docker image download from an unrecognized registry	L'alerta indica la descàrrega d'una imatge Docker sospitosa des d'un registre no reconegut. Això podria indicar un intent d'introduir imatges malicioses en l'entorn Docker.	1. Anàlisi de la Imatge Docker: Investigar la imatge Docker descarregada per a determinar la seva legitimitat i contingut. 2. Revisió de Registres Docker: Revisar els registres de Docker per a obtenir detalls addicionals sobre la descàrrega de la imatge des del registre no reconegut. 3. Escaneig d'Imatge Docker: Realitzar un escaneig de la imatge Docker a la recerca de possibles vulnerabilitats de seguretat o malware. 4. Restricció de Descàrregues: Considerar la implementació de polítiques que restringeixin la descàrrega d'imatges Docker des de registres no autoritzats. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar descàrregues d'imatges Docker sospitoses i reforçar les polítiques de seguretat en entorns de contenidors.

Suspicious executable detected	L'alerta indica la detecció d'un executable sospitós en el sistema. Això podria ser indicatiu de la presència de malware, eines malicioses o arxius executables desconeguts.	1. Aïllament de l'Executable: Aïllar l'executable detectat per a evitar possibles impactes en el sistema i en la xarxa. 2. Anàlisi de l'Executable: Analitzar l'executable sospitós en un entorn segur per a entendre el seu comportament i determinar si és maliciós. 3. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb l'executable detectat. 4. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la detecció de l'executable sospitós.

Suspicious File Modification	L'alerta assenyala modificacions sospitoses en un arxiu. Les modificacions no autoritzades en arxius poden ser indicatives d'activitat maliciosa, com la manipulació de dades o la introducció de malware.	1. Aïllament de l'Arxiu: Aïllar l'arxiu modificat per a evitar que el canvi es propagui a altres sistemes. 2. Anàlisi de l'Arxiu: Analitzar l'arxiu modificat en un entorn controlat per a entendre la naturalesa de les modificacions i avaluar el seu impacte. 3. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre les modificacions sospitoses. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb les modificacions de l'arxiu. 5. Restauració des de Còpies de seguretat: Restaurar l'arxiu afectat des de còpies de seguretat de confiança si és necessari. 6. Notificació a Equips de Seguretat: Notificar a l'equip de seguretat sobre la detecció per a anàlisi addicional i presa de mesures correctives.

Suspicious LNK file created from Office	L'alerta indica la creació d'un arxiu LNK (access shortcut) sospitós des d'una aplicació d'Office. Els arxius LNK poden ser utilitzats per a executar comandos o llançar programes de manera maliciosa.	1. Anàlisi de l'Arxiu LNK: Investigar el contingut de l'arxiu LNK creat des de l'aplicació d'Office per a determinar la seva intenció i potencial maliciós. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la creació de l'arxiu LNK. 3. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb l'arxiu LNK sospitós. 4. Restricció d'Execució de LNK Considerar la implementació de polítiques que restringeixin l'execució d'arxius LNK des d'ubicacions no segures. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat relacionades amb arxius LNK.

Suspicious Process Creation	L'alerta indica la creació d'un procés sospitós en el sistema. La creació de processos inusuals pot ser indicativa d'activitat maliciosa, com l'execució de malware o eines no autoritzades.	1. Anàlisi del Procés Creat: Investigar el procés creat per a entendre la seva funció i determinar si és maliciós. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la creació del procés sospitós. 3. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb el procés sospitós. 4. Restricció d'Execució: Considerar la implementació de polítiques que restringeixin l'execució de processos no autoritzats o sospitosos. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.

Unsigned and unpopular process performed an injection	L'alerta indica que un procés no signat i poc comú ha realitzat una injecció en un altre procés. Les injeccions de codi poden ser indicatives de tècniques utilitzades per malware per a evadir la detecció i executar codi maliciós en el context de processos legítims.	1. Aïllament del Procés No Signat: Aïllar el procés no signat per a evitar que continuï interactuant amb altres processos i propagant possibles amenaces. 2. Anàlisi d'Injecció: Analitzar la injecció realitzada per a comprendre la seva naturalesa i avaluar qualsevol impacte potencial. 3. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la injecció realitzada. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb el procés no signat i la injecció. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.
Unsigned and unpopular process performed injection into a process signed by a security vendor	L'alerta indica que un procés no signat i poc comú ha realitzat una injecció en un altre procés que està signat per un proveïdor de seguretat. Aquest comportament pot ser indicatiu d'intents d'evadir la detecció de seguretat.	1. Aïllament de Processos: Aïllar tant el procés no signat com el procés signat pel proveïdor de seguretat per a evitar qualsevol interacció addicional. 2. Anàlisi d'Injecció: Analitzar la injecció realitzada per a entendre la seva intenció i avaluar qualsevol possible impacte. 3. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la injecció en el procés signat pel proveïdor de seguretat. 4. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb la injecció. 5. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i enfortir les polítiques de seguretat.

Vulnerable driver loaded	L'alerta indica que s'ha carregat un controlador (driver) vulnerable en el sistema. Els controladors vulnerables poden ser explotats per atacants per a comprometre la integritat i seguretat del sistema.	1. Desactivació del Controlador: Desactivar o desinstal.lar el controlador vulnerable per a evitar possibles explotacions. 2. Actualització de Controladors: Actualitzar el controlador a l'última versió disponible que corregeixi les vulnerabilitats conegudes. 3. Revisió de Configuracions: Revisar les configuracions de seguretat per a assegurar-se que només es carreguin controladors signats i de confiança. 4. Escaneig de Malware: Realitzar un escaneig de malware a la recerca de possibles amenaces associades amb la presència del controlador vulnerable.
WildFire Malware	L'alerta indica la detecció de malware tipus WildFire en el sistema. WildFire és un terme que sovint s'associa amb malware avançat i perillós.	1. Aïllament del Sistema: Aïllar el sistema afectat per a evitar que el malware es propagui a altres sistemes. 2. Anàlisi del Malware: Realitzar una anàlisi profunda del malware per a entendre el seu comportament, funcions i possibles impactes. 3. Eliminació del Malware: Utilitzar eines de seguretat de confiança per a l'eliminació efectiva del malware del sistema. 4. Revisió d'Activitats Recents: Revisar les activitats recents en el sistema per a identificar possibles vectors d'infecció i punts d'entrada del malware. 5. Notificació a Equips de Seguretat: Notificar als equips de seguretat sobre la detecció per a anàlisi addicional i presa de mesures correctives. 6. Actualització de Signatures de Seguretat: Assegurar-se que les signatures de seguretat estiguin actualitzades per a detectar i prevenir futures amenaces similars.

Windows LOLBIN executable connected to a rare external host	L'alerta indica que un executable de Windows considerat com Living Off the Land Binary (LOLBin) ha establert una connexió amb un host extern poc comú. Els LOLBins són eines legítimes de Windows utilitzades pels atacants per a executar comandos de manera legítima i evadir deteccions.	1. Aïllament del Sistema: Aïllar el sistema afectat per a evitar que la connexió maliciosa afecti altres sistemes. 2. Anàlisi de l'Executable LOLBIN: Investigar l'executable LOLBIN per a comprendre la seva funció i determinar si la seva connexió amb el host extern és legítima o maliciosa. 3. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre la connexió del LOLBIN al host extern. 4. Anàlisi de Trànsit de Xarxa: Analitzar el trànsit de xarxa associat amb la connexió per a identificar patrons maliciosos i determinar la naturalesa de la comunicació. 5. Bloqueig de Connexió: Bloquejar la connexió al host extern si es confirma activitat maliciosa per a prevenir la transmissió de dades no autoritzades. 6. Monitoratge Continu: Establir un monitoratge continu per a detectar activitats similars i reforçar les polítiques de seguretat.
WmiPrvSe.exe Rare Child Command Line	L'alerta indica que el procés WmiPrvSe.exe ha executat un comando inusual o rar. WmiPrvSe.exe és el procés de servei de host de WMI (Windows Management Instrumentation). Un comando inusual pot indicar intents d'abús o comportament maliciós.	1. Anàlisi del Comando Executat: Investigar el comando executat per WmiPrvSe.exe per a entendre la seva intenció i avaluar qualsevol comportament maliciós. 2. Revisió de Registres d'Esdeveniments: Revisar els registres d'esdeveniments del sistema per a obtenir detalls addicionals sobre el comando executat per WmiPrvSe.exe. 3. Escaneig de Malware: Realitzar un escaneig complet del sistema a la recerca de possibles amenaces associades amb el comando executat. 4. Monitoratge Continu de WMI: Establir un monitoratge continu per a detectar comandos inusuals executats pel servei de host de WMI. 5. Actualització de Signatures de Seguretat: Assegurar-se que les signatures de seguretat estiguin actualitzades per a detectar i prevenir futurs comportaments maliciosos.