Benemérita Universidad

Autónoma de Puebla

Facultad de Ciencias de la Computación

PROPUESTA DE MEJORA METODOLÓGICA DEL ANÁLISIS DE INCIDENTES DESPLEGANDO UNA PLATAFORMA DE RESPUESTA A INCIDENTES OPEN-SOURCE Y TECNOLOGÍAS SOAR EN EQUIPOS CON SERVICIOS ESPECIALIZADOS EN CIBERSEGURIDAD.

Tesis para obtener el grado de:

Licenciado en Ing. Ciencias de la Computación

Presenta:

Sebastián Méndez Méndez

Director de Tesis:

M.C. María del Carmen Santiago Díaz

Asesor(es) de Tesis:

M.C. Ana Claudia Zenteno Vázquez

Puebla, Pue. Febrero 2025

RESUMEN

Esta tesis examina las ventajas potenciales de integrar plataformas de respuesta a incidentes de ciberseguridad (IRP), Sistemas de Información y Gestión de Eventos (SIEM), Antivirus de Nueva Generación (NGAV), Endpoint Detection and Response (EDR), Extended Threat Intelligence Platforms (XTI), y herramientas de orquestación, automatización y respuesta (SOAR) en las operaciones de ciberseguridad. El estudio investiga el estado actual de las prácticas de respuesta a incidentes e identifica los retos y limitaciones asociados a los métodos tradicionales. Posteriormente, la tesis propone un enfoque integrador con estas herramientas para agilizar el proceso de atención a incidentes y proponiendo un método de mejora operacional. La metodología de investigación incluye una revisión de la literatura, estudios de casos y estadísticas de esta área emergente en el mercado en los últimos años. Los resultados indican que la integración de las diferentes herramientas de seguridad de la información puede mejorar significativamente los procesos de análisis y detección además de reducir el tiempo medio de respuesta (MTTR) mediante la automatización de las tareas manuales y la orquestación de la información. Sin embargo, su implantación requiere una inversión significativa en términos de tiempo, recursos y formación del personal. Este proyecto contribuye al conjunto de conocimientos existentes proporcionando una memoria técnica y un análisis de las ventajas y limitaciones de la integración de diferentes soluciones de ciberseguridad utilizando servicios en la nube. Los resultados de este estudio tienen implicaciones prácticas para los profesionales del área y las organizaciones que buscan mejorar sus procesos. El estudio concluye con recomendaciones para futuras investigaciones y aplicaciones prácticas de la integración de estas tecnologías.

ABSTRACT

This thesis examines the potential advantages of integrating cybersecurity incident response platforms (IRP), Systems Information and Event Management (SIEM), Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Extended Threat Intelligence Platforms (XTI), and tools for orchestration, automation, and response (SOAR) into cybersecurity operations. The study investigates the current state of incident response practices and identifies the challenges and limitations associated with traditional methods. Subsequently, the thesis proposes an integrative approach using these tools to streamline the incident response process and proposing an operational improvement method. The research methodology includes a literature review, case studies and statistics of this emerging area in the market in recent years. The results indicate that the integration of different information security tools can significantly improve analysis and detection processes in addition to reducing the mean time of response (MTTR) by automating manual tasks and orchestration of information. However, its implementation requires a significant investment in terms of time, resources and staff training. This project contributes to the existing body of knowledge by providing a technical report and analysis of the advantages and limitations of integrating different cybersecurity solutions using cloud services. The results of this study have practical implications for practitioners in the field and organizations seeking to improve their processes. The study concludes with recommendations for future research and practical applications of integrating these technologies.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Capítulo 1.- Introducción

En el presente proyecto, se propone una metodología para el manejo de respuesta a incidentes en ciberseguridad, mediante la realización de una prueba de concepto (PoC) que permita albergar una interfaz open-source capaz de interconectar diferentes proveedores de inteligencia en ciberamanezas (CTI) para analizar posibles (Indicadores de Compromiso) IoCs identificados en eventos de seguridad. Dicho laboratorio utiliza en gran medida Application Programming Interfaces (APIs) las cuales son un conjunto de definiciones y protocolos que permiten construir e integrar aplicaciones o servicios (WEB o móviles) que siguen los principios de la arquitectura de transferencia de estado representacional (REST). Utiliza operaciones HTTP estándar (GET, POST, etc.) para interactuar con recursos (objetos o servicios) identificados por URLs únicas, transfiriendo la información en formatos como JSON o XML. Estas propiedades ayudan integrar u orquestar todas las soluciones de seguridad en una misma plataforma.

El objetivo principal es aprovechar la concentración de toda la información posible de proveedores de CTI asociado a cada evento de seguridad en una sola consola principal, proporcionando la capacidad de tomar decisiones en un periodo corto de tiempo. Siguiendo este enfoque es sumamente importante señalar que este recurso es muy valioso pues mientras más rápido se progresa en las fases de la respuesta a incidentes, menor es la probabilidad de que una amenaza afecte deliberadamente uno de los activos más importantes en cualquier organización como lo es la información. Está característica es un indicador clave de desempeño (KPI) del proyecto, así como un correcto análisis de los eventos.

Es necesario prevenir que las acciones que comprometen a la Confidencialidad, Integridad y Disponibilidad (CIA) de la información por sus siglas en inglés, ocurran de manera inesperada. Debido a ello, es posible establecer flujos de trabajo (Workflows) realizados con herramientas de automatización otorgando la posibilidad de realizar acciones de mitigación en base a los IoC’s encontrados con el fin de establecer como requerimiento su eliminación y evitar que los atacantes

informáticos, accedan de forma deliberada o sin permiso a la información o dañar recursos valiosos. De esta manera, es posible actuar con certeza al analizar las tácticas, técnicas y procedimientos (TTP's) que están descritos por marcos de trabajo, como el conocido Mitre Attack que realiza un mapeo de la tácticas, técnicas y procedimientos más comunes que lo atacantes utilizan, lo que justifica la inclusión de medidas y controles de seguridad, que garantizan que estos, sean completos y otorguen protección a los sistemas.

1.1 Antecedentes

El proyecto surge de la necesidad de incorporar las tecnologías más emergentes en el mercado con la finalidad de proveer inteligencia y rapidez en el proceso de respuesta a incidentes, visualizar la carga de trabajo que lleva a cabo un equipo de profesionales de TI encargados de la ciberseguridad día con día, disminuir la probabilidad de errores humanos durante el análisis, concentrar las fuentes de información en una sola plataforma para su correlación y proporcionar una respuesta automática que mitigue la amenaza que está afectando a la información. Por tanto, la mejora continua en los procesos de ciberseguridad y el ahorro de tiempo y esfuerzo mediante la automatización de tareas manuales son la principal razón de esta investigación.

El reporte Digital Trust Insights 2024, edición México, revela una situación crítica respecto a la ciberseguridad en el país, destacando la necesidad urgente de colocarla en el centro de la innovación tecnológica [1]. Entre los hallazgos más importantes se encuentran:

- **Preocupaciones en ciberseguridad**: La filtración de datos, hackeos y amenazas a la nube son las principales preocupaciones tanto a nivel nacional como global. Un 50% de las empresas están preocupadas por amenazas relacionadas con la nube.

- **Gestión de riesgos y resiliencia**: Aunque cuatro de cada diez empresas mexicanas responden rápidamente a las amenazas, seis de cada diez están mejorando la resiliencia en ciberseguridad identificando procesos críticos del negocio.

- **Integración de la seguridad en la nube**: Se destaca la necesidad de integrar la seguridad en la nube dentro de la estrategia general de ciberseguridad, con énfasis en la mejora continua de planes de recuperación y la negociación de contratos con proveedores de servicios en la nube.

- **Adopción de IA generativa**: El uso de herramientas de inteligencia artificial generativa se vislumbra como una oportunidad para desarrollar nuevas líneas de negocio y aumentar la productividad. Sin embargo, se reconoce el riesgo de ciberataques asociados.

- **Líneas de acción recomendadas**: El informe sugiere acciones concretas, como colocar la ciberseguridad en el centro de todas las iniciativas digitales, adoptar un enfoque estratégico, maximizar la inversión en tecnología y talento humano, y fomentar una cultura organizacional que priorice la seguridad cibernética en todos los niveles jerárquicos.

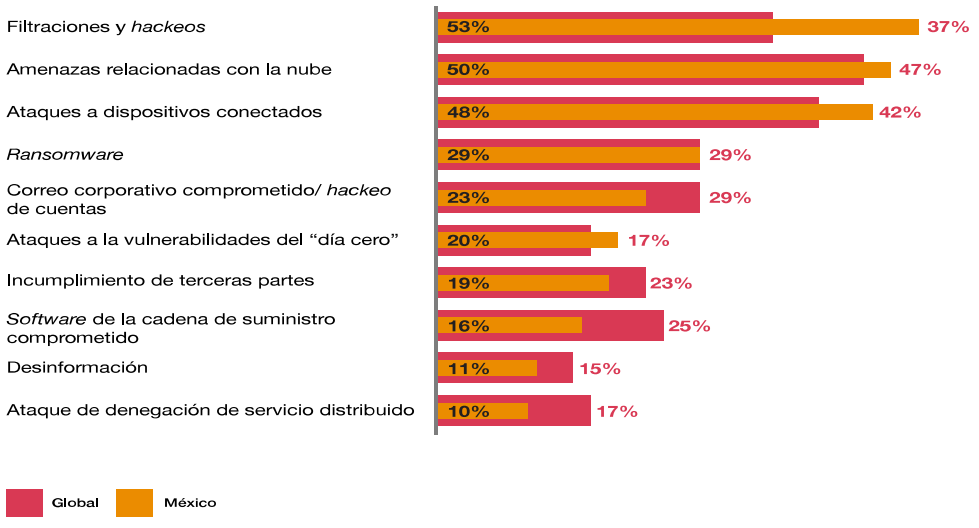


Fig. 1 *Principales resultados sobre las posibles amenazas para las organizaciones en México y a nivel global en los siguientes 12 meses. [1].*

En 2024, México se posiciona como uno de los países más vulnerables a la inseguridad digital. Según Aníbal Rojas del grupo expansión, esto subraya la necesidad urgente de estrategias de seguridad cibernética más robustas en América Latina, donde países como Colombia, Argentina, Chile y Brasil también enfrentan altos niveles de ciberataques.

Rojas propone varias estrategias clave para fortalecer la ciberseguridad, como realizar evaluaciones de riesgos anuales, capacitar al personal en prácticas seguras, y crear políticas de seguridad claras y concisas. Además, implementar controles de seguridad como firewalls, antivirus y sistemas de detección de intrusiones, junto con la encriptación de datos es esencial para proteger la información confidencial.

Así mismo, se destaca la importancia de diseñar planes de respuesta a incidentes para asegurar una respuesta rápida y efectiva ante cualquier violación de seguridad. La cooperación internacional y el intercambio de inteligencia sobre amenazas son vitales para abordar los desafíos de ciberseguridad de manera eficaz en la era digital actual [2].

En un informe presentado por ESET, empresa especializada en ciberseguridad, se reveló que un tercio de las organizaciones en América Latina fueron víctimas de ciberataques durante 2023. Los sectores más afectados incluyen gobierno, tecnología y banca, enfrentándose a amenazas crecientes como el ransomware con tácticas de doble extorsión, que han impactado significativamente a industrias clave como petróleo, manufactura y salud. Además, vulnerabilidades en plataformas ampliamente utilizadas como Microsoft Office, junto con la proliferación de Troyanos de Acceso Remoto (RAT) como Agent Tesla, se identificaron entre las principales amenazas detectadas. Preocupantemente, un 62% de las empresas encuestadas manifestó que sus presupuestos destinados a ciberseguridad son insuficientes para afrontar estos desafíos [3].

De acuerdo con el CyberEdge 2022 Cyberthreat Defense Report, México ocupa el cuarto lugar entre 17 países analizados como uno de los más afectados por la ciberdelincuencia. Según el informe, el 90.6% de las compañías mexicanas reportaron haber sido atacadas por ciber amenazas, y al menos uno de estos ataques resultó exitoso durante el año analizado. En el contexto de América Latina, Colombia registra la mayor tasa de ciberataques exitosos, con un 93.9% de las organizaciones indicando haber sido comprometidas al menos una vez. Este patrón destaca la creciente exposición de la región a ciberataques sofisticados.

Los altos índices de ataques exitosos en México y Colombia reflejan una tendencia regional donde los actores maliciosos emplean amenazas cada vez más persistentes. Esto podría atribuirse a factores como la rápida adopción de tecnologías digitales, el crecimiento del comercio electrónico y las posibles brechas en la implementación de medidas robustas de ciberseguridad. Además, el informe destaca que la falta de capacitación del personal y las inversiones limitadas en ciberseguridad son factores clave que agravan la vulnerabilidad en América Latina.

Por el contrario, países europeos como el Reino Unido y Alemania registraron tasas notablemente más bajas de éxito en los ataques. Según el informe, el 81.4% de las organizaciones en el Reino Unido y el 72.6% en Alemania informaron haber sido atacadas exitosamente. La menor incidencia en estos países sugiere la existencia de marcos más maduros de ciberseguridad y una cultura organizacional enfocada en la prevención, respaldada por presupuestos más sólidos para la protección contra ciber amenazas.

El informe también destaca diferencias sectoriales en la exposición a ataques cibernéticos. En América Latina, sectores como la educación, con un 90.5% de ataques exitosos, y las finanzas, enfrentan riesgos particularmente altos debido a una combinación de infraestructura vulnerable y datos sensibles. En Europa, aunque sectores como las finanzas y la sanidad enfrentan amenazas significativas, los porcentajes de éxito son generalmente más bajos, lo que refleja mejores prácticas.

De cara al futuro, en Latinoamérica las compañías se enfrentan un panorama desafiante debido a los índices consistentemente altos de ciberataques exitosos. Sin embargo, su capacidad para responder eficazmente está limitada por restricciones presupuestarias y una falta de cultura organizacional enfocada en la ciberseguridad. En contraste, dentro del territorio europeo, aunque también expresan preocupación por amenazas crecientes, parecen mejor preparadas gracias a marcos regulatorios avanzados y asignaciones presupuestarias más generosas. La inversión en ciberseguridad, tanto en América Latina como en Europa, seguirá siendo un factor decisivo para reducir los riesgos y responder a las amenazas en constante evolución [4].

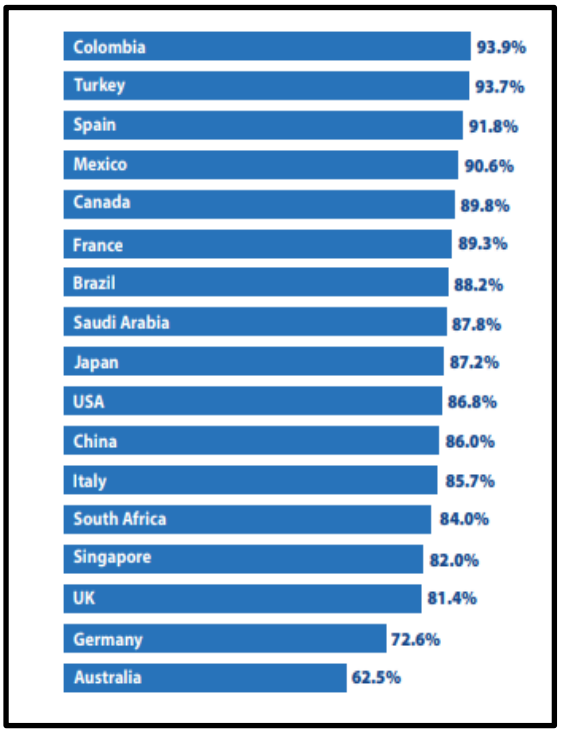


Fig. 2 *Porcentaje de ciber-ataques con éxito durante el 2022, por país. México ocupa el 4to lugar a nivel internacional [4].*

Tras la pandemia de COVID-19 en México, los delitos cibernéticos experimentaron un crecimiento exponencial, pasando de 300.3 millones de intentos en 2019 a 120 mil millones en 2021, lo que representa un incremento de casi 400 veces. Este aumento posicionó a México como el país más atacado en América Latina, reflejando una alarmante vulnerabilidad en su ecosistema digital [5].

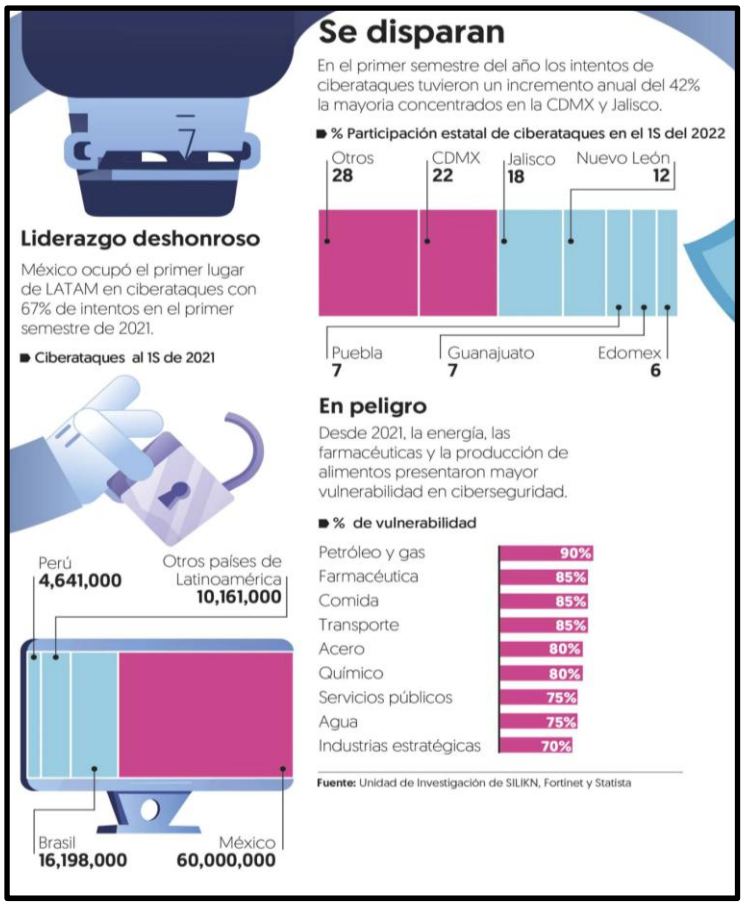


Fig. 3 *Infografía sobre el contexto en los últimos años de México en ciberseguridad. [5]*

Especialistas atribuyen este incremento a la transición masiva hacia el trabajo remoto durante la pandemia, que amplió significativamente la superficie de ataque disponible para los ciberdelincuentes. Según estimaciones globales, los ingresos generados por el cibercrimen alcanzaron los 6 billones de dólares en 2021 y se proyecta que para 2025 asciendan a 15 billones de dólares. En algunos países, como España y Argentina, la ciberdelincuencia ya genera más ingresos que el narcotráfico, lo que evidencia la magnitud del problema.

El primer informe semestral de Silikn en 2022 reveló que los ciberatacantes emplearon ransomware (secuestro de información) como una de las principales herramientas para comprometer sistemas. La explotación de conexiones de acceso remoto poco seguras fue responsable del 48.6% de los intentos, mientras que el phishing —correos electrónicos con contenido engañoso cargado de malware— representó el 39% de los accesos exitosos. Este tipo de ataques no solo paralizan

operaciones, sino que también comprometen la privacidad de las víctimas, con un 71% de los incidentes investigados resultando en filtración de información sensible [5].

El panorama de la ciberseguridad en México para los próximos años es preocupante. Los crecientes índices de ataques no solo afectan a empresas y gobiernos, sino también a ciudadanos individuales, destacando la urgente necesidad de adoptar medidas preventivas y robustecer las estrategias de protección digital en todos los niveles. Este contexto exige una inversión considerable en tecnologías de ciberseguridad y la capacitación de personal para enfrentar amenazas cada vez más sofisticadas.

En 2023, Víctor Ruiz, fundador de SILIKN, destacó en un informe anual que solo el 41.7% de las empresas y organismos gubernamentales en México lograron implementar medidas preventivas efectivas para defenderse de los ciberataques. Como resultado, el 58.3% de los ataques lanzados contra estas organizaciones tuvieron éxito, lo que refleja una vulnerabilidad significativa en el panorama de la ciberseguridad del país [6]. Esta situación subraya la urgente necesidad de adoptar medidas inmediatas para mitigar riesgos y fortalecer las defensas cibernéticas.

Entre las principales razones de esta vulnerabilidad se encuentran la falta de un enfoque preventivo robusto, una limitada concienciación sobre ciberseguridad, y la ausencia de políticas y procedimientos estandarizados de protección digital. Muchas organizaciones tampoco cuentan con una gestión adecuada de sus recursos en la nube ni con metodologías eficaces para identificar y gestionar activos, amenazas y riesgos de seguridad. Además, la falta de integración de soluciones avanzadas, como herramientas para gestionar identidades y privilegios de acceso, agrava el problema.

Para mejorar la postura de ciberseguridad en México, Ruiz propone una serie de medidas clave, entre las que se incluyen:

- La integración efectiva de datos de identidad y privilegios de acceso para limitar accesos no autorizados.
- El aumento de recursos dedicados a estrategias preventivas de ciberseguridad.
- La implementación de programas de formación y concienciación en seguridad cibernética dirigidos a empleados y directivos.
- La adopción de políticas de seguridad robustas y el despliegue de soluciones tecnológicas de protección avanzada.

Sin una acción coordinada y un compromiso real, México seguirá enfrentándose a riesgos cibernéticos significativos que podrían tener graves repercusiones en su economía, sociedad y seguridad nacional. Ruiz también resalta la importancia de una mejor coordinación entre organizaciones públicas y privadas para compartir información y estrategias, junto con la necesidad de invertir en un marco regulatorio sólido que fomente estándares de ciberseguridad.
Por último, enfatiza la urgencia de priorizar la educación en ciberseguridad como un pilar para construir una defensa más sólida contra el creciente número de amenazas cibernéticas [6].

Hoy en día, contratar servicios de ciberseguridad para compañías de diferentes industrias, tanto a nivel nacional como internacional, se ha convertido en una necesidad crítica. En América Latina, se estima que las inversiones en servicios y soluciones de ciberseguridad alcanzaron los 3,600 millones de dólares en 2023, representando un incremento del 11.1% respecto al año anterior [7]. Este aumento subraya el creciente reconocimiento, sobre la importancia de adoptar un enfoque holístico hacia la seguridad cibernética, que no solo incluye la adquisición de tecnología, sino también la inversión en consultoría, implementación y operación continua de estas soluciones.

Un aspecto clave identificado por IDC Latín América (empresa de TI, con sede en Estados Unidos) es que los servicios de gestión de ciberseguridad representan el 56%

del gasto total en la región, reflejando la necesidad de enfoques integrales y dinámicos para proteger la infraestructura tecnológica. Las principales razones detrás de la demanda de estos servicios son el cumplimiento normativo y la necesidad urgente de proteger información sensible, especialmente después de haber sufrido ciberataques previos. Esto evidencia una mayor madurez en la percepción de los riesgos cibernéticos por parte de las empresas.

De cara al futuro, diversas comunidades consideran que los presupuestos de ciberseguridad deben centrarse en tres áreas prioritarias:

- **Mejora de las habilidades de seguridad**: La capacitación constante del personal en temas de ciberseguridad se percibe como esencial para enfrentar un panorama de amenazas en rápida evolución. Esto incluye desde entrenamientos básicos hasta formación avanzada en detección y respuesta a incidentes.

- **Implementación de tecnologías avanzadas**: La adopción de soluciones innovadoras, como herramientas de inteligencia artificial y automatización, es crucial para optimizar las capacidades de detección, prevención y respuesta frente a ataques cada vez más sofisticados.

- **Cuantificación de riesgos cibernéticos**: Es evidente la necesidad de evaluar y medir de manera más precisa los riesgos cibernéticos. Esto permitirá diseñar estrategias de mitigación efectivas, priorizando inversiones en áreas de mayor impacto y asegurando la sostenibilidad de las operaciones.

Este enfoque integrado no solo permite a las empresas mitigar las amenazas actuales, sino que también las posiciona estratégicamente para enfrentar desafíos futuros en un entorno digital cada vez más complejo y dinámico.
Según IDC, esta evolución en la inversión y gestión de ciberseguridad será determinante para fortalecer la resiliencia tecnológica en la región [7].

1.2 Estado del arte

El estudio, análisis e implementación de soluciones avanzadas de ciberseguridad es un desafío reciente que instituciones privadas, particularmente empresas de TI cuyos servicios de Managed Security Service Providers (MSSP), han comenzado a abordar debido a la rápida evolución de las necesidades comerciales y las tecnologías de detección, correlación y respuesta a incidentes. Este dinamismo ha llevado a una creciente automatización de procesos tradicionalmente manuales, mejorando tanto la eficiencia como la precisión en la gestión de amenazas.

En el panorama actual, existen numerosas plataformas comerciales disponibles que permiten a las organizaciones evaluar su idoneidad mediante pruebas de concepto (PoC). Este enfoque permite determinar cómo estas tecnologías pueden integrarse de manera efectiva en las operaciones existentes. En este proyecto se investigaron varias de estas plataformas probadas de forma metodológica en ambientes productivos, evaluando sus ventajas, desventajas, capacidades más relevantes y posibles áreas de mejora. Esto busca no solo proporcionar mayor visibilidad sobre sus funcionalidades, sino también facilitar la toma de decisiones informadas para su adopción en entornos específicos.

Un sistema destacado en el ámbito de la ciberseguridad es SMS-I, una herramienta avanzada diseñada para optimizar el proceso de investigación forense en incidentes de seguridad. Este sistema integral combina múltiples componentes, como un mecanismo de sincronización de datos, un motor de aprendizaje automático, un motor de minería de reglas de asociación, una base de datos de investigación, un calendarizador y una aplicación web interactiva. Estos elementos trabajan en conjunto para adquirir, procesar y almacenar datos, predecir incidentes y ofrecer una interfaz gráfica de usuario (GUI) intuitiva que permite a los analistas de un Security Operation Center (SOC) interactuar con la herramienta de manera eficiente [8].

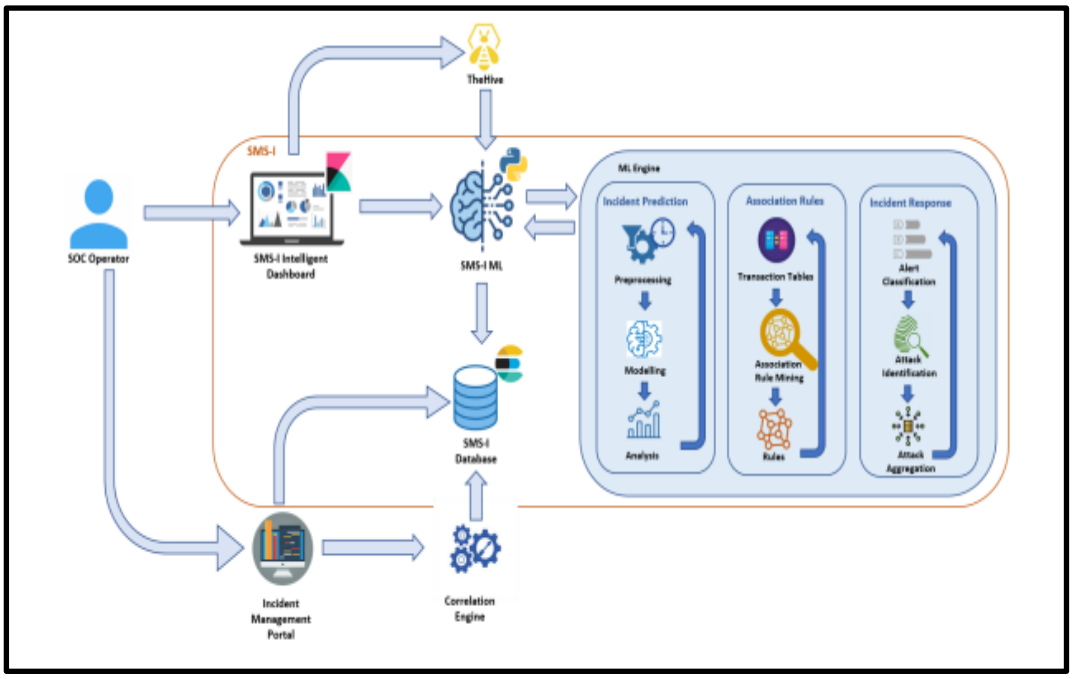


Fig. 4 *Arquitectura de SMS-I. [8]*

SMS-I utiliza técnicas de inteligencia artificial avanzadas, como algoritmos supervisados y modelos basados en bosques aleatorios, para analizar datos multidimensionales. Su objetivo principal es predecir la probabilidad de que una alerta sea un incidente real, facilitando la identificación de situaciones anómalas y reduciendo el tiempo de respuesta. La información generada por estos análisis se presenta a través de cuadros de mando interactivos que simplifican la visualización y priorización de amenazas, mejorando significativamente la calidad y velocidad de las decisiones [8].

Componentes principales y funcionalidad de SMS-I

La herramienta se estructura en tres grupos funcionales principales:

- **Predicción de probabilidad de incidentes**: Utiliza algoritmos supervisados para determinar la probabilidad de que una alerta represente una amenaza real.
- **Reglas de asociación**: Identifica correlaciones entre múltiples alertas para detectar patrones complejos en el comportamiento de los atacantes.
- **Respuesta a incidentes**: Automatiza las medidas paliativas necesarias para mitigar amenazas en tiempo real.

SMS-I aborda de manera integral dos desafíos críticos dentro de un SOC:

- **Clasificación de alertas entrantes**: Prioriza las alertas basándose en su relevancia y probabilidad de ser incidentes reales.
- **Agrupación de alertas similares**: Organiza y consolida eventos relacionados para reducir redundancias y mejorar el análisis.

Integración con herramientas y aplicaciones

SMS-I se integra con The Hive, una reconocida herramienta de gestión de incidentes de código abierto, para fomentar la colaboración entre profesionales de seguridad. Esta integración permite compartir información crítica y mejorar la calidad de las investigaciones mediante datos más precisos y completos. Además, SMS-I proporciona modelos personalizables para la clasificación y agregación de alertas, así como para la detección de anomalías, adaptándose a las necesidades específicas de cada organización [8].

Implementación y resultados

La herramienta ha sido implementada con éxito en entornos críticos, como aeropuertos europeos, donde ha demostrado su capacidad para mejorar los procesos de toma de decisiones en los SOC. Los resultados incluyen una mayor eficiencia en la detección de amenazas, una reducción en el tiempo necesario para analizar incidentes y una colaboración más efectiva entre los equipos de seguridad. Entre las mejoras planificadas para el futuro se encuentra el reentrenamiento automático de modelos predictivos y pruebas en otros entornos organizacionales, lo que ampliará aún más su aplicabilidad y eficacia [8].

Impacto y perspectivas

SMS-I representa una solución innovadora en el ámbito de la ciberseguridad, destacándose por su capacidad para automatizar procesos, reducir falsos positivos y proporcionar información procesable a los analistas de seguridad.

Su integración con herramientas de código abierto y el uso de inteligencia artificial consolidan su posición como una herramienta clave para fortalecer la infraestructura de ciberseguridad en organizaciones críticas. Los trabajos futuros apuntan a expandir su funcionalidad, mejorar los algoritmos de predicción y ampliar su implementación en sectores adicionales, lo que promete contribuir significativamente a la resiliencia frente a las crecientes amenazas cibernéticas [8].

Los honeypots son sistemas de engaño utilizados por equipos profesionales de ciberseguridad para recopilar información sobre amenazas y defenderse de ciberataques. Desde finales de los años 90, han desempeñado un papel fundamental como capa adicional de protección, proporcionando un beneficio significativo al disminuir el número de ataques dirigidos a hosts estáticos con el tiempo. Sin embargo, su despliegue presenta desafíos, como la detección de atacantes internos y la atracción de atacantes externos, particularmente cuando no se colocan de forma dinámica dentro de la red. Para superar estas limitaciones, los SOC requieren tecnologías de engaño personalizadas que integren un Security Orchestration, Automation, and Response (SOAR), capaz de desplegar honeypots dinámicamente en función del comportamiento de los atacantes. Este enfoque minimiza los riesgos al atraer a los atacantes hacia sistemas falsos y proteger los activos reales [9].

Investigación en el Instituto Tecnológico de India, Kanpur

Un proyecto de investigación realizado en el Instituto Tecnológico de India en Kanpur identificó una importante laguna en la literatura existente sobre honeypots, proponiendo un motor de orquestación como solución para mejorar su efectividad. Este motor combina varios componentes clave diseñados para supervisar, analizar y responder al comportamiento de los atacantes en tiempo real. Entre sus principales elementos se encuentran:

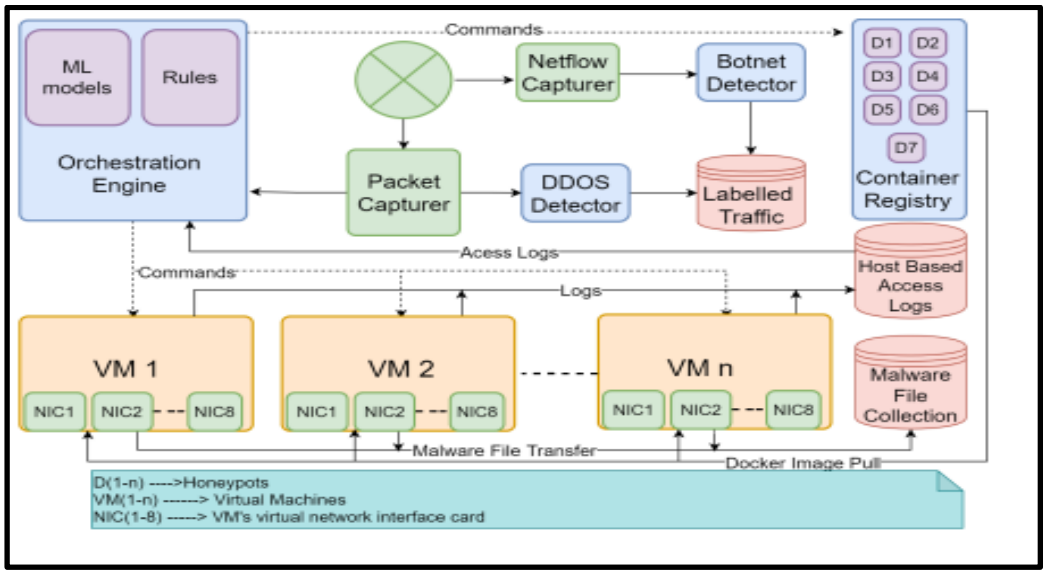


Fig. 5 *Arquitectura de SMS-I. [9]*

- **Máquina anfitriona y máquinas virtuales**: Proveen la infraestructura necesaria para el despliegue flexible de honeypots.
- **Registro de contenedores y almacenamiento**: Facilitan la gestión de datos y registros generados por las interacciones con los atacantes.
- **Rastreador de tráfico**: Monitorea el tráfico entrante para identificar patrones sospechosos y posibles amenazas.
- **Detectores de botnets y DDoS**: Identifican actividades maliciosas específicas y contribuyen a la respuesta automatizada.
- **Herramienta de orquestación**: Centraliza la toma de decisiones y la ejecución de acciones basadas en reglas predefinidas y algoritmos de aprendizaje automático.
- **Registros de acceso**: Documentan las actividades para facilitar análisis posteriores y mejorar las estrategias de defensa [9].

Funcionamiento del motor de orquestación

El motor propuesto despliega honeypots dinámicamente en función del comportamiento observado de los atacantes, ampliando así el tiempo de intervención de estos dentro de la red y permitiendo una mejor recopilación de datos.

El proceso de toma de decisiones utiliza un enfoque híbrido que combina aprendizaje automático y sistemas basados en reglas. Esta combinación no solo optimiza la respuesta a incidentes, sino que también facilita la adaptación a patrones de ataque cambiantes.

Resultados de la implementación

La solución fue probada en un entorno real, mostrando mejoras significativas en comparación con los sistemas existentes:

- **Incremento en la participación de los atacantes**: El motor permitió captar 965 paquetes de ataques DDoS, lo que evidencia su efectividad en atraer y capturar información sobre amenazas.
- Reducción del uso de recursos: Ahorró un 89% del tiempo de CPU en comparación con sistemas tradicionales, demostrando su eficiencia operativa.
- Flexibilidad y adaptabilidad: Los honeypots desplegados dinámicamente ofrecieron una mejor cobertura frente a ataques dirigidos, reduciendo la probabilidad de comprometer activos reales [9].

Desafíos y trabajos futuros

Los investigadores destacaron áreas de mejora, incluyendo:

- **Algoritmos de selección de IP**: Optimizar estos algoritmos podría incrementar la efectividad del motor al dirigir mejor los recursos hacia áreas vulnerables.
- **Incremento del número de honeypots**: Aumentar la densidad de despliegue para abordar amenazas más complejas, como el movimiento lateral de los atacantes una vez que comprometen un sistema.

Desde una perspectiva enfocada en la optimización de recursos, AutoSOC se presenta como una solución empresarial innovadora desarrollada por G.W.P. Chamickara, M.I.M. Cooray, entre otros, del Departamento de Ingeniería de Sistemas de Información de la Facultad de Computación del Sri Lanka Institute of Information Technology. Esta plataforma está diseñada específicamente para pequeñas y medianas empresas (PyMEs) con el objetivo de reducir los costos de implementación en ciberseguridad y, al mismo tiempo, aumentar la eficacia y precisión en la detección de amenazas. AutoSOC destaca por su capacidad de eliminar falsos positivos y vulnerabilidades erróneas mediante un enfoque basado en el aprendizaje continuo sobre la red, lo que lo convierte en una solución adaptable y flexible para organizaciones con presupuestos limitados [10].

Componentes principales.

La plataforma está completamente automatizada e integra varias tecnologías clave que trabajan de manera sinérgica para fortalecer la postura de ciberseguridad:

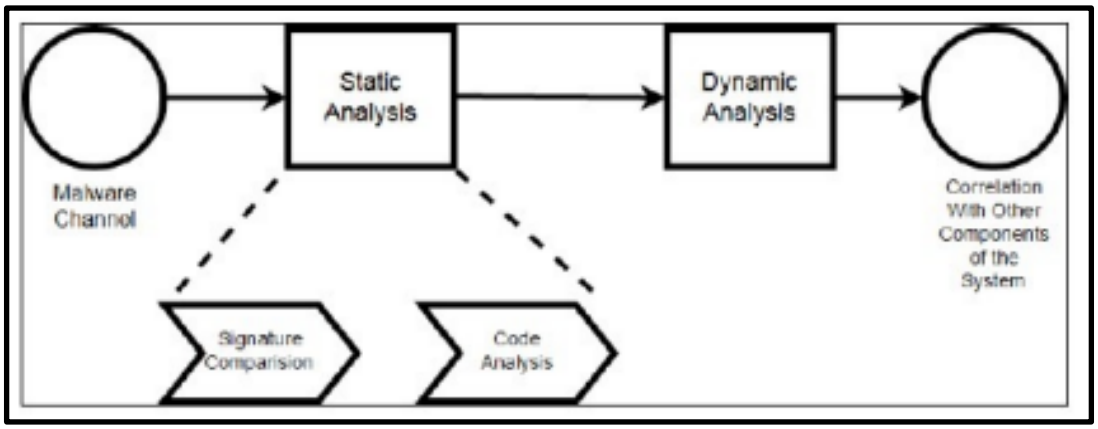


Fig. 6 *Vista general del sistema donde ocurre un análisis estático y dinámico de los canales de información entrantes. [10]*

- **Sistema Inteligente de Detección y Prevención de Intrusiones (IIDPS**): Este componente central detecta y previene ataques potenciales mediante un análisis continuo del tráfico y las actividades en la red. Actúa como una barrera proactiva que mitiga amenazas antes de que comprometan los sistemas.

- **System Information and Event Management (SIEM)**: Diseñado para recopilar, almacenar y analizar datos de registro, el SIEM permite identificar patrones anómalos en el comportamiento de los sistemas. Además, facilita la respuesta a incidentes, análisis forenses y cumplimiento normativo, garantizando la trazabilidad de eventos.

- **Sistema de Análisis de Malware**: Este módulo utiliza técnicas de análisis estático y dinámico, incluyendo ingeniería inversa y pruebas en entornos aislados (sandbox), para identificar y clasificar diferentes tipos de malware que pueden afectar a los usuarios. El análisis estático se basa en la comparación de firmas de malware y la ingeniería inversa, mientras que el análisis dinámico utiliza técnicas de aprendizaje automático para monitorear comportamientos sospechosos en tiempo real [10].

- **Sistema Simple de Investigación Forense**: Proporciona capacidades de investigación para analizar incidentes pasados, ayudando a aprender de ellos y prevenir ataques similares en el futuro. Este sistema se enfoca en el análisis de metadatos, procesos, paquetes de red y otros componentes críticos para determinar la causa raíz de los incidentes [10].

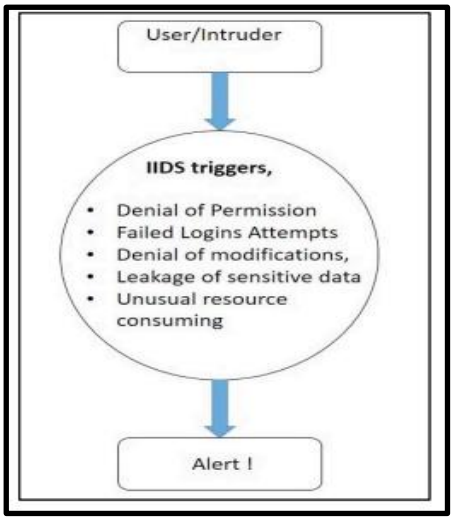


Fig. 7 *Vista general del sistema donde ocurre un análisis estático y dinámico de los canales de información entrantes. [10]*

Arquitectura centrada en SOC

La arquitectura del sistema se enfoca en mejorar las funciones de un (SOC), garantizando la integración de componentes críticos como:

- Procesos estandarizados y efectivos.
- Gobernanza clara para la toma de decisiones.
- Personal capacitado en la identificación y gestión de amenazas.
- Un compromiso continuo con la mejora de las capacidades de seguridad.}

Los autores enfatizan que un SOC exitoso requiere una combinación equilibrada de estos elementos, apoyada en tecnologías avanzadas como AutoSOC para maximizar su efectividad [10].

Uso de Inteligencia Artificial

Para adaptarse rápidamente a situaciones cambiantes, AutoSOC incorpora ramas avanzadas de inteligencia artificial (IA), como Machine Learning y Deep Learning, que permiten:

- Analizar grandes volúmenes de datos en tiempo real.
- Predecir posibles amenazas basándose en patrones históricos.
- Automatizar respuestas a incidentes, reduciendo la carga de trabajo de los analistas.

Además, se utiliza **Docker** como plataforma para garantizar la portabilidad y flexibilidad del sistema, lo que permite su implementación en diversos entornos sin problemas de compatibilidad [10].

Retos y soluciones durante el desarrollo

Durante la fase de implementación, los desarrolladores enfrentaron dificultades relacionadas con la integración de la API de VirusTotal mediante PHP. Estas limitaciones se resolvieron utilizando un script independiente desarrollado en Python, que almacena los datos en una base de datos MariaDB accesible a través de una interfaz web.

Este enfoque no solo resolvió los problemas técnicos, sino que también mejoró la eficiencia operativa del sistema.

Adicionalmente, se planea la implementación del mismo escenario en Django, lo que promete reducir la complejidad del código y mejorar la escalabilidad del sistema. Los autores también trabajan en un mecanismo de aprendizaje automatizado que permita detectar y responder rápidamente a posibles ataques, optimizando aún más la capacidad de respuesta de la plataforma [10].

Impacto y perspectivas

AutoSOC representa un avance significativo en la democratización de la ciberseguridad al ofrecer una solución asequible, pero altamente eficaz, para PyMEs. Su enfoque en la automatización, la eliminación de falsos positivos y el análisis avanzado de amenazas lo posiciona como una herramienta crucial para la protección de su entorno, activos e información.

En el futuro, se espera que las mejoras en los algoritmos de aprendizaje y la integración de nuevas tecnologías de análisis permitan a AutoSOC expandir su aplicabilidad y adaptarse a entornos de amenaza cada vez más complejos [10].

La plataforma Advanced Threat Intelligence Orchestrator (ATIO), desarrollada en el marco del proyecto IRIS financiado por la Unión Europea (acuerdo de subvención No 101021727), se presenta como una solución innovadora para gestionar y priorizar información sobre incidentes de ciberseguridad en ecosistemas de IoT (Internet de las Cosas) y IA (Inteligencia Artificial) en ciudades inteligentes. Diseñada para abordar desafíos complejos en la seguridad cibernética, esta herramienta se basa en un enfoque avanzado de SOAR, utilizando la plataforma de código abierto Shuffle como núcleo. ATIO proporciona una infraestructura altamente personalizable que optimiza la respuesta a incidentes y la gestión de riesgos en entornos urbanos inteligentes, facilitando la colaboración entre SOC, Equipos de Respuesta a Incidentes de Seguridad (CSIRT / CERTs) y proveedores de infraestructura de IA [11].

Propósito y funcionalidad principal

ATIO tiene como objetivo simplificar y agilizar los procesos de ciberseguridad mediante la automatización de tareas rutinarias, la supervisión y la priorización de alertas críticas. Al hacerlo, permite a los equipos SOC y a los expertos en ciberseguridad centrarse en actividades de mayor impacto. Entre sus funciones principales destacan:

- **Flujos de trabajo esquemáticos**: Los usuarios pueden crear y personalizar escenarios de respuesta a incidentes, lo que facilita una reacción ágil y adaptativa ante amenazas emergentes. Estos flujos de trabajo se basan en playbooks y runbooks, que documentan procedimientos y valores culturales para abordar tareas de manera consistente.

- **Integración con herramientas y APIs**: ATIO interactúa con una amplia gama de tecnologías mediante integraciones API, permitiendo una comunicación fluida y una operación eficiente. Entre las herramientas integradas se encuentran MISP, Wazuh, TheHive, y otras plataformas de gestión de amenazas.

Fig. 8 *Entorno visual de Gestión y Seguimiento de alertas basándose en el entorno de diseño SHUFFLE [11].*

- **Gestión de vulnerabilidades**: Ofrece capacidades avanzadas para identificar, priorizar y mitigar vulnerabilidades en sistemas IoT y otros entornos críticos, utilizando técnicas de análisis estático, dinámico e híbrido.

- **SIEM integrado**: Proporciona información correlacionada y contexto adicional para mejorar la toma de decisiones durante la respuesta a incidentes [11].

Componentes clave

La arquitectura de esta plataforma se compone de seis subcomponentes principales, cada uno diseñado para abordar aspectos específicos de la ciberseguridad:

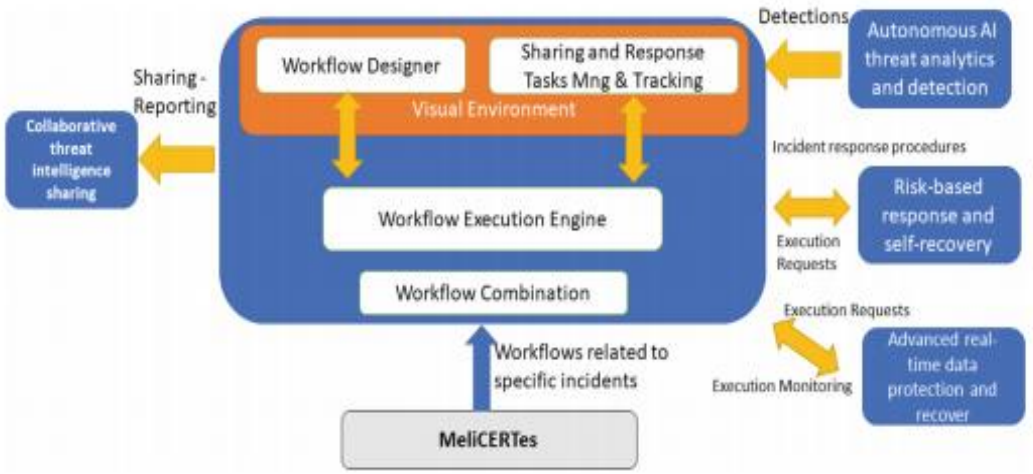


Fig. 9 *La estructura interna del Orquestador y su relación con la información de entrada y salida. [11]*

- **Entornos visuales**:
    - **Diseñador de flujos de trabajo**: Permite la creación de múltiples escenarios de respuesta a incidentes, basados en procedimientos documentados y actualizables.

    - **Threat Sharing and Response Tasks Management & Tracking**: Facilita la comunicación y el intercambio de información entre equipos SOC, CSIRTs/CERTs y proveedores de infraestructura de IA y nube. Este entorno utiliza flujos de trabajo dinámicos y actualizables para responder a incidentes.

- **Backend robusto**:
    - **Motor de ejecución de flujos de trabajo**: Implementa los flujos de trabajo definidos, ejecutando intercambios de datos y solicitudes de comandos a los componentes.

    - **Motor de combinación de flujos de trabajo**: Combina procedimientos existentes con conocimientos expertos de plataformas como MeliCERTes para habilitar respuestas proactivas [11].

- **Marco de solicitudes de ejecución de comandos:** Basado en especificaciones OpenAPI, este marco gestiona las solicitudes de ejecución desde el orquestador hacia los componentes, automatizando procesos y compartiendo información.

- **Interfaz de usuario:** Ofrece un acceso intuitivo para gestionar flujos de trabajo, permitiendo tanto la ejecución predefinida como la personalización de respuestas según el contexto.

- **Interconexión con MeliCERTes:** Este módulo añade conocimientos especializados que mejoran la automatización de procesos iterativos, ahorrando tiempo en tareas repetitivas y garantizando una respuesta estandarizada y eficiente.

Aplicaciones en ciudades inteligentes

ATIO se ha diseñado específicamente para reducir los riesgos asociados con las ciudades inteligentes, donde la proliferación de dispositivos IoT y sistemas interconectados aumenta significativamente la superficie de ataque. La plataforma permite a los SOC gestionar eficazmente incidentes complejos al:

- Automatizar tareas repetitivas, liberando recursos para análisis más profundos.
- Mejorar la eficacia general de la respuesta mediante la integración de tecnologías avanzadas.
- Proporcionar una solución escalable y adaptable a medida que las amenazas evolucionan [11].

Impacto y beneficios

Este desarrollo representa un activo valioso para los que buscan fortalecer su postura de ciberseguridad y garantizar una respuesta rápida y eficaz ante incidentes. Su enfoque en la integración, automatización y estandarización de procesos contribuye a:

- Reducir el tiempo de respuesta: Al automatizar flujos de trabajo, los analistas pueden reaccionar más rápidamente ante amenazas emergentes.

- Optimizar recursos: La plataforma minimiza el tiempo y esfuerzo invertido en tareas rutinarias, maximizando la eficiencia operativa.

- Mejorar la colaboración: Facilita el intercambio de información y estrategias entre diferentes equipos, fortaleciendo el ecosistema de ciberseguridad [11].

Perspectivas futuras

Los desarrolladores de ATIO están trabajando en ampliar sus capacidades para abordar desafíos emergentes en ciberseguridad. Esto incluye el desarrollo de algoritmos más avanzados para la detección y mitigación de amenazas, así como la integración de nuevas tecnologías IoT y de inteligencia artificial para mantener la relevancia de la plataforma en un panorama de amenazas en constante evolución.

Para comprender más profundamente el funcionamiento y diseño de las plataformas SOAR, Islam, Babar y Nepal (2020) propusieron una metodología arquitectónica innovadora que aborda los desafíos asociados con la integración de herramientas de seguridad en estas plataformas. Esta propuesta se basa en un modelo centrado en la arquitectura, estructurado en capas, que permite gestionar eficientemente herramientas y procesos relacionados con la orquestación de seguridad. La investigación destaca atributos clave que deben poseer las plataformas SOAR: integralidad, interoperabilidad e interpretabilidad, elementos fundamentales para satisfacer las necesidades de seguridad de las organizaciones modernas [12].

Arquitectura por capas para plataformas SOAR

La arquitectura propuesta se divide en seis capas principales, cada una diseñada para abordar aspectos específicos de la integración y el funcionamiento de una plataforma SOAR:

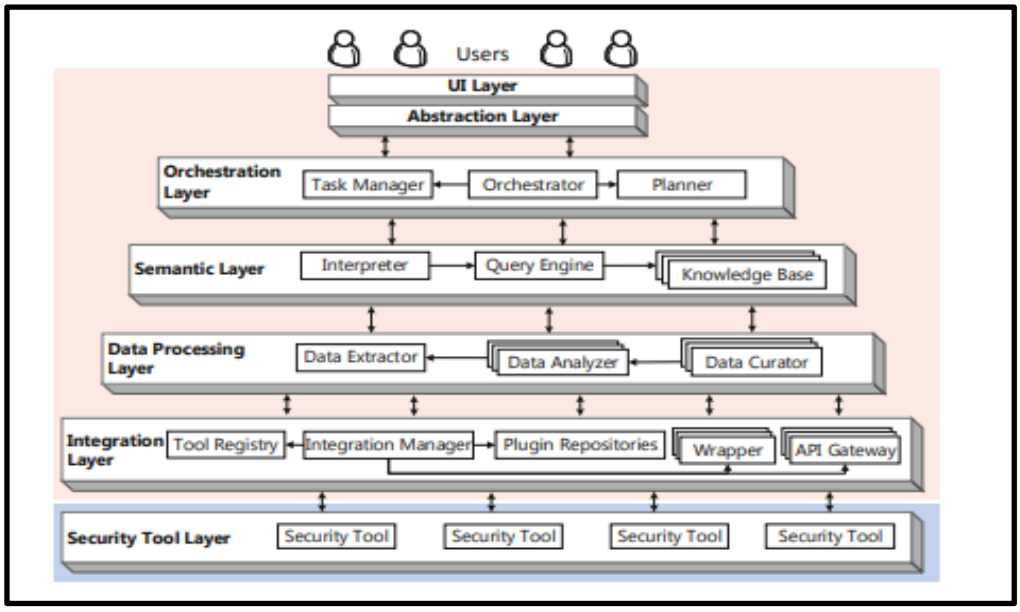


Fig. 10 *Arquitectura de alto nivel de la plataforma SOAR [12]*

- **Capa de Herramientas de Seguridad:**

Esta capa incluye herramientas esenciales para la detección, análisis y respuesta a incidentes de seguridad, como sistemas de detección de intrusos (IDS), herramientas de monitoreo de red, firewalls, y sistemas de prevención de intrusiones (IPS).

Estas herramientas son la primera línea de defensa en la identificación de amenazas.

- **Capa de Integración:**

Facilita la conexión de diversas herramientas de seguridad mediante el uso de APIs, complementos o módulos personalizados. Esta capa es crucial para garantizar la interoperabilidad entre sistemas heterogéneos, permitiendo que las herramientas trabajen de manera conjunta y coordinada.

- **Capa de Procesamiento de Datos:**

Se encarga de la recopilación, normalización y análisis de los datos de seguridad provenientes de múltiples fuentes. Esta capa transforma los datos brutos en información procesable, lo que permite una toma de decisiones más informada y rápida.

- **Capa Semántica:**

Proporciona un marco para interpretar y correlacionar los datos recopilados. Utiliza ontologías y modelos semánticos para dar sentido a la información, lo que facilita la identificación de patrones y la detección de amenazas complejas. Esta capa es fundamental para la interpretabilidad de los datos.

- **Capa de Distribución de Datos:**

Coordina la ejecución de planes de respuesta mediante playbooks, que son conjuntos de instrucciones automatizadas diseñadas para responder a incidentes específicos. Estos playbooks son desarrollados por equipos CERT y están adaptados a las necesidades y políticas de seguridad de cada organización.

- **Capa de Interfaz de Usuario:**

Ofrece un entorno interactivo donde el personal de seguridad puede gestionar y ejecutar los planes de respuesta a incidentes (IRP). Esta capa proporciona una interfaz intuitiva que permite a los usuarios monitorear, analizar y responder a

incidentes de manera eficiente, adaptándose a los requisitos y políticas de la organización.

- **Proceso de orquestación basado en playbooks**

El enfoque arquitectónico se basa en la ejecución de playbooks, que son conjuntos de instrucciones automatizadas diseñadas para responder a incidentes específicos. Estos playbooks son desarrollados por equipos CERT, adaptados a las necesidades de cada organización. Esta metodología asegura que las respuestas a incidentes sean coherentes y alineadas con las políticas de seguridad vigentes.

Implementación y prueba de concepto

La prueba de concepto (PoC) de esta arquitectura se diseñó para ser adaptable y escalable, demostrando la viabilidad de integrar múltiples herramientas de seguridad de código abierto. Las herramientas seleccionadas incluyeron Snort, Splunk, LimaCharlie, MISP, Windows Defender, Wireshark y WinPCap, elegidas por su capacidad para abordar diversos aspectos de la seguridad cibernética.

La integración se logró mediante APIs y un recopilador que canalizaba los datos hacia el orquestador a través de un intérprete semántico.

Este enfoque permitió a la plataforma:

- Interpretar automáticamente las actividades de seguridad.
- Ejecutar los IRP de manera eficiente en función de los objetivos del usuario y las herramientas disponibles.
- Reducir la complejidad operativa al formalizar el análisis y la respuesta [12].

Innovaciones clave

- **Ontologías semánticas**: Estas se desarrollaron para formalizar las herramientas y los IRP, facilitando la interpretación y correlación de datos de seguridad.
- **Adaptabilidad**: La arquitectura propuesta demostró ser capaz de adaptarse rápidamente a cambios en el entorno de seguridad, optimizando el uso de herramientas disponibles.
- **Automatización**: Se lograron altos niveles de automatización en la integración de herramientas y ejecución de respuestas, reduciendo la intervención manual y mejorando la eficiencia.

Limitaciones actuales y propuestas futuras

Los autores identificaron que muchas plataformas SOAR carecen de mecanismos de descomposición y un enfoque arquitectónico claro. Para abordar esto, propusieron una arquitectura en capas que separa los componentes críticos, mejorando el modularidad y la flexibilidad del sistema. Además, sugirieron la necesidad de:

- Explorar más a fondo el diseño arquitectónico de las plataformas SOAR.
- Ampliar la automatización del despliegue para reducir la complejidad de implementación.
- Desarrollar nuevas ontologías que mejoren la interoperabilidad entre herramientas de seguridad.

El trabajo de los autores establece un marco robusto para el diseño y despliegue de plataformas SOAR, destacando la importancia de un enfoque arquitectónico centrado en la integración y la automatización. Este enfoque no solo mejora la capacidad de respuesta ante incidentes, sino que también sienta las bases para futuras investigaciones en la evolución de plataformas SOAR más adaptativas y escalables, lo que las posiciona como herramientas esenciales para la ciberseguridad en entornos complejos y en constante cambio [12].

En 2024, Dwivedi et al y equipo presentaron IntelliSOAR, una plataforma avanzada diseñada para enriquecer alertas de seguridad utilizando un SOAR desarrollado internamente. Su trabajo, publicado en el contexto de la conferencia Information Systems Security (ICISS 2024), aborda la creciente necesidad de optimizar los procesos de gestión de alertas en entornos complejos. La investigación se centra en la implementación de un sistema que no solo mejora la eficiencia operativa en la gestión de incidentes, sino que también reduce significativamente los falsos positivos y mejora la correlación entre eventos de seguridad [13].

Propósito y contribuciones clave

La motivación principal detrás de IntelliSOAR es resolver problemas comunes en la gestión de alertas, como la falta de contexto, la sobrecarga de información y los falsos positivos. Se argumenta que los enfoques tradicionales en la gestión de incidentes a menudo carecen de un sistema inteligente que permita enriquecer las alertas con información relevante y procesable. A través de su arquitectura, IntelliSOAR aborda estas deficiencias proporcionando:

- Enriquecimiento automatizado de alertas: Mediante la integración de múltiples fuentes de datos, la plataforma contextualiza cada alerta, facilitando su clasificación y priorización.
- Correlación avanzada de eventos: Utiliza técnicas de aprendizaje automático y reglas de asociación para identificar patrones entre alertas aparentemente independientes.
- Optimización de recursos: Automatiza tareas repetitivas, permitiendo que los analistas de seguridad se concentren en incidentes críticos.

Arquitectura del sistema

La arquitectura de IntelliSOAR se estructura en varias capas interconectadas, diseñadas para maximizar la eficiencia y escalabilidad del sistema:

- Capa de recopilación de datos: Integra fuentes de datos internas y externas, como sistemas SIEM, bases de datos de inteligencia de amenazas y registros de aplicaciones. Esta capa actúa como la entrada principal para datos sin procesar.
- Capa de procesamiento y correlación: Utiliza algoritmos de aprendizaje automático para analizar los datos recopilados. Los modelos se entrenan para identificar relaciones entre eventos, detectando patrones sospechosos y reduciendo la probabilidad de falsos positivos.
- Capa de enriquecimiento: Proporciona contexto adicional a las alertas mediante la integración de información de bases de datos externas, como registros de vulnerabilidades conocidas y listas negras de direcciones IP maliciosas.
- Capa de orquestación: Coordina las respuestas automatizadas a las amenazas detectadas, ejecutando playbooks previamente definidos según las políticas de la organización.
- Capa de interfaz de usuario: Permite a los analistas visualizar alertas enriquecidas, acceder a informes detallados y realizar ajustes en tiempo real a los flujos de trabajo.

Innovaciones técnicas

Se destacan varias innovaciones que diferencian a IntelliSOAR de las plataformas tradicionales:

- **Integración modular**: La arquitectura admite la incorporación de nuevas herramientas y fuentes de datos sin necesidad de modificaciones significativas en el sistema.
- **Modelos de aprendizaje adaptativos**: Los algoritmos se actualizan dinámicamente en función de nuevas amenazas y patrones de ataque.
- **Reducción de falsos positivos**: Gracias al enriquecimiento de alertas y la correlación avanzada, la plataforma reduce la carga operativa asociada con la revisión de alertas irrelevantes.

Implementación y resultados

La plataforma fue probada en un entorno empresarial real, donde demostró ser eficaz en la reducción del tiempo de respuesta a incidentes y en la mejora de la precisión en la detección de amenazas. Los resultados incluyen:

- Reducción del 40% en falsos positivos: Gracias al contexto adicional proporcionado por la capa de enriquecimiento.
- Incremento del 30% en la eficiencia operativa: Debido a la automatización de tareas y la optimización de flujos de trabajo.
- Mejora en la correlación de eventos: Identificación de amenazas complejas que requerían múltiples pasos de análisis manual en sistemas tradicionales [13].

Relevancia y perspectivas futuras

La investigación establece un precedente importante en el desarrollo de plataformas SOAR inteligentes. IntelliSOAR no solo mejora las capacidades de respuesta a incidentes, sino que también establece un marco para futuras investigaciones en la integración de aprendizaje automático y enriquecimiento de alertas. Los autores sugieren que el próximo paso en el desarrollo de la plataforma incluirá:

- Mayor integración con tecnologías de inteligencia artificial: Como el procesamiento de lenguaje natural (NLP) para analizar contenido no estructurado.
- Escalabilidad mejorada: Adaptando la arquitectura para manejar mayores volúmenes de datos en entornos globales.
- Pruebas en dominios específicos: Como sectores de salud y finanzas, donde las alertas de seguridad suelen ser más complejas y críticas [13].

En 2022, Christian, Luis Paulino y Alan Oliveira de Sá presentan una solución innovadora para la orquestación, automatización y respuesta en seguridad (SOAR) basada en la nube, diseñada específicamente para ser de bajo costo, eficiente y escalable. Este trabajo destaca por su enfoque en resolver los desafíos asociados con las soluciones SOAR comerciales, cuyo alto costo y complejidad las hacen inaccesibles para muchas organizaciones. La propuesta se fundamenta en tecnologías nativas de la nube, reduciendo los costos operativos a menos de $65 USD por mes, mientras que soluciones comerciales comparables cuestan entre $10,000 y $40,000 USD mensuales [14].

Propósito y contribuciones clave

Los autores establecen que la solución propuesta busca cerrar la brecha entre la teoría y la práctica en el diseño de SOAR. A través de experimentos en un entorno empresarial real, demuestran que el sistema:

- Reduce la duración de tareas de seguridad en un 99.02% en promedio.
- Escala fácilmente para manejar más de 10,000 incidentes de seguridad al mes.
- Minimiza los costos de operación mediante tecnologías de pago por uso.

Estas contribuciones hacen que la solución sea accesible para organizaciones con recursos limitados, sin comprometer la efectividad [14].

Arquitectura del sistema

La arquitectura de la solución se basa en un modelo modular, diseñado para garantizar la interoperabilidad y escalabilidad. Sus componentes principales incluyen:

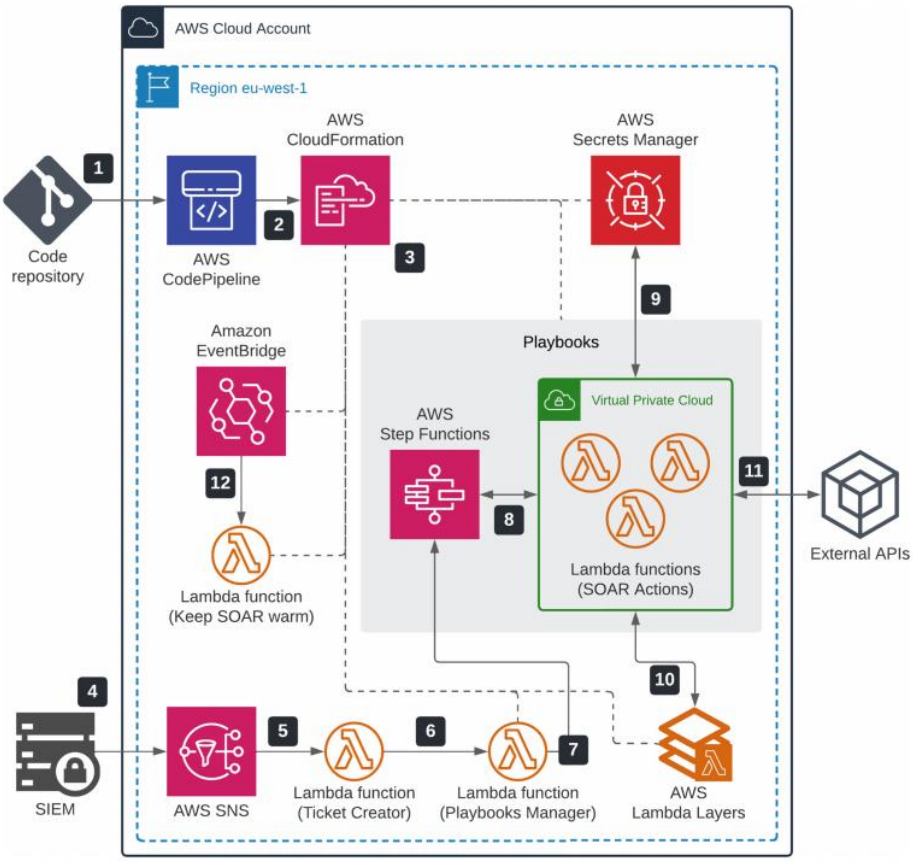


Fig. 11 *Arquitectura de alto nivel de la plataforma SOAR [14]*

La arquitectura se divide en componentes que garantizan escalabilidad, seguridad y eficiencia:

- **Repositorio de código**: Gestionado en GitHub Cloud, asegura el control de versiones y la automatización de despliegues.
- **Integración con SIEM**: Compatible con plataformas como Splunk Cloud, permite recibir datos de incidentes de seguridad en tiempo real.
- **Capa de automatización**: Construida con AWS Lambda y AWS Step Functions, ejecuta playbooks automatizados que responden a incidentes específicos.
- **Gestión de secretos**: AWS Secrets Manager asegura credenciales y datos sensibles tanto en tránsito como en reposo.
- **Escalabilidad dinámica**: Utiliza servicios sin servidor como AWS Lambda para garantizar que los recursos sean escalados según la demanda.

Innovaciones técnicas

La solución propuesta incluye varias innovaciones técnicas que la diferencian de las plataformas tradicionales:

- Uso de servicios nativos en la nube: La arquitectura aprovecha tecnologías como Amazon Web Services (AWS), Google Cloud Platform (GCP) y Azure, lo que reduce significativamente la necesidad de infraestructura local.
- Automatización de playbooks: Los flujos de trabajo predefinidos están diseñados para ejecutarse con precisión y rapidez, reduciendo los tiempos de respuesta hasta en un 60% en comparación con sistemas tradicionales.
- Capacidades de integración ampliadas: Mediante APIs y contenedores, la solución se adapta fácilmente a herramientas de terceros, como Splunk, Wazuh y VirusTotal.

Resultados y estadísticas

El sistema fue probado en una empresa multinacional, mostrando resultados altamente positivos:

- **Reducción drástica en tiempos de respuesta**: Por ejemplo, una tarea que manualmente tomaba 900 segundos fue automatizada a solo 8 segundos.
- Ahorro significativo de tiempo: 4,550 minutos de tareas manuales fueron reducidos a solo 31.2 minutos gracias al SOAR.
- Reducción de costos operativos: Menos de $65 USD mensuales en comparación con los $10,000 USD de soluciones comerciales.
- Estabilidad y confiabilidad: Incluso en escenarios de alta demanda, la arquitectura soportó más de 10,000 incidentes mensuales con alta eficiencia [14].

Estadísticas clave

Durante las pruebas, el sistema gestionó 363 incidentes de seguridad y más de 9,000 procesos de inteligencia de amenazas, logrando:

- Ahorros operativos: 99% menos tiempo por tarea.
- Velocidad incrementada: Las respuestas automatizadas fueron más de 10 veces más rápidas que las manuales.
- Reducción de errores humanos: La ejecución automatizada eliminó fallos comunes en procesos manuales [14].

Perspectivas futuras

Se identifican áreas clave para la evolución de la plataforma, incluyendo:

- Transición a herramientas independientes de proveedores: Adoptar soluciones como Terraform o Ansible para evitar dependencia de un único proveedor de nube.
- Ampliación de capacidades de IA: Integrar aprendizaje automático avanzado para mejorar la detección de amenazas y el análisis predictivo.
- Aplicaciones ampliadas: Probar el sistema en sectores críticos como salud, finanzas y gobiernos [14].

Conclusión

La propuesta establece un modelo asequible y eficaz para la implementación de SOAR en organizaciones con recursos limitados. Su enfoque en tecnologías nativas en la nube, combinado con innovaciones en automatización y análisis, ofrece una solución robusta que responde a las necesidades actuales de ciberseguridad. Este trabajo marca un avance significativo en la democratización de las plataformas SOAR, haciendo accesibles sus beneficios a un mayor número de organizaciones [14].

1.3 Objetivo Generales y Específicos del Proyecto.

General

El objetivo de esta tesis es abordar las principales necesidades que en la práctica de respuesta a eventos/incidentes de ciberseguridad surgen de manera rudimentaria, explorando el uso de The Hive Project, una plataforma de automatización en el contexto de un laboratorio diseñado para mejorar los procesos de un SOC.

Específicos

- Automatización: Utilizar herramientas de automatización para ayudar a los especialistas a clasificar y responder eficazmente a los incidentes, aunado al ahorro de tiempo y mejora de la calidad.

- Integración: Utilizar la orquestación para reunir varias plataformas y proporcionar un proceso de respuesta a incidentes racionalizado basado en los playbooks más utilizados dentro de la industria.

- Visualización de datos: Proporcionar una interfaz visual para que los especialistas comprendan fácilmente el alcance y el impacto de los incidentes, integrando diversas tecnologías y fuentes de datos para obtener una visión más completa de los casos a los cuales se brinda atención.

Capítulo 2.- Marco Teórico

2.1 Ciberseguridad

La ciberseguridad es la disciplina que abarca estrategias, tecnologías y procesos diseñados para proteger sistemas, redes, dispositivos y datos frente a accesos no autorizados, daños, robos o interrupciones malintencionadas. Este campo busca garantizar la confidencialidad, integridad y disponibilidad de la información, adaptándose constantemente a las nuevas amenazas que emergen en el entorno digital.

El Instituto Nacional de Normas y Tecnología (NIST) define la ciberseguridad como "la capacidad de proteger y defender el uso de los sistemas cibernéticos frente a ciberataques". Esta definición subraya la importancia de implementar controles robustos en todos los niveles tecnológicos para prevenir y mitigar riesgos [15]. Por su parte, la Unión Internacional de Telecomunicaciones (UIT) la describe como "un conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos contra ciberataques". Esto refleja la necesidad de combinar medidas técnicas con políticas organizacionales para mantener un entorno cibernético seguro [16].

La Cybersecurity and Infrastructure Security Agency (CISA) define la ciberseguridad como " La ciberseguridad es el arte de proteger redes, dispositivos y datos de accesos no autorizados o usos delictivos y la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información.". Esta definición destaca el enfoque integral requerido para garantizar la resiliencia frente a ciber amenazas [17].

El Departamento de Seguridad Nacional de Estados Unidos (DHS) añade que la ciberseguridad involucra herramientas, políticas, conceptos de seguridad, salvaguardas y mejores prácticas diseñadas para proteger el entorno cibernético y los activos digitales de las organizaciones, asegurando su continuidad operativa y minimizando los impactos ante incidentes [18].

La ciberseguridad es una preocupación fundamental para particulares, empresas y gobiernos, dada la creciente frecuencia y sofisticación de los ciberataques. Estos ataques pueden provocar pérdidas financieras, robo de propiedad intelectual, daños a la reputación e incluso daños físicos en algunos casos. El proteger a los activos de una forma eficaz requiere un enfoque a varios niveles que incluya una combinación de medidas técnicas, de procedimiento y humanas. Esto puede incluir el uso de cortafuegos, software antivirus, sistemas de detección de intrusos, encriptación, controles de acceso y otras tecnologías de seguridad para proteger los sistemas y los datos de accesos y ataques no autorizados. Además de las medidas técnicas, la ciberseguridad también implica el desarrollo y aplicación de políticas de seguridad, procedimientos y programas de formación para garantizar que los empleados y otros usuarios de sistemas electrónicos y datos sean conscientes de los riesgos potenciales y tomen las medidas adecuadas para proteger la información sensible. Es un campo en constante evolución, ya que las ciber amenazas y las técnicas de ataque siguen evolucionando y volviéndose más sofisticadas.

2.1.1 Confidencialidad

La confidencialidad es un principio fundamental de la seguridad de la información que asegura la protección de datos sensibles frente al acceso, divulgación o exposición no autorizados. Este concepto garantiza que únicamente las personas, sistemas o procesos autorizados puedan acceder a la información, preservando su privacidad y evitando su uso indebido.

De acuerdo con el NIST, la confidencialidad se define como "la preservación de las restricciones autorizadas al acceso y divulgación de la información, incluidos los medios para proteger la privacidad personal y la información propietaria". Este enfoque subraya la importancia de implementar controles que limiten el acceso y aseguren el manejo adecuado de los datos confidenciales [19].

En una definición complementaria, la Organización Internacional de Normalización (ISO) describe la confidencialidad como "la propiedad de que la información no esté disponible ni se revele a personas, entidades o procesos no autorizados". Esta definición, contenida en el estándar ISO/IEC 27001, refuerza la necesidad de controles técnicos y organizacionales para prevenir accesos no autorizados y proteger la integridad de los datos sensibles [20].

Por su parte, en el libro Computer Security: Principles and Practice, William Stallings y Lawrie Brown definen la confidencialidad como "la garantía de que la información no se revela a individuos, procesos o dispositivos no autorizados". Este enfoque enfatiza la protección activa contra amenazas internas y externas, destacando que la confidencialidad no solo protege la información en reposo, sino también durante su transmisión [21].

En resumen, la confidencialidad es un pilar esencial en la seguridad de la información, garantizando que los datos permanezcan seguros y accesibles únicamente para quienes tienen autorización. Este principio se aplica en múltiples contextos, desde la

protección de datos personales y empresariales hasta la seguridad de sistemas críticos y comunicaciones sensibles.

2.1.2 Integridad

La integridad es un principio clave en ciberseguridad que se refiere a la protección de los datos frente a modificaciones no autorizadas, borrado o corrupción, asegurando que los mismos permanezcan precisos, completos y confiables. Este principio garantiza que cualquier cambio realizado en los datos esté autorizado, sea legítimo y pueda ser verificado.

El NIST define la integridad como "la protección contra la modificación o destrucción indebida de la información, e incluye garantizar el no repudio y la autenticidad de la información". Esta definición pone de manifiesto la importancia de preservar no solo el contenido, sino también la legitimidad de las transacciones y el origen de la información [22].

Desde otra perspectiva, el (CISA, por sus siglas en inglés) define la integridad como la protección contra la modificación o destrucción no autorizada de información, asegurando que los datos sean confiables y precisos. Esto implica salvaguardar la información contra alteraciones accidentales o malintencionadas, garantizando que refleje fielmente la realidad a la que está asociada. Por ejemplo, en su "Guía para el reporte de vulnerabilidades para los administradores electorales de las Américas", CISA señala que las vulnerabilidades pueden comprometer la confidencialidad, integridad o disponibilidad de la información, enfatizando la importancia de mantener la integridad de los datos para asegurar su confiabilidad y precisión [23].

En su obra Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson define la integridad como "la propiedad de que los datos no han sido alterados o destruidos de forma no autorizada". Anderson destaca la importancia de combinar controles técnicos, como firmas digitales y sumas de comprobación, con medidas organizativas para proteger los datos en entornos distribuidos. Por ejemplo, en el Capítulo 5, "Cryptography", Anderson analiza cómo las firmas digitales y las sumas de comprobación se utilizan para garantizar la integridad de los datos, y en el

Capítulo 6, "Distributed Systems", enfatiza la necesidad de implementar medidas organizativas junto con controles técnicos para proteger la integridad de la información en sistemas distribuidos. [24]

Técnicas de protección de la integridad

Para garantizar la integridad, se emplean diversas técnicas y controles, entre los que destacan:

1. **Sumas de comprobación y códigos hash:** Estas herramientas permiten detectar cambios no autorizados en los datos al comparar valores calculados antes y después de una operación.

2. **Firmas digitales:** Aseguran la autenticidad e integridad de los datos mediante algoritmos criptográficos que verifican la identidad del emisor y la integridad del contenido.

3. **Controles de acceso:** Limitan quién puede modificar los datos, asegurando que solo los usuarios o sistemas autorizados tengan los permisos necesarios.

4. **Auditorías y registros:** Documentan todas las modificaciones realizadas en los datos, lo que facilita la identificación de alteraciones no autorizadas y permite realizar un análisis forense en caso de incidentes.

2.1.3 Disponibilidad

La disponibilidad es un principio fundamental de la ciberseguridad que asegura que los sistemas, datos y servicios sean accesibles y utilizables por los usuarios autorizados en el momento en que se necesiten. Este concepto busca garantizar que los recursos críticos permanezcan operativos y protegidos contra interrupciones, ya sean causadas por fallos internos o ataques externos, como los de denegación de servicio (DoS) y distribución de denegación de servicio (DDoS).

Según el NIST, la disponibilidad se define como "garantizar el acceso oportuno y fiable a la información y su uso". Este enfoque destaca la importancia de mantener la continuidad operativa y minimizar las interrupciones en los sistemas digitales [25].

Por su parte, la ISO describe la disponibilidad como "la propiedad de que los datos sean accesibles y los servicios estén disponibles cuando se necesiten". Esta definición enfatiza que tanto los datos como los servicios deben estar diseñados para resistir fallos y responder rápidamente a las necesidades de los usuarios [20].

En el libro Computer Security: Principles and Practice, Stallings y Brown definen la disponibilidad como "la propiedad de que un sistema o servicio esté operativo y accesible para los usuarios autorizados cuando sea necesario". Este enfoque resalta la necesidad de implementar medidas técnicas y organizativas que aseguren la resiliencia de los sistemas frente a interrupciones inesperadas [21].

Técnicas para garantizar la disponibilidad

La disponibilidad suele lograrse mediante la implementación de diversas estrategias y tecnologías:

- Sistemas redundantes y tolerancia a fallos: Incluyen hardware, software y redes diseñados para mantener la operatividad incluso ante fallos críticos.
- Copias de seguridad y recuperación ante desastres: Garantizan la restauración de los datos y servicios tras incidentes, como ataques o fallos del sistema.
- Conmutación por error: Permite redirigir automáticamente las operaciones a sistemas alternativos en caso de interrupciones.
- Protección contra DoS y DDoS: Utiliza medidas como firewalls avanzados, sistemas de mitigación de tráfico y herramientas de monitorización en tiempo real para detectar y contrarrestar estos ataques.

2.1.4 Amenaza

Las amenazas a la ciberseguridad representan riesgos potenciales que pueden comprometer la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos sensibles. Estas amenazas pueden tomar múltiples formas, desde ataques sofisticados basados en malware y ransomware hasta tácticas como el phishing, ciber espionaje y ataques de denegación de servicio (DoS). A menudo, explotan vulnerabilidades en hardware, software o configuraciones de red para causar daños financieros, reputacionales o funcionales.

Según el NIST, las amenazas en ciberseguridad son "eventos o sucesos potenciales que pueden causar daños a los sistemas informáticos, redes y datos". Estas amenazas pueden originarse desde múltiples fuentes, como piratas informáticos, empleados malintencionados, grupos criminales, actores estatales y activistas.

Además, el NIST enfatiza que dichas amenazas no solo tienen el potencial de explotar vulnerabilidades técnicas, sino también humanas y organizativas [26].

Por su parte, el CISA clasifica las amenazas cibernéticas en cuatro categorías principales:

- Ciberataques: Acciones deliberadas que buscan comprometer la seguridad de sistemas y datos.
- Ciber espionaje: Actividades orientadas a robar información sensible con fines políticos, económicos o militares.
- Ciberdelincuencia: Delitos como fraude, extorsión y robo de identidad mediante el uso de sistemas informáticos.
- Ciberterrorismo: Uso de tecnologías digitales para llevar a cabo actos de terrorismo, como ataques a infraestructuras críticas [27].

La Agencia de Ciberseguridad de la Unión Europea (ENISA) añade una perspectiva detallada al clasificar las amenazas en tres categorías principales:

- Ingeniería social: Implica manipular a individuos para obtener acceso a sistemas o datos, mediante técnicas como phishing o pretexting.
- Amenazas basadas en redes: Incluyen el uso de malware, ransomware y explotación de vulnerabilidades en sistemas y aplicaciones.
- Amenazas físicas: Comprenden accesos no autorizados al hardware, manipulación de dispositivos y sabotajes [28].

2.1.5 Vulnerabilidad

Una vulnerabilidad en ciberseguridad es una debilidad, defecto o falla en sistemas informáticos, redes, software o procedimientos que puede ser explotada por atacantes para comprometer la confidencialidad, integridad o disponibilidad de los datos y sistemas. Estas vulnerabilidades pueden originarse a partir de fallos de diseño, errores de codificación, configuraciones incorrectas o deficiencias en los controles de seguridad, creando riesgos significativos.

El NIST define la vulnerabilidad como "una debilidad en un sistema de información, procedimientos de seguridad, controles internos o implementación que podría ser explotada para comprometer la seguridad de un sistema o sus datos" [29]. De manera similar, la ISO describe la vulnerabilidad como "una debilidad en el sistema o su implementación que podría ser aprovechada por atacantes para violar los objetivos de seguridad de confidencialidad, integridad y disponibilidad" [20].

Clasificación y Evaluación de Vulnerabilidades

El Common Vulnerability Scoring System (CVSS) proporciona un marco estándar para evaluar la severidad de las vulnerabilidades de ciberseguridad. Este sistema considera factores como:

- **Vector de ataque**: Ruta por la cual un atacante puede explotar la vulnerabilidad.
- **Complejidad del ataque**: Nivel de habilidad requerido para explotar el fallo.

- **Impacto**: Consecuencias en la confidencialidad, integridad y disponibilidad de los sistemas afectados [30].

Además, el Open Web Application Security Project (OWASP) identifica vulnerabilidades específicas en aplicaciones web, incluyendo:

- **Fallos de inyección**: Como SQL Injection, que permite manipular bases de datos.
- **Problemas de autenticación y gestión de sesiones rotas**: Que permiten accesos no autorizados.
- **Cross-site scripting (XSS)**: Que posibilita la ejecución de scripts maliciosos en el navegador de un usuario.
- **Errores de configuración de seguridad**: Que dejan sistemas abiertos a ataques [31].

Niveles de Vulnerabilidades

Las vulnerabilidades pueden existir en diferentes niveles del ecosistema digital:

- **Hardware**: Fallos en dispositivos o componentes que facilitan accesos no autorizados.
- **Software**: Errores de codificación o falta de actualizaciones que dejan sistemas expuestos.
- **Redes**: Configuraciones incorrectas o falta de cifrado en las comunicaciones.
- **Humanos**: Errores humanos, como contraseñas débiles o falta de capacitación, que abren puertas a los atacantes.

Importancia de la Gestión de Vulnerabilidades

Para mitigar el impacto de estas debilidades, los equipos de administración de vulnerabilidades deben adoptar un enfoque proactivo que incluya:

- **Evaluaciones periódicas de vulnerabilidades**: Utilizando herramientas como escáneres de seguridad y auditorías externas.
- **Actualizaciones y parches**: Que solucionen errores conocidos antes de que

puedan ser explotados.

- **Formación del personal**: Para reducir los errores humanos y reforzar las mejores prácticas de seguridad.
- **Pruebas de penetración**: Simulaciones de ataques reales para identificar debilidades antes que los atacantes.

2.1.6 Evento en ciberseguridad

Un evento de seguridad es cualquier suceso observable en un sistema o red que podría tener implicaciones para la seguridad o requerir análisis adicional. Estos eventos pueden incluir intentos de acceso no autorizado, cambios en configuraciones del sistema, introducción de nuevo software o hardware, y otras actividades que podrían indicar posibles amenazas o anomalías. Los eventos de seguridad representan la base para la detección y gestión de incidentes cibernéticos.

Según el NIST, un evento de seguridad es "una ocurrencia en un sistema de información o red que indica una posible violación de las políticas de seguridad, procedimientos o políticas de uso aceptable". Por su parte, la ISO lo define como "un suceso o cambio de un conjunto particular de circunstancias que puede ser detectado, registrado y analizado". Estas definiciones subrayan la importancia de identificar, registrar y responder de manera efectiva a eventos que puedan comprometer los sistemas informáticos y los datos críticos [32] [20].

Formato Común de Eventos (CEF)

El Formato Común de Eventos (CEF) es un estándar ampliamente adoptado para registrar eventos de seguridad de manera consistente e interoperable. Este formato permite la captura de información relevante en registros estructurados, facilitando su análisis en herramientas como SIEM.

Un ejemplo de nomenclatura de CEF:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Fig. 12 *Nomenclatura del Formato Común de Eventos. [33].*

Un ejemplo práctico proporcionado por Trend Micro Deep Security Manager:

En este registro:

```
CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|User
Signed In|3|src=10.52.116.160 suser=admin target=admin
msg=User signed in from 2001:db8::5
```

Fig. 13 *Ejemplo de registro de sistema utilizando CEF de la empresa Trend Micro. [33]*

- CEF:0 indica la versión del formato.
- Trend Micro es el proveedor del dispositivo.
- Deep Security Manager es el producto.
- 600 es el ID de la firma.
- User Signed In describe el evento.
- denota la severidad (moderada).
- src y suser identifican la IP de origen y el usuario respectivamente.

Clasificación y Gestión de Eventos

De acuerdo con la Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información, elaborada por el gobierno de Colombia [34]. Los eventos de seguridad pueden clasificarse en función de:

1. Según su impacto

- **Eventos informativos**: No representan una amenaza, pero pueden ser indicativos de un posible incidente (ej., inicios de sesión exitosos, escaneos de red legítimos).
- **Eventos de advertencia**: Indican una actividad inusual que podría convertirse en un incidente (ej., múltiples intentos fallidos de autenticación).
- **Eventos críticos**: Representan una amenaza confirmada con impacto en la seguridad de la organización (ej., una brecha de datos o la ejecución de malware).

2. Según su origen

- **Eventos internos**: Generados dentro de la organización (ej., empleados accediendo a datos no autorizados).
- **Eventos externos**: Provenientes de fuentes externas (ej., ataques de phishing, intentos de intrusión desde direcciones IP desconocidas).
- **Eventos híbridos**: Involucran tanto fuentes internas como externas (ej., ataque de malware iniciado por un empleado mediante un archivo descargado).

3. Según el tipo de amenaza

- **Acceso no autorizado**: Intentos de ingreso sin permisos a sistemas o datos.
- **Ataques de malware**: Eventos relacionados con virus, troyanos, ransomware, etc.
- **Ataques de denegación de servicio (DoS/DDoS)**: Actividades que buscan afectar la disponibilidad de un servicio.
- **Exfiltración de datos**: Transferencia no autorizada de información sensible.
- **Modificación de datos**: Alteración maliciosa de información sin autorización.
- **Uso indebido de privilegios**: Actividades de usuarios con acceso legítimo, pero que abusan de sus permisos.

4. Según la fuente de detección

- Eventos de red: Detectados a través de herramientas como IDS/IPS o firewalls.
- Eventos de endpoint: Generados por sistemas de seguridad en dispositivos finales (ej., antivirus, EDR).
- Eventos de aplicación: Relacionados con accesos indebidos o vulnerabilidades en software.
- Eventos de sistema: Logs de sistemas operativos y bases de datos que indican actividad sospechosa. **Gravedad**: Impacto potencial en los sistemas.

4. Tipo de resolución

En adición, el NIST en su guía para los Sistemas de Detección y Prevención (IDPS, por sus siglas en inglés) establece las características que debe cumplir un evento de seguridad según el tipo de resolución [35]:

- **Verdadero Positivo (True Positive)**: Una alerta que indica correctamente la presencia de una actividad maliciosa o una vulnerabilidad real. Por ejemplo, la detección de un malware activo en un sistema que realmente está comprometido.

- **Falso Positivo (False Positive)**: Una alerta que señala una actividad como maliciosa cuando, en realidad, es legítima. Esto puede llevar a una asignación innecesaria de recursos para investigar eventos que no representan una amenaza real.

- **Verdadero Negativo (True Negative)**: La ausencia de una alerta cuando no hay actividad maliciosa presente. Indica que el sistema de detección funciona correctamente al no generar alertas innecesarias.
- **Falso Negativo (False Negative)**: La falta de una alerta cuando hay una actividad maliciosa real. Este es el escenario más peligroso, ya que una amenaza pasa desapercibida y puede causar daños sin ser detectada.

Estas clasificaciones son esenciales para evaluar la eficacia de los sistemas de detección de intrusiones y otras herramientas de seguridad. Una alta tasa de falsos positivos puede llevar a la "fatiga de alertas", donde los analistas pueden pasar por alto amenazas reales debido al volumen de alertas no relevantes. Por otro lado, los falsos negativos representan riesgos significativos, ya que las amenazas no detectadas pueden comprometer la seguridad de la organización.

2.1.7 Incidente de ciberseguridad

Un incidente de ciberseguridad es cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los datos, sistemas o redes de información. Según el NIST, un incidente es definido como "una violación o amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar" [36]. Por su parte, la norma ISO/IEC 27035-1:2016 lo describe como "un evento de seguridad de la información único o una serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocio" [37].

Los incidentes pueden ser causados por una variedad de factores, como errores humanos, fallos en configuraciones, vulnerabilidades en el software, malware y ataques externos. Entre sus posibles consecuencias se incluyen pérdida o robo de datos, interrupción del servicio, daños a la reputación y pérdidas económicas significativas.

La gestión y respuesta a incidentes es un proceso crítico que busca minimizar su impacto y prevenir futuros incidentes. Este proceso abarca varias etapas, incluyendo la detección, contención, análisis, erradicación, recuperación y aprendizaje posterior.

Una respuesta adecuada no solo reduce los daños inmediatos, sino que también fortalece la postura de seguridad de la organización [38].

Para estar preparados, se debe implementar un plan integral de respuesta a incidentes que incluya políticas claras, procedimientos bien definidos y herramientas adecuadas. Este plan debe detallar las funciones y responsabilidades de los equipos, los canales de comunicación y los protocolos de escalado. La preparación y ejecución eficaz de estos planes permite reducir el tiempo de respuesta y mitigar las repercusiones adversas de los incidentes en las operaciones críticas.

2.2 Actores

Los actores en ciberseguridad son individuos, grupos u organizaciones con la capacidad de lanzar ataques o explotar vulnerabilidades en un sistema de información. Estos actores pueden representar una amenaza significativa para la seguridad de los activos digitales y ocasionar pérdidas financieras, operativas y reputacionales. Comprender sus características y motivaciones es clave para mitigar riesgos y mejorar la postura de seguridad organizacional.

A continuación, se describen los principales tipos de actores, sus atributos y su impacto potencial en la seguridad de una organización.

2.2.1 Amenazas Persistentes Avanzadas (APT)

Las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés) son actores altamente sofisticados que emplean tácticas avanzadas para infiltrarse en redes y sistemas con el fin de llevar a cabo espionaje, robo de datos o sabotaje. Se caracterizan por su capacidad de operar de manera encubierta durante largos períodos sin ser detectadas.

A menudo, están patrocinadas por estados y pueden contar con vastos recursos financieros y técnicos [39].

Las APT suelen utilizar métodos como spear-phishing, exploits de día cero, movimientos laterales en redes, y escalamiento de privilegios. Ejemplos notorios incluyen el grupo APT29 (Cozy Bear) asociado con Rusia y APT41, vinculado con China, ambos documentados por la comunidad de inteligencia de ciberseguridad [40].

2.2.2 Amenazas Internas

Las amenazas internas provienen de individuos con acceso autorizado a sistemas, datos y redes dentro de una organización. Estas amenazas pueden ser accidentales (errores humanos, configuraciones incorrectas) o intencionadas (empleados descontentos, excolaboradores, espías corporativos).

Las motivaciones más comunes incluyen beneficios económicos, venganza, ideología o negligencia. Según el informe Verizon Data Breach Investigations Report (DBIR) 2023, más del 30% de las brechas de seguridad involucran a actores internos [41].

Ejemplos de amenazas internas incluyen:

- Robo de datos por empleados con acceso legítimo.
- Fugas accidentales de información sensible.
- Uso indebido de privilegios por parte de insiders malintencionados.
- Medidas como la implementación de Zero Trust Architecture (ZTA) y monitoreo continuo pueden ayudar a mitigar estas amenazas [42].

2.2.3 Script Kiddies

Los script kiddies son actores con habilidades técnicas limitadas que utilizan herramientas preexistentes para ejecutar ataques sin un conocimiento profundo de cómo funcionan. Generalmente, descargan software malicioso de foros en la dark web y realizan ataques de fuerza bruta, defacement de sitios web o denegación de servicio (DoS).

A pesar de su falta de sofisticación, pueden representar una amenaza significativa, ya que pueden explotar vulnerabilidades en sistemas desactualizados o mal configurados [43].

2.2.4 Grupos Cibercriminales

Los grupos de cibercriminales operan con el objetivo principal de obtener beneficios económicos. Estos actores pueden estar involucrados en actividades como fraude financiero, estafas en línea, robo de credenciales, distribución de ransomware y ataques a infraestructura crítica.

Ejemplos de grupos criminales incluyen:

- REvil y Conti (ransomware-as-a-service).
- Carbanak (ataques a bancos y cajeros automáticos).

- FIN7 (fraude con tarjetas de crédito).
- Estos grupos suelen operar en la deep web, vendiendo datos robados y herramientas de hacking en mercados clandestinos [44].

2.2.5 Hackers: Autorizados, No Autorizados y Semi-autorizados

Los hackers pueden clasificarse en tres categorías principales:

- Hackers autorizados (White Hat): Profesionales de seguridad que realizan pruebas de penetración y auditorías para mejorar la seguridad organizacional.

- Hackers no autorizados (Black Hat): Individuos que explotan vulnerabilidades con fines maliciosos, como robo de datos, espionaje o sabotaje.

- Hackers semi-autorizados (Gray Hat): Expertos que encuentran y explotan fallos de seguridad sin permiso, aunque no siempre con intenciones maliciosas.

- Los hackers éticos certificados, como los Certified Ethical Hackers (CEH), desempeñan un papel clave en la protección contra ciberataques [45].

2.2.6 Shadow IT

El término Shadow IT se refiere al uso no autorizado de software, hardware o servicios en la infraestructura de una organización. Este fenómeno ocurre cuando empleados o departamentos implementan herramientas sin aprobación del área de TI, lo que puede generar vulnerabilidades y riesgos de fuga de datos [46].

Ejemplos de Shadow IT incluyen:

- Uso de aplicaciones de almacenamiento en la nube no aprobadas (Dropbox, Google Drive).

- Implementación de software de comunicación no controlado (WhatsApp, Telegram).
- Conexión de dispositivos personales a redes corporativas sin controles de seguridad.

Para mitigar este riesgo, se deben establecer políticas claras de uso de tecnologías y reforzar la supervisión mediante soluciones de Cloud Access Security Broker (CASB) [47].

2.2.7 Competidores como Amenaza

Los competidores también pueden representar una amenaza a la ciberseguridad de una organización. A través de espionaje industrial o ataques dirigidos, pueden intentar obtener propiedad intelectual o información estratégica. Algunas tácticas utilizadas incluyen:

- Ingeniería social para obtener información confidencial.
- Explotación de vulnerabilidades en sistemas de la competencia.
- Ataques de denegación de servicio para afectar la disponibilidad de servicios.

El espionaje corporativo es una preocupación creciente en sectores altamente competitivos como la tecnología, la biotecnología y las telecomunicaciones [48].

Conclusión

Los actores de ciberseguridad tienen distintos niveles de intención, sofisticación, recursos y capacidades. Pueden ser internos o externos y variar desde individuos con conocimientos limitados hasta grupos patrocinados por estados. Para fortalecer la defensa contra estas amenazas, sobre las cuales se deben adoptar estrategias basadas en detección temprana, monitoreo proactivo y respuesta a incidentes, alineadas con marcos como NIST Cybersecurity Framework, ISO/IEC 27001 y MITRE ATT&CK.

2.3 Controles de seguridad

Los controles de ciberseguridad son un aspecto crítico de la protección de los activos y datos digitales de una organización. Estos controles se dividen en tres categorías principales: de gestión, operativos y técnicos. Dentro de estas categorías, se pueden implementar varios tipos de controles para prevenir, detectar, corregir o compensar incidentes de seguridad. Además, algunos controles pueden ser de naturaleza disuasoria o física.

Los controles de gestión están diseñados para proporcionar orientación y dirección general al programa de seguridad de una organización. Estos controles incluyen políticas, procedimientos y directrices.

- Los preventivos pueden incluir programas de formación y concienciación, su objetivo es evitar que se produzca una violación de la seguridad. Algunos ejemplos son:
    - El control de acceso (que limita el acceso a datos sensibles)
    - Los programas de formación y concienciación en materia de seguridad.

- Los correctivos se aplican para mitigar el impacto de un incidente de seguridad que ya se ha producido. Algunos ejemplos son:
    - Restauración de datos a partir de copias de seguridad
    - El parcheado de vulnerabilidades de software

- Los controles operativos se aplican para garantizar que las actividades cotidianas de seguridad se realizan correcta y eficazmente. Ejemplos de controles operativos son el control de acceso y la gestión de cambios.

- Los controles técnicos se utilizan para proteger los activos digitales y los datos del acceso no autorizado, el robo o la destrucción. Estos controles pueden incluir cortafuegos, cifrado o sistemas de detección de intrusos.

- Los controles de detección están diseñados para identificar los incidentes de

seguridad en el momento en que se producen. Algunos ejemplos son:

- Los sistemas de detección de intrusos
- La supervisión continua de la seguridad.

- Los disuasorios están diseñados, valga la redundancia, para disuadir a los atacantes potenciales de entrar los sistemas y datos de una organización. Ejemplos:
  - Son la señalización de seguridad
  - Las cámaras de seguridad visibles
  - Las patrullas de seguridad

- Los controles compensatorios se aplican cuando un control no puede aplicarse debido a limitaciones técnicas o prácticas.

- Los controles físicos son tan claros como los torniquetes o los controles de acceso biométricos, que están diseñados para restringir físicamente el acceso a las instalaciones de una organización.

Diferentes autores hacen hincapié en la importancia de cada tipo de control, dependiendo de las necesidades de la organización y del tipo de amenaza a la que se enfrente. Por tanto, implementar un conjunto completo de controles de ciberseguridad que cubran todas las categorías y tipos de controles es crucial para proteger los activos y datos digitales de una organización. La elección de los controles dependerá de las necesidades de la organización, del tipo de amenaza a la que se enfrente y de los recursos disponibles [49].

2.4 Tipos de Ataques

Los ciberataques han evolucionado significativamente en los últimos años, abarcando no solo amenazas tradicionales como el malware, sino también explotando vulnerabilidades en áreas críticas como la identidad, la nube y los endpoints. A continuación, se presenta una visión ampliada de los tipos de ataques, incluyendo sus características actuales.

Malware Tradicional y Avanzado

El malware sigue siendo una de las principales amenazas, con variantes como el ransomware, que cifra los datos de la víctima y exige un rescate para su liberación [50]. Los troyanos se disfrazan como software legítimo para engañar a los usuarios, mientras que los gusanos se propagan automáticamente a través de redes sin intervención humana [51]. Los virus sin archivos operan en la memoria del sistema, evitando la detección tradicional basada en firmas [52].

Ataques a la Identidad

Los ataques a la identidad, como el robo de credenciales y los ataques de suplantación de identidad (phishing), son cada vez más sofisticados. Los atacantes utilizan técnicas como el phishing spear para dirigirse a individuos específicos, a menudo aprovechando información obtenida de redes sociales o filtraciones de datos [53]. Además, el secuestro de sesiones (session hijacking) permite a los atacantes tomar el control de sesiones autenticadas, lo que es especialmente peligroso en entornos de trabajo remoto [54].

Amenazas en la Nube

Con la adopción masiva de servicios en la nube, los ataques a infraestructuras cloud han aumentado. Entre ellos destacan:

- Configuraciones incorrectas de la nube: Dejan expuestos datos sensibles a accesos no autorizados [55].

- Ataques a APIs: Las interfaces de programación de aplicaciones mal protegidas son explotadas para acceder a sistemas y datos [56].

- Secuestro de cuentas cloud (cloud account hijacking): Los atacantes obtienen acceso a cuentas de servicios en la nube para robar datos o lanzar ataques adicionales [57].

Ataques a Endpoints

Los endpoints, como computadoras portátiles, dispositivos móviles y servidores, son objetivos frecuentes. Los ataques de día cero (zero-day) explotan vulnerabilidades desconocidas antes de que se publiquen parches, mientras que los ataques de fuerza bruta intentan adivinar contraseñas para obtener acceso no autorizado [58]. Además, los ataques a la cadena de suministro comprometen software legítimo para distribuir malware a través de actualizaciones aparentemente inocuas [59].

Técnicas de Comando y Control (C2)

Los ataques de comando y control permiten a los atacantes mantener una conexión persistente con los sistemas comprometidos, utilizando servidores remotos para enviar instrucciones y exfiltrar datos [60]. Estas técnicas son comunes en campañas de Advanced Persistent Threats (APT), donde los atacantes permanecen en la red durante largos períodos sin ser detectados [59].

Amenazas Emergentes

Ataques a la cadena de identidad: Los atacantes explotan vulnerabilidades en sistemas de autenticación multifactor (MFA) para suplantar identidades [61].

Ataques a dispositivos IoT: Los dispositivos conectados, a menudo con seguridad insuficiente, son explotados para crear botnets o acceder a redes corporativas [62].

Ingeniería social avanzada: Los atacantes utilizan técnicas psicológicas para manipular a los usuarios y obtener acceso a sistemas o información sensible [63].

Motivaciones y Actores

Los creadores de malware y los perpetradores de ciberataques pueden ser actores internos o externos, con motivaciones que van desde el beneficio económico hasta el espionaje político o el activismo [64]. Los grupos patrocinados por estados-nación suelen tener recursos significativos y objetivos estratégicos, mientras que los cibercriminales buscan principalmente ganancias financieras.

Los tipos de ataques han evolucionado para explotar vulnerabilidades en áreas críticas como la identidad, la nube, los equipos de punto final en general. Para mitigar estos riesgos, es esencial adoptar un enfoque de seguridad integral que incluya la protección de identidades, la configuración segura de servicios en la nube y la defensa avanzada de endpoints, de los cual se hablará en secciones posteriores.

2.5 Proceso de respuesta a incidentes

El ciclo de vida del proceso de respuesta a incidentes es crítico en ciberseguridad, ya que ayuda a responder a ellos y minimizar su impacto. Esto implica un conjunto de actividades destinadas a detectar, analizar y mitigar, así como para restablecer la normalidad de las operaciones empresariales. En base al NIST en su publicación especial 800-61 [65], se resume este proceso de seis fases que se describen a continuación, cada una de ellas requiere acciones, herramientas y conocimientos específicos para garantizar que se gestionen con eficacia y eficiencia.

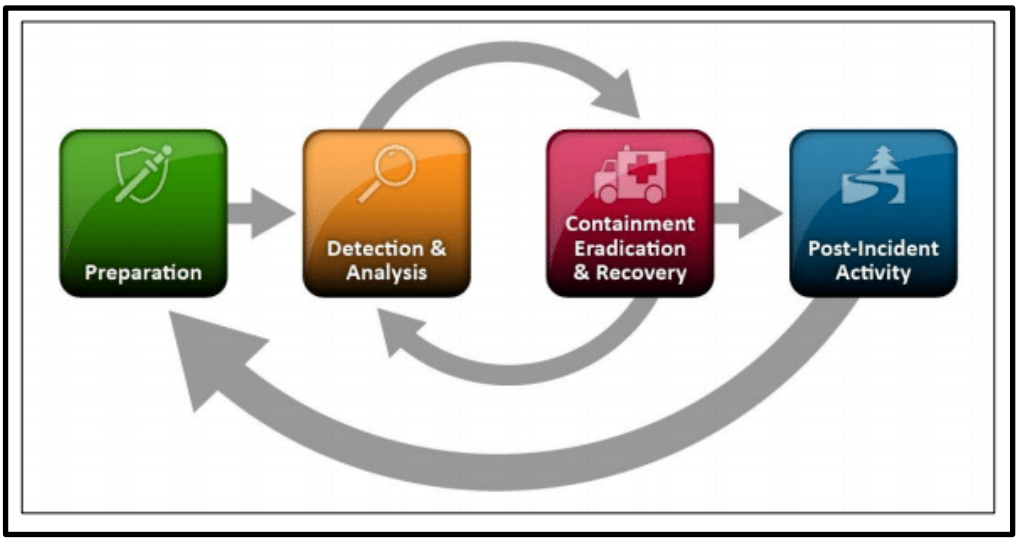


Fig. 14 *Ciclo de vida del proceso de respuesta a incidentes [65].*

2.5.1 Preparación

Esta fase incluye actividades que ayudan a los equipos de ciberseguridad a prepararse para posibles incidentes mediante la definición de procedimientos estandarizados, el establecimiento de canales de comunicación y la creación de equipos, asignando sus responsabilidades.

El principal objetivo de esta fase es garantizar que la organización dispone de los recursos y procedimientos necesarios para gestionar los incidentes de seguridad con rapidez y eficacia.

Las preocupaciones más importantes durante esta fase son desarrollar y probar planes de respuesta a incidentes, identificar los activos críticos, establecer canales de comunicación adecuados con socios externos y crear equipos de respuesta a incidentes. El resultado de esta fase es un plan de respuesta a incidentes bien definido y probado.

2.5.2 Identificación

Esta fase consiste en detectar y analizar los incidentes de seguridad para determinar su naturaleza, alcance e impacto. El objetivo principal de esta fase es identificar el origen del incidente, su vector de ataque, posibles vulnerabilidades explotadas, así como evaluar las implicaciones en los sistemas y datos de la organización. Las preocupaciones más importantes son supervisar los registros del sistema y el tráfico de la red, identificar el tipo de incidente y determinar hasta dónde llegó el compromiso o si es que se siguen realizando acciones de forma activa

El resultado de esta fase es un informe detallado del incidente, que incluye principalmente alcance, impacto y gravedad.

2.5.3 Contención

Esta fase consiste en contener el incidente para evitar que se propague y cause más daños. El objetivo principal es limitar el impacto del incidente en los sistemas y datos de la organización. Las preocupaciones más importantes durante este periodo de tiempo son aislar los sistemas comprometidos, bloquear el tráfico de red y desactivar las cuentas de usuario si es necesario.

Como resultado se obtiene un incidente contenido que no puede propagarse ni causar más daños.

2.5.4 Erradicación

Esta fase consiste en eliminar el malware u otros componentes maliciosos de los sistemas y datos de la organización. El objetivo principal de esta fase es eliminar la causa raíz del incidente y asegurarse de que todos los sistemas comprometidos están limpios. Las preocupaciones más importantes durante esta fase son escanear y limpiar los sistemas infectados, instalar parches y actualizaciones y restablecer las contraseñas.

El resultado de esta fase es un sistema confiable y seguro.

2.5.5 Recuperación

Esta fase consiste en restablecer el funcionamiento normal de los sistemas y datos de la organización. El objetivo principal de esta fase es minimizar la interrupción causada por el incidente y reanudar el funcionamiento normal de la empresa. Las preocupaciones más importantes durante esta fase son restaurar los datos de las copias de seguridad, verificar la integridad de los datos y restaurar las configuraciones del sistema.

El resultado de esta fase es una infraestructura totalmente funcional.

2.5.6 Lecciones aprendidas

Esta fase consiste en revisar el proceso de respuesta a incidentes para identificar áreas de mejora e incorporar esas mejoras en futuros planes de respuesta a incidentes. El principal objetivo de esta fase es garantizar que la organización aprenda del actual incidente y esté mejor preparada para futuros eventos. Las preocupaciones más importantes durante esta fase son llevar a cabo una revisión posterior, documentar las acciones tomadas, medir el comportamiento y rendimiento tanto del equipo, como del software utilizado, así como actualizar los planes de respuesta a incidentes.

El resultado de esta fase es un proceso de respuesta a incidentes mejorado que puede gestionar mejor futuros incidentes de seguridad.

2.6 Evaluaciones de seguridad

Son valoraciones realizadas para determinar la eficacia y adecuación de las medidas de seguridad de una organización a la hora de proteger sus activos de información y tecnología frente a las ciber amenazas, ya que desempeñan un papel fundamental a la hora de identificar vulnerabilidades, mitigar riesgos y garantizar el cumplimiento de los requisitos. Así, mismo ayudan a detectar vulnerabilidades, reducir riesgos y cumplir con normativas vigentes. A medida que los ataques evolucionan, estas evaluaciones se han convertido en una práctica fundamental para la protección de los activos de información.

Entre los métodos más utilizados se encuentran las evaluaciones de riesgos, pruebas de penetración y auditorías de cumplimiento, los cuales se detallan a continuación:

2.6.1. Evaluaciones de Riesgos

En base a lo que menciona Check Point Software Technologies (empresa de ciberseguridad), en su artículo - "¿Qué es una Evaluación de Riesgos de ciberseguridad?" [66]. Las evaluaciones de riesgos de ciberseguridad son procesos sistemáticos que buscan identificar, analizar y priorizar posibles amenazas y vulnerabilidades en los sistemas de información de una organización. El objetivo principal es comprender las amenazas potenciales y tomar medidas proactivas para mitigarlas antes de que se conviertan en incidentes. Este proceso implica:

- **Identificación de Activos**: Catalogar todos los sistemas, datos y recursos tecnológicos que la organización utiliza.

- **Análisis de Amenazas y Vulnerabilidades**: Determinar qué amenazas podrían afectar a los activos identificados y evaluar las vulnerabilidades existentes.

- **Evaluación del Impacto**: Estimar las posibles consecuencias de una explotación de las vulnerabilidades, considerando factores como pérdidas financieras, daños a la reputación y cumplimiento normativo.

- **Priorización de Riesgos**: Clasificar los riesgos según su probabilidad e impacto para abordar primero los más críticos.

Realizar evaluaciones de riesgos permite implementar estrategias de seguridad más efectivas y asignar recursos de manera eficiente para proteger sus activos más valiosos.

2.6.2. Pruebas de Penetración

Las pruebas de penetración, comúnmente conocidas como "pentesting", son evaluaciones de seguridad en las que se simulan ataques reales contra los sistemas de una organización para identificar y explotar vulnerabilidades [67]. El propósito es descubrir debilidades antes de que los atacantes malintencionados las aprovechen. Este proceso incluye:

- **Planificación y Reconocimiento**: Definir el alcance de la prueba y recopilar información sobre los sistemas objetivo.

- **Escaneo**: Utilizar herramientas para identificar puertos abiertos, servicios activos y posibles puntos de entrada.

- **Explotación**: Intentar acceder a los sistemas mediante técnicas como inyección de código, escalada de privilegios o ingeniería social.

- **Análisis y Reporte**: Documentar las vulnerabilidades encontradas, evaluar su impacto y proporcionar recomendaciones para su mitigación.

Las pruebas de penetración ayudan a las organizaciones a fortalecer sus defensas al identificar y corregir vulnerabilidades antes de que puedan ser explotadas por atacantes reales.

2.6.3 Auditorias de Cumplimiento

Las auditorías de cumplimiento son evaluaciones que verifican si una organización cumple con las leyes, regulaciones, estándares y políticas internas relacionadas con la seguridad de la información. Estas auditorías aseguran que la organización esté alineada con las mejores prácticas y normativas aplicables [68] . El proceso generalmente implica:

- Revisión de Políticas y Procedimientos: Evaluar las políticas de seguridad y procedimientos operativos para garantizar que estén actualizados y sean efectivos.

- Evaluación de Controles Técnicos y Administrativos: Verificar la implementación y eficacia de controles como firewalls, sistemas de detección de intrusos, gestión de accesos y capacitación del personal.

- Análisis de Registros y Documentación: Revisar registros de actividad, incidentes de seguridad y documentación relacionada para asegurar el cumplimiento continuo.

- Informe de Hallazgos y Recomendaciones: Proporcionar un informe detallado de las áreas de no conformidad y sugerir acciones correctivas.

Las auditorías de cumplimiento son esenciales para identificar brechas en la conformidad y garantizar que la organización mantenga una postura de seguridad robusta y esté preparada para responder a requisitos regulatorios.

Existen varios marcos y estándares reconocidos internacionalmente que guían estas auditorías, entre los cuales destacan:

- **PCI DSS (Payment Card Industry Data Security Standard):** Este estándar se aplica a organizaciones que procesan, almacenan o transmiten datos de tarjetas de crédito. Establece requisitos específicos para proteger la información del titular de la tarjeta y prevenir fraudes financieros. Una de las exigencias clave es la realización regular de pruebas de penetración para detectar y corregir vulnerabilidades en la red y en las aplicaciones. El cumplimiento con PCI DSS no solo protege los datos de pago, sino que también previene fraudes financieros, protegiendo tanto a los comerciantes como a los consumidores.

- **GDPR (General Data Protection Regulation)**: Reglamento europeo que establece directrices para la protección de datos personales de los ciudadanos de la Unión Europea. Requiere que las organizaciones implementen medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad acorde al riesgo, incluyendo la realización de evaluaciones de impacto y la notificación de brechas de seguridad.

- **ISO 27001**: Es un estándar internacional para la gestión de la seguridad de la información. Proporciona un marco para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Aunque ISO 27001 y PCI DSS comparten similitudes en cuanto a la protección de datos, ISO 27001 es más amplio y se aplica a todo tipo de información, mientras que PCI DSS se centra específicamente en datos de tarjetas de pago.

  Implementar estos métodos de evaluación permite identificar proactivamente vulnerabilidades, fortalecer sus defensas y asegurar el cumplimiento de las normativas vigentes en materia de ciberseguridad.

2.7 Recursos durante una investigación.

Cuando se lleva a cabo una investigación, es esencial tener acceso a datos relevantes que puedan apoyar la investigación y ayudar a identificar posibles sospechosos o fuentes de un incidente. Los datos que respaldan una investigación pueden proceder de diversas fuentes, como registros del sistema, datos de tráfico de red y metadatos.

2.7.1 Dashboards de un SIEM

En un SIEM se ofrece una representación visual centralizada de datos clave de seguridad, permitiendo a los profesionales monitorear, analizar y responder eficazmente a incidentes. Estos paneles proporcionan visibilidad en tiempo real de eventos e incidentes, facilitando la identificación rápida de amenazas y el análisis forense para determinar el alcance y el impacto de un incidente [69].

Fig. 15 *Ejemplo de dashboard del SIEM QRadar donde se muestran las alertas y estadísticas de los últimos 30 días [69].*

2.7.2 Archivos de registro

Los archivos de registro son registros históricos de todas las actividades que ocurren dentro de un sistema, incluyendo transacciones, errores e intrusiones. Contienen información detallada sobre la actividad del sistema y el comportamiento de los usuarios, lo que es esencial para rastrear actividades, identificar cambios en el

sistema y proporcionar evidencia de posibles brechas de seguridad o accesos no autorizados. [70]

2.7.3 Metadatos

Los metadatos son descritos como las fechas de creación de los archivos y las cabeceras de los paquetes de red, proporcionan información valiosa para las investigaciones, ya que pueden utilizarse para reconstruir la cronología de los acontecimientos e identificar las posibles fuentes de un incidente, pueden utilizarse para rastrear el movimiento de archivos o datos entre sistemas, identificar el origen del tráfico de red y proporcionar pruebas de una posible exfiltración de datos u otra actividad maliciosa [71].

2.7.4 Análisis de vulnerabilidades.

El uso de escáneres de vulnerabilidades permite identificar posibles puntos débiles en sistemas y aplicaciones que podrían ser explotados por atacantes. Herramientas como Nessus facilitan la generación de informes detallados sobre las vulnerabilidades detectadas, ayudando a priorizar las acciones correctivas.

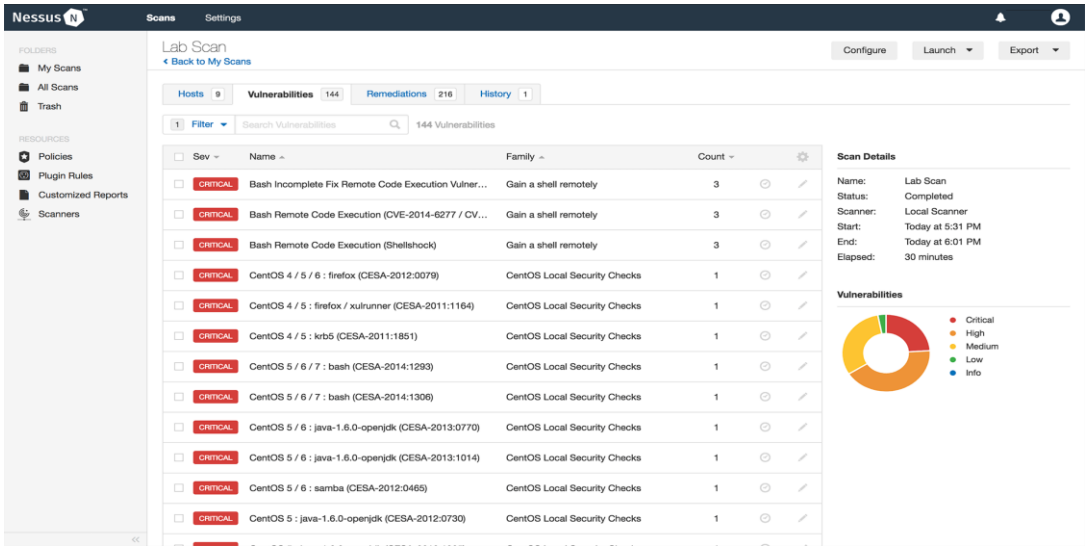


Fig. 16 *Evaluación de vulnerabilidades avanzada de Nesus Professional | Tenable [72]*

2.7.5 Análisis de Inteligencia de Código Abierto. (OSINT)

La recopilación y análisis de información disponible públicamente, conocida como OSINT, puede proporcionar contexto adicional durante una investigación. Esto incluye datos de redes sociales, foros, registros públicos y otras fuentes abiertas que pueden ofrecer pistas sobre posibles amenazas o actores maliciosos.

2.7.6 Caza de Amenazas (Threat Hunting)

La caza proactiva de amenazas implica buscar de manera activa signos de actividad maliciosa dentro de una red antes de que se generen alertas. Esto se realiza mediante el análisis de patrones de comportamiento, indicadores de compromiso y otras señales que podrían indicar la presencia de actores maliciosos.

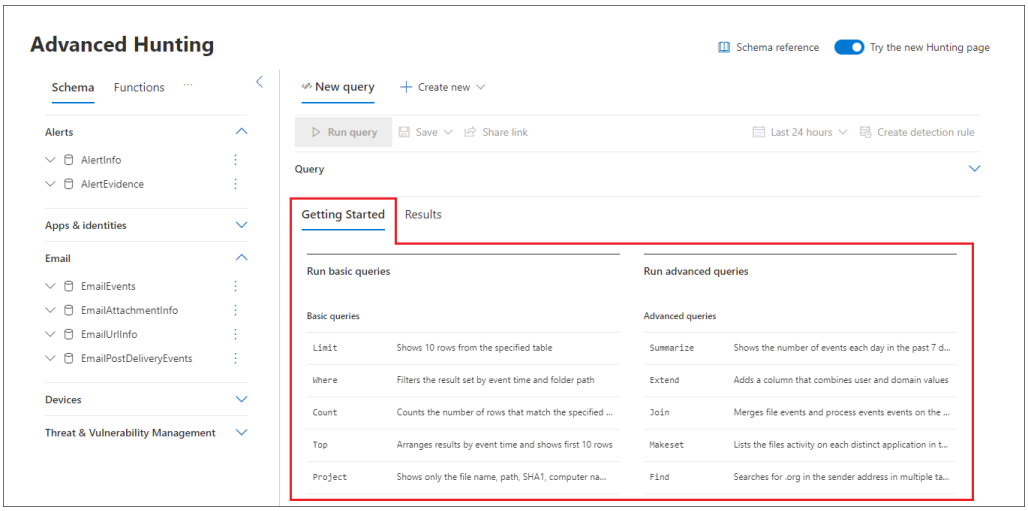


Fig. 17 *Microsoft Advanced Hunting Portal es una herramienta de búsqueda de amenazas basada en consultas que permite explorar hasta 30 días de datos sin procesar. [73]*

2.7.6 Mitre Att&ck Framework

El MITRE ATT&CK Framework es una base de conocimiento accesible globalmente que detalla las tácticas, técnicas y procedimientos (TTPs) utilizados por adversarios cibernéticos, basándose en observaciones del mundo real. Desarrollado por la corporación MITRE, este marco se ha convertido en una herramienta esencial para comprender y contrarrestar comportamientos adversarios en el ámbito de la ciberseguridad [74].

Componentes Clave del MITRE ATT&CK Framework:

- Tácticas: Representan los objetivos estratégicos que un adversario intenta lograr durante una intrusión, como la escalada de privilegios o la evasión de defensas.

- Técnicas: Describen las formas específicas en que los adversarios logran estos objetivos. Cada técnica puede tener múltiples sub-técnicas que proporcionan detalles adicionales sobre cómo se lleva a cabo.

Aplicaciones del MITRE ATT&CK Framework:

- Evaluación de Amenazas: Permite modelar y comprender las tácticas y técnicas que los adversarios podrían emplear contra ellas, facilitando la identificación de brechas en sus defensas.

- Desarrollo de Estrategias de Defensa: Proporciona una base para desarrollar y priorizar estrategias de mitigación y detección, asegurando que las defensas estén alineadas con las amenazas actuales.

- Evaluaciones de Seguridad: Sirve como referencia para evaluar la eficacia de las medidas de seguridad existentes y para planificar mejoras basadas en comportamientos adversarios conocidos.

El MITRE ATT&CK Framework se organiza en matrices que cubren diferentes dominios, incluyendo entornos empresariales, móviles y sistemas de control industrial. Cada matriz está estructurada en columnas que representan tácticas y filas que detallan técnicas asociadas, proporcionando una visión clara y estructurada de las posibles acciones adversarias.

2.7.7 Orquestación, Automatización y Respuesta de Seguridad

Los SOAR son una estrategia integral que combina la integración de diversas tecnologías de seguridad con la automatización de flujos de trabajo para optimizar la respuesta a incidentes y minimizar la intervención manual. Este enfoque permite gestionar de manera más eficiente las operaciones de seguridad, automatizando tareas rutinarias, priorizando incidentes y proporcionando visibilidad en tiempo real de los eventos de seguridad, lo cual es realmente útil durante el tiempo de investigación y respuesta [75].

Dentro del contexto de SOAR, los playbooks y runbooks desempeñan roles fundamentales:

- Playbooks: Son flujos de trabajo automatizados que guían la respuesta a incidentes específicos. Estos playbooks pueden comunicarse continuamente con las mismas herramientas de endpoint para ejecutar consultas sobre procesos, conexiones de red, historial del navegador, entre otros, con el fin de rastrear y mitigar amenazas de manera eficiente.

- Runbooks: Aunque el término se utiliza a menudo de manera intercambiable con playbooks, los runbooks tradicionalmente se refieren a procedimientos documentados que describen las acciones necesarias para completar una tarea o proceso específico. En el contexto de SOAR, los runbooks pueden ser utilizados para estandarizar procesos de respuesta a incidentes, asegurando que las acciones se realicen de manera coherente y efectiva [76]

Al implementar SOAR con playbooks y runbooks bien definidos, los equipos SOC pueden mejorar significativamente su capacidad para detectar, responder y recuperarse de incidentes de seguridad, fortaleciendo así su postura general de ciberseguridad.

2.8 Técnicas de mitigación

Reducen el impacto de los incidentes de seguridad y minimizan los daños a los sistemas y datos de una organización. Las estrategias de mitigación eficaces requieren una combinación de personas, procesos y tecnología para responder rápida y eficazmente a los incidentes de seguridad.

2.8.1 Contención

La contención implica aislar sistemas o redes comprometidas para evitar la propagación de un incidente de seguridad. Esta técnica limita el daño y proporciona tiempo a los equipos de seguridad para investigar y remediar la situación. Según el (NIST), la contención es una fase crítica en la gestión de incidentes, ya que ayuda a prevenir daños adicionales y a mantener la integridad de otros sistemas.[65]

2.8.2 Aislamiento

El aislamiento es una técnica de mitigación que consiste en separar un sistema o red comprometida del resto de la infraestructura de la organización. Esta medida previene la propagación de amenazas y protege los sistemas y datos críticos. La agencia CISA recomienda el aislamiento de sistemas afectados para contener incidentes y minimizar el impacto en operaciones esenciales. [77]

2.8.3 Segmentación

La segmentación de red implica dividir la red en subredes o segmentos más pequeños, cada uno con sus propios controles de seguridad y reglas de acceso. Esta práctica limita el alcance de un ciberataque al aislar sistemas comprometidos e impedir el movimiento lateral dentro de la red. El Centro de Seguridad Cibernética del Reino Unido (NCSC) destaca que la segmentación ayuda a contener incidentes y protege activos críticos al restringir el acceso no autorizado. [78]

También facilita la detección y respuesta a un ataque, ya que éste puede contenerse en un único segmento en lugar de propagarse por toda la red.

Existen diferentes enfoques para la segmentación, incluida la segmentación física, en la que la red se divide físicamente en subredes separadas, y la segmentación lógica, en la que se utilizan particiones virtuales para separar el tráfico de red. La segmentación es una técnica de mitigación importante en la ciberseguridad moderna, especialmente frente a ciber amenazas sofisticadas como las amenazas persistentes avanzadas (APT) y los exploits de día cero.

En adición la empresa Palo Alto Networks menciona que, la segmentación puede ayudar a reducir la superficie de ataque, controlar el acceso a sistemas y datos críticos y mejorar la visibilidad del tráfico de red [79].

2.8.4 Cambios de configuración

Los cambios de configuración pueden utilizarse como técnica de mitigación para prevenir futuros incidentes de seguridad ajustando la postura de seguridad de sistemas y redes. Los cambios de configuración pueden incluir la actualización de las reglas del cortafuegos, el parcheado de vulnerabilidades y la desactivación de servicios innecesarios para reducir la superficie de ataque y prevenir posibles ataques.

2.8.5 Reconfigurar las soluciones de seguridad endpoints

Las soluciones de seguridad de punto final, como el software antivirus y las herramientas de detección y respuesta de punto final (EDR), pueden configurarse para mejorar su eficacia en la detección y respuesta a incidentes de seguridad. Esto puede incluir el ajuste de las reglas de detección de amenazas, la configuración de políticas para impedir el acceso no autorizado y la habilitación de funciones de seguridad avanzadas como Indicadores de Ataque (IOA), o IOC’s obtenidos de fuentes OSINT.

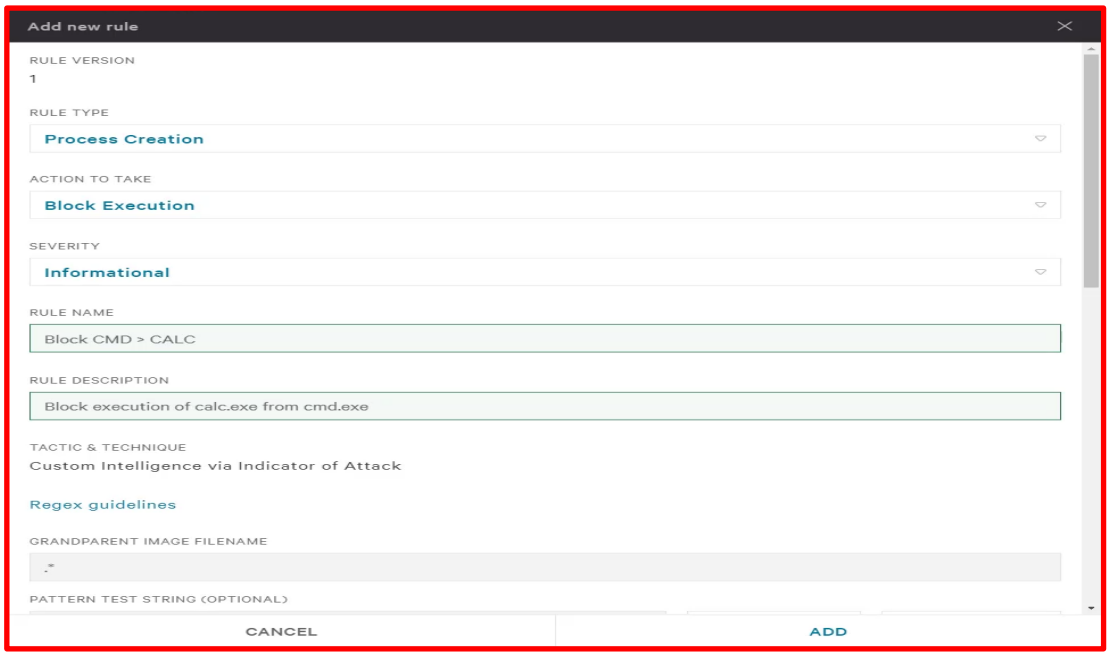


Fig. 18 *Ejemplo de configuración de una regla personalizada para el bloqueo de un Indicador de Ataque en Crowdstrike Platform [80]*

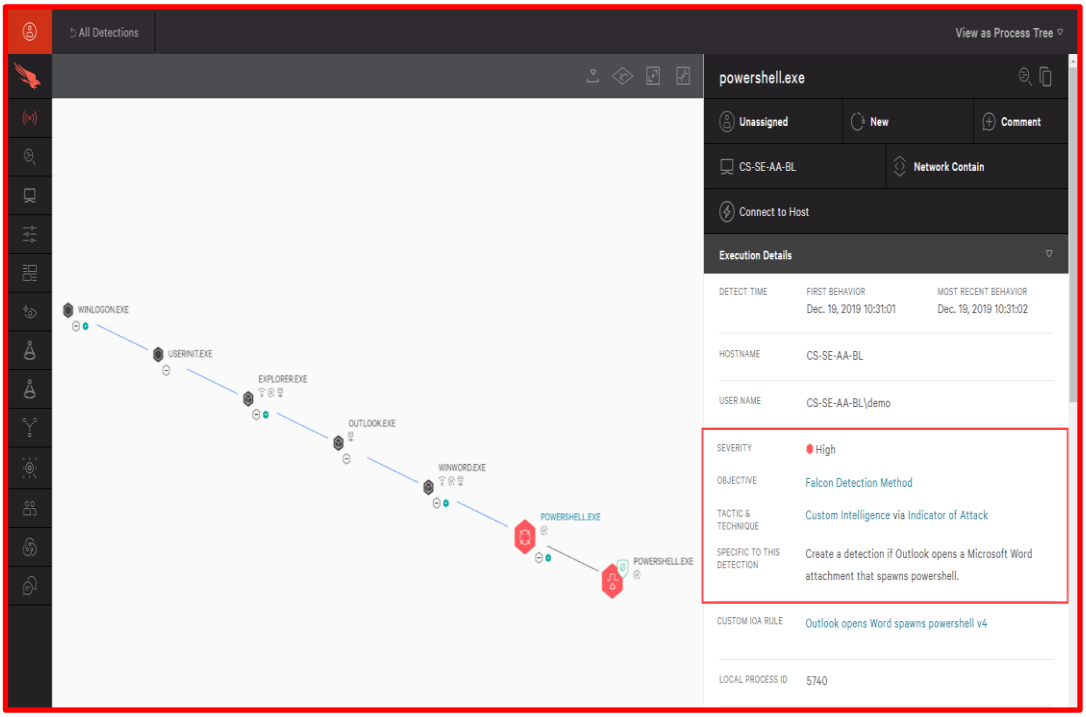


Fig. 19 *Ejemplo de detección (evento de seguridad) dada una regla personalizada para el bloqueo de un Indicador de Ataque en Crowdstrike Platform. [80]*

Capítulo 3.- Metodología

El campo de la respuesta a incidentes ha evolucionado significativamente en los últimos años debido al aumento en la complejidad y frecuencia de los ciberataques. Este panorama ha puesto de manifiesto la necesidad urgente de que las organizaciones cuenten con metodologías eficaces y eficientes para gestionar y mitigar incidentes de ciberseguridad. En este contexto, la presente tesis propone una mejora en estas metodologías mediante la integración de The Hive Project, una plataforma de código abierto que se ha consolidado como una herramienta clave en la automatización y gestión de respuestas a incidentes, junto con tecnologías emergentes.

A medida que los ciberataques evolucionan y adoptan técnicas más sofisticadas, se hace evidente la necesidad de un enfoque más holístico y automatizado para la respuesta a incidentes. Este enfoque incluye la adopción de plataformas SOAR, como Falcon Fusion, que centralizan la gestión y la automatización de procesos críticos. Además, la integración de soluciones como Microsoft 365 Defender, CrowdStrike y MISP permite proporcionar inteligencia de amenazas y capacidades de análisis avanzadas que fortalecen la capacidad de un SOC para responder de manera ágil y efectiva.

En este capítulo se exploran los beneficios y limitaciones de estas plataformas, los desafíos inherentes a su integración y el impacto general en los procesos de respuesta a incidentes. Con ello, se espera que los lectores tendrán una comprensión clara de cómo estas herramientas pueden ser utilizadas para optimizar las capacidades de respuesta y proteger de manera más efectiva a los activos e información frente a las crecientes amenazas cibernéticas.

3.1 Requerimientos

Para la implementación de la metodología propuesta, se identificaron y documentaron los requerimientos técnicos necesarios para asegurar la funcionalidad y eficacia del proyecto (para mayor detalle consultar el apéndice de este documento). A continuación, se presentan estos requerimientos organizados en categorías clave que reflejan las necesidades al realizar el despliegue de la plataforma.

Requerimientos Técnicos

Los requerimientos técnicos incluyen las herramientas, servicios y soluciones necesarias para soportar la metodología. En la siguiente tabla se describen las soluciones de seguridad identificadas y sus respectivas funciones:

Categoría	**Herramienta/Solución**	**Descripción**
EDR	CrowdStrike Falcon	Solución de detección y respuesta en endpoints que permite identificar y mitigar amenazas avanzadas en tiempo real.
Seguridad de correos	Microsoft 365 Defender	Sistema de seguridad para correos electrónicos que protege contra phishing, malware y otras amenazas en archivos adjuntos o enlaces.
Threat Intelligence	MISP	Plataforma para compartir y analizar inteligencia de amenazas, enriqueciendo el contexto de los incidentes.
	VirusTotal	Herramienta para analizar archivos y URLs en busca de malware y amenazas conocidas.
	Abuse IP	Servicio que verifica la reputación de direcciones IP y detecta posibles actividades maliciosas.

Seguridad Perimetral	Firewall (Ejemplo: Palo Alto, Fortinet)	Dispositivo de seguridad que controla y monitorea el tráfico de red, protegiendo contra accesos no autorizados.
	IDS/IPS (Ejemplo: Snort, Suricata)	Sistemas de detección y prevención de intrusiones que identifican y bloquean actividades sospechosas o maliciosas en la red.
Gestión de Logs	SIEM (Ejemplo: Splunk, Elastic SIEM)	Sistema de correlación de eventos y análisis de logs que centraliza datos de seguridad para identificar patrones y amenazas.
Orquestación	Crowdstrike Falcon Fusion SOAR	Plataforma SOAR que permite la automatización de tareas repetitivas y la orquestación de flujos de trabajo en la respuesta a incidentes.
Gestion de Vulnerabilidades	Qualys	Plataforma que permite identificar, priorizar y remediar vulnerabilidades en infraestructura, aplicaciones y dispositivos en tiempo real.
Brand Protection (XTI)	SOC Radar	Herramienta para la protección de la marca, que monitorea la dark web, mercados clandestinos y redes sociales en busca de posibles riesgos relacionados con la organización.

Tabla 1. Requerimientos técnicos de interoperabilidad entre soluciones de ciberseguridad generales para la operación del SOC.

3.1.1 Análisis de Factibilidad Operativa

La factibilidad operativa evalúa la capacidad del laboratorio de ciberseguridad y los equipos SOC para implementar y utilizar eficazmente la solución propuesta, considerando aspectos como la preparación del personal, la adecuación de los procesos existentes y la aceptación organizacional. Este apartado detalla cómo estos factores garantizan el éxito de la integración de The Hive Project con las tecnologías seleccionadas.

Capacitación del Personal

El éxito de cualquier solución tecnológica depende en gran medida de que los especialistas estén capacitados para utilizarla eficazmente.

Identificación de necesidades de formación: Los equipos SOC requieren formación en el uso de diferentes soluciones de seguridad. Esto incluye, entre otras habilidades:

- Gestión de incidentes utilizando cualquier solución de ciberseguridad.
- Configuración y uso de APIs para la integración de herramientas.
- Automatización de procesos utilizando playbooks y flujos de trabajo personalizados.
- Administración de sistemas operativos para aquellas soluciones que requieren una instalación en servidores físicos o virtuales en la nube.
- Modelos de redes y configuración de protocolos de red, reglas de firewall o túneles VPN para el cifrado de la información.

Diseño del programa de capacitación: Se propone un programa de formación dividido en etapas:

- **Introducción**: Conceptos básicos de gestión de incidentes y características principales de The Hive Project.
- **Entrenamiento práctico**: Ejercicios simulados utilizando escenarios de ciberseguridad basados en datos reales.

- **Especialización**: Configuración avanzada e integración con otras herramientas.

Impacto esperado: Con la capacitación adecuada, los especialistas podrán aprovechar al máximo la solución, reduciendo el tiempo de respuesta a incidentes y aumentando la precisión en su manejo.

Adecuación de los Procesos Existentes

La implementación de una solución nueva no solo requiere herramientas técnicas, sino también ajustes en los procesos operativos para alinearlos con las capacidades y características del sistema.

Evaluación de los procesos actuales: Se identificaron áreas clave en los flujos de trabajo del SOC donde la integración de puede optimizar los tiempos y mejorar la gestión:

- Priorización y clasificación de incidentes.
- Comunicación entre equipos durante la gestión de incidentes.
- Documentación y cierre de casos.

Ajustes en los flujos de trabajo. Se propone:

- Centralizar la gestión de incidentes en The Hive Project, reemplazando sistemas manuales o fragmentados.
- Establecer nuevos protocolos para la escalación de incidentes, automatizados en base a playbooks.
- Reforzar la colaboración entre equipos utilizando las funcionalidades de colaboración integrada.
- Crear un único canal de documentación, utilizar gráficos e información puntual de esta plataforma para evaluar el SLA’s (Service Level Agreement) o bien enviar reportes detallados a los clientes.

Aceptación Organizacional

La aceptación por parte de los equipos SOC y otros interesados es clave para asegurar la implementación exitosa de la solución.

Percepción inicial: Las entrevistas realizadas a los miembros del SOC indican un alto nivel de aceptación de la solución propuesta, principalmente debido a su capacidad para reducir tareas repetitivas y optimizar tiempos de respuesta.

Gestión del cambio: Aunque la aceptación es positiva, se propone un plan de gestión del cambio para facilitar la transición:

- **Comunicación efectiva**: Explicar claramente los beneficios de la solución a todos los niveles de la organización.
- **Implementación por fases**: Introducir la solución gradualmente para minimizar interrupciones en las operaciones.
- **Soporte continuo**: Brindar soporte técnico y operativo durante las primeras etapas de implementación para resolver dudas o problemas rápidamente.

Recursos Humanos y Operativos

La implementación de la solución requiere asignar recursos humanos y operativos específicos.

Roles y responsabilidades:

- Un administrador de la plataforma se encargará de gestionar y configurar The Hive Project.
- Los analistas SOC utilizarán la plataforma en su flujo de trabajo diario para gestionar incidentes.
- Un equipo de soporte técnico estará disponible para resolver problemas durante las primeras fases de adopción.

Carga de trabajo: La automatización de tareas reducirá significativamente la carga de trabajo en tareas manuales, permitiendo a los especialistas enfocarse en actividades estratégicas.

Impacto en la Operación Diaria

La solución está diseñada para integrarse sin causar disrupciones significativas en las operaciones existentes.

Mejoras operativas esperadas:

- Reducción de tiempos en la clasificación de incidentes.
- Mayor precisión en la identificación y respuesta a amenazas gracias a la inteligencia compartida entre plataformas.
- Mitigación de riesgos: La implementación por fases y la capacitación previa reducen el riesgo de errores operativos o resistencia al cambio.

La factibilidad operativa de la solución propuesta es alta, ya que los equipos SOC cuentan con los recursos, disposición y capacidades necesarias para adoptarla. Con un plan de capacitación sólido, ajustes en los procesos actuales y un enfoque estratégico en la gestión del cambio, la implementación de The Hive Project y sus tecnologías asociadas contribuirá significativamente a mejorar la eficacia y eficiencia en la respuesta a incidentes.

3.1.2 Análisis de Factibilidad Técnica

TheHive se puede implementar en un servidor independiente o como un clúster. La aplicación se basa en:

- Apache Cassandra para almacenar datos (Versión compatible: 4.x).
- Elasticsearch como motor de indexación (Versión soportada: 7.x).
- También se requiere una solución de almacenamiento de archivos; el sistema de archivos local del servidor que aloja la aplicación es adecuado en el escenario de un servidor independiente.

Cada capa, la aplicación The Hive, la base de datos, el motor de índices y el almacenamiento de archivos son independientes y se pueden configurar como un nodo o clúster independiente.

Caso de estudio:

Todas las aplicaciones están instaladas en el mismo servidor:

- Casandra
- Elasticsearch
- Los archivos se almacenan en el sistema de archivos.
- The Hive
- NGINX (opcional): para gestionar las comunicaciones HTTPS

Los requisitos de hardware dependen de la cantidad de usuarios simultáneos (incluidas las integraciones) y de cómo usan el sistema. La siguiente tabla muestra los umbrales seguros cuando se alojan todos los servicios en la misma máquina:

Número de usuarios	The hive	Cassandra	ElasticSearch
<10	2 cpu cores / 2 GB Ram	2 cpu cores / 2 GB Ram	2 cpu cores / 2 GB Ram
<20	2-4 cpu cores / 4 GB Ram	2-4 cpu cores / 4 GB Ram	2-4 cpu cores / 4 GB Ram
<50	4-6 cpu cores / 8 GB Ram	4-6 cpu cores / 8 GB Ram	4-6 cpu cores / 8 GB Ram

Tabla 2. Requerimientos de hardware mínimos para la operación del proyecto.

Sistemas Operativos Soportados

- Ubuntu 20.04 LTS
- Debian 11
- RHEL 8
- Fedora 35

3.1.2.1 Estimando el tamaño de los requerimientos

Tomando en cuenta, la implementación actual, el MISP en producción y que la integración aún puede contener a un SOAR cómo SHUFFLE o n8n ejecutándose en segundo plano. Mínimamente, se recomienda la siguiente infraestructura:

Núcleos	RAM	Disk Space
6 (The hive) + 4 (MISP & CORTEX) + 2 (SOAR) = 12	32 GB	500 GB

Tabla 3. Requerimientos de hardware mínimos para la operación del proyecto.

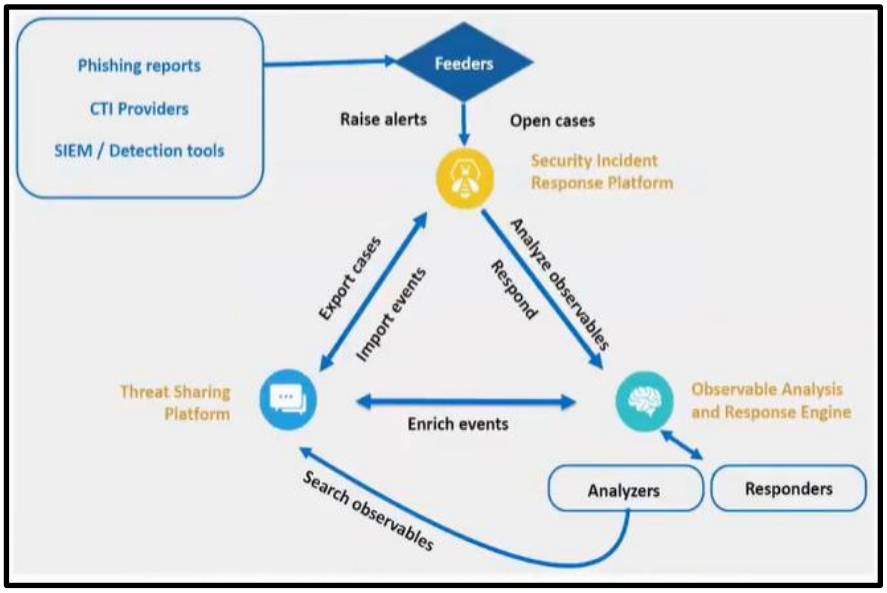


Fig. 20 *Modelo de funcionamiento al realizar la integración de algunos feeds en el nodo principal. [81]*

*Si la integración es con un (SaaS), como Tines.io o Falcon Fusion puede utilizarse una cantidad de recursos menor a la analizada mínimamente.

3.1.3 Análisis de Factibilidad Económica

La factibilidad económica del proyecto es justificada en base a que se trata de una solución de software libre, lo que implica que no se requiere pagar por licenciamientos.

The Hive Project es una plataforma de respuesta a incidentes de seguridad de código abierto, lo que significa que cualquier persona puede acceder al código fuente y utilizarlo de forma gratuita. Esto resulta en una importante ventaja económica, ya que el proyecto fue desarrollado sin la necesidad de adquirir licencias costosas.

Además, el costo de la infraestructura necesaria para operar la plataforma y el SOAR depende del proveedor de servicios de nube. Existen diversos proveedores, como Google Cloud Platform, Azure y AWS, entre otros, que ofrecen una gran variedad de opciones de infraestructura y tarifas que pueden adaptarse a las necesidades y presupuesto del proyecto.

A continuación, se muestra una tabla comparativa de los costes anuales en (MXN) tomando en cuenta los requerimientos mínimos de operación, según cada proveedor:

Recursos	**1 Año**	**3 Años**	**5 Años**
AWS	2,000	6,000	10,000
GCP VM	3,180	9,540	15,900

Tabla 4. Costos por renta de infraestructura de forma anual.

En resumen, la factibilidad económica es válida al tratarse de una solución de software libre y el costo de la infraestructura varía dependiendo del proveedor de servicios de nube elegido. Además, existen SOAR que no requieren licenciamiento y que pueden ser operados bajo el mismo servidor que la plataforma de respuesta a incidentes, lo que resulta en una reducción de costos de mantenimiento y administración.

3.2 Infraestructura y modelo de integración

Hardware y software: Es necesario disponer de infraestructura de hardware y software para alojar y ejecutar el proyecto. Esto puede incluir servidores, máquinas virtuales, e infraestructura.

A continuación, se presenta el diagrama de alto nivel con la arquitectura a desarrollar.

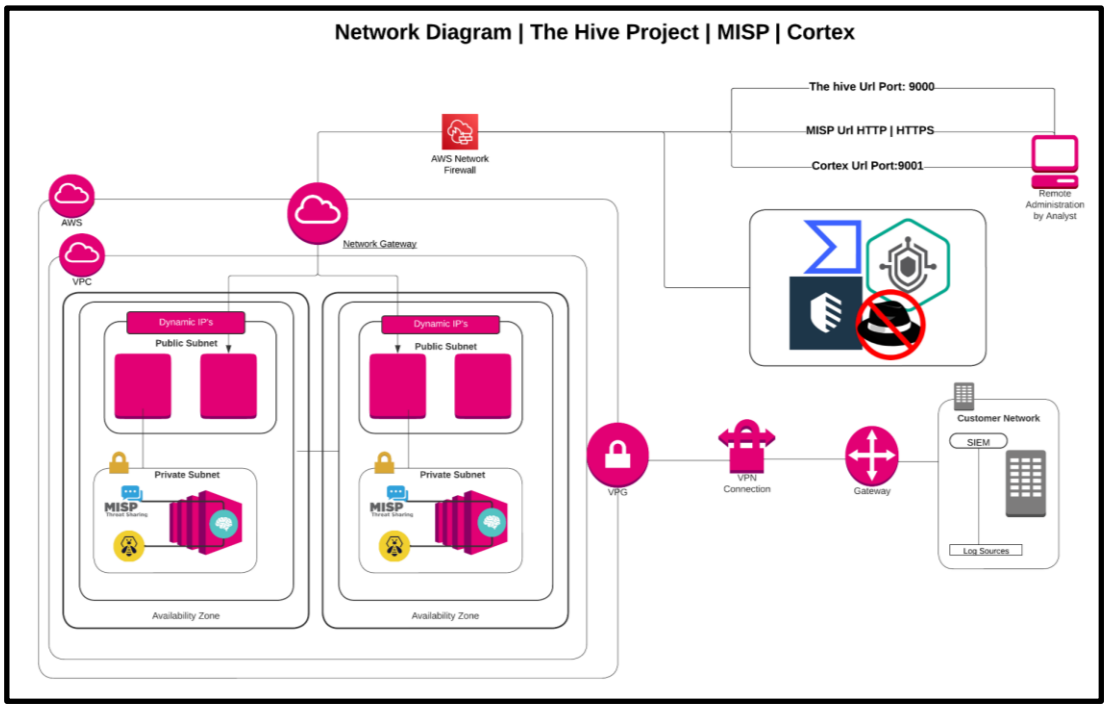


Fig. 21 *Diagrama de interacción entre servicios de nube, proyecto, red de externa y analizadores. Autoría propia*

3.2.1 The hive project

TheHive es una plataforma de respuesta a incidentes de seguridad escalable, estrechamente integrada con MISP (plataforma de intercambio de información de malware), diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que deben investigarse y actuar rápidamente.

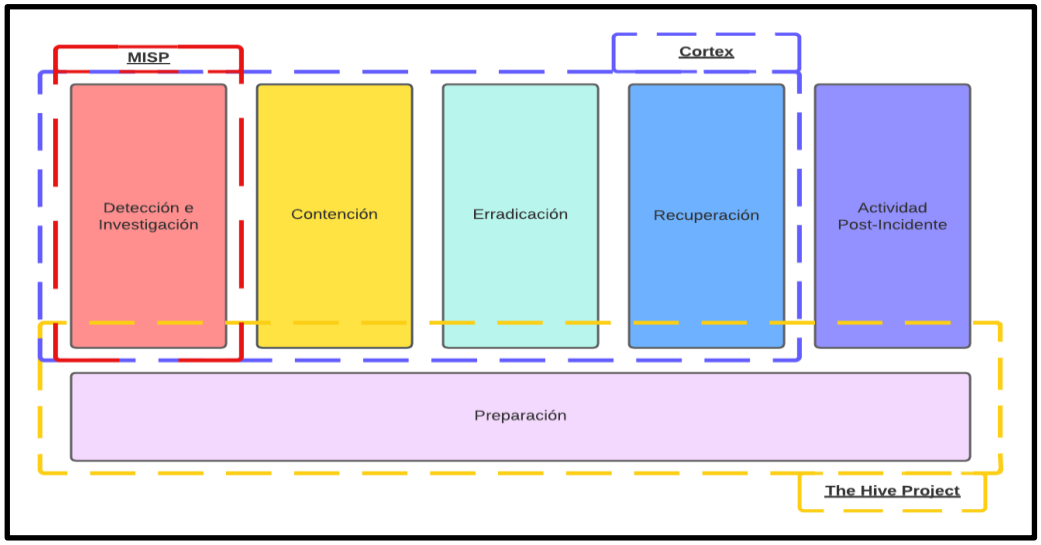


Fig. 22 *The hive, Cortex y MISP dentro de las fases de respuesta a incidentes. Autoría propia*

3.2.2 Cortex

Los elementos observables, como las direcciones IP y de correo electrónico, las URL, los nombres de dominio, los archivos o los hashes, se pueden analizar mediante la interfaz de Cortex. Los analistas también pueden automatizar estas operaciones y enviar grandes conjuntos de observables desde The Hive a través de la API REST de Cortex. Cuando se usa junto con The Hive, Cortex facilita en gran medida la **fase de contención** gracias a sus funciones de **respuesta activa**.

TheHive también puede aprovechar los responders de Cortex para realizar acciones específicas sobre **alertas, casos, tareas y observables recopilados en el curso de la investigación**: enviar un correo electrónico a los integrantes, bloquear una dirección IP a nivel de proxy, notificar a los miembros del equipo que se debe enviar una alerta, ser atendido con urgencia y mucho más.

Muchas características están incluidas con Cortex:

- Administra múltiples organizaciones (es decir, multiusuario).
- Administrar usuarios por organizaciones y roles
- Especifique la configuración del analizador y respondedor por organización
- Define límites de tarifas: evita consumir todas tus cuotas a la vez
- Caché: un análisis no se vuelve a ejecutar para el mismo observable si se llama a un determinado analizador en ese observable varias veces dentro de un período de tiempo específico (10 minutos por defecto, se puede ajustar para cada analizador).

3.2.3 MISP

MISP es un potente software de código abierto que permite intercambiar y compartir inteligencia sobre amenazas, indicadores de compromiso (IoC), fraudes financieros y cualquier otro tipo de inteligencia dentro de una comunidad de miembros de confianza. El modelo distribuido de MISP contiene información técnica y no técnica

que puede compartirse en comunidades cerradas, semiprivadas o abiertas. Al compartir esta información se consigue una detección más rápida de los ataques selectivos, se mejoran los radios de detección y se reducen los falsos positivos.

En cuanto a los requisitos de hardware, las necesidades de MISP son relativamente modestas. Un servidor web con al menos 2 núcleos y 8-16 GB de memoria debería ser suficiente, aunque disponer de más recursos siempre es mejor.
Los requisitos específicos de hardware dependen de varios factores, como el número de usuarios, los datos ingeridos, los puntos de datos utilizados, el número de eventos, el número de correlaciones y el uso de la API.

Varios factores pueden influir en los requisitos de hardware del MISP, como el número de muestras y archivos adjuntos (que afectan directamente al uso del disco), el uso de memoria y la utilización de la CPU causados por el recuento de usuarios simultáneos (especialmente con una lista de usuarios de la API que consultan el MISP con frecuencia), y el número de fuentes y servidores remotos almacenados en caché y mantenidos en memoria (que pueden aumentar los requisitos de memoria).

En los servidores operativos, los centros de intercambio más pequeños y los MISP de punto final suelen utilizar 16 GB de memoria y 2 vcpus. En cambio, las grandes comunidades de compartición, como la comunidad del sector privado CIRCL, utilizan 128 GB de memoria con 32 núcleos de CPU físicos en modernas CPU Xeon.
La comunidad COVID MISP, que da servicio a más de mil usuarios, funciona con 8 GB de memoria y 4 vcpus. Las instancias de formación pueden funcionar con unos escasos 2 GB de memoria y una sola vcpu, pero esto no es recomendable para nada que no sea formación o experimentación.
La base de datos principal de MISP se basa en MariaDB, y el uso de SSDs es muy recomendable para asegurar una baja latencia y un acceso eficiente a la base de datos. El tipo de almacenamiento utilizado por MariaDB también puede afectar a la latencia y el espacio en disco utilizado. Además, el almacenamiento en caché de feeds utiliza RAM para almacenar elementos de los feeds habilitados y almacenados en caché. Si

todos los feeds predeterminados están habilitados, el almacenamiento en caché de feeds puede utilizar hasta 1,2 GB de memoria [Sizing your MISP instance (misp-project.org)].

3.2.3 SOCRadar

SOCRadar proporciona un sistema de alerta temprana con una plataforma de *inteligencia de amenazas extendida (XTI)*, rastrea los cambios y riesgos en los activos digitales, brinda protección proactiva a las empresas y proporciona información sobre ataques en el mundo cibernético. La inteligencia de amenazas, como sugiere el nombre, investigará amenazas potenciales y ayudará a construir una seguridad más sólida con los datos que proporciona.

La inteligencia de amenazas tradicional promete recopilar y analizar datos sobre los activos existentes. Por otro lado, *XTI* realiza un inventario, determina la superficie de ataque externa y comparte datos contextuales. Mantener un inventario de activos actualizado y escaneos regulares desde una perspectiva externa facilita la detección de vulnerabilidades explotadas.

Ventajas

- Detectar actividades sospechosas dentro de la red de la corporación y responder rápidamente.
- Observar convenientemente las infiltraciones de red y firewall.
- Descubrir posibles fugas de datos, lo antes posible.
- Detectar futuros ciberataques antes de que ocurra alguno.
- Permitir que los clientes organicen de una mejor manera los presupuestos de ciberseguridad.

Tres partes del monitoreo de seguridad

- Gestión de la superficie de ataque
- Monitoreo de la dark web.
- Supervisión web de la superficie de ataque.

3.2.4 Integración

La API de análisis de amenazas de SOCRadar permite que a los equipos de *búsqueda de amenazas* tomen decisiones rápidas al acceder a los grandes datos de SOCRadar , analizando las *puntuaciones de IP y hashes, la ubicación de IP, el estado de la lista blanca, la reputación, el DNS pasivo y la información del dominio*. Además de proporcionar el gran conjunto de datos que el equipo de *Threat Hunting* necesita con el enfoque de inteligencia extendida contra amenazas de SOCRadar.

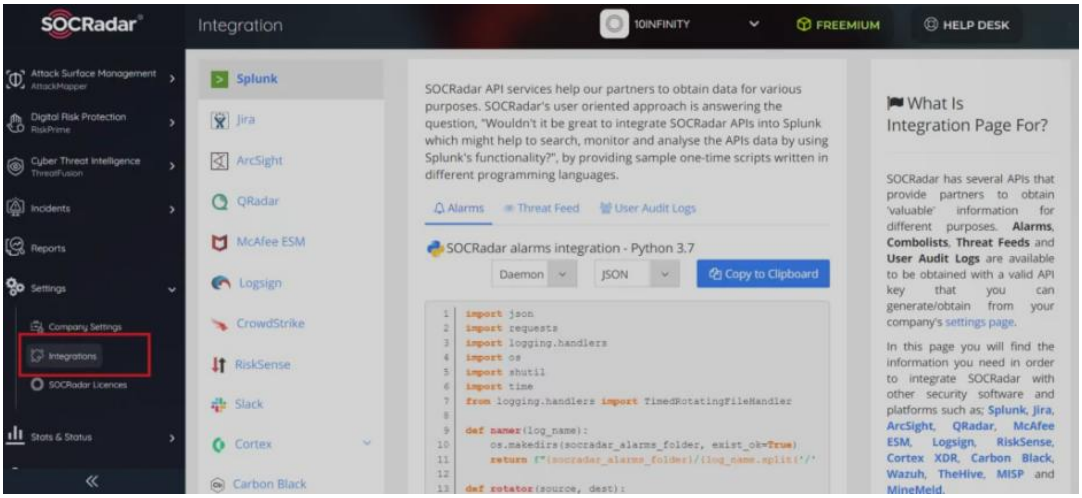


Fig. 23 *Integración disponibles y portal guías de configuración disponibles dentro de la plataforma. [82]*

Con la integración de ***SIEM Alarm***, el equipo SOC puede administrar alarmas a través de SIEM y recibir IoC actualizados diariamente con la integración de SIEM Threat Feed IoC.

Productos con integración completa: Splunk, QRadar, LogSign, ArcSight.

El equipo SOC puede administrar alarmas a través de **SOAR**. Con la integración de IoC de SOAR Threat Feed, se pueden recibir IoC actualizados diariamente, para preparar las acciones en la detección de IoC con las reglas que se establezcan.

Productos con integración completa: Cortex XSOAR Incident APP, Threat Feed APP

Se puede gestionar el **trabajo/tickets** con respecto a las alarmas transmitidas por SOCRadar a través de las aplicaciones de gestión de trabajo/emisión de entradas.

Productos con integración completa: Jira, The Hive

3.2.5 Crowdstrike

CrowdStrike aprovecha aplicaciones y técnicas avanzadas de EDR (detección y respuesta de terminales) para brindar una oferta de NGAV (antivirus de última generación) líder en la industria con aprendizaje automático para garantizar la detención de vulneraciones antes de que ocurran.

CrowdStrike es un sensor basado en agente que se puede instalar en computadoras de escritorio o plataformas de servidores con sistemas operativos Windows, Mac o Linux. Estas plataformas dependen de una solución SaaS alojada en la nube para administrar políticas, controlar datos de informes, administrar amenazas y responder a ellas.

CrowdStrike Falcon Sensor se comunica directamente con la nube a través de dos URL principales:

- ts01-b.cloudsink.net
- lfodown01-b.cloudsink.net

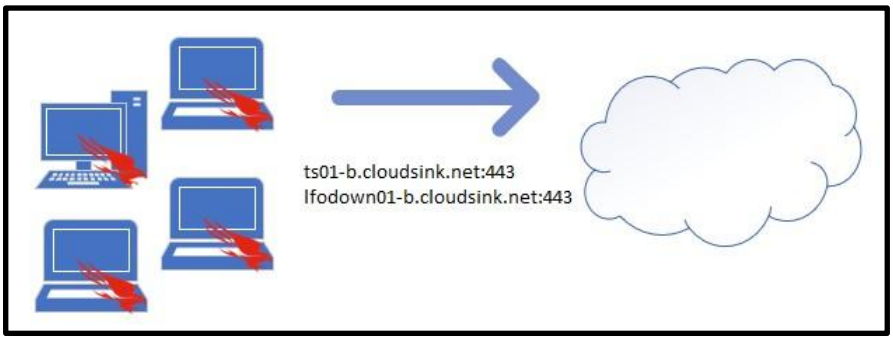


Fig. 24 *Más información en: Dell Support.(2022). ¿Qué es Crowdstrike?[83]*

Estas URL se aprovechan para actualizar agentes, sincronizar datos y cargar amenazas. CrowdStrike puede trabajar sin conexión o en línea para analizar archivos que se intenten ejecutar en los terminales. Esto se realiza mediante los siguientes elementos:

- Hashes de prevención predefinidos
- Indicador de comportamiento de ataques
- Known Malware
- Mitigación de vulnerabilidades

Para acceder a la API de Falcon es necesario el administrador, realice la configuración apropiada a través del menú (Support and resources -> API clients and keys -> Add new API client):

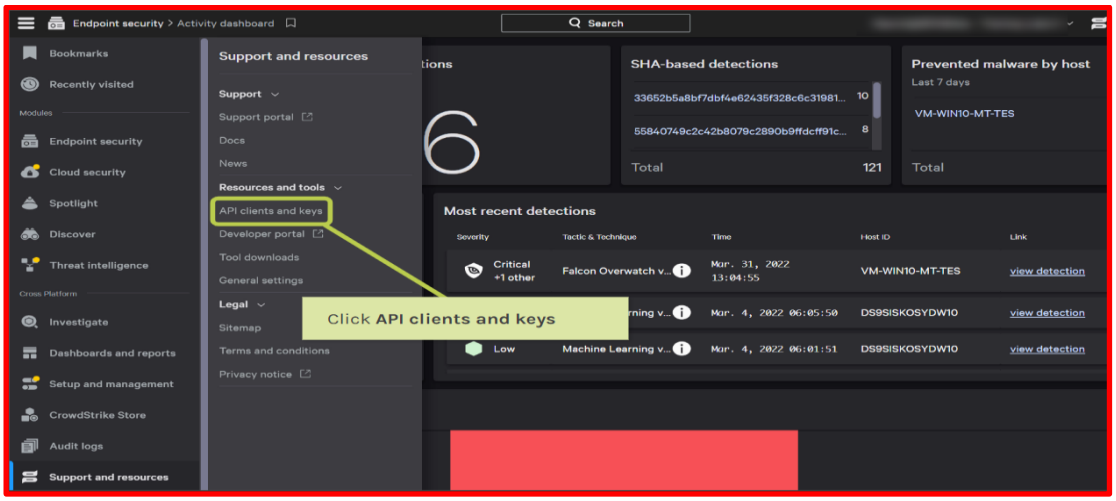


Fig. 25 *Accediendo al módulo de clientes API y llaves para la conexión de eventos a Crowdstrike Falcón. [84]*

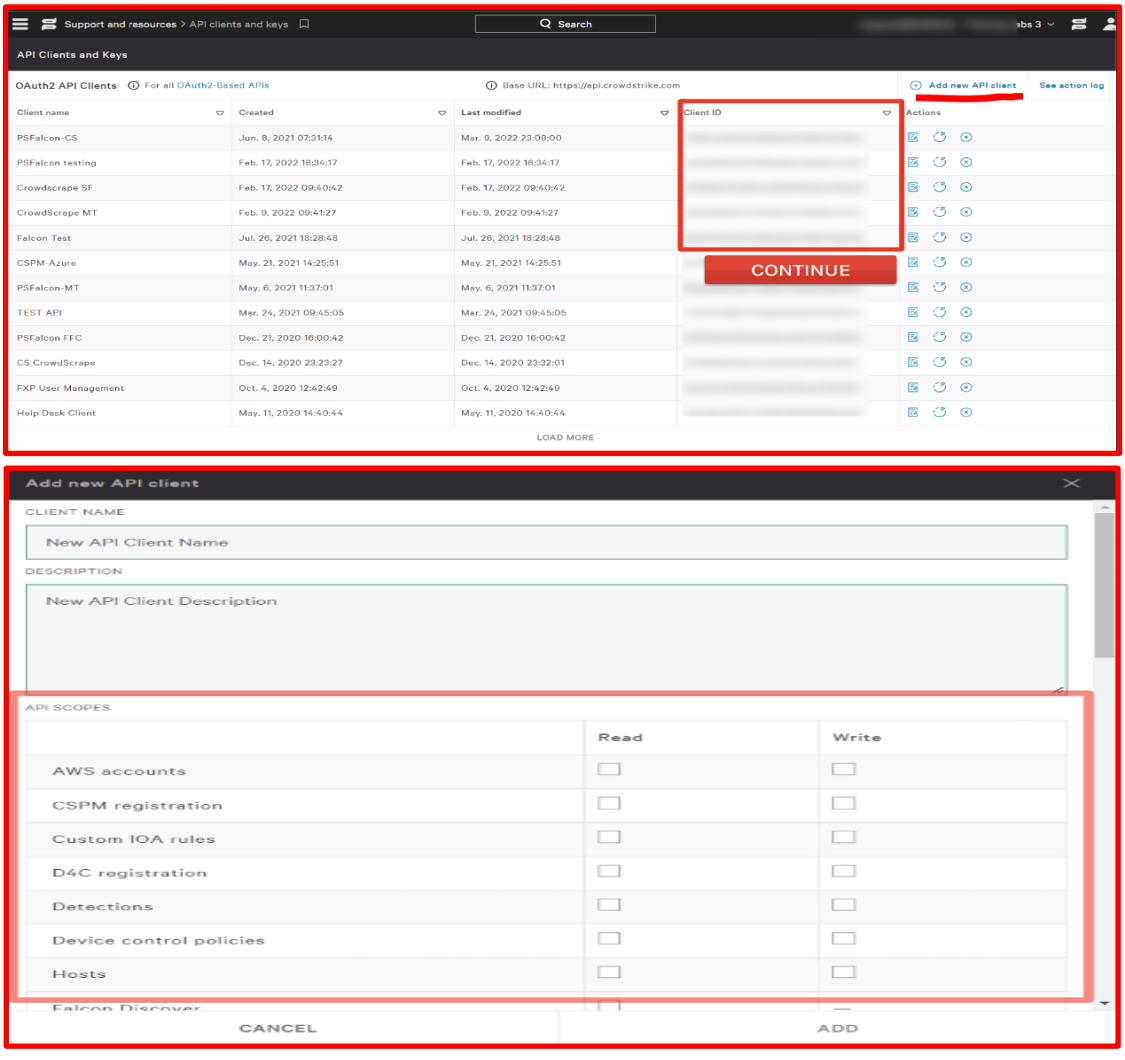


Fig. 26 *Creación y configuración de un nuevo cliente API. [84]*

Posteriormente en será necesario registrar los datos de que dará uso a esa API, descripción y los permisos necesarios (lectura, escritura) para obtener obtener la información.

Es importante guardar la clave (SECRET) y el CLIENT ID para poder realizar la autenticación primero mediante, el protocolo OAuth2.0.

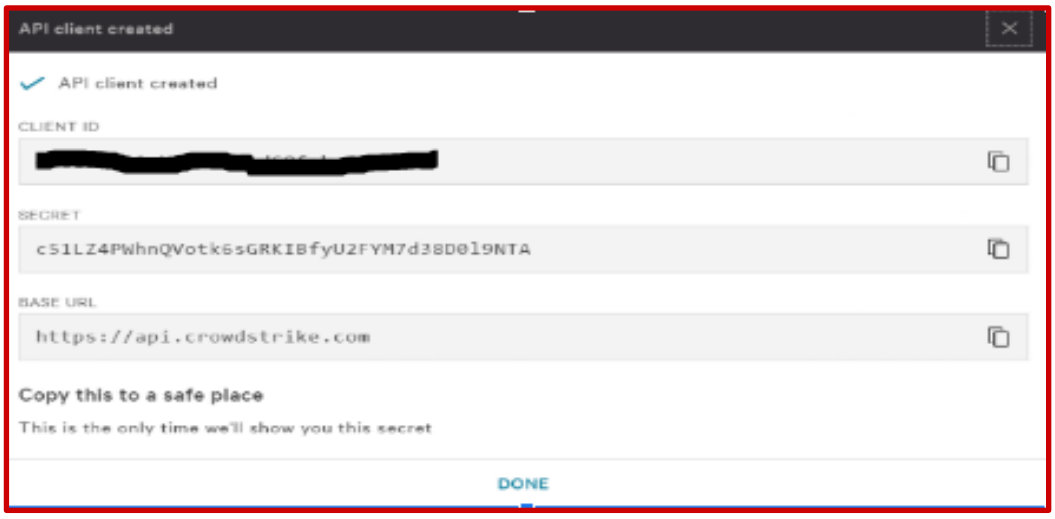


Fig. 27 *Registro de clave SECRET, CLIENT ID y baseurl desde el Crowdstrike UI. [84]*

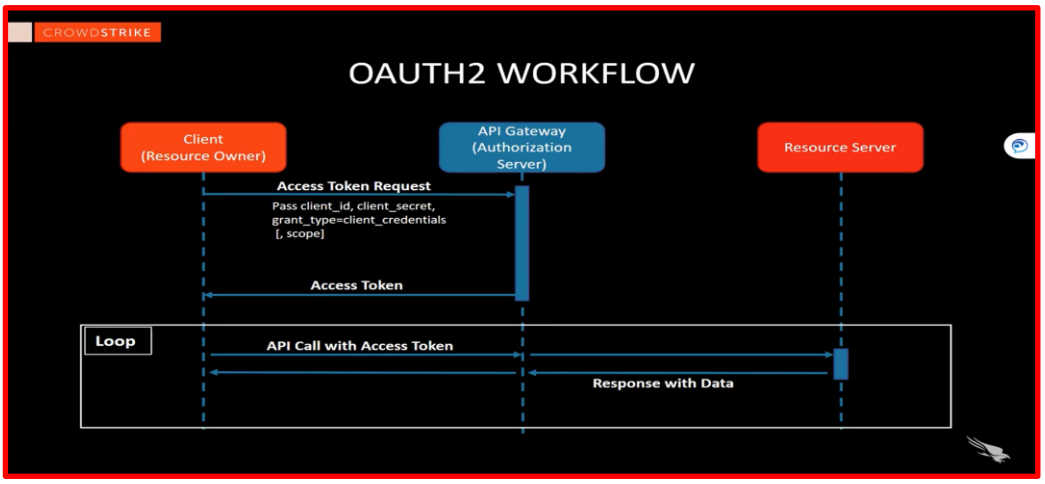


Fig. 28 *Modelo de funcionamiento de Oauth2 para acceder a la API de Crowdstrike. [84]*

OAuth 2.0 es un protocolo de autorización de estándar abierto que permite a las aplicaciones de terceros obtener acceso limitado a los recursos de un usuario, como los datos de un servicio web, sin que el usuario tenga que compartir sus credenciales (por ejemplo, nombre de usuario y contraseña).

El protocolo permite a los usuarios otorgar y revocar el acceso a sus recursos sin compartir sus contraseñas u otra información sensible. La funcionalidad de OAuth 2.0 se puede desglosar en varios pasos:

1. Un usuario solicita acceso a un recurso de una aplicación de terceros.
2. La aplicación redirige al usuario al propietario del recurso (por ejemplo, el servicio web) para autenticar y autorizar el acceso.
3. El propietario del recurso verifica la identidad del usuario y otorga o deniega el acceso a la aplicación.
4. Si se otorga el acceso, el propietario del recurso devuelve un token de acceso a la aplicación, que luego puede utilizar para acceder a los recursos del usuario en el servidor del propietario del recurso.
5. La aplicación utiliza el token de acceso para realizar solicitudes autorizadas al servidor del propietario del recurso en nombre del usuario.

OAuth 2.0 admite varios tipos de concesión diferentes, incluidos código de autorización, implícito, contraseña, credenciales de cliente y concesión de token de actualización, cada uno adecuado para diferentes usos.

Ventajas de la nueva API de Falcon:

- Auto servicio a través de la interfaz de usuario de Falcon
- Crear, modificar y eliminar clientes de API
- Restaurar secretos a través de la interfaz de usuario de Falcon
- Múltiples ID de cliente por CID
    - Definir alcance por cliente de API
    - Cambiar el alcance de la API de manera fluida
    - Control granular sobre los permisos de la API
    - Controlar el acceso de lectura o escritura para cada cliente de API
    - Registros de auditoría de clientes de API
    - Amplia documentación

- Conectividad de red: Necesitarás disponer de conectividad de red entre los distintos componentes de la infraestructura, para permitir compartir datos entre los distintos sistemas.

- Integración API: Se necesita tener una integración API entre los diferentes sistemas para permitir que los datos se transfieran entre ellos. Esto puede incluir la creación de integraciones personalizadas, el uso de conectores preconfigurados o el uso de estándares abiertos como las API REST.

- Medidas de seguridad: La infraestructura está protegida contra ciberataques, violaciones de datos y otras amenazas a la seguridad. Esto puede incluir la aplicación de medidas de seguridad como cortafuegos, sistemas de detección de intrusiones y controles de acceso.

- Mantenimiento y supervisión: Se debe tener un plan para mantener y supervisar la infraestructura, incluyendo actualizaciones regulares de software, copias de seguridad y supervisión de fallos del sistema, problemas de rendimiento e incidentes de seguridad.

3.3 Proceso de respuesta a incidentes

A continuación, se describe de manera puntual, el conjunto de pasos para poder abordar la respuesta a incidentes de forma metodológica y muy general. Es importante recordar que dependiendo del caso de uso estos pasos pueden variar significativamente por lo que se aconseja consultar fuentes adicionales para complementar cada incidente de seguridad en específico.

3.3.1 Preparación

Evaluación de riesgos: Evaluar los riesgos asociados a los ciberataques, incluida la probabilidad de que se produzca un ataque y el impacto potencial en la organización.

- Identificar vulnerabilidades: Existen diferentes, pero las más comunes son: Falta de formación de los empleados, las políticas de seguridad deficientes, el software obsoleto, así como malas prácticas durante configuraciones.
- Determinar la probabilidad de que un evento de seguridad ocurra: Teniendo en cuenta factores como el sector de la organización, la ubicación geográfica y las tendencias históricas.
- Determinar el impacto de que un evento de seguridad ocurra: Posible pérdida de datos, pérdidas financieras y daños a la reputación.
- Asignar calificaciones de riesgo: Asigna calificaciones de riesgo a cada amenaza y vulnerabilidad potenciales, teniendo en cuenta la probabilidad y el impacto.
- Desarrollar estrategias de mitigación: Para cada riesgo identificado, como la aplicación de políticas de seguridad, la formación de los empleados y la implementación de software antivirus.
- Supervisar y revisar: La eficacia de las estrategias de mitigación, y realizar los ajustes necesarios para garantizar que la organización permanezca protegida.

La identificación de activos es un paso crucial en la fase de preparación del proceso de respuesta a incidentes. A continuación, se indican algunos pasos que se pueden seguir para llevar a cabo la identificación de activos:

- Inventario de activos: Realice un inventario de todos los activos de la organización, incluidos el hardware, el software y los datos.

- Clasificar los activos: Cada activo dentro de una organización tiene una clasificación dependiendo de su valor y criticidad. Ejemplos: Datos confidenciales, información de clientes, dispositivos, registros financieros, infraestructura.

- Identificar vulnerabilidades: Identifique las vulnerabilidades asociadas a cada activo, como software obsoleto, contraseñas débiles y conexiones de red inseguras.

- Asignación de prioridades y criticidad: En un evento de seguridad esta información es relevante pues le permite a los analistas e ingenieros determinar el tiempo y esfuerzo adicional requerido para completar una investigación o priorizar una alerta.

- Desarrollar estrategias de protección: Desarrolle estrategias de protección para cada activo, como controles de acceso basado en roles, listas de acceso, cortafuegos, cifrado. Un concepto muy utilizando es Security In Depth lo cual dictamina que entre mayores y más diversas sean las medidas de protección serán mejores los resultados frente a los actores maliciosos.

Los siguientes son algunos ejemplos de activos que podrían descubrirse durante el proceso de identificación de activos:

- **Datos**: información sensible de clientes, registros financieros confidenciales, propiedad intelectual y otra información de propiedad.
- **Sistemas**: servidores, dispositivos de punto final (endpoints), dispositivos móviles y dispositivos de red.
- **Aplicaciones**: aplicaciones web, aplicaciones de escritorio y aplicaciones

móviles.

- **Redes**: redes de área local (LAN), redes de área amplia (WAN), redes privadas virtuales (VPN) y redes inalámbricas.
- **Personal**: empleados, contratistas y proveedores que tienen acceso a datos y sistemas sensibles.

Formación de los empleados: Se debe formar a los empleados sobre cómo identificar y alertar intentos de phishing, exploits, malware y proporcionarles las mejores herramientas para proteger la información cuidando la confidencialidad, integridad y disponibilidad.

- **Contenido**: Se debe desarrollar un programa de capacitación donde exista el contenido para la formación de concienciación de los empleados, incluyendo presentaciones, vídeos y ejercicios interactivos. Dicho material debe adaptarse a las necesidades específicas de la organización y debe abarcar temas como la forma de identificar programas maliciosos, los peligros de hacer clic en enlaces o archivos adjuntos sospechosos y la forma de como denunciar los intentos de comprometer la información.

- **Programe la formación**: Es necesario programar sesiones de entrenamiento (asistidas o autónomas dependiendo del contenido), periódicamente cuya duración y periodo sea a una hora que sea conveniente para los empleados, y avise con antelación para garantizar la máxima asistencia / aprovechamiento.

- **Impartición de la formación**: La formación debe ser distribuida utilizando diversos formatos, como sesiones presenciales, seminarios web o módulos de formación en línea, en la actualidad hay diversas plataformas gratuitas como YouTube, LinkedIn o TryHackMe que pueden mejorar la forma de aprender utilizando nuevos mecanismos de aprendizaje.

- **Refuerce la formación**: Refuerce la formación proporcionando recordatorios y actualizaciones continuas, como recordatorios semanales o mensuales por correo electrónico, carteles o folletos en zonas comunes.
- **Evalúe la eficacia**: Evalúe la eficacia de la formación de concienciación de los empleados recogiendo sus comentarios y realizando evaluaciones para medir su comprensión y retención del material.
- **Actualice la formación**: Actualice el contenido de la formación y los métodos de impartición según sea necesario basándose en los comentarios y los resultados de la evaluación para garantizar que sigue siendo pertinente y eficaz.

Plan de respuesta a incidentes: Este documento es primordial antes de comenzar con la operación, monitoreo, configuración y mejora de cualquier SOC. Un plan de respuesta a incidentes debe incluir detalles específicos para cada tipo de ataque en el que se describen las funciones y responsabilidades de todos los miembros de la operación, los canales de comunicación y los pasos más importantes que deben darse para contener y erradicar el incidente. Algunos de estos son:

- **Definir el alcance**: Esto significa definir hasta que momento el equipo SOC tiene la habilidad y posibilidad de remediar o recuperarse de un ataque real. Esto debe incluir los tipos de incidentes que se cubrirán, quién participará en la respuesta y de qué tipos recursos se dispondrá.

- **Establezca un equipo de respuesta a incidentes (CERT)**: Defina claramente las funciones y responsabilidades de cada miembro. Este equipo debe incluir miembros con habilidades esenciales que les permita comprender los sucesos durante un evento/incidente de seguridad. Una forma simple es definir equipos como con tareas como: (Inteligencia de amenazas, Administración de Vulnerabilidades, Pruebas de penetración, Administración de Identidades, Ingeniería, Monitoreo, etc).

- **Desarrolle procedimientos**: Para detectar, evaluar, contener y solucionar incidentes. Estos procedimientos deben cubrir los aspectos técnicos y no técnicos de la respuesta, como la comunicación con las partes interesadas y la realización de revisiones tras el incidente.

- **Poner a prueba el plan**: Mediante ejercicios prácticos y simulacros de incidentes. Esto ayuda a identificar cualquier laguna o debilidad en el plan y proporciona una oportunidad para perfeccionarlo y mejorarlo.

- **Actualice el plan**: En función de los cambios en el panorama de amenazas, la tecnología y las necesidades empresariales de la organización.

- **Obtener el apoyo de la** dirección: Obtener el apoyo de la dirección para el plan de respuesta a incidentes, incluyendo financiación, recursos y autoridad para aplicar el plan.

- **Comunicar el plan**: Comunique el plan de respuesta a incidentes a todos los empleados y partes interesadas, e imparte formación sobre cómo seguir los procedimientos del plan.

Herramientas y recursos: Asegúrese de que el equipo de respuesta a incidentes dispone de las herramientas y recursos necesarios para detectar y responder a los ataques de phishing, como filtros de correo electrónico, protección de puntos finales y herramientas de supervisión de la red.

- Sistemas de Información de Seguridad y Gestión de Eventos (SIEM): Los sistemas SIEM pueden ayudar a los especialistas en ciberseguridad a supervisar su red y sus sistemas para detectar actividades sospechosas y generar alertas cuando se detectan posibles incidentes de seguridad.

- Fuentes de información sobre amenazas: Los feeds de inteligencia de amenazas proporcionan información en tiempo real sobre las últimas amenazas y vulnerabilidades, lo que permite a las organizaciones identificar y mitigar proactivamente los posibles riesgos de seguridad.

- Exploradores de vulnerabilidades: Los escáneres de vulnerabilidades pueden ayudar a identificar vulnerabilidades en el software, los sistemas y las redes, que pueden abordarse antes de que puedan ser explotadas por los atacantes.

- Ejercicios de simulación de incidentes: Como ejercicios tabletop o ataques simulados, puede ayudar a identificar posibles puntos débiles en sus planes de respuesta a incidentes y a prepararse para incidentes del mundo real.

- Copias de seguridad y soluciones de recuperación: Las copias de seguridad periódicas y las soluciones de recuperación pueden ayudar a recuperarse rápidamente de un incidente de seguridad y minimizar el impacto en las operaciones comerciales.

Plan de comunicación: Establezca canales y protocolos de comunicación para informar y responder a un incidente de phishing, tanto dentro del equipo de respuesta a incidentes como con otras partes interesadas dentro de la organización.

Procedimientos de notificación de incidentes: Desarrolle procedimientos para informar y documentar incidentes de phishing, incluido el registro, el seguimiento y la notificación de incidentes.

Pruebas y validación: Probar y validar periódicamente el plan y los procedimientos de respuesta a incidentes para garantizar que son eficaces y están actualizados.

3.3.2 Análisis y detección

La fase de detección y análisis es un paso crítico en el proceso de respuesta a incidentes, ya que implica identificar y analizar el alcance y la gravedad de un ciberataque. A continuación, se indican algunos pasos que pueden seguirse para resolver eficazmente un incidente en esta fase:

- Alerta y notificación: Una vez detectado un posible incidente de seguridad, se debe alertar y notificar inmediatamente al equipo de respuesta a incidentes. Esto puede hacerse a través de una plataforma de respuesta a incidentes o mediante métodos de notificación manual como llamadas telefónicas o mensajes de texto.

La plataforma de respuesta a incidentes desempeña un papel crucial en este paso, ya que permite gestionar las alertas provenientes de otras herramientas basadas en reglas y umbrales predefinidos. Por ejemplo, la plataforma puede gestionar un conjunto de alertas de seguridad cuando se detectan diferentes tipos de comportamiento o patrones de ataque que afectan un mismo activo, como un ataque DDoS o una infección de malware.

También puede utilizarse para realizar un seguimiento del proceso de respuesta a incidentes, incluido el paso de alerta implementando un modelo (shift-left), que permite desahogar a los equipos cuando la volumetría de alertas es muy alta. La plataforma puede configurarse para enviar alertas a miembros específicos del equipo en función de sus funciones y responsabilidades. Por ejemplo, una infección de malware podría requerir la atención inmediata del equipo de respuesta a incidentes, mientras que un incidente menos crítico podría requerir únicamente la notificación al departamento de TI.

Además, es posible hacer un seguimiento del estado de cada incidente y garantizar que todos los miembros del equipo estén al tanto del incidente y tomen las medidas adecuadas. Así mismo, se puede documentar el proceso de respuesta a incidentes y generar informes para fines de gestión y cumplimiento normativo.

- Evaluación inicial: El equipo de respuesta a incidentes debe realizar una evaluación inicial para determinar el tipo y el alcance del incidente. Esto puede incluir la identificación de los sistemas y datos afectados, la evaluación de la gravedad del incidente y la recopilación de toda la información posible sobre el mismo.

- Análisis e investigación: El equipo de respuesta a incidentes debe realizar un análisis y una investigación detallados para determinar la causa raíz del incidente, el alcance de los daños y cualquier posible filtración de datos. Esto puede implicar el análisis de los registros del sistema, la revisión del tráfico de red y el examen de cualquier malware u otro código malicioso que pueda haberse utilizado en el ataque. La plataforma de respuesta a incidentes The Hive y junto con Cortex proporcionan potentes herramientas para el análisis y la investigación de incidentes de seguridad.

A continuación, se indican algunas formas de mejorar estas plataformas para llevar a cabo un proceso de análisis más eficaz:

- Integración con fuentes de inteligencia sobre amenazas: Para enriquecer automáticamente los datos entrantes. Esto puede ayudar a identificar indicadores maliciosos conocidos y acelerar el proceso de análisis.

- Automatización de tareas repetitivas: Como la búsqueda de IOC's en múltiples fuentes de datos. Esto puede ayudar a liberar tiempo de los analistas y permitirles centrarse en tareas de análisis más complejas.

- Colaboración entre analistas: Permiten que varios analistas colaboren en un incidente en tiempo real. Esto puede ayudar a acelerar el proceso de análisis y mejorar la precisión del análisis aprovechando la experiencia de varios analistas.

- Integración con otras herramientas de seguridad: Pueden integrarse otras herramientas de seguridad, como un SIEM donde ser observen logs de firewalls, IDS, IPS, logs de seguridad o administración de Windows para proporcionar una visión más completa de los incidentes de seguridad. Esto puede ayudar a identificar la causa raíz de un incidente y prevenir futuros incidentes.

Notificación: El equipo de respuesta a incidentes debe informar del incidente a la alta dirección, a las partes interesadas y a los organismos reguladores, según proceda. Esto puede incluir un análisis detallado del incidente, un resumen de los pasos dados para contener y mitigar el ataque, y recomendaciones para mejorar la seguridad de la organización y prevenir futuros incidentes. Normalmente esto se realiza mediante los canales de comunicación previamente definidos en la etapa de preparación, utilizando plantillas o formatos que faciliten el envío de la información, sean claros y permitan que los que la reciban entiendan la razón de la posible urgencia e impacto de dichas alertas.

3.3.3 Contención, Erradicación y recuperación

Aislamiento y contención: El equipo de respuesta a incidentes debe trabajar para aislar y contener los sistemas afectados para evitar que el ataque se propague aún más. Esto puede implicar deshabilitar el acceso a la red de los sistemas afectados, desconectarlos de la red o apagarlos por completo.

Métodos para contener un incidente:

- Aislar los sistemas afectados: Se trata de desconectar de la red los sistemas afectados para evitar que el incidente se propague a otros sistemas. Por ejemplo, si un sistema está infectado con malware, puede aislarse desconectándolo de la red o desactivando su conexión de red.

- Implementar la segmentación de la red: Al dividir la red en segmentos más pequeños y aislados, resulta más fácil contener un incidente. Si se produce un incidente en un segmento, quedará contenido en él y no se propagará a otros segmentos.

- Bloqueo del tráfico malicioso: El tráfico de red identificado como malicioso puede bloquearse mediante cortafuegos o sistemas de detección/prevención de intrusiones (IDS/IPS). Esto impide que el incidente se comunique con su servidor de mando y control (C2) o se propague a otros sistemas.

- Utilización de EDR's: Las herramientas de protección de puntos finales, como el antivirus de nueva generación, pueden ayudar a contener un incidente detectando y bloqueando la actividad maliciosa en sistemas individuales. Algunas acciones que estos programas pueden emplear son:

    - Eliminación del proceso en tiempo real.
    - Cuarentena de archivos.
    - Bloqueo de operaciones en memoria y sistema de archivos.

- Utilizar la virtualización o el sandboxing: La virtualización o el sandboxing pueden utilizarse para crear entornos aislados en los que el incidente pueda analizarse y contenerse de forma segura sin arriesgarse a dañar otros sistemas. En un caso particular de ransomware, es necesario emplear este tipo de técnicas para determinar el tipo y de que forma se puede evitar su propagación.

- Parches y actualizaciones: mantener los sistemas actualizados con los últimos parches de seguridad puede prevenir la explotación de vulnerabilidades conocidas.

- Políticas de contraseñas: implementar políticas de contraseñas fuertes y cambiarlas periódicamente puede prevenir el acceso no autorizado a sistemas y reducir la propagación de un incidente.

Remediación y recuperación: Una vez que el incidente ha sido contenido y se ha determinado el alcance del ataque, el equipo de respuesta a incidentes debe trabajar para remediar cualquier vulnerabilidad o debilidad que haya sido explotada en el ataque. También deben trabajar para recuperar cualquier dato o sistema que se haya visto afectado por el ataque, asegurándose de que son totalmente operativos y seguros antes de volver a su uso normal.

- Pasos para identificar y eliminar la causa raíz del incidente:
  - Revisión del incidente: El primer paso es revisar la información recopilada durante las fases de detección y análisis del incidente. Esto ayudará a entender los síntomas y a identificar los posibles puntos de entrada o de propagación del incidente.

  - Análisis de los sistemas afectados: Se debe analizar detalladamente los sistemas o dispositivos afectados para identificar cualquier actividad sospechosa o cambios recientes. Se puede utilizar herramientas de análisis de registro, monitoreo de red y análisis de malware para obtener información adicional. Un ejemplo en concreto nace con las herramientas

llamadas File Integrity Monitoring (FIM), ya que generan un evento de seguridad cuando el contenido/atributo de un archivo o ruta es modificado al especificarse en una regla en concreto.

- Análisis de los registros de auditoría: Se deben revisar los registros de auditoría de los sistemas afectados para buscar cualquier actividad inusual o sospechosa. Esto puede proporcionar información valiosa sobre el momento y la naturaleza del ataque.

- Identificación de la causa raíz: Una vez que se haya revisado toda la información disponible, se puede comenzar a identificar la causa raíz del incidente. Se puede utilizar técnicas para profundizar en el análisis y descubrir las causas fundamentales del incidente.

- Eliminación de la causa raíz: Una vez que se ha identificado la causa raíz del incidente, se deben tomar medidas para eliminarla. Esto puede incluir la aplicación de parches de seguridad, la eliminación de software malicioso o la corrección de vulnerabilidades.

- Monitoreo continuo: Después de haber eliminado la causa raíz del incidente, es importante monitorear de forma continua los sistemas afectados para asegurarse de que el incidente no vuelva a ocurrir.

- Estrategias para eliminar todo rastro del incidente de los sistemas afectados

  - Realizar una revisión exhaustiva del sistema: Para identificar cualquier rastro del incidente, se debe realizar una revisión exhaustiva del sistema. Esto implica revisar todos los registros de actividad, los registros del sistema, las bases de datos y cualquier otro lugar donde el incidente pueda haber dejado huellas.

- Restaurar desde copias de seguridad: Si se sospecha que el incidente ha afectado significativamente los sistemas, se pueden restaurar desde copias de seguridad previas al incidente. Esto eliminará cualquier rastro del incidente, pero también puede resultar en la pérdida de datos.

- Utilizar herramientas de eliminación de malware: Si el incidente fue causado por malware, se pueden utilizar herramientas de eliminación de malware para limpiar los sistemas afectados. Estas herramientas escanearán el sistema en busca de malware y lo eliminarán.

- Realizar un análisis forense: Si el incidente fue grave, puede ser necesario realizar un análisis forense para identificar la causa raíz del incidente y cualquier rastro que haya dejado. Esto puede ser útil para eliminar cualquier rastro del incidente y prevenir futuros incidentes similares.

- Cambiar credenciales: Si se sospecha que los atacantes han obtenido credenciales, es importante cambiar todas las contraseñas y credenciales de los sistemas afectados para eliminar cualquier posible acceso no autorizado.

- Cómo validar que el incidente se ha erradicado por completo:

  - Pruebas de penetración: se pueden realizar pruebas de penetración para asegurarse de que no existen vulnerabilidades que puedan ser explotadas. Esto se puede hacer internamente o mediante una empresa de seguridad externa.

  - Actualizaciones de seguridad: se deben aplicar todas las actualizaciones de seguridad necesarias para prevenir futuros incidentes. Esto puede incluir actualizaciones de software, parches de seguridad y cambios en la configuración de seguridad.

- Cómo restaurar los sistemas y los datos a su estado anterior al incidente

    - Restauración de datos: Restaure los datos a partir de las copias de seguridad más recientes o snapshots (copias de imágenes de un sistema operativo). Asegúrese de que la integridad de los datos se mantenga durante la transferencia. Es necesario utilizar métodos de almacenamiento seguros y encriptados para proteger los datos.

    - Restauración de sistemas: Una vez que se han restaurado los datos, restaure los sistemas afectados a su estado anterior al incidente. Esto puede implicar la reinstalación del sistema operativo, las aplicaciones y las configuraciones del sistema. En un plan de recuperación ante desastres es común definir dos métricas asociada a la cantidad máxima de perdida de datos, Recovery Point Objective (RPO) y la cantidad máxima de tiempo que un sistema puede estar no disponible, Recovery Time Objective (RTO).

    - Pruebas de funcionamiento: Una vez que se han restaurado los sistemas y datos, realice pruebas exhaustivas para asegurarse de que todo funciona como debería. Asegúrese de que las aplicaciones, servicios y sistemas estén disponibles y funcionen correctamente.

- Estrategias para priorizar y programar los esfuerzos de recuperación:

    - Identificar los activos críticos: En primer lugar, es importante identificar los activos críticos de la organización, como sistemas, aplicaciones, datos y recursos clave. Estos activos deben ser priorizados para la recuperación y restauración.

    - Establecer objetivos de recuperación: Los objetivos de recuperación deben ser claros y específicos, para que los equipos de respuesta sepan exactamente lo que se espera de ellos. Se deben establecer objetivos para

la recuperación de los activos críticos, así como para la recuperación general del sistema.

- Asignar prioridades: Es importante asignar prioridades a los esfuerzos de recuperación. Los activos críticos deben ser restaurados primero, seguidos por los activos menos críticos.

- Establecer un orden de trabajo: Es importante establecer un orden de trabajo para los equipos de recuperación. Esto asegurará que los esfuerzos de recuperación se realicen en el orden correcto y que los recursos se utilicen de manera eficaz.

- Establecer plazos: Es importante establecer plazos claros para la recuperación y restauración. Esto asegurará que los esfuerzos de recuperación se realicen de manera oportuna y que se minimice el tiempo de inactividad.

- Documentar el proceso: Es importante documentar todo el proceso de recuperación. Esto incluye los objetivos de recuperación, la asignación de prioridades, el orden de trabajo y los plazos. La documentación detallada ayudará a la organización a mejorar sus procesos de recuperación en el futuro.

3.3.4 Actividad post-incidente

El objetivo es realizar un análisis exhaustivo del incidente e identificar áreas de mejora en el plan de respuesta a incidentes. Esta fase es fundamental para evitar que se produzcan incidentes similares en el futuro y para reforzar la postura general de ciberseguridad de la organización.

Los siguientes son algunos pasos clave en la fase de lecciones aprendidas de la respuesta a incidentes:

- Realizar una revisión posterior al incidente: Es necesario recopilar toda la información relevante sobre el incidente, incluyendo cómo ocurrió (vectores de ataque, identificación de IoC's o logs).

    - Reconstruir los sucesos paso a paso, desde el inicio hasta el final para ello es importante aprender a diferenciar entre el momento de inicio del incidente, así como el tiempo que le tomo a los sistemas y analistas determinar que se trata de una amenaza real.

- ¿Cómo se gestionó? (Determinar la clasificación del tipo de amenaza, análisis de los tiempos de reconocimiento, investigación, escalación y respuesta), así como las medidas se tomaron para remediarlo.

    - Identificar causas reales normal son provocados por fallos técnicos o errores de desarrollo o humanos y vulnerabilidades.
    - Evaluar el desempeño de los integrantes del equipo CERT de acuerdo con su rol una vez identificada la amenaza, así como el plan de respuesta a incidentes, playbooks desarrollados para ese evento en específico.

Esta información debe utilizarse para crear un informe detallado que pueda compartirse con las principales partes interesadas. Este informe es normalmente conocido como Reporte Causa-Raíz.

- Analizar el incidente: Revise el informe del incidente e identifique los puntos débiles del plan de respuesta al incidente o las áreas en las que se podría haber mejorado la respuesta. Busque patrones o tendencias en los datos del incidente para identificar posibles áreas de mejora.

- Identifique áreas de mejora: Basándose en el análisis, elabore una lista de mejoras recomendadas para el plan de respuesta a incidentes, incluidos cambios en las políticas, los procedimientos y las tecnologías.

- Priorizar las mejoras: Desarrollar un plan para aplicar las mejoras recomendadas, dando prioridad a las que tendrán mayor impacto en la mejora de la respuesta a incidentes y en la reducción de la probabilidad de futuros incidentes.

- Aplicar las mejoras: Aplicar las mejoras recomendadas y actualizar el plan de respuesta a incidentes en consecuencia. Esto puede implicar la revisión de políticas y procedimientos, la formación adicional del personal o la inversión en nuevas tecnologías.

- Probar el plan de respuesta a incidentes: Pruebe periódicamente el plan de respuesta a incidentes para asegurarse de que es eficaz y está actualizado. Esto puede implicar la realización de incidentes simulados para identificar áreas de mejora.

Capítulo 4.- Resultados

En esta sección se presentan los resultados obtenidos tras la implementación de la metodología propuesta, integrando The Hive Project con herramientas avanzadas de ciberseguridad. Los resultados reflejan la eficacia de la solución en el contexto del laboratorio de ciberseguridad y su aplicabilidad en equipos SOC. Se evalúan aspectos clave como la mejora en los tiempos de respuesta, los beneficios de la integración exitosa con herramientas de Threat Intelligence y la efectividad de las estrategias de automatización implementadas. Estos resultados se analizan con base en indicadores para medir el impacto y la viabilidad de la solución.

4.1 Casos de Uso

En un estudio realizado durante el 2024, se abordaron 40 eventos de seguridad diferentes de cuatro diferentes casos de uso relacionados a correos de Phishing, Impersonificación de Dominio, Impossible Travel Activity y Detección de Malware en endpoints basado en IoC's. Utilizando 2 métodos (A – Utilizando The Hive Project, B – Utilizando las plataformas y procesos convencionales). A continuación, se describen:

1. Correos de Phishing

Este caso de uso se centra en la detección y respuesta a correos electrónicos diseñados para engañar a los usuarios y obtener información confidencial, como credenciales, datos bancarios o información personal.

Descripción del evento: Los correos de phishing suelen contener enlaces maliciosos o archivos adjuntos que redirigen a sitios fraudulentos o ejecutan malware.

Herramientas involucradas:

- Microsoft 365 Defender para analizar el contenido del correo, detectar enlaces maliciosos y bloquear remitentes sospechosos.

- MISP y VirusTotal para identificar indicadores de compromiso (IoC) asociados a los correos.

Impacto esperado: Evitar la exposición de credenciales y reducir la probabilidad de comprometer datos sensibles.

2. Impersonificación de Dominio

Este caso aborda los intentos de suplantación de identidad mediante la creación de dominios similares al de una organización legítima con el objetivo de engañar a empleados, socios o clientes.

Descripción del evento: Los atacantes registran dominios con ligeras variaciones (typosquatting) y los utilizan para enviar correos fraudulentos o crear sitios web maliciosos.

Herramientas involucradas:

- SOC Radar para monitorear el registro de dominios similares al de la organización y detectar actividades sospechosas.
- The Hive Project para correlacionar estos eventos con otros incidentes relacionados.

Impacto esperado: Proteger la reputación de la organización y prevenir ataques de phishing o fraude asociados a la suplantación de dominio.

3. Impossible Travel Activity

Este caso se enfoca en detectar actividades inusuales de inicio de sesión que, por lógica geográfica o temporal, no pueden ser realizadas por un usuario legítimo.

Descripción del evento: Un usuario accede desde una ubicación geográfica y, en un corto periodo, realiza otro acceso desde una ubicación físicamente imposible de alcanzar en ese tiempo.

Herramientas involucradas:

- Microsoft 365 Defender for Identity para monitorear patrones de acceso sospechosos.
- The Hive Project y MISP para enriquecer el evento con datos de contexto, como direcciones IP y geolocalización.

Impacto esperado: Identificar y bloquear cuentas comprometidas, minimizando el riesgo de movimientos laterales o accesos no autorizados.

4. Detección de Malware en Endpoint Basado en IoCs

Este caso se centra en la identificación y respuesta a malware detectado en endpoints mediante el uso de Indicadores de Compromiso.

Descripción del evento: Los endpoints reportan actividades maliciosas, como archivos ejecutables sospechosos, conexiones con dominios maliciosos o comportamientos inusuales.

Herramientas involucradas:

- CrowdStrike Falcon para detectar actividades maliciosas en tiempo real.
- VirusTotal y AbuseIP para analizar IoCs asociados al malware detectado.
- The Hive Project para gestionar y centralizar la respuesta al incidente.

Impacto esperado: Contener y erradicar el malware antes de que se propague, reduciendo el impacto en la operación del endpoint comprometido.

4.2 Conclusiones

Los resultados obtenidos tras la implementación de la metodología propuesta reflejan mejoras significativas en la precisión de la clasificación de eventos de seguridad y en la eficiencia operativa del equipo SOC. A continuación, se destacan los principales hallazgos:

Resultados Clave Basados en Métricas

La tabla de métricas clave evidencia una mejora significativa en los tiempos promedio relacionados con la gestión y respuesta a incidentes de seguridad:

Métrica	Resultado Inicial (Promedio)	Resultado Final (Promedio)	Mejora (%)
MTTA	12 minutos	3 minutos	75%
MTTI	45 minutos	23 minutos	48.89%
MTTE	55 minutos	26 minutos	52.37%
MTTR	1 hora y 20 minutos	40 minutos	50%

Tabla 5. Métricas de rendimiento durante las fases de respuesta a incidentes (promedio, observadas) durante el experimento.

Estas métricas demuestran una notable reducción en los tiempos de respuesta, destacando:

- MTTA (Tiempo Promedio para Reconocer): Reducción del 75%, lo que refleja la capacidad mejorada para identificar incidentes rápidamente tras su detección.
- MTTI (Tiempo Promedio para Investigar): Reducción del 48.89%, gracias al enriquecimiento automatizado de datos y al uso de flujos de trabajo más eficientes.
- MTTE (Tiempo Promedio para Escalar): Reducción del 52.37%, lo que evidencia procesos de escalación más claros y automatizados.

- MTTR (Tiempo Promedio para-Responder/Remediar): Reducción del 50%, mejorando significativamente la capacidad de mitigación.

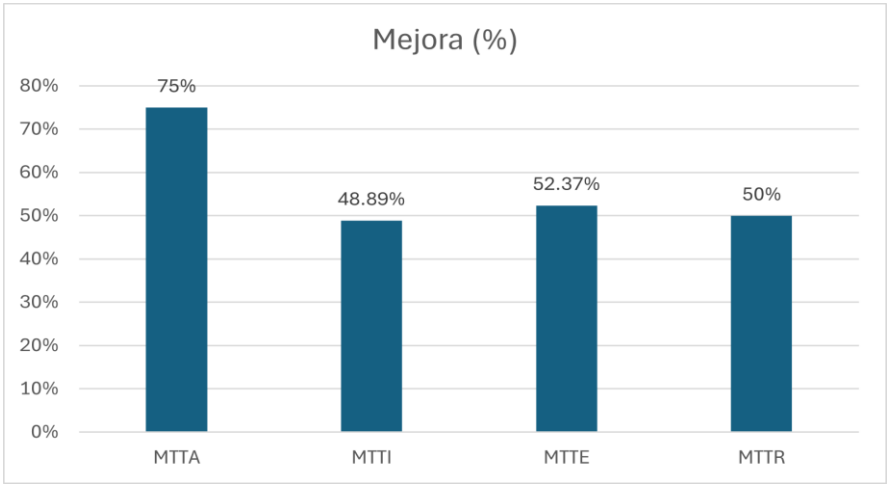
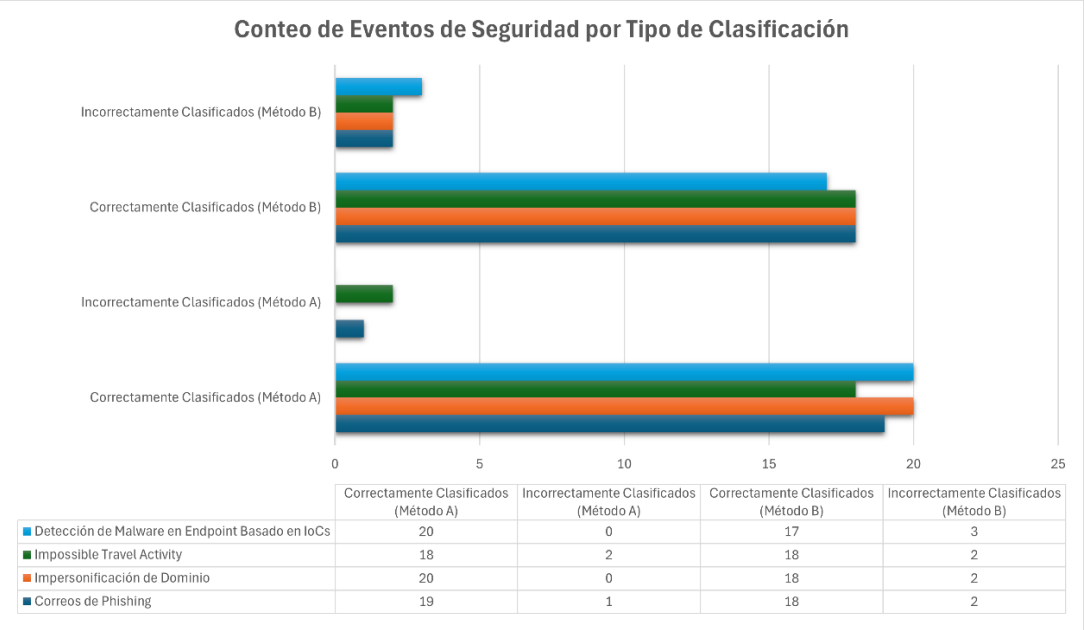


Fig. 29 *Gráfica de barras que muestra los porcentajes de mejora con respecto a cada métrica de evaluación de rendimiento en tiempo.*

El siguiente gráfico muestra un análisis comparativo entre dos métodos utilizados para clasificar eventos de seguridad. Los tipos de eventos evaluados incluyen detección de malware en endpoints, actividad de viaje imposible, suplantación de dominio e intentos de phishing.

- El Método A alcanzó una tasa de clasificación correcta superior, destacando en escenarios como "Detección de Malware" e "Impersonificación de Dominio", donde todos los eventos fueron correctamente identificados.
- El Método B presentó una mejora en ciertos aspectos operativos, aunque con un ligero incremento en las clasificaciones incorrectas.
- En total, el desempeño general fue optimizado, con una precisión promedio del 95% en eventos clasificados correctamente al implementar las herramientas de automatización y enriquecimiento.



	Correctamente Clasificados (Método A)	Incorrectamente Clasificados (Método A)	Correctamente Clasificados (Método B)	Incorrectamente Clasificados (Método B)
Detección de Malware en Endpoint Basado en IoCs	20	0	17	3
Impossible Travel Activity	18	2	18	2
Impersonificación de Dominio	20	0	18	2
Correos de Phishing	19	1	18	2

Fig. 30 *Gráfica de barras que muestra el conteo de eventos de eventos de seguridad con respecto a aquellos que fueron correcta e incorrectamente clasificados por tipo de métodos.*

4.3 Trabajo Futuro

La implementación de la metodología no solo permitió una mejora cuantitativa en los tiempos y la precisión de clasificación, sino que también incrementó la efectividad del equipo SOC al permitirles centrarse en incidentes de mayor prioridad, minimizando esfuerzos en falsos positivos.

Con base en los resultados obtenidos se continuara trabajando en una metodología que permita el correcto análisis de los comentarios y eventos de seguridad analizados por el equipo SOC centrándose en enfoque que funcione diariamente tomando en cuenta características relativas como (tipo de clasificación, numero de eventos analizados a un mismo caso, calidad en la descripción durante la investigación), dichas métricas será evaluadas por lideres de equipo y compartirán retroalimentación dentro de la plataforma para que el equipo de expertos pueda mejorar su nivel de análisis así como encontrar áreas de oportunidad en las que se necesiten reforzar ciertos conocimientos.

Por otro lado, se plantea mejorar las acciones automáticas utilizando los playbooks dentro de Falcon Fusion (plataforma SOAR de Crowdstrike), para disminuir las interacciones de analistas dentro de la plataforma en tareas rudimentarias como asignación de alerta, documentación, búsqueda de información sobre amenazas o indicadores de compromiso clave, contención del equipo o acciones de mitigación como eliminación de archivos maliciosos de forma remota, desplegar procesos de **análisis y extracción de artefactos Kroll (KAPE)** durante incidentes mejorando así las fases de detección, investigación y contención del proceso de respuesta a incidentes.

Bibliografía

1. PricewaterhouseCoopers. (2024). Encuesta Digital Trust Insights 2024, México | PwC MX. PwC. https://www.pwc.com/mx/es/ciberseguridad/digital-trust.html

2. Rojas, A. (2024, marzo 14). México, uno de los países más expuestos a la inseguridad digital en 2024. Expansión. https://expansion.mx/opinion/2024/03/14/mexico-uno-de-los-paises-mas-expuestos-a-la-inseguridad-digital-en-2024

3. Riquelme, R. (2024, julio 23). Una de cada tres organizaciones en América Latina ha sido víctima de un ciberataque: ESET. El Economista. https://www.eleconomista.com.mx/tecnologia/Una-de-cada-tres-organizaciones-en-America-Latina-ha-sido-victima-de-un-ciberataque-ESET-20240723-0034.html

4. CyberEdge Group. (2022). 2022 Cyberthreat Defense Report. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf

5. Calderón, C. (2022, junio 9). México 'clientazo' de los ciberataques: Crecen 42% amenazas por internet. El Financiero. https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

6. Ruiz, V. (2024, enero 4). Ciberseguridad en México 2024, SILIKN. Revista Más Seguridad. https://www.revistamasseguridad.com.mx/ciberseguridad-en-mexico-2024-silikn/

7. International Data Corporation. (2023, marzo 8). *IDC Latin America presentó las principales tendencias de los segmentos de TI y Telecom y las oportunidades para el mercado regional. IDC. https://www.idc.com/getdoc.jsp?containerId=prLA50472023*

8. Maia, E., Sousa, N., Oliveira, N., Wannous, S., Sousa, O., & Praça, I. (2022). SMS-I: Intelligent Security for Cyber–Physical Systems. En Information (Vol. 13, Issue 9, p. 403). MDPI AG. DOI: https://doi.org/10.3390/info13090403

9. Bartwal, U., Mukhopadhyay, S., Negi, R., & Shukla, S. (2022). Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. En 2022 IEEE Conference on Dependable and Secure Computing (DSC). 2022 IEEE Conference on Dependable and Secure Computing (DSC). IEEE. DOI: https://doi.org/10.1109/dsc54232.2022.9888808

10. Chamiekara, G. W. P., Cooray, M. I. M., Wickramasinghe, L. S. A. M., Koshila, Y. M. S., Abeywardhana, K. Y., & Senarathna, A. N. (2017). AutoSOC: A low budget flexible security operations platform for enterprises and organizations. National Information Technology Conference (NITC). 2017 National Information Technology Conference (NITC). IEEE. DOI: https://doi.org/10.1109/nitc.2017.8285644

11. Bilali, V.-G., Kosyvas, D., Theodoropoulos, T., Ouzounoglou, E., Karagiannidis, L., & Amditis, A. (2022). IRIS Advanced Threat Intelligence Orchestrator- A Way to Manage Cybersecurity Challenges of IoT Ecosystems in Smart Cities. En Internet of Things (pp. 315–325). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-031-20936-9_25

12. Islam, C., Babar, M. A., & Nepal, S. (2020). Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform. En Software Architecture (pp. 165–181). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-58923-3_11

13. Dwivedi, S., Rajendran, B., Akshay, P.V., Acha, A., Ampatt, P., Sudarsan, S.D. (2025). IntelliSOAR: Intelligent Alert Enrichment Using Security Orchestration Automation and Response (SOAR). In: Patil, V.T., Krishnan, R., Shyamasundar, R.K. (eds) Information Systems Security. ICISS 2024. Lecture Notes in Computer Science, vol 15416. Springer, Cham. https://doi.org/10.1007/978-3-031-80020-7_27

14. Christian, J., Paulino, L., de Sá, A.O. (2022). A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response. In: Su, C., Gritzalis, D., Piuri, V. (eds) Information Security Practice and Experience. ISPEC 2022. Lecture Notes in Computer Science, vol 13620. Springer, Cham. https://doi.org/10.1007/978-3-031-21280-2_7

15. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/cyber_security

16. Unión Internacional de Telecomunicaciones. (2008). Cybersecurity Definition. Recuperado en 2024, de https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

17. Cybersecurity and Infrastructure Security Agency (CISA). (2021). What is cybersecurity? Recuperado en 2024, de https://www.cisa.gov/news-events/news/what-cybersecurity

18. Department of Homeland Security (DHS). (2018). Computer Security Resource Center. Recuperado de https://www.dhs.gov/cybersecurity

19. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/confidentiality

20. Organización Internacional de Normalización (ISO). (2013). ISO/IEC 27001:2013 Information Security Management Systems. Ginebra: ISO.

21. Stallings, W., & Brown, L. (2012). Computer Security: Principles and Practice (3rd ed.). Pearson.

22. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/integrity

23. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Guide to vulnerability reporting for the Americas' election administrators. Retrieved from https://www.cisa.gov/sites/default/files/2023-07/7_PUB_Guide-vulnerability-reporting-americas-election-admins_combined508.pdf

24. Ross Anderson. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

25. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/availability

26. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/threat

27. Cybersecurity and Infrastructure Security Agency (CISA). (2021). Cyber Threats and Advisories. Recuperado de https://www.cisa.gov

28. European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape Report. Recuperado de https://www.enisa.europa.eu

29. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/vulnerability

30. Forum of Incident Response and Security Teams (FIRST). (2021). Common Vulnerability Scoring System (CVSS) v3.1 Specifications Document. Recuperado de https://www.first.org/cvss

31. Open Web Application Security Project (OWASP). (2021). Top 10 Web Application Security Risks. Recuperado de https://owasp.org

32. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/event

33. Trend Micro. (2020). Syslog Parsing. Deep Security Help Center. Retrieved March 4, 2023, from https://help.deepsecurity.trendmicro.com/11_2/aws/Events-Alerts/syslog-parsing.html

34. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

35. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

36. National Institute of Standards and Technology (NIST). (2020). Computer Security Resource Center. Recuperado de https://csrc.nist.gov/glossary/term/incident

37. International Organization for Standardization. (2016). ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. ISO. Recuperado de https://www.iso.org/standard/60803.html

38. ENISA. (2023). Incident Response Planning. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/

39. MITRE. (2023). MITRE ATT&CK Knowledge Base on APT Groups. MITRE. Recuperado de https://attack.mitre.org/groups/

40. Mandiant. (2022). APT Groups: Tracking Nation-State Cyber Threats. Mandiant. Recuperado de https://www.mandiant.com/resources/apt-groups

41. Verizon. (2023). 2023 Data Breach Investigations Report (DBIR). Verizon. Recuperado de https://www.verizon.com/business/resources/reports/dbir/

42. National Institute of Standards and Technology. (2020). Zero Trust Architecture (SP 800-207). NIST. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-207/final

43. CISA. (2022). Understanding Script Kiddies and Their Impact on Cybersecurity. Cybersecurity and Infrastructure Security Agency. Recuperado de https://www.cisa.gov/publication/understanding-script-kiddies-and-their-impact-cybersecurity

44. Europol. (2023). Cybercrime Threats: Ransomware, Phishing & Financial Fraud. Europol. Recuperado de https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cybercrime-threats

45. EC-Council. (2023). Certified Ethical Hacker (CEH) Certification. EC-Council. Recuperado de https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

46. Gartner. (2023). Shadow IT: Managing Risks in a Decentralized Workforce. Gartner. Recuperado de https://www.gartner.com/en/information-technology/glossary/shadow-it

47. International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Controls. ISO. Recuperado de https://www.iso.org/standard/75652.html

48. National Cyber Security Centre. (2023). Industrial Espionage and Cyber Threats to Businesses. NCSC UK. Recuperado de https://www.ncsc.gov.uk/section/advice-guidance/all-topics

49. IBM. (2023). Security controls. IBM. Recuperado en Julio, 2024, de https://www.ibm.com/mx-es/topics/security-controls

50. IBM. (2023). What is Ransomware?. Recuperado de https://www.ibm.com/topics/ransomware

51. Kaspersky Lab. (2023). What is Malware? Types and Examples. Recuperado de https://www.kaspersky.com/resource-center/threats/malware

52. Symantec (Broadcom). (2022). Fileless Malware: The Invisible Threat. Recuperado de https://www.symantec.com/blogs/threat-intelligence/fileless-malware

53. Verizon Business. (2023). Data Breach Investigations Report (DBIR) 2023. Recuperado de https://www.verizon.com/business/resources/reports/dbir/

54. **Microsoft Corporation.** (2023). *Identity and Access Management in Azure Active Directory*. Recuperado de https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-and-access-management

55. Gartner, Inc. (2023). Cloud Security Risks and Best Practices. Recuperado de https://www.gartner.com/en/documents/4008676

56. Open Web Application Security Project (OWASP). (2023). API Security Top 10. Recuperado de https://owasp.org/www-project-api-security/

57. **Cloud Security Alliance (CSA).** (2023). *Top Threats to Cloud Computing: The Egregious 11*. Recuperado de https://cloudsecurityalliance.org/research/top-threats/

58. **CrowdStrike.** (2023). *Global Threat Report 2023: Adversary Tradecraft and the Importance of Speed*. Recuperado de https://www.crowdstrike.com/resources/reports/global-threat-report/

59. FireEye (Mandiant). (2023). Advanced Persistent Threats (APT) Groups. Recuperado de https://www.mandiant.com/resources/apt-groups

60. Palo Alto Networks. (2023). What is Command and Control (C2) in Cybersecurity? Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-command-and-control

61. Okta, Inc. (2023). Identity Threat Report 2023: The State of Identity Security. Recuperado de https://www.okta.com/resources/identity-threat-report-2023/

62. Fortinet. (2023). IoT Security: Challenges and Solutions. Recuperado de https://www.fortinet.com/resources/cyberglossary/iot-security

63. Proofpoint, Inc. (2023). Human Factor Report 2023: The Psychology of Cybercrime. Recuperado de https://www.proofpoint.com/us/resources/threat-reports/human-factor

64. **Europol.** (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Recuperado de https://www.europol.europa.eu/crime-areas-and-trends/iocta

65. NIST. (2023). Computer Security Incident Handling Guide. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

66. Check Point Software Technologies. (2024). ¿Qué es una Evaluación de Riesgos de ciberseguridad? Recuperado de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-cyber-security-risk-assessment/

67. IBM. (2024). ¿Qué es una prueba de penetración? Recuperado de https://www.ibm.com/mx-es/topics/penetration-testing

68. IT Governance. (2025). Cumplimiento y pruebas de penetración. Recuperado de https://www.itgovernance.eu/es-es/compliance-and-penetration-testing-es

69. IBM. (2024). ¿Qué es SIEM y cómo mejora la seguridad de la información? IBM Security. Recuperado de https://www.ibm.com/think/topics/siem

70. CrowdStrike. (2024). Log files: Definition, types, and importance in cybersecurity. CrowdStrike. Recuperado de https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/log-file/

71. Proven Data. (2025). What is metadata forensics & how is it used in investigations?. Proven Data Forensics. Recuperado de https://www.provendata.com/blog/what-is-metadata-forensics/

72. Tenable, Inc. (2024). Nessus Professional: The Industry Standard for Vulnerability Assessment. Tenable. Recuperado de https://es-la.tenable.com/products/nessus/nessus-professional

73. Microsoft. (2024, 18 de octubre). Conozca el lenguaje de consulta de búsqueda avanzada. Microsoft Learn. Recuperado de https://learn.microsoft.com/es-es/defender-xdr/advanced-hunting-query-language

74. MITRE. (2024). MITRE ATT&CK®: A knowledge base of adversary tactics and techniques based on real-world observations. Recuperado de https://attack.mitre.org/

75. Palo Alto Networks. (2024). What is SOAR? Security Orchestration, Automation, and Response Explained. Palo Alto Networks Cyberpedia. Recuperado el 31 de enero de 2025, de https://www.paloaltonetworks.com/cyberpedia/what-is-soar

76. Palo Alto Networks. (2020). Managing a Remote SOC: Playbooks for Monitoring Remote User Activity. Palo Alto Networks Blog. Recuperado el 31 de enero de 2025, de https://www.paloaltonetworks.com/blog/2020/04/cortex-monitoring-remote-user-activity/

77. Cybersecurity and Infrastructure Security Agency (CISA). (2022). Incident Response Plan Basics. Recuperado de https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

78. **National Cyber Security Centre (NCSC).** (2021). *Preventing Lateral Movement*. Recuperado de https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

79. Palo Alto Networks. (s.f.). ¿Qué es la segmentación de la red? Cómo funciona y su importancia en la ciberseguridad. Palo Alto Networks Cyberpedia. Recuperado de https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation

80. CrowdStrike. (2020). How to Create Custom Rules with CrowdStrike [Video]. YouTube. Recuperado de https://www.youtube.com/watch?v=75E_edpAmp4

81. Leonard, J. (2017, 19 de junio). TheHive, Cortex and MISP: How They All Fit Together. TheHive Project Blog. Recuperado de https://blog.thehive-project.org/2017/06/19/thehive-cortex-and-misp-how-they-all-fit-together/

82. SOCRadar. (2024). How to Use SOCRadar Integrations? SOCRadar® Cyber Intelligence Inc. Recuperado el 31 de enero de 2025, de https://socradar.io/how-to-use-socradar-integrations/

83. Dell Technologies. (2024). ¿Qué es la plataforma CrowdStrike Falcon?. Dell Support. Recuperado el 31 de enero de 2025, de https://www.dell.com/support/kbdoc/es-mx/000126839/que-es-crowdstrike

84. CrowdStrike. (2020). Accessing the CrowdStrike API [Video]. YouTube. Recuperado de https://www.youtube.com/watch?v=9vOQlIzNuWU&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs

Apéndices

A.- Implementación de The hive Project y uso

Google Cloud Platform

Google Cloud Platform es la infraestructura masiva y en la nube de Google, que opera el tráfico y el trabajo de todos los usuarios de Google. Sus servicios se basan principalmente en la creación e implementación de aplicaciones y sitios web con Google.

Destaca por su amplia gama de servicios, como Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) o Software como Servicio (SaaS). Cuenta con soluciones para Bases de Datos, almacenamiento en la nube y networking. Además, los clientes de GCP pueden acceder a la consola en la nube gratuita.

Compute Engine

Es la IaaS (Infraestructura de Servicios) de Google. Permite la creación bajo demanda de máquinas virtuales en la nube. Se destaca por construir un Centro de Datos en minutos y asegurar la infraestructura con Disaster Recovery.

High cost of infrastructure

Es un PaaS (Platform as a service) que permite la creación de aplicaciones con Google como administrador de la infraestructura. Su autogestión lo hace más escalable y con mejores resultados.

Kubernetes Engine

Mejor conocido como Google Kubernetes Engine (GKE), es un servicio administrado de Google Cloud que facilita la implementación, administración y escalado de aplicaciones en contenedores usando Kubernetes.

Características clave de Kubernetes (y GKE):

- Orquestación de contenedores: Kubernetes automatiza la implementación, administración y escalado de aplicaciones en contenedores, lo que mejora la eficiencia operativa.

- Clusters: Kubernetes organiza aplicaciones en contenedores en clusters. Un cluster es un conjunto de nodos (máquinas virtuales) que ejecutan aplicaciones y servicios.

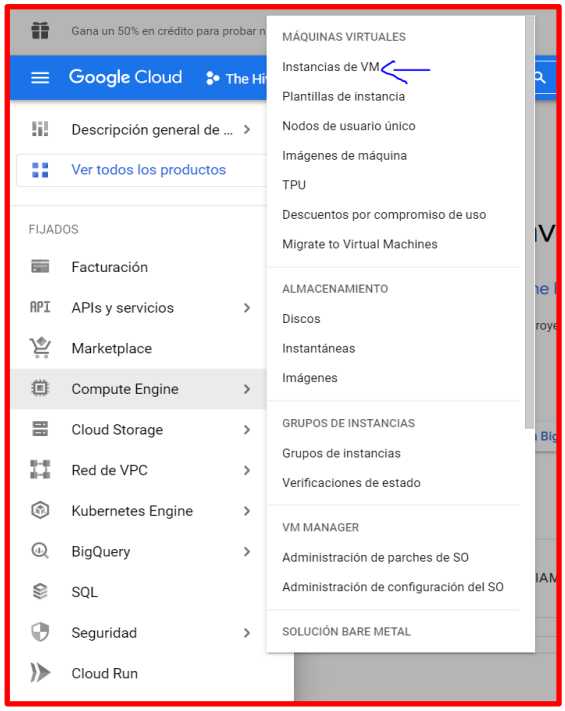
- Autoscaling: Ajusta automáticamente los recursos para manejar la carga de trabajo, tanto horizontalmente (añadiendo más nodos o pods) como verticalmente (asignando más recursos a los pods).

- Balanceo de carga: Kubernetes dirige el tráfico a los contenedores disponibles de manera eficiente, asegurando alta disponibilidad.

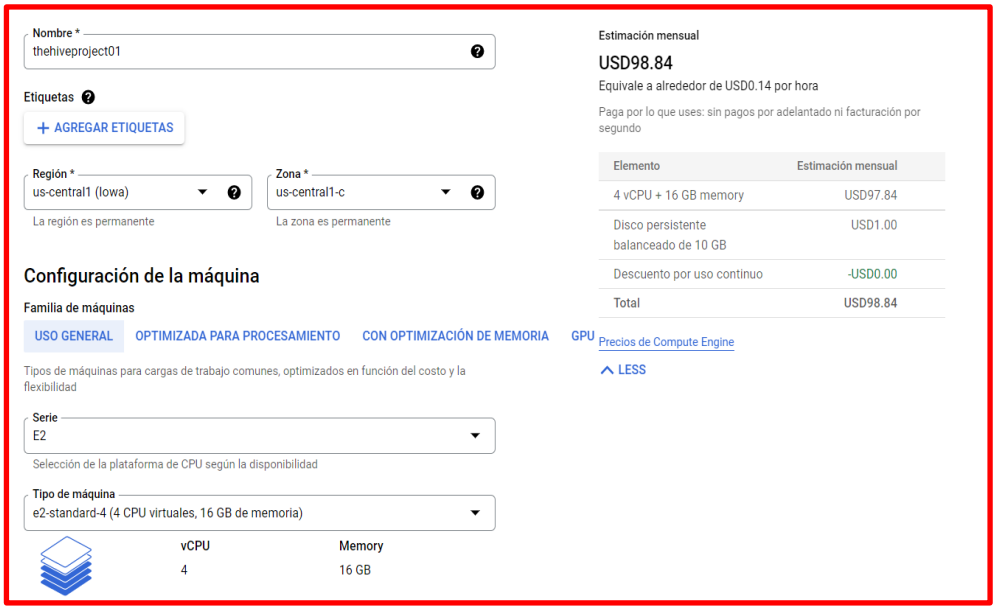
Pasos de configuración

Creación de una máquina virtual en la nube de GCP.

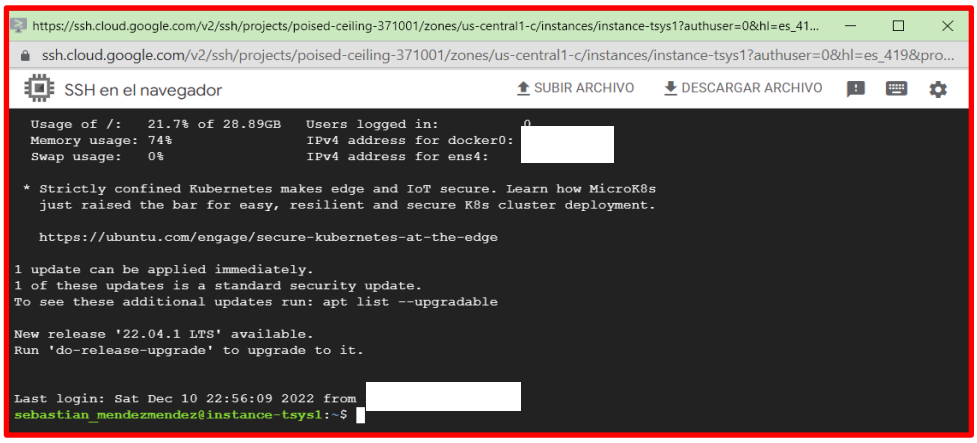
1. Seleccionamos la opción. “Instancias de VM”.



2. Se configuran sus características de acuerdo a los requerimientos mínimos de The Hive Project.

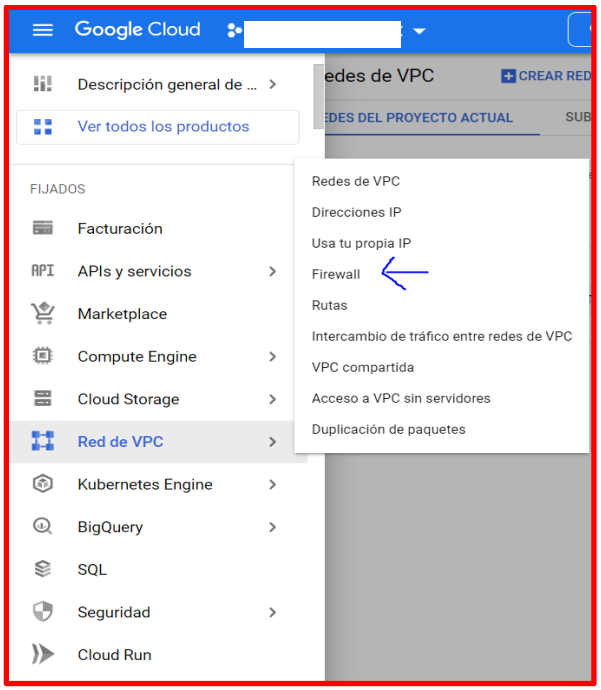


3. Una vez creada, se verifica el acceso por ssh, a la máquina virtual.

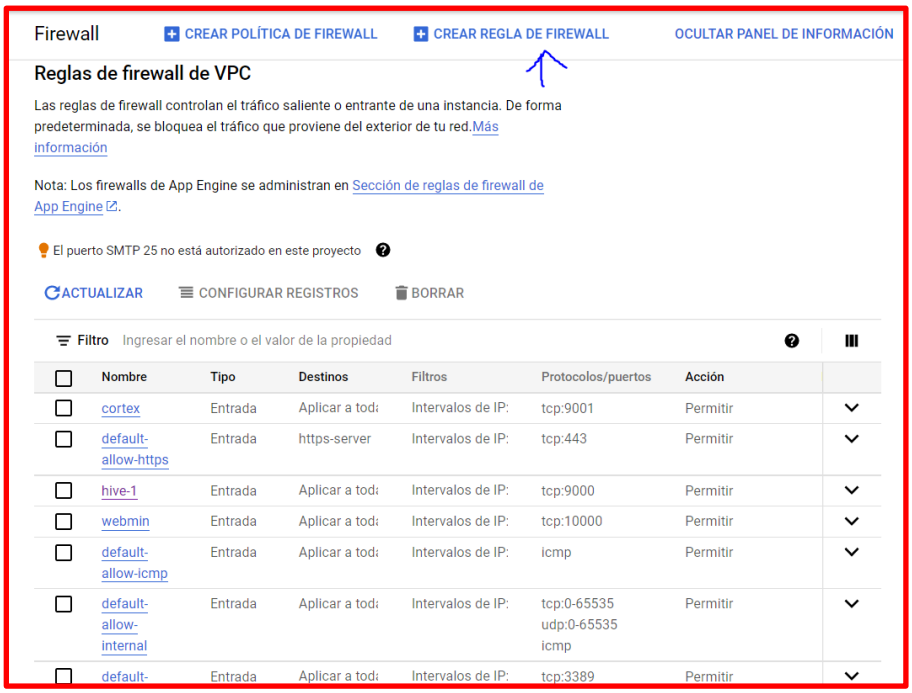


4. Se configuran reglas de entrada y salida en firewall, por seguridad.

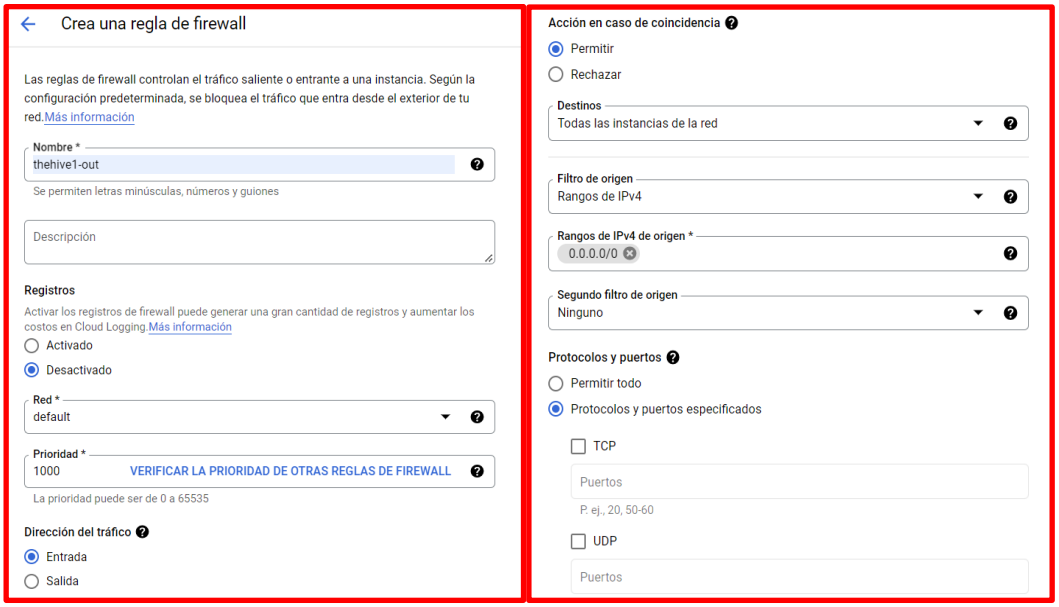
4.1. Para acceder es en consola Red de VPC -> Firewall



4.2 Accedemos al panel de reglas



4.3 Se configura el nombre, descripción, dirección del tráfico, acción, rangos de IP y protocolos y puertos.



Instalación de The Hive, Córtex

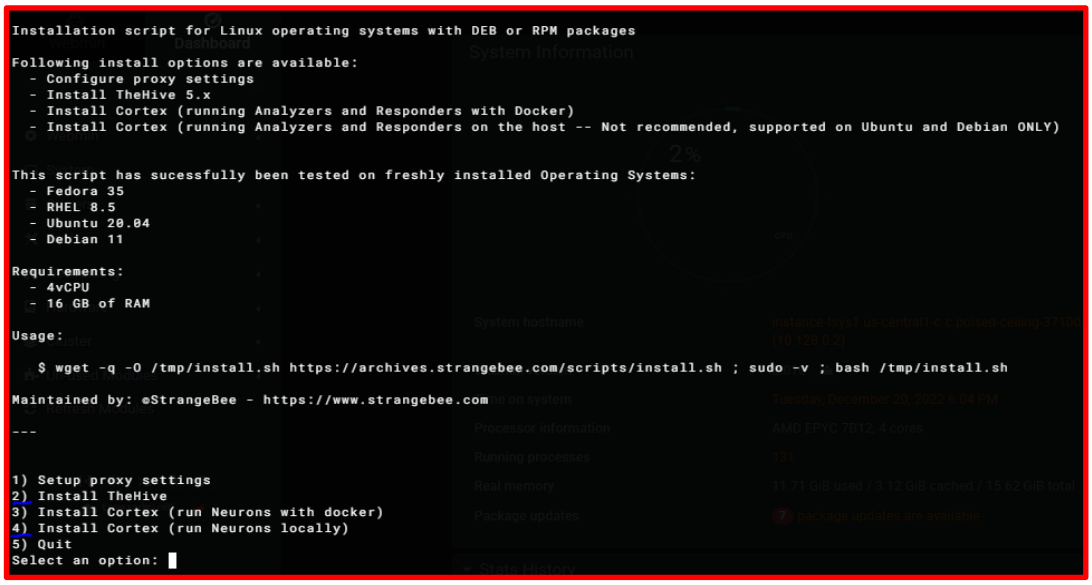
1. El comando se utiliza para descargar información de la última versión de la lista de paquetes del repositorio de software de su distribución y cualquier repositorio de terceros que haya configurado.

```
sebastian_mendezmendez@instance-tsys1:~$ sudo apt-get update
Hit:1 http://us-central1.gce.archive.ubuntu.com/ubuntu focal InRelease
```

2. Descarga del script de instalación y se validan las credenciales del usuario para autenticarse si es necesario.

```
root@instance-tsys1:~# wget -q -O /tmp/install.sh
root@instance-tsys1:~# sudo -v
```

3. Ejecución del Script. -



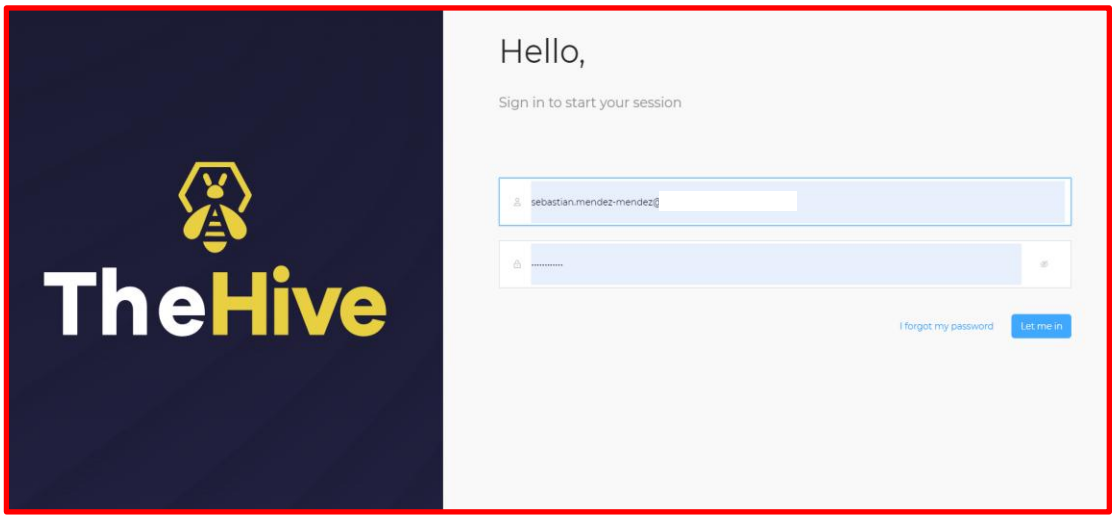
Vistas y configuraciones

The hive project

Los perfiles predeterminados son:

- **admin** : Puede *administrar* todos los objetos y usuarios globales. No se puede crear el casos de uso.
- **analista** : Puede gestionar casos de uso y otros objetos relacionados (observables, tareas, …), incluso eliminarlos.
- **org-admin** : *Todos los* permisos *excepto* los relacionados con objetos globales.
- **solo lectura** : *Sin* permisos.

●Inicio de sesión

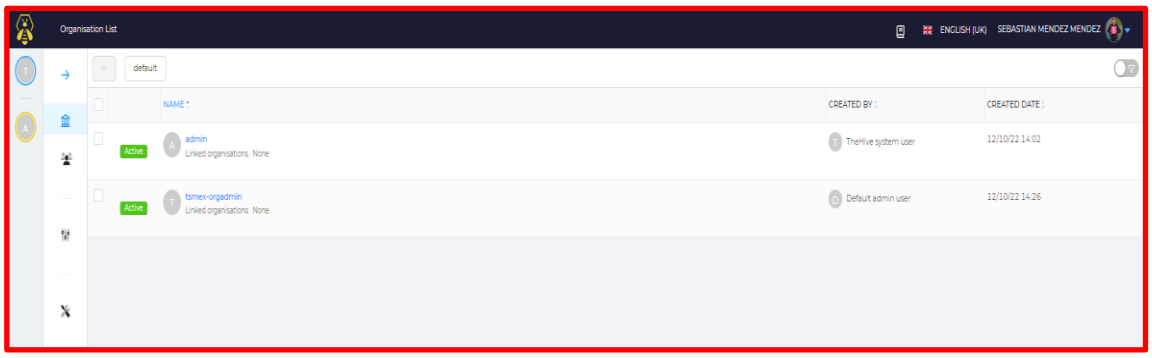


●Lista de organizaciones

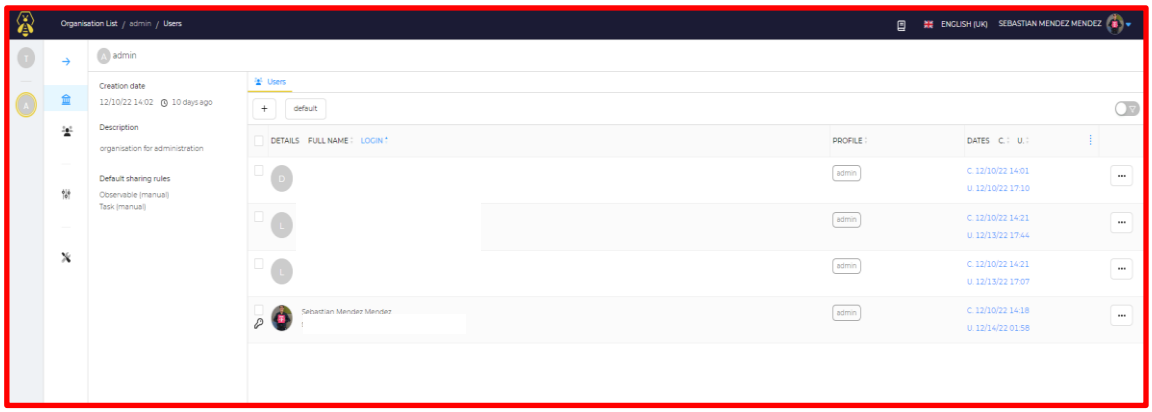
Un usuario es miembro de ***una o más organizaciones***. Un usuario tiene un perfil para cada organización y puede tener diferentes perfiles para diferentes organizaciones.

Por ejemplo:

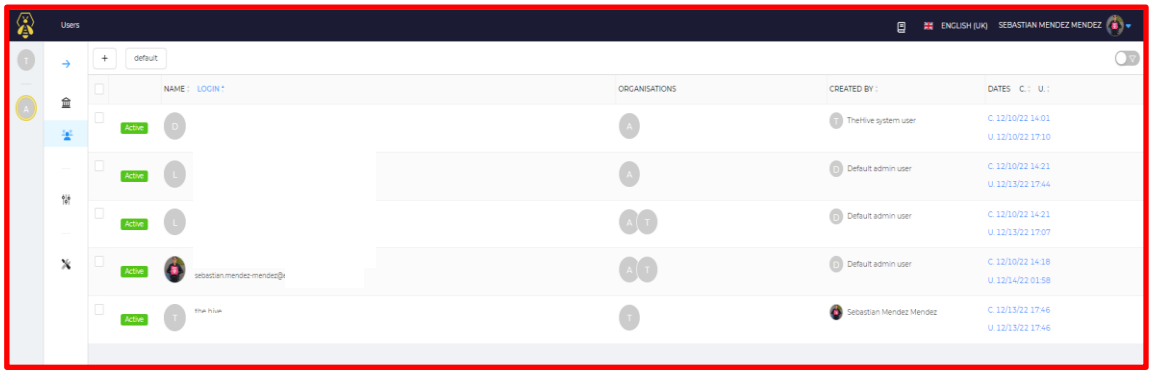
●“analyst” en “ orgA ”
●“ administrator ” en “ orgB ”
●" read-only " en " orgC “



●Lista de usuarios de una organización



●Lista de usuarios



●Datos de un usuario y tipos de cuentas de usuario:

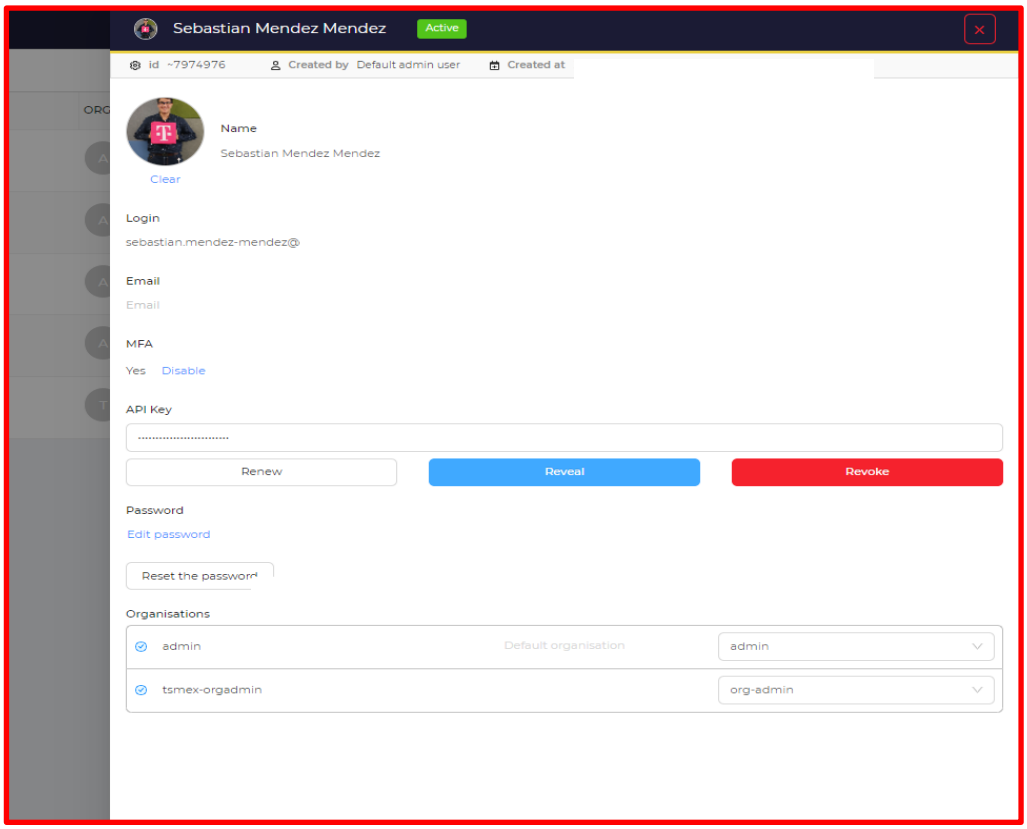
A partir de The Hive 5.0, existen dos tipos de cuentas en la aplicación:

Cuentas normales

●Se utilizan para usuarios estándar, como analistas. Estas cuentas se pueden usar para abrir una sesión en la interfaz de usuario web, usar todos los métodos de autenticación disponibles y las claves API si están habilitadas.

Cuentas de servicio

●Se recomiendan para ser utilizadas por cuentas encargadas de la automatización en la aplicación, como las utilizadas por las Alertas creadas. Estas cuentas solo se pueden usar para autenticar la aplicación a través de la API, con una clave de API.



● Administración de identidades

TheHive viene con perfiles predeterminados, pero se pueden actualizar y eliminar (si no se usan). Se pueden crear nuevos perfiles.

Un *perfil* es un conjunto de permisos adjuntos a un *usuario* y una *organización*. Define lo que el usuario puede hacer sobre un objeto en poder de la organización.

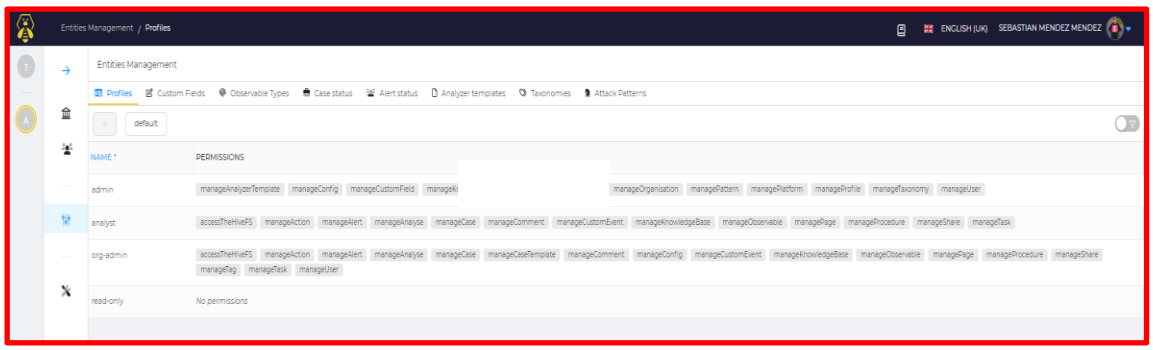
The Hive tiene una lista finita de permisos:

●**manageOrganisation** (1): el usuario puede *crear* , *actualizar* una organización
●**manageConfig** (1): el usuario puede *actualizar* la configuración
●**manageProfile** (1): el usuario puede *crear* , *actualizar* y *eliminar* perfiles
●***manageTag*** (1): el usuario puede *crear* , *actualizar* y *eliminar* etiquetas
●**manageCustomField** (1): el usuario puede *crear* , *actualizar* y *eliminar* campos personalizados
●**manageCase** : el usuario puede *crear* , *actualizar* y *eliminar* casos
●**manageObservable** : el usuario puede *crear* , *actualizar* y *eliminar* observables
●**manageAlert** : el usuario puede *crear* , *actualizar* e *importar* alertas
●**manageUser** : el usuario puede *crear* , *actualizar* y *eliminar* usuarios
●**manageCaseTemplate** : el usuario puede *crear* , *actualizar* y *eliminar* plantillas de casos
●**manageTask** : el usuario puede *crear* , *actualizar* y *eliminar* tareas.
●**manageShare** : el usuario puede *compartir* casos, tareas y observables con otra organización

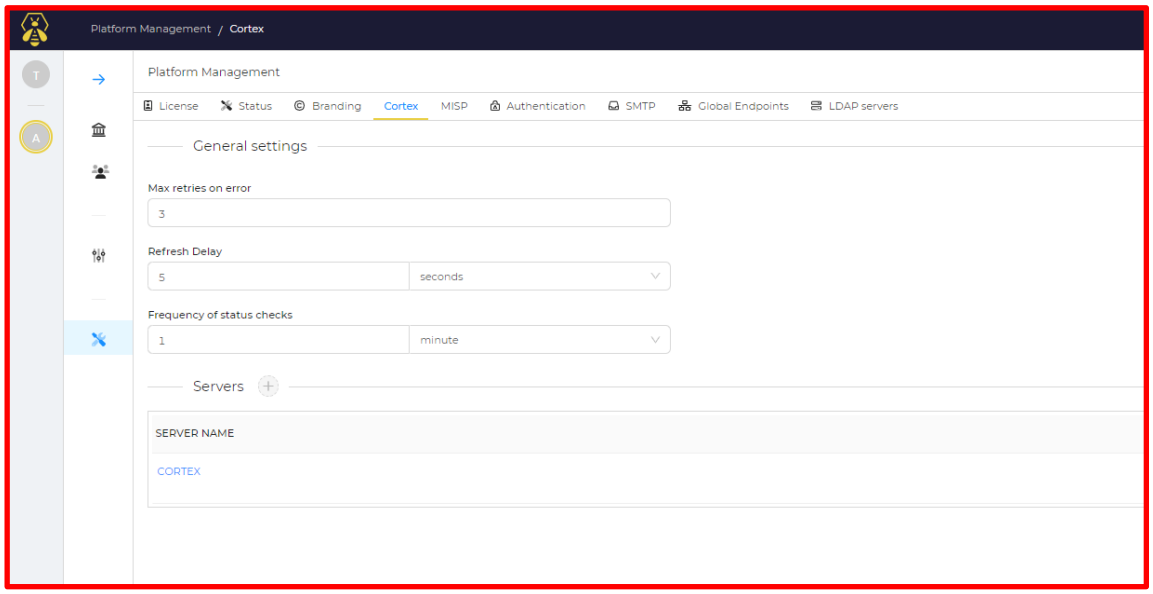
●**manageAnalyse** (2): el usuario puede *ejecutar* analizar
●**manageAction** (2): el usuario puede *ejecutar* acciones
●**manageAnalyzerTemplate** (2): el usuario puede *crear* , *actualizar* y *eliminar* la plantilla del analizador (anteriormente llamada plantilla de informe)

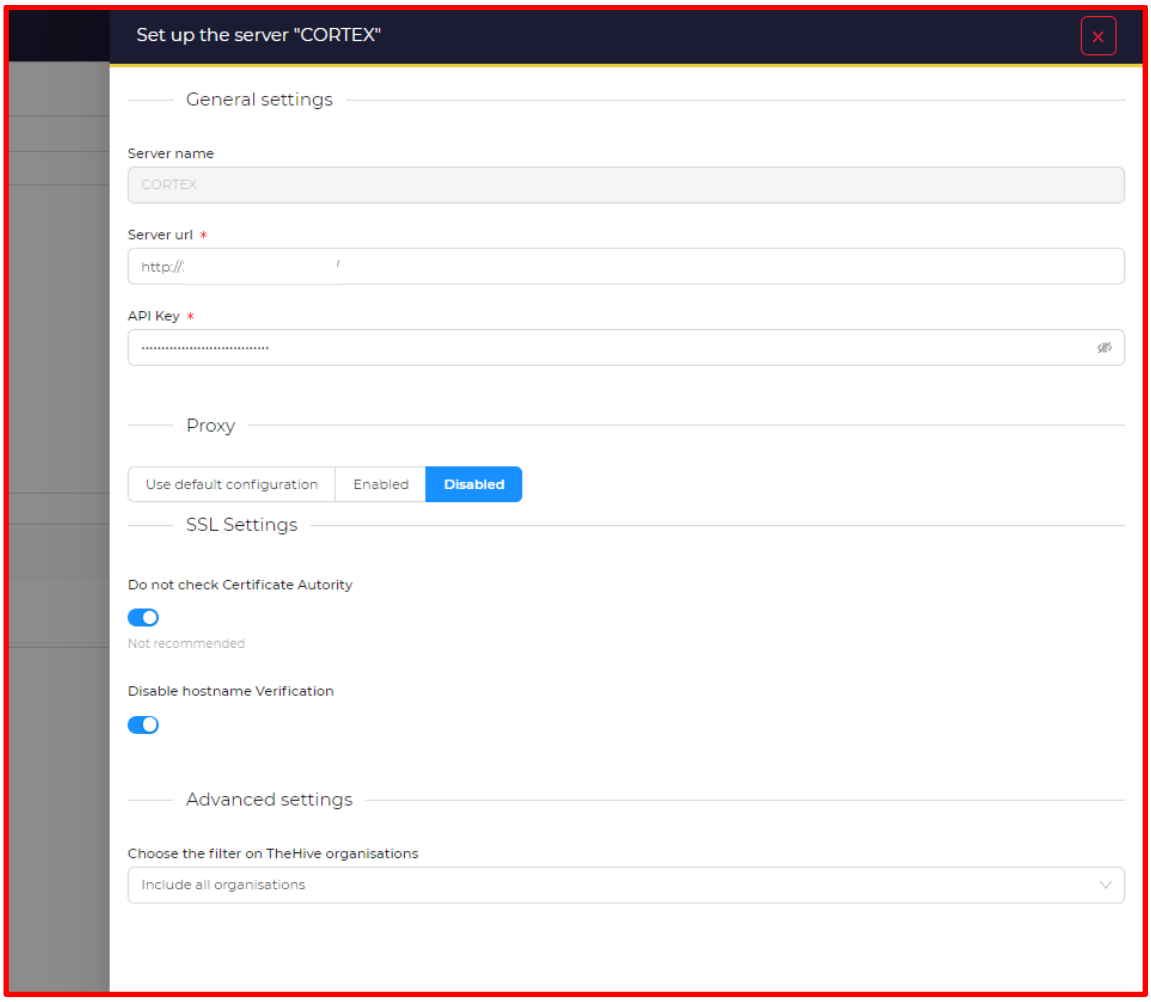
Notas

●Las organizaciones, la configuración, los perfiles y las etiquetas son objetos globales. Los permisos relacionados son efectivos solo en la organización *"administradora"* .
●Las acciones, el análisis y la plantilla están disponibles solo si el conector Cortex está habilitado

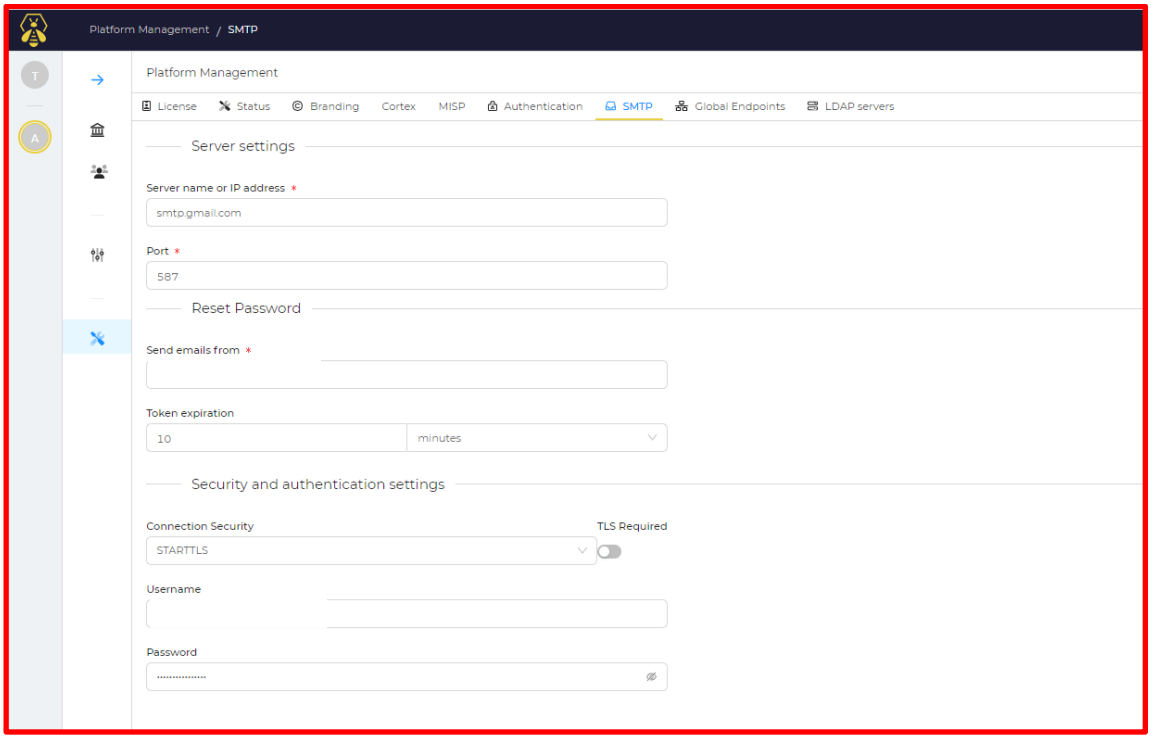


●Configuración de Cortex



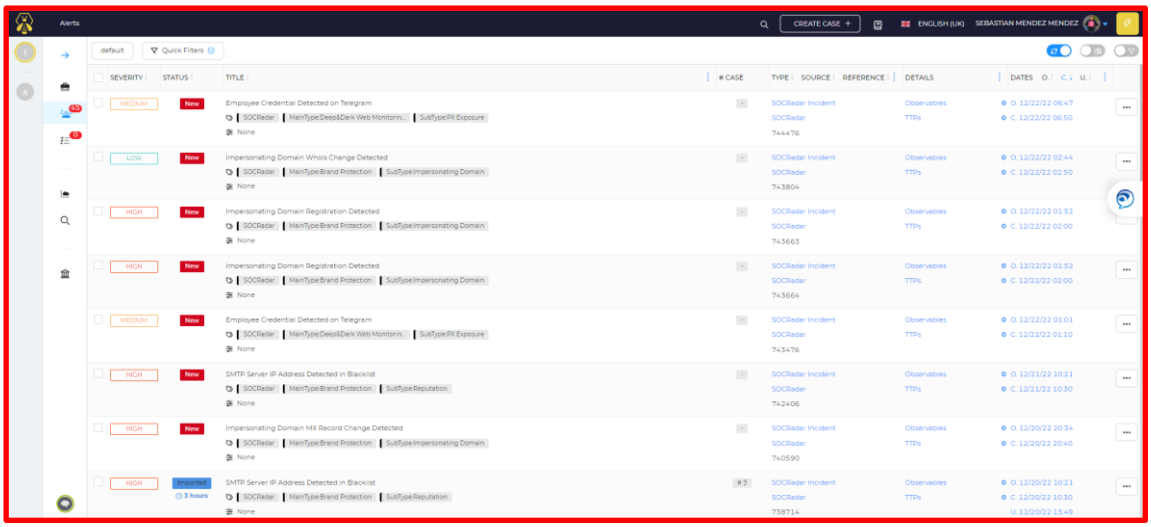


●Configuración SMTP



●Con el rol (org-admin):

Alertas: En esta sección se visualizan las alertas integradas de diferentes plataformas.

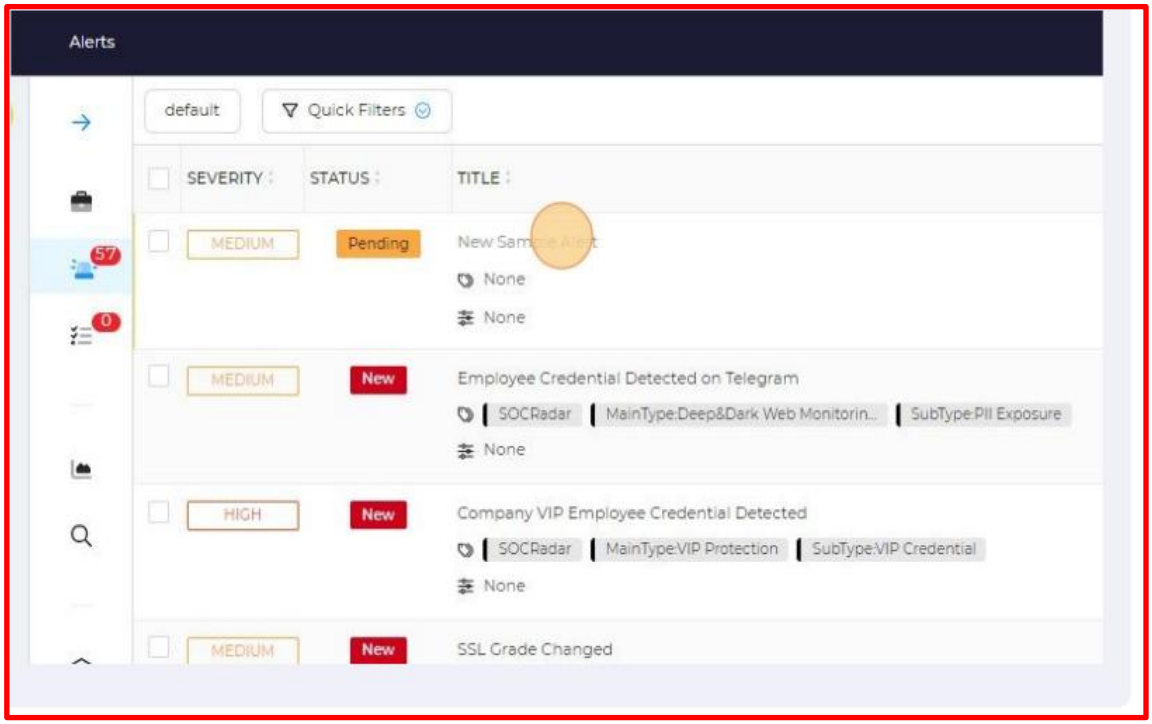


Gestión de casos

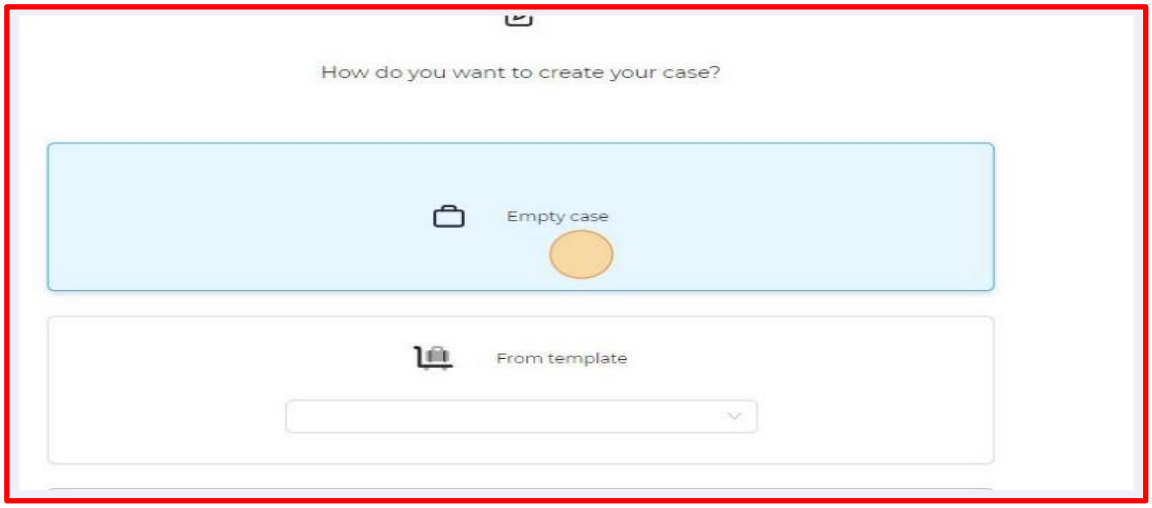
Crear un caso es una de las funcionalidades básicas de TheHive.

●Para crear un caso, debe tener el permiso *manage Case*

Desde una alerta, de click en la alerta:



Luego, puede optar por usar un template, o iniciarlo desde cero usando Caso vacío.



Ingrese:

- El título del caso de uso.
- La fecha de creación
- Severidad
- **PAP (Permissible Actions Protocol)** es un protocolo que describe cuánto aceptamos que un atacante puede detectar del estado de análisis actual o acciones defensivas.

Está diseñado para indicar lo que el receptor puede hacer con la información y lo logra mediante el uso de un esquema de color.

PAP tiene semejanzas con ***TLP o Traffic Light Protocol*** porque utiliza el mismo esquema de color, el protocolo TLP le permite compartir información confidencial y mantener el control sobre la distribución de la información.

- **PAP:RED:** Solo acciones no detectables. Los destinatarios no pueden usar la información de PAP:RED en la red. Solo acciones pasivas sobre registros, que no son detectables desde el exterior.

○TLP:RED: Fuerte limitado, solo tus compañeros.

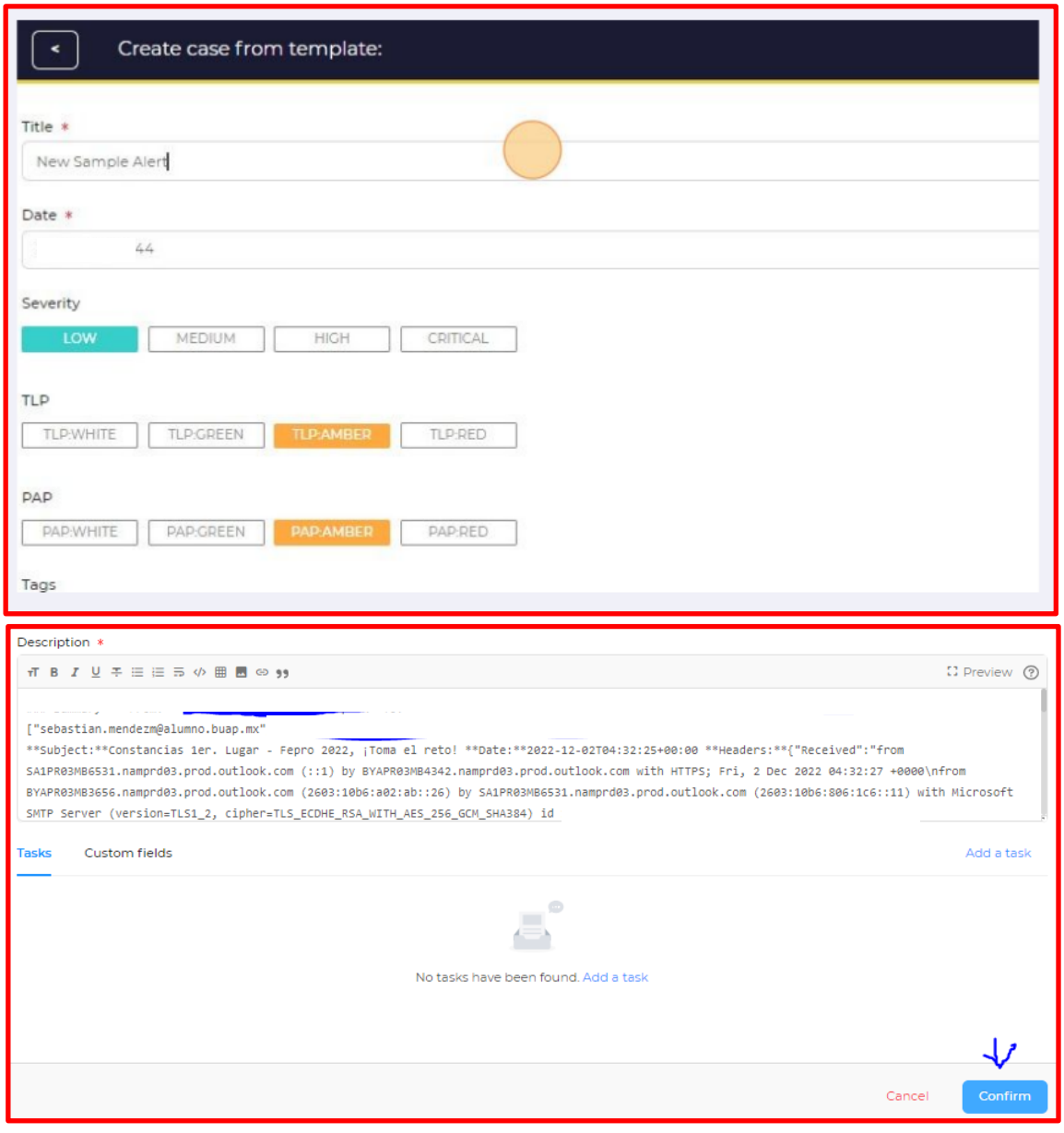
●**PAP:AMBER**: los destinatarios pueden usar la información de PAP:AMBER para realizar verificaciones en línea, cómo usar servicios proporcionados por terceros (por ejemplo, VirusTotal), o configurar un sistema de monitoreo.

○TLP:AMBER: Limitado, solo personas que actúan sobre la información.

●**PAP:VERDE:** Acciones activas. Los destinatarios pueden usar la información PAP:GREEN para hacer ping al objetivo, bloquear el tráfico entrante/saliente desde/hacia el objetivo o configurar específicamente los señuelos para interactuar con el objetivo.

○TLP:VERDE: Relajado, conocido por el círculo interno.

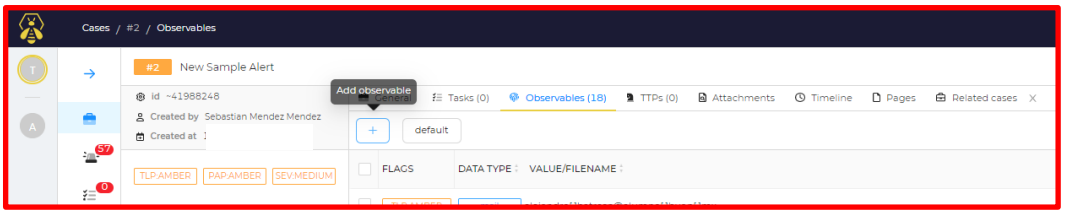
●**PAP:WHITE**: Abierto, sin restricciones



Observables

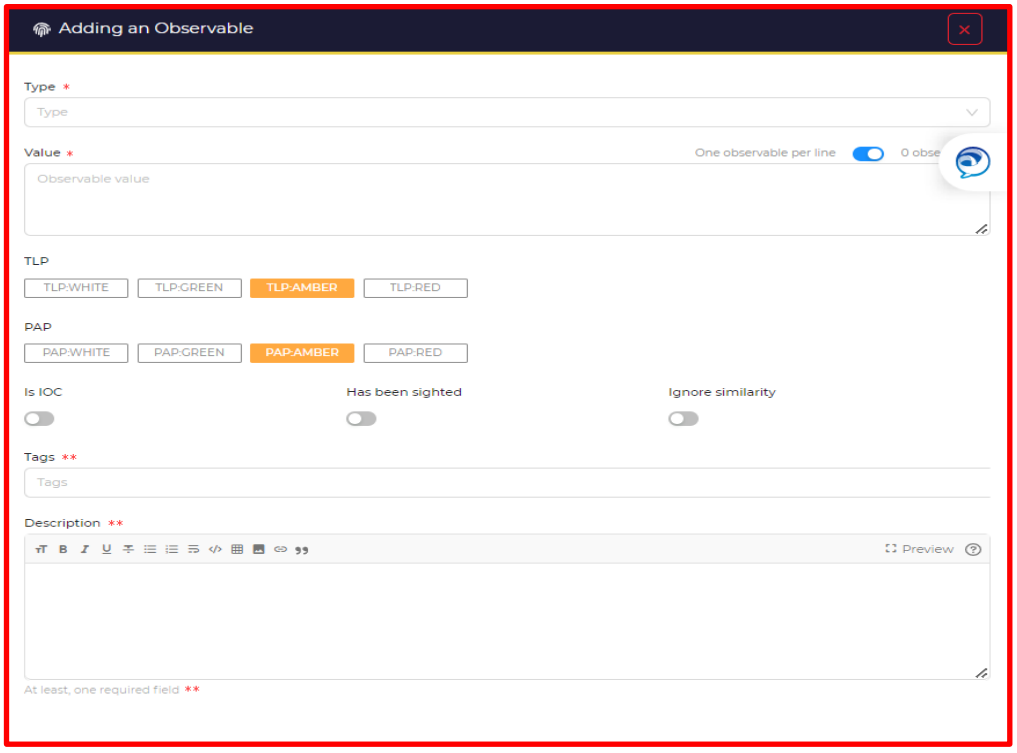
En un caso, se pueden declarar observables.

Encontrará el botón Agregar observable en la pestaña Observables:



En la ventana emergente, tiene que completar los detalles:

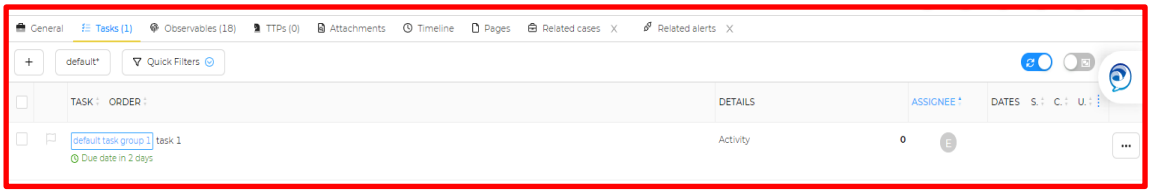
- Tipo: El observable dataType (Ej: ip, hash, dominio,etc)
- Valor: El valor del observable (por ejemplo: 8.8.8.8)
- TLP: Definir aquí la forma en que se debe compartir la información.
- Es IOC: Márquelo si esto observable se considera como Indicador de Compromiso.
- Ignorar por similitud: No correlacionar este observable con otros similares.
- Etiquetas: etiquetas asociadas a un observable con información perspicaz.
- Descripción: Descripción del observable.



Gestión de tareas

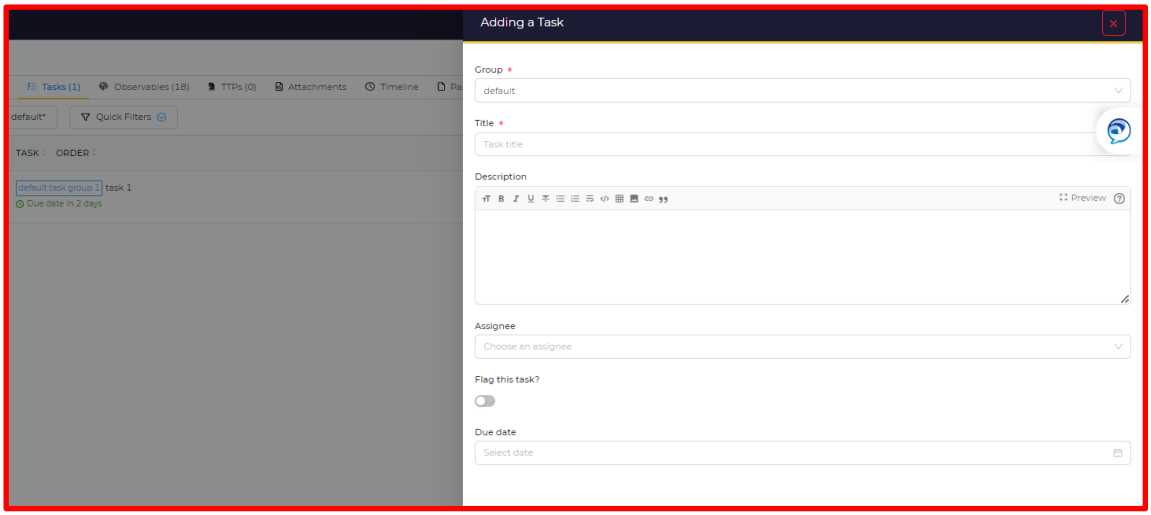
La lista contiene la siguiente información:

- Grupo: La pertenencia al grupo
- Tarea: El título
- Fecha: La fecha de inicio.
- Cesionario: El usuario asignado.
- Acciones: eliminar, iniciar/cerrar o desencadenar un responder.



Abra su *lista de tareas* y haga clic en el botón *Crear tarea* . A la derecha de la lista de tareas, aparecerá una ventana que en la que tendrá que llenar la siguiente información:

- Título de la tarea
- Grupo de tareas
- Asignatario de la tarea
- Fecha de inicio de la tarea
- Duración de la tarea
- Estado de la tarea

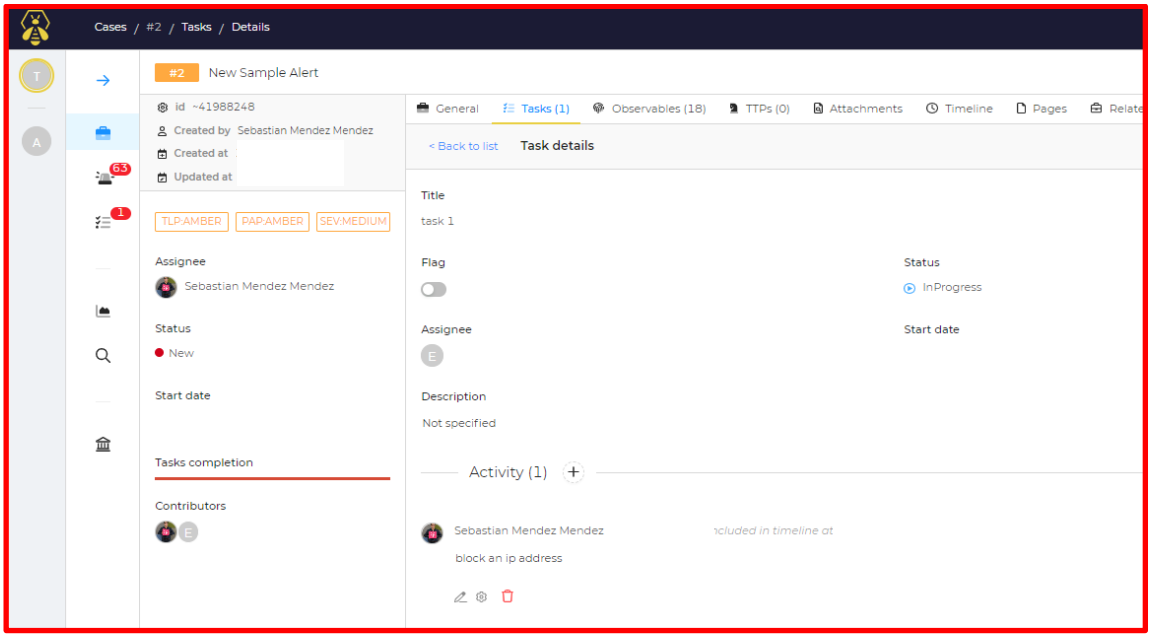


También es posible crear registros a esas tareas, verlos en la sección de actividad y agregar archivos a ellas:

Acciones para los registros (Disponibles):

- Crear un registro de tareas
- Modificar un registro de tareas
- Eliminar un registro de tareas

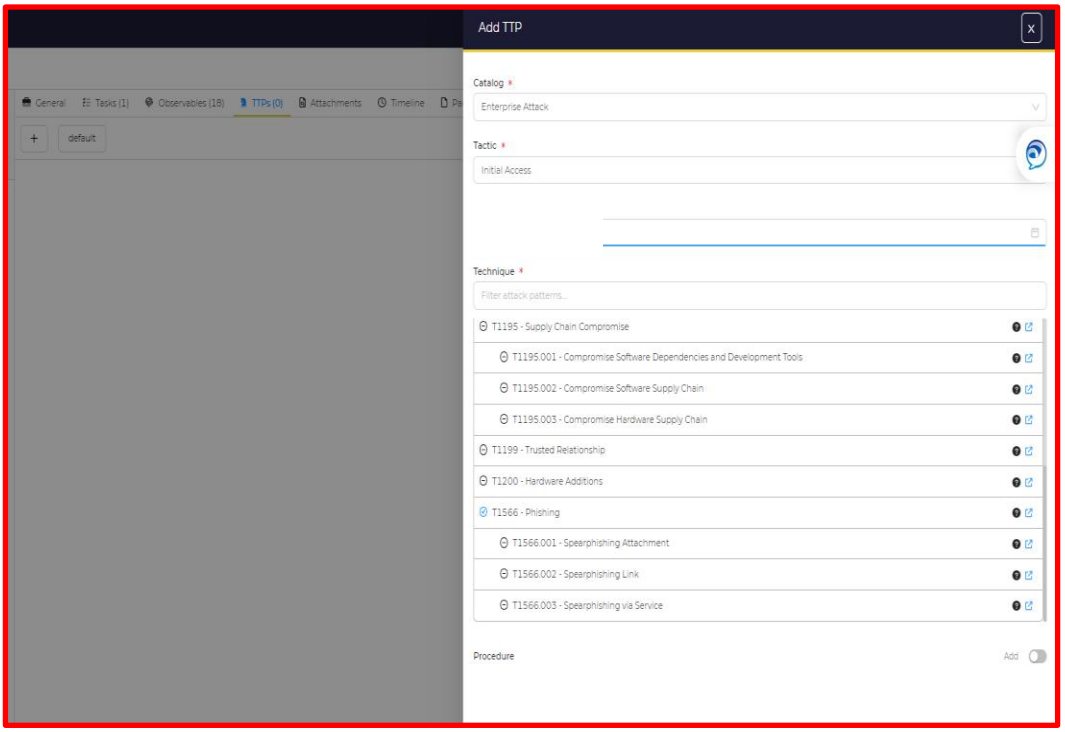
●Activar un responder en el registro de tareas



TTP´s

En la ventana emergente Agregar táctica, técnica y procedimiento, puede seleccionar:

●La fecha de ocurrencia
●La táctica
●La Técnica (puedes usar filtros en las técnicas)
●El Procedimiento (haga clic en Agregar procedimiento para abrir este campo de texto libre)



CORTEX

Cortex resuelve dos problemas comunes a los que se enfrentan con frecuencia los SOC en el curso de la inteligencia de amenazas, el análisis forense digital y la respuesta a incidentes:

●Analizar los observables que han recopilado, a escala, consultando una sola herramienta en lugar de varias.
●Responder activamente a las amenazas e interactuar con el electorado y otros equipos.

Muchas características están incluidas con Cortex:

●Administra múltiples organizaciones (es decir, multiusuario).
●Administrar usuarios por organizaciones y roles.
●Especifique la configuración del analizador y respondedor por organización.
●Define límites de tarifas: evita consumir todas tus cuotas a la vez.
●Caché: un análisis no se vuelve a ejecutar para el mismo observable si se llama a un determinado analizador en ese observable varias veces dentro de un período de tiempo específico.

Usuarios

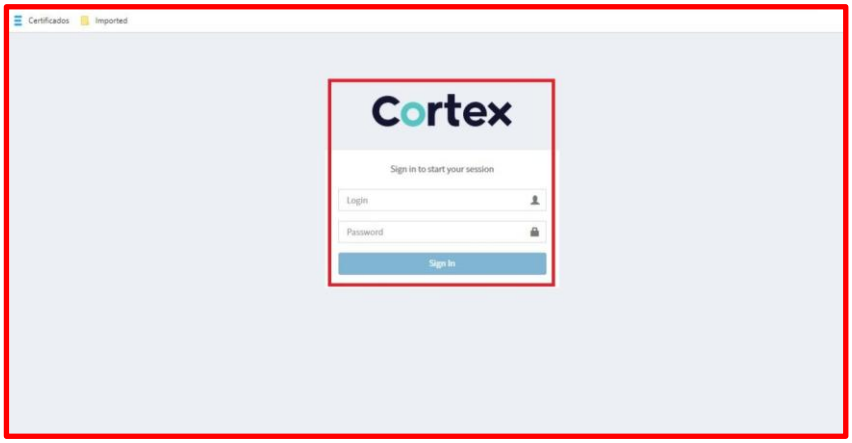
Cortex define cuatro roles:

Actions	read	analyze	orgAdmin	superAdmin
Read reports	X	X	X	
Run jobs		X	X	
Enable/Disable analyzer			X	
Configure analyzer			X	
Create org analyst			X	X
Delete org analyst			X	X
Create org admin			X	X
Delete org admin			X	X
Create Org				X
Delete Org				X
Create Cortex admin user				X

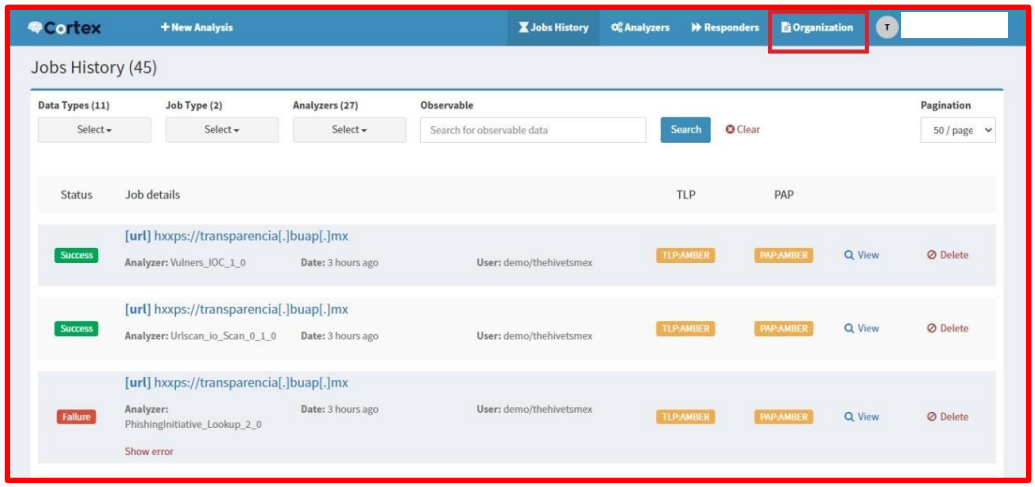
Analizadores

●Integrar un analizador

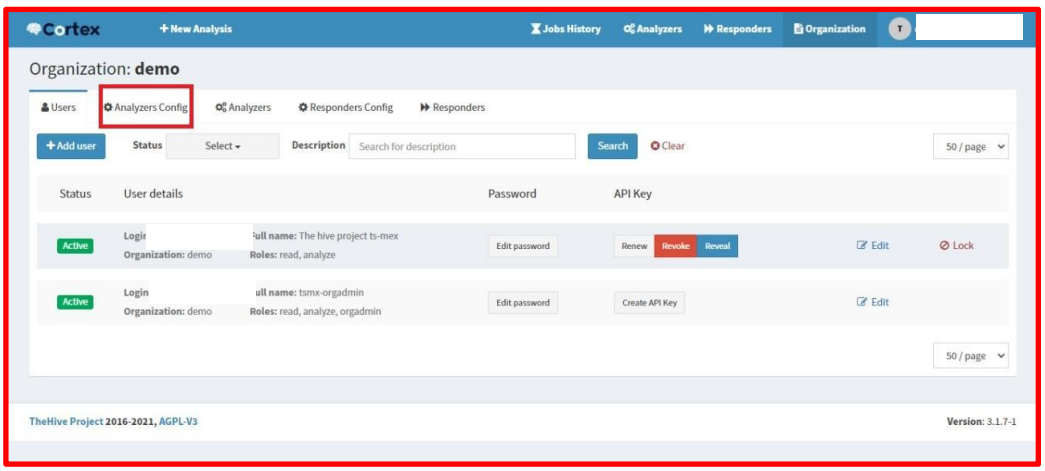
Se ingresa al córtex llenando los siguientes campos.



●Se ingresa a la ventana de Organization.

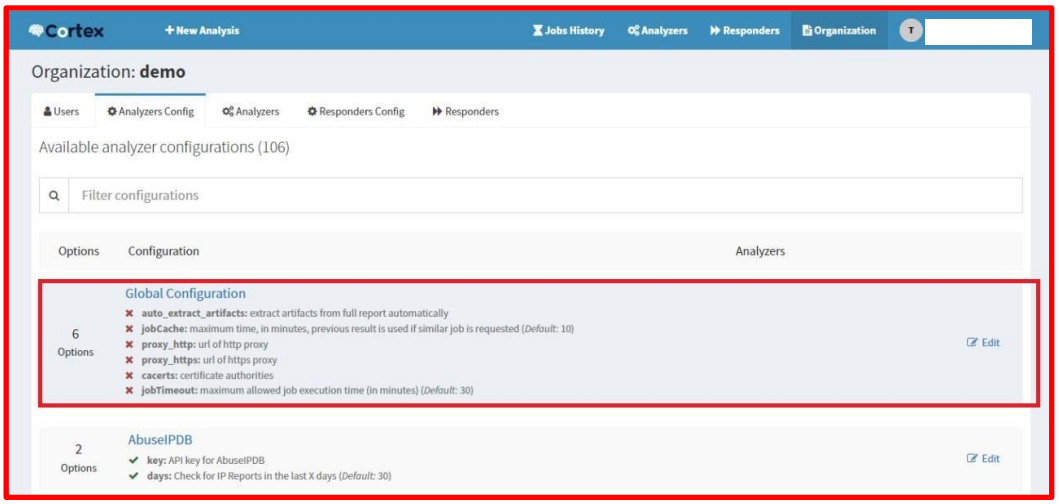


●Se da click en la herramienta de Analysers Config.

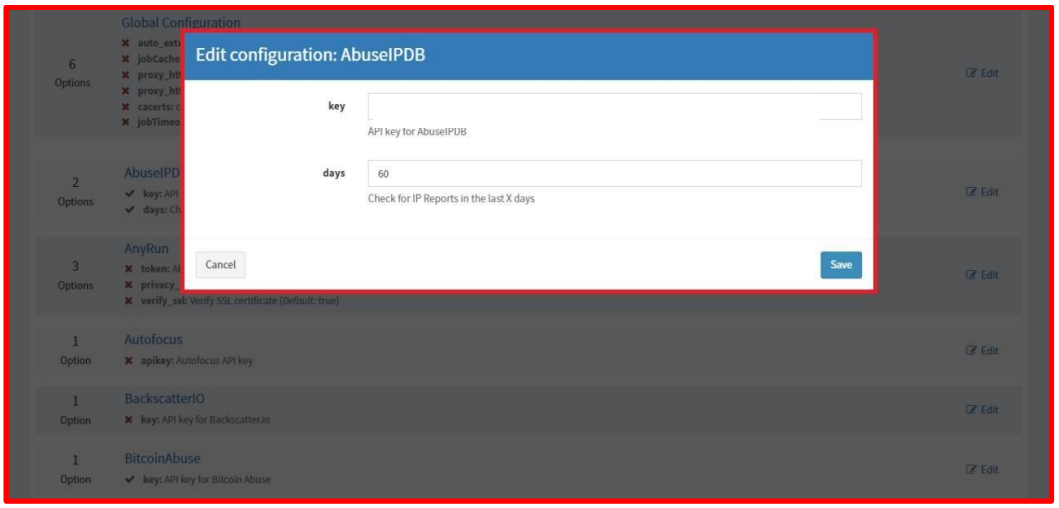


Se edita cualquier Analyzer que se requiera ocupar, cada Analyzer necesita diferentes campos que necesitan ser llenados, algunos necesitan una suscripción de paga para poder ser integrados a Cortex.

Debajo del nombre de la herramienta, se puede observar todo lo que necesita para ser habilitado.

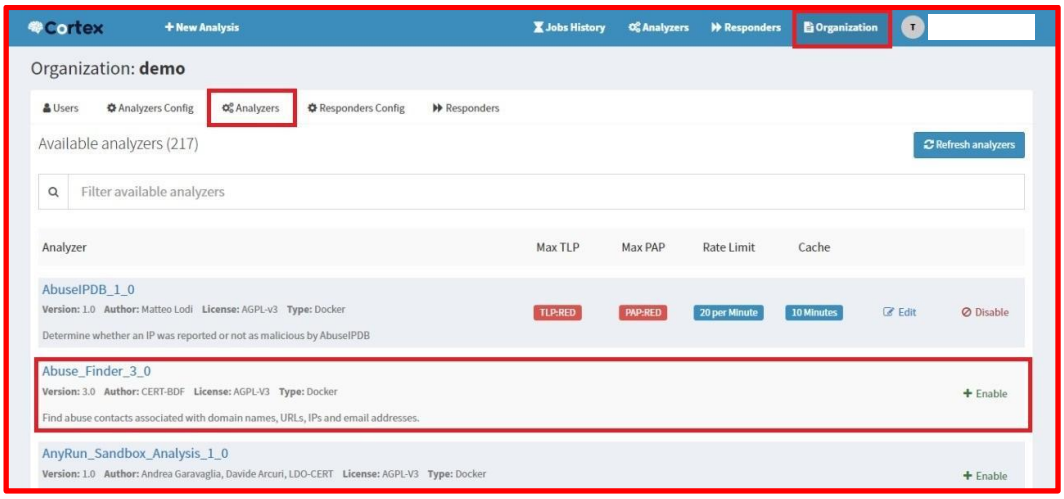


La mayoría de los analizadores se pueden integrar con una KEY, la cual se puede generar al usar la versión gratuita.

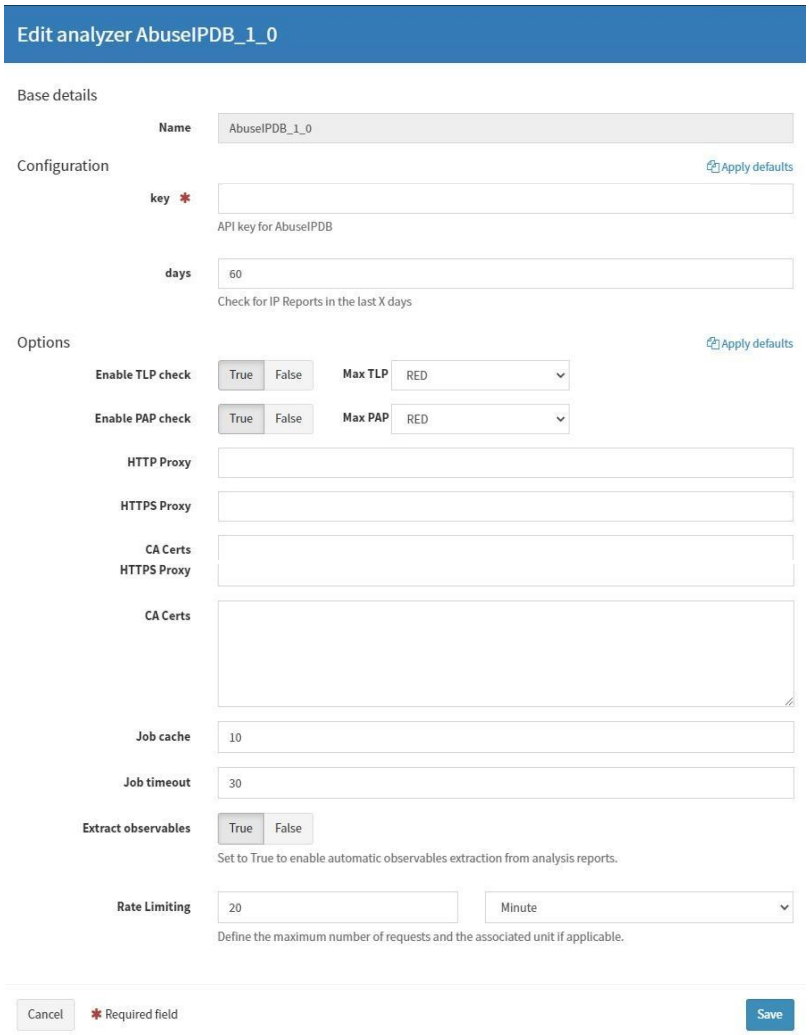


●Habilitar un analizador

Para habilitar un analizador, en la pestaña de Analyzers que también se encuentra en Organization, se deben de buscar las herramientas que fueron integradas previamente. Para habilitar un analizador, en la pestaña de Analyzers que también se encuentra en Organization, se deben de buscar las herramientas que fueron integradas previamente.



●Una vez que se da el botón “Enable”, se puede configurar los analyzers, en nuestro caso habilitamos la extracción de observables, con un rango límite de 20 minutos.



Analizadores integrados

Fuente	Descripción	Características principales	Costos	Ventajas	Desventajas
AbuseIPDB	Base de datos colaborativa que recopila y comparte información sobre direcciones IP sospechosas de actividades maliciosas	Permite buscar y verificar direcciones IP sospechosas	Gratuito	Gran comunidad de usuarios que colabora en la recopilación de datos	Los datos pueden no estar siempre actualizados o ser incompletos
CheckPhish	Herramienta de detección de phishing que analiza y evalúa URLs sospechosas	Verifica si una URL es maliciosa o sospechosa	Planes de precios disponibles	Interfaz fácil de usar y resultados rápidos	Algunas características avanzadas pueden requerir una suscripción paga
EchoTrail	Plataforma de inteligencia de amenazas que proporciona información sobre ciberataques y actividades maliciosas	Recopila datos de múltiples fuentes y muestra inteligencia de amenazas en tiempo real	Planes de precios disponibles	Amplia cobertura de fuentes de inteligencia de amenazas	No se especifican los costos en su sitio web
Hunter.io	Herramienta de búsqueda de direcciones de correo electrónico y verificación de dominios	Permite encontrar direcciones de correo electrónico asociadas a un dominio y verificar su existencia	Planes de precios disponibles	Amplia base de datos de correos electrónicos	Las funciones avanzadas pueden requerir una suscripción paga
IPvoid	Servicio en línea que proporciona información detallada sobre direcciones IP	Ofrece un conjunto completo de herramientas para analizar direcciones IP y obtener información relevante	Planes de precios disponibles	Proporciona información detallada sobre una dirección IP, incluyendo geolocalización y reputación.	Algunas funciones y datos están restringidos a los planes de pago

Intezer Community	Comunidad de inteligencia de amenazas centrada en el análisis de malware	Proporciona información y anáIisis de malware para identificar posibles compromisos	Gratuito	Acceso a análisis de malware realizados por expertos	No ofrece información tan amplia sobre otros tipos de indicadores de compromiso
Kaspersky TIP	Threat Intelligence Platform de Kaspersky que proporciona información sobre amenazas cibernéticas	Ofrece información sobre indicadores de compromiso y permite compartir y recibir inteligencia de amenazas	Planes de precios disponibles	Integración con otras soluciones de seguridad de Kaspersky	No se especifican los costos en su sitio web
Maltiverse	Plataforma de inteligencia de amenazas que recopila y analiza datos relacionados con ciberataques	Proporciona información sobre indicadores de compromiso y permite buscar y compartir datos de amenazas	Planes de precios disponibles	Amplia variedad de fuentes de datos y capacidades de búsqueda avanzada	Algunas funciones y datos están restringidos a los planes de pago
OTXQuery	Plataforma de inteligencia de amenazas de AlienVault/Open Threat Exchange	Permite buscar y compartir información sobre indicadores de compromiso	Gratuito	Gran comunidad de usuarios que comparten información sobre amenazas	La base de datos puede no ser tan completa como otras fuentes de inteligencia de amenazas
Onyphe	Motor de búsqueda de inteligencia de amenazas que recopila datos de diversas fuentes	Proporciona información en tiempo real sobre amenazas cibernéticas.	Planes de precios disponibles	Amplia cobertura de fuentes de inteligencia de amenazas	Las funciones avanzadas y el acceso a algunos datos pueden requerir una suscripción paga
Pulsedive	Plataforma de inteligencia de amenazas que agrega datos de múltiples fuentes	Permite buscar y analizar indicadores de compromiso y recibir alertas de seguridad	Planes de precios disponibles	Integración con otras herramientas y servicios de seguridad	Algunas funciones y datos están restringidos a los planes de pago.

Shodan	Motor de búsqueda especializada en dispositivos conectados a Internet	Permite buscar dispositivos y servicios en línea y proporciona información sobre su seguridad	Planes de precios disponibles	Planes de precios disponibles	Amplia cobertura de dispositivos conectados a Internet
urlscan.io	Herramienta de análisis de sitios web que examina y escanea URLs	Realiza un análisis exhaustivo de las URLs para identificar posibles amenazas	Gratuito	Muestra información detallada sobre el comportamiento y contenido de un sitio web	No proporciona información sobre otros tipos de indicadores de compromiso
Vulners	Base de datos y motor de búsqueda de vulnerabilidades en software y sistemas	Proporciona información sobre vulnerabilidades conocidas y posibles indicadores de compromiso	Planes de precios disponibles	Amplia cobertura de vulnerabilidades y exploits	Algunas funciones y datos están restringidos a los planes de pago

Tabla. Comparación de analizadores y motores de búsqueda integrados al proyecto.