Plataformas SOAR. Respuesta Orquestada y Automatizada de la Seguridad

Alejandro del Pino Medina

Máster de universitario en Ciberseguridad y Privacidad

TFM-Seguridad Empresarial

Manuel Mendoza Flores

Víctor García Font

Junio de 2021

Agradecimientos

Quiero dar las gracias a mi mujer y mis hijos por la paciencia y compresión que me han demostrado. A Ellos son a los que más tiempo he quitado para poder realizar el Máster.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Plataformas SOAR. Evolución e importancia ante los nuevos ataques inteligentes.
Nombre del autor:	*Alejandro del Pino Medina*
Nombre del consultor/a:	*Manuel Mendoza Flores*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	*Plan de estudios del estudiante*
Área del Trabajo Final:	*Máster Universitario de Ciberseguridad y Privacidad*
Idioma del trabajo:	*Castellano*
Palabras clave	*SOAR, SIEM, IA*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El presente trabajo busca situar al lector en la importancia de la monitorización de las comunicaciones para aumentar la seguridad, haremos un repaso por las principales sistemas de monitorización de comunicaciones, profundizaremos en los SIEMs actuales y su evolución, para centrarnos en el conocimiento de las Plataformas SOAR (Security Orchestration, Automation and Response Solutions), de donde surgen, cuáles son sus componentes y la importancia que van a tener en el futuro ante el uso de IA para la realización de ataques informáticos.

También se analizarán las soluciones SOAR actuales que está teniendo mayor éxito en el mercado y su importancia como herramienta que pueda actuar en tiempo real ante incidentes, previniendo daños mayores actuando de manera automática.

A modo de laboratorio mostraremos los componentes necesarios para implementar una solución SOAR Open Source, para ello analizaremos el funcionamiento el Proyecto TheHive, describiremos la arquitectura, la instalación y fuuncionamiento.

También analizaremos diferentes soluciones Cloud Pública centrándonos en la plataforma Amazon GuardDuty.

Realizaremos pruebas de concepto del Proyecto TheHive y GuardDuty.

Abstract (in English, 250 words or less):

This paper seeks to place the reader on the importance of communication monitoring to increase security, we will review the main communication monitoring systems, we will delve into current SIEMs and their evolution, to focus on the knowledge of the Platforms SOAR (Security Orchestration, Automation and Response Solutions), where they arise, what are their components and the importance that they will have in the future in the face of the use of AI to carry out computer attacks.

The current SOAR solutions that are having greater success in the market will also be analyzed and their importance as a tool that can act in real time in the event of incidents, preventing greater damage by acting automatically.

As a laboratory we will show the necessary components to implement an Open Source SOAR solution, for this we will analyze the operation of the TheHive Project, we will describe the architecture, installation and operation.

We will also analyze different Public Cloud solutions focusing on the Amazon GuardDuty platform.

We will conduct proofs of concept for Project TheHive and GuardDuty.

Índice

Lista de Ilustraciones

1. Introducción

1.1 Contexto y justificación del Trabajo

En 2017, Gartner acuñó el término orquestación, automatización y respuesta de seguridad (SOAR) para describir la categoría emergente de plataformas nacidas de la respuesta a incidentes, la automatización de la seguridad, la gestión de casos y otras herramientas de seguridad.

Las plataformas SOAR ofrecen conjuntos de funciones profundas que las hacen adecuadas para manejar investigaciones e incidentes graves. Los incidentes actuales son tan complejos que los equipos de respuesta no pueden permitirse coordinar manualmente el flujo de trabajo y los silos de información. La mayor complejidad en las funciones permite que SOAR sea una herramienta para mejoras sistemáticas a largo plazo, en lugar de una mera clasificación de alertas a corto plazo.

A lo largo de este TFM nos situaremos en el contexto actual de las plataformas SOAR, el estado del arte y sus componentes.

Veremos también como es posible instalar y configurar varias Plataformas SOAR que utilizaremos como prueba de concepto demostrando las ventajas que pueden suponer ante la sofisticación de amenazas actuales y futuras.

1.2 Objetivos del Trabajo

A lo largo de este TFM veremos:

- Visión general de los sistemas de monitorización de las comunicaciones para aumentar la seguridad (IDS/IPS, SIEM y SOAR)
- cómo surgen las Plataformas SOAR,
- los principales proveedores,
- casos de uso,
- evolución de los SOC,
- cómo funcionan.

También analizaremos los principales retos que se plantean en la adopción de SOAR y cómo se relaciona con el resto de los sistemas de Seguridad dentro de un SOC.

Finalmente realizaremos dos pruebas de concepto:

- Instalación de una Plataforma SOAR on premise basándonos en herramientas open source, en concreto en el Proyecto TheHive (https://thehive-project.org/).
- Solución SOAR en nube de AWS llamada GuardDuty.

1.3 Enfoque y método seguido

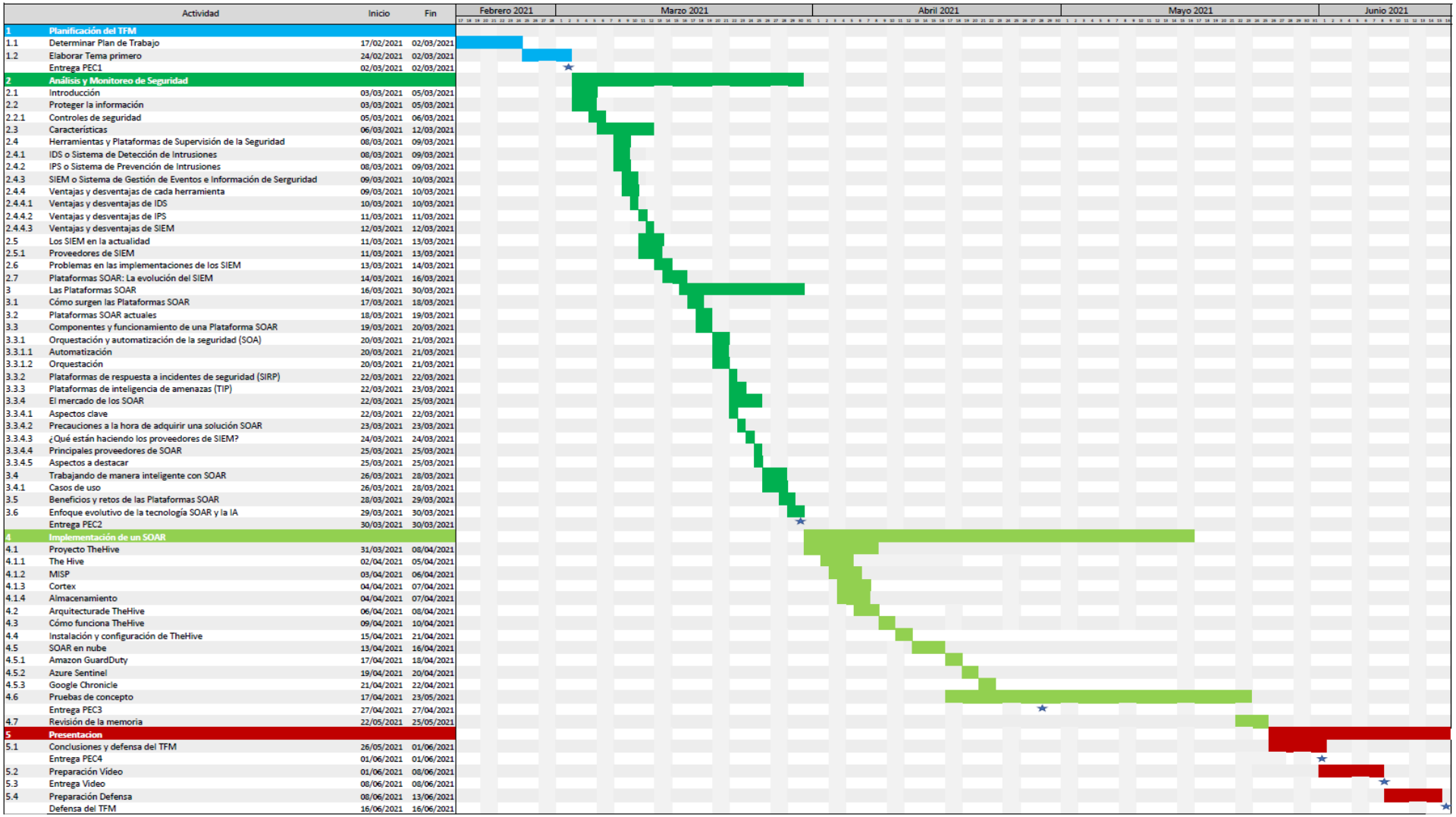
Realizaremos el estudio e investigación de documentación especializada tanto de fabricantes como por investigadores a través de documentos técnicos.

Para la prueba de concepto haremos un recorrido por el Proyecto TheHive, por su arquitectura, su instalación y configuración. También analizaremos las soluciones en Nube centrándonos en Amazon GuardDuty.

1.4 Planificación del Trabajo

Los plazos del TMF están marcados por las propias entregas planificadas dentro del Aula Virtual. Las entregas son las siguientes:

Entrega	Inicio	Fin
Plan de Trabajo	17/02/2021	02/03/2021
Entrega 2	03/03/2021	30/03/2021
Entrega 3	31/03/2021	27/04/2021
Memoria Final	28/04/2021	01/06/2021
Presentación en vídeo	02/06/2021	08/06/2021
Defensa del TFM	14/06/2021	18/06/2021



	Actividad	Inicio	Fin
1	**Planificación del TFM**		
1.1	Determinar Plan de Trabajo	17/02/2021	02/03/2021
1.2	Elaborar Tema primero	24/02/2021	02/03/2021
	Entrega PEC1	02/03/2021	02/03/2021
2	**Análisis y Monitoreo de Seguridad**		
2.1	Introducción	03/03/2021	05/03/2021
2.2	Proteger la información	03/03/2021	05/03/2021
2.2.1	Controles de seguridad	05/03/2021	06/03/2021
2.3	Características	06/03/2021	12/03/2021
2.4	Herramientas y Plataformas de Supervisión de la Seguridad	08/03/2021	09/03/2021
2.4.1	IDS o Sistema de Detección de Intrusiones	08/03/2021	09/03/2021
2.4.2	IPS o Sistema de Prevención de Intrusiones	08/03/2021	09/03/2021
2.4.3	SIEM o Sistema de Gestión de Eventos e Información de Serguridad	09/03/2021	10/03/2021
2.4.4	Ventajas y desventajas de cada herramienta	09/03/2021	10/03/2021
2.4.4.1	Ventajas y desventajas de IDS	10/03/2021	10/03/2021
2.4.4.2	Ventajas y desventajas de IPS	11/03/2021	11/03/2021
2.4.4.3	Ventajas y desventajas de SIEM	12/03/2021	12/03/2021
2.5	Los SIEM en la actualidad	11/03/2021	13/03/2021
2.5.1	Proveedores de SIEM	11/03/2021	13/03/2021
2.6	Problemas en las implementaciones de los SIEM	13/03/2021	14/03/2021
2.7	Plataformas SOAR: La evolución del SIEM	14/03/2021	16/03/2021
3	Las Plataformas SOAR	16/03/2021	30/03/2021
3.1	Cómo surgen las Plataformas SOAR	17/03/2021	18/03/2021
3.2	Plataformas SOAR actuales	18/03/2021	19/03/2021
3.3	Componentes y funcionamiento de una Plataforma SOAR	19/03/2021	20/03/2021
3.3.1	Orquestación y automatización de la seguridad (SOA)	20/03/2021	21/03/2021
3.3.1.1	Automatización	20/03/2021	21/03/2021
3.3.1.2	Orquestación	20/03/2021	21/03/2021
3.3.2	Plataformas de respuesta a incidentes de seguridad (SIRP)	22/03/2021	22/03/2021
3.3.3	Plataformas de inteligencia de amenazas (TIP)	22/03/2021	23/03/2021
3.3.4	El mercado de los SOAR	22/03/2021	25/03/2021
3.3.4.1	Aspectos clave	22/03/2021	22/03/2021
3.3.4.2	Precauciones a la hora de adquirir una solución SOAR	23/03/2021	23/03/2021
3.3.4.3	¿Qué están haciendo los proveedores de SIEM?	24/03/2021	24/03/2021
3.3.4.4	Principales proveedores de SOAR	25/03/2021	25/03/2021
3.3.4.5	Aspectos a destacar	25/03/2021	25/03/2021
3.4	Trabajando de manera inteligente con SOAR	26/03/2021	28/03/2021
3.4.1	Casos de uso	26/03/2021	28/03/2021
3.5	Beneficios y retos de las Plataformas SOAR	28/03/2021	29/03/2021
3.6	Enfoque evolutivo de la tecnología SOAR y la IA	29/03/2021	30/03/2021
	Entrega PEC2	30/03/2021	30/03/2021
4	**Implementación de un SOAR**		
4.1	Proyecto TheHive	31/03/2021	08/04/2021
4.1.1	The Hive	02/04/2021	05/04/2021
4.1.2	MISP	03/04/2021	06/04/2021
4.1.3	Cortex	04/04/2021	07/04/2021
4.1.4	Almacenamiento	04/04/2021	07/04/2021
4.2	Arquitecturade TheHive	06/04/2021	08/04/2021
4.3	Cómo funciona TheHive	09/04/2021	10/04/2021
4.4	Instalación y configuración de TheHive	15/04/2021	21/04/2021
4.5	SOAR en nube	13/04/2021	16/04/2021
4.5.1	Amazon GuardDuty	17/04/2021	18/04/2021
4.5.2	Azure Sentinel	19/04/2021	20/04/2021
4.5.3	Google Chronicle	21/04/2021	22/04/2021
4.6	Pruebas de concepto	17/04/2021	23/05/2021
	Entrega PEC3	27/04/2021	27/04/2021
4.7	Revisión de la memoria	22/05/2021	25/05/2021
5	**Presentacion**		
5.1	Conclusiones y defensa del TFM	26/05/2021	01/06/2021
	Entrega PEC4	01/06/2021	01/06/2021
5.2	Preparación Vídeo	01/06/2021	08/06/2021
5.3	Entrega Video	08/06/2021	08/06/2021
5.4	Preparación Defensa	08/06/2021	13/06/2021
	Defensa del TFM	16/06/2021	16/06/2021

Ilustración 1. Diagrama de Gantt

1.5 Breve sumario de productos obtenidos

Se obtendrá la memoria final del proyecto junto con el vídeo de la defensa, así como un vídeo a modo de prueba de concepto de cómo funciona una plataforma SOAR “on premise”, como es el Proyecto TheHive y una plataforma SOAR en nube como es AWS GuardDuty.

1.6 Breve descripción de los otros capítulos de la memoria

El trabajo consta de los siguientes capítulos:

- **Introducción**. Capítulo en el que se listan los objetivos y la forma de conseguirlos referentes a la realización del TFM.

- **Análisis y Monitoreo de Seguridad**. El segundo capítulo versa sobre las ventajas de monitorizar las comunicaciones con el objetivo de detectar e investigar incidentes de seguridad.

- **Las Plataformas SOAR**. El tercer capítulo, se centra en las Plataformas SOAR como soluciones para la detección, investigación y análisis de amenazas.

- **Implementación de un SOAR**. El tercer capítulo principalmente práctico, se centra en la implementación de un SOAR basándonos en el Proyecto TheHive.

- **Conclusiones**. El cuarto y último capítulo está relacionado con las conclusiones finales y líneas a desarrollar en el futuro.

1.7 Estado del Arte

A medida que las plataformas SOAR evolucionan, requieren menos experiencia por parte de los usuarios. Los proveedores integran la experiencia en seguridad en los productos, en forma de playbooks prediseñados, flujos de trabajo de investigación guiada y priorización automatizada de alertas.

Las funciones de automatización y orquestación también han alcanzado un nivel de sofisticación en el que pueden integrarse dentro de un marco de seguridad existente sin depender de que los usuarios sepan exactamente qué se debe automatizar. Las plataformas SOAR mantendrán a los analistas involucrados al exigir aprobaciones para acciones importantes, pero ya no se espera que los analistas sean expertos en automatización y orquestación.

Además, la capacidad de las plataformas SOAR para recopilar y contextualizar inteligencia sobre amenazas facilita que los analistas menos experimentados tomen las decisiones correctas durante la respuesta a incidentes. Debido a que los avances técnicos están sucediendo tan rápidamente, las empresas compran herramientas rápidamente, pero no están tan comprometidas a invertir en la capacitación y contratación necesarias para integrar y ejecutar la tecnología en su entorno único. Los avances de SOAR están ayudando a cerrar esta brecha.

Lo emocionante es que SOAR sigue siendo una categoría relativamente nueva y todavía quedan muchas innovaciones por venir. La automatización y la orquestación han evolucionado

hasta convertirse en herramientas indispensables, y pronto se complementarán en muchas plataformas con el aprendizaje automático, la inteligencia artificial y otras tecnologías emergentes.

Es fácil sentirse ansioso por el futuro cercano de la ciberseguridad, con métodos sofisticados de ataque, piratería informática patrocinada por el estado y falta de personal calificado para defenderse de estas amenazas. Sin embargo, SOAR debería ser la fuente de cierto optimismo para los equipos de seguridad, con su creciente capacidad para ser un multiplicador de fuerzas en el SOC.

2. Análisis y Monitoreo de Seguridad

2.1 Introducción

Entre 1984 y 1986, varios investigadores realizaron múltiples investigaciones sobre el sistema de detección de intrusiones. De entre ellos destaca James P. Anderson[1] el cuál participó en muchos estudios sobre vulnerabilidades y seguridad de la información. En 1980 presentó una investigación sobre la detección de intrusiones basada en pistas de auditoría, actualmente conocido como sistema de detección de intrusiones (IDS).

A mediados de la década de 1990, los productos IDS fueron comercializados por primera vez. En 1995 NetRanger era un conocido IDS de Wheelgroup que funcionaba escaneando el tráfico de la red. Cisco adquirió Wheelgroup en febrero de 1998; hoy, forma parte intrínseca de la seguridad de Cisco. Se comenzó a emplear la técnica de reconocimiento de firmas lo cual requería una continua actualización de las bases de datos para reconocer nuevos ataques, aún más, cuando la conmutación de red y paquetes comenzó a aumentar incrementándose la velocidad de megabits a gigabits por segundo. Este supuso un gran desafío, ya escanear, analizar el tráfico y detectar ataques en tiempo real se volvió más complicado; por lo tanto, los investigadores se vieron obligados a diseñar un IDS adecuado para redes de alta velocidad. Esto llevó a la invención de IDS basados en host, por ejemplo, TCP Wrappers, Tripwire y Snort, que proporcionaban análisis de registros del sistema en tiempo real.

Hoy en día, a medida que avanza la funcionalidad de IDS, los atacantes exploran medios para detectar, omitir y deshabilitar IDS antes de penetrar en la infraestructura. Los expertos en seguridad tienen como objetivo frenar estos ataques mediante el uso de IDS, IPS, SIEM y SOAR. Debido al número creciente de vulnerabilidades, la identificación del ataque el beneficio que supone actuar sobre él en el menor tiempo posible es esencial.

Además, en los últimos tiempos, el mundo digital se ha vuelto cada vez más complejo, conceptos como traer su propio dispositivo (BYOD), Internet de las cosas (IoT) y la computación

[1] Anderson, J.P.: Computer Security Planning Study. Washington (1972) *https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72.pdf*

en la nube están muy escaladas, son muy dinámicas y están fuera de nuestras formas tradicionales de control basados en la seguridad. Esto da como resultado una falta de visibilidad e incapacidad para hacer cumplir las políticas.

Esta complejidad también crea una brecha de habilidades dentro de las organizaciones; muchas están intentando utilizar tecnologías más autónomas e inteligentes para tratar de cerrar esta brecha. La reducción de la complejidad de las operaciones de seguridad es un objetivo clave para muchas organizaciones.

2.2 Proteger la información

Las organizaciones quieren proteger la información contenida en sus redes informáticas; sin embargo, el hecho de que en la actualidad tanto usuarios internos como externos de la red puedan conectarse de forma local o remota, incrementa considerablemente la probabilidad de que ésta sea atacada, razón por la cual se han desarrollado diferentes herramientas y estrategias, tanto de hardware como de software, para detectar y prevenir accesos intrusivos a la red con intenciones maliciosas.

Para evitar ataques procedentes de fuentes externas existen:

- Cortafuegos (firewalls) y
- Redes Privadas Virtuales (VPNs).

Tales herramientas restringen el tráfico de servicios desconocidos, en el caso de los cortafuegos, mediante el bloqueo de puertos. Ante estos dispositivos los atacantes aún tienen forma de vulnerar la seguridad desde el exterior encapsulando los ataques en el tráfico en servicios permitidos por el dispositivo. Ante esta situación, estas herramientas no son capaces de controla los ataques que se generan desde el interior de la red. Para subsanar este inconveniente se han desarrollado sistemas monitorización de redes que analizan el tráfico que entra o sale de una red y son de vital importancia para la seguridad de la red de las empresas identificando el tráfico malicioso y, una vez detectado y aprendido el ataque por parte del sistema, lo bloquean, documentan e incluso lo contrarrestan tomando represalias contra el posible atacante.

2.2.1 Controles de seguridad

Los controles de seguridad son contramedidas o salvaguardas que se utilizan para reducir las posibilidades de que una amenaza aproveche una vulnerabilidad.

Si bien, es casi imposible prevenir todas las amenazas, la mitigación del riesgo busca disminuir el riesgo al reducir las posibilidades de que una amenaza aproveche una vulnerabilidad.

Ilustración 2. Mitigación del Riesgo[2]

La mitigación de riesgos se logra mediante la implementación de diferentes tipos de controles de seguridad en función de:

- El objetivo de la contramedida o salvaguardia.
- El nivel al que se debe minimizar el riesgo.
- La gravedad del daño que puede infligir la amenaza.

El objetivo principal de implementar controles de seguridad es prevenir o reducir el impacto de un incidente de seguridad.

La implementación efectiva de un control de seguridad se basa en su clasificación en relación con el incidente de seguridad.

Los tipos de clasificaciones comunes se enumeran a continuación junto con su descripción correspondiente:

- Controles preventivos: intentan evitar que ocurra un incidente.
- Controles detectivos: intentan detectar incidentes después de que hayan ocurrido. Entre los principales controles detectivos se encuentran:
    - Monitoreo de registros
    - SIEM
    - Auditorías de seguridad
- Controles correctivos: intentan revertir el impacto de un incidente. Entre los principales controles correctivos se encuentran:
    - IDS
    - Copias de seguridad y recuperación del sistema.

Implementar los controles enumerados no es un asunto trivial.

Por ejemplo, una organización que otorga una alta prioridad a la reducción del riesgo, generalmente tiene un perfil de riesgo que contempla el costo potencial de un riesgo que impacta negativamente y los recursos humanos requeridos para implementar los controles.

---

[2] *extraído de: https://purplesec.us/security-controls/#Detective*

La estratificación es un enfoque que combina múltiples controles de seguridad para desarrollar lo que se llama una estrategia de defensa en profundidad.

La defensa en profundidad es una estrategia común utilizada en seguridad cibernética mediante la cual se implementan múltiples capas de control.

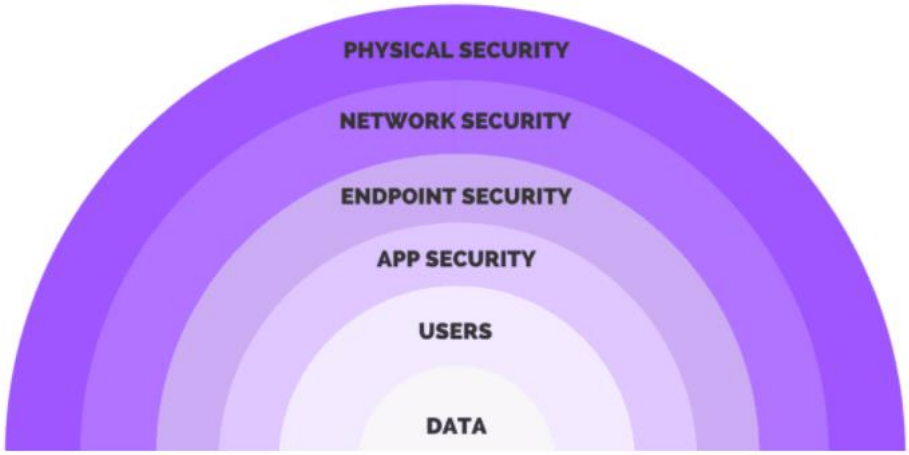


Ilustración 3. Capas de control[3]

Al combinar controles en múltiples capas de seguridad, se asegura que, si una capa no contrarresta una amenaza, las otras capas ayudarán a prevenir una brecha en sus sistemas.

Cada capa de seguridad trabaja para contrarrestar amenazas específicas, lo que requiere que los programas de seguridad cibernética inviertan en múltiples tecnologías y procesos para evitar que los sistemas o las personas se vean comprometidos.

Por ejemplo, las soluciones de respuesta y detección de endpoints son excelentes para evitar que los virus y el malware infecten computadoras y servidores. Sin embargo, la detección de endpoints no está preparada para registrar y monitorizar el tráfico en una red como un SIEM, o detectar y prevenir un ataque en tiempo real como un IPS.

2.3 Características

La monitorización de redes es uno de los pilares de la defensa en profundidad de los sistemas. La monitorización permite conocer, entre otros, el comportamiento en las comunicaciones e identificar acciones fuera de lo habitual, bien sea por tipo de tráfico, por el momento en el que se llevan a cabo o por su volumen.
El proceso de monitorización consiste en:

- la recolección,
- análisis y
- escalado de indicadores y alertas

[3] *extraído de: https://purplesec.us/security-controls/#Detective*

con el objeto de detectar y responder a intrusiones, aunque también se puede ver como la manera de encontrar agentes ajenos a la red y llevar a cabo las acciones necesarias antes de que dañen los sistemas.

Algunos de los beneficios más importantes que puede proporcionar esta estrategia aplicada de forma correcta son:

- **Detectar y corregir comportamientos anómalos**: Un buen sistema de monitorización ayuda a detectar malos hábitos, carencias de capacidad, servicios que consumen el ancho de banda de la red y, por supuesto, focos de problemas.
- **Gestionar la calidad del servicio con exactitud**: la gran mayoría de herramientas de monitorización permiten crear indicadores en los que visualizar el estado del servicio en intervalos predefinidos configurables.
- **Visualización rápida y sencilla**: Casi cualquier cosa se puede representar en una gráfica, lo que permite hacer análisis visuales de correlación a un operador entrenado, y de un vistazo comprobar que todo va bien en la monitorización de red.

Ilustración 4. Detección de Intrusiones

2.4 Herramientas y Plataformas de Supervisión de la Seguridad

Hacer una distinción entre herramientas y plataformas no es un juego de palabras. Al contrario, refleja el patrón básico de evolución que se puede observar en muchas categorías de soluciones de ciberseguridad a lo largo del tiempo, desde una mezcla de herramientas de nivel inferior para personal de TI técnico especializado hasta la autointegración empresarial de soluciones puntuales, la integración de proveedores de conjuntos de productos e integración de plataformas de proveedores y ecosistemas.

Un informe reciente de IBM y Aberdeen Research, "El valor comercial de una plataforma de análisis y monitoreo de seguridad"[4], encuestó a casi 11.000 instalaciones actuales de

[4] *https://www.ibm.com/account/reg/us-en/signup?formid=mrs-form-12163*

soluciones en la categoría de análisis y monitoreo de seguridad, y proporciona algunas ideas interesantes basadas en hechos sobre la situación actual y la adopción de herramientas en el mercado frente a plataformas.

Los sistemas IDS, IPS y SIEM monitorizan el tráfico que entra o sale de una red y son de vital importancia para la seguridad de la red de las empresas, pero cada uno de ellos cuenta con sus propias características, así como ventajas e inconvenientes. Aunque las tres herramientas se usan para **monitorizar y detectar intrusiones en los equipos o en la red** de la empresa son diferentes entre sí.

Estas herramientas **permiten** a las empresas **enfrentarse**, ya sea de forma pasiva (automatizada) o activa **a las amenazas que puedan afectar al buen funcionamiento de los sistemas**, como pueden ser redes de comunicaciones, dispositivos o sensores IoT, ya que en menor o mayor medida ayudan a detectar y neutralizar las intrusiones, amenazas o comportamientos sospechosos que ponen en riesgo la ciberseguridad de la empresa. Dicho de otra manera, son un paso natural en la evolución de la ciberseguridad. A continuación, describimos cada una de ellas.

2.4.1 IDS o Sistema de Detección de Intrusiones

Es una aplicación usada para **detectar accesos no autorizados a un ordenador o a una red**, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, **emiten una alerta a los administradores del sistema** quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas **sólo detectan los accesos sospechosos** emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es **reactiva**.

2.4.2 IPS o Sistema de Prevención de Intrusiones

Es un software que se utiliza para **proteger a los sistemas de ataques e intrusiones**. Su actuación es **preventiva**. Estos sistemas llevan a cabo un **análisis en tiempo real** de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y **permitiendo el control de acceso a la red**, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

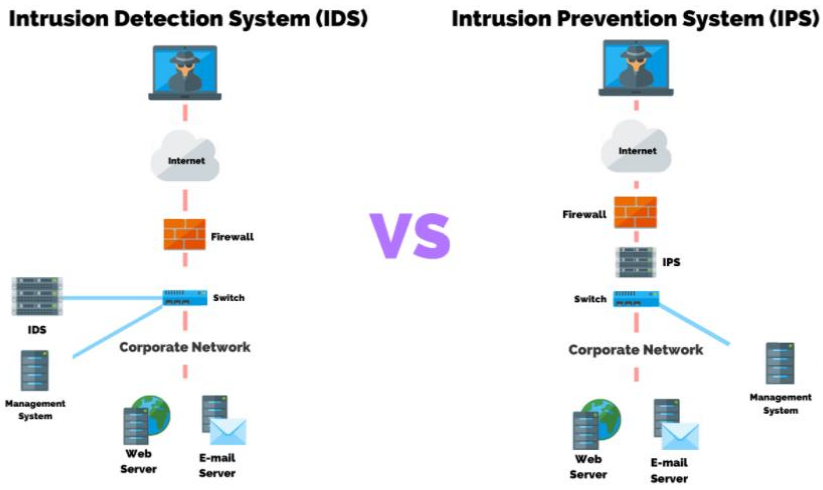


Ilustración 5. Comparativa IDV vs IPS[5]

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés, Unified Threat Management o Gestión Unificada de Amenazas) que controlan el acceso en función de reglas sobre protocolos y sobre el destino u origen del tráfico.

2.4.3 SIEM o Sistema de gestión de Eventos e Información de Seguridad

Es una **solución híbrida centralizada** que engloba la **gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager).** La tecnología SIEM proporciona un **análisis en tiempo** real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red. Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una **herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas**.

[5] *https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/*

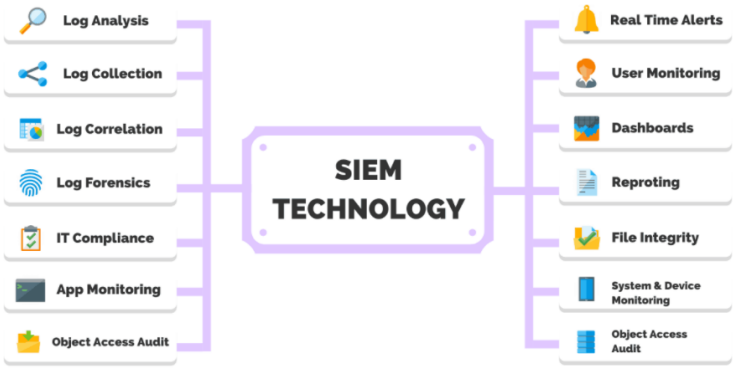


Ilustración 6. Características de los SIEM[6]

2.4.4 Ventajas y desventajas de cada herramienta

2.4.4.1 Ventajas y desventajas de IDS

Las principales ventajas de un sistema IDS son:

- Permite ver lo que está sucediendo en la red en tiempo real en base a la información recopilada,
- Reconocer modificaciones en los documentos y
- Automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red.

Su principal desventaja es qué estas herramientas, sobre todo en el caso de las de tipo pasivo:

- No es están diseñadas para prevenir o detener los ataques que detecten y,
- Son vulnerables a los ataques DDoS que pueden provocar la inoperatividad de la herramienta.

2.4.4.2 Ventajas y desventajas de IPS

Las ventajas de un IPS son:

- Escalabilidad al gestionar multitud de dispositivos conectados a la misma red;
- protección preventiva al comprobarse de forma automatizada comportamientos anómalos mediante el uso de reglas prefijadas;
- Fácil instalación, configuración y administración al estar disponibles multitud de configuraciones predefinidas y centralizar en un punto su gestión, aunque puede ser contraproducente para su escalabilidad;
- Defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;
- Aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Entre sus desventajas, destacan:

---

[6] *https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/*

- Los efectos adversos que pueden producirse en el caso de que se detecte un falso positivo, si por ejemplo se ejecuta una política de aislamiento de las máquinas de la red o
- En el caso de que se reciban ataques de tipo DDoS o DoS pueden quedar inutilizados.

2.4.4.3 Ventajas y desventajas de SIEM

Entre las ventajas de contar con un SIEM destacan:

- La **centralización de la información y eventos**, es decir, se proporciona un punto de referencia común. La centralización permite automatizar tareas, con su consiguiente ahorro de tiempo y costes, el seguimiento de los eventos para detectar anomalías de seguridad o la visualización de datos históricos a lo largo del tiempo.
- Los sistemas SIEM muestran al administrador la existencia de vulnerabilidades, así como si están siendo aprovechadas en los ataques.

Entre sus desventajas, en el caso de que se encargue de su mantenimiento un departamento de la empresa destacan:

- Altos costes de implantación.
- Una curva de aprendizaje larga al tener que formar personal propio para esta tarea y una integración limitada con el resto del sistema.

En el caso de que se externalice esta tarea se experimenta una pérdida de control de la información generada o un acceso limitado a determinada información y una fatiga por la alta recepción de notificaciones. Estos aspectos pueden gestionarse con el proveedor del servicio a través de los acuerdos de nivel de servicios o ANS.

2.5 Los SIEM en la actualidad

A medida que las tecnologías evolucionan, también las amenazas de ciberseguridad y los vectores de ataque. Los usuarios con intenciones maliciosas utilizan herramientas y tecnologías sofisticadas para ataques dirigidos que se pueden ejecutar más rápido para capturar gran cantidad de datos y/o causar más daño. Y para defender estos ataques, las herramientas y tecnologías de seguridad también están evolucionando.

El término actual SIEM fue acuñado por dos analistas de Gartner. En un informe de de 2005 titulado "Mejorar la seguridad de TI con gestión de vulnerabilidades"[7], los analistas propusieron un nuevo sistema de información de seguridad basado en dos tecnologías de generación anterior conocidas como Gestión de información de seguridad (SIM) y Gestión de eventos de seguridad (SEM).

[7] *https://www.gartner.com/en/documents/480703*

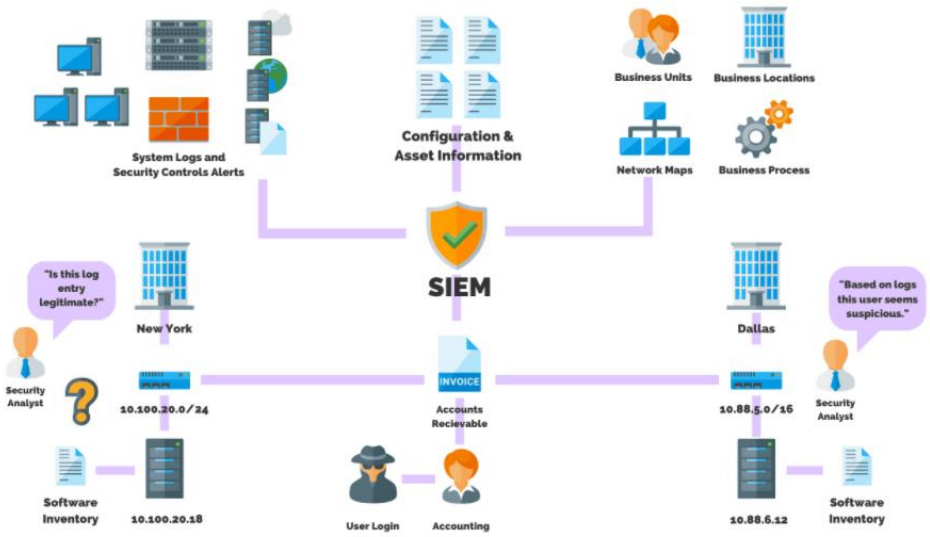


Ilustración 7. Esquema de un SIEM

La tecnología SIM de primera generación se construyó sobre los sistemas tradicionales de gestión de recopilación de registros. SIM introdujo el análisis de almacenamiento a largo plazo, la generación de informes sobre los datos de registro y los registros combinados con inteligencia de tratamiento.

La tecnología SEM de segunda generación abordó eventos de seguridad, agregación, correlación y notificación de eventos de sistemas de seguridad como antivirus, firewalls y sistemas de detección de intrusiones (IDS), así como eventos reportados directamente por autenticación, trampas SNMP, servidores y bases de datos.

Unos años después, los proveedores introdujeron una combinación de SIM y SEM para crear el SIEM, de ahí una nueva definición según la investigación de Gartner.

Una solución SIEM funciona mediante la recopilación de datos de varias fuentes, como computadoras, dispositivos de red, servidores y más. Luego, los datos se normalizan y agregan. A continuación, los profesionales de la seguridad analizan los datos para descubrir y detectar amenazas. Como resultado, las empresas pueden identificar las infracciones de seguridad y permitir que las organizaciones investiguen las alertas.

El proceso de cómo el SIEM recopila y alerta sobre eventos detectados incluye:

- Recopilación de datos de varias fuentes.
- Normalizar y agregar datos recopilados.
- Analizar los datos para descubrir y detectar amenazas.
- Identificar brechas de seguridad y permitir que las organizaciones investiguen alertas.

Ilustración 8. Solución SIEM

Los beneficios de una organización que posee un SIEM superan con creces las consecuencias de no tener un SIEM. Sin un SIEM, el personal de TI carecerá de una vista centralizada de todos los registros y eventos. Con una visibilidad limitada, el personal de TI probablemente perderá eventos críticos de sus sistemas, lo que generará una gran cantidad de eventos atrasados que pueden contener incidentes que requieren una investigación inmediata.

Por otro lado, tener un SIEM:

- Aumenta la eficiencia y mejora el programa de respuesta a incidentes.
- Tendremos un panel de control.
- Un SIEM bien ajustado puede notificar sobre una serie de categorías predefinidas y umbrales de eventos.

La mayoría de los SIEM modernos de hoy tienen inteligencia incorporada que puede detectar límites de umbral configurables y eventos por un período de tiempo determinado, junto con resúmenes e informes personalizables. Los SIEM más avanzados ahora están incorporando IA (Inteligencia Artificial) para alertar sobre el análisis de patrones y comportamiento.

Las funciones de informes y notificaciones permiten al personal de TI reaccionar y responder rápidamente a posibles incidentes. Esta inteligencia refuerza la capacidad del SIEM de detectar ataques maliciosos antes de que ocurran, como la detección de patrones de eventos que se asemejan a las primeras etapas de un ataque de ransomware.

La presencia del SIEM en la red puede reducir el costo de una violación de seguridad en toda regla, lo que le ahorra a una organización una cantidad incalculable de ingresos y pérdida de reputación.

2.5.1 Proveedores de SIEM

Dado que Gartner es responsable del acrónimo SIEM, es un buen recurso para identificar los mejores y peores SIEM. La razón por la que mencionamos el Cuadrante Mágico de SIEM Gartner es que SIEM como SOAR son tecnologías contemporáneas en seguridad cibernética, trabajan muy de cerca, y el crecimiento de SIEM como tecnología está estrechamente relacionado con el crecimiento de SOAR en el futuro. Por supuesto, SIEM como término se

acuñó en 2005, mientras que SOAR saltó a la fama en 2017, pero las operaciones de estas dos tecnologías están estrechamente entrelazadas.

Para el análisis de herramientas SIEM hemos estudiado el Cuadrante Mágico de Gartner de febrero de 2020 y el informe que realiza Forrester de Plataformas de Análisis de Seguridad en el último trimestre de 2020, considerándolas dos de las más reconocidas consultoras tecnológicas en la actualidad.

Ilustración 9. Cuadrante Mágico de Gartner[8] y Onda de Forrester[9]

La consultora Forrester prefiere evaluar proveedores de Plataformas de Seguridad sin clasificarlas como proveedoras de SIEM.

Ilustración 10. Líderes del mercado SIEM

[8] *https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage*

[9] *https://www.bankinfosecurity.com/whitepapers/forrester-wave-security-analytics-platforms-q4-2020-w-7414*

Para el presente documento hemos analizado, en detalle, los cuatro productos líderes coincidentes entre Gartner y Forrester y con las diferentes características, hemos elaborado las siguientes tablas:

<table>
<tr><td colspan="2"> 

Compañía fundada en 2003 por Michael Baum, Erik Swan y Rob Das. El nombre "Splunk" proviene del término inglés que hace referencia a la exploración de cuevas, ya que se asemeja a lo que hace Splunk: espeleología en los datos del usuario. Tiene sus oficinas centrales en San Francisco.</td></tr>
<tr><td colspan="2">Productos</td></tr>
<tr><td colspan="2">• Splunk Enterprise
• Splunk Cloud. SaaS que utiliza la infraestructura de AWS.</td></tr>
<tr><td colspan="2">Módulos</td></tr>
<tr><td colspan="2">• Splunk Enterprise Security (ES). ofrece la mayor parte del contenido de seguridad y las capacidades de monitoreo de eventos, incluidas consultas, visualizaciones y paneles de control específicos de seguridad, y algunas capacidades de gestión de casos, flujo de trabajo y respuesta a incidentes.
• Splunk UBA. Agrega analítica avanzada no supervisada, impulsada por Machine Learning.
• Splunk Phantom. Proporciona capacidades SOAR y está diseñado para proporcionar corrección y mitigación automatizadas de incidentes de seguridad.</td></tr>
<tr><td>Fortalezas</td><td>Aspectos a mejorar</td></tr>
<tr><td>• Las múltiples opciones de implementación: on premise, IaaS o Híbrido.
• El enfoque de Splunk para proporcionar recopilación y análisis de datos centralizados, con soluciones premium además del producto principal, atrae a las organizaciones que desean una solución que pueda admitir varios equipos.
• Splunk ha fomentado un ecosistema denso de socios y alianzas tecnológicas capaces de extender el valor nativo de Splunk a través de aplicaciones que son específicas para casos de uso o proveedores.
• Los clientes de Splunk otorgan altas calificaciones por la facilidad de integración, la calidad y disponibilidad para la capacitación del usuario final y la calidad de la comunidad de pares, en comparación con su competencia.</td><td>• La valoración general del cliente en cuanto a la evaluación y negociación de contratos, servicio y soporte, precios y flexibilidad de contratos, y la relación calidad-precio están por debajo de la mayoría de sus competidores.
• La falta de sensores de red y de endpoint requiere que los compradores busquen soluciones complementarias de terceros para cumplir con los requisitos de un SOC moderno (por ejemplo, SIEM + UEBA + SOAR + EDR + NTA).
• Splunk UBA todavía no está integrado en el núcleo de Splunk y sigue siendo un modelo local o alojado, lo que puede afectar a los compradores de Splunk Cloud.
• El contenido de Splunk está disponible en diferentes plataformas, se debe tener una licencia por separado para acceder a ese contenido y requiere múltiples mecanismos para organizar y actualizar el contenido.</td></tr>
</table>

Ofrece una gama de tecnologías y servicios de seguridad y tiene su sede en Cambridge, Massachusetts.

Productos

- QRadar SIEM
- QRadar on Cloud (QROC), basada en la nube de IBM

Módulos

- IBM QRadar Vulnerability Manager: integración de datos de evaluación de vulnerabilidades.
- IBM QRadar Network Insights: visibilidad de aplicaciones e inspección de contenido de paquetes.
- QRadar Risk Manager: capacidades de simulación de amenazas y supervisión de dispositivos de red.
- IBM QRadar User Behavior Analytics (UBA): módulo complementario gratuito que aborda algunos casos de uso de amenazas internas.
- IBM QRadar Incident Forensics: soporte de investigación forense.
- IBM QRadar Advisor con Watson: motor de atribución e identificación basado en análisis avanzado.
- IBM también ofrece Security App Exchange, que permite a los clientes de QRadar descargar contenido seleccionado desarrollado por IBM o por terceros.
- IBM Resilient: una solución SOAR que soporta integración entre Resilient y la solución QRadar SIEM.

Fortalezas	Aspectos a mejorar
• IBM cuenta con amplios recursos internos y asociaciones para respaldar las ventas, la implementación y el soporte operativo, incluidos los servicios administrados para QRadar, en múltiples regiones geográficas. • Ofrece a los usuarios amplias opciones en la arquitectura de implementación, con una variedad de factores de forma que se pueden implementar en varias combinaciones. • Tiene una extensa API abierta para permitir que los clientes y socios desarrollen integraciones con la plataforma. El mercado de aplicaciones tiene amplias integraciones proporcionadas por IBM y por terceros. • Ofrece sólidas capacidades para gestionar la recopilación de eventos. • QRadar incluye UBA en la licencia base por lo que no hay ningún costo adicional para adquirir UBA. • QRadar Advisor with Watson ofrece un sólido soporte para la investigación de incidentes al proporcionar un enriquecimiento del contexto de fuentes internas y externas, sugiriendo los siguientes pasos basados en las acciones de los atacantes y priorizando las alertas para acciones futuras.	• Los diversos modelos de licencias y esquemas de precios para los diversos componentes asociados con la plataforma QRadar presentan un conjunto complejo de opciones para los clientes potenciales. • QRadar ofrece opciones limitadas para la recopilación de datos para análisis forense de endpoints/ hosts. • La falta de capacidad EDR nativa de IBM contrasta con las capacidades más completas para el monitoreo de redes. Los clientes deben implementar productos de terceros o confiar en su agente WinCollect o en la colección Sysmon para Windows. • La modernización de la experiencia del usuario (UX) para QRadar todavía es un trabajo en progreso y la interfaz de usuario no es coherente en los diversos componentes de la plataforma. • Los componentes de la plataforma QRadar se encuentran en diferentes niveles de madurez e integración con otros componentes y con las nuevas ofertas de gestión de la nube de IBM. • El análisis de Qradar, los perfiles de comportamiento, y los procesos de ventas / contratación del proveedor son áreas de mejora.

Compañía con sede en Foster City, California, creada en 2013. El nombre proviene de la conjunción de Exa como referencia la gran cantidad de datos que procesaría en el orden de exabyte y el producto sería como un haz de luz entre tantos registros[10].

Productos

- Plataforma de gestión de seguridad (SMP) de Exabeam. Está disponible como software para implementaciones locales y se ofrece como un SIEM basado en la nube, alojado y administrado por Exabeam.

Módulos

- Exabeam Data Lake: recopila datos desde cualquier lugar, ya sea local, remoto o en la nube
- Exabeam Cloud Connectors: permite recopilar registros de más de 40 servicios en la nube, como AWS, GitHub, Google, Microsoft Office 365, Salesforce y muchas otras aplicaciones de seguridad.
- Exabeam Advanced Analytics: detecta los comportamientos indicativos de una amenaza.
- Exabeam Threat Hunter: simplifica el proceso de creación de consultas de búsqueda complejas.
- Exabeam Entity Analytics: establece el comportamiento de referencia para los patrones de comunicación, el uso de puertos y protocolos y la actividad operativa.
- Exabeam Case Manager: centraliza toda la evidencia de incidentes de seguridad en en un solo lugar.
- Exabeam Incident Responder: Orquestación centralizada de la seguridad.

Fortalezas	Aspectos a mejorar
• SMP permite la adopción por fases de capacidades que pueden comenzar con un SIEM central (Data Lake, Advanced Analytics, Case Manager) y luego expandirse a Incident Responder para SOAR o Cloud Connectors para casos de uso de SaaS e IaaS. • Exabeam SMP proporciona una base sólida para monitozar usuarios, entidades e identidades. Lo realiza con el módulo de análisis central (Advanced Analytics) a través de las características nativas de UEBA. • Smart Timelines de Exabeam es compatible con los usuarios de SIEM menos experimentados al aprovechar el aprendizaje automático (ML) para organizar registros y eventos relevantes en una vista de línea de tiempo, lo que simplifica las actividades de investigación y respuesta. • El modelo de precios de Exabeam es simple. • Exabeam ha demostrado un fuerte crecimiento y una mayor visibilidad. • Los clientes evalúan positivamente varios elementos, como servicios de implementación y soporte, evaluación y contratos.	• Aunque tiene operaciones de ventas en múltiples geografías, todavía es comprado principalmente por en América del Norte. Los compradores fuera de Norteamérica deben validar la cobertura de ventas, servicios profesionales y soporte (ya sea directo o a través de socios) para las ubicaciones de sus organizaciones. • Aún está desarrollando su red de socios, especialmente para servicios como SIEM administrado. • Debería definir mejor las capacidades relevantes para los compradores en industrias verticales en las que los desafíos pueden ser diferentes a los del público general de compras (por ejemplo, energía y servicios públicos). • Puede mejorar su integración e implementación, y la facilidad de personalización de reglas existentes, informes predefinidos y calidad y estabilidad del producto.

[10] *https://www.exabeam.com/about/*

Securonix tiene su sede en Addison, Texas.

Productos

- Securonix Next-Gen SIEM. Cloud SIEM en SaaS basado en AWS.

Módulos

- Securonix Next-Gen SIEM: combina la gestión de registros; análisis de comportamiento de usuarios y entidades (UEBA); y orquestación, automatización y respuesta de la seguridad en una plataforma completa de operaciones de seguridad de extremo a extremo.
- Securonix Security Data Lake: plataforma de datos abierta y altamente escalable que ingiere cantidades masivas de datos.
- Securonix UEBA: aprovecha el aprendizaje automático sofisticado y el análisis de comportamiento para analizar y correlacionar las interacciones entre usuarios, sistemas, aplicaciones, direcciones IP y datos.
- Securonix SOAR: ayuda a los equipos de operaciones de seguridad a mejorar sus tiempos de respuesta a incidentes proporcionando automatización, sugiere guías y pasos para guiar a los analistas.
- Securonix NTR: monitoreo avanzado de amenazas que combina tráfico de red, registros de seguridad y contexto de entidad.

Fortalezas	**Aspectos a mejorar**
• Tiene un sólido compromiso y soporte en la nube. Su SIEM es nativo de la nube y se ofrece como un servicio, con tres modelos de inquilinos diferentes (compartido, dedicado y aislado). • Ofrece análisis multicapa, con capacidades UEBA para análisis avanzado y modelado de comportamiento en usuarios y entidades. • Securonix proporciona un extenso contenido listo para usar, organizado en paquetes verticales. Incluye casos de uso completos, análisis, alertas, paneles e incluso guías de respuesta. • La introducción de SNYPR-EYE proporciona a los administradores de SIEM aislamiento de las tecnologías de Hadoop, al tiempo que permite que aquellos con recursos suficientes accedan a las infraestructuras subyacentes de Hadoop. • Ofrece funciones de ofuscación avanzadas, con flujos de trabajo de control de acceso basado en roles (RBAC), así como funciones de cifrado nativas que van más allá de las proporcionadas de forma nativa por AWS. • Securonix recibe altas calificaciones por sus capacidades de análisis y monitoreo de usuarios.	• El enfoque de Securonix para llenar los vacíos de cobertura funcional por parte de revendedores y asociaciones de tecnología presenta riesgos, porque se crean dependencias. • Los esfuerzos de Securonix en el marketing de su marca y herramientas necesitan una inversión continua y deberían aprovechar mejor su alianza tecnológica, relaciones con socios. • Será difícil para Securonix SIEM continuar abordando casos de uso complejos y organizaciones maduras, sin dejar de ser lo suficientemente simple como para atraer a organizaciones no maduras. • La habilitación de la cobertura funcional completa de Securonix SIEM requiere esfuerzo y experiencia.

2.5.1.1 Aspectos a destacar

Después de analizar las principales características que los principales SIEM del mercado para este trabajo podemos destacar los siguientes aspectos:

- Los SIEMs más destacados tienen sedes centrales en Estados Unidos.
- Los principales SIEMs del mercado son modulares. Dicha modularidad, permite gran flexibilidad de adquisición, pero añade complejidad a las implementaciones.
- Todas incluyen módulos de análisis de comportamiento (UBA o UEBA) a través de machine learning.
- Incluyen un módulo opcional con características de SOAR.
    - Splunk → Splunk Phantom
    - IBM Security → IBM Resilient
    - Exabeam → Exabeam Incident Responder
    - Securonix → Securonix SOAR
- Todas deben mejorar sus integraciones con los dispositivos de la red y endpoint.
- Proporcionan servicios en nube:
    - Nube propia: IBM Security y Exabeam
    - Nube de terceros: Splunk (AWS) y Securinox (nativo de la nube de AWS)
- Están en constante evolución, la tendencia a la prestación de servicio en nube está al alza.

2.6 Problemas en las implementaciones de los SIEM

Los SIEM han supuesto un gran paso a la hora del registro y gestión de amenazas, pero también tienen sus problemas y desventajas:

- La inversión en una solución SIEM completa puede resultar cara.
- No es el tipo de herramienta "configúrelo y olvídese". Es una tecnología compleja que requiere ingenieros y analistas de TI capacitados para administrar y brindar soporte.
- El personal de TI que respalda el SIEM debe ser capaz de ajustar el sistema para eventos relevantes, interpretar patrones de ataques maliciosos y haber demostrado conocimiento del proceso de respuesta a incidentes. Si el personal adecuado no supervisa el SIEM las 24 horas del día, los 7 días de la semana, los 365 días del día, agregará poco o ningún valor comercial al programa de seguridad y puede dejar a la organización vulnerable a un ataque.
- Los Proveedores de Servicios de Seguridad Administradas (MSSP) también son una opción si la experiencia técnica para administrar el SIEM no está presente dentro de la organización.

Un SIEM puede ser una inversión bastante sustancial si la organización tiene múltiples fuentes de datos que producen una gran cantidad de eventos registrados. Muchos proveedores de SIEM cobran en función de la cantidad de alertas activadas y la cantidad de almacenamiento

necesario para retener los eventos. Se requiere una investigación cuidadosa para estimar el costo total de propiedad de SIEM.

Hay varias razones por las que fallan las implementaciones de SIEM, que incluyen:

- **Falta de planificación**. Falta de estrategia para SIEM - planificación de capacidad, ejercicios limitados de prueba de concepto con múltiples proveedores, comprensión de la escalabilidad y tener el personal interno adecuado para hacer las preguntas correctas al proveedor.
- **Falta de metas y objetivos para la solución SIEM**. Liderazgo sénior no comprometido y a bordo con la implementación y el resultado de SIEM.
- **Falta de capacitación**. Se requieren los conocimientos adecuados para ajustar y configurar SIEM. Puede requerir algunos conocimientos de secuencias de comandos para productos SIEM avanzados
- **Falta de recursos de seguridad para administrar la herramienta SIEM**. La herramienta es inútil si no hay suficientes recursos capacitados para respaldar el SIEM
- **Complejidad SIEM**. Un SIEM puede generar miles de eventos por hora. El personal de soporte deberá saber cómo eliminar el "ruido de alerta" y correlacionar eventos reales para maximizar el valor del SIEM.
- **Usar SIEM únicamente para cumplimiento**. No aprovechar todo el potencial del valor SIEM, como la detección de malware, el manejo de ataques de fuerza bruta y el monitoreo del comportamiento del usuario.
- **No acelerar el valor con SIEM**. No incorporar fuentes de inteligencia de amenazas con SIEM para ayudar a mejorar la detección y respuesta de amenazas.

2.7 Plataformas SOAR: La evolución del SIEM

Las plataformas SOAR surgen principalmente por el gran volumen de amenazas y la escasez de profesionales bien formados en respuesta a incidentes.

Un SIEM es principalmente tecnología de detección. Pero no es suficiente con detectar un incidente, también hay que saber responder y hacerlo a tiempo. Para ello es preciso:

- priorizar la respuesta de unos incidentes sobre otros a través de información técnica y de negocio,
- automatizar los procesos repetitivos, liberando tiempo al analista, y
- dotar de una herramienta que permita que los equipos de seguridad e IT trabajen conjuntamente de modo efectivo.

SOAR, o Security Orchestration and Automation Response, agiliza la respuesta ante incidentes de seguridad y la toma de decisiones. Cada vez más incidentes de seguridad requieren de más especialistas capaces de hacer frente al creciente volumen de alarmas. SOAR llega para hacer frente a este reto, para sustituir los análisis manuales con decisiones automatizadas. Su función combina la recopilación de datos, estandarización, análisis de flujo de trabajo y análisis integrales para proporcionar a las organizaciones la capacidad de implementar sofisticadas capacidades de defensa en profundidad basadas en fuentes de datos internas y externas. De

forma que las herramientas de SOAR pueden mejorar la eficacia, la eficiencia y la consistencia de las operaciones de seguridad utilizando:

- la orquestación y automatización de la inteligencia de amenazas,
- la monitorización de eventos de seguridad y
- los procesos de respuesta ante incidentes.

Aunque la automatización de la seguridad es posible sin orquestación de seguridad, se ve limitada por la falta de contexto y la incapacidad para validar cuándo una acción está realmente justificada. Al combinar la automatización y la orquestación, los equipos de seguridad pueden manejar más alertas sin agregar sobrecarga.

Los equipos de seguridad son reducidos y los eventos a analizar y tratar, muchos. La aplicación de tecnología para automatizar la respuesta es fundamental.

La ventaja más significativa de una solución SOAR es la respuesta inmediata y simplificada, es decir, se produce una respuesta específica en base a un conjunto de eventos que ocurren. Y se establece una respuesta "segura" por conjunto de eventos de seguridad.

SOAR no ha venido a sustituir al SIEM, sino para complementarlo al reducir el ruido de las alertas y hacer que los datos de SIEM sean procesables.

Gartner predijo que, para finales de 2020, el 15% de las organizaciones con un equipo de seguridad de más de cinco personas aprovechará las soluciones SOAR[11]. Su enorme potencial para mejorar la eficiencia y eficacia de las operaciones de seguridad significa que es probable que desempeñe un papel crucial para ayudar a dar forma al desarrollo del futuro SIEM.

La clave para la adopción de herramientas SOAR por parte de los proveedores de soluciones SIEM será demostrar que se puede confiar en la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning) para hacer cambios en los sistemas. Si bien, las personas que toman las decisiones seguirán siendo vitales para la detección y respuesta de amenazas.

Aprovechar al máximo el SIEM, para ayudar a enfrentarnos a los crecientes desafíos de seguridad, no solo dependerá de algoritmos más inteligentes, sino de personal mejor capacitado que puedan usar los sistemas con mayor eficacia y validar alertas.

La superficie de ataque, que ya se ha transformado drásticamente desde la introducción de SIEM, continuará cambiando a gran velocidad en los próximos años. Las organizaciones solo podrán responder a estos cambios con mejores herramientas y una fuerza laboral más capacitada y eficiente.

La demanda de tecnología SIEM sigue siendo fuerte, con la gestión de amenazas como el principal impulsor. Casi todos los proveedores de SIEM están mejorando sus capacidades de investigación introduciendo integraciones para acciones de respuesta a través de capacidades nativas o soluciones SOAR adquiridas de terceros.

Si bien SIEM ha sido parte de la realidad de las empresas durante algunos años, SOAR es una tecnología que complementa SIEM para la respuesta a incidentes.

---

[11] *https://ciberseguridad.blog/por-que-las-herramientas-soar-revitalizaran-el-ecosistema-siem/*

SIEM agrega datos de seguridad de diferentes fuentes, aplica análisis para detectar posibles incidentes de seguridad y genera un evento o incidente.

SOAR usa alertas y desarrolla la respuesta para ayudar a determinar si una alerta es un incidente.

Es responsabilidad del líder del Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT), determinar el camino a seguir ante una investigación, pero SOAR ayuda permitiendo mejores decisiones y una respuesta más rápida. Por lo tanto, brindará la capacidad de respaldar la investigación y selección del mejor flujo de trabajo para responder al incidente. SOAR potencialmente puede automatizar la ejecución de los flujos de trabajo que responderán al incidente, reduciendo significativamente el tiempo de respuesta.

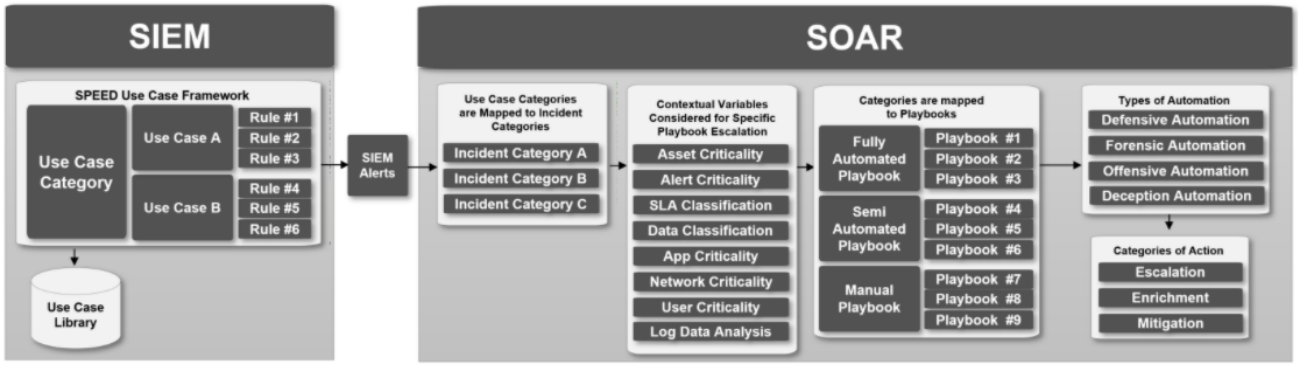


Ilustración 11. SOAR complementa a SIEM[12]

3. Las Plataformas SOAR

3.1 Cómo surgen las Plataformas SOAR

A finales de la década de 1990, los trabajos de los analistas de seguridad dependían de herramientas técnicas como TCPdump y Ethereal/Wireshark para buscar actividades sospechosas dentro de los paquetes de red. El siguiente paso fue buscar pistas a través de Syslog y esto llevó al uso de herramientas de administración de registros y luego a la evolución de SIEM en el período 1999-2000.

Ciertamente hemos progresado en los últimos años, pero hay un patrón constante. Las tecnologías de operaciones de seguridad siguen estando centradas en las amenazas y/o la telemetría. En otras palabras, cada herramienta fue diseñada para recopilar, filtrar y correlacionar elementos de datos basados en reglas, heurísticas de comportamiento o algoritmos de análisis, con el objetivo de encontrar algún tipo de aguja en un pajar en constante crecimiento.

[12] *http://correlatedsecurity.com/soar-critical-success-factors/*

El volumen de información que se procesa por los SIEM está en constante crecimiento y los equipos de seguridad deben de ser ágiles para neutralizar las amenazas en el menor tiempo posible.

El mercado de la tecnología de seguridad, en general, se encuentra en un estado de sobrecarga, con presión sobre los presupuestos, escasez de personal y demasiadas soluciones puntuales. Las empresas que usan SIEM suelen mencionar problemas de sobrecarga de eventos o alertas, complejidad y duplicación de herramientas. Ante esta situación, los fabricantes de soluciones comenzaron a automatizar tareas para facilitar la gestión de incidentes, y de esta manera en 2017, Gartner acuñó el término SOAR (Orquestación, Automatización y Respuesta de Seguridad) para describir la categoría emergente de plataformas nacidas de la respuesta a incidentes, la automatización de la seguridad, la gestión de casos y otras herramientas de seguridad.

Las plataformas SOAR están desarrolladas para ayudar a los equipos de seguridad a administrar y responder a un sinfín de amenazas a velocidad de máquina. Se adoptan principalmente para mejorar los procesos relacionados con la detección y la respuesta mediante el enriquecimiento del contexto y mejorando la priorización y la eficiencia posteriores. En la mayoría de los casos, este es el objetivo de las organizaciones y proveedores de servicios que operan centros de operaciones de seguridad (SOC). Sin embargo, las herramientas SOAR son pragmáticas y flexibles, lo que les permite aplicarse a una variedad de casos de uso de operaciones de seguridad.

Las funciones que se exigen a los SOAR son:

- **Automatización avanzada**. En lugar de simplemente desencadenar una acción de remediación discreta, los equipos de SOC requieren automatizar sus procedimientos operativos estándar (SOP) en la mayor medida posible. Esto significa alinear las acciones automatizadas con los playbooks de una manera fácil e intuitiva. Algunos proveedores proporcionan configuraciones basadas en secuencias de comandos y GUI, mientras que otros lo realizan a través de plantillas y playbooks predefinidos. La automatización avanzada también incluye la capacidad de ayudar a automatizar las actividades de los analistas (es decir, clasificación, priorización, investigaciones, etc.).
- **Orquestación de procesos a través de herramientas heterogéneas.** La palabra clave aquí es "proceso". Por ejemplo, un proceso de investigación de phishing requiere obtener datos, analizarlos, determinar incidentes de phishing, comunicar los resultados y luego tomar algún tipo de acción. Hacer esto correctamente significa perfeccionar el proceso e integrarse con los elementos tecnológicos adecuados para que esto suceda. Esto significa que los productos líderes deben tener API abiertas, soporte para desarrolladores y socios del ecosistema de tecnología de ciberseguridad. Algunos proveedores facilitan a las organizaciones la implementación de su propia orquestación, mientras que otros proporcionan playbooks basados en las mejores prácticas.
- **Manejo de casos**. Las grandes organizaciones necesitan capacidades de administración central para iniciar, monitorizar y comunicar las actividades de SOC a lo largo de los ciclos de vida de los eventos. Para la ciberseguridad, la gestión de casos también debe incluir una sólida funcionalidad de comunicaciones para permitir los procesos que requieren múltiples personas del equipo SOC o procesos compartidos entre la

ciberseguridad y las operaciones de TI. Tenga en cuenta que muchas organizaciones intentan utilizar sistemas de gestión de casos y tickets genéricos, pero a menudo me dicen que estas herramientas son inadecuadas para las necesidades de ciberseguridad.

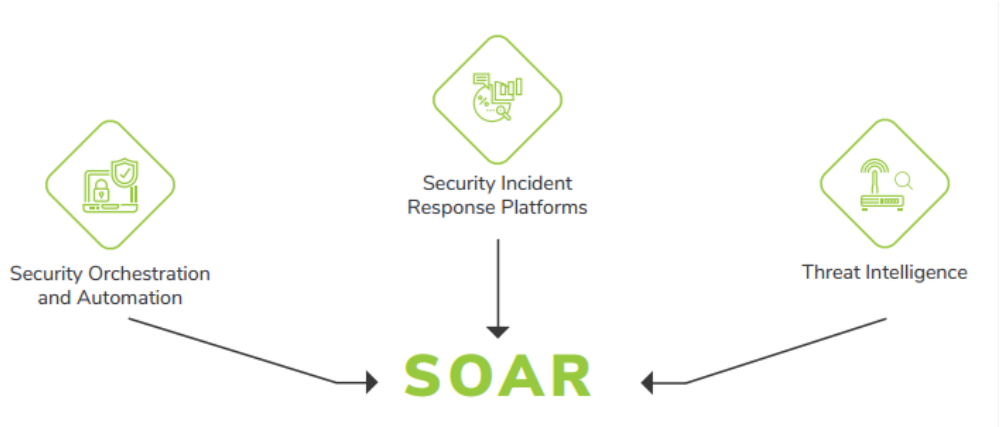


Ilustración 12. Security Orchestration, Automation and Response (SOAR)[13]

3.2 Plataformas SOAR actuales

Gartner define la orquestación, automatización y respuesta de seguridad (SOAR) como aquellas tecnologías que permiten a las organizaciones recoger entradas de una variedad de fuentes, principalmente de información de seguridad y sistemas de gestión de eventos (SIEM) y con el análisis de esa información aplicar flujos de trabajo alineados con procesos y procedimientos. Estos pueden organizarse mediante integraciones con otras tecnologías y automatizarse para lograr el resultado deseado y una mayor visibilidad. Las capacidades adicionales incluyen:

- funciones de gestión de incidentes y casos;
- la capacidad de administrar información sobre amenazas,
- paneles de control e informes;
- y análisis que se pueden aplicar a varias funciones.

Las herramientas SOAR mejoran significativamente las actividades de operaciones de seguridad, como la detección y respuesta de amenazas, al proporcionar asistencia impulsada por máquinas a analistas humanos para mejorar la eficiencia y la coherencia de las personas y los procesos. También se utilizan para documentar e implementar procesos; apoyar la gestión de incidentes de seguridad; y aplicar asistencia basada en máquinas a analistas y operadores de seguridad humanos.

Las ofertas específicas denominadas orquestación, automatización y respuesta de seguridad (SOAR) han estado en el mercado desde finales de 2017, y la mayoría se centra en cómo hacer que las funciones de detección de seguridad sean más efectivas y eficientes.

[13] *https://www.logsign.com/blog/security-orchestration-automation-and-response-soar-overview/*

La capacidad de solucionar automáticamente un problema sin tener que ser analizado y dirigido por humanos es el punto clave. Sin embargo, la verdad sobre la implementación exitosa de tales funciones es que está lejos de ser simple. El alcance de dicha funcionalidad es muy difícil y una respuesta de seguridad totalmente automatizada es un mito.

Las herramientas SOAR a menudo se malinterpretan como una "solución milagrosa" que, una vez implementada, conectará las funciones de alerta con conjuntos de herramientas preventivas como firewalls, sistemas de detección y prevención de intrusiones (IDPS) y plataformas de protección de terminales (EPP). Por el contrario, la función de las tecnologías SOAR es permitir que las organizaciones recopilen entradas monitoreadas por el equipo de operaciones de seguridad, como alertas, y automatizar parcialmente los procesos de análisis y clasificación de incidentes. Estas capacidades están diseñadas para ayudar a definir, priorizar e impulsar actividades estandarizadas de respuesta a incidentes de acuerdo con un flujo de trabajo predefinido.

SOAR es, por tanto, una combinación de:

- Procesamiento automatizado de la información de seguridad. El procesamiento automatizado de datos de seguridad puede incluir información de seguridad y alertas de gestión de eventos (SIEM) o inteligencia de amenazas.
- La orquestación de elementos de un flujo de trabajo que implica la recopilación de datos, aprobaciones y otros marcadores basados en auditorías.

En las plataformas SOAR convergen tres tecnologías SIRP, SOA y TIP.

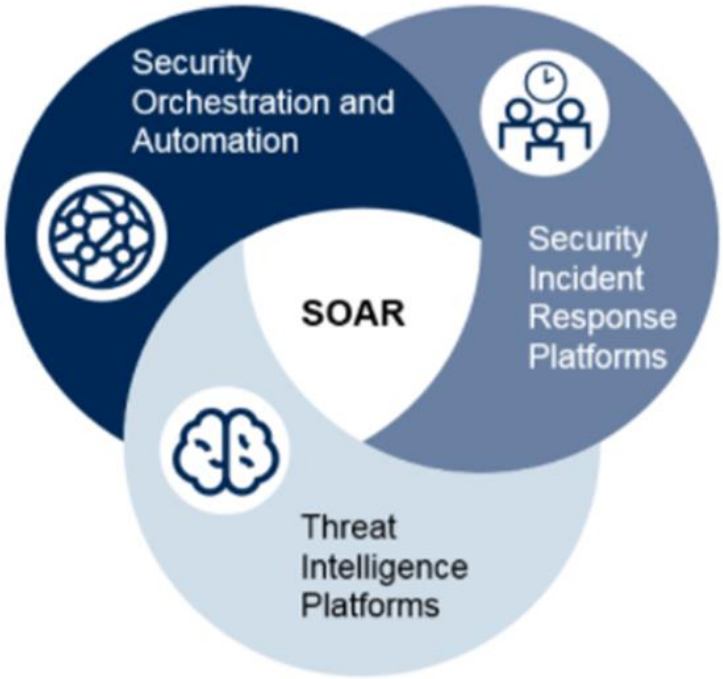


Ilustración 13. SOA+SIRP+TIP = SOAR[14]

[14]*https://www.platinbilisim.com.tr/EN/Media/Promotions/how-ready-is-your-organization-for-the-soar-platform*

La mayoría de los productos SOAR tienen un enfoque central único y algunos beneficios adicionales. Este enfoque central generalmente se divide en una de tres categorías principales:

Flujo de trabajo: muchos productos en el mercado tienen como objetivo facilitar el proceso de gestión de un incidente de seguridad, ayudar con la autorización de cambios o categorizar y asignar correctamente los tickets a las áreas correctas. También garantizan que el problema se resuelva dentro de escalas de tiempo predefinidas y con un nivel de detalle constante.

Enriquecimiento: ya sea después de la identificación del incidente o durante la recopilación y el procesamiento de datos, las soluciones SOAR pueden ayudar a integrar la inteligencia de amenazas externas, realizar búsquedas contextuales internas o ejecutar procesos para recopilar más datos sobre problemas.

Respuesta: la respuesta automatizada proporciona una resolución "sin analistas" a problemas comunes mediante la aplicación de algún tipo de aplicación a una tecnología de seguridad dentro del estado de TI de una organización. Algunos pueden bloquear a un usuario y otros aplicar cambios a las puertas de enlace de correo. Esta funcionalidad es la más impactante, pero también la más compleja y rara vez se implementa solo para uno o dos casos de uso triviales.

3.3 Componentes y funcionamiento de una Plataforma SOAR

Las soluciones de ciberseguridad de SOAR extraen datos de amenazas o alarmas de cada plataforma interconectada o integrada y los organizan en un solo lugar.

La tecnología viene con administración de casos, que ayuda a los usuarios o analistas a investigar, evaluar y realizar investigaciones adicionales de un solo caso.

Las soluciones de ciberseguridad SOAR establecen la integración como un medio para respaldar una respuesta a incidentes altamente automatizada y sofisticada para ofrecer resultados más rápidos al promover una defensa adaptativa.

Las soluciones SOAR son la fusión de tres tecnologías históricamente distintas que tienen atributos comunes y ofrecen una amplia utilidad a los equipos de operaciones de seguridad:

- Plataformas de respuesta a incidentes de seguridad (SIRP)
- Orquestación y automatización de la seguridad (SOA)
- Plataformas de inteligencia de amenazas (TIP)

Ilustración 14. SOAR Convergencia de tres tecnologías[15]

3.3.1 Orquestación y automatización de la seguridad (SOA)

3.3.1.1 Automatización

Cualquier ejecución de un proceso impulsado por una máquina puede denominarse automatización. También es la ejecución impulsada por una máquina de las herramientas de seguridad y los sistemas de TI como parte de la "respuesta a incidentes".

Anteriormente, estas tareas las realizaban humanos, pero ahora, con la función de automatización de las herramientas SOAR, el equipo de seguridad de TI puede formalizar el flujo de trabajo de toma de decisiones, describir pasos de automatización estandarizados, acciones de cumplimiento y capacidades de auditoría.

Para la automatización productiva, las tareas de respuesta realizadas por los sistemas automatizados deben definirse secuencialmente. La automatización ofrece medidas de seguridad tanto proactivas como reactivas.

De forma proactiva, el manual de estrategias de automatización puede realizar operaciones de seguridad y búsqueda de amenazas. Ayuda a los analistas a identificar vulnerabilidades o amenazas antes de que ocurra un incidente real. Por otro lado, de manera reactiva, el libro de estrategias de automatización puede monitorear y rastrear las métricas de respuesta a incidentes, realizar la gestión de casos y llevar a cabo la 'respuesta a incidentes'.

3.3.1.2 Orquestación

La orquestación de seguridad es el proceso de integrar diferentes tecnologías y conectar varias herramientas de seguridad (tanto no específicas de seguridad como específicas de seguridad) que incluye herramientas SIEM modernas para que funcionen juntas y mejoren la respuesta a incidentes. La integración inteligente de herramientas SIEM con la plataforma SOAR fortalece la arquitectura de seguridad de la organización.

---

[15] *https://www.gartner.com/doc/reprints?id=1-24GXYQKN&ct=201027&st=sb%20*

En el escenario actual, los ciberataques son sofisticados y más frecuentes que antes. Además, la capacidad de la organización para responder a estos ataques es inadecuada e ineficiente.

Por ejemplo, el sistema de alerta utilizado por sus herramientas de seguridad SOAR no es completamente capaz de determinar si un correo electrónico es malicioso o no. En cambio, los usuarios o el analista tienen que actuar como Sherlock Holmes para buscar pistas y hacerse preguntas como:

¿Algún otro sistema recibió un correo electrónico de este tipo?

¿Cuál es el origen del correo electrónico o la dirección IP?

3.3.2 Plataformas de respuesta a incidentes de seguridad (SIRP)

Una plataforma de respuesta a incidentes es un sistema de software que guía, ayuda y automatiza la respuesta a incidentes. Los servicios de respuesta a incidentes brindan tres capacidades clave:

- **Respaldar los flujos de trabajo de los analistas**: ayudar a los analistas de seguridad a colaborar en torno a un incidente de seguridad, proporcionando administración de casos. La gestión de casos permite a los analistas abrir un caso para un incidente de seguridad, recopilar datos de su investigación y guardarlos como parte del caso, priorizar casos y compartir datos con otros analistas.
- **Inteligencia y análisis**: ayuda a los equipos de seguridad a recopilar datos de eventos de seguridad mediante la integración con la gestión de eventos e información de seguridad (SIEM) y otras herramientas, clasificarlos, agregar contexto para crear cronogramas de eventos y combinarlos con inteligencia de amenazas para identificar incidentes de seguridad con un esfuerzo mínimo.
- **Automatización de la seguridad**: automatizar las respuestas utilizando playbooks. Estos son flujos de trabajo automatizados que la plataforma puede ejecutar cuando se detecta un incidente de seguridad específico. Los playbooks de respuesta a incidentes pueden ser muy efectivos para reducir el tiempo de respuesta y pueden ayudar a ahorrar tiempo a los equipos de seguridad.

Al manejar un incidente de seguridad, habrá mucha información que debe procesarse y analizarse. Una plataforma ideal de respuesta a incidentes de seguridad debería poder hacer lo siguiente:

- Recibir alertas y eventos de seguridad de diferentes fuentes (SIEM, IDS, correo electrónico, EDR)
- La gestión de casos de incidentes de seguridad debe permitir que un analista de seguridad agregue registros, IOC o hallazgos relacionados durante el ciclo de vida de la gestión de casos de incidentes.
- Ser capaz de comparar su análisis con información de amenazas externas, como VirusTotal, para identificar los comportamientos maliciosos de un archivo, hash, dominio o dirección IP.

3.3.3 Plataformas de inteligencia de amenazas (TIP)

El panorama actual de la ciberseguridad está marcado por algunos problemas comunes: volúmenes masivos de datos, falta de analistas y ataques adversarios cada vez más complejos. Las infraestructuras de seguridad actuales ofrecen muchas herramientas para gestionar esta información, pero poca integración entre ellas. Esto se traduce en una cantidad frustrante de esfuerzo de ingeniería para administrar sistemas y una pérdida inevitable de recursos y tiempo ya limitados.

Para combatir estos problemas, muchas empresas están optando por implementar una plataforma de inteligencia de amenazas (TIP). Las plataformas de inteligencia de amenazas se pueden implementar como una solución SaaS o local para facilitar la gestión de la inteligencia de amenazas cibernéticas y las entidades asociadas, como actores, campañas, incidentes, firmas, boletines y TTP. Se define por su capacidad para realizar cuatro funciones clave:

- Agregación de inteligencia de múltiples fuentes
- Curación, normalización, enriquecimiento y puntuación de riesgo de datos
- Integraciones con sistemas de seguridad existentes
- Análisis e intercambio de inteligencia sobre amenazas

Una ventaja de los TIP es la capacidad de compartir inteligencia sobre amenazas con otras partes interesadas y comunidades. Los adversarios suelen coordinar sus esfuerzos en foros y plataformas. Un TIP proporciona un hábitat común que hace posible que los equipos de seguridad compartan información sobre amenazas entre sus propios círculos de confianza, interactúen con expertos en seguridad e inteligencia y reciban orientación sobre la implementación de contramedidas coordinadas. Los TIP con todas las funciones permiten a los analistas de seguridad coordinar simultáneamente estas actividades tácticas y estratégicas con la respuesta a incidentes, las operaciones de seguridad y los equipos de gestión de riesgos, mientras se agregan datos de comunidades de confianza

3.3.4 El mercado de los SOAR

Para realizar el estudio nos hemos basado en un informe de Gartner revisado el 22 de septiembre de 2020 desde el cuál podemos concluir que las soluciones SOAR están ganando terreno de manera constante en el uso en el mundo real para mejorar las operaciones de seguridad. Los líderes de seguridad y gestión de riesgos deben evaluar cómo estas soluciones pueden respaldar y optimizar sus capacidades de operaciones de seguridad más amplias.

3.3.4.1 Aspectos Clave

- Los principales clientes de SOAR son equipos de seguridad con procesos bien establecidos y probados principalmente para mejorar la productividad general, la eficiencia y la coherencia en sus centros de operaciones de seguridad (SOC).
- La orquestación y la automatización, la gestión básica de incidentes / casos y la puesta en funcionamiento de la inteligencia de amenazas son "elementos clave" de las herramientas SOAR.
- SOAR también se está volviendo omnipresente en la seguridad y servicios gestionados de detección y respuesta al ayudar a los proveedores a mejorar las interacciones con los clientes, la velocidad y la coherencia al detectar y responder a las amenazas.

- Los casos de uso para respaldar las operaciones de seguridad más allá del monitoreo y la detección de amenazas, la inteligencia de amenazas y la respuesta a incidentes y la búsqueda de amenazas, aún son incipientes.
- Los proveedores de gestión de eventos e información de seguridad continúan agregando capacidades SOAR a través de adquisiciones, acuerdos o desarrollo interno; sin embargo, las soluciones todavía se venden principalmente como complementos premium y no se fusionan con herramientas SIEM.

3.3.4.2 Precauciones a la hora de adquirir una solución SOAR

- Examinar en detalle los requisitos para el uso de una herramienta SOAR, que impulsará los casos de uso iniciales y posteriores.
- No participar en proyectos SOAR centrados en la automatización sin asegurarse de que los procesos estén definidos; de lo contrario, deberán desarrollarse antes de su implementación.
- Gestionar bien recursos adecuados para la implementación inicial, así como el funcionamiento continuo de una herramienta SOAR; Habrá un esfuerzo inicial y una gestión continua para realizar y mantener el valor de SOAR. Planifique la implementación y el funcionamiento y administración continuos de las herramientas SOAR mediante el uso de una combinación de servicios profesionales, recursos internos y proveedores de servicios.
- Establecer un plan de contingencia en caso de que se adquiera un proveedor SOAR. Las adquisiciones ocurren con frecuencia a medida que evoluciona el mercado, y observamos diferentes caminos después de las adquisiciones para los cuales los compradores deben estar preparados.
- Exigir que los proveedores proporcionen API abiertas en sus productos al actualizar o adquirir nuevas soluciones; de lo contrario, requerirá un conjunto de habilidades de desarrollo en el equipo SOC. Las API limitadas en curso en una gama de productos de seguridad todavía se consideran un impedimento para lograr todas las capacidades que pueden ofrecer las herramientas SOAR.

3.3.4.3 ¿Qué están haciendo los proveedores de SIEM?

Los proveedores de gestión de eventos e información de seguridad (SIEM) están adoptando y adquiriendo/integrando soluciones SOAR en sus ecosistemas, generalmente como aplicaciones premium que operan en conjunto con las soluciones SIEM. Las tecnologías que incorporan con SOAR son:

- Seguridad del correo electrónico
- Detección y respuesta de endpoints (EDR)
- Detección y respuesta de red (NDR)
- Detección y respuesta extendidas (XDR)[16]

[16] *https://secrutiny.com/2021/04/edr-ndr-xdr-wtfdr-confused/*

3.3.4.4 Principales proveedores de SOAR

Gartner aún no realiza un cuadrante mágico específico para plataformas SOAR ya que considera por el momento que tanto SIEM como SOAR son tecnologías contemporáneas en seguridad cibernética, trabajan muy de cerca, y el crecimiento de SIEM como tecnología está estrechamente relacionado con el crecimiento de SOAR en el futuro. La consultora Forrester ha empezado a utilizar el término SOAR recientemente debido al predominio en el mercado ya que, hasta ahora, prefería el término SAO (Automatización y Orquestación de Seguridad)[17].

A continuación, enumeramos a los vendedores más representativos en el mercado actual por orden alfabético[18] .

Vendedores más representativos			
Vendedor	**Producto, Servicio o Solución**	**Vendedor**	**Producto, Servicio o Solución**
Anomali	ThreatStream	McAffe	McAffe ePolicy Orchestrator
Ciberbit	SOC 3D	Micro Focus (ATAR Labs)	ArcSight SOAR
Cyware	Virtual Cyber Fusion Center	Palo Alto Networks	Cortex XSOAR
D3 Security	D3 SOAR	Rapid7	InsightConnect
DFLabs	IncMan SOAR	ServiceNow	Security Operations
EclecticIQ	EclecticIQ Platform	Securinox	Securinox SOAR
Exabeam	Exabeam Incident Responder	Siemplify	Siemplify SOAR Platform
FireEye	Helix	Splunk	Splunk Phantom
Fortinet (CyberSponse)	FortiSOAR	Swimlane	Swimlane SOAR Platform
Honeycomb	SOCAutomation	ThreatConnect	ThreatConnect SOAR Platform
IBM Security	Resilient	ThreatQuotient	ThreatQ
LogicHub	SOAR+	Tines	Tines
Logsign	Logsign SOAR		

Muchos de los fabricantes son proveedores de SIEM como IBM, Splunk, Rapid7, Exabeam, o Securinox, etc., otros fabricantes, son reconocidos por sus herramientas de detección de amenazas como Anomali, Palo Alto, Fortinet, McAffe, etc. Y también hay proveedores provienen de productos de automatización como ServiceNow, Honeycomb o Tines, en definitiva, como Plataformas SOAR confluyen diferentes proveedores de los distintos componentes de un SOAR.

---

[17] *https://go.forrester.com/blogs/schrodingers-soar-feature-or-abstraction/*

[18] *https://www.itcentralstation.com/landing/report-security-orchestration-automation-and-response-soar y https://www.gartner.com/doc/reprints?id=1-24GXYQKN&ct=201027&st=sb%20*

Ilustración 15. Confluencia de diferentes tecnologías[19]

Revisando diferentes rankings de publicaciones de tecnología[20], podríamos destacar que los proveedores de SOAR más valorados son:

- Palo Alto con el producto Cortex XSOAR fruto de la adquisición de Demisto en febrero de 2019.
- IBM con el producto IBM Resilient fruto de la adquisición de Co3 Systems en 2016.
- Splunk con el producto Splunk Phantom fruto de la adquisición de Phantom Cyber en 2018.
- Rapid 7 con el producto InsightConnect fruto de la adquisición de SOAR Komand en julio de 2017.

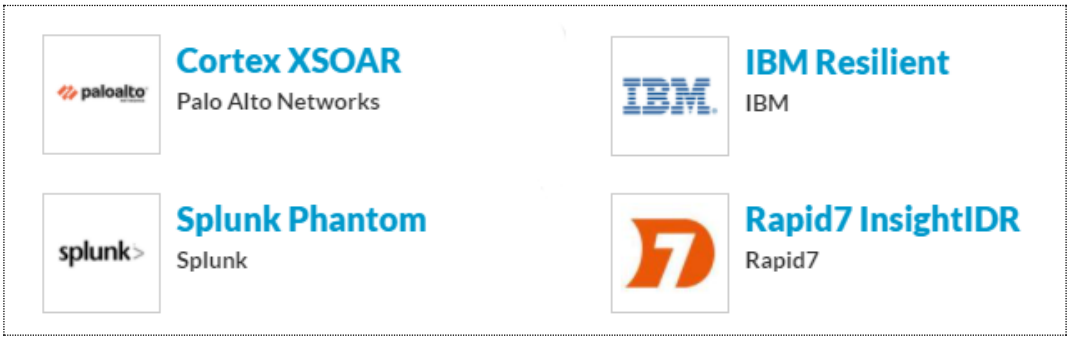


Ilustración 16. SOAR más valorados[21]

[19] *https://www.logichub.com/blog/what-soar-and-what-know-you-buy*
[20] *https://solutionsreview.com/security-information-event-management/the-8-best-soar-security-companies/, https://geekflare.com/best-soar-tools/, https://em360tech.com/top-10/top-10-soar-companies-watch-2021 y https://www.itcentralstation.com/categories/security-orchestration-automation-and-response-soar*
[21] *https://sourcefoge.net/software/compare/Cortex-XSOAR-vs-IBM-Resilient-vs-Splunk-Phantom-vs-InsightIDR/*

3.3.4.5 Aspectos a destacar

- Todos se ofrecen en como solución SaaS, tendencia clara en el mercado actual.
- Con las adquisiciones de empresas en los últimos años podemos concluir que la tecnología SOAR está en plena expansión y crecimiento.
- No es requisito que el proveedor de la solución SOAR haya desarrollado también un producto SIEM. De la selección que hemos hecho, los tres últimos son proveedores de SIEM con reconocimiento en el mercado que han incorporado capacidades SOAR. En cambio, destaca la irrupción de Cortex XSOAR de Palo Alto, empresa líder en firewalls de red[22] que, con la adquisición de la empresa israelí Demisto, aparece entre las soluciones SOAR más destacadas, Demisto fue fundada en 2015 y fue concebida como solución de seguridad empresarial que combinan la gestión de incidentes, el aprendizaje automático y la investigación interactiva, así que para llegar a ser una solución SOAR no es requisito imprescindible haber sido previamente una solución SIEM.
- En una Plataforma SOAR confluyen diferentes tecnologías y los proveedores de dichas plataformas provienen de herramientas especializadas: Detección de Amenazas, Automatización y SIEM.
- Tener un SIEM líder en el mercado no te asegura tener un buen producto SOAR, Exabeam y Securinox no aparecen entre los más destacados.

3.4 Trabajando de manera inteligente con SOAR

La tecnología SOAR se emplea principalmente para dar apoyo a los equipos de analista de seguridad. Bien sea en un SOC, un centro de respuesta a incidentes (CSIRT/FIRST) o simplemente un departamento de seguridad.

Actualmente los principales compradores de SOAR son:

- Grandes empresas con un SOC (Security Operation Center) que han desplegado un SIEM y están buscando en SOAR la automatización final. Son compañías maduras en cuanto a su postura frente a la seguridad.
- Empresas de tamaño medio (por encima de los 2.000 empleados), no tan maduras como las grandes empresas, pero motivadas y ágiles.
- Proveedores de servicios gestionados de seguridad (MSSP). Además, algunas empresas que usan un MSSP adoptan SOAR para administrar la última solución e investigar las alertas que reciben de su MSSP.

[22] *https://www.fortinet.com/solutions/gartner-network-firewalls*

3.4.1 Casos de uso

Uno de los factores clave para el uso de SOAR incluye un aumento en el volumen de amenazas, lo que requiere que las organizaciones reduzcan el tiempo para responder, contener y remediar esas amenazas automatizando los procesos y utilizando mejor las capacidades de personal disponible.

Las organizaciones usan SOAR por una variedad de razones y casos de uso, dependiendo de las prioridades y herramientas de seguridad existentes que integran con SOAR. Vamos a ver los usos que se les está dando en la actualidad:

- **Ataques de Phising**
  Una plataforma SOAR permite a los equipos de seguridad automatizar la detección y mitigación del phishing ya que ahorra un tiempo valioso a los equipos de seguridad.
  Puede determinar el nivel de riesgo de cada correo electrónico mediante la realización de un análisis exhaustivo que cubra la línea de asunto, el correo electrónico del remitente, destinatario (s), contenido del mensaje, enlaces, archivos adjuntos, etc. Un playbook dirigirá las acciones necesarias, como puede ser, poner en cuarentena a un correo electrónico sospechoso, bloquear remitentes y verificar si algún usuario hizo clic en correos electrónicos sospechosos antes de ser puestos en cuarentena.

- **Triaje de Incidentes**
  Muchas herramientas de seguridad en el mercado generan alertas desde que detectan comportamientos maliciosos o anormales. Sin embargo, las alertas sin información contextual son en su mayoría inútiles.
  Para una gestión eficaz de incidentes, el simple conocimiento de alertas e incidentes no es suficiente. Los equipos de seguridad necesitan información procesable para clasificar y resolver las alertas. Sin información contextual, los equipos de seguridad gastarán la mayor parte de su tiempo para encontrar dicha información para cada alerta. Esto aumentará su carga de trabajo, además de sus responsabilidades.
  La provisión de información contextual ayudará a la seguridad ya que los analistas tomarán decisiones informadas, la información enriquece la calidad de las alertas. Si el equipo de seguridad identifica una actividad anormal, contextualizar la información les ayudará a comprender rápidamente antecedentes de este comportamiento, tomar una decisión y responde sin perder tiempo.

- **Caza de amenazas (Threat Hunting)**
  A los atacantes les basta con tener éxito una sola vez, y es cuestión de minutos para que comprometan un sistema. Los equipos de Seguridad deben trabajar las 24 horas del día para defender la infraestructura de TI contra amenazas emergentes. A menudo, lleva semanas y meses que un equipo de seguridad detecte que sus sistemas han sido comprometidos. Para minimizar el tiempo necesario para detectar y responder, los equipos de seguridad necesitan de una solución que automatice las actividades de búsqueda de amenazas.
  La plataforma ideal, crearía un caso y generaría una alarma tan pronto como detecte una amenaza. Puede agregar información adicional sobre la amenaza y comenzar a tomar acciones, si están disponibles.

- **Detección de amenazas internas**
  La amenaza interna es uno de los tipos de filtraciones de datos más costosos.
  Teniendo en cuenta que se trata de usuarios confiables, son relativamente difíciles de detectar. Sin embargo, al implementar una solución de prevención de pérdida de datos (DLP) y conectarlo con un SOAR, es posible detectar filtración de datos no autorizadas e inesperadas. Muchas plataformas SOAR vienen con manuales incorporados para la detección de amenazas internas. Tan pronto como la plataforma SOAR detecte un comportamiento sospechoso de amenaza interna, comienza a recopilar información sobre el usuario, su comunicación y dirección origen. Estas direcciones de origen se clasifican como fuentes de amenaza de manera inteligente para determinar la probabilidad de que sean maliciosas. También se pueden agregar otras fuentes de información a Plataformas SOAR para proporcionar información contextual adicional sobre alertas.

- **Protección Endpoint**
  Los Endpoints son puntos de entrada que utilizan los usuarios finales para interactuar con una red corporativa. Los endpoints incluyen dispositivos como: dispositivos móviles, portátiles, ordenadores de sobremesa, impresoras, dispositivos IoT, etc.
  Los ataques avanzados como malware sin archivos, polimórficos y los ataques de día cero son cada vez más populares.
  Una solución SOAR acepta datos de registro de varios dispositivos de seguridad, como la detección y respuesta de puntos finales (EDR). Si bien, los equipos de seguridad tienen una funcionalidad limitada con EDR, una plataforma SOAR permite a un equipo de seguridad comprender el contexto, investigar una alerta, comprobar los endpoints, y orquestar cambios en todos ellos de una sola vez.
  Si bien el número de endpoints es proporcional a la cantidad de alertas que genera una organización, SOAR utiliza información contextual para automatizar la resolución de alertas con la ayuda de playbooks y flujos de trabajo.

- **Investigación Rápida**
  Cuando una plataforma SOAR detecta una alerta o evento de alto riesgo, el tiempo es fundamental. Los equipos de seguridad no pueden perder tiempo recopilando información manual de diferentes fuentes.
  Una solución SOAR proporciona una plataforma para ayudar a los equipos a completar su investigación en el menor tiempo posible. En algunos casos, una parte de las acciones de respuesta a incidentes se automatiza, mientras que el resto debe hacerse manualmente. En otros casos, la situación se invierte.
  La disponibilidad de información contextual ayuda a los equipos de seguridad a tomar decisiones informadas y preparar los informes de alerta sin demora. Con la ayuda de la información disponible, los equipos de seguridad pueden realizar una investigación y proceder en consecuencia.

- **Gestión de Vulnerabilidades**
  Las vulnerabilidades sin parchear o sin mitigar permiten a los atacantes obtener acceso no autorizado a los sistemas en la red de la organización. En los últimos años, los atacantes han comenzado a adoptar ataques sigilosos para evitar ser detectados por las herramientas de seguridad.
  Una solución SOAR proporciona a un equipo de seguridad información en tiempo real

del estado de seguridad de la organización. Es capaz de analizar rápidamente grandes cantidades de datos, proporciona información detallada sobre vulnerabilidades y lo combina con información derivada de inteligencia de amenazas.
Esto coloca a los equipos de seguridad en una mejor posición para tomar decisiones y abordar las vulnerabilidades existentes con toda la información que necesitan. Esta respuesta a las vulnerabilidades puede ser automatizada, semiautomática o manual. Como práctica general, las plataformas SOAR envían una alerta a los equipos de seguridad si encuentran una vulnerabilidad que es potencialmente nociva y considerada de naturaleza grave.

- **Trafico de red Malicioso**
  Las redes corporativas a menudo encuentran tráfico malicioso en varias formas, el propósito detrás de dicho tráfico suele ser invasivo. Un atacante puede intentar cerrar el sitio web, robar información confidencial del usuario y venderla en la deep web.
  Las plataformas SOAR han demostrado ser particularmente útiles en la identificación y análisis de tráfico de red malicioso. Con datos la recogida de datos para escanear el tráfico de la red una Plataforma SOAR está en una mejor posición para identificar comportamientos sospechosos.
  Con la ayuda de playbooks y otros recursos disponibles, una solución SOAR puede bloquear el tráfico de red malicioso antes de que impacte en las operaciones de la red.

- **Inteligencia de Amenazas**
  Las soluciones SOAR progresan cuanto mayor sea la cantidad de datos tengan disponibles, ya que mejoran la precisión y la toma de decisiones. Para el manejo efectivo de incidentes, la inteligencia de amenazas es un componente crucial. Una plataforma SOAR debe proporcionar información valiosa al analizar las fuentes de inteligencia de amenazas. Un equipo de seguridad necesita conocer tácticas, técnicas y procedimientos (TTP) para responder a un incidente. Cuando una plataforma SOAR recopila esta información de fuentes de inteligencia de amenazas, también proporciona información contextual, ya que se encuentra en una posición única para agregar información procesable.
  Las plataformas SOAR ideales serían capaces de correlacionar las fuentes de inteligencia de amenazas con los registros entrantes de una organización para descubrir patrones de ataque, vulnerabilidades y cualquier comportamiento anormal. Si bien la plataforma SOAR se encarga de la correlación automatizada, los equipos de seguridad también pueden realizar una correlación visual para buscar patrones o comportamientos que los métodos automatizados podrían haber pasado por alto. Para que esto suceda, una plataforma SOAR debe presentar esta información de una manera fácil de ver.

De entre los principales casos de uso de las Plataformas SOAR en la actualidad, los tres más populares son:

1. Triaje de incidentes (65%),
2. Respuesta a ataques de phishing (62%)
3. Detección de inteligencia de amenazas (62%)

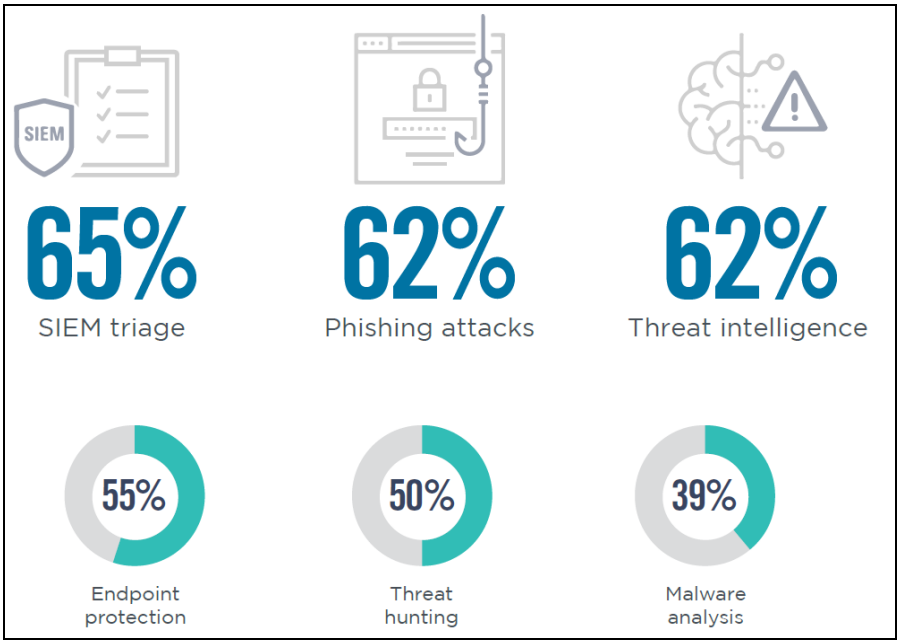


Ilustración 17. Casos de uso de SOAR[23]

3.5 Beneficios y retos de las Plataformas SOAR

Los beneficios de los sistemas Security Orchestration, Automation and Response (SOAR) son obvios para casi todos los analistas CISO y de seguridad.

Los beneficios para los Centros de Operaciones de Seguridad (SOCs) incluyen:

- Automatización de tareas para ayudar a los SOCs con personal limitado aumentando la productividad de manera exponencial.
- Automatizar la clasificación básica de seguridad, para que las alertas se manejen de manera integral y las alertas importantes nunca se pasen por alto debido a la carga de trabajo del personal.
- Liberar a los analistas de seguridad para trabajar en tareas no repetitivas, como la búsqueda proactiva de amenazas y la colaboración con unidades de negocios, una vez que las operaciones de rutina son automatizadas, lo que mejora la efectividad general del SOC.
- Lograr la excelencia operacional al reemplazar los procesos ad hoc con las mejores prácticas documentadas, automatizadas y realizadas de manera consistente.

[23] *https://swimlane.com/resources/2020-soar-report-swimlane-cybersecurity-insiders*

Pero mientras los SOC reconocen los beneficios de los sistemas SOAR, también podemos enumerar una larga lista de retos que pueden limitar la efectividad de una implementación SOAR, o hacer que una implementación de herramientas SOAR parezca poco práctica. Y es que los que vivimos en el mundo de la tecnología, conocemos los problemas y dolores de cabeza que produce introducir una nueva tecnología.

Aquí hay una rápida lista de obstáculos en el despliegue de herramientas SOAR:

- **Precio Elevado**. Muchos sistemas SOAR son demasiado caros. Las nuevas tecnologías potentes a menudo tienen precios exorbitantes cuándo se presentan. Los automóviles solían ser accesibles solo por los aficionados más ricos. Con el tiempo, se convirtieron en necesidades asequibles para todos los hogares. Muchos sistemas SOAR de hoy solo son asequibles para SOC con grandes presupuestos.
- **Programación**. Los sistemas SOAR requieren programación, pero la mayoría de los equipos SOC carecen de desarrolladores: Muchos sistemas SOAR requieren que los usuarios escriban en Python para construir playbooks e integrarlos con otras herramientas y aplicaciones de seguridad. La gran mayoría de los equipos de SOC carecen de las habilidades de programación en Python y el tiempo para asumir un nuevo trabajo de integración, por lo que el requisito de la programación se convierte en un factor decisivo.
- **Dificultades de integración**. Las llamadas capacidades de integración son demasiado limitadas: Los SOAR deben integrarse con herramientas de seguridad para las que puedan recopilar alertas y otros datos de ellos y emitir comandos, orquestando las respuestas a las amenazas. Algunos proveedores SOAR ofrecen integraciones, pero los SOC pronto descubren que las integraciones no incluyen funciones para las tareas y características de las que dependen. Con demasiada frecuencia, los SOC se ven obligados a desarrollar integraciones o contratar a expertos externos para crear integraciones no proporcionadas por los proveedores.
- **Limitación con las API**. Las API de las herramientas de seguridad son demasiado limitadas: Para complicar aún más el desafío de integrar SOARs con herramientas de seguridad, está la limitación de muchas API de herramientas de seguridad. Estas herramientas pueden ofrecer APIs para unas pocas operaciones básicas, suficientes para aprobar una demostración, pero no lo suficiente como para admitir la automatización efectiva de sus operaciones. Hay datos en los que ciertos SOCs solo han integrado un 30%[24] de las funciones de sus herramientas de seguridad debido a la disposición de las APIs. Sin APIs para aprovechar, la automatización de la seguridad se termina confiando en comandos. Hasta ahora, la mayoría de los sistemas SOAR siguen siendo débiles en esta área de automatización, y por ello, debemos conocer muy bien nuestro alcance de integración.
- **Personalización**. Los SOCs creen que sus procesos son demasiado ad hoc o especializados para ser automatizados: Escuchamos esta objeción de muchos analistas

[24] *https://ciberseguridad.blog/por-que-las-herramientas-soar-revitalizaran-el-ecosistema-siem/*

de seguridad. Están convencidos de que lo que hacen es demasiado único o complicado de documentar. Y es que, si no se puede documentar, no se puede automatizar.

- **Falta de tiempo**. Los SOCs carecen del tiempo necesario para construir y ajustar las automatizaciones por sí solas: La construcción de la automatización lleva tiempo. Se necesita atención sostenida y un poco de ensayo y error. Desafortunadamente, la mayoría de los SOCs están tan ocupados luchando contra su clasificación de amenazas que no pueden disponer de las horas o los días para crear lo que les supondría ahorrarse semanas o meses a lo largo del año.

3.6 Enfoque evolutivo de la tecnología SOAR y la inteligencia artificial

A medida que los piratas informáticos se vuelven más inteligentes, no es suficiente que una corporación proteja los sistemas de red para reconocer una amenaza antes, durante o incluso después de que sus dispositivos de red se vean comprometidos. La explotación de dispositivos inteligentes y dispositivos IoT, así como las innovaciones de los ciberdelincuentes, están dando lugar a ataques multivectoriales más frecuentes y complejos. Este dramático aumento en los ataques y su tamaño también se debe a que los atacantes acumulan redes de bots gigantes y complejas que incluyen dispositivos de IoT inseguros. Los ataques multivectoriales combinados con inundaciones de gran volumen, incluidos los ataques a la capa de aplicación y los ataques de agotamiento del estado de TCP, aumentan las posibilidades de éxito de los atacantes.

SOAR ayuda a los equipos de operaciones de seguridad a proteger eficazmente el perímetro de la red de las empresas optimizando su capacidad para detectar y responder a las amenazas (tanto de entrada como de salida) más rápido, cuantificar los indicadores clave de rendimiento y reducir la carga de trabajo diaria a través de inteligencia e informes mejorados, flujos de trabajo optimizados y playbooks de estrategias de respuesta automatizada.

Es muy preocupante el hecho de que los hackers cibernéticos hayan comenzado a utilizar la automatización y la inteligencia artificial, para llevar a cabo ataques a velocidades efectivas para eludir los comandos y controles de seguridad. Por lo tanto, las capacidades de respuesta proactiva son esenciales para la seguridad de las redes actuales y deben ser más que anticipatorias. La inteligencia automatizada y SOAR, no solo son el avance de la próxima generación en ciberseguridad, sino que son el enfoque evolutivo para proteger las redes en el futuro.

SOAR no solo debe prevenir todas las formas conocidas de ciberataque, sino que también puede "aprender" a anticipar cualquier ataque futuro de una nueva amenaza de ataque mutada "invisible". Las funciones de automatización y orquestación de SOAR han alcanzado un nivel de sofisticación que permite integrarlo en un sistema de seguridad existente sin depender de la asistencia humana.

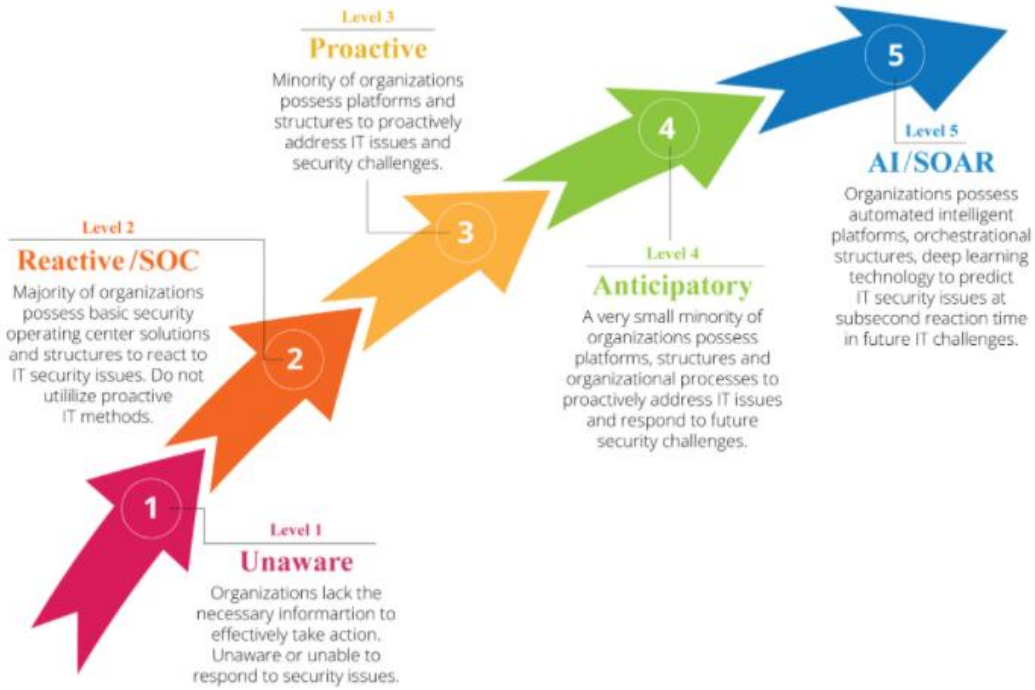


Ilustración 18. La evolución de la Ciberseguridad[25]

4. Implementación de Plataformas SOAR

4.1 Proyecto The Hive

En el año 2014 un grupo de profesionales experimentados en Análisis Forense Digital y Respuesta a Incidentes, desencantados en su búsqueda de una plataforma sólida y escalable que les ayudara a investigar y colaborar en incidentes de seguridad de la información, deciden comenzar con el desarrollo de una aplicación a principios de 2014. Varios meses más tarde una primera versión utilizable se puso en producción en octubre de ese mismo año, así nació TheHive y desde entonces ha sido utilizado a diario por múltiples analistas.

TheHive es un software de código abierto y gratuito publicado bajo la AGPL[26] (Licencia pública general de Affero). TheHive Project, tiene el firme compromiso de garantizar que siga siendo un proyecto gratuito y de código abierto a largo plazo.

Los principales objetivos de TheHive Project son:

- Tener un repositorio/dashboard centralizado, para manejo de alertas y casos.
- Un medio de Automatizar Análisis y respuestas.
- Un medio donde organizar tareas y playbooks.

[25] *https://scardot.medium.com/the-evolution-of-cyber-security-be9fedc8f4c5*
[26] *https://es.wikipedia.org/wiki/GNU_Affero_General_Public_License*

El proyecto TheHive integra tres herramientas:

- TheHive
- MISP
- Cortex

Ilustración 19. TheHive+MISP+Cortex

El proyecto **The Hive** tiene como fin facilitar a los analistas al tratamiento de las alertas de seguridad, siendo una herramienta creada exclusivamente para el sector de la ciberseguridad y apoyada principalmente por la comunidad, ya que se trata de un proyecto totalmente Open Source, lo que le ha permitido crecer enormemente gracias a las distintas colaboraciones y, a su vez, recibir apoyos de empresas de sectores tanto privados como públicos.

Conectado a The Hive se encuentra la pieza fundamental que necesita todo analista de ciberseguridad, **Cortex**. Se trata de una herramienta que posee más de 120 analizadores de IOC (Indicadores de Compromiso) distintos, con los cuales la probabilidad de que se escape un detalle es casi nula.

Como punto de encuentro entre Cortex y The Hive se encuentra el proyecto **MISP**, herramienta desarrollada íntegramente por CIRCL[27] (Computer Incident Response Center Luxembourg), que tiene como principal acometido la compartición, almacenaje y correlación de IOC de ataques dirigidos, siendo la comunidad de usuarios la que aporta inteligencia en las investigaciones, mediante las cuales se pueden generar contramedidas, con el fin de evitar futuros ataques mediante movimientos similares a los que ha sufrido el usuario que lo ha aportado en el sistema.

4.1.1 The Hive

TheHive es una plataforma de respuesta a incidentes de seguridad (SIRP) de código abierto, escalable y diseñada para facilitar la vida de los SOC, CSIRT, CERT y de cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que deben investigarse rápidamente. Puede recibir alertas de diferentes fuentes (SIEM, IDS, correo electrónico, etc.) a través de su API REST llamada TheHive4py.

Ilustración 20. Logo de TheHive

[27] *https://www.circl.lu/*

4.1.2 MISP

Principalmente, MISP (Malware Information Sharing Platform)[28] es una plataforma de inteligencia de amenazas creada para compartir, almacenar y correlacionar Indicadores de Compromiso (IoCs) de ataques dirigidos, permitiendo así a las distintas organizaciones compartir información sobre Malware y sus indicadores.

Ha sido desarrollada por CIRCL (Computer Incident Response Center Luxembourg), el equipo de Defensa de Bélgica, y la OTAN (NCIRC).

Ilustración 21. Logo de MISP

4.1.3 Cortex

Cortex es un motor de análisis independiente y compañero perfecto para TheHive y MISP. El poder de Cortex realmente entra en juego cuando usamos su API REST. TheHive habla nativamente con Cortex (como lo hace MISP).

Cortex resuelve dos problemas comunes que se encuentran con frecuencia los SOC, los CSIRT y los investigadores de seguridad en el respecto a la inteligencia de amenazas, análisis forense digital y respuesta a incidentes:

- ¿Cómo analizar los observables que sea han recopilado consultando una sola herramienta en lugar de varias?
- ¿Cómo responder activamente a las amenazas e interactuar con el sistema y otros equipos?

Cortex, es un software de código abierto y gratuito, ha sido creado por TheHive Project. Los objetos observables, como direcciones IP y de correo electrónico, URL, nombres de dominio, archivos o hashes, se pueden analizar uno por uno o en modo masivo utilizando una interfaz web. Los analistas también pueden automatizar estas operaciones gracias a la API REST de Cortex

Cortex está escrito en Scala. El front-end usa AngularJS con Bootstrap. Su API REST no tiene estado, lo que le permite ser escalable horizontalmente. Los analizadores están escritos en Python. Se pueden escribir analizadores adicionales utilizando el mismo lenguaje o cualquier otro lenguaje compatible con Linux.

---

[28] *https://www.misp-project.org/*

Gracias a Cortex, TheHive puede analizar diferentes tipos de observables utilizando decenas de analizadores. Actualmente hay más de 120[29] analizadores disponibles públicamente.

Ilustración 22. Logo de Cortex

4.1.4 Almacenamiento

Como almacenamiento TheHive lleva utilizando ElasticSearch desde sus inicios, aunque con la última versión de la plataforma TheHive 4.1 pasará a utilizar una base de datos gráfica, dejando Elasticsearch para pasar a Apache Cassandra y se apoyandose en Apache Hadoop como sistema de archivos distribuido (HDFS).

Gracias a esta nueva arquitectura, TheHive 4 es escalable horizontalmente. Puede agregar tantos nodos TheHive, Cassandra y HDFS a su clúster de Security Incident Response Platform y sostener cualquier carga sin merma de rendimiento.

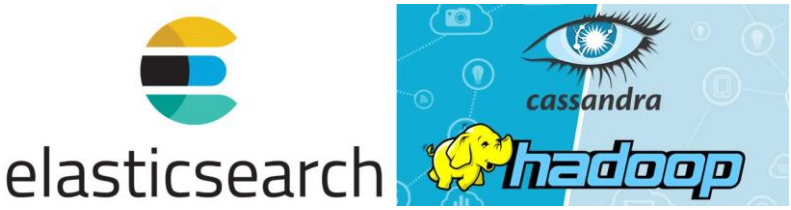


Ilustración 23. Almacenamientos de TheHive

4.2 Arquitectura de TheHive

El Front-End está desarrollado con AngularJS[30] que es un Framework de Javascript mantenido por Google, también utiliza la biblioteca multiplataforma Bootstrap[31] para diseño de sitios y aplicaciones web.

El Core de TheHive 4 está desarrollado en Scala[32], y posee conectores nativos con Cortex y MISP.

Con JanusGraph, TheHive 4 estructura la información en gráficos y los almacena en una base de datos Apache Cassandra. Todos los archivos que adjunta a los registros de tareas o agrega como observables se almacenan en un sistema de archivos distribuido de Hadoop (HDFS).

---

[29] *https://blog.thehive-project.org/2019/06/09/more-than-120-ways-of-analyzing-your-observables/*

[30] *https://es.wikipedia.org/wiki/AngularJS*

[31] *https://es.wikipedia.org/wiki/Bootstrap_(framework)*

[32] *https://es.wikipedia.org/wiki/Scala_(lenguaje_de_programaci%C3%B3n)*

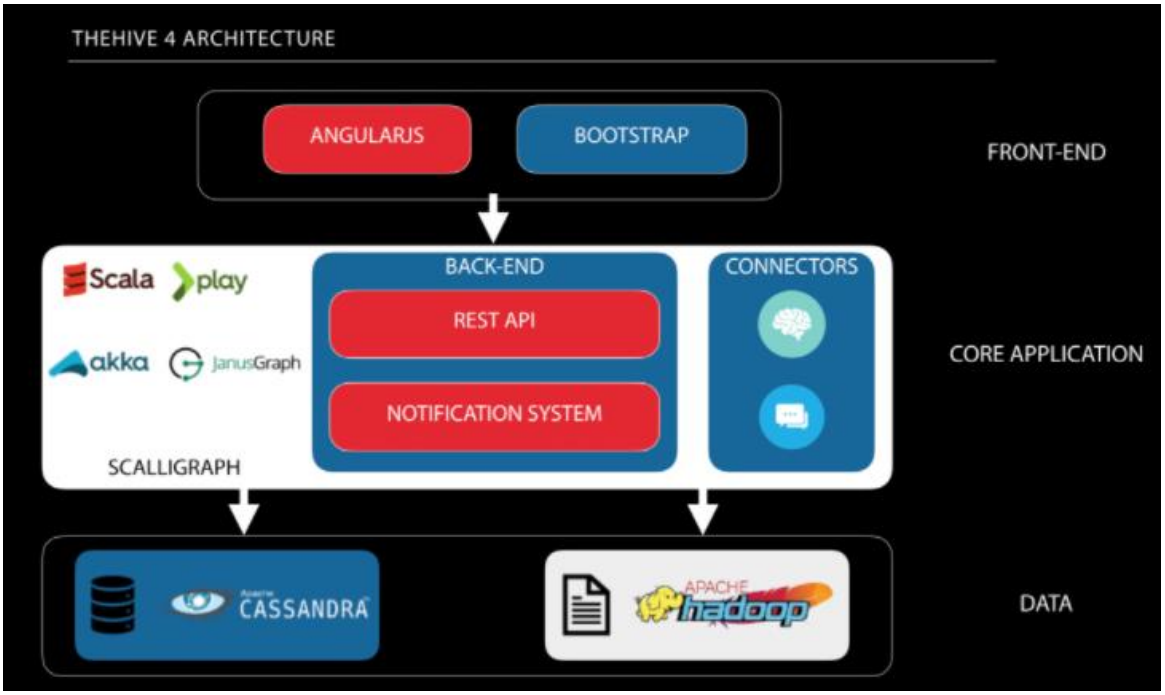


Ilustración 24. Arquitectura de TheHive 4

4.3 Cómo funciona TheHive

TheHive puede recibir alertas de diferentes fuentes (SIEM, IDS, correo electrónico, etc.) a través de su API REST, y es aquí donde los alimentadores de alerta (Alert Feeders) entran en juego.

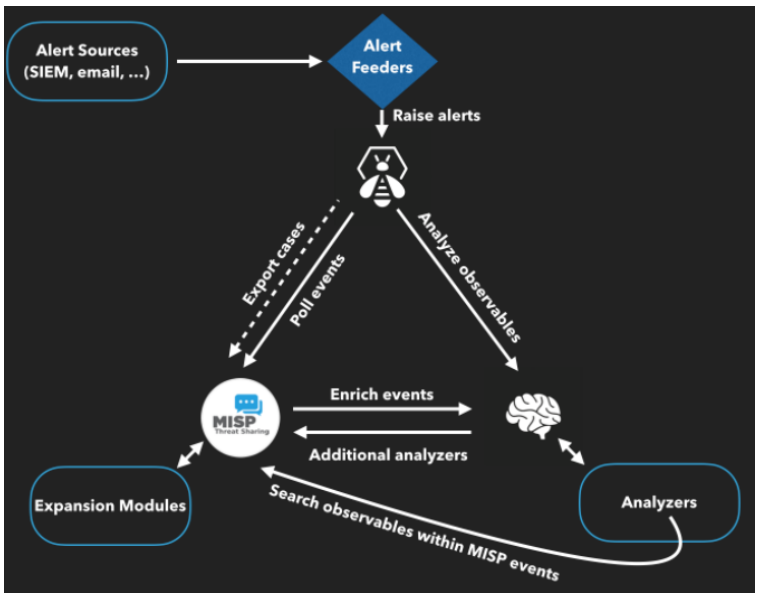


Ilustración 25. Funcionamiento de TheHive

TheHive, Cortex y MISP son tres productos de código abierto y gratuitos que pueden ayudarnos a combatir las amenazas y mantener a raya a los "malos".

TheHive, como SIRP, nos permite investigar incidentes de seguridad de forma rápida y colaborativa. Varios analistas pueden trabajar simultáneamente en tareas y casos. Si bien los casos se pueden crear desde cero, TheHive puede recibir alertas de diferentes fuentes gracias

a los alimentadores de alertas que consumen eventos de seguridad generados por múltiples fuentes y alimentan a TheHive utilizando la biblioteca TheHive4py. TheHive también se puede sincronizar con una o varias instancias MISP para recibir eventos nuevos y actualizados que aparecerán en el panel de alertas con todas las otras alertas generadas por otras fuentes. Posteriormente, los analistas pueden obtener una vista previa de las nuevas alertas para decidir si se debe actuar o no. Si es así, se pueden transformar en casos de investigación utilizando plantillas.

Para analizar los observables recopilados de una investigación y/o importados de un evento MISP, TheHive puede confiar en uno o varios motores de análisis Cortex. Cortex es otro producto independiente, cuyo único propósito es permitirnos analizar observables a escala gracias a su gran cantidad de analizadores, módulos de expansión MISP y cualquier analizador desarrollado. Cortex tiene una API REST que se puede utilizar para potenciar otros productos de seguridad, como software de "análisis", SIRP alternativo o MISP.

TheHive puede enriquecer los atributos gracias a Cortex, ya que tiene una integración nativa con él. La colaboración es clave en ciberseguridad.

4.4 Instalación y configuración de TheHive

Este apartado no pretende ser una guía de instalación de TheHive, pero si mostrar las posibilidades y decisiones a tomar al realizar la instalación.

La arquitectura modular de TheHive hace que sea compatible con varios tipos de bases de datos, sistemas de almacenamiento de archivos y sistemas de indexación. Las elecciones iniciales que decidamos para la arquitectura de destino y la configuración son cruciales, especialmente para la base de datos.

Si se necesita alta disponibilidad y tolerancia a fallos, la implementación de un clúster puede ser la opción, y dicha elección determina la base de datos, el almacenamiento de archivos y el sistema de indexación que se instalará.

Es posible instalar TheHive con paquetes RPM, DEB, Binarios y como una imagen de Docker.

Los requisitos de hardware dependen del número de usuarios simultáneos y de cómo utilizan el sistema. La siguiente tabla proporciona información para elegir el hardware:

Number of users	CPU	RAM
< 3	2	4-8
< 10	4	8-16
< 20	8	16-32

Ilustración 26. Requisitos hardware según el número de usuarios

TheHive soporta muchos tipos de bases de datos, pero la recomendada en desde la versión 4.1.0 es Apache Cassandra.

Al igual que para las bases de datos, existen varias opciones con respecto al sistema de archivos. Básicamente, para configuraciones independientes, usar el sistema de archivos local es lo más sencillo. Si decidimos instalar un clúster, hay varias opciones:

- Usar una carpeta compartida de NFS
- Usando Apache Hadoop, un sistema de archivos distribuido
- Usando un servicio de almacenamiento compatible con S3

Para la indexación, TheHive 4.1 se ha publicado con un sistema de indexación dedicado. Para una configuración independiente es suficiente con usar un índice local con Lucene[33]. En el caso de un clúster, todos los nodos deben conectarse al mismo índice: para ello se requiere una instancia de Elasticsearch.
Para la instalación seguiremos el siguiente orden:

1. Máquina virtual de Java.
2. Base de datos elegida.
3. Motor de indexación
4. Sistema de Archivos
5. TheHive Project
6. Configuración de TheHive
7. Cortex
8. Configuración de Cortex
9. MISP
10. Configuración de MISP

4.5 SOAR's en nubes públicas

Para los clientes más pequeños la entrega de esta tecnología en la nube es cada vez más frecuente. Gartner ve en la nube un vehículo viable para muchos escenarios. La paridad de funciones con las soluciones locales (para los proveedores que admiten la nube) es prácticamente la misma, por lo que a menudo no hay riesgo de que la "versión en nube sea menos rica en funciones". La mayoría de los proveedores que tienen versiones en la nube también están realizando implementaciones ágiles, enviando más actualizaciones, con más frecuencia en comparación con una cadencia más lenta para las versiones locales. Esto se cumple especialmente cuando dentro del sistema se incorporan trabajadores remotos, de manera que la orquestación pasa a trabajar principalmente con soluciones de punto final (a menudo en la nube), como EPP y, en particular, EDR, puertas de enlace web seguras (SWG) y agentes de seguridad de acceso a la nube (CASB). para actividades de respuesta.

En este apartado vamos a ver las soluciones de nube pública que están ofreciendo los grandes proveedores en la actualidad.

4.5.1 Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas a través de monitoreo continuo de actividad de red para detectar actividades maliciosas y comportamientos no autorizados

[33] *https://lucene.apache.org/core/3_0_3/fileformats.html*

con el fin de proteger sus datos, cargas de trabajo y cuentas de AWS almacenados en Amazon S3. Con la nube, las tareas de recopilación y la adición de cuentas las actividades de red se simplifican.

GuardDuty proporciona una solución inteligente y rentable para la detección constante de amenazas en AWS. El servicio utiliza el aprendizaje automático (ML), la detección de anomalías y la inteligencia contra amenazas integrada para identificar y priorizar las posibles amenazas. GuardDuty analiza miles de millones de eventos a través de varios orígenes de datos de AWS, como los registros de eventos de AWS CloudTrail, los registros de flujo de Amazon VPC y los registros de DNS. Con tan solo unos pocos clics en la consola de administración de AWS, se puede activar GuardDuty sin necesidad de implementar o mantener software o hardware. Mediante la integración con Amazon CloudWatch Events, las alertas de GuardDuty son procesables, fáciles de agregar a diferentes cuentas y fáciles de insertar en los sistemas existentes de flujos de trabajo y administración de eventos.

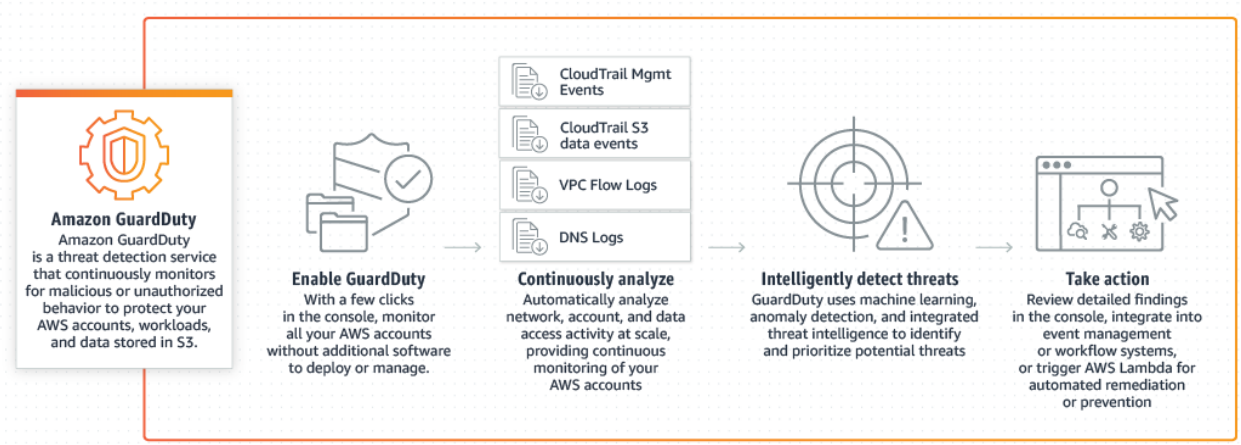


Ilustración 27. Funcionamiento de GuardDuty

4.5.2 Azure Sentinel

Microsoft Azure Sentinel es una solución **de administración de eventos de información de seguridad (SIEM)** y **respuesta automatizada de orquestación de seguridad (SOAR)** que es escalable y nativa de la nube. Azure Sentinel ofrece análisis de seguridad inteligente e inteligencia frente a amenazas en toda la empresa, de forma que proporciona una única solución para la detección de alertas, la visibilidad de amenazas, la búsqueda proactiva y la respuesta a amenazas.

Azure Sentinel permite obtener una vista general de toda la empresa, lo que suaviza la tensión de ataques cada vez más sofisticados, volúmenes de alertas cada vez mayores y plazos de resolución largos.

- **Recopile datos a escala de nube** de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.
- **Detecte amenazas que antes no se detectaban** y reduzca los falsos positivos mediante el análisis y la inteligencia de amenazas sin precedentes de Microsoft.
- **Investigue amenazas con inteligencia artificial** y busque actividades sospechosas a escala, aprovechando el trabajo de ciberseguridad que ha llevado a cabo Microsoft durante décadas.

- **Responda a los incidentes con rapidez** con la orquestación y la automatización de tareas comunes integradas.

Forrester en su análisis de Plataformas de Seguridad del año 2020 en el Q4[34], destaca a Azure Sentinel como uno de los líderes destacando sobre las demás en su estrategia.

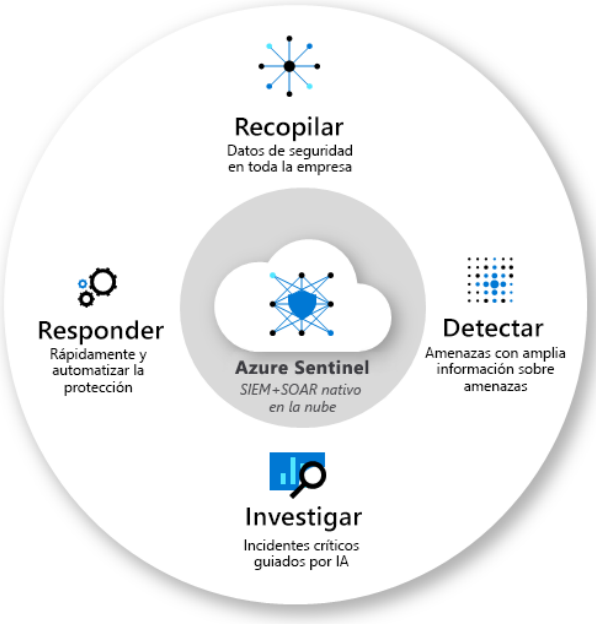


Ilustración 28. Funcionamiento de Azure Sentinel

4.5.3 Google Chronicle

Es la plataforma de análisis de seguridad de Google Cloud la cual permite a los equipos almacenar y analizar todos sus datos de seguridad en un solo lugar para detectar e investigar amenazas a gran escala. Como dato destacado reciente, BBVA incorporará en su estrategia de seguridad las innovadoras capacidades de inteligencia artificial de Google Cloud.

Chronicle Detect es una solución de detección de amenazas construida en la infraestructura de Google para ayudarlo a identificar amenazas a una velocidad y escala incomparables. Los equipos de seguridad pueden enviar su telemetría para que los datos de seguridad puedan tenerse en cuenta para las detecciones. Chronicle Detect hace que esos datos de seguridad sean útiles asignándoles automáticamente un modelo de datos común entre máquinas, usuarios e indicadores de amenazas, para que pueda aplicar rápidamente poderosas reglas de detección a un conjunto unificado de datos.

Ilustración 29. Logo de Chronicle Detect

[34] *https://www.bankinfosecurity.com/whitepapers/forrester-wave-security-analytics-platforms-q4-2020-w-7414*

5. Pruebas de concepto

5.1 Plataforma TheHive

La Plataforma TheHive fue creada como un producto Open Source al cual la Comunidad y proveedores aportarían mayor riqueza.

Aquí podemos ver uno de los que contiene la plataforma Dashboard.

Ilustración 30. Diferentes dashboards en TheHive Project

Antes de realizar la prueba de concepto de la Plataforma TheHive conviene familiarizarse con el entorno y los diferentes módulos, para ello se puede consultar el *Anexo A. Usando TheHive Project*.

Para realizar la prueba de concepto, lo primero que haremos será crear un nuevo caso en TheHive y comprobaremos los resultados que devuelven los analizadores incluidos en la plataforma llamados Analizers.

Comenzamos creando un nuevo caso en TheHive.

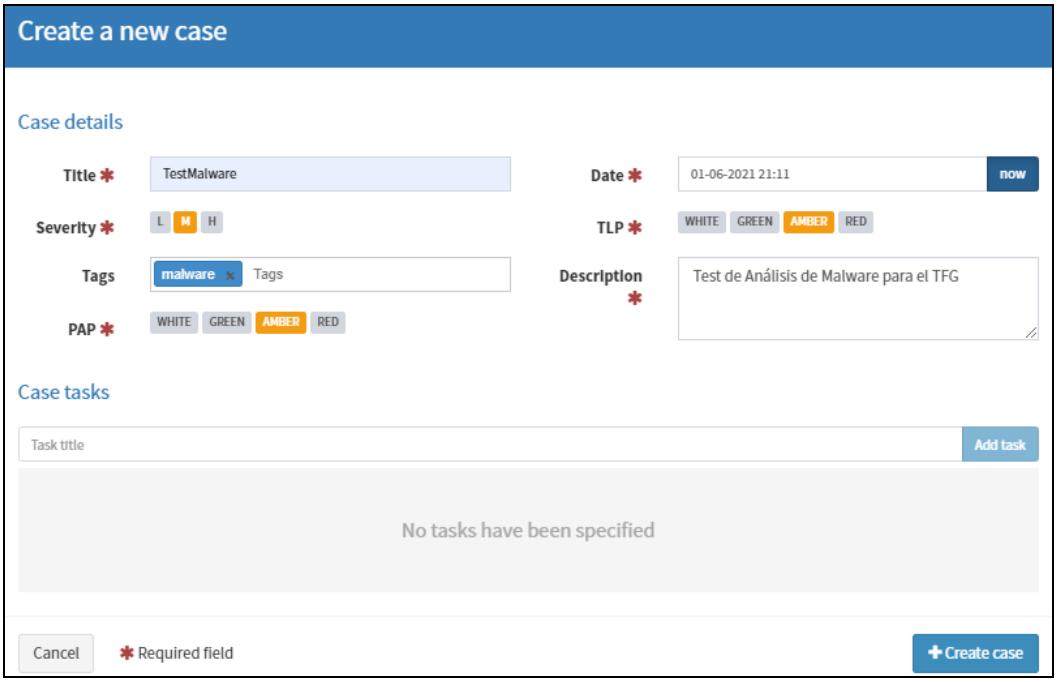


Ilustración 31. Creación nuevo caso en TheHive

Una vez creado el caso iremos a la pestaña **Observables** donde pulsaremos sobre **+Add observable(s)**. Y lo rellenaremos adjuntando el fichero sospechoso y seleccionamos **+Create observable**.

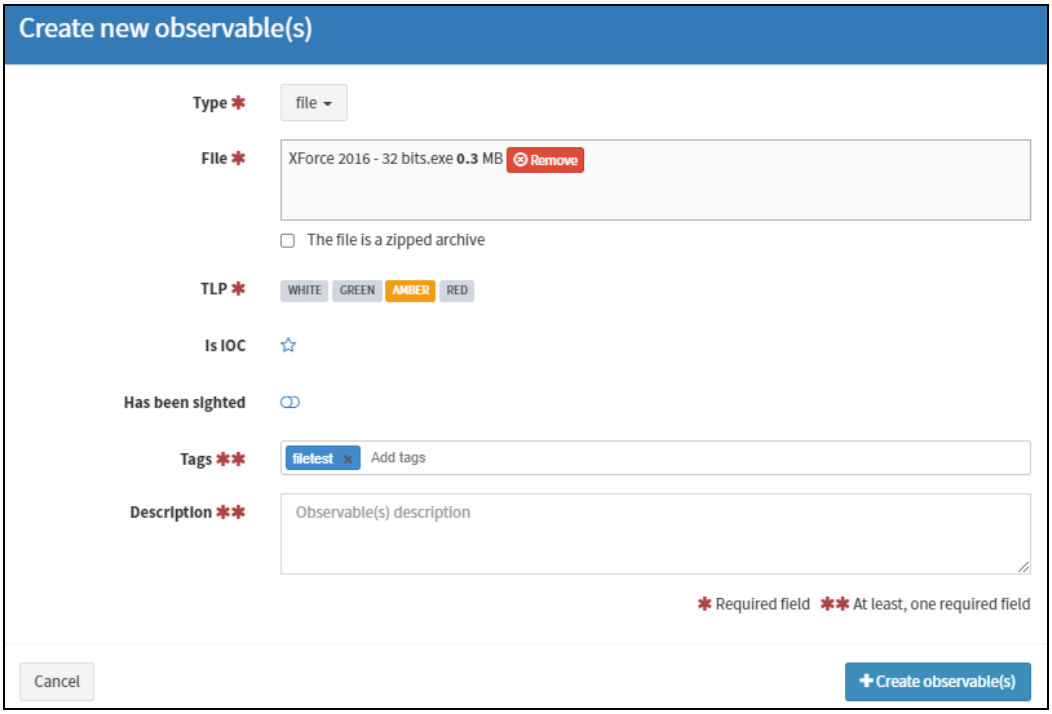


Ilustración 32. Creación de Observable en TheHive

Una vez creados los diferentes observables seleccionamos el que queremos analizar.

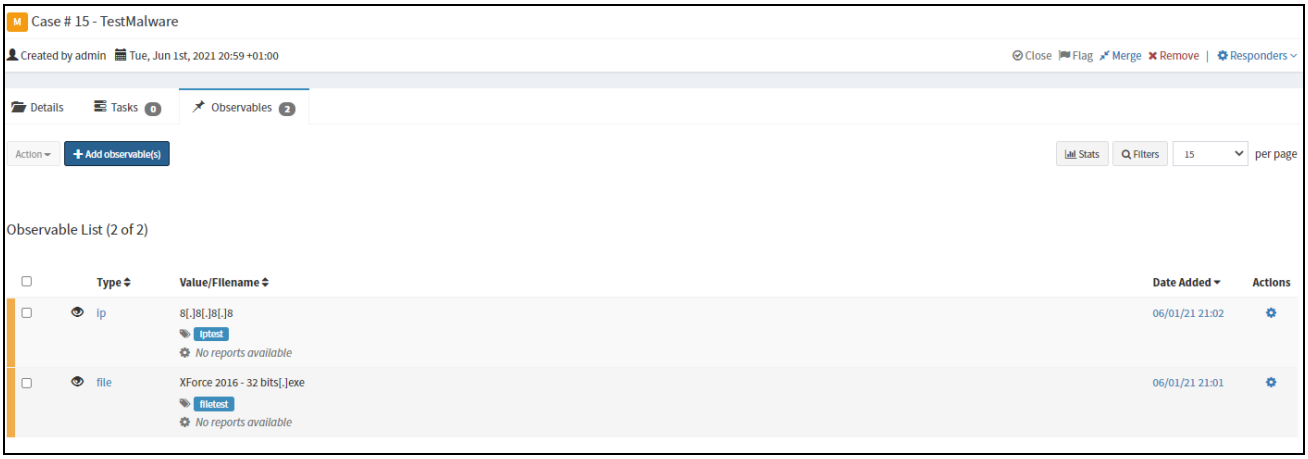


Ilustración 33. Listado de observables de TheHive

Y a continuación seleccionamos **Run all** para utlizar los analizadores sobre el fichero que habíamos añadido.

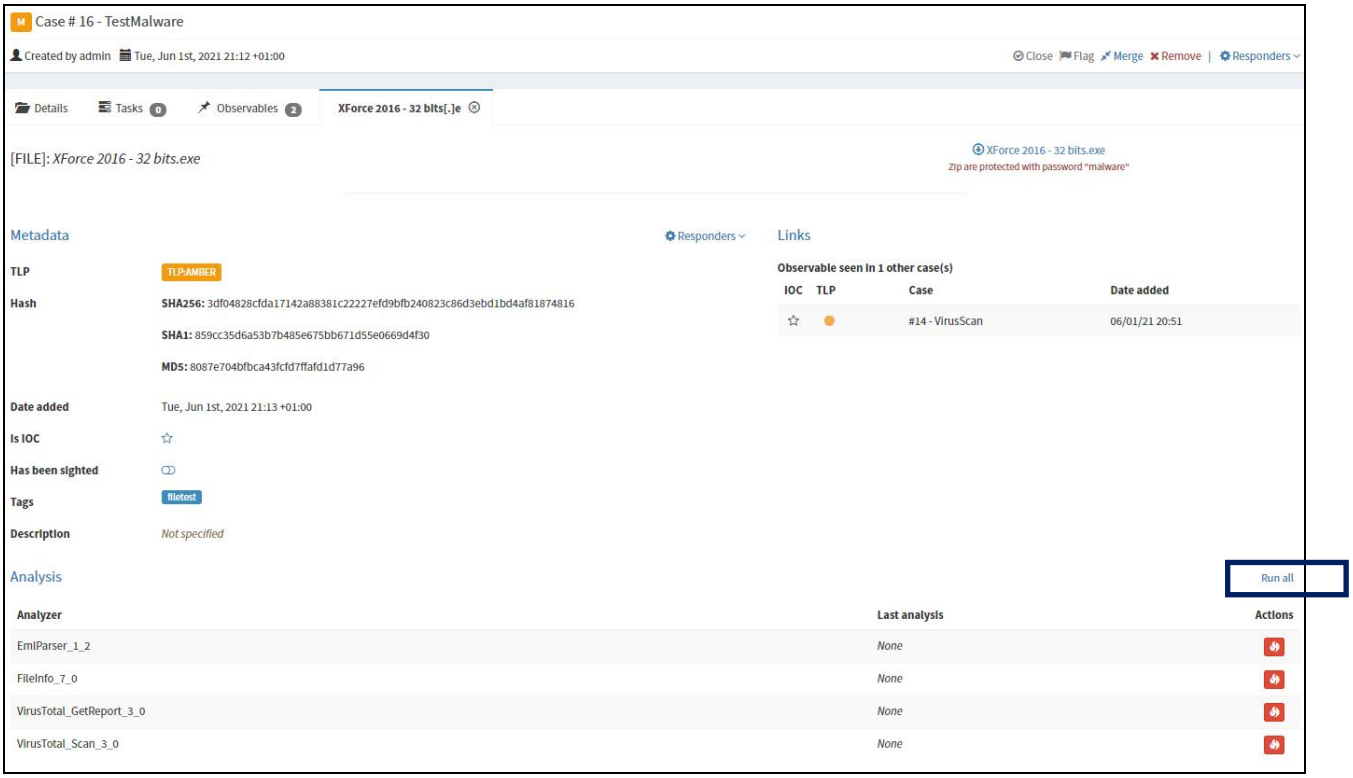


Ilustración 34. Análisis de observables en TheHive

La ejecución de Analyzers se irán completando y podremos ver la historia en la parte derecha

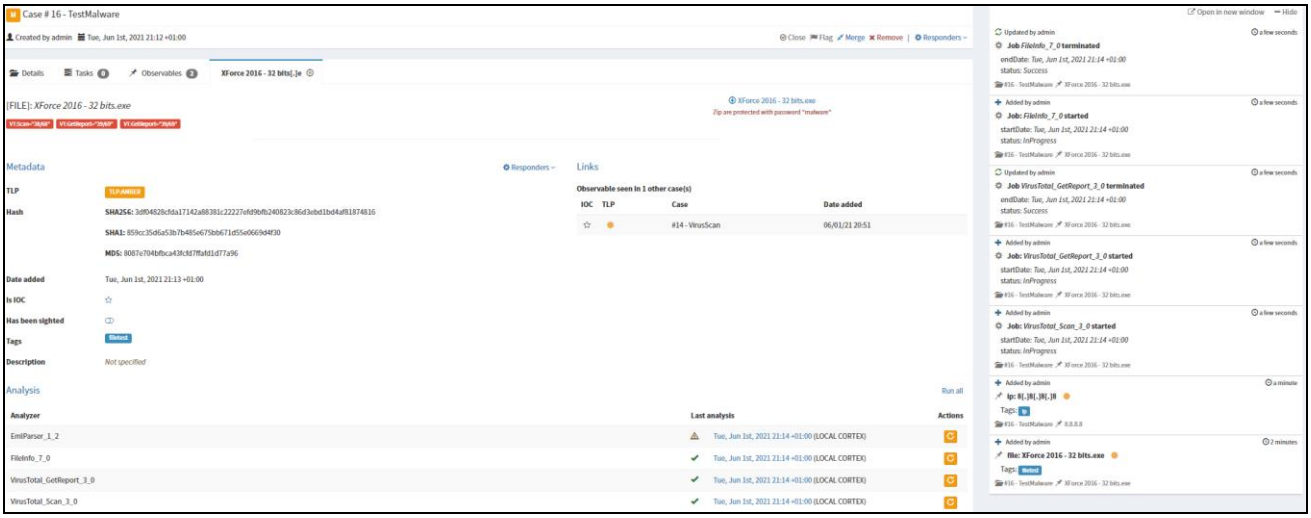


Ilustración 35. Ejecución de observables en TheHive

También podemos ver el resultado de cada Analyzers.

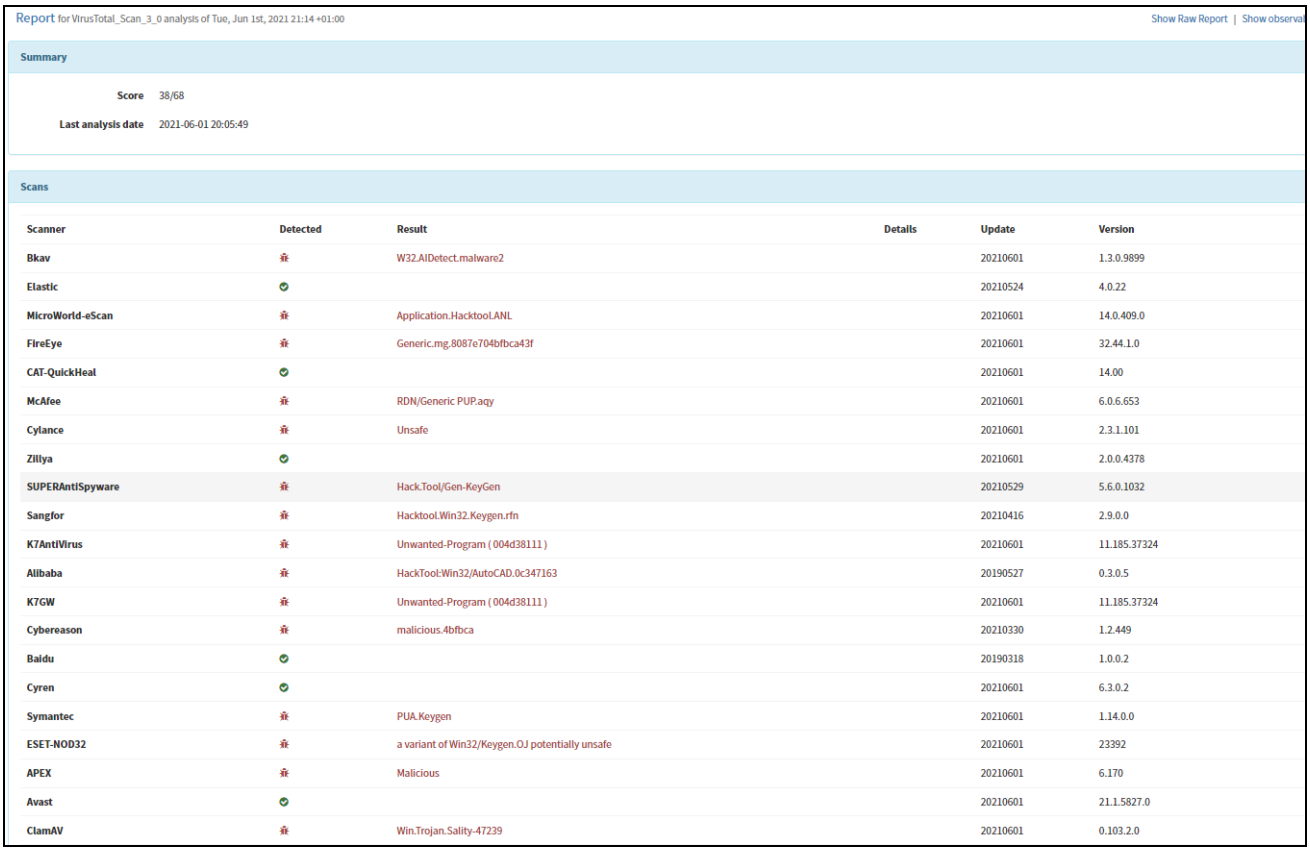


Ilustración 36. Resultado de Analyzer VirusTotal

Si nos vamos a Cortex vemos que los mismos análisis aparecen en el apartado **Jobs History**.

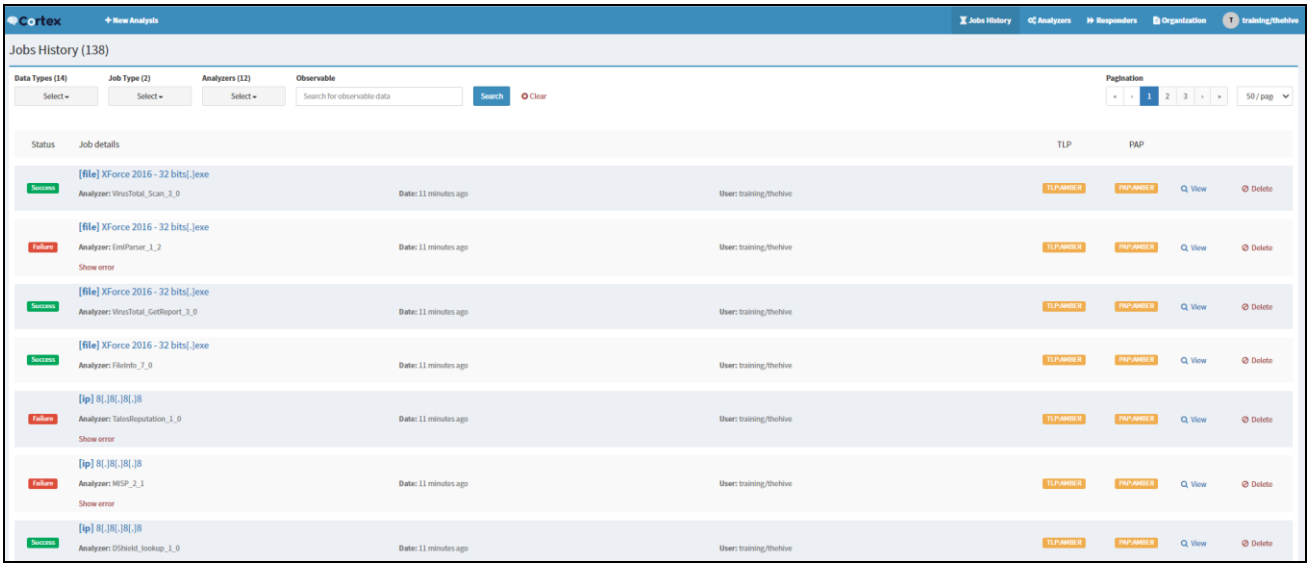


Ilustración 37. Acciones Analyzers en Cortex

5.1.1 Corolario

TheHive es una plataforma muy completa. Nos permite testear el comportamiento de una plataforma por parte de diferentes analistas. Al ser un software libre y con diferentes versiones en funcionamiento a la vez, no resulta sencillo poder configurarla en su totalidad y ver su completo funcionamiento ya que requeriría la integración a través de las diferentes APIs desarrolladas por el equipo de TheHive Project. Pero ha sido interesante la prueba y comprobar que la comunidad de usuarios de TheHive es muy variada y aportan mucha ayuda.

La plataforma goza de cierta popularidad en Internet, aunque los creadores, están tratando de monetizar el producto con servicios de soporte, formación, instalación y configuración. El siguiente paso en su hoja de ruta consiste en ofrecer TheHive y Cortex como un SaaS[35].

[35] *https://www.strangebee.com/cloud*

5.2 Plataforma GuardDuty

Para la prueba de concepto conviene familiarizarnos con el entorno, para ello conviene consultar el *Anexo B. Usando Amazon GuardDuty*.

Utilizaremos una función Lambda llamada "GuardDutytoACL-GuardDutytoACLLambda" cuyo código se puede se encuentra en el *Anexo C. Función lamdda GuardDuty_to_acl* y la cual forma parte de una plantilla de CloudFormation que desplegaremos para la prueba.

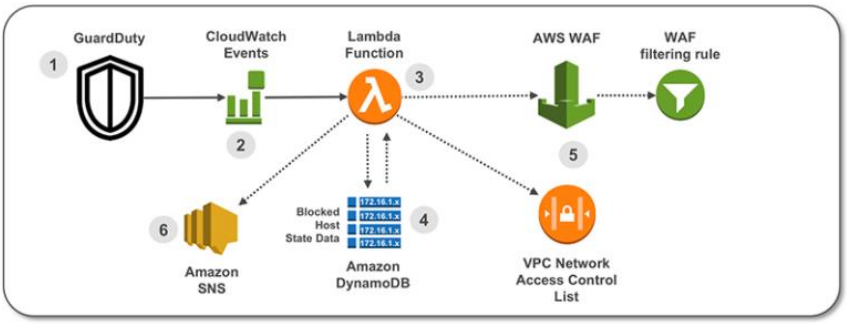


Ilustración 38. Plantilla GuardDutyACL

Esta función Lambda funciona de la siguiente manera:

1. Cuando CloudWatch clasifica un ataque de fuerza bruta sobre una instancia EC2 (UnauthorizedAccess:EC2/RDPBruteForce).
2. Se crea una entrada en las ACL (Access Control List) de destino para denegar el host sospechoso.
3. La función Lambda envía una notificación a una dirección de correo electrónico.
4. Al introducir la IP origen en la ACL se bloquea el tráfico del host sospechoso ayudando a mitigar la amenaza mientras se realiza una investigación y corrección adicional.

Comprobamos lo que ha creado la plantilla:

1. Una lista negra de IPs en AWS WAF.

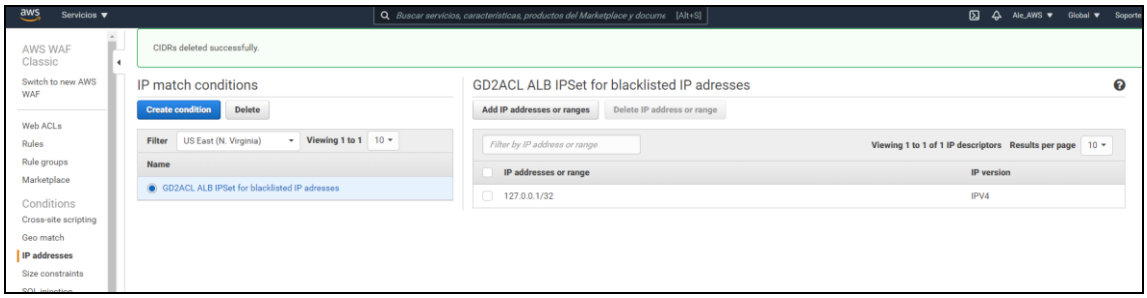


Ilustración 39. Contenedor de IPs marcadas como Blacklist

2. Dos funciones Lambda

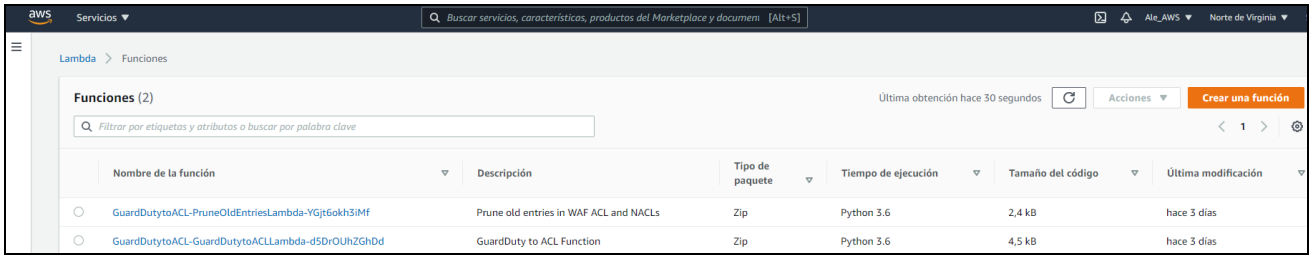


Ilustración 40. Listado de funciones Lambda

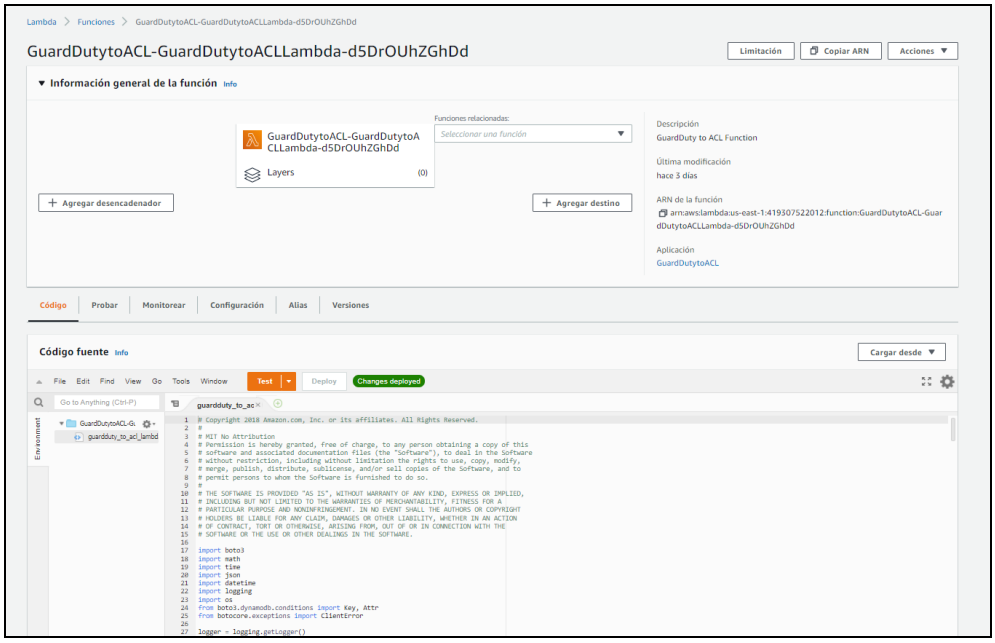


Ilustración 41. Detalle de la función Lambda GuardDutytoACL

3. Un tema y suscripción a SNS con la cuenta de correo que hayamos elegido en el despliegue de la plantilla.

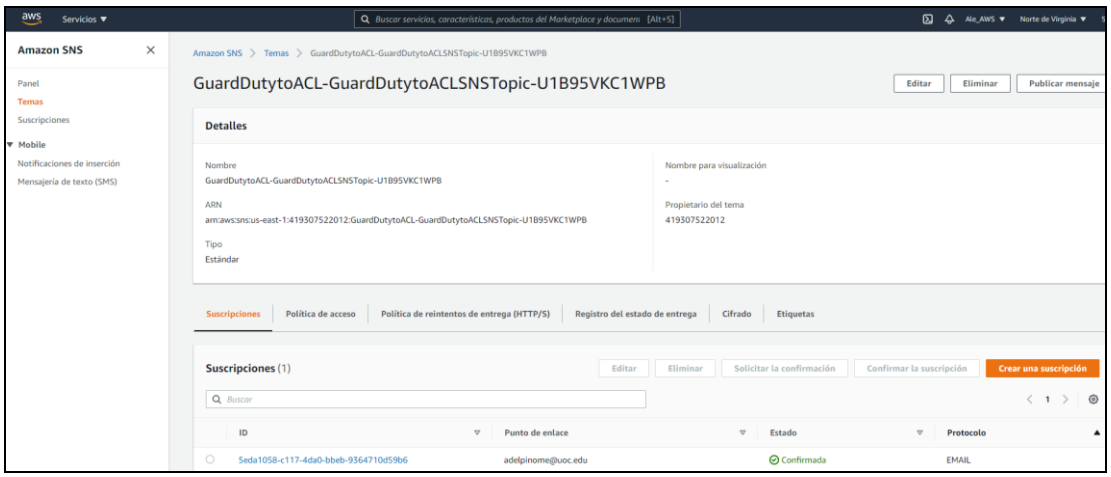


Ilustración 42. Detalle de SNS

La prueba consistirá en un ataque de fuerza bruta a través del programa xHydra contenido dentro de una máquina virtual con la conocida distribución Kali. Desde dicha máquina realizaremos un ataque a través de RDP contra una instancia EC2 ubicada en AWS.

El ataque lo realizaremos desde una IP Dinámica que en el momento de la prueba era: 85.155.196.168.

Ilustración 43. Detalle de IP de origen del ataque

Un esquema sencillo de entender para la prueba es el siguiente:

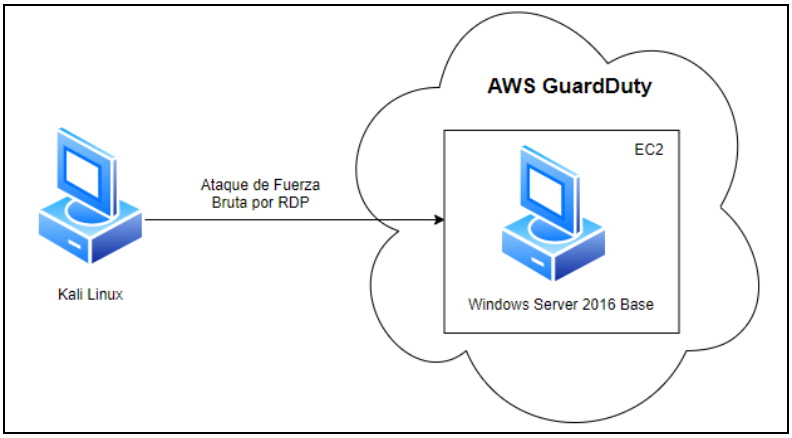


Ilustración 44. Esquema de ataque de Fuerza Bruta RDP a una instancia de AWS

Comenzaremos creando una instancia en EC2 vulnerable y accesible remotamente:

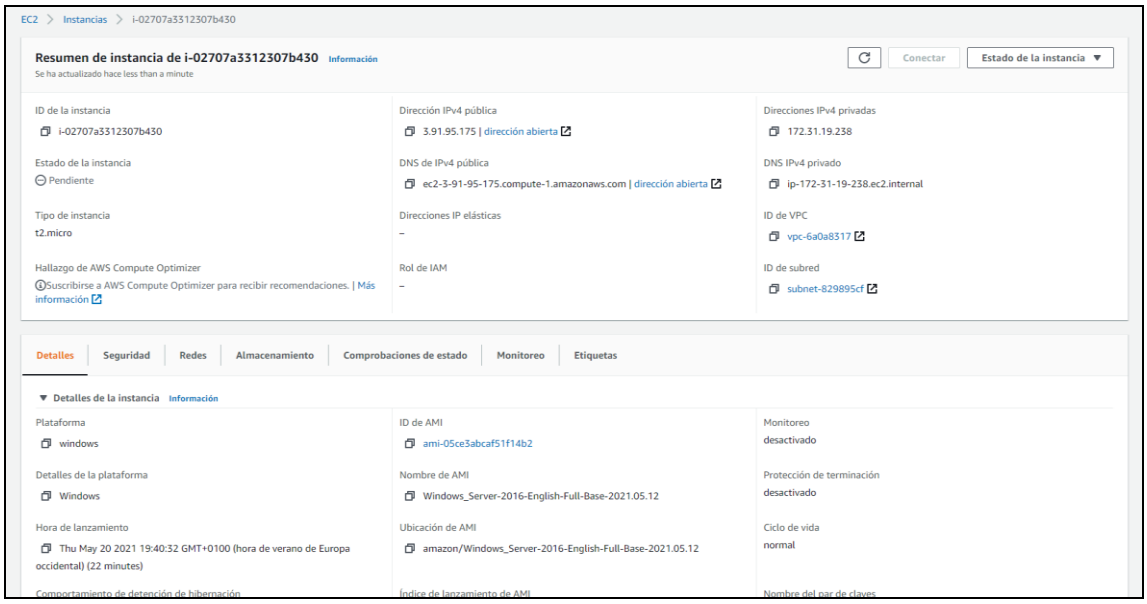


Ilustración 45. Instancia de EC2 vulnerable

Comprobamos que es posible realizar la conexión desde xHydra utilizando el usuario y contraseña legítimo:

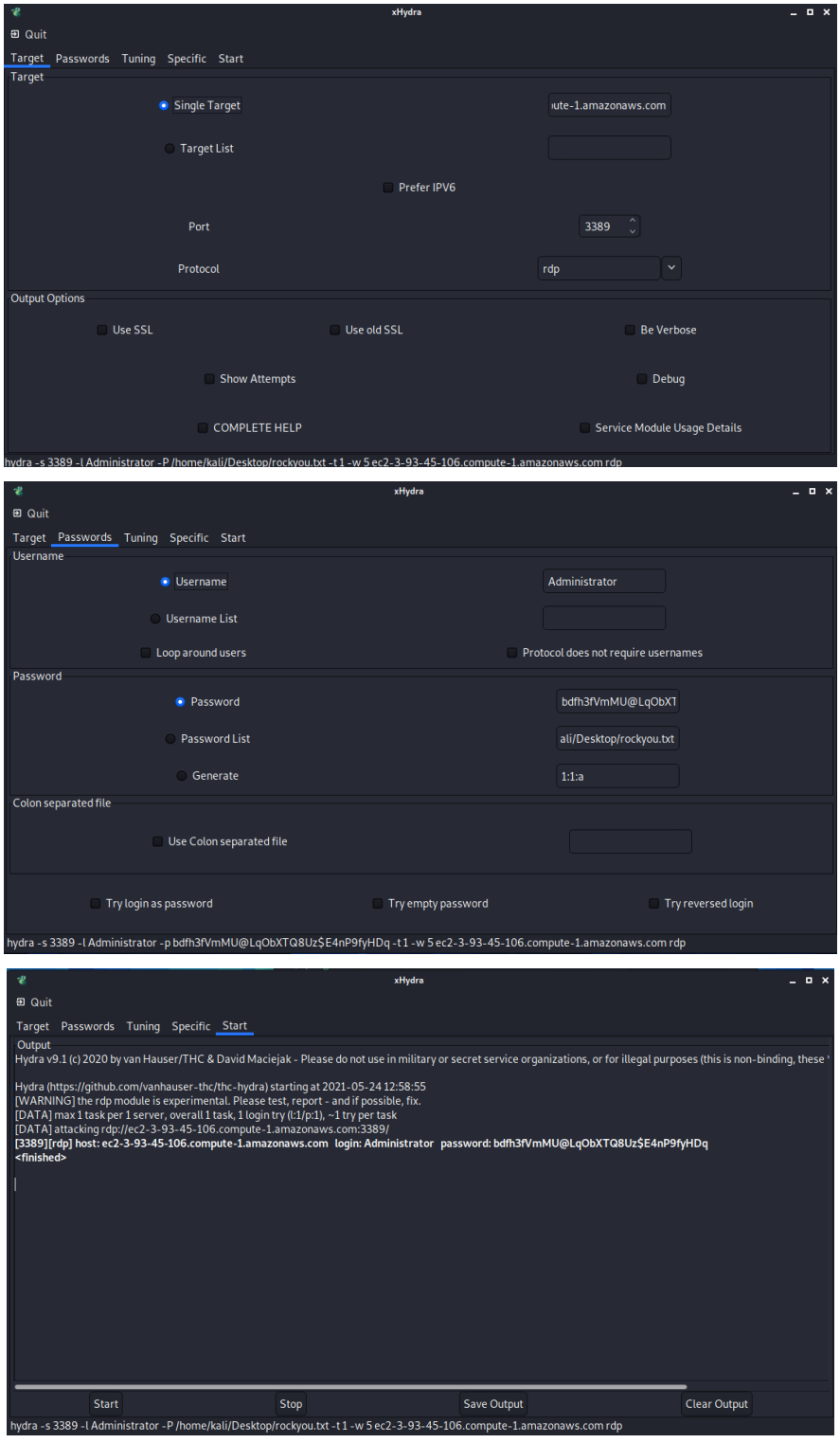


Ilustración 46. Conexión exitosa desde xHydra

A continuación, realizamos el ataque a la instancia EC2 Vulnerable utilizando un ataque de diccionario.

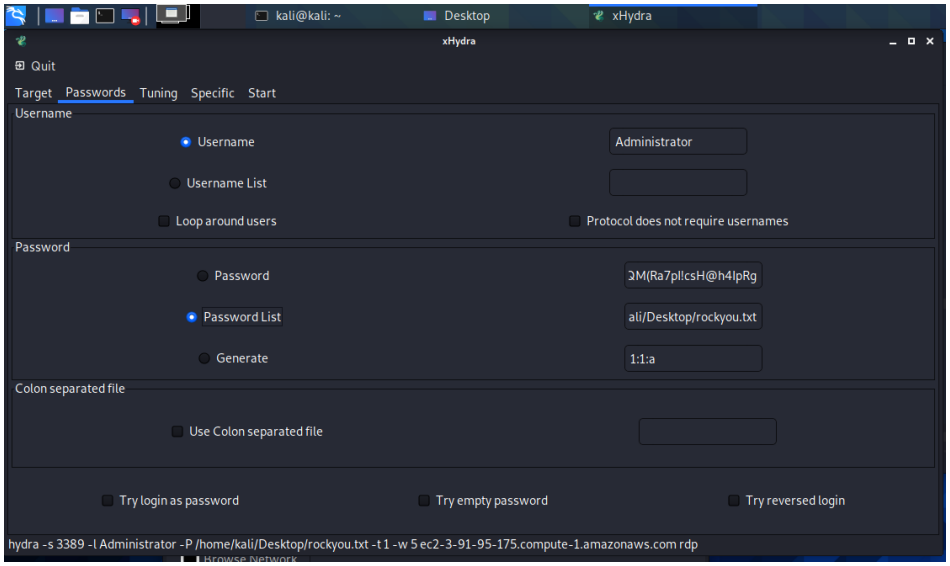


Ilustración 47. Configuración de ataque de diccionario desde xHydra

Observamos que después de varios intentos vemos que se pierde la conexión ya que la instancia en EC2 ha dejado de estar accesible.

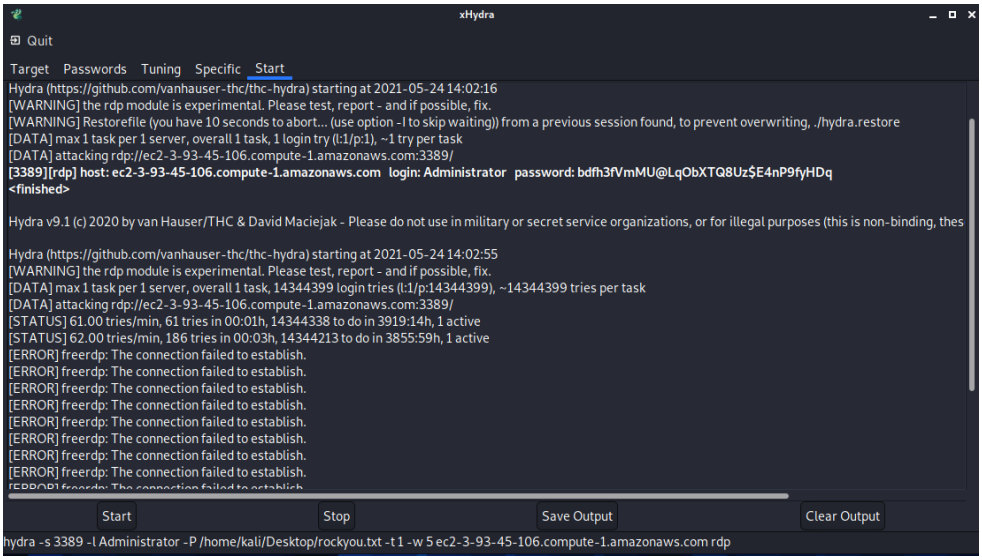


Ilustración 48. Detalle de pérdida de conexión desde xHydra

Revisemos lo que ha ocurrido en el momento que se perdió la conexión:

1. Nos ha llegado un correo indicándonos que se ha detectado una actividad sospechosa.

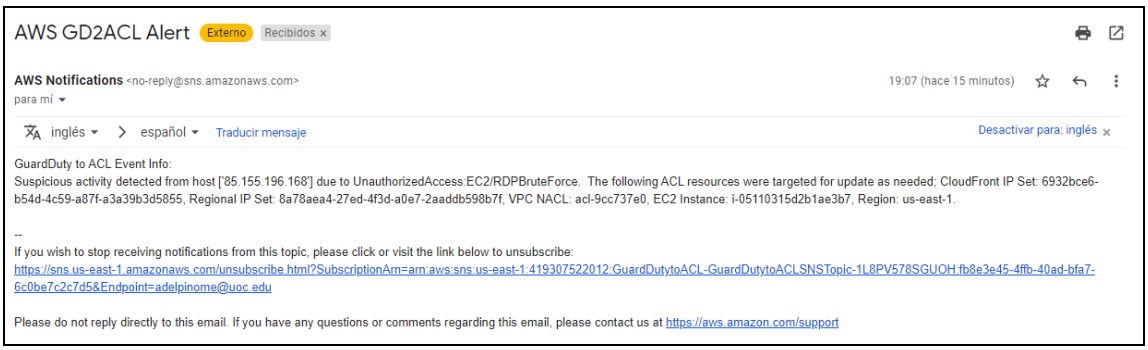


Ilustración 49. Correo de alerta de AWS

2. Revisamos las ejecuciones de la función Lambda “GuardDutytoACL-GuardDutytoACLLambda”. Y vemos que se ha ejecutado recientemente.

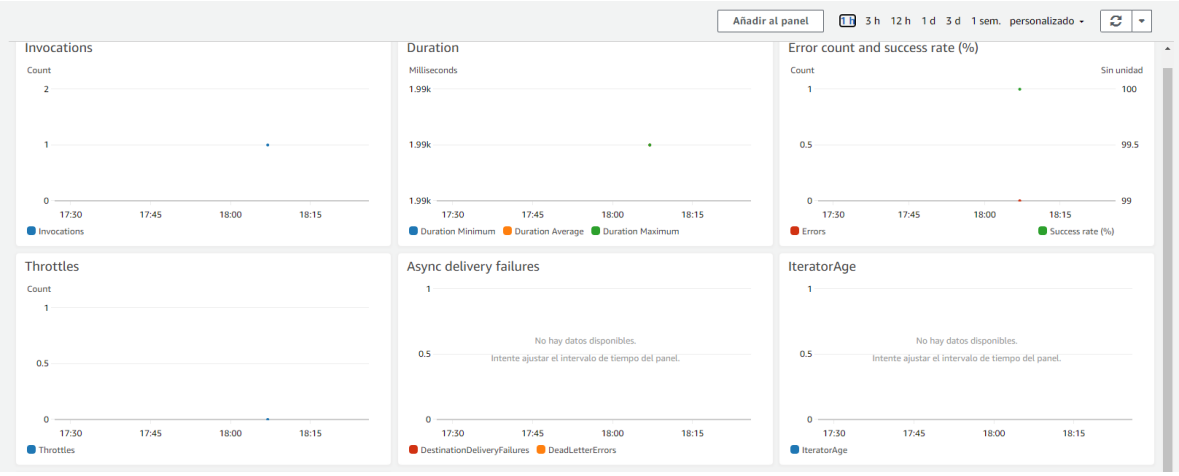


Ilustración 50. Dashboard de ejecución de GuarDutytoACLLambda

3. Revisamos los registros de CloudWatch y vemos el detalle de las acciones, donde nos indica que se ha encontrado un hallazgo y se ha añadido la IP origen: 85.155.196.168 a la lista ACL y se ha creado una renueva regla de firewall (71) para denegar la conexión.

Ilustración 51. Detalle de eventos en AWS

4. Revisamos la regla de firewall en el la subnet 172.31.16.0/20 de VPC y comprobamos que en al apartado **Network ACL** que se ha creado una regla de entrada que deniega la conexión a la dirección ip: 85.155.196.168/32

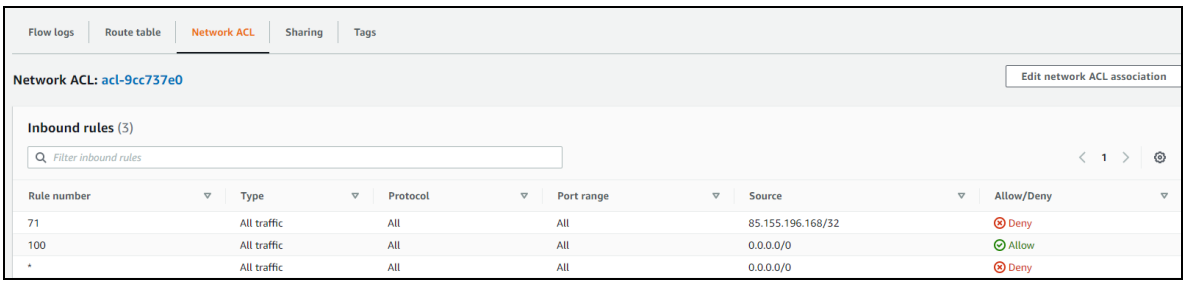


Ilustración 52. Regla creada en VPC

5. Comprobamos que en el servicio WAF & Shield que la dirección ip: 85.155.196.168/32 ha sido introducida en la lista negra.

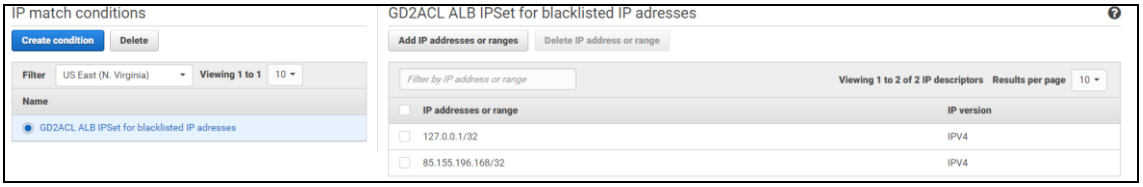


Ilustración 53. Registros de IP incluidos en la Blacklist

5.2.1 Corolario

Las funciones Lambda son las que ejecutarán aquellas acciones de remediación temporales o permanentes ante los eventos detectados por GuardDuty.

En nuestro caso, cuando se ha detectado un ataque RDP de fuerza bruta, la IP ha origen ha sido introducida en una lista negra para su posterior análisis, pero de manera preventiva se crea una regla de denegación de acceso, automatizando el proceso de protección de la instancia.

El ecosistema de AWS es muy amplio y variado, permite una gran flexibilidad, y proporciona a herramientas de SOC de una manera muy sencilla e intuitiva.

6. Conclusiones

A continuación, se describen las conclusiones finales del trabajo, así como algunas lecciones aprendidas:

- Las plataformas SOARs se están convirtiendo en la principal herramienta de uso por parte de los SOC. Vienen a complementar a las soluciones SIEM que están muy implantadas en la actualidad.
- El hecho de poder automatizar respuestas ante amenazas es un gran logro a la hora de prevenir y tomar acciones inmediatas ante las amenazas.
- Hay dos cosas principales que debe ser abordada por el SOC de próxima generación, el procesamiento de una gran cantidad de datos estructurados y no estructurados y proporcionar las alertas predictivas basadas en el aprendizaje continuo de la infraestructura dinámica de TI.
- Las herramientas SIEM de próxima generación utilizarán el aprendizaje automático que básicamente está combinando las reglas o algoritmos con las estadísticas, que se pueden utilizar para hacer análisis inteligentes basados en el conocimiento que producirán resultados predictivos procesables.
- La mayor integración SIEM+SOAR será parte importantísima en los SOC. Junto con el mayor desarrollo de la Inteligencia Artificial y Machine Learning. Para poder detectar en el menor tiempo posible los ataques multivector que se están produciendo en la actualidad.
- La vida de los analistas de seguridad será más fácil liberándolos de las tareas repetitivas y así usar su tiempo e inteligencia en la definición y ejecución del plan de respuesta a incidentes para reducir el impacto.
- Es esencial que las organizaciones utilicen la tecnología proactiva de seguridad, orquestación, automatización, respuesta (SOAR) y las capacidades de mitigación inteligente automatizadas integrales a través de sus redes de datos para mantenerse al día con la creciente sofisticación y organización de delincuentes cibernéticos bien equipados y bien financiados y actores de amenazas basados en el Estado.
- Las plataformas SOAR en nube van a facilitar su adopción. Tal es así, que las grandes nubes públicas tienen sus propios productos que irán evolucionando, acercando el uso de SOAR a PYMES que se puedan beneficiar de su uso.

6.1 Seguimiento de la planificación y metodología

La motivación que me llevó a elegir el tema del TFM, era principalmente porque desconocía por completo que era una plataforma SOAR, tampoco tenía muy clara la labor de un SOC y cómo ciertos términos se relacionaban, como son: CERT, CSIRT o MSSP.

Ante tal desconocimiento, la planificación incluía gran cantidad de búsqueda de referencias e información, junto con una planificación que me ayudara a poner en contexto la importancia

que tienen actualmente las plataformas SOAR o al menos lo que se espera de ellas según evolucionen.

En general la planificación se ha podido seguir sin muchos problemas, es cierto que cuanta más información encontraba y encajaba, la cantidad de apartados iban en aumento, así como los títulos de cada apartado.

Gracias a los comentarios del tutor he podido corregir el enfoque con el que afrontaba el trabajo. Me ha servido de motivarme a realizar un mejor trabajo documental mejorando mi conocimiento de las herramientas de edición de texto.

Enfrentarse a un TFM ha sido una muy buena experiencia, la recopilación de información, para plasmarla en un documento formal, el análisis en el mercado de las plataformas y poder experimentar con plataforma reales de uso en la actualidad, complementan un documento que aglutina mucha información que puede ser útil en investigaciones actuales y futuras.

El uso del término SOAR tiene algo de polémica, ya que lo empezó a utilizar Gartner no hace mucho (2017). Hubiera sido de gran utilidad que Gartner tuviera definido un cuadrante mágico para este tipo de plataformas, pero lamentablemente, a día de hoy, no lo tiene debido a que consideran que tanto SIEM como SOAR son tecnologías contemporáneas en seguridad, trabajan muy de cerca, y el crecimiento de SIEM como tecnología está estrechamente relacionado con el crecimiento futuro de SOAR. Lógicamente yo no tengo el tiempo, medios ni conocimiento suficiente para realizar estos análisis por mi cuenta. Lo cierto es que la consultora Forrester no usaba el término SOAR hasta hace muy poco ya que preferían usar el término SOA. Tampoco tienen una onda específica de dichas plataformas, lo engloban todo en análisis de Plataformas de Seguridad.

6.2 Líneas de Trabajo futuro

Cómo líneas de trabajo futura se me ocurre la implementación completa de un SOC que haga uso de un SIEM y un SOAR, puede resultar compleja, pero la Plataforma TheHive al ser de código abierto ofrece esa posibilidad, es cierto, que hay determinados pasos en la instalación y configuración que no están bien descritos y bien referenciados según la versión, pero puede ser un modelo de SOC a bajo coste a implementar por medianas empresas con personal suficiente y maduras en cuanto a la importancia de la seguridad.

Otra línea de investigación podría ser el estudio de los diferentes playbooks que usan las diferentes plataformas SOAR y cómo es su programación. Sin perder de vista como se elaboran en las grandes plataformas de nube pública (AWS, Azure y Google).

Por la onda de Forrester de 2020, los avances de Azure en cuanto a seguridad son muy destacables, y tienen un SOAR muy visual como es Azure Sentinel, quizás una comparativa de plataformas de seguridad en nube pública pudiera ser otra línea de trabajo futura.

7. Glosario

AI: “Artificial Intelligence”, es la inteligencia llevada a cabo por máquinas. Coloquialmente, el término inteligencia artificial se aplica cuando una máquina imita las funciones «cognitivas» que los humanos asocian con otras mentes humanas.

API: “Application Programming Interface”, es un conjunto de rutinas que provee acceso a funciones de un determinado software. Son publicadas por los constructores de software para permitir acceso a características de bajo nivel o propietarias, detallando solamente la forma en que cada rutina debe ser llevada a cabo y la funcionalidad que brinda, sin otorgar información acerca de cómo se lleva a cabo la tarea.

Ataque de día cero: (en inglés zero-day attack o 0-day attack) es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Esto supone que aun no hayan sido arregladas.

AWS: “Amazon Web Services”, es una colección de servicios de computación en la nube pública (también llamados servicios web) que en conjunto forman una plataforma de computación en la nube.

Deep Web. “Internet profunda”, es el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores.

DevOps: “Development -desarrollo- y Operations -operaciones-“es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software (Dev) y la operación del software (Ops). La principal característica del movimiento DevOps es defender enérgicamente la automatización y el monitoreo en todos los pasos de la construcción del software, desde la integración, las pruebas, la liberación hasta la implementación y la administración de la infraestructura.

Endpoints: Un EndPoint es un dispositivo informático remoto que se comunica con una red a la que está conectado. Los ejemplos de Enpoint incluyen: ordenadores de escritorio, portátiles, tables, servidores, estaciones de trabajo,...

EPS: Executive Protection Specialist.??

Hadoop: es una estructura de software de código abierto para almacenar datos y ejecutar aplicaciones en clústeres de hardware comercial. Proporciona almacenamiento masivo para cualquier tipo de datos, enorme poder de procesamiento y la capacidad de procesar tareas o trabajos concurrentes virtualmente ilimitados.

HDFS: (Hadoop Distributed File System) es el componente principal del ecosistema Hadoop. Esta pieza hace posible almacenar data sets masivos con tipos de datos estructurados, semi-estructurados y no estructurados como imágenes, vídeo, datos de sensores, etc. Está optimizado para almacenar grandes cantidades de datos y mantener varias copias para garantizar una alta disponibilidad y la tolerancia a fallos.

IPS: “Intrusion Prevention System”, es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

IDS: “Intrusion Detection System”, es un programa de detección de accesos no autorizados a un computador o a una red.

IOC: “Indicator of Compromise”, es toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento. La intención de un IOC esquematizar la información que se recibe o se extrae durante el análisis de un incidente, de tal manera que pueda reutilizarse por otros investigadores o afectados, para descubrir la misma evidencia en sus sistemas y llegar a determinar si han sido o no comprometidos ya sea desde el punto de vista de monitorización frente a amenazas o por análisis forense.

Malware: es un término general para referirse a cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento.

Markdown: es un lenguaje de marcado ligero creado por John Gruber que trata de conseguir la máxima legibilidad y facilidad de publicación tanto en su forma de entrada como de salida, inspirándose en muchas convenciones existentes para marcar mensajes de correo electrónico usando texto plano.

ML: “Machine Learning” es el subcampo de las ciencias de la computación y una rama de la inteligencia artificial, cuyo objetivo es desarrollar técnicas que permitan que las computadoras *aprendan.*

MSSP: “Managed Security Service Provider” Los servicios MSSP de gestión de dispositivos de seguridad comprenden tanto la implantación como la configuración y mantenimiento de los mismos, operando sobre ellos en base al alcance establecido.

NTA: “Network Traffic Analysis”, es el proceso de registrar, revisar y analizar el tráfico de la red con el propósito conocer el rendimiento, seguridad y/o operaciones y administración generales de la red.

Playbooks: de respuesta ante incidentes. Todas las organizaciones tienen planes para diferentes incidentes que podrían afectar la resistencia del negocio a ellos si no están preparados. El propósito de un playbook es proporcionar a todos los miembros de una organización una clara comprensión de sus responsabilidades respecto de las normas de ciberseguridad y las prácticas aceptadas antes, durante y después de un incidente de seguridad. Por lo tanto, son líneas de acción que, teniendo como base un protocolo establecido, pueden mejorar las acciones y los tiempos de respuestas antes los incidentes.

SaaS: “Software as a Service”, es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente.

Sandbox: entorno de pruebas separado del entorno de producción.

SecOps: “Security -seguridad- y Operations -operaciones-“, es una colaboración entre los equipos de operaciones y seguridad de TI que integra herramientas, procesos y tecnología para mantener la seguridad de una empresa mientras se reduce el riesgo.

SIEM:” Security Information and Event Management”. Es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales.

SMP: “Security Management Program”, es un programa de gerencia en seguridad, riesgo y cumplimiento con una consola de administración. SMP elimina la complejidad del proceso de seguridad utilizando los controles ISO y el modelo planear, hacer, verificar y actuar (PHVA).

SOC: “Security Operation Center” Es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

SOAR: “Security Orchestration, Automation, and Response”, se refiere a una colección de soluciones y herramientas de software que permiten a las organizaciones optimizar las operaciones de seguridad en tres áreas clave: gestión de amenazas y vulnerabilidades, respuesta a incidentes y automatización de operaciones de seguridad.

SRM: Security Risk Management, es un proveedor líder de servicios de soluciones de seguridad, con un largo historial internacional de adoptar discretamente un enfoque preventivo para proteger los intereses de sus clientes.

TLP: Es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información. A través de este esquema, de una forma ágil y sencilla, el autor de una información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y este debe consultar al autor original cuando la información necesite ser distribuida a terceros.

UBA: “User Behavior Analytics”, Análisis de comportamiento.

UEBA: “User and Entity Behavior Analytics”, detección por comportamiento.

UTM: “Unified Threat Management”, dispositivo que permite la gestión unificada de amenazas

XDR: “Extended Detection and Response”. es una detección y respuesta en múltiples capas. XDR recopila y correlaciona automáticamente datos en múltiples capas de seguridad: emails, endpoints, servidores, workloads en la nube y redes, por lo que se puede detectar a las amenazas más rápido y los analistas de seguridad pueden mejorar los tiempos de respuesta e investigación.

8. Bibliografía

8.1 Libros consultados

- Tony Hsu. “Hands-On Security in DevOps”
  URL: https://www.oreilly.com/library/view/hands-on-security-in/9781788995504/
  Fecha de visita: 21/03/2021

8.2 Vídeos consultados

- YouTube. The SANS Cyber Defense Network Channel.
  Título: “Leveraging TheHive & Cortex for automated IR”
  URL: https://www.youtube.com/watch?v=K6K1fNpbf9w
  Fecha de visita: 25/04/2021
- YouTube. Canal: RandoriSec. Jérôme Leonard & Nabil Adouani. “Speed up IR with TheHive”
  URL:https://www.youtube.com/watch?v=lrYxdSAY8KY&list=PLy-SBx6KOB-efrrug9439Chopi5aFdWup
  Fecha de visita: 26/04/2021
- YouTube. Canal: The SANS Cyber Defense Network Channel. “Leveraging TheHive & Cortex for automated IR”
  URL: https://www.youtube.com/watch?v=K6K1fNpbf9w
  Fecha de visita: 01/05/2021
- YouTube. Canal: Amazon Web Services. “Threat Detection on AWS: An Introduction to Amazon GuardDuty (FND216)”
  URL: https://www.youtube.com/watch?v=czsuZXQvD8E
  Fecha de visita: 25/04/2021
- YouTube. Canal: Amazon Web Services. “Introduction to Amazon GuardDuty”
  URL: https://www.youtube.com/watch?v=ocZjGirQT9A
  Fecha de visita: 25/04/2021
- YouTube. Canal: The SANS Cyber Defense Network Channel “Leveraging TheHive & Cortex for automated IR”
  URL: https://www.youtube.com/watch?v=K6K1fNpbf9w
  Fecha de visita: 24/04/2021
- YouTube. Canal: Bsides Lisbon. “BSides Lisbon 2018: Cruising Ocean Threat With TheHive, Cortex & MISP Without Sinking - Saâd Kadhi”
  URL: https://www.youtube.com/watch?v=HMP1OcGkN4E
  Fecha de visita: 24/04/2021

8.3 Revistas consultadas

La Evolución del SIEM

- Juan Ramón Melara, Juan Ramón Melara, Arancha Asenjo, Bárbara Madariaga. IT Digital Security de octubre de 2018. "Orquestando la Seguridad"
  URL:https://www.itdigitalsecurity.es/whitepapers/content-download/fa60911a-dcc2-4e84-8c9c-8c634a5bb022/itds-12.pdf?s=web
  Fecha de visita: 16/03/2021

8.4 Páginas web consultadas

Análisis y monitoreo de seguridad.

- Artículo. "Intrusión Detection and Prevention Systems: An Updated Review"
  URL:https://www.researchgate.net/publication/336807986_Intrusion_Detection_and_Prevention_Systems_An_Updated_Review
  Fecha de visita: 06/03/2021
- Michael Swanagan. "The 3 Types Of Security Controls (Expert Explains)"
  URL: https://purplesec.us/security-controls/#Detective
  Fecha de visita: 06/03/2021
- Platin. "How ready is your organization for the SOAR Platform?"
  URL:https://www.platinbilisim.com.tr/EN/Media/Promotions/how-ready-is-your-organization-for-the-soar-platform
  Fecha de visita: 07/03/2021
- Artículo de investigación. "Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM"
  URL: https://revistascientificas.cuc.edu.co/ingecuc/article/view/225
  Fecha de visita: 09/03/2021

Análisis y monitoreo de seguridad. Herramientas y Plataformas de Supervisión de la Seguridad

- Derek Brink. "Security Monitoring and Analytics: From Tools to Platforms"
  URL:https://securityintelligence.com/security-monitoring-and-analytics-from-tools-to-platforms/
  Fecha de visita: 10/03/2021
- Europa Press. "Sistemas IDS, IPS y SIEM: qué son y por qué son importantes para la seguridad de la red de las empresas"
  URL:https://www.europapress.es/portaltic/ciberseguridad/noticia-sistemas-ids-ips-siem-son-son-importantes-seguridad-red-empresas-20200912113036.html
  Fecha de visita: 10/03/2021
- INCIBE. "Monitorizando redes y eventos en SCI: más información, más seguridad"
  URL:https://www.incibe-cert.es/blog/monitorizando-redes-y-eventos-sci-mas-

informacion-mas-seguridad
Fecha de visita: 11/03/2021

- INCIBE. ¿Qué son y para qué sirven los SIEM, IDS e IPS?
  URL: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
  Fecha de visita: 11/03/2021

Análisis y monitoreo de seguridad. Los SIEM en la actualidad

- Wikipedia. Splunk
  URL: https://es.wikipedia.org/wiki/Splunk
  Fecha de visita: 12/03/2021
- Rapid7. "Magic Quadrant for Security Information and Event Management"
  URL: https://www.rapid7.com/c/2020-siem-mq/
  Fecha de visita: 13/03/2021
- Gartner: "Improve IT Security With Vulnerability Management"
  URL: https://www.gartner.com/en/documents/480703
  Fecha de visita: 13/03/2021
- Gartner: "Gartner Magic Quadrant for Security Information and Event Management"
  URL:https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage
  Fecha de visita: 13/03/2021
- Forrester: "The Forrester Wave™: Security Analitics Platforms, Q4 2020"
  URL:https://www.bankinfosecurity.com/whitepapers/forrester-wave-security-analytics-platforms-q4-2020-w-7414
  Fecha de visita: 14/03/2021

Plataformas SOAR

- Rubén Ramiro. "Por qué las herramientas SOAR revitalizarán el ecosistema SIEM"
  URL:https://ciberseguridad.blog/por-que-las-herramientas-soar-revitalizaran-el-ecosistema-siem/
  Fecha de visita: 16/03/2021
- Jon Oltsik. "The rise of analyst-centric security operations technologies"
  URL:https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html
  Fecha de visita: 17/03/2021
- Jon Oltsik. "The evolution of security operations, automation and orchestration"
  URL:https://www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html
  Fecha de visita: 17/03/2021
- Gartner. "Market Guide for Security Orchestration, Automation and Response Solutions"
  URL: https://www.gartner.com/doc/reprints?id=1-24GXYQKN&ct=201027&st=sb%20
  Fecha de visita: 18/03/2021

- Trendmicro. “¿Qué es XDR?”
  URL: https://www.trendmicro.com/es_es/what-is/xdr.html
  Fecha de visita: 18/03/2021
- Amos Kingatua. “8 Best SOAR Solutions for Small to Enterprise Business”
  URL: https://geekflare.com/best-soar-tools/
  Fecha de visita: 19/3/2021
- IT Central Station. “Security Orchestration Automation and Response (SOAR)”
  URL:https://www.itcentralstation.com/categories/security-orchestration-automation-and-response-soar
  Fecha de visita: 20/03/2021
- ANLYZ. “What is SOAR Cyber Security and how can it improve detection?”
  URL: https://anlyz.co/soar-security#
  Fecha de visita: 21/03/2021
- Stan Engelbrecht. “The Evolution of SOAR Platforms”
  URL: https://www.securityweek.com/evolution-soar-platforms
  Fecha de visita: 22/03/2021
- Cynet.com. “Incident Response Platform: The Road to Automating IR”
  URL:https://www.cynet.com/incident-response-services/incident-response-platform-the-road-to-automating-ir/
  Fecha de visita: 23/03/2021
- Logsign. “Security Orchestration, Automation and Response (SOAR) Buyer’s Guide”
  URL: https://www.logsign.com/uploads/SOAR_Buyer_s_Guide_c91a5734e7.pdf
  Fecha de visita: 23/03/2021
- Anomali. “What is a Threat Intelligence Platform (TIP)?”
  URL: https://www.anomali.com/resources/what-is-a-tip
  Fecha de visita: 24/03/2021
- Wikipedia. “Threat Intelligence Platform”
  URL: https://en.wikipedia.org/wiki/Threat_Intelligence_Platform
  Fecha de visita: 25/03/2021
- Swinlane. “SOAR Report”
  URL: https://swimlane.com/resources/2020-soar-report-swimlane-cybersecurity-insiders
  Fecha de visita: 26/03/2021
- John M. Bell, Ph.D. and Stephen C. Cardot. “The Evolution of Cyber Security”
  URL: https://scardot.medium.com/the-evolution-of-cyber-security-be9fedc8f4c5
  Fecha de visita: 27/03/2021

Implementación de Plataformas SOAR

- Saâd Kadhi. Entrada en el blog TheHive Project. “Introducción de TheHive”
  URL: https://blog.thehive-project.org
  Fecha de visita: 15/04/2021

- Rubén Ramiro. “Un trío perfecto con TheHive, Cortex y MISP”
  URL: https://ciberseguridad.blog/un-trio-perfecto-con-thehive-cortex-y-misp/
  Fecha de visita: 18/04/2021
- Sothis. “Security Made In LU: The Hive Project Workshop”
  URL: https://www.sothis.tech/security-made-in-lu-the-hive-project-workshop/
  Fecha de visita: 01/05/2021
- Nabil Adouani. Blog de “TheHive Project”
  URL: https://blog.thehive-project.org/
  Fecha de visita: 19/04/2021
- Zachary Burnham. “Installing TheHive – a Security IR Platform”
  URL:https://burnhamforensics.com/2018/12/17/installing-thehive-a-security-ir-platform/
  Fecha de visita: 21/04/2021
- MISP Team. “Features of MISP, the open source threat sharing platform”
  URL: https://www.misp-project.org/features.html
  Fecha de visita: 20/04/2021
- TheHive Team. Repositorio de Github “TheHive-Project/Cortex”
  URL: https://github.com/TheHive-Project/Cortex#analyzers
  Fecha de visita: 20/04/2021
- TheHive Team. Repositorio de Github “TheHive-Project/CortexDocs”
  URL: https://github.com/TheHive-Project/CortexDocs
  Fecha de visita: 20/04/2021
- Amazon Team. “Amazon GuardDuty”
  URL: https://aws.amazon.com/es/guardduty/
  Fecha de visita: 20/04/2021
- Microsoft. “¿Qué es Azure Sentinel?”
  URL: https://docs.microsoft.com/es-es/azure/sentinel/overview
  Fecha de visita: 21/04/2021
- Google. “Google Scale Threat Detection”
  URL: https://chronicle.security/
  Fecha de visita: 21/04/2021
- BBVA. “BBVA y Google Cloud establecen una alianza para promover la innovación en la seguridad de los servicios financieros”
  URL:https://www.bbva.com/es/bbva-y-google-cloud-establecen-una-alianza-para-promover-la-innovacion-en-la-seguridad-de-los-servicios-financieros/
  Fecha de visita: 21/04/2021
- TheHive. “Installation & configuration guides”
  URL:https://docs.thehive-project.org/thehive/installation-and-configuration/installation/step-by-step-guide/
  Fecha de visita: 21/04/2021

- Github. “TheHiveDocs/training-material.md”
  URL:https://github.com/TheHive-Project/TheHiveDocs/blob/master/training-material.md
  Fecha de visita: 20/05/2021
- Adrian. “Integrate TheHive and Cortex”
  URL: https://blog.agood.cloud/posts/2019/09/27/integrate-thehive-and-cortex/#
  Fecha de visita: 20/05/2021
- Tom. “IR using the Hive Project”
  URL: https://isc.sans.edu/forums/diary/IR+using+the+Hive+Project/23099/
  Fecha de visita: 21/05/2021
- Chris Sanders. “Investigation Case Management with TheHive”
  URL: https://chrissanders.org/2017/03/case-management-the-hive/
  Fecha de visita: 22/05/2021
- Ibrahim Ayadhi. “Case management”
  URL: https://medium.com/@ibrahim.ayadhi
  Fecha de visita: 23/05/2021
- Sothis. “Security Made In LU: The Hive Project Workshop”
  URL: https://www.sothis.tech/security-made-in-lu-the-hive-project-workshop/
  Fecha de visita: 23/05/2021
- Tom Asselman. “Creating Responders in The Hive”
  URL: https://blog.nviso.eu/2020/01/13/creating-responders-in-the-hive/
  Fecha de visita: 23/05/2021
- Blue Teams Academy. “How to Install and use The Hive Project in Incident Management”
  URL: https://www.blueteamsacademy.com/hive/
  Fecha de visita: 29/05/2021
- Christian Van Heurck. “Orchestation of CSIRT Tools”
  URL: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-training-modules-and-tb.pdf
  Fecha de visita: 29/05/2021
- Github. “How to Write and Submit an Analyzer”
  URL:https://github.com/TheHive-Project/CortexDocs/blob/master/api/how-to-create-an-analyzer.md
  Fecha de visita: 30/05/2021
- Anthony Miracle. “Handling Incidents as Bees in TheHive”
  URL:https://events.educause.edu/special-topic-events/security-professionals-conference/2019/agenda/handling-incidents-as-bees-in-thehive
  Fecha de visita: 31/05/2021

- AWS. “What is Amazon GuardDuty?”
  URL:https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-ug.pdf#what-is-guardduty
  Fecha de visita: 08/05/2021
- AWS. “Getting started with GuardDuty”
  URL: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_settingup.html
  Fecha de visita: 08/05/2021
- AWS. “Getting Hands on with Amazon GuardDuty”
  URL: https://hands-on-guardduty.awssecworkshops.com/
  Fecha de visita: 09/05/2021
- Greg McConnel (AWS Solution Arquitect). “GuardDuty Hands-on Lab”
  URL: https://es.slideshare.net/AmazonWebServices/guardduty-handson-lab
  Fecha de visita: 10/05/2021
- Alex Tomic (AWS Solution Arquitect). “Automate Threat Mitigation Using AWS WAF and Amazon GuardDuty”
  URL:https://pages.awscloud.com/rs/112-TZM-766/images/2018_0814-SID_Slide-Deck.pdf?mkt_tok
  Fecha de visita: 11/05/2021

Anexo A. Usando TheHive Proyect

Para la prueba de concepto con hemos utilizado una máquina virtual creada por el Proyecto TheHive y preconfigurada para entrenamiento que incluye TheHive y Cortex[36].

Cuentas y credenciales de la VM			
Tipo de acceso	**Módulo**	**Usuario**	**contraseña**
Training VM system account (ssh)	TheHive	thehive	thehive1234
TheHive Admin account	TheHive	admin	thehive1234
Cortex superAdmin account	Cortex	admin	thehive1234
Cortex "training" Org admin account	Cortex	thehive	thehive1234

El módulo Cortex tiene preinstalada una de organización de entrenamiento con una cuenta con usuario: thehive contraseña: thehive1234. Esta cuenta tiene privilegios de lectura / análisis / orgAdmin y TheHive ya está configurada para usar el servicio Cortex con su API.

TheHive y Cortex están configurados e integrados en la misma VM aunque tiene pocos analizadores habilitados en la VM de entrenamiento:

- Buscador de abuso,
- CyberCrime-Tracker,
- DShield_lookup,
- File_Info, EMLParser,
- Fortiguard_URLCategory,
- MaxMind GeoIP,
- UnshortenLink,
- TalosReputación,
- _URLHaus,
- Urlscan_io_Search.

Las plantillas de informes están preinstaladas.

Comenzamos desplegando la VM y desde la pantalla de login nos aparece la forma de acceder a los módulos vía web.

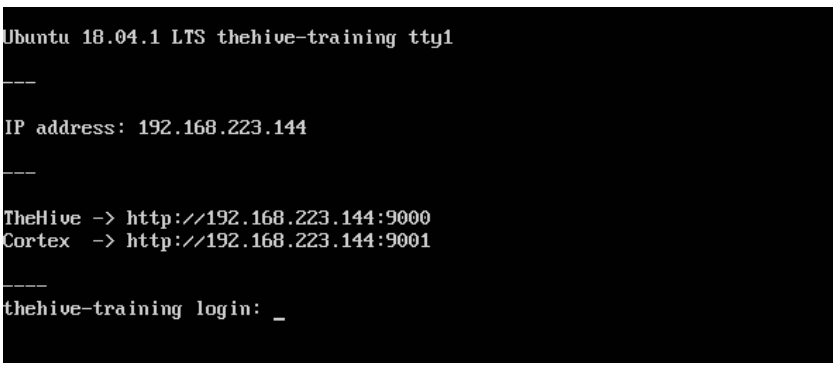


Ilustración 54. Pantalla inicial de la Training VM de TheHive

[36] *https://github.com/TheHive-Project/TheHiveDocs/blob/master/training-material.md*

Probamos que podemos acceder a TheHive con usuario: admin y contraseña: thehive1234.

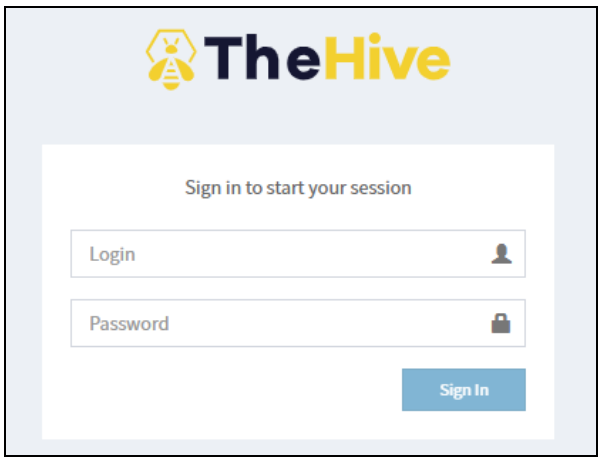


Ilustración 55. Pantalla de login de TheHive

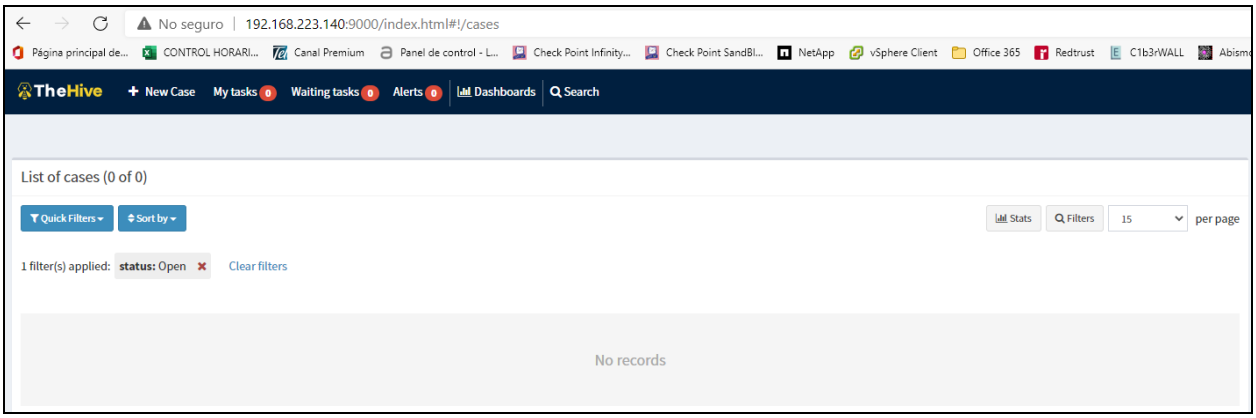


Ilustración 56. Pantalla inicial de TheHive

Comencemos a explorar cómo usar TheHive, para ello vamos al apartado **Admin** → **Users** y elegimos **Add User** y añadimos el usuario PruebasTFM.

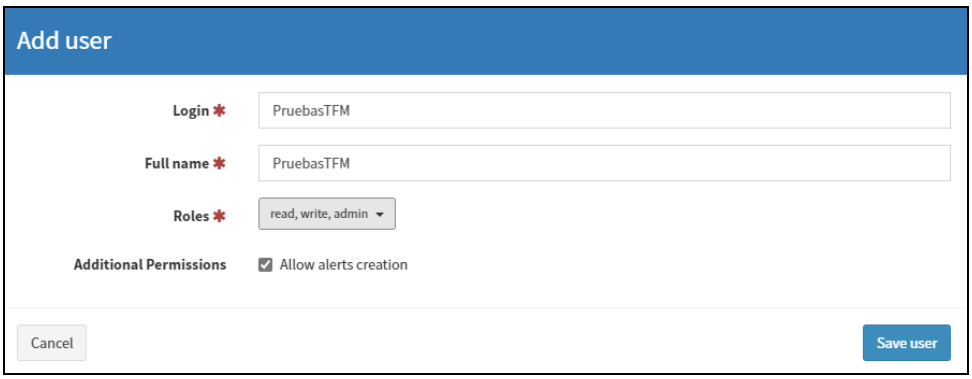


Ilustración 57. Pantalla de añadir usuario en TheHive

Ilustración 58. Listado de usuarios en TheHive

Creamos una contraseña al usuario **pruebastfm** y añadimos un caso eligiendo del menú principal "**New Case**".

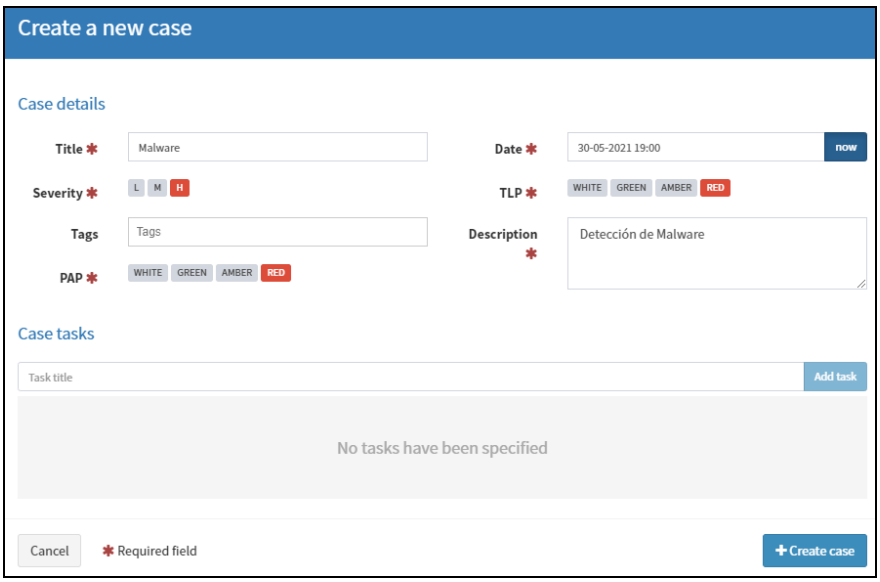


Ilustración 59. Detalle de un caso en TheHive

Una vez creado el caso veremos el listado de casos creados en TheHive.

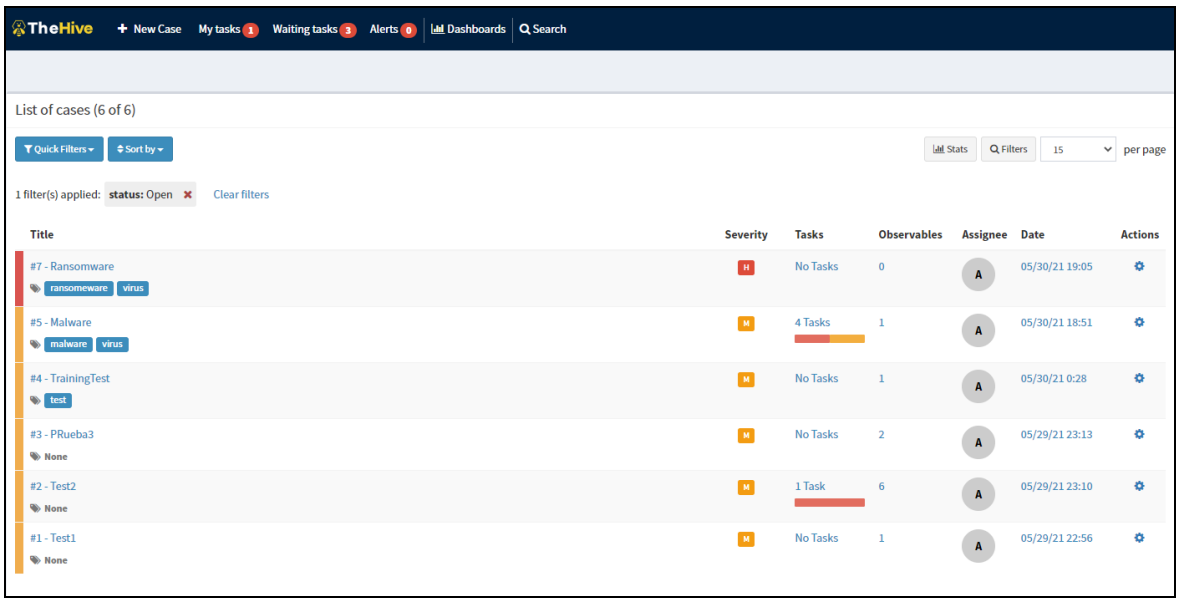


Ilustración 60. Listado de casos en TheHive

Si lo seleccionamos, podemos ver las diferentes acciones que podemos realizar sobre él, que son: cerrarlo, marcarlo, fusionarlo con otro caso relacionado, borrarlo o aplicarle **Responders** como acción de remediación.

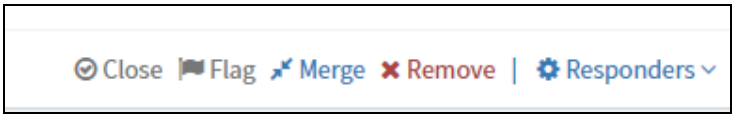


Ilustración 61. Acciones sobre un caso en TheHive

De un caso, podemos ver las Tasks (tareas) y si han sido comenzadas o no.

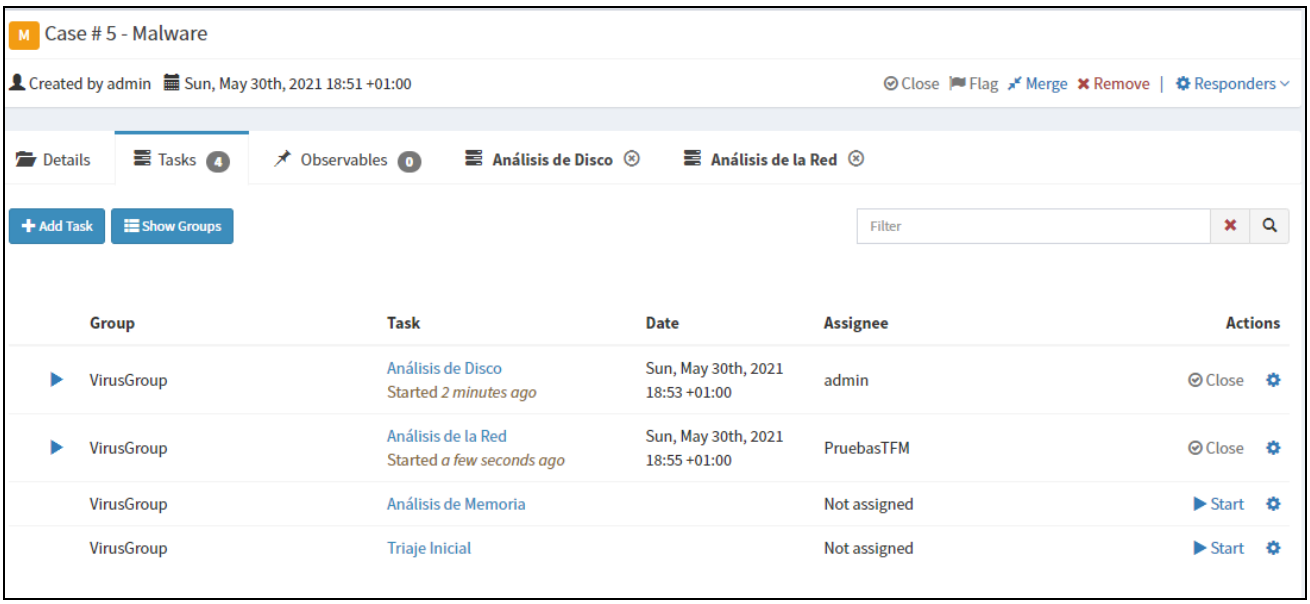


Ilustración 62. Detalle de tareas de un caso en TheHive

Y los observables.

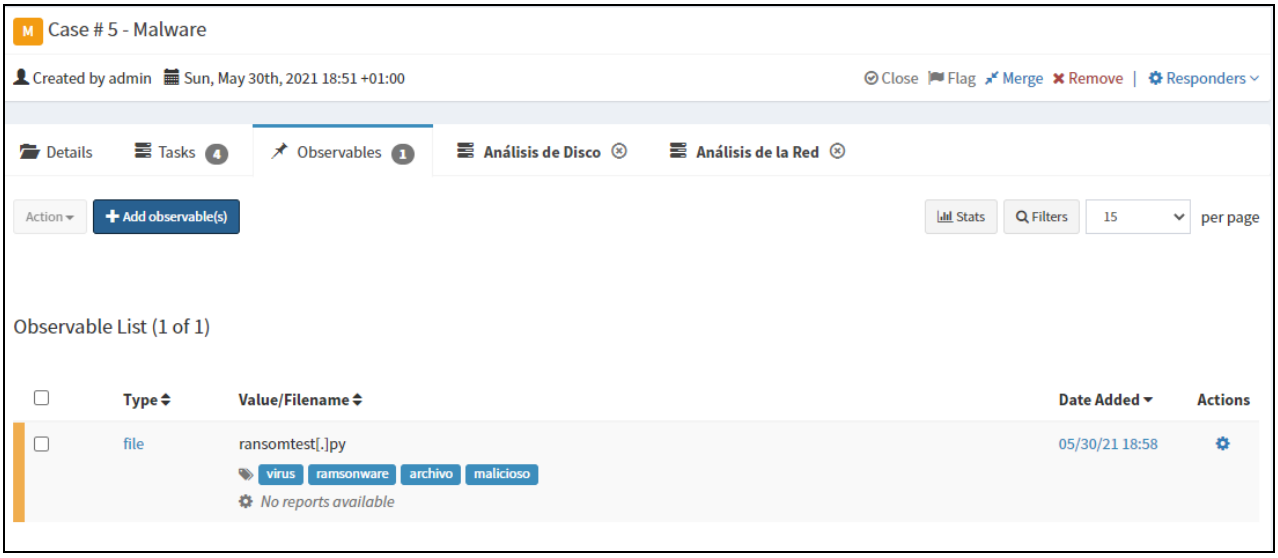


Ilustración 63. Observables de un caso en TheHive

En la barra principal podemos ver los diferentes indicadores. Ya que TheHive está diseñado para un trabajo de equipo, los miembros podrán ver las tareas que tiene asignadas y aquellas que están pendientes, así como Alertas y los diferentes Dashboards de la aplicación.

Ilustración 64. Indicadores en TheHive

En la parte derecha de la pantalla veremos el histórico de eventos registrados en TheHive.

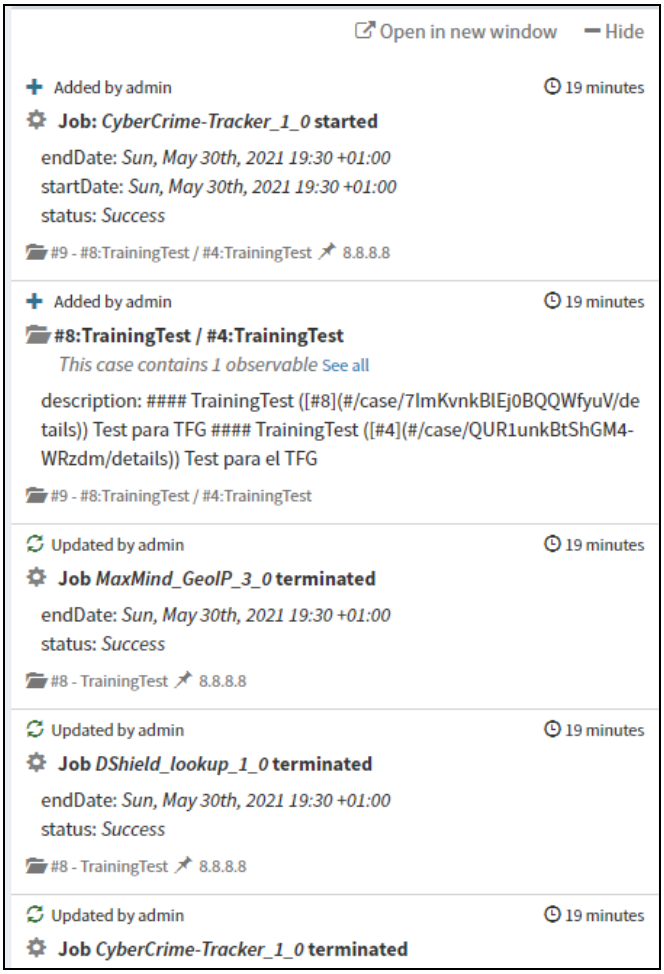


Ilustración 65. Histórico de acciones en TheHive

El otro componente principal del Proyecto TheHive es Cortex, al cuál entraremos vía web con el usuario admin y contraseña: thehive1234.

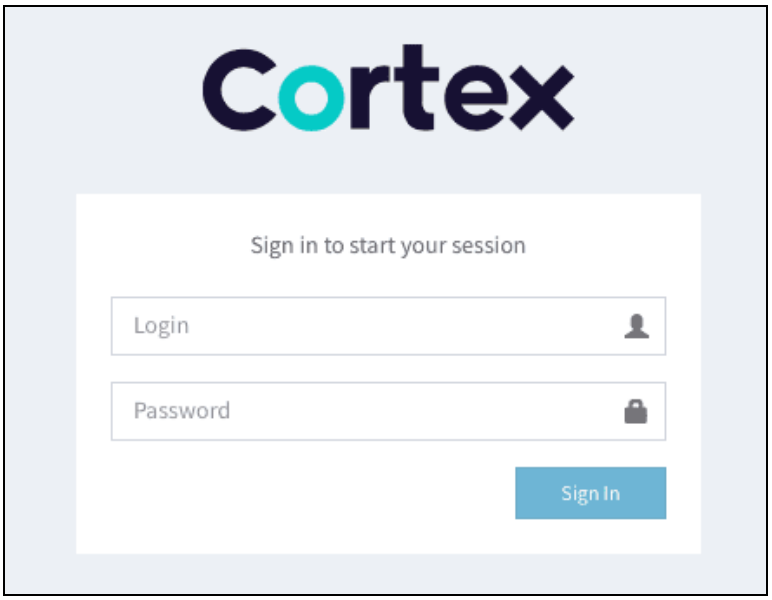


Ilustración 66. Pantalla de login de Cortex

Cortex intenta resolver un problema común que encuentran con frecuencia los SOC, los CSIRT y los investigadores de seguridad en el curso de inteligencia de amenazas, análisis forense digital y respuesta a incidentes: ¿cómo analizar los observables que han recopilado, a escala, consultando una sola herramienta en lugar de varias? Para ello Cortex cuenta con dos componentes que están en constante crecimiento, los Analyzers y los Responders.

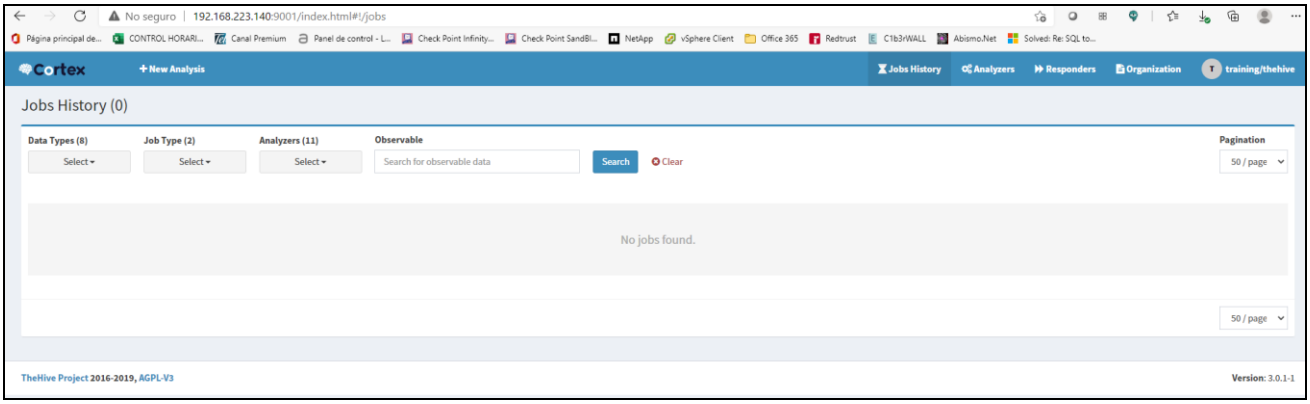


Ilustración 67. Pantalla inicial de Cortex, historial de tareas

La configuración de Analyzers y Responders se realiza en el apartado **Organization** de Cortex la mayoría utilizan API Keys de conexión entre servicios y es posible habilitar certificados.

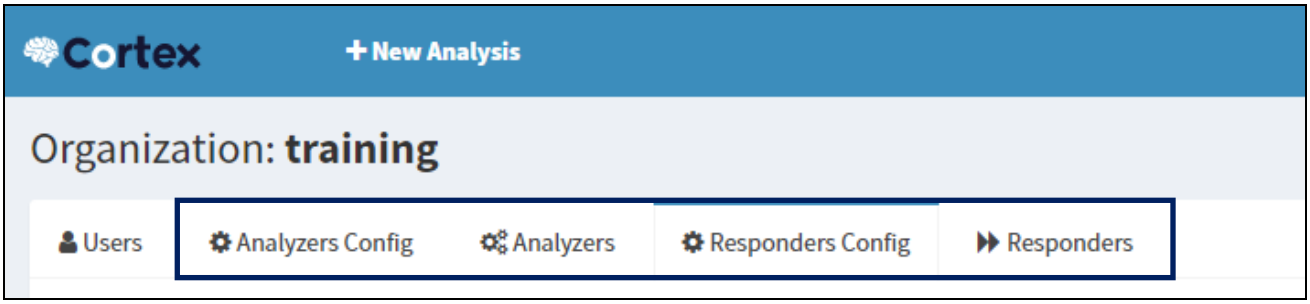


Ilustración 68. Analyzers y Responders en Cortex

Analyzers

Un analizador es un programa que toma un observable e información de configuración como entrada sin procesar, analiza el observable y produce un resultado como salida sin procesar. Está compuesto por al menos dos de estos tipos de archivos:

- El programa en sí, la mayoría están escritos en Phyton, pero se puede escribir en Ruby, Perl o incluso Scala.
- Uno o varios archivos de interacción de servicios o sabores.
- Un archivo de requisitos en Python, el cual sólo es necesario si el analizador está escrito en Python.

TheHive va incrementando la cantidad de Analyzers con la ayuda de la comunidad y proveedores de soluciones. Los Analyzers deben ser configurados y normalmente requieren el uso de API del servicio que queramos ejecutar. Pongamos de ejemplo la configuración del Analizer de VirusTotal.

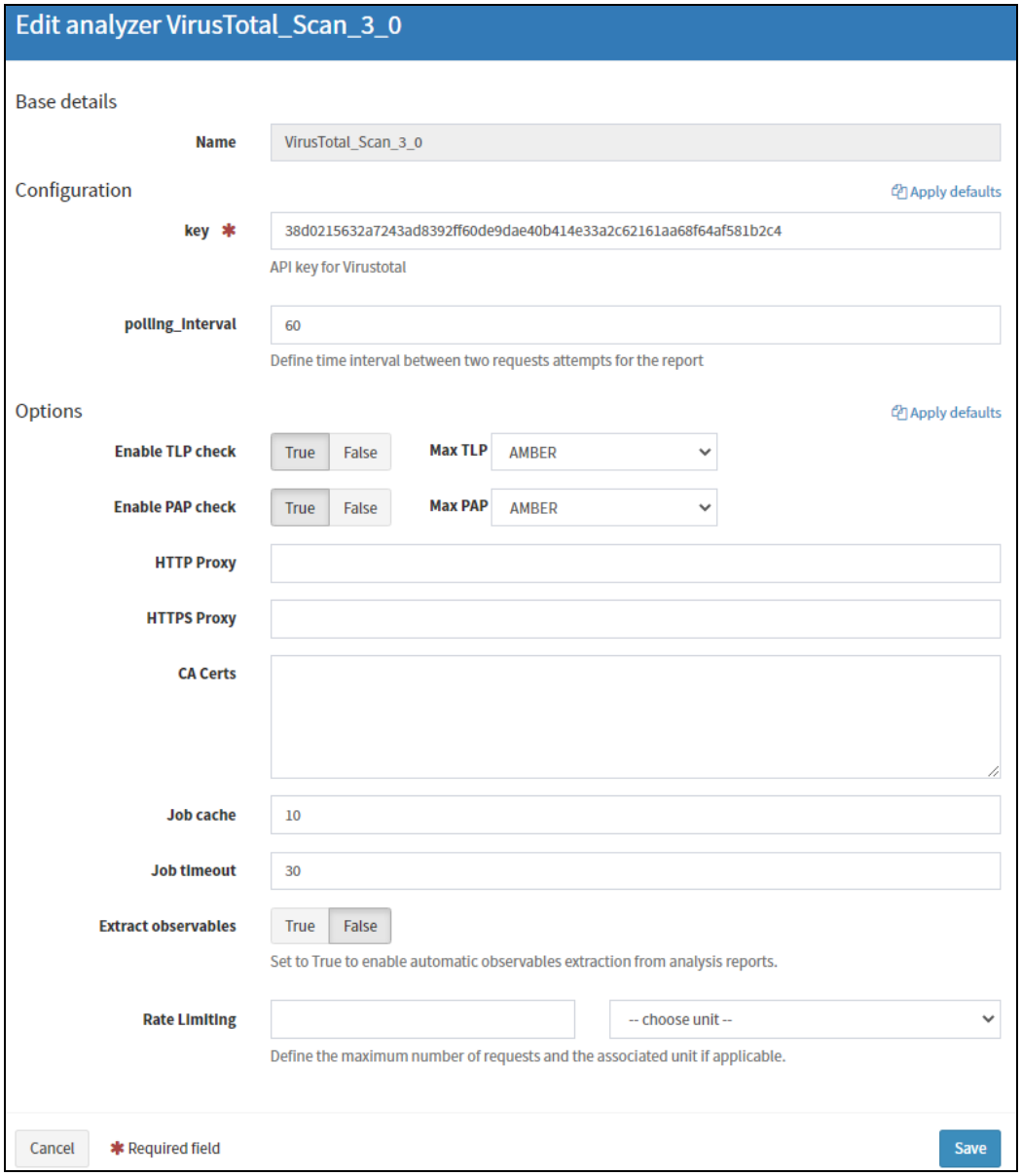


Ilustración 69. Analyzer VirusTotal_Scan

Responders

Los responders se realizarán acciones a realizar para remediar el incidente. Es posible crear nuestros propios Responders. Los creadores de TheHive proporcionan información sobre la creación de ellos, aunque todavía algunas cosas quedan indocumentadas, y algunos escollos no se mencionan.

Para que su Responder funcione, al menos tendría que proporcionar dos archivos:

- Un archivo de configuración JSON.
- Un archivo de Python con el propio código, también es compatible con Perl, Ruby y Scala.

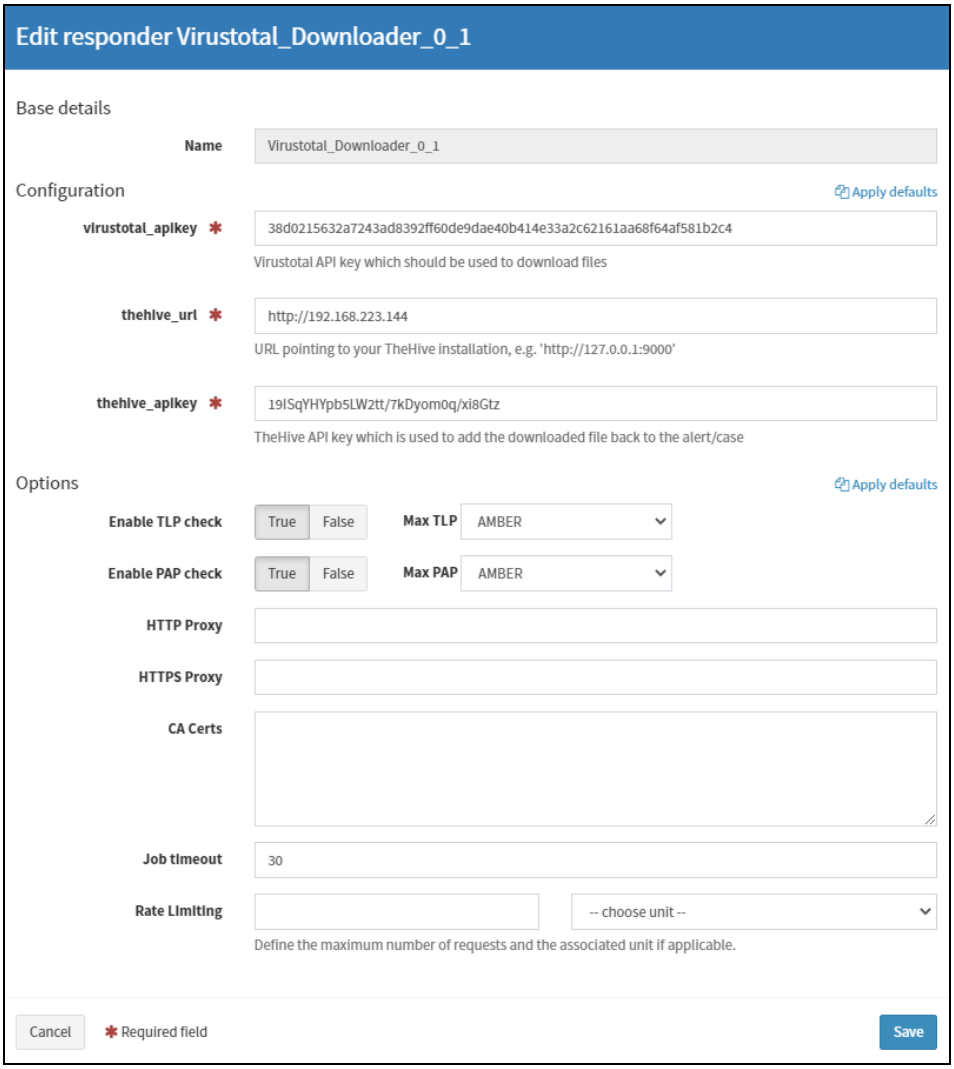


Ilustración 70. Responder VirusTotal_Downloader

Un ejemplo de Investigación y remediación con TheHive podría consistir en la investigación de un posible phishing.

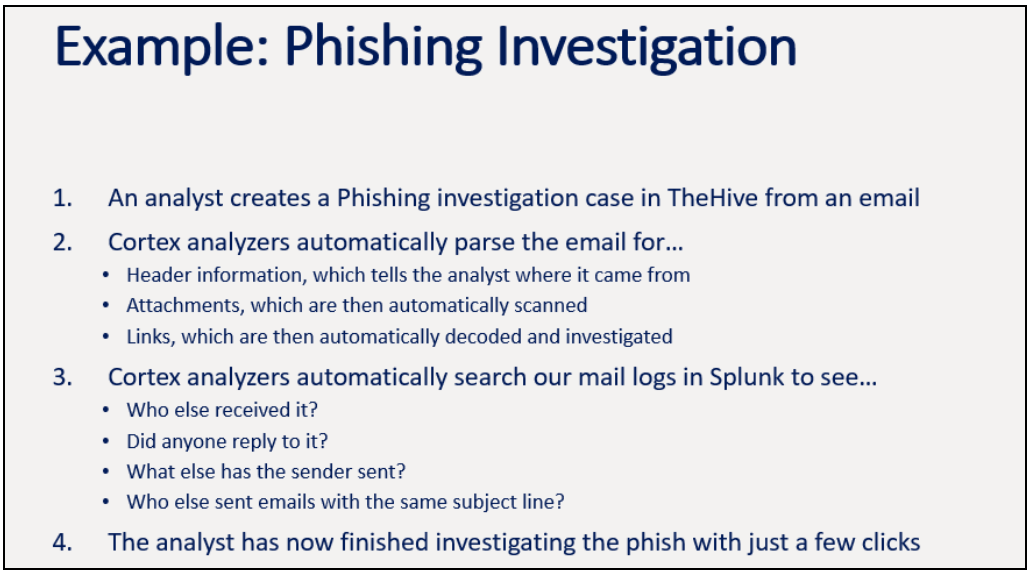


Ilustración 71. Ejemplo de Investigación en TheHive

Una vez finalizada la investigación el analista puede utilizar los Responders de Cortex para facilitar la remediación.

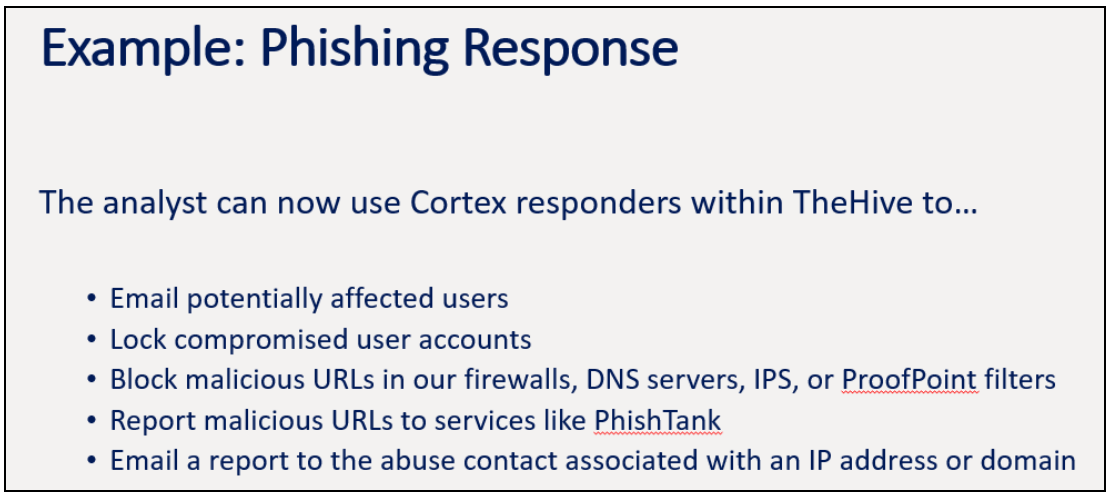


Ilustración 72. Remediación con TheHive

Anexo B. Usando Amazon GuardDuty

Hemos elegido AWS como nube pública con servicios SOAR, ya que es una de las plataformas líderes en la actualidad y además en su Marketplace permite integración con la mayoría de las plataformas propietarias que hemos visto en este documento: Splunk, QRadar, Rapid7, Cortex, XCortex, Fortinet, etc.

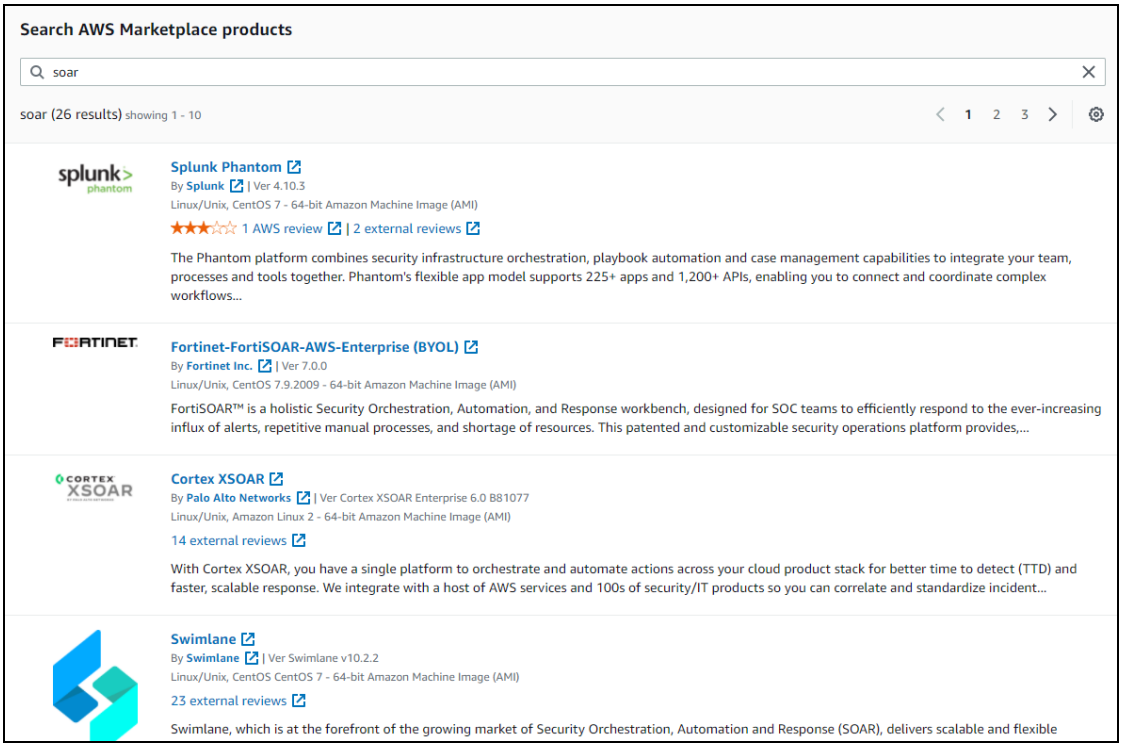


Ilustración 73. AWS Marketplace para integración con otros SOAR

Para realizar dicha prueba nos creamos una cuenta en AWS. https://aws.amazon.com/es/.

AWS es una plataforma con una gran cantidad de servicios. Los servicios de AWS que utilizaremos son:

- **CloudWatch**: es un servicio de monitorización y observación que recopila datos de monitorización y operaciones en formato de registros, métricas y eventos, lo cual ofrece una vista unificada de los recursos, las aplicaciones y los servicios de AWS que se ejecutan en servidores locales y de AWS. Se puede usar CloudWatch para detectar comportamientos anómalos en sus entornos, definir alarmas, comparar registros y métricas, realizar acciones automatizadas, resolver problemas y descubrir información para mantener las aplicaciones en ejecución sin problemas.
- **EC2**: es un servicio web que proporciona capacidad informática en la nube segura y de tamaño modificable.
- **CloudFormation**: ofrece una forma sencilla de modelar un conjunto de recursos relacionados de AWS y de terceros, aprovisionarlos de manera rápida y consistente y administrarlos a lo largo de sus ciclos de vida tratando la infraestructura como un

código. La plantilla de CloudFormation describe los recursos que desea y sus dependencias para que los pueda lanzar y configurar juntos como una pila.

- **Lambda**: es un servicio informático sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores, crear una lógica de escalado de clústeres basada en la carga de trabajo, mantener integraciones de eventos o administrar tiempos de ejecución. Con Lambda se puede ejecutar código para casi cualquier tipo de aplicación o servicio backend sin tener que realizar tareas de administración. Simplemente cargue su código como un archivo ZIP o una imagen de contenedor y Lambda asigna de manera automática y precisa la potencia de ejecución de cómputo y ejecuta el código en función de la solicitud o el evento entrante para cualquier escala de tráfico. Configure el código para que se active automáticamente desde 140 servicios de AWS o llámelo directamente desde cualquier aplicación web o móvil. Puede escribir funciones de Lambda en su lenguaje favorito (Node.js, Python, Go, Java y más) y utilizar herramientas de contenedor y sin servidor, como AWS SAM o la CLI de Docker, para compilar, probar e implementar las funciones.
- **VPC**. (Virtual Private Cloud) es un servicio que permite lanzar recursos de AWS en una red virtual aislada de forma lógica que usted defina. Puede controlar todos los aspectos del entorno de red virtual, como la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y gateways de red.
- **WAF**. es un firewall para aplicaciones web que ayuda a proteger sus aplicaciones web o API contra ataques web y bots comunes que pueden afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos.
- **EventBridge**. es un bus de eventos sin servidor que facilita la creación de aplicaciones basadas en eventos a escala a través de eventos generados por sus aplicaciones. EventBridge distribuye un flujo de datos generados en tiempo real a partir de orígenes de eventos.

Y una vez realizada la verificación de usuario y cuenta bancaria y dentro de nuestra cuenta de AWS, buscamos el servicio GuardDuty.

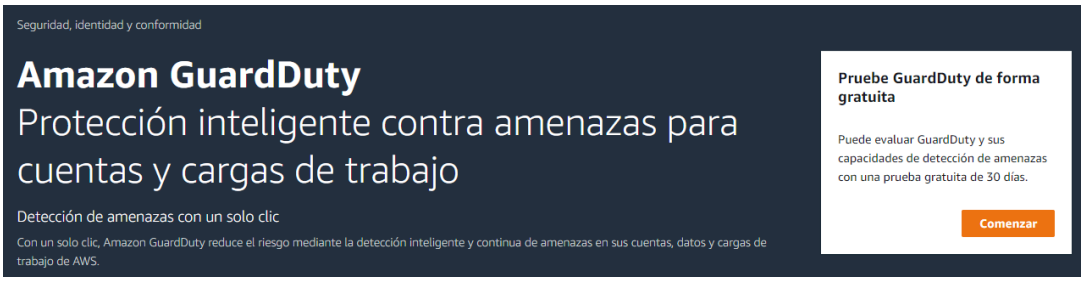


Ilustración 74. Prueba gratuita de 30 días GuardDuty

Habilitar GuardDuty es extremadamente sencillo basta con:

- Abrir la consola de GuardDuty en https://console.aws.amazon.com/guardduty/.
- Elegimos **Comenzar.**
- Y finalmente seleccionamos **Activar GuardDuty.**

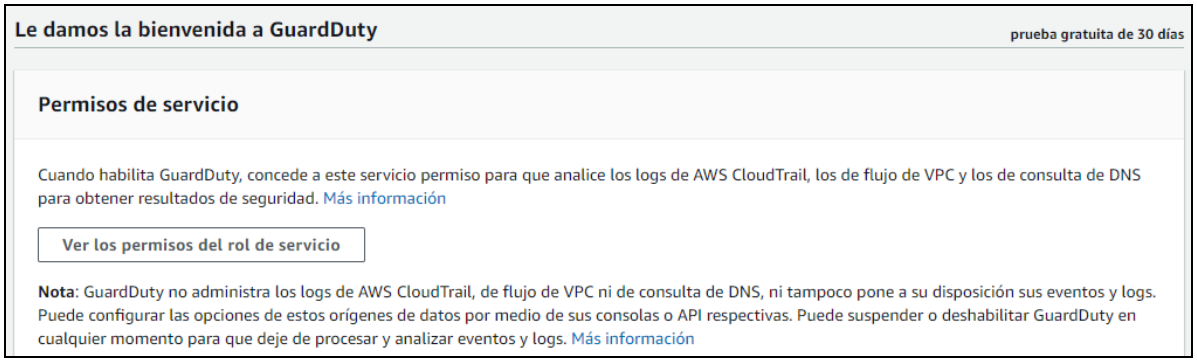


Ilustración 75. Asistente AWS de GuardDuty

Desde el momento en que habilitamos GuardDuty, comienza a analizar todos los registros de flujo de VPC (Amazon Virtual Private Cloud) , registros de CloudTrail y registros de DNS en esa región. Los registros de DNS se generan a partir de los resolutores de DNS predeterminados de AWS que se utilizan para sus VPC y no son una fuente de datos disponible para los clientes.

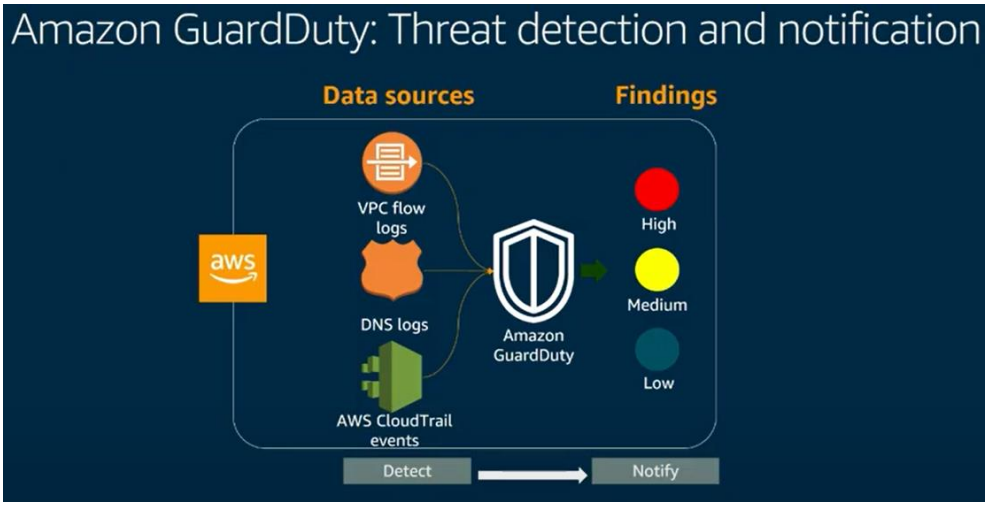


Ilustración 76. GuardDuty Detección de Amenazas y notificación

GuardDuty accede a todas estas fuentes de datos sin que ninguna de ellas tenga que estar habilitada; aunque es una práctica recomendada habilitar CloudTrail y VPC Flow Logs para su propio análisis. GuardDuty es un servicio regional, por lo que para que el servicio pueda monitorizar estas fuentes de datos en otras regiones, deberá habilitarse en cada una.

Cuando GuardDuty descubre un problema de seguridad, genera un **hallazgo**. Un hallazgo de GuardDuty es un conjunto de datos que contiene detalles relacionados con ese problema de seguridad único. Los detalles del hallazgo se pueden utilizar para ayudarnos a investigar el problema.

GuardDuty admite la generación de resultados de muestra con valores de marcador de posición, que se pueden usar para probar GuardDuty. Conviene familiarizarse con los hallazgos antes de tener que responder a un problema real.

Para crear resultados de muestra:

1. En el panel de navegación, elija **Configuración**.
2. En la página **Configuración**, en **Resultados de muestra**, elija **Generar resultados de muestra**.

3. En el panel de navegación, elija **Hallazgos**. Los resultados de muestra se muestran en los resultados clasificados por gravedad (alta, media o baja).

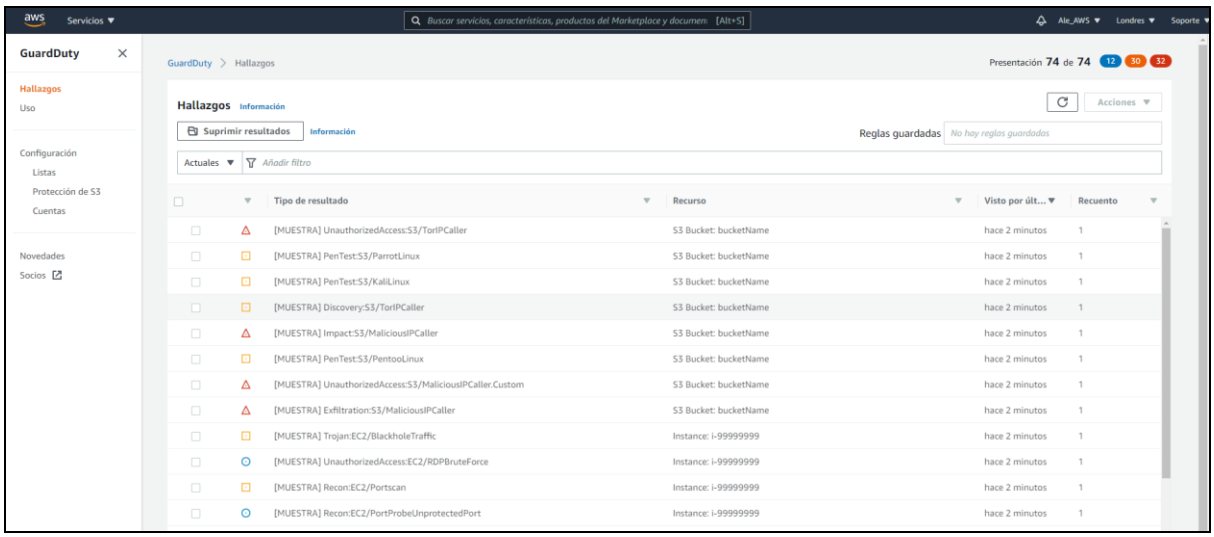


Ilustración 77. Resultados de muestra AWS

A continuación, vemos una tabla explicativa de los niveles de gravedad (IoC) de GuardDuty:

Nivel Gravedad		Explicación
⚠	Alto	indica que el recurso en cuestión (una instancia EC2 o un conjunto de credenciales de usuario de IAM) está comprometido y se está utilizando activamente para fines no autorizados
▣	Medio	indica una actividad sospechosa que se desvía del comportamiento normalmente observado y, según su caso de uso, puede ser indicativo de un compromiso de recursos
⊙	Bajo	indica un intento de actividad sospechosa que no comprometió su red, por ejemplo, un escaneo de puertos o un intento de intrusión fallido.

Ilustración 78. Niveles de gravedad

Al seleccionar un hallazgo podemos ver los diferentes campos de información en el panel de detalles del hallazgo. Diferentes tipos de hallazgos pueden tener diferentes campos de información.

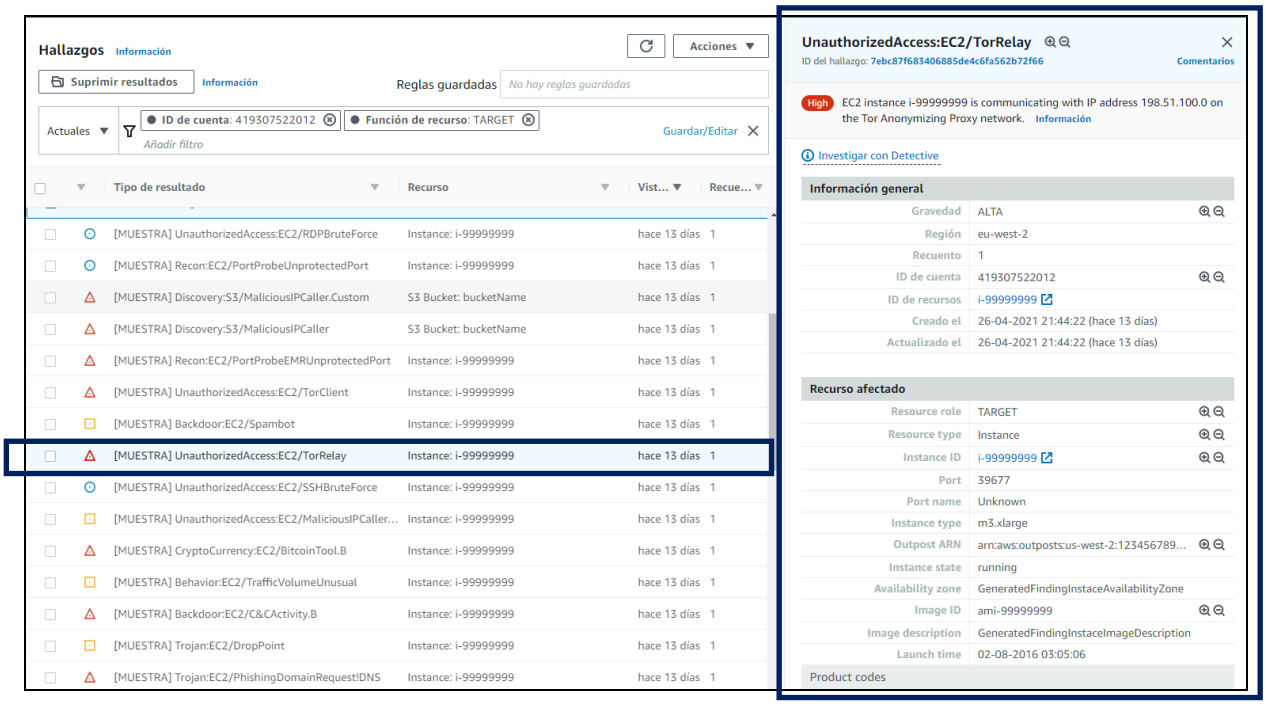


Ilustración 79. GuardDuty, detalle de un hallazgo

Podemos ver más información sobre el hallazgo y recomendaciones de remediación. En la parte superior del detalle de hallazgo encontramos el **ID del hallazgo** donde podemos ver el JSON completo del hallazgo con información adicional no incluida en la vista de la consola, dicho JSON puede ser utilizado por otras herramientas y servicios.

En la sección Recurso afectado podremos identificar el recurso de la cuenta que debe ser investigado y se incluye un enlace la consola de AWS correspondiente donde se encuentra dicho recurso.

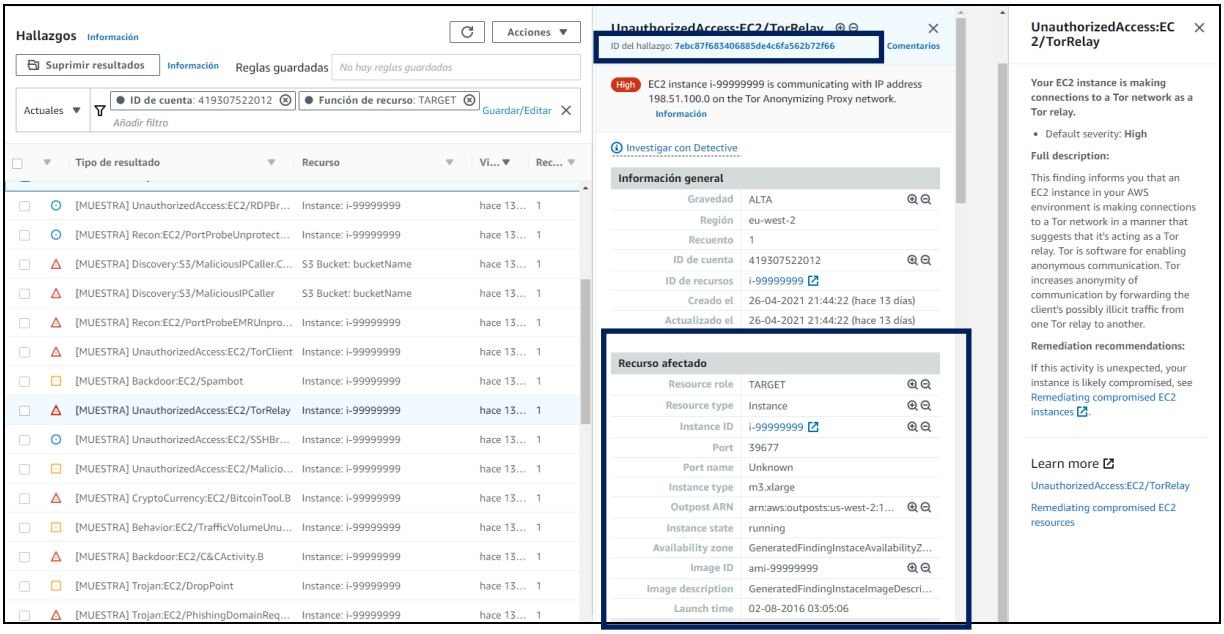


Ilustración 80. GuardDuty, detalle adicional de un hallazgo

Para archivar los resultados de un hallazgo los marcamos y en **Acciones** elegimos **Archivado**. GuardDuty recomienda la configuración de exportación de hallazgos en un bucket S3 con clave KMS de cifrado, si no se archivan los hallazgos, estos desaparecerán a los 90 días del panel de hallazgos.

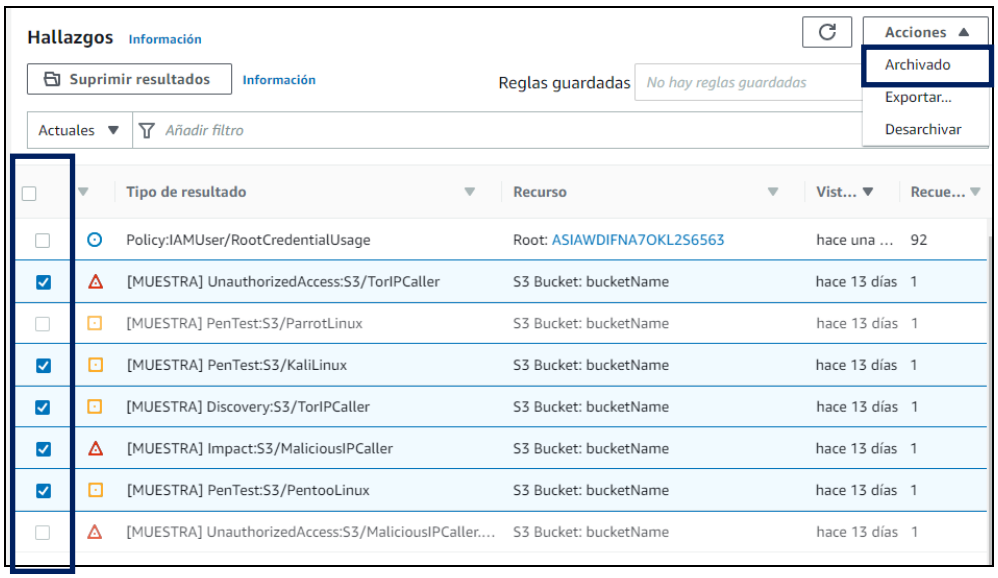


Ilustración 81. GuardDuty, archivado de hallazgos

Otro de los pasos a configurar en GuardDuty son las alertas de hallazgos a través de SNS (Simple Notification Service), ya que GuardDuty se integran con Amazon EventBridge, el cual lo podemos utilizar para automatizar respuestas a nuestros hallazgos conectando los eventos de hallazgos a destinos como funciones de AWS Lambda, Amazon EC2 System Manager Automation, Amazon Simple Notificacion Service (SNS) y más.

Para crear un SNS para los hallagos hacemos lo siguiente:

1. Vamos a la consola https://console.aws.amazon.com/sns/v3/home.
2. Seleccionamos **Temas** del panel de navegación y creamos un tema estándar.

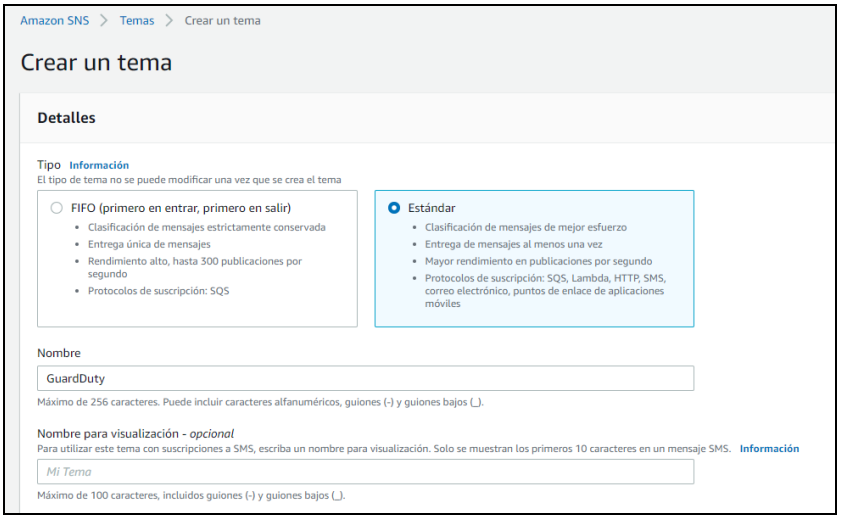


Ilustración 82. GuardDuty, Creación de Tema para SNS

3. Luego creamos una suscripción con el ARN del Tema creado en el paso anterior, como protocolo elegimos Correo electrónico y en punto de enlace ponemos la cuenta de correo donde queremos recibir las notificaciones.

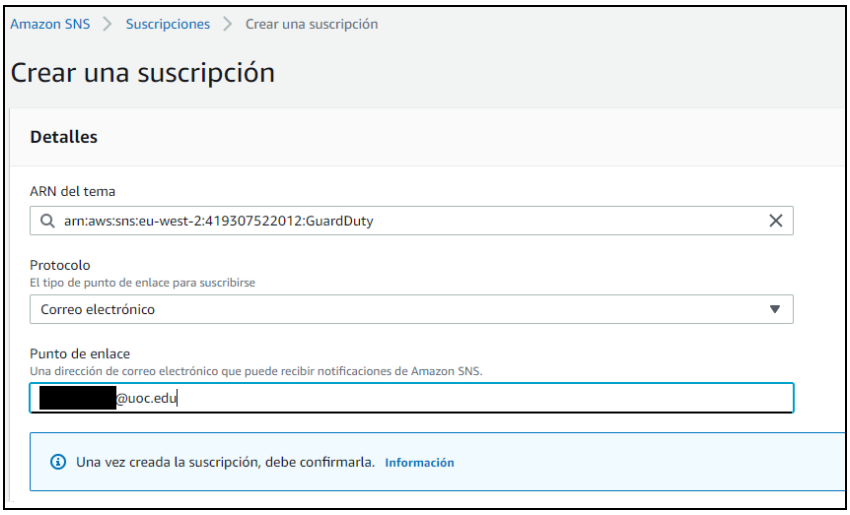


Ilustración 83. GuardDuty, crear suscripción para SNS

Dicha suscripción debemos confirmarla seleccionando **Confirm subscription** en el enlace que contendrá el correo que recibiremos en el buzón de la cuenta que hemos configurado como Punto de enlace.

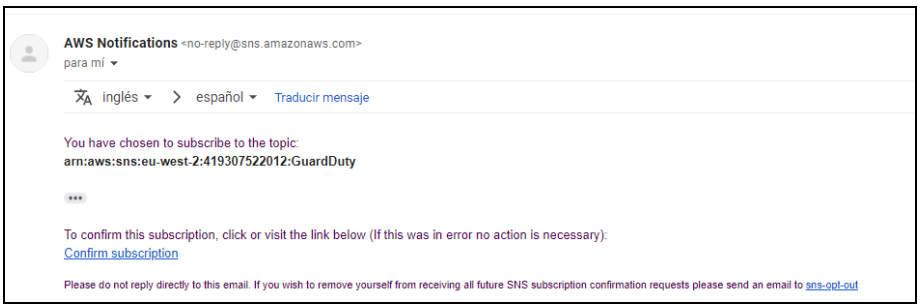


Ilustración 84. GuardDuty, mensaje suscripción SNS

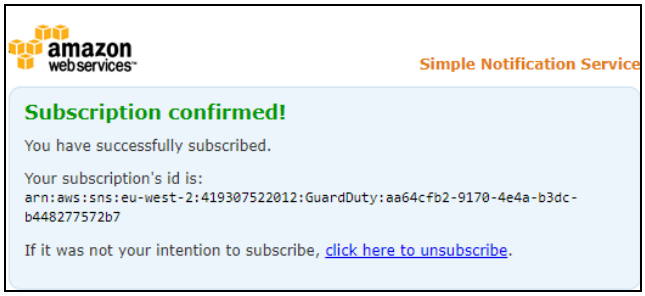
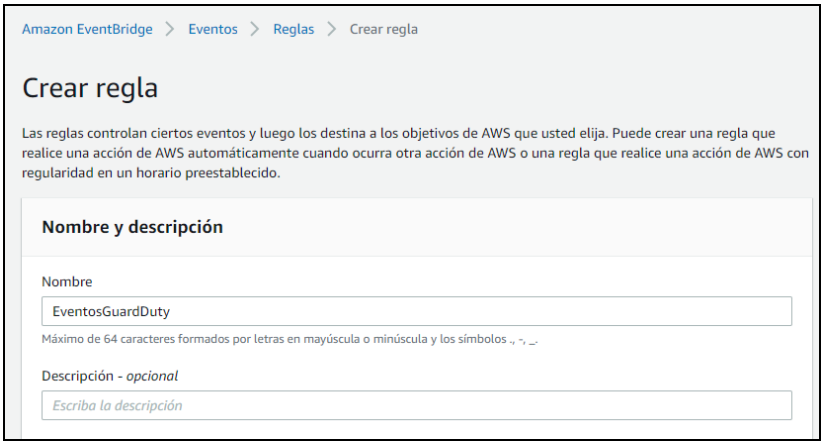


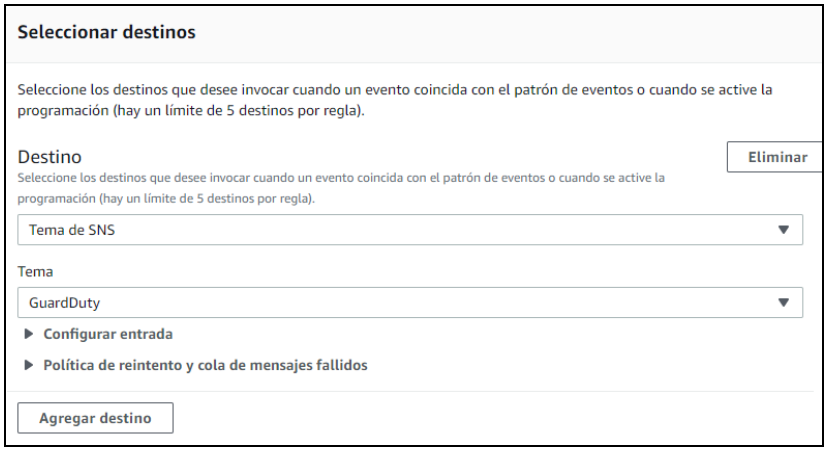
Ilustración 85. GuardDuty. confirmación SNS

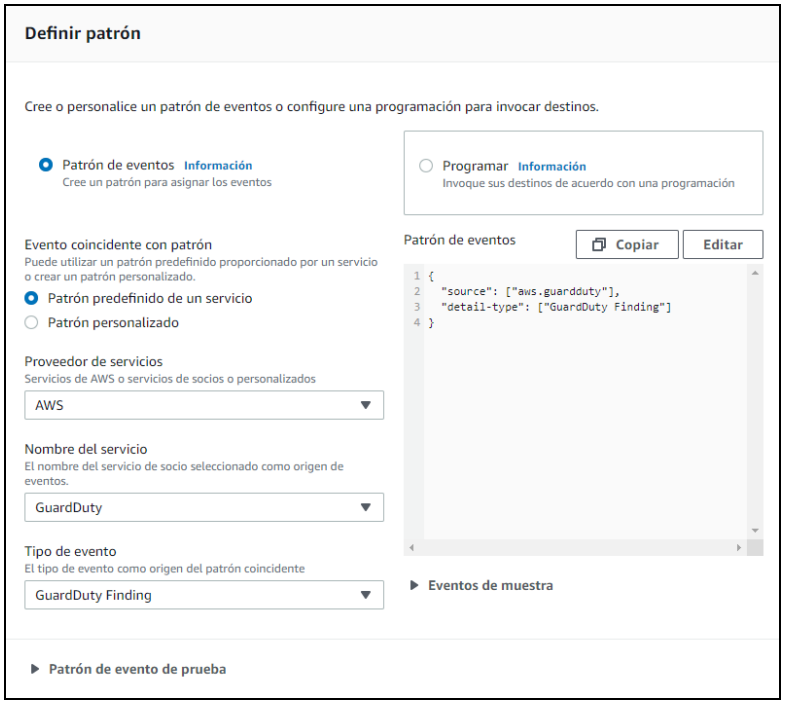
Finalmente creamos una regla en EventBridge

1- Abrimos la consola desde https://console.aws.amazon.com/events/

2- En el panel de navegación elegimos **Reglas** y creamos una nueva regla con los siguientes valores:







3- Y finalmente seleccionamos **Crear**.

Funcionamiento de GuardDuty

GuardDuty envía notificaciones basadas en Amazon CloudWatch Events cuando se produce algún cambio en los hallazgos. Estas notificaciones se envían dentro de los 5 minutos posteriores al hallazgo. Todas las apariciones posteriores de un hallazgo existente tendrán el mismo ID que el hallazgo original y las notificaciones se enviarán cada 6 horas después de la notificación inicial. Esto es para evitar la fatiga de alerta relacionada con el mismo hallazgo.

Generando un hallazgo

Una sencilla prueba para ver el correcto funcionamiento de GuardDuty sería provocando que se generara un hallazgo.

Para ello hemos utilizaremos una instancia de un Windows Server 2016 Base.

Ilustración 86. Creación de instancia en EC2 de AWS

Una vez desplegada la instancia nos conectamos a ella por RDP.

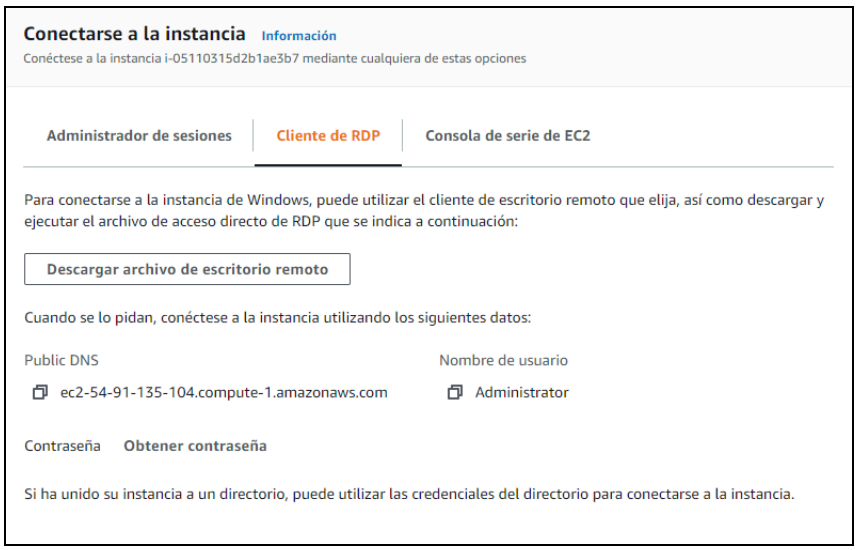


Ilustración 87. Detalle de conexión a una instancia en EC2 por RDP

Una vez conectados a la instancia instalamos el navegador Tor y navegamos por alguna página .onion. Esta acción provocará que aparezca dos nuevos hallazgos en GuardDuty calificados de Gravedad Alta que además, nos enviará un correo electrónico alertándonos de dicho hallazgo.

Ilustración 88. Hallazgos Gravedad Alta

Y si observamos los detalles del hallazgo vemos mayor detalle:

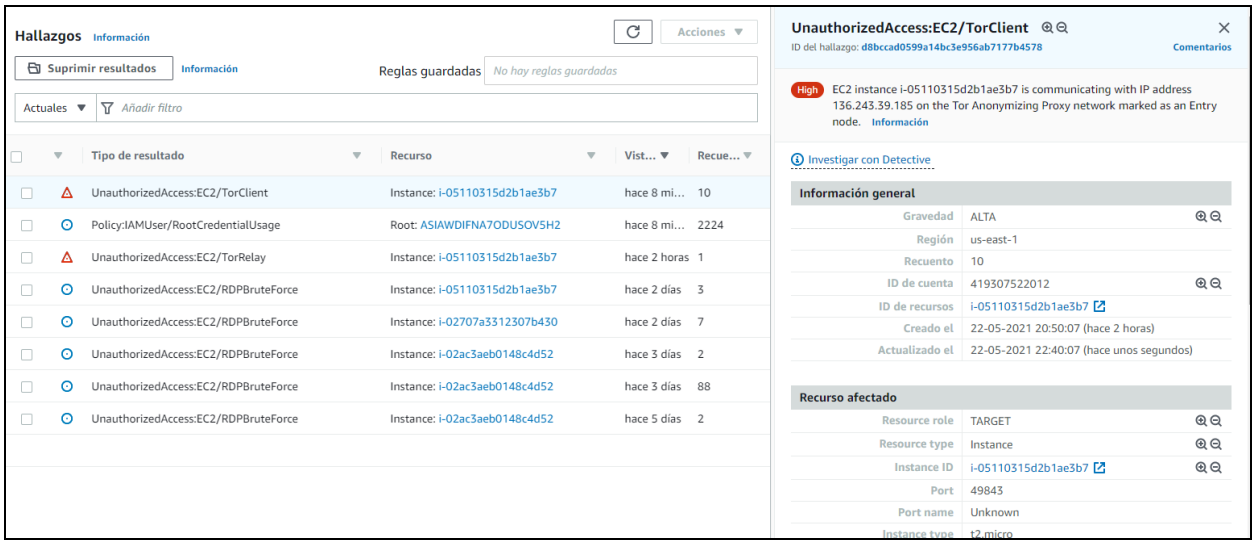


Ilustración 89. Detalle de hallazgo de Gravedad Alta

Por lo tanto, vemos que la orquestación de GuardDuty funciona correctamente y automatiza un envío de correo electrónico. Pero, ¿qué pasa con la respuesta? ¿Cómo podemos automatizar que se ponga remedio a los eventos?

Para automatizar respuestas AWS tiene las funciones Lambda que se comportan con el siguiente patrón:

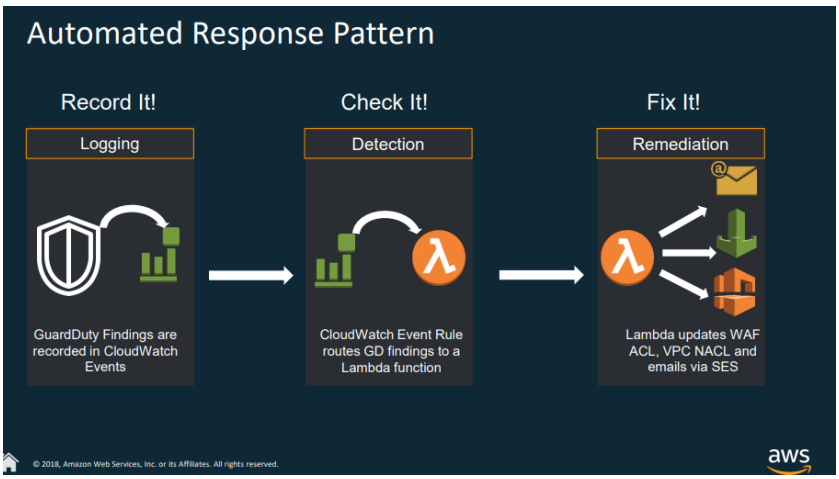


Ilustración 90. Patrón de Automatización de Remediación con función Lambda

Esto significa que GuardDuty registra los eventos de CloudWatch, si se produce un evento que cumpla alguna regla configurada para que se ejecute una función Lambda, ésta se encargará de la remediación.

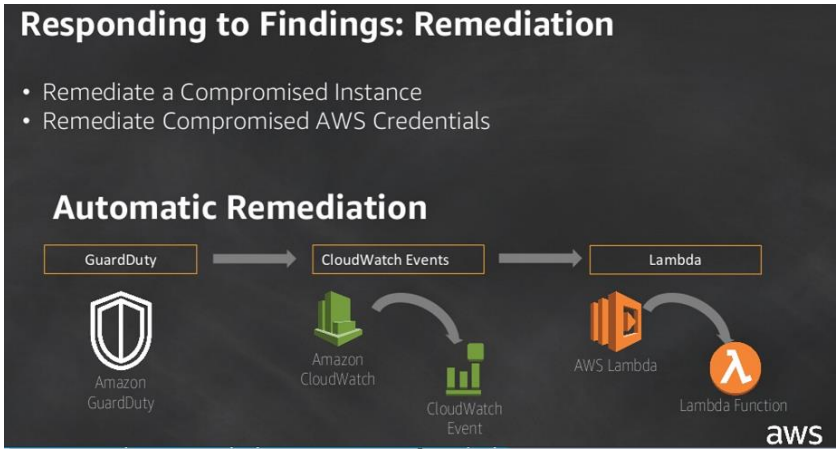


Ilustración 91. Respondiendo a hallazgos con remediaciones

Un ejemplo de Automatización sería el siguiente:

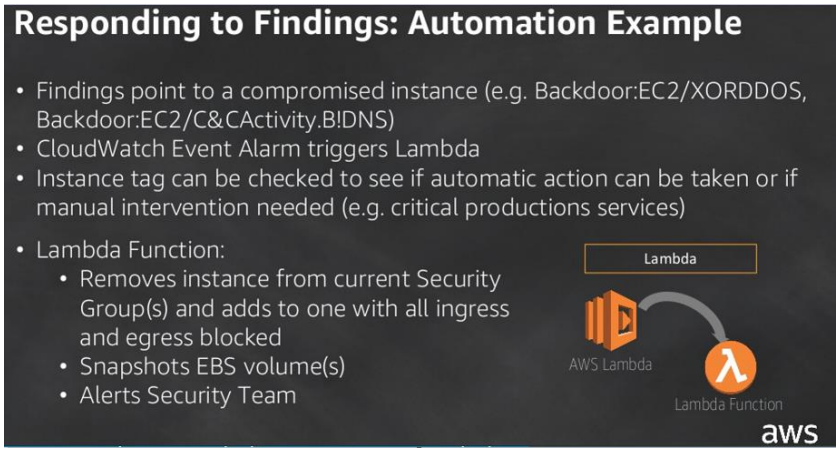


Ilustración 92. Ejemplo de Automatización en AWS

Para familiarizarnos con los servicios y características de AWS es muy interesante revisar alguno de los hands on de que dispone AWS.

Utilizando plantillas de CloudFormation que podemos crear un conjunto de recursos de AWS y familiarizarnos con ellos. Yo he utilizado dos:

- La plantilla utilizada en el artículo. "Getting Hands on with Amazon GuardDuty"[37] llamada: amazon-guard-duty-revamped-v2.yml.
- La plantilla utilizada en el artículo "How to use Amazon GuardDuty and AWS Web Application Firewall to automatically block suspicious hosts"[38] llamada: guarddutytoacl.template. Esta plantilla incluye una función lambda que utilizaremos para remediar un ataque de fuerza bruta.

---

[37] *https://hands-on-guardduty.awssecworkshops.com/#getting-hands-on-with-amazon-guardduty*

[38] *https://aws.amazon.com/es/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/*

Anexo C. Función lamdda GuardDuty_to_acl

GuardDuty_to_acl_lambda.py

```
# Copyright 2018 Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
# MIT No Attribution
# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

import boto3
import math
import time
import json
import datetime
import logging
import os
from boto3.dynamodb.conditions import Key, Attr
from botocore.exceptions import ClientError

logger = logging.getLogger()
logger.setLevel(logging.INFO)

#============================================================================================================================
# Variables
#============================================================================================================================
API_CALL_NUM_RETRIES = 1
ACLMETATABLE = os.environ['ACLMETATABLE']
SNSTOPIC = os.environ['SNSTOPIC']
CLOUDFRONT_IP_SET_ID = os.environ['CLOUDFRONT_IP_SET_ID']
ALB_IP_SET_ID = os.environ['ALB_IP_SET_ID']

#============================================================================================================================
# Auxiliary Functions
#============================================================================================================================
# Update WAF IP set
def waf_update_ip_set(waf_type, update_type, ip_set_id, source_ip):

    if waf_type == 'alb':
        session = boto3.session.Session(region_name=os.environ['AWS_REGION'])
        waf = session.client('waf-regional')
    elif waf_type == 'cloudfront':
        waf = boto3.client('waf')

    for attempt in range(API_CALL_NUM_RETRIES):
        try:
            response = waf.update_ip_set(IPSetId=ip_set_id,
                ChangeToken=waf.get_change_token()['ChangeToken'],
                Updates=[{
                    'Action': update_type,
                    'IPSetDescriptor': {
                        'Type': 'IPV4',
                        'Value': "%s/32"%source_ip
                    }
                }]
            )
            logger.info("log -- waf_update_ip_set %s IP %s - IPset %s, WAF type %s successfully..." % (update_type, source_ip, ip_set_id, waf_type))
        except Exception as e:
            logger.error(e)
            delay = math.pow(2, attempt)
            logger.info("log -- waf_update_ip_set retrying in %d seconds..." % (delay))
            time.sleep(delay)
        else:
            break
    else:
        logger.info("log -- waf_update_ip_set failed ALL attempts to call WAF API")
```

```
# Get the current NACL Id associated with subnet
def get_netacl_id(subnet_id):

    try:
        ec2 = boto3.client('ec2')
        response = ec2.describe_network_acls(
            Filters=[
                {
                    'Name': 'association.subnet-id',
                    'Values': [
                        subnet_id,
                    ]
                }
            ]
        )

        netacls = response['NetworkAcls'][0]['Associations']

        for i in netacls:
            if i['SubnetId'] == subnet_id:
                netaclid = i['NetworkAclId']

        return netaclid
    except Exception as e:
        return []

# Get the current NACL rules in the range 71-80
def get_nacl_rules(netacl_id):
    ec2 = boto3.client('ec2')
    response = ec2.describe_network_acls(
        NetworkAclIds=[
            netacl_id,
            ]
    )

    naclrules = []

    for i in response['NetworkAcls'][0]['Entries']:
        naclrules.append(i['RuleNumber'])

    naclrulesf = list(filter(lambda x: 71 <= x <= 80, naclrules))

    return naclrulesf

# Get current DDB state data for NACL Id
def get_nacl_meta(netacl_id):
    ddb = boto3.resource('dynamodb')
    table = ddb.Table(ACLMETATABLE)
    ec2 = boto3.client('ec2')
    response = ec2.describe_network_acls(
        NetworkAclIds=[
            netacl_id,
            ]
    )

    # Get entries in DynamoDB table
    ddbresponse = table.scan()
    ddbentries = response['Items']

    netacl = ddbresponse['NetworkAcls'][0]['Entries']
    naclentries = []

    for i in netacl:
            entries.append(i)

    return naclentries

#Update NACL and DDB state table
def update_nacl(netacl_id, host_ip, region):
    logger.info("log -- GD2ACL entering update_nacl, netacl_id=%s, host_ip=%s" % (netacl_id, host_ip))

    ddb = boto3.resource('dynamodb')
```

```
table = ddb.Table(ACLMETATABLE)
timestamp = int(time.time())

hostipexists = table.query(
   KeyConditionExpression=Key('NetACLId').eq(netacl_id),
   FilterExpression=Attr('HostIp').eq(host_ip)
)

# Is HostIp already in table?
if len(hostipexists['Items']) > 0:
   logger.info("log -- host IP %s already in table... exiting GD2ACL update." % (host_ip))
else:
   # Get current NACL entries in DDB
   response = table.query(
      KeyConditionExpression=Key('NetACLId').eq(netacl_id)
   )
   # Get all the entries for NACL
   naclentries = response['Items']

   # Find oldest rule and available rule numbers from 71-80
   if naclentries:
      rulecount = response['Count']
      rulerange = list(range(71, 81))

      ddbrulerange = []
      naclrulerange = get_nacl_rules(netacl_id)

      for i in naclentries:
         ddbrulerange.append(int(i['RuleNo']))

      # Check state and exit if NACL rule not in sync with DDB
      ddbrulerange.sort()
      naclrulerange.sort()
      synccheck = set(naclrulerange).symmetric_difference(ddbrulerange)

      if ddbrulerange != naclrulerange:
         logger.info("log -- current DDB entries, %s." % (ddbrulerange))
         logger.info("log -- current NACL entries, %s." % (naclrulerange))
         logger.error('NACL rule state mismatch, %s exiting' % (sorted(synccheck)))
         exit()

      # Determine the NACL rule number and create rule
      if rulecount < 10:
         # Get the lowest rule number available in the range
         newruleno = min([x for x in rulerange if not x in naclrulerange])

         # Create new NACL rule, IP set entries and DDB state entry
         logger.info("log -- adding new rule %s, HostIP %s, to NACL %s." % (newruleno, host_ip, netacl_id))
         create_netacl_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno)
         create_ddb_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno, region=region)
         waf_update_ip_set('alb', 'INSERT', ALB_IP_SET_ID, host_ip)
         waf_update_ip_set('cloudfront', 'INSERT', CLOUDFRONT_IP_SET_ID, host_ip)

         logger.info("log -- all possible NACL rule numbers, %s." % (rulerange))
         logger.info("log -- current DDB entries, %s." % (ddbrulerange))
         logger.info("log -- current NACL entries, %s." % (naclrulerange))
         logger.info("log -- new rule number, %s." % (newruleno))
         logger.info("log -- rule count for NACL %s is %s." % (netacl_id, int(rulecount) + 1))

      if rulecount >= 10:
         # Get oldest entry in DynamoDB table
         oldestrule = table.query(
            KeyConditionExpression=Key('NetACLId').eq(netacl_id),
            ScanIndexForward=True, # true = ascending, false = descending
            Limit=1,
         )

         oldruleno = int((oldestrule)['Items'][0]['RuleNo'])
         oldrulets = int((oldestrule)['Items'][0]['CreatedAt'])
         oldhostip = oldestrule['Items'][0]['HostIp']
         newruleno = oldruleno

         # Delete old NACL rule and DDB state entry
```

```
            logger.info("log -- deleting current rule %s for IP %s from NACL %s." % (oldruleno, oldhostip, netacl_id))
            delete_netacl_rule(netacl_id=netacl_id, rule_no=oldruleno)
            delete_ddb_rule(netacl_id=netacl_id, created_at=oldrulets)

            # check if IP is also recorded in a fresh finding, don't remove IP from blacklist in that case
            response_nonexpired = table.scan( FilterExpression=Attr('CreatedAt').gt(oldrulets) & Attr('HostIp').eq(host_ip) )
            if len(response_nonexpired['Items']) == 0:
               waf_update_ip_set('alb', 'DELETE', ALB_IP_SET_ID, oldhostip)
               waf_update_ip_set('cloudfront', 'DELETE', CLOUDFRONT_IP_SET_ID, oldhostip)
               logger.info('log -- deleting ALB and CloudFront WAF IP set entry for host, %s from CloudFront Ip set %s and ALB IP set %s.' % (oldhostip,
CLOUDFRONT_IP_SET_ID, ALB_IP_SET_ID))

            # Create new NACL rule, IP set entries and DDB state entry
            logger.info("log -- adding new rule %s, HostIP %s, to NACL %s." % (newruleno, host_ip, netacl_id))
            create_netacl_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno)
            create_ddb_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno, region=region)
            waf_update_ip_set('alb', 'INSERT', ALB_IP_SET_ID, host_ip)
            waf_update_ip_set('cloudfront', 'INSERT', CLOUDFRONT_IP_SET_ID, host_ip)

            logger.info("log -- all possible NACL rule numbers, %s." % (rulerange))
            logger.info("log -- current DDB entries, %s." % (ddbrulerange))
            logger.info("log -- current NACL entries, %s." % (naclrulerange))
            logger.info("log -- rule count for NACL %s is %s." % (netacl_id, int(rulecount)))

      else:
         # No entries in DDB Table start from 71
         naclrulerange = get_nacl_rules(netacl_id)
         newruleno = 71
         oldruleno = []
         rulecount = 0
         naclrulerange.sort()

         # Error and exit if NACL rules already present
         if naclrulerange:
            logger.error("log -- NACL has existing entries, %s." % (naclrulerange))
            exit()

         # Create new NACL rule, IP set entries and DDB state entry
         logger.info("log -- adding new rule %s, HostIP %s, to NACL %s." % (newruleno, host_ip, netacl_id))
         create_netacl_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno)
         create_ddb_rule(netacl_id=netacl_id, host_ip=host_ip, rule_no=newruleno, region=region)
         waf_update_ip_set('alb', 'INSERT', ALB_IP_SET_ID, host_ip)
         waf_update_ip_set('cloudfront', 'INSERT', CLOUDFRONT_IP_SET_ID, host_ip)

         logger.info("log -- rule count for NACL %s is %s." % (netacl_id, int(rulecount) + 1))

      if response['ResponseMetadata']['HTTPStatusCode'] == 200:
         return True
      else:
         return False

# Create NACL rule
def create_netacl_rule(netacl_id, host_ip, rule_no):

   ec2 = boto3.resource('ec2')
   network_acl = ec2.NetworkAcl(netacl_id)

   response = network_acl.create_entry(
   CidrBlock = host_ip + '/32',
   Egress=False,
   PortRange={
      'From': 0,
      'To': 65535
   },
   Protocol='-1',
   RuleAction='deny',
   RuleNumber= rule_no
   )

   if response['ResponseMetadata']['HTTPStatusCode'] == 200:
      logger.info("log -- successfully added new rule %s, HostIP %s, to NACL %s." % (rule_no, host_ip, netacl_id))
      return True
   else:
```

```
        logger.error("log -- error adding new rule %s, HostIP %s, to NACL %s." % (rule_no, host_ip, netacl_id))
        logger.info(response)
        return False

# Delete NACL rule
def delete_netacl_rule(netacl_id, rule_no):

    ec2 = boto3.resource('ec2')
    network_acl = ec2.NetworkAcl(netacl_id)

    response = network_acl.delete_entry(
        Egress=False,
        RuleNumber=rule_no
    )

    if response['ResponseMetadata']['HTTPStatusCode'] == 200:
        logger.info("log -- successfully deleted rule %s, from NACL %s." % (rule_no, netacl_id))
        return True
    else:
        logger.info("log -- error deleting rule %s, from NACL %s." % (rule_no, netacl_id))
        logger.info(response)
        return False

# Create DDB state entry for NACL rule
def create_ddb_rule(netacl_id, host_ip, rule_no, region):

    ddb = boto3.resource('dynamodb')
    table = ddb.Table(ACLMETATABLE)
    timestamp = int(time.time())

    response = table.put_item(
        Item={
            'NetACLId': netacl_id,
            'CreatedAt': timestamp,
            'HostIp': str(host_ip),
            'RuleNo': str(rule_no),
            'Region': str(region)
            }
        )

    if response['ResponseMetadata']['HTTPStatusCode'] == 200:
        logger.info("log -- successfully added DDB state entry for rule %s, HostIP %s, NACL %s." % (rule_no, host_ip, netacl_id))
        return True
    else:
        logger.error("log -- error adding DDB state entry for rule %s, HostIP %s, NACL %s." % (rule_no, host_ip, netacl_id))
        logger.info(response)
        return False

# Delete DDB state entry for NACL rule
def delete_ddb_rule(netacl_id, created_at):

    ddb = boto3.resource('dynamodb')
    table = ddb.Table(ACLMETATABLE)
    timestamp = int(time.time())

    response = table.delete_item(
        Key={
            'NetACLId': netacl_id,
            'CreatedAt': int(created_at)
            }
        )

    if response['ResponseMetadata']['HTTPStatusCode'] == 200:
        logger.info("log -- successfully deleted DDB state entry for NACL %s." % (netacl_id))
        return True
    else:
        logger.error("log -- error deleting DDB state entry for NACL %s." % (netacl_id))
        logger.info(response)
        return False

# Send notification to SNS topic
def admin_notify(iphost, findingtype, naclid, region, instanceid):
```

```
  MESSAGE = ("GuardDuty to ACL Event Info:\r\n"
             "Suspicious activity detected from host " + iphost + " due to " + findingtype + "."
             "  The following ACL resources were targeted for update as needed; "
             "CloudFront IP Set: " + CLOUDFRONT_IP_SET_ID + ", "
             "Regional IP Set: " + ALB_IP_SET_ID + ", "
             "VPC NACL: " + naclid + ", "
             "EC2 Instance: " + instanceid + ", "
             "Region: " + region + ". "
            )

  sns = boto3.client(service_name="sns")

  # Try to send the notification.
  try:
    sns.publish(
      TopicArn = SNSTOPIC,
      Message = MESSAGE,
      Subject='AWS GD2ACL Alert'
    )
    logger.info("log -- send notification sent to SNS Topic: %s" % (SNSTOPIC))

  # Display an error if something goes wrong.
  except ClientError as e:
    logger.error('log -- error sending notification.')
    raise


#=============================================================================================================================
# Lambda Entry Point
#=============================================================================================================================

# Lambda handler
def lambda_handler(event, context):

  logger.info("log -- Event: %s " % json.dumps(event))

  try:

    if event["detail"]["type"] == 'Recon:EC2/PortProbeUnprotectedPort':
        HostIp = []
        Region = event["region"]
        SubnetId = event["detail"]["resource"]["instanceDetails"]["networkInterfaces"][0]["subnetId"]
        for i in event["detail"]["service"]["action"]["portProbeAction"]["portProbeDetails"]:
          HostIp.append(str(i["remoteIpDetails"]["ipAddressV4"]))
        instanceID = event["detail"]["resource"]["instanceDetails"]["instanceId"]
        NetworkAclId = get_netacl_id(subnet_id=SubnetId)

    else:
      Region = event["region"]
      SubnetId = event["detail"]["resource"]["instanceDetails"]["networkInterfaces"][0]["subnetId"]
      HostIp = [event["detail"]["service"]["action"]["networkConnectionAction"]["remoteIpDetails"]["ipAddressV4"]]
      instanceID = event["detail"]["resource"]["instanceDetails"]["instanceId"]
      NetworkAclId = get_netacl_id(subnet_id=SubnetId)

    if NetworkAclId:

      # Update VPC NACL, global and regional IP Sets
      for ip in HostIp:
        response = update_nacl(netacl_id=NetworkAclId, host_ip=ip, region=Region)

      #Send Notification
      admin_notify(str(HostIp), event["detail"]["type"], NetworkAclId, Region, instanceid = instanceID)

      logger.info("log -- processing GuardDuty finding completed successfully")

    else:
      logger.info("log -- unable to determine NetworkAclId for instanceID: %s, HostIp: %s, SubnetId: %s. Confirm resources exist." % (instanceID,
HostIp, SubnetId))
      pass

  except Exception as e:
    logger.error('log -- something went wrong.')
    raise
```