Implementación de una plataforma de inteligencia de amenazas.

Threat Intelligence.

Fabián Enrique Calvopiña Estrella

Implementación de una plataforma de inteligencia de amenazas.
Seguridad empresarial

Tutor de TF
Miguel Angel Flores Terrón
Profesor responsable de la asignatura
Víctor García Font

Universitat Oberta de Catalunya

Fecha Entrega:
13/06/2023

GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación de una plataforma de Inteligencia de amenazas (Threat Intelligence)*
Nombre del autor:	*Fabián Enrique Calvopiña Estrella*
Nombre del consultor/a:	*Miguel Angel Flores Terron*
Nombre del PRA:	*Víctor Garcia Font*
Fecha de entrega :	*06/2023*
Titulación o programa:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Threat Intelligence, ataques, plataforma.*

Resumen del Trabajo

Hoy en día la tecnología, se encuentra en casi todo tipo de industrias u organizaciones las mismas que han revolucionado en todo el mundo, sin embargo, han traído riesgos en forma de ataques cibernéticos.

La inteligencia de amenazas es el conocimiento que le permite prevenir o mitigar esos ataques, proporcionando un contexto, como quién lo está atacando, cuáles son sus motivaciones y capacidades, qué indicadores de compromiso en sus sistemas buscar, que lo ayuda a tomar decisiones informadas sobre su seguridad.

El presente trabajo tiene la finalidad de realizar una investigación en profundidad sobre la aplicación de Threat Intelligence haciendo uso de herramientas open source.

Dentro de este ámbito se considera trabajar como base la plataforma **OpenCTI** (open-source) e integrarlo con la herramienta **TheHive**, con el objetivo principal de maximizar la eficacia en la búsqueda y gestión de amenazas cibernéticas. Con lo cual nuestra metodología a utilizar se complementa en vincularlo con el framework de **MITRE ATT&CK**.

Finalmente, como resultado de la investigación, se pretende obtener una solución innovadora que combine las habilidades y capacidades tanto de la

plataforma y de la(s) herramienta(s) seleccionada(s), de tal forma que sea más flexible y que se adapte de modo personalizado para las organizaciones con el fin de mitigar el riesgo de ciberamenazas.

Abstract

Today's technology, found in almost every type of industry or organization, has revolutionized the world; however, it has brought risks in the form of cyber attacks.

Threat intelligence is the knowledge that allows you to prevent or mitigate those attacks by providing context, such as who is attacking you, what their motivations and capabilities are, and what indicators of compromise in your systems to look for, which helps you make informed decisions about your security.

The purpose of this work is to conduct in-depth research on the application of Threat Intelligence, preferably using open-source tools.

Within this scope it is considered to work as a base the OpenCTI platform (open-source) and integrate it with TheHive tool, with the main objective of maximizing the effectiveness in the search and management of cyber threats. With which our methodology to be used is complemented by linking it with the MITRE ATT&CK framework.

Finally, as a result of the research, it is intended to obtain an innovative solution that combines the skills and capabilities of both the platform and the selected tool, which implies being more flexible and customizable for organizations to mitigate the risk of cyber threats.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

El ámbito actual de la seguridad cibernética se ha convertido en un panorama de amenazas muy complejo que cambia constantemente y va en aumento, por lo que las empresas sienten la necesidad de adelantarse a las nuevas tendencias de ataques informáticos estableciendo por ejemplo programas de inteligencia de amenazas (**Threat Intelligence**) para mejorar sus capacidades de defensa y mitigar el riesgo.

A veces dichas amenazas permanecen inactivas hasta que se les dirige a atacar, o comprometen silenciosamente la seguridad de organizaciones y / o individuos. threat Intelligence recopila y compila los datos sin procesar sobre las amenazas que surgen de diferentes fuentes.

Las mejores soluciones utilizan el aprendizaje automático para automatizar la recopilación y el procesamiento de datos, integrarse con sus soluciones existentes, tomar datos no estructurados de fuentes dispares y luego conectar los puntos al proporcionar contexto sobre los indicadores de compromiso (IoC) y las tácticas, técnicas y procedimientos. (TTP) de los actores de amenazas.

Las amenazas cibernéticas dirigidas a las empresas son identificadas por **Threat Intelligence** donde, los especialistas en TI y las herramientas complejas exclusivas pueden leer y analizar las amenazas/ataques. "Enraizada en los datos, la inteligencia de amenazas proporciona un contexto, como quién lo está atacando, cuáles son sus motivaciones y capacidades, y qué indicadores de compromiso en sus sistemas buscar, que lo ayudan a tomar decisiones informadas sobre su seguridad." (Conti et al., 2018)

Esta información ayuda a planificar, prevenir y reconocer las amenazas cibernéticas con la esperanza de explotar los activos más importantes de la organización.

El conocimiento de las amenazas cibernéticas puede ayudar a las asociaciones a obtener información importante sobre estas amenazas, construir equipos de defensa exitosos y aliviar las amenazas que podrían dañar su reputación.

La gente a menudo confunde entre términos de seguridad cibernética como inteligencia de amenazas y datos de amenazas. Los datos de amenazas son una lista de amenazas probables. Además, por ejemplo, los feeds de Facebook son como una lista continua de posibles problemas.

Figura 1: Proceso feedback CTI

De acuerdo con (Ciberseguridad.com, 2021) resulta importante, contar con una inteligencia de amenazas ya que es una parte vital de la ciberseguridad, una herramienta de este tipo se denomina CTI y puede:

- Evitar la pérdida de datos.
- Al tenerlo muy organizado y configurado, la organización puede detectar amenazas cibernéticas, evitando así que las violaciones de datos filtren información crítica.
- Detecta los diseños utilizados por los piratas informáticos.
- Empodera a las partes interesadas en la seguridad cibernética al revelar los motivos del adversario y sus tácticas, técnicas y procedimientos (TTP).
- "Ayuda a los profesionales de seguridad a entender mejor el proceso de decisión del actor de amenazas." (“Inteligencia de amenazas, todo lo que debes saber - Ciberseguridad”)
- Empodera a las partes interesadas del negocio , como juntas ejecutivas, CISO, CIO y CTO; invertir sabiamente, mitigar el riesgo, ser más eficiente y tomar decisiones más rápidas.

La prevención del fraude, el análisis de riesgos y otros procesos de seguridad de alto nivel se enriquecen con la comprensión del panorama actual de amenazas que proporciona la inteligencia de amenazas.

"Las soluciones de inteligencia de amenazas que se basan en procesos de aprendizaje automático para la recopilación de datos automatizados a gran escala pueden superar muchos de estos problemas al intentar desarrollar una inteligencia de amenazas operativa eficaz." (CYBERVIE, 2020)

En cuanto a dónde se utiliza la inteligencia de amenazas, existen diversas fuentes y herramientas que las organizaciones y empresas pueden utilizar para recopilar, analizar y aplicar la inteligencia de amenazas, como pueden ser los feeds de seguridad, la inteligencia de código abierto, las soluciones de seguridad de proveedores, las comunidades de seguridad, entre otros.

La inteligencia de amenazas es una parte fundamental de la estrategia de seguridad de cualquier organización que desee mantenerse protegida frente a

los crecientes riesgos de seguridad cibernética, dentro de este ámbito, es utiliza en diversas áreas y contextos como, por ejemplo:

- **Defensa y seguridad nacional:** Las agencias de inteligencia y defensa utilizan la inteligencia de amenazas para identificar y prevenir ataques cibernéticos a nivel nacional. Esto incluye la identificación de actores malintencionados y su motivación, los métodos de ataque y las posibles consecuencias para la seguridad nacional.

- **Empresas y organizaciones:** Las empresas y organizaciones utilizan la inteligencia de amenazas para proteger sus redes, sistemas y datos de ataques cibernéticos. La inteligencia de amenazas ayuda a identificar vulnerabilidades en los sistemas, a detectar posibles ataques en tiempo real y a tomar medidas preventivas y de mitigación.

- **Proveedores de servicios de seguridad:** Los proveedores de servicios de seguridad utilizan la inteligencia de amenazas para mejorar sus productos y servicios, incluyendo soluciones de seguridad de red, antivirus, firewalls y otros productos de seguridad.

- **Investigación y desarrollo:** La inteligencia de amenazas también se utiliza en la investigación y el desarrollo de nuevas soluciones de seguridad cibernética, así como para identificar nuevas amenazas y tendencias en el ámbito de la seguridad.

Una plataforma que se encarga de realizar este gran trabajo es **OpenCTI**[1]**,** misma que se trata de un tablero de código abierto, se ha creado para estructurar, almacenar, organizar y visualizar información técnica y no técnica sobre amenazas cibernéticas. Es decir, es una plataforma de inteligencia de amenazas que permite a las organizaciones administrar sus conocimientos, notas de inteligencia de amenazas cibernéticas, recopilar, enriquecer y compartir información sobre amenazas de seguridad.

Figura 2: Interfaz OpenCTI

[1] https://github.com/OpenCTI-Platform/opencti

La estructuración de los datos se realiza utilizando un esquema de conocimiento basado en el **Normas STIX2**[2]. Está diseñado como una aplicación web moderna que incluye un **API GraphQL** y una interfaz orientada a UX. Además, OpenCTI se puede integrar con otras herramientas y aplicaciones como MISP, La colmena, MITRE ATT&CK, etc[3].

Por otra parte, (Stojkovski, 2021) indica que existen varias herramientas de seguridad como por ejemplo **TheHive** que es una plataforma de gestión de incidentes de seguridad que permite a los equipos de seguridad de una organización recopilar, analizar y responder a dichos incidentes.

TheHive y OpenCTI son dos herramientas de seguridad diferentes que pueden integrarse para proporcionar una solución de gestión de incidentes de seguridad más completa y eficaz.

Con todo este contexto explicado, de las herramientas a utilizar, se complementa con una metodología basada en el framework de **MITRE ATT&CK**. Adversarial Tactics, Techniques & Common Knowledge) es un marco de referencia de ciberseguridad que describe las tácticas, técnicas y procedimientos (TTPs) utilizados por los atacantes para comprometer sistemas y redes. Se basa en la recopilación de datos de ataques reales y representa un catálogo de las actividades y técnicas que los atacantes utilizan para infiltrarse en sistemas, moverse lateralmente dentro de una red, mantener el acceso y exfiltrar datos.

Por tanto, el presente trabajo de fin de máster se centra en la implementación e integración de TheHive con OpenCTI, misma que permitirá a los equipos de seguridad de una organización acceder a información detallada sobre las amenazas de seguridad y utilizar esta información para tomar decisiones más informadas y precisas sobre cómo responder a los incidentes de seguridad.

Como resultado final, se obtendrá un recurso dual que combine las habilidades y capacidades tanto de la plataforma y de la herramienta escogida, de tal forma que complemente y potencie el efecto para inteligenciar la mitigación de amenazas.

A modo personal, y de acuerdo con la experiencia laboral recorrida, he palpado que, en las empresas o instituciones en el país, se desconoce del alcance o la importancia de la seguridad informática, además no existe personal 100% capacitado para gestionar este tipo de trabajo, lo cual me motiva para generar un aporte significativo y de valor a toda la sociedad en general.

A nivel local, representa un aporte sustancial para las organizaciones en cuanto a seguridad cibernética se refiere, ya que actualmente no cuentan con una herramienta apropiada que ofrezca todos los beneficios que se han mencionado y ahora se podrá contar una vez que se logré implementar esta innovadora plataforma.

---

[2] https://oasis-open.github.io/cti-documentation/
[3] “https://github.com/OpenCTI-Platform/opencti-KolMitE

1.2. Objetivos del Trabajo

Los objetivos principales para este trabajo de fin de máster son los siguientes:

Objetivos a nivel de investigación y estudios:

- Estudio, análisis y diferencias entre Threat Intelligence y Threat Hunting
- Revisar el estado del arte sobre el contexto Threat Intelligence.

Objetivos a nivel de implementación y desarrollo:

- Implementar una plataforma base para inteligencia de amenazas como OpenCTI.
- Integrar como segunda plataforma TheHive para gestión de incidentes de seguridad.
- Aplicar como metodología de soporte, como el framework de MITRE ATT&CK.

Objetivos a nivel académico/entrega:

- Desarrollar las entregas parciales y enviarlas en tiempo y forma.
- Desarrollar la memoria final del TFM.
- Generar un PPT y video que sintetice todo el proyecto.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

- **Dimensión sostenibilidad:** existe un ahorro en recursos de software, por lo cual genera desarrollo en su período de uso ya que es un producto de innovación y mejora. Por lo cual, su impacto es positivo en lo que se refiere a los ODS (7, 9, 11, 12, 13, 14, 15).

- **Dimensión comportamiento ético y de responsabilidad social (RS):** basándonos en que se trabaja con herramientas de uso libre no existe uso fraudulento en el producto/resultado final, ni en reputación del propietario/usuario, también respeta los principios deontológicos profesionales. En tal virtud, su impacto es positivo en los ODS (1, 2, 6, 8, 16),

- **Dimensión diversidad, género y derechos humanos:** el impacto en los **ODS 5 y ODS 10** son positivos porque su beneficio no distingue raza, religión, orientación sexual, funcional, etnia, ideología; no existe afectación en la privacidad o propiedad intelectual porque son herramientas open-source probadas y de libre uso. En conclusión, no hay alguna preocupación sobre diversidad/género o derechos humanos.

1.4. Enfoque y método seguido

El presente proyecto se enfoca en el ámbito empresarial, el cual consiste en implementar una plataforma más robusta y efectiva que las tradicionales para lograr este fin, se investigará sobre **OpenCTI** que es un marco de trabajo de

inteligencia de amenazas de código abierto, proporciona una plataforma para la recopilación, análisis y compartición de información de amenazas entre diferentes organizaciones y herramientas de seguridad. Además, es altamente personalizable y se puede integrar con otras herramientas de seguridad y fuentes de datos para aumentar la eficacia de la gestión de amenazas.

Asi mismo, correlaciona grandes cantidades de información de amenazas, incluyendo indicadores de compromiso, tácticas, técnicas y procedimientos de ataque; asi mismo, los equipos de seguridad pueden colaborar y compartir información con otras organizaciones.

El objetivo será que OpenCTI se integre con **TheHive**, que es una plataforma de análisis y respuesta de seguridad de código abierto que ayuda a las organizaciones a gestionar incidentes de seguridad de manera eficiente y colaborativa. Permite a los equipos de seguridad centralizar, investigar y responder a incidentes de seguridad en tiempo real, lo que les permite tomar decisiones informadas y rápidas.

Según (Ciberseguridad.com, 2021), la manera adecuada a tratar en un proyecto se divide en dos partes, una parte teórica y otra práctica.

- La primera parte ***teórica*** es referente a la investigación sobre las herramientas a utilizar concerniente a la gestión de amenazas. Además, se profundiza en varios conceptos complementarios de seguridad para establecer una base teórica fundamentada.

- La segunda parte consiste en seleccionar las ***herramientas*** más adecuadas luego del análisis y estudio previo realizado se implementen en una sola plataforma de acuerdo con una metodología establecida.

Por lo dicho, es fundamental que, para llegar a cumplir los objetivos planteados, se considere como estrategia dividir la parte teórica y posterior la aplicación de la práctica, para relacionarlos adecuadamente tanto la investigación como la implementación. En cuanto a la metodología que permita llegar a cumplir con los objetivos nos basaremos en las referencias del framework de MITRE ATT&CK.

Finalmente, se comprobará insitu dentro de una organización real, la efectividad y eficiencia de los resultados una vez que se compare la plataforma propuesta versus las herramientas tradicionales para la gestión de inteligencia de amenazas. Por consiguiente, se puede ir evidenciando las actividades y resultados que se producen de inicio a fin en el proyecto.

1.5. Planificación del Trabajo

Descripción de las etapas de la planificación:

- **Planificación**: esta fase se encarga de recopilar información en base a los esquemas especificados por UOC para establecer el problema, definir los objetivos, la metodología y el cronograma de trabajo.

- **Análisis:** aquí trabajamos en el estudio del arte y conceptual de los temas y subtemas que involucra Threat Intelligence.
- **Implementación:** abarca todo el proceso de ejecución que implica la instalación de la plataforma y/o herramientas necesarias previo la implementación de inteligencia de amenazas.
- **Diseño:** es la fase en la cual específicamente se va a implementar las tácticas y herramientas seleccionadas para nuestra plataforma.
- **Pruebas:** es la última fase donde evidentemente se realizarán pruebas de funcionalidad y operatividad.

  Esto se muestra en el diagrama Gantt de la la **Figura 3,** las ultimas actividades a realizar refieren a la entrega del proyecto y proceso del desarrollo de a memoria final TFM.

Planificación del Proyecto.

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Avance (%)
IMPLEMENTACION DE UNA PLATAFORMA DE THREAT INTELLIGENCE.	**87 días**	**mié 1/3/23**	**jue 29/6/23**		
1. Planificación	**10 días**	**mié 1/3/23**	**mar 14/3/23**		
1.1. Revisión de contenidos y guias TFM	5 días	mié 1/3/23	mar 7/3/23		100%
1.2. Establecer problema a resolver	1 día	mié 8/3/23	mié 8/3/23	3	100%
1.3. Definición de Objetivos	1 día	jue 9/3/23	jue 9/3/23	4	100%
1.4. Definir propuesta metodológica	1 día	vie 10/3/23	vie 10/3/23	5	100%
1.5. Elaborar el cronograma de Trabajo	1 día	lun 13/3/23	lun 13/3/23	6	100%
1.6. Envío PEC 1 (Plan de Trabajo)	1 día	mar 14/3/23	mar 14/3/23	7	100%
2. Análisis	**20 días**	**mié 15/3/23**	**mar 11/4/23**		
2.1. Investigación sobre Threat Intelligence.	**20 días**	**mié 15/3/23**	**mar 11/4/23**		
2.1.1. Estudio de Threat Intelligence	7 días	mié 15/3/23	jue 23/3/23	8	100%
2.1.2.Estudio de herramientas Open-source	5 días	vie 24/3/23	jue 30/3/23	11	100%
2.1.3. Estudio de OpenCTI	3 días	vie 31/3/23	mar 4/4/23	12	100%
2.1.4. Estudio de TheHive	3 días	mié 5/4/23	vie 7/4/23	13	100%
2.1.5. Estudio de MITRE ATT&CK	1 día	lun 10/4/23	lun 10/4/23	14	100%
2.1.6. Envío PEC 2 (Entrega de Seguimiento)	1 día	mar 11/4/23	mar 11/4/23	15	100%
3. Implementación	**35 días**	**mié 12/4/23**	**mar 30/5/23**		
3.1. Requerimientos	**3 días**	**mié 12/4/23**	**vie 14/4/23**		
3.1.1. Instalación y configuración de prerrequisitos para montar máquina virtual	1 día	mié 12/4/23	mié 12/4/23	16	100%
3.1.2. Configuración de parámetros para levantar ISO Ubuntu	1 día	jue 13/4/23	jue 13/4/23	19	100%
3.1.3. Ejecución de Actualizaciones Ubuntu	1 día	vie 14/4/23	vie 14/4/23	20	100%
3.2. Despliegue	**29 días**	**lun 17/4/23**	**jue 25/5/23**		
3.2.1. Despliegue de Docker y Docker Compose	3 días	lun 17/4/23	mié 19/4/23	21	100%

3.2.2. Despliegue de Portainer	3 días	jue 20/4/23	lun 24/4/23	23	100%
3.2.3. Preparación y configuración de componentes Docker OpenCTI y TheHive	3 días	mar 25/4/23	jue 27/4/23	24	100%
3.2.4. Despliegue de la plataforma OpenCTI	7 días	vie 28/4/23	lun 8/5/23	25	100%
3.2.5. Despliegue de la plataforma TheHive	7 días	mar 9/5/23	mié 17/5/23	26	100%
3.2.6. Implementación de conectores: MITRE, TheHive, AbuseIPDB.	3 días	jue 18/5/23	lun 22/5/23	27	100%
3.2.7. Recopilar información sobre la implantación	2 días	mar 23/5/23	mié 24/5/23	28	100%
3.2.8. Envío PEC 3 (Redacción del documento)	1 día	jue 25/5/23	jue 25/5/23	29	100%
3.3. Pruebas	**3 días**	**vie 26/5/23**	**mar 30/5/23**		
3.1. Integración	1 día	vie 26/5/23	vie 26/5/23	30	100%
3.2. Verificación	1 día	lun 29/5/23	lun 29/5/23	32	100%
3.3. Test finales	1 día	mar 30/5/23	mar 30/5/23	33	100%
4. Presentación	**22 días**	**mié 31/5/23**	**jue 29/6/23**		
4.1. Desarrollo de Memoria Final del TFM. (PEC 4)	10 días	mié 31/5/23	mar 13/6/23	34	100%
4.2. Presentación en Video	5 días	mié 14/6/23	mar 20/6/23	36	0%
4.3. Defensa del TFM	7 días	mié 21/6/23	jue 29/6/23	37	0%

Tabla 1: Planificación del Proyecto

Diagrama Gantt

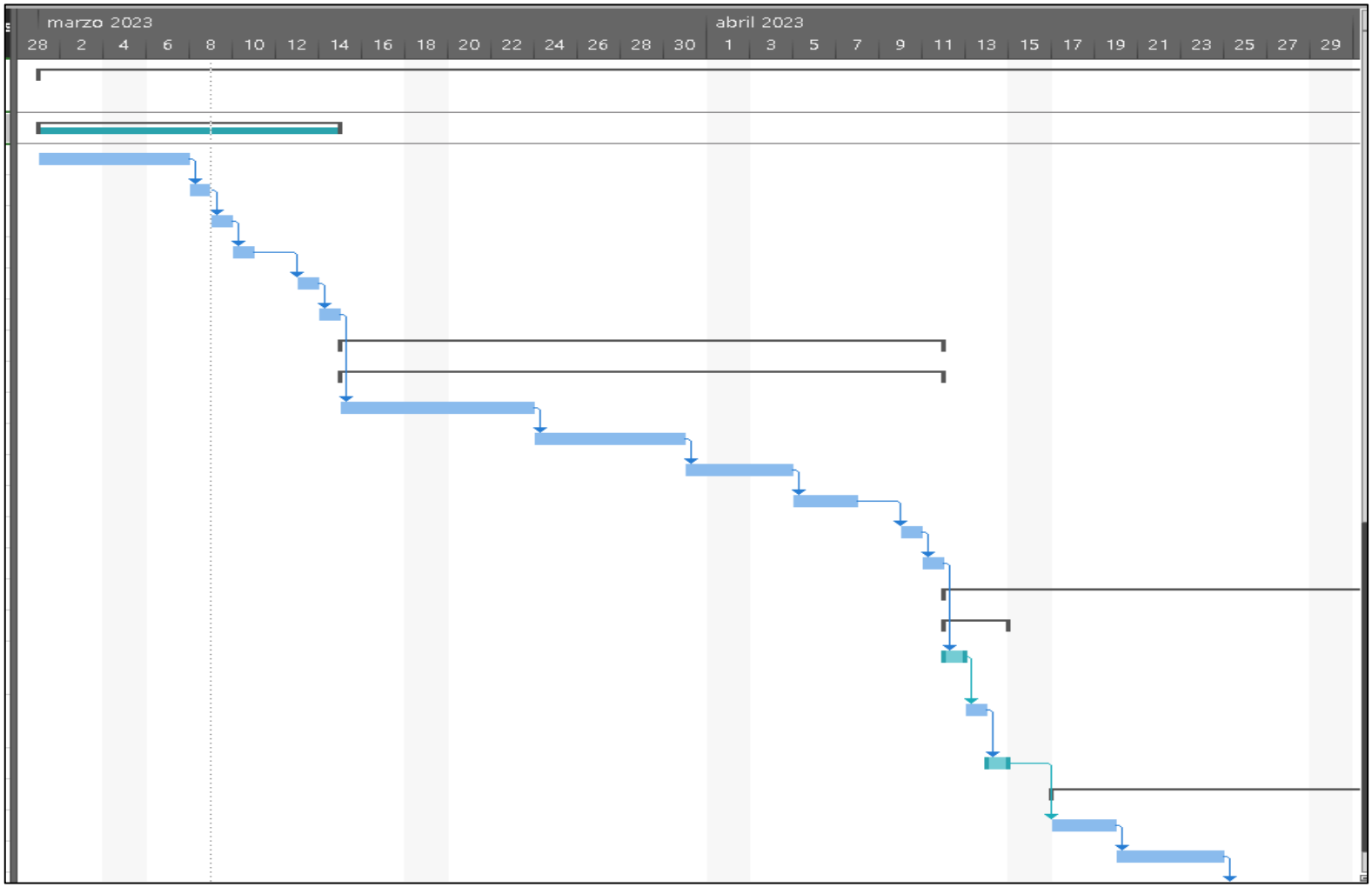


Figura 3: Diagrama GANTT (1 de 2)

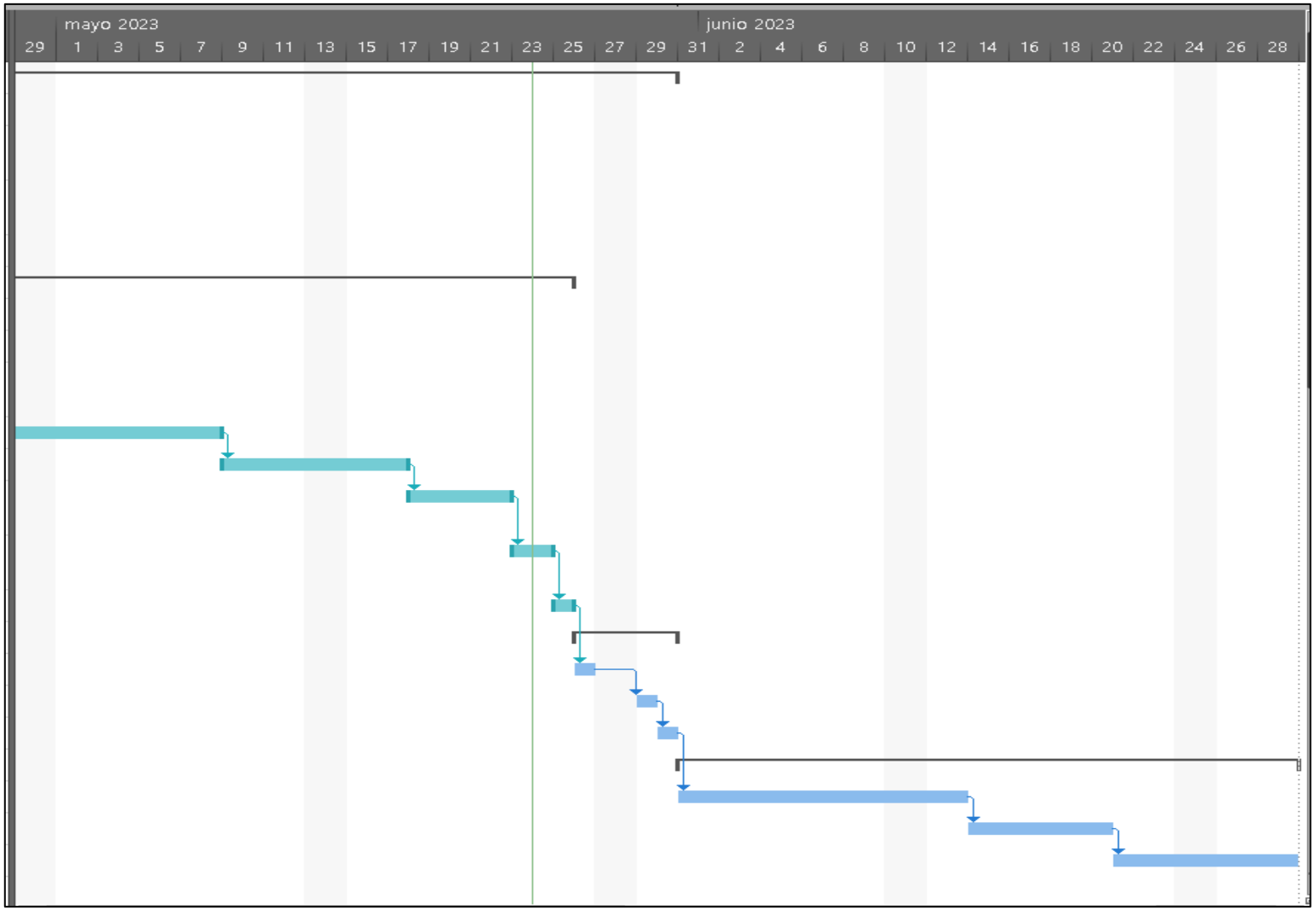


Figura 4: Diagrama GANTT (2 de 2)

1.6. Breve sumario de productos obtenidos

El trabajo final de máster se divide en los siguientes entregables parciales, que formarán parte del resultado final del proyecto:

- **PEC1:** Muestra el plan de trabajo, enmarcado en el desarrollo del proyecto, contexto, objetivos, impacto en sostenibilidad, enfoque y planificación.
- **PEC2:** trata una primera entrega parcial sobre el estudio y análisis investigativo sobre Threat Intelligence.
- **PEC 3:** trata una segunda entrega parcial donde ponemos en práctica la aplicación e integración de herramientas estudiadas en la entrega anterior con el objetivo de presentar los resultados de la implementación de una Plataforma para Threat Intelligence integrada con OpenCTI y sus complementos.
- **PEC 4:** sintetiza todo el trabajo completo realizado para generar la memoria final del proyecto con las respectivas conclusiones, bibliografía, anexos y recomendaciones a futuro sobre el producto obtenido y su aplicación.
- **PEC 5:** se presenta una grabación en video, donde se explica el resumen del trabajo final.

1.7. Breve descripción de los otros capítulos de la memoria.

El estado del arte, profundiza un estudio de Threat Intelligence, en su ámbito, éxitos, problemática, posibles aplicaciones, software y hardware existente.

Luego hablamos de la plataforma OpenCTI acerca de principales capacidades y características, posibilidades que ofrece, y los conectores necesarios para su operación de análisis.

Aquí ampliaremos el contexto de los conectores que se elegirán para nuestro estudio y posterior aplicación en la plataforma. Al final el objetivo será integrar capacidades con la utilización de otras herramientas Opensource.

También revisamos el tema de MITRE ATT&CK, el cual nos sirve de metodología para analizar las técnicas y ataques que se pueden dar en los diferentes escenarios existentes.

2. Estado del Arte

2.1. Qué es Threat Intelligence (CTI)

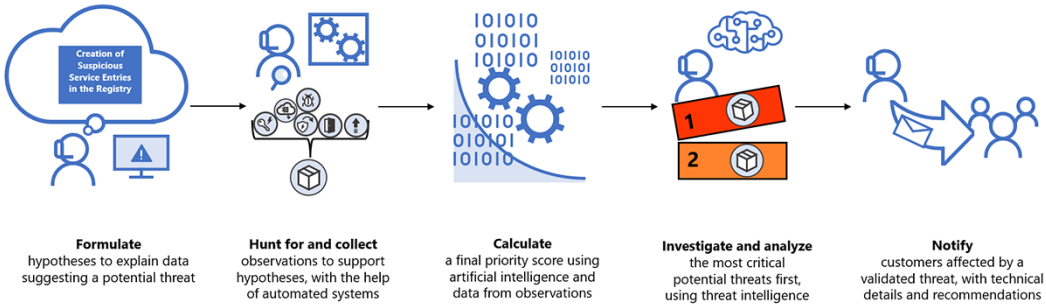


Figura 5: Cyber Threat Intelligence

También conocida como Threat Intelligence, es un campo en constante evolución debido al aumento de la sofisticación de las amenazas en línea. El objetivo de la inteligencia de amenazas es proporcionar información oportuna y precisa sobre las amenazas de seguridad actuales y potenciales para ayudar a las organizaciones a tomar medidas preventivas.

Según (Kaspersky, 2023) la definición de la inteligencia de amenazas suele confundirse con otros términos de ciberseguridad. Lo más habitual es que las personas confundan “datos de amenazas” con “inteligencia de amenazas”, pero son dos conceptos diferentes:

Los datos de amenazas son una lista de posibles amenazas, en cambio la inteligencia de amenazas se centra en cuestiones más globales: examina los datos y el contexto más general para elaborar una narrativa que aporte información para la toma de decisiones.

Básicamente, la inteligencia de amenazas permite que las organizaciones tomen decisiones sobre la seguridad más rápido y con más información. Fomenta las acciones proactivas, en lugar de las reactivas, en la lucha contra los ciberataques.

Es decir, la inteligencia de amenazas es el proceso de identificar y analizar ciberamenazas. El término “inteligencia de amenazas” puede hacer referencia a los datos reunidos sobre una potencial amenaza o al proceso de recopilar, procesar y analizar esos datos para comprender mejor las amenazas. La inteligencia de amenazas consiste en revisar los datos, examinarlos en contexto para detectar problemas e implementar soluciones específicas para el problema encontrado.

En la actualidad, es una parte importante de muchas estrategias de seguridad cibernética, y las empresas están invirtiendo cada vez más en tecnologías y soluciones de inteligencia de amenazas para mejorar su postura de seguridad.

De acuerdo con (CIBERCI, 2022), entre algunos de los beneficios que ofrece Threat Intelligence tenemos:

- Disminuir los riesgos de los ataques conocidos.
- Mejorar la eficiencia de nuestros equipos de seguridad.
- Mejora de la eficacia de las medidas de seguridad
- Identificación temprana de amenazas
- Análisis de riesgos
- Respuesta rápida en tiempo real sobre ataques
- Reducción del riesgo de pérdida de datos
- Ahorro de costos

2.2. Ciclo de Vida –Threat Intelligence (Inteligencia de Amenazas)

De acuerdo con (Equipo Flaspoint, 2021), el ciclo de vida de la inteligencia de amenazas es un marco fundamental para todos los programas de fraude, físicos y de ciberseguridad, ya sean maduros y sofisticados en sus operaciones, o simplemente aspirantes.

Según (Daniele, 2021) en su artículo como consultor de DNC, pretende compartir formas específicas en que las técnicas analíticas de inteligencia cibernética y los métodos de recopilación pueden integrarse en procesos de inteligencia más amplios.

Por lo tanto, podemos decir que Threat Intelligence se enfoca en la identificación y análisis de amenazas en general, ya sean físicas, financieras, políticas, entre otras. Puede incluir información sobre amenazas cibernéticas, pero también puede incluir información sobre otras amenazas que puedan afectar a una organización, como el robo de identidad, el fraude financiero, la competencia desleal, entre otros. En la Figura 6 y visualiza las fases de su ciclo de vida.

Figura 6 - Ciclo de Vida

El ciclo de vida de la inteligencia se divide en cinco fases, mismas que se explican a continuación:

Fase del ciclo de vida	**Descripción**
1. ***Recopilación de datos***	En esta fase, se recopilan los datos necesarios para el análisis de inteligencia de amenazas. Los datos pueden provenir de fuentes internas, como registros de red y eventos de seguridad, así como de fuentes externas, como feeds de inteligencia de amenazas y sitios de intercambio de información de seguridad.
2. ***Procesamiento y análisis***	En esta fase, se procesan los datos recopilados y se analizan para identificar patrones y tendencias. Esto puede incluir la eliminación de datos irrelevantes o duplicados, la correlación de eventos y la identificación de indicadores de compromiso (IoC).
3. ***Generación de informes***	En esta fase, se elaboran informes que resumen los hallazgos del análisis de inteligencia de amenazas. Estos informes pueden incluir información sobre amenazas específicas, tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios, y recomendaciones para mejorar la postura de seguridad de la organización.
4. ***Diseminación de información***	En esta fase, se comparten los informes de inteligencia de amenazas con las partes interesadas, como los equipos de seguridad de la organización, proveedores de servicios de seguridad gestionada (MSSP) y otros organismos de seguridad.
5. ***Retroalimentación y mejora***	En esta fase, se recopila información sobre la efectividad de la inteligencia de amenazas para mejorar las fases anteriores del ciclo de vida. Esto puede incluir la revisión de los procedimientos de recopilación y análisis de datos, la evaluación de la calidad de los informes generados y la identificación de nuevas fuentes de inteligencia de amenazas.

Tabla 2: Fases Ciclo de Vida
Fuente: Elaboración propia

Es importante destacar que este ciclo de vida puede variar según la metodología utilizada y las necesidades específicas de cada organización.

Además, es se debe mencionar que el ciclo de vida de Threat Intelligence también incluye la evaluación y mejora continua. Esto significa que después de la implementación de las estrategias de inteligencia de amenazas, se debe evaluar su efectividad y realizar ajustes y mejoras para asegurarse de que estén cumpliendo con los objetivos establecidos.

2.3. Desarrollos en el campo de Threat Intelligence

Una vez conocido el ciclo de vida, podemos mencionar, algunos de los desarrollos recientes en el campo de la inteligencia de amenazas:

- **Integración de inteligencia artificial y aprendizaje automático:** la inteligencia de amenazas está utilizando cada vez más tecnologías de inteligencia artificial y aprendizaje automático para procesar grandes cantidades de datos de amenazas y automatizar la identificación de patrones y comportamientos maliciosos.

- I**nteligencia de amenazas basada en la nube:** muchas soluciones de inteligencia de amenazas ahora se ofrecen como servicios en la nube, lo que permite a las empresas acceder a la inteligencia de amenazas en tiempo real y sin la necesidad de hardware y software adicionales.

- **Colaboración y compartición de información de amenazas:** las empresas están comenzando a colaborar y compartir información de amenazas entre sí para mejorar la identificación y respuesta a las amenazas.

- **Inteligencia de amenazas centrada en el usuario:** los atacantes están cada vez más enfocados en los usuarios finales como el punto de entrada a una organización, lo que ha llevado al desarrollo de soluciones de inteligencia de amenazas centradas en el usuario para detectar y prevenir ataques dirigidos a los usuarios.

Como se puede apreciar, la inteligencia de amenazas es una parte fundamental de la estrategia de seguridad cibernética y se está desarrollando constantemente para hacer frente a las amenazas en línea cada vez más sofisticadas y peligrosas.

2.4. Ámbito del Threat Intelligence

Dentro del ámbito de Threat Intelligence, existen varias subáreas que se enfocan en diferentes aspectos del análisis de amenazas. Algunas de estas son:

- **Análisis de inteligencia de amenazas:** se enfoca en la recolección, procesamiento y análisis de información sobre amenazas y actores maliciosos. Incluye la identificación de patrones y tendencias, así como la evaluación de la credibilidad y relevancia de la información.

- **Análisis de vulnerabilidades:** se orienta en el análisis de sistemas y aplicaciones para identificar vulnerabilidades y debilidades que puedan ser explotadas por los atacantes.

- **Análisis de malware:** identifica y analiza software malicioso, incluyendo virus, troyanos, gusanos y otros tipos de malware.

- **Análisis de incidentes de seguridad:** apunta a la investigación de incidentes de seguridad, incluyendo la identificación de los actores involucrados, los vectores de ataque y el impacto en el sistema afectado.

- **Análisis de inteligencia de amenazas cibernéticas:** está encaminado a la recolección, procesamiento y análisis de información específica sobre amenazas en el ámbito de la ciberseguridad, como ataques a redes y sistemas.

- **Análisis de inteligencia de amenazas físicas:** se enfoca en la recolección, procesamiento y análisis de información sobre amenazas físicas, como ataques terroristas, robos y otros tipos de violencia física.

Cada subárea requiere habilidades y conocimientos específicos, y juntas conforman el panorama completo del análisis de amenazas y la inteligencia de seguridad.

2.5. Casos de éxito:

Asi mismo, el threat intelligence ha logrado varios éxitos en la identificación y prevención de amenazas cibernéticas y físicas como, por ejemplo:

- **Identificación** de grupos de hackers y actores maliciosos: mediante la recopilación y análisis de información, se han identificado varios grupos de hackers y actores maliciosos que operan en la web oscura y en la red abierta, lo que ha permitido a las organizaciones tomar medidas preventivas y defenderse contra futuros ataques.

- **Prevención** de ataques cibernéticos: ha permitido a las organizaciones prevenir o minimizar el impacto de ataques cibernéticos mediante la identificación de vulnerabilidades, la implementación de medidas de seguridad adicionales y la detección temprana de actividades sospechosas.

- Identificación y prevención de **amenazas físicas**: ha ayudado en la identificación y prevención de amenazas físicas, como ataques terroristas, robos y otros tipos de violencia física, a través de la vigilancia, el monitoreo y la recolección de información.

- **Respuesta** rápida a incidentes de seguridad: ha proporcionado una respuesta más rápida y eficiente a los incidentes de seguridad, reduciendo el tiempo de inactividad y minimizando el impacto en las operaciones comerciales.

- Identificación de **nuevas amenazas**: ha permitido la identificación temprana de nuevas amenazas y vulnerabilidades emergentes, lo que ha permitido a las organizaciones prepararse y tomar medidas preventivas antes de que se produzcan ataques.

Por lo cual, el threat intelligence ha sido fundamental para mejorar la seguridad de las organizaciones y reducir los riesgos de los ciberataques y las amenazas físicas.

2.6. Problemática:

A medida que la amenaza cibernética continúa evolucionando, también lo hacen los problemas a los que se enfrenta la inteligencia de amenazas, algunos de los problemas más importantes que se están trabajando actualmente en el campo de la inteligencia de amenazas son:

- La falta de **estándares** comunes: actualmente no hay un conjunto común de estándares para la inteligencia de amenazas, lo que dificulta la colaboración y el intercambio de información entre las organizaciones.

- La **sobrecarga** de información: con la cantidad de información de amenazas que se genera diariamente, muchas organizaciones luchan por procesar y utilizar de manera efectiva la información relevante.

- La falta de **habilidades** y **experiencia**: la inteligencia de amenazas requiere habilidades especializadas y experiencia en la recopilación, análisis e interpretación de datos, lo que puede ser difícil de encontrar en un mercado laboral competitivo.

- La **complejidad** de las amenazas: las amenazas cibernéticas están cada vez más sofisticadas y pueden ser difíciles de detectar y mitigar, lo que aumenta la importancia de contar con una inteligencia de amenazas efectiva.

- La necesidad de **automatización**: para hacer frente a la sobrecarga de información y la complejidad de las amenazas, es necesario contar con soluciones de inteligencia de amenazas que puedan automatizar gran parte del proceso de detección y respuesta a las amenazas.

Se evidencia que día a día sigue enfrentando desafíos significativos a medida que las amenazas cibernéticas continúan evolucionando. Las organizaciones deben trabajar para abordar estos problemas y mejorar su capacidad para detectar y mitigar las amenazas en línea.

2.7. Posibles aplicaciones:

La inteligencia de amenazas tiene una amplia gama de aplicaciones potenciales en la ciberseguridad y puede ayudar a las organizaciones a mejorar su postura de seguridad y protegerse contra las amenazas en línea. A continuación, podemos citar algunos casos:

- Detección y respuesta de **amenazas**: puede ayudar a las organizaciones a detectar y responder rápidamente a las amenazas de seguridad, proporcionando información actualizada sobre las amenazas actuales y potenciales.

- Identificación de **vulnerabilidades**: puede ser empleada para identificar posibles vulnerabilidades en la infraestructura de una organización y ayudar a priorizar la mitigación de esas vulnerabilidades.

- Análisis de **riesgos**: puede favorecer a las organizaciones para evaluar el riesgo potencial de nuevas amenazas y tomar medidas proactivas para mitigar ese riesgo.

- Monitoreo de la **reputación** en línea: puede ser utilizada para monitorear la actividad maliciosa en línea que pueda afectar la reputación de una organización, como la divulgación de información confidencial o las críticas en redes sociales.

- Investigación de **incidentes**: puede ser destinada para investigar y gestionar incidentes de seguridad y proporcionar información en tiempo real sobre las amenazas y los ataques en curso como determinar el origen y el alcance de una brecha de seguridad.

- Protección de la **cadena de suministro**: puede ser adoptada para evaluar el riesgo de la cadena de suministro y ayudar a las organizaciones a protegerse contra posibles amenazas de seguridad.

2.8. Software para Threat Intelligence:

Las siguientes plataformas son solo algunos ejemplos de las muchas opciones disponibles entre software de pago y open-source:

- **IBM X-Force Exchange:** Es una plataforma que proporciona información actualizada sobre vulnerabilidades, malware y otros riesgos de seguridad. Es un producto privado de IBM.

- **MISP** (Plataforma de Compartición de Información de Amenazas): Es una herramienta de código abierto que permite a los analistas de seguridad compartir y colaborar en información de amenazas.

- **VirusTotal**: Es una plataforma de análisis de malware que utiliza múltiples motores de análisis de malware para identificar y analizar archivos sospechosos. Ofrece una API para la integración con otras herramientas.

- **Shodan**: Es un motor de búsqueda que permite a los usuarios buscar dispositivos en línea y sus vulnerabilidades asociadas. Tiene una API que permite la integración con otras herramientas.

- **OpenCTI**: Es una plataforma de inteligencia de amenazas de código abierto que permite a los analistas de seguridad recopilar, gestionar y compartir información de amenazas.

- **Maltiverse**: Es una plataforma que utiliza técnicas de análisis de datos para correlacionar y analizar información de amenazas. Ofrece una API para la integración con otras herramientas.

Es importante investigar y probar diferentes herramientas para encontrar la que mejor se adapte a las necesidades y presupuesto de la empresa. Sin embargo, la propuesta va enfocada en el estudio inicial de **OpenCTI.**

2.9. Hardware para Threat Intelligence:

Asi mismo, existen varios tipos de hardware que pueden estar relacionados con la inteligencia de amenazas (threat intelligence), incluyendo:

- Sistemas de detección y prevención de intrusiones (**IDS/IPS**): estos sistemas utilizan hardware especializado para inspeccionar el tráfico de red en busca de patrones de comportamiento maliciosos y pueden bloquear los ataques en tiempo real.

- Dispositivos de **seguridad perimetral**: estos dispositivos, como los firewalls de próxima generación, también utilizan hardware especializado para inspeccionar el tráfico de red y proteger los sistemas de posibles ataques.

- Sistemas de **análisis de registro**: estos sistemas utilizan hardware especializado para recopilar, almacenar y analizar grandes cantidades de registros de eventos, como registros de seguridad de sistemas, registros de red, registros de aplicaciones, etc.

- Sistemas de **gestión de amenazas**: estos sistemas pueden utilizar hardware especializado para analizar grandes cantidades de datos de amenazas y generar informes de inteligencia de amenazas para ayudar a las organizaciones a protegerse de los posibles ataques.

Con esto queremos decir que, cualquier hardware relacionado con la inteligencia de amenazas que pueda ayudar a las organizaciones a detectar, prevenir o responder a los ataques de seguridad; siempre será muy importante para conseguir el objetivo deseado.

3. Estudio de OpenCTI

3.1. Qué es OpenCTI:

De acuerdo con (Filigran, 2022) OpenCTI es una plataforma de código abierto que permite a las organizaciones administrar sus conocimientos y observables de inteligencia de amenazas cibernéticas. Ha sido creado con el fin de estructurar, almacenar, organizar y visualizar información técnica y no técnica sobre amenazas cibernéticas.

El objetivo es crear una herramienta integral que permita a los usuarios capitalizar información técnica (como TTP y observables) y no técnica (como atribución sugerida, victimología, etc.) mientras vincula cada pieza de información a su fuente primaria (un informe, un evento MISP, etc.), con características tales como enlaces entre cada información, primeras y últimas fechas vistas, niveles de confianza, etc. La herramienta puede utilizar el marco MITRE ATT&CK (a través de un conector dedicado) para ayudar a estructurar los datos. El usuario también puede optar por implementar sus propios conjuntos de datos. En la figura 8, se muestra la interfaz de la plataforma OpenCTI.

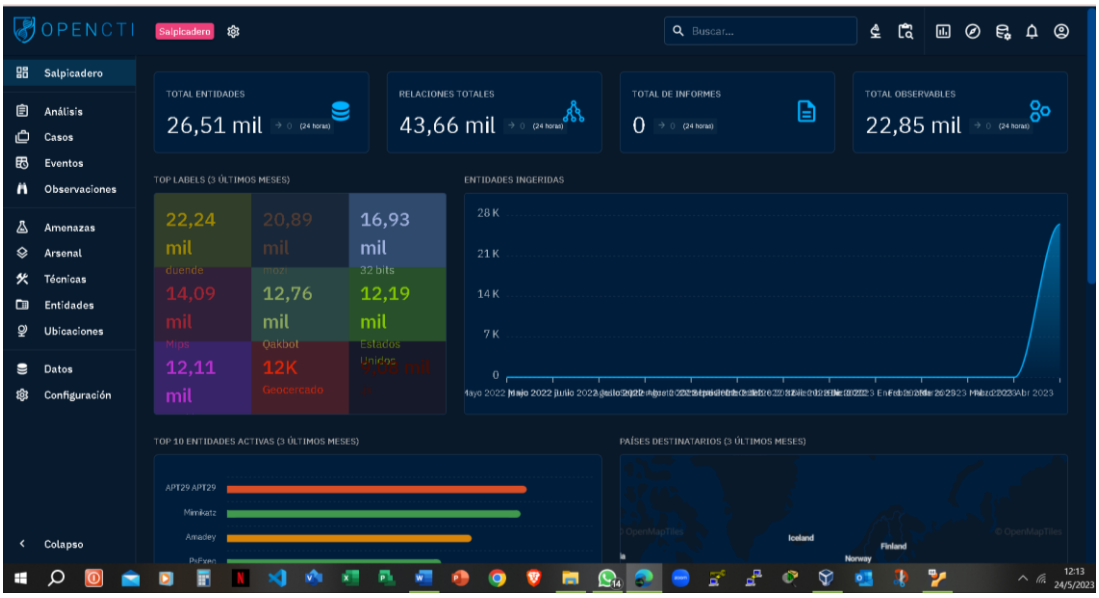


Figura 7: Dashboard OpenCTI

Una vez que los datos han sido capitalizados y procesados por los analistas dentro de OpenCTI, se pueden inferir nuevas relaciones de las existentes para facilitar la comprensión y la representación de esta información. Esto permite al usuario extraer y aprovechar el conocimiento significativo de los datos sin procesar.

OpenCTI no solo permite importar sino también exportar datos bajo diferentes formatos (CSV, paquetes STIX2, etc.). Los conectores se desarrollan actualmente para acelerar las interacciones entre la herramienta y otras plataformas.

3.2 Principales capacidades y características

De acuerdo al contexto que se menciona en la plataforma OpenCTI para la gestión de amenazas cibernéticas en la organización (OpenCTI, 2021). A continuación, se muestra una tabla donde se presenta las principales características y capacidades de OpenCTI:

Característica/Capacidad	**Descripción**
Fuente de datos múltiples	OpenCTI puede recopilar y procesar datos de múltiples fuentes, incluyendo feeds de inteligencia de amenazas, registros de eventos de seguridad y fuentes internas de la organización.
Procesamiento y enriquecimiento de datos	OpenCTI puede procesar y enriquecer los datos recopilados, normalizar diferentes formatos de datos y enriquecerlos con información adicional, como la reputación de direcciones IP o dominios y geolocalización.
Motor de búsqueda avanzado	OpenCTI utiliza tecnologías de búsqueda avanzadas, como Apache Solr o Elasticsearch, para proporcionar una búsqueda rápida y precisa de los datos.
Análisis de amenazas avanzado	OpenCTI puede analizar y clasificar diferentes tipos de amenazas, incluyendo malware, phishing y otros vectores de ataque.
Visualización y análisis de datos	OpenCTI proporciona interfaces gráficas de usuario personalizables para visualizar y analizar los datos de inteligencia de amenazas, como paneles de control y gráficos de red.

Integración con otras herramientas de seguridad	OpenCTI se integra con otras herramientas de seguridad, como SIEM, plataformas de automatización de seguridad y herramientas de gestión de vulnerabilidades.
Arquitectura modular y escalable	La arquitectura modular y escalable de OpenCTI permite una fácil integración con diferentes componentes y la capacidad de escalar horizontalmente para manejar grandes volúmenes de datos.
Licencia de código abierto	OpenCTI se distribuye bajo la licencia de código abierto Apache 2.0, lo que significa que es de uso gratuito y puede ser modificado y distribuido por la comunidad de desarrolladores.

Tabla 3: Características OpenCTI
Fuente: Elaboración propia

3.3 ¿Qué posibilidades ofrece la plataforma OpenCTI?

La plataforma OpenCTI es una herramienta de inteligencia de amenazas de código abierto que entre algunas de las posibilidades que ofrece esta plataforma son:

- **Recopilación y gestión** de inteligencia de amenazas: permite a los usuarios recopilar información sobre amenazas, vulnerabilidades y riesgos de diferentes fuentes, como feeds de inteligencia de amenazas, bases de datos de vulnerabilidades y feeds RSS.

- **Análisis y correlación** de datos: La plataforma permite a los usuarios analizar y correlacionar datos para identificar patrones y tendencias en las amenazas de seguridad. También ofrece herramientas de visualización de datos para ayudar a los usuarios a entender y presentar los hallazgos de forma clara y concisa.

- **Compartir** información de inteligencia de amenazas: como indica el nombre, permite a los usuarios compartir información de inteligencia de amenazas de forma segura y controlada con otros miembros de su equipo o con la comunidad más amplia de inteligencia de amenazas. Esto ayuda a mejorar la colaboración y la toma de decisiones.

- **Automatización** de tareas: La plataforma también ofrece herramientas de automatización que permiten a los usuarios automatizar tareas repetitivas y ahorrar tiempo. Por ejemplo, se pueden crear reglas para automatizar la recopilación de información de inteligencia de amenazas a partir de ciertos feeds o fuentes.

Como se indica, brinda una amplia gama de posibilidades, lo que beneficia en la mejora de seguridad de una organización y a prevenir posibles ciberataques.

3.4. Arquitectura OpenCTI

La plataforma OpenCTI depende de varias bases de datos y servicios externos para funcionar.

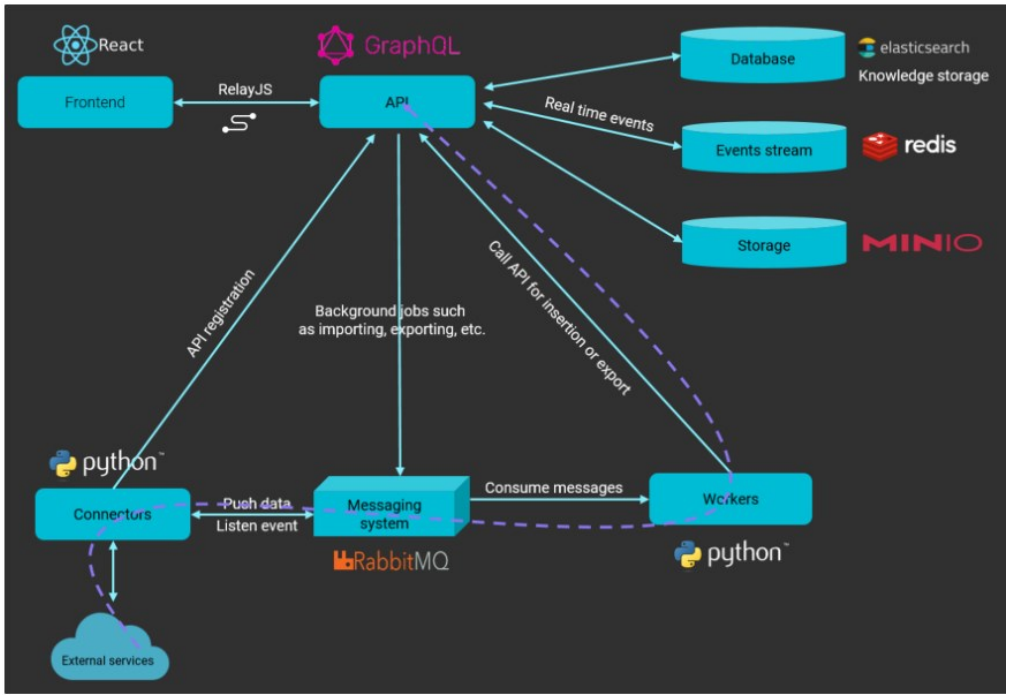


Figura 8: Arquitectura OpenCTI

La arquitectura de OpenCTI es altamente modular y escalable, lo que permite a los analistas de seguridad personalizar la plataforma según sus necesidades específicas y expandirla a medida que sus requisitos cambien. Además, como plataforma de código abierto, OpenCTI es una herramienta valiosa para la comunidad de seguridad cibernética, que puede contribuir con nuevas funcionalidades y mejorar la plataforma en general.

Los componentes de la plataforma están diseñados para trabajar juntos de manera efectiva y proporcionar una solución completa para la inteligencia de amenazas cibernéticas. A continuación, mencionamos rápidamente su función:

- **API GraphQL**

  La API es la parte central de la plataforma OpenCTI, permitiendo a los clientes (incluyendo el frontend) interactuar con la base de datos y el broker

(sistema de mensajería). Construido en NodeJS, implementa el lenguaje de consulta GraphQL. Como la API aún no está completamente documentada, puedes explorar los métodos y parámetros disponibles a través de un playground GraphQL.

- **Workers**

Los workers son procesos Python independientes que consumen mensajes del broker RabbitMQ para realizar consultas de escritura asíncronas. Puede lanzar tantos workers como necesite para aumentar el rendimiento de escritura. En algún momento, el rendimiento de escritura estará limitado por el rendimiento de la base de datos (Elasticsearch), si no tienes el rendimiento esperado con 3 o 4 trabajadores, entonces será inútil lanzar más y tendrás que pensar en mejorar el hardware de los nodos de la base de datos (o ampliar tu configuración a un clúster).

- **Conectores**

Los conectores son piezas de software de terceros (procesos Python) que pueden desempeñar cuatro funciones diferentes en la plataforma:

Tipo	Descripción	Ejemplo
EXTERNAL_IMPORT	Extraer datos de fuentes remotas, convertirlos a STIX2 e insertarlos en la plataforma OpenCTI.	MITRE, MISP, CVE, AlienVault, FireEye, etc.
INTERNAL_IMPORT_FILE	Extraer datos de archivos cargados en OpenCTI a través de la interfaz de usuario o la API.	Extracción de indicadores a partir de PDF, importación de STIX2, etc.
INTERNAL_ENRICHMENT	Escucha de nuevas entidades OpenCTI o solicitudes de usuarios, extrae datos de fuentes remotas para enriquecerlos.	Enriquecimiento de observables mediante servicios externos, actualización de entidades, etc.
INTERNAL_EXPORT_FILE	Generar exportaciones a partir de los datos de OpenCTI, basándose en el listado de entidades o en una entidad y sus relaciones.	Exportación STIX2, exportación PDF, generación de listas CSV, etc.
STREAM	Consumir el flujo de datos de la plataforma	Historial, Sincronizador, Tanium, etc.

Tabla 4: Funciones de los conectores

Los principales componentes de la arquitectura de OpenCTI se muestra en la siguiente tabla 5:

Componente	Descripción	Características	Ejemplo
Recolector de datos	Recopila datos de diversas fuentes, como feeds de inteligencia de	▪ Admite múltiples fuentes de datos, incluyendo feeds RSS, STIX/TAXII,	▪ Feeds de inteligencia de amenazas: se pueden agregar feeds de

	amenazas, registros de eventos de seguridad y otros datos relevantes. El recolector de datos es altamente configurable y se puede personalizar según las necesidades específicas del usuario.	Syslog, entre otros. ▪ Permite la configuración de múltiples recolectores para manejar diferentes fuentes de datos. ▪ Incluye mecanismos de filtrado y de duplicación de datos.	diferentes proveedores y fuentes, como VirusTotal, Abuse.ch, Spamhaus, etc. ▪ Registros de eventos de seguridad: pueden recopilarse datos de logs de servidores, firewalls, sistemas de detección de intrusiones (IDS), entre otros. ▪ Fuentes internas de la organización: la plataforma puede recolectar datos de fuentes internas como registros de sistemas de información, correos electrónicos, entre otros.
Procesador de datos	Como tal procesa los datos recopilados y los enriquece con información adicional, como la reputación de las direcciones IP o los dominios, la ubicación geográfica y otra información contextual. También se encarga de normalizar los datos y de	▪ Admite múltiples fuentes de datos, incluyendo feeds RSS, STIX/TAXII, Syslog, entre otros. ▪ Incluye herramientas para normalizar y transformar los datos en diferentes formatos. ▪ Admite la integración de herramientas de análisis de datos y de	▪ Normalización de datos: se pueden transformar diferentes formatos de datos en un formato común para ser almacenados en la base de datos. ▪ Enriquecimiento de datos: se pueden enriquecer los datos con información adicional, como la reputación de direcciones IP o

	asegurarse de que se almacenen de manera coherente en la base de datos.	enriquecimiento de información.	dominios, geolocalización, entre otros. ▪ Detección de amenazas: se pueden identificar patrones y comportamientos sospechosos en los datos para detectar posibles amenazas.
Base de datos	Es el componente central de la plataforma y almacena los datos procesados y enriquecidos. La base de datos está diseñada para ser escalable y puede manejar grandes volúmenes de datos.	▪ Utiliza una base de datos NoSQL para manejar grandes volúmenes de datos. ▪ Admite la replicación y distribución de datos para mejorar la escalabilidad y la disponibilidad. ▪ Proporciona mecanismos de seguridad y acceso para proteger los datos almacenados.	▪ Uso de bases de datos NoSQL: se pueden usar tecnologías de bases de datos NoSQL como MongoDB, Cassandra o Elasticsearch para almacenar grandes volúmenes de datos y realizar búsquedas y análisis rápidos. ▪ Escalabilidad: se puede escalar la base de datos horizontalmente mediante la adición de nodos para manejar un mayor volumen de datos.
Motor de búsqueda	Permite a los analistas de seguridad buscar y recuperar datos de la base de datos. Este motor utiliza tecnologías de indexación avanzadas para proporcionar resultados de	▪ Utiliza un motor de búsqueda de texto completo para permitir búsquedas rápidas y precisas. ▪ Admite la indexación de diferentes tipos de datos, como texto, fechas,	▪ Uso de tecnologías de búsqueda: se pueden utilizar tecnologías de búsqueda avanzadas, como Apache Solr o Elasticsearch, para proporcionar una búsqueda rápida

	búsqueda rápidos y precisos.	ubicaciones, entre otros. ▪ Proporciona mecanismos de consulta avanzados, como búsqueda por proximidad y búsqueda por facetas.	y precisa de los datos. ▪ Indexación: se puede indexar los datos para permitir una búsqueda rápida y fácil.
Analizador de amenazas	Analiza los datos de inteligencia de amenazas y los clasifica en categorías como phishing, malware, exploits y otras amenazas. También utiliza técnicas de análisis de redes para identificar patrones y relaciones entre los datos de amenazas.	▪ Utiliza herramientas de análisis de datos y de machine learning para identificar patrones y comportamientos anómalos. ▪ Proporciona capacidades de correlación de datos para identificar relaciones entre diferentes amenazas. ▪ Admite la integración de herramientas de análisis y de visualización de datos.	▪ Análisis de malware: se puede utilizar técnicas de análisis de malware para detectar y clasificar diferentes tipos de malware. ▪ Detección de phishing: se pueden identificar y clasificar correos electrónicos y sitios web de phishing utilizando técnicas de análisis de contenido.
Visualizador	Proporciona interfaces gráficas de usuario para visualizar y analizar los datos de inteligencia de amenazas. El visualizador es altamente personalizable y se puede configurar según las necesidades	▪ Proporciona una interfaz de usuario intuitiva y fácil de usar. ▪ Admite la visualización de diferentes tipos de datos, como mapas, gráficos y tablas. ▪ Proporciona capacidades de análisis y de filtrado de datos para permitir a los analistas de seguridad	▪ Paneles de control: se pueden crear paneles de control personalizados para visualizar los datos de amenazas de una manera fácil de entender. ▪ Gráficos de red: se pueden crear gráficos de red para visualizar las relaciones entre los

	específicas del usuario.	explorar y analizar los datos de manera eficiente.	diferentes datos de amenazas, como las relaciones entre los dominios, direcciones IP y sitios web.

Tabla 5: Componentes arquitectura OpenCTI

3.5. Arquitectura de Conectores

Como lo menciona (Papaioannou, 2021) para alimentar la plataforma OpenCTI, se necesitan varios conectores con el fin de que se puedan importar datos de diferentes fuentes.

Son un conjunto de herramientas y bibliotecas que se utilizan para integrar diferentes fuentes de inteligencia de amenazas en la plataforma de forma automatizada y modular, lo que permite una mayor eficiencia en la gestión de la inteligencia de amenazas.

Los conectores se encargan de enviar eventos a la plataforma, un evento puede ser cualquier tipo de información que se considere relevante para la inteligencia de amenazas, como indicadores de compromiso (**IOCs**), informes de incidentes, información de vulnerabilidades o cualquier otro tipo de información que se considere útil.

Esta arquitectura de conectores de OpenCTI se basa en un diseño modular y flexible que permite la integración con una amplia variedad de fuentes de datos y sistemas de seguridad. Los conectores se ejecutan como servicios en segundo plano y pueden ser programados para ejecutarse en intervalos regulares o en respuesta a eventos específicos.

Asi mismo, proporciona un conjunto de conectores integrados que se pueden utilizar para integrar fuentes de inteligencia de amenazas comunes, como VirusTotal, Shodan, MISP, etc. También es posible crear conectores personalizados utilizando una API sencilla.

Los conectores de OpenCTI utilizan diferentes métodos de autenticación y autorización para acceder a las fuentes de inteligencia de amenazas. Algunos conectores utilizan claves API o tokens de acceso, mientras que otros requieren credenciales de usuario y contraseña.

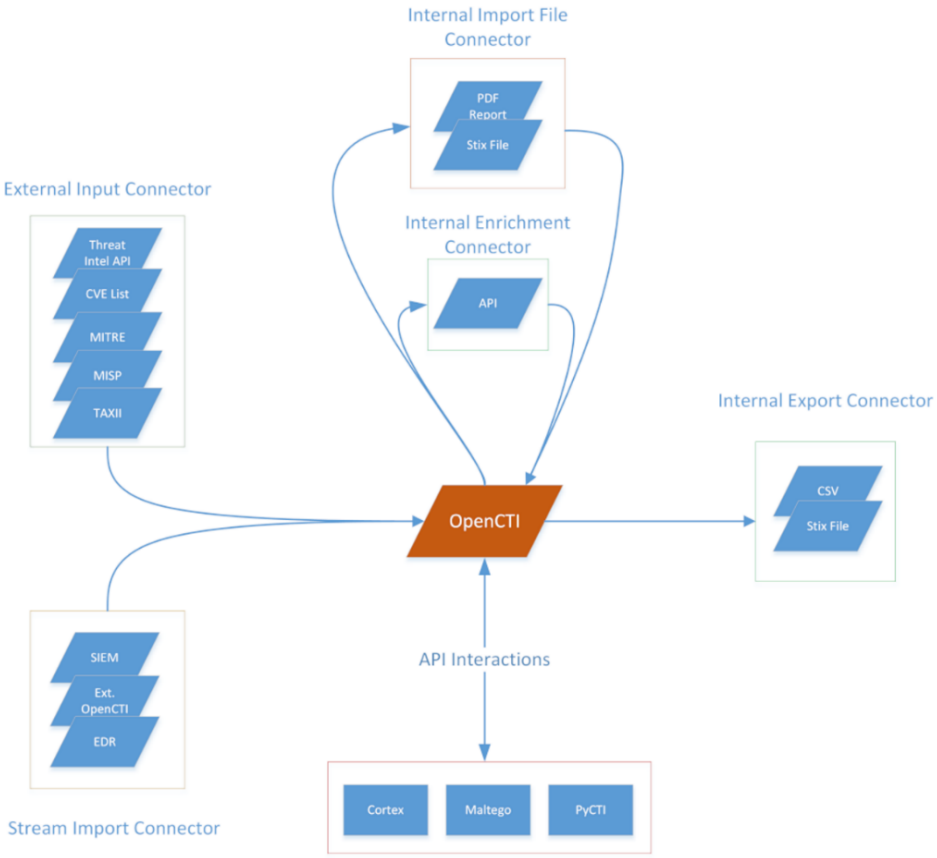


Figura 9: Arquitectura Conector

Los conectores se dividen en dos tipos principales: conectores de importación y conectores de exportación.

Los **conectores de importación** se utilizan para recopilar información sobre amenazas de seguridad de diferentes fuentes, como feeds de inteligencia de amenazas, registros de eventos de seguridad, sistemas de detección de intrusiones y otros sistemas de seguridad. Estos conectores se ejecutan en segundo plano y recopilan información de forma automática y continua.

Los **conectores de exportación**, por otro lado, se utilizan para enviar información sobre amenazas de seguridad a otros sistemas, como sistemas de detección de intrusiones, sistemas de análisis de vulnerabilidades, herramientas de respuesta a incidentes y otros sistemas de seguridad. Estos conectores permiten que la información recopilada en OpenCTI se comparta con otros sistemas de seguridad y se utilice para mejorar la detección y respuesta a amenazas.
Los conectores son la piedra angular de la plataforma OpenCTI y permiten a las organizaciones introducir, enriquecer o exportar fácilmente nuevos datos en la plataforma.

Según su funcionalidad y caso de uso, se clasifican en las siguientes clases:

- **Conector de entrada externo (External Input Connector)**
  Recupera automáticamente información de una entidad o servicio externo y la importa a OpenCTI.

- **Conector de entrada de flujo (Stream Input Connector)**
  Conecta con un flujo de datos e ingiere continuamente la información recuperada en OpenCTI. Cuando se utiliza en combinación con sistemas EDR como Tanium, el conector también puede responder al sistema de origen y convertirlo en una interacción bidireccional entre otro sistema y OpenCTI.

- **Conector de enriquecimiento interno (Internal Enrichment Connector)**
  Los SDO y SCO pueden enriquecerse utilizando servicios de búsqueda externos para aumentar el conocimiento de ese objeto en OpenCTI. Un ejemplo sería la búsqueda whois de una dirección IP.

- **Conector interno de importación de archivos (Internal Import File Connector)**
  La información de un archivo cargado puede extraerse e introducirse en OpenCTI. Algunos ejemplos son los archivos adjuntos a un informe o un archivo json (STIX2).

- **Conector interno de exportación (Internal Export Connector)**
  La información almacenada en OpenCTI puede extraerse a diferentes formatos de archivo como .csv o .json (STIX 2).

Estos conectores deben iniciarse con un usuario que tenga un rol de "Administrador" (con todas las capacidades de bypass habilitadas).

3.5.1. Interacciones API

Las interacciones API no son conectores por definición, sin embargo, permiten a un script o a un programa interactuar con OpenCTI utilizando una biblioteca cliente.

Procesamiento de la información

En la figura 11, se muestra todos los datos que el conector desea enviar a OpenCTI deben convertirse en un objeto STIX2, que se enviará a través de un sistema de mensajería al worker de OpenCTI.

El worker se encarga de gestionar los errores y el rendimiento, así como de interactuar con la interfaz API de OpenCTI para crear o actualizar los objetos correspondientes.

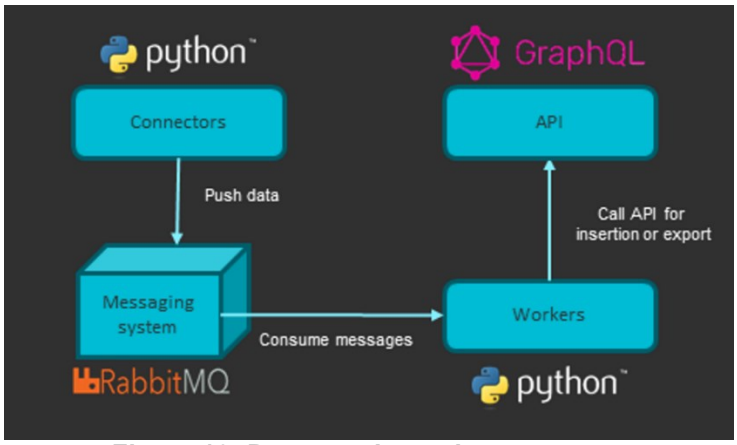


Figura 10: Procesamiento de conectores

Algunos de los conectores que podrían ser necesarios se indica a continuación:

CONECTOR	DESCRIPCION
STIX/TAXII Connector	Este conector es esencial para importar datos de amenazas de fuentes que utilizan el formato de intercambio de amenazas STIX (Structured Threat Information Expression) y el protocolo de intercambio TAXII (Trusted Automated eXchange of Indicator Information).
MISP Connector	Este conector es necesario para importar datos de amenazas de la plataforma MISP (Malware Information Sharing Platform), que es una plataforma de código abierto para compartir información sobre amenazas.
Vulnerability Scanner Connector	Indispensable para importar datos de escáneres de vulnerabilidades, como Nessus o Qualys, que pueden proporcionar información sobre vulnerabilidades en sistemas y aplicaciones.
SIEM Connector	Esencial para importar datos de eventos de seguridad de un SIEM (Security Information and Event Management), como Splunk, LogRhythm, ArcSight, entre otros.
Threat Intelligence Feeds Connector	Primordial para importar feeds de inteligencia de amenazas de diferentes proveedores, como Recorded Future, FireEye, y otras.
TheHive	TheHive es una plataforma de gestión de incidentes de seguridad de código abierto que permite a los analistas colaborar en tiempo real, crear casos desde múltiples fuentes y analizar observables mediante el uso de analizadores de terceros.

Tabla 6: Tipos de Conectores

La arquitectura de conectores de OpenCTI se basa en una estructura de plug-in, lo que significa que se pueden agregar nuevos conectores de forma fácil y rápida, esto permite que la plataforma sea altamente personalizable y adaptable a las necesidades de cada organización.

En síntesis, los conectores mínimos necesarios para "alimentar" la plataforma OpenCTI dependerán de las fuentes de datos que se quieran integrar. Sin embargo, los conectores mencionados anteriormente son algunos de los conectores más comunes que se necesitan para importar datos de amenazas de diferentes fuentes.

4. Estudio de TheHive

4.1. Qué es TheHive

Según (TheHive, 2021) es una plataforma de gestión de incidentes y casos de seguridad, diseñada para ayudar a los equipos de seguridad a detectar, investigar y responder a incidentes de seguridad de manera eficiente y efectiva.

Es una herramienta de código abierto que permite a los usuarios crear casos, agregar observables (como direcciones IP, nombres de dominio y hashes de archivos) y colaborar en tiempo real con otros miembros del equipo de seguridad. Ofrece integraciones con otras herramientas de seguridad como **MISP, Cortex y otras**, lo que permite una automatización avanzada y una mayor eficiencia en la gestión de incidentes. Como se observa en la figura 12.

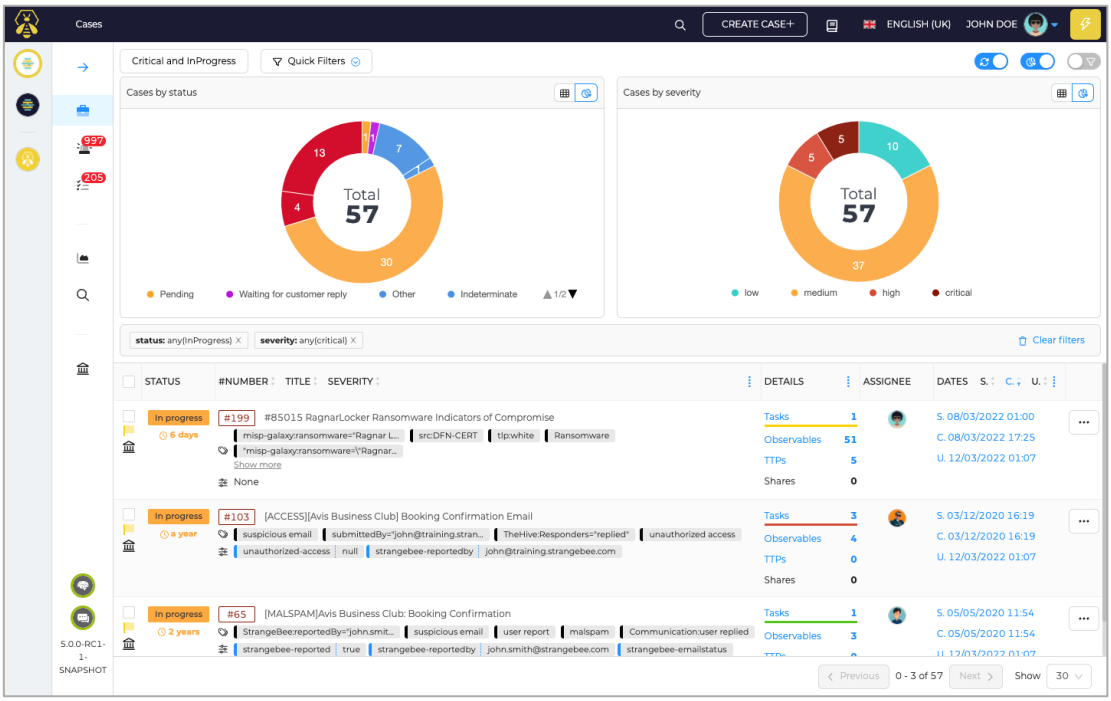


Figura 11: Interfaz TheHive

Podemos señalar que es una plataforma escalable de respuesta a incidentes de seguridad 3 en 1 y gratuita, diseñada para facilitar la vida de los **SOC, CSIRT, CERT** y cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que deben investigarse y actuar rápidamente. Es el compañero perfecto para MISP. Puede sincronizarlo con una o varias instancias MISP para iniciar investigaciones a partir de eventos MISP. También puede exportar los resultados de una investigación como un evento MISP para ayudar a sus compañeros a detectar y reaccionar ante los ataques con los que ha tratado.

Por ejemplo, cuando **TheHive** se usa junto con **Cortex**, los analistas e investigadores de seguridad pueden analizar fácilmente decenas, si no cientos de observables como se indican a continuación:

- **Colaborar:** TheHive permite que múltiples analistas trabajen en el mismo caso simultáneamente y en tiempo real utilizando la transmisión en vivo.

- **Elaborar:** Cada investigación en TheHive corresponde a un caso que se puede crear desde cero o importar desde eventos MISP, alertas SIEM, informes por correo electrónico y otras fuentes de eventos de seguridad. Los casos se pueden dividir en una o más tareas, que se pueden asignar a analistas específicos y se pueden crear plantillas de casos para automatizar tareas tediosas.

- **Analizar:** Los usuarios pueden agregar observables a cada caso y previsualizar eventos MISP para decidir si justifican una investigación. Los observables también se pueden asociar con un TLP y la fuente que los proporcionó o generó utilizando etiquetas. Los analistas pueden utilizar analizadores de una o varias instancias Cortex para analizar los observables y los COI, y también pueden agregar sus propios analizadores de secuencias de comandos.

- **Panel de alertas:** TheHive tiene un panel de alertas que muestra alertas SIEM, phishing y otros correos electrónicos sospechosos y otros eventos de seguridad que se pueden previsualizar, importar a casos o ignorar. Los observables que ya se han visto en casos anteriores se identifican automáticamente, y los analistas pueden marcar fácilmente los observables como COI y aislarlos mediante una consulta de búsqueda.

4.1.1. Características principales

A continuación, se indica las principales características de TheHive:

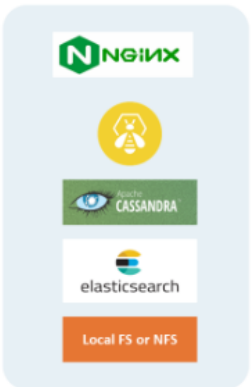
Característica	**Descripción**
Colaboración	Múltiples analistas de una organización pueden trabajar juntos en el mismo caso simultáneamente en tiempo real.
Creación de casos	Los casos se pueden crear desde cero o desde MISP eventos, alertas SIEM, informes por correo electrónico y cualquier otra fuente notable de eventos de seguridad.
Creación de tareas	Cada caso se puede dividir en una o más tareas, que pueden ser creadas de forma individual o mediante plantillas predefinidas.
Asignación de tareas	Cada tarea puede ser asignada a un analista determinado o puede ser tomada por cualquier miembro del equipo.

Análisis de observables	TheHive permite agregar uno o cientos de observables a cada caso y utilizar analizadores de Cortex para analizarlos.
Integración con MISP	TheHive se integra con una o varias instancias MISP para previsualizar eventos y agregarlos a casos existentes o nuevos.
Panel de alertas	TheHive tiene un panel de alertas donde se pueden previsualizar, importar o ignorar eventos de seguridad, y donde los observables pueden ser marcados como COI y exportados para buscar en otras tiendas de datos.
Integración con Cortex	Los analizadores de Cortex permiten analizar decenas o cientos de observables con herramientas como DomainTools, Virus Total, PassiveTotal, Joe Sandbox y búsquedas de amenazas.
Personalización de analizadores	Los analistas pueden agregar sus propios analizadores a Cortex y personalizar su comportamiento de acuerdo con el nivel de confidencialidad del caso.

Tabla 7: Características TheHive

4.4.2. Arquitectura TheHive

Cada capa, la aplicación TheHive[4], el motor de base de datos e índice y el almacenamiento de archivos son independientes y se pueden configurar como un nodo o clúster independiente. Como resultado, TheHive podría configurarse y trabajar en una compleja arquitectura agrupada, utilizando direcciones IP virtuales y equilibradores de carga.



Todas las aplicaciones se instalan en el mismo servidor.

- Casandra
- Elasticsearch
- Los archivos se almacenan en el sistema de archivos (o MinIO si se desea)
- La Colmena
- NGINX (opcional): para gestionar las comunicaciones HTTPS

Figura 12: Arquitectura TheHive

[4] https://thehive-project.org/

Se puede instalar cada capa y nodo:

- En un sistema operativo dedicado
- Con otra aplicación (por ejemplo: 1 nodo de Cassandra con 1 no de Elasticseach)

La guía de instalación para construir un clúster de 3 nodos da todos los detalles para una configuración más compleja, cada uno de los cuales incluye:

- Cassandra como base de datos
- Elasticsearch como motor de indexación
- Almacenamiento de datos Minio S3
- TheHive
- Haproxy (para ilustrar un equilibrador de carga)
- Keepalived (para ilustrar la configuración de una IP virtual)

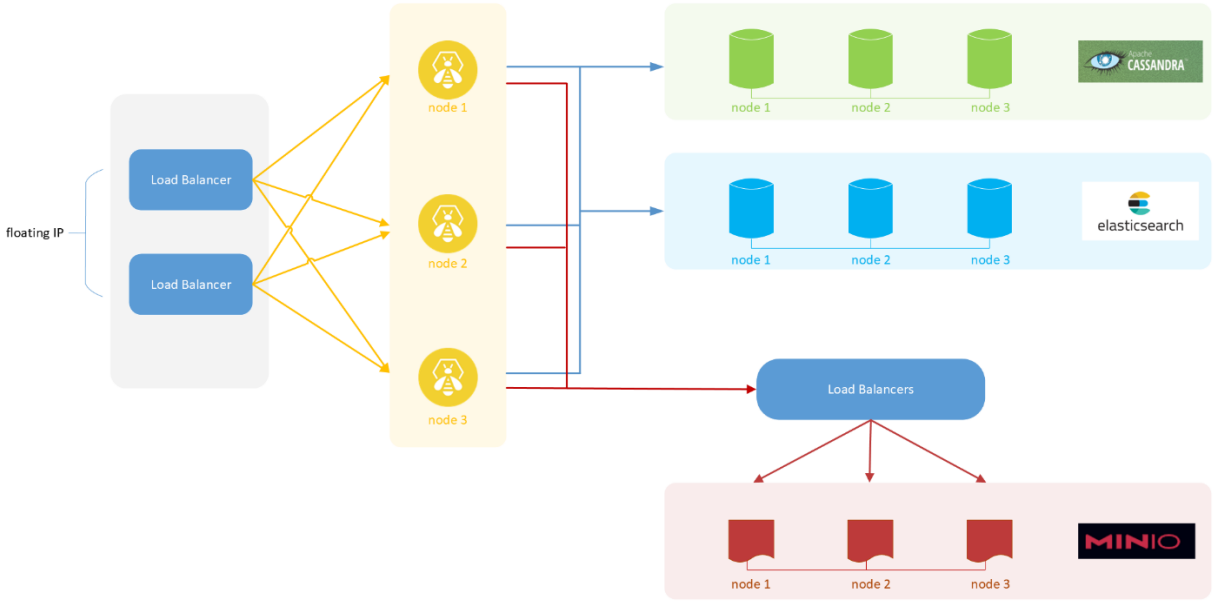


Figura 13: Arquitectura híbrida (clúster)

Todas estas aplicaciones se pueden instalar en su propio servidor o compartido en uno mismo, considerando configurar un clúster de 3 nodos activos de Cassandra con un factor de replicación de 3. Eso significa que todos los nodos están activos y los datos están presentes en cada nodo. Esta configuración es tolerante a un error de 1 nodo.

En este ejemplo, el clúster se compone de:

- 3 Nodos TheHive
- 3 Nodos Cassandra
- 3 Nodos de Elasticsearch
- 3 nodos Min.IO

En cuanto a los requisitos de hardware dependen del número de usuarios simultáneos (incluidas las integraciones) y de cómo utilizan el sistema. En la tabla siguiente se muestran los umbrales seguros al hospedar todos los servicios en el mismo equipo:

Número de usuarios	La Colmena	Casandra	ElasticSearch
< 10	2 / 2 GB	2 / 2 GB	2 / 2 GB
< 20	2-4 / 4 GB	2-4 / 4 GB	2-4 / 4 GB
< 50	4-6 / 8 GB	4-6 / 8 GB	4-6 / 8 GB

Tabla 8: Umbrales para hospedar servicios

La gama de integraciones es muy variada, si se necesita alguno en específico, existe un repositorio dedicado con todos los detalles y referencias conocidos, que se actualiza con frecuencia y se puede encontrar en su web oficial[5].

5. MITRE ATT&CK

5.1. El marco MITRE ATT&CK

MITRE ATT&CK [6](Adversarial Tactics, Techniques, and Common Knowledge) es un marco de trabajo de ciberseguridad que proporciona una estructura para describir tácticas, técnicas y procedimientos (TTP) utilizados por adversarios en el mundo real. Esta base de conocimiento se utiliza para desarrollar modelos y metodologías de amenazas específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

ATT&CK es accesible globalmente y se utiliza para comparar grupos adversarios, con otros grupos y con las defensas, para abordar algunos de los retos de la ciberseguridad. Los analistas y defensores pueden estructurar su información utilizando ATT&CK, lo que permite a los analistas estructurar la inteligencia sobre el comportamiento del adversario, y a los defensores estructurar la información sobre qué comportamiento pueden detectar y mitigar.

Es decir, es una herramienta útil para mejorar la capacidad de defensa en el ámbito de la ciberseguridad, en la siguiente Figura 14, se muestra la matriz ATT&CK para empresas:

[5] https://github.com/TheHive-Project/awesome.
[6] https://attack.mitre.org/

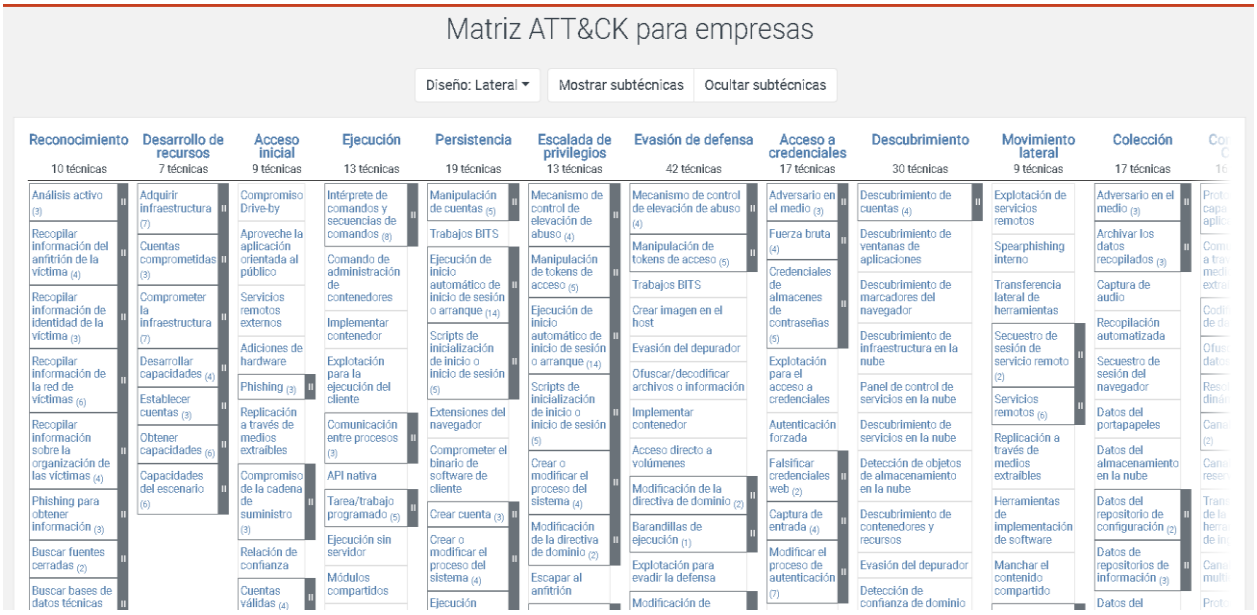


Figura 14: Matrix MITRE ATT&CK

5.2. Enfoque tradicional de inteligencia de amenazas cibernéticas

MITRE ATT&CK es una base de conocimiento globalmente accesible que describe tácticas y técnicas utilizadas por adversarios en el mundo real. Esta base de conocimiento es utilizada como fundamento para el desarrollo de modelos y metodologías específicas de amenazas por sectores privados, gubernamentales y por la comunidad de productos y servicios de ciberseguridad.

Al crear ATT&CK, MITRE cumple su misión de unir a las comunidades para desarrollar una ciberseguridad más efectiva. Estos informes pueden referirse a un grupo de amenazas particular, una vulnerabilidad que se aprovecha en la naturaleza o una tendencia reciente en un vector de ataque. Las organizaciones utilizan indicadores de actividad maliciosa, tales como direcciones IP, dominios, direcciones de correo electrónico y certificados SSL/TLS, para alertar y buscar apoyo en la defensa de la red.

5.3. Cómo puede ayudar ATT&CK

Según el artículo de (Níquel, 2018), el marco de trabajo MITRE ATT&CK proporciona una forma estructurada de describir las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios en los ataques cibernéticos. Tanto los analistas como los defensores pueden estructurar su información utilizando ATT&CK, lo que les permite comparar a los grupos adversarios consigo mismos, con otros grupos y con las defensas. Al superponer la información de dos o más grupos, se puede crear una conciencia basada en las amenazas sobre las lagunas que existen y que los analistas saben que los adversarios están explotando.

El proceso de convertir informes de prosa no estructurados en ejemplos estructurados de técnicas ATT&CK permite a los analistas hacer valiosas

comparaciones entre grupos de amenazas o grupos de amenazas con defensas. Este proceso de "análisis técnico" requiere un conocimiento del comportamiento del adversario en la matriz ATT&CK, así como las formas comunes en que los analistas describen este comportamiento. En definitiva, la realización de este tipo de análisis no solo ayuda a los analistas a mejorar su comprensión de las tácticas y técnicas utilizadas por los adversarios, sino que también mejora la capacidad de actuación de la inteligencia sobre amenazas cibernéticas.

5.4. Aplicación de MITRE ATT&CK

Etapa	*Acción*	*Uso de MITRE ATT&CK*
Diseño de la plataforma	Identificación de técnicas y tácticas utilizadas por atacantes	Se utilizó el conocimiento de MITRE ATT&CK para identificar las técnicas y tácticas utilizadas por atacantes en diferentes fases del ciclo de vida del ataque, lo que permitió diseñar una plataforma que pueda detectarlas y prevenirlas.
Implementación de OpenCTI	Identificación de indicadores de compromiso (IOC)	Se utilizó el marco de MITRE ATT&CK para identificar los IOC que son relevantes para detectar y prevenir los ataques.
Configuración de los conectores	Identificación de técnicas y tácticas utilizadas por los atacantes	Se utilizó MITRE ATT&CK para identificar las técnicas y tácticas utilizadas por los atacantes y así poder configurar los conectores de tal manera que recolecten información relevante.
Integración con TheHive	Identificación de incidentes	Se utilizó MITRE ATT&CK para identificar incidentes y así poder clasificar y priorizar los incidentes según su gravedad y relevancia.
Análisis de amenazas	Identificación de patrones de ataque	Se utilizó MITRE ATT&CK para identificar patrones de ataque y así poder detectar nuevas amenazas y prevenir futuros ataques.

Mejora continua	Identificación de debilidades en la plataforma	Se utilizó MITRE ATT&CK para identificar debilidades en la plataforma y así poder mejorar continuamente la plataforma para enfrentar mejor las amenazas.

Tabla 9: Aplicación MITRE ATTCK
Fuente: Elaboración propia

En resumen, MITRE ATT&CK se utiliza en todas las etapas del ciclo de vida de la plataforma de Threat Intelligence, desde el diseño hasta la mejora continua, para identificar técnicas, tácticas, IOC, incidentes, patrones de ataque y debilidades, y así poder detectar y prevenir ataques y mejorar continuamente la plataforma para enfrentar mejor las amenazas.

6. Diseño y Caso de Uso

6.1. Estrategia

Preparar una estrategia bien definida previo a trabajar con una plataforma de Threat Intelligence puede ofrecernos un mejor resultado de éxito en la implementación, para nuestro caso incluimos los siguientes elementos:

Elemento	Descripción
Definición de objetivos	Establecer claramente los objetivos de la implementación de la plataforma de Threat Intelligence, como la identificación de amenazas, la prevención de ataques y la respuesta a incidentes.
Selección de herramientas	Seleccionar cuidadosamente las herramientas y plataformas que se van a utilizar, teniendo en cuenta la capacidad de integración y la funcionalidad necesaria para lograr los objetivos establecidos.
Integración de herramientas	Asegurarse de que todas las herramientas y plataformas se integren de manera adecuada y efectiva, permitiendo una gestión eficiente y efectiva de los datos de inteligencia.
Definición y ejecución de procesos	Definir los procesos y procedimientos necesarios para la gestión de la inteligencia de amenazas, desde la recopilación y análisis de datos hasta la toma de decisiones y la respuesta a incidentes.
Capacitación y entrenamiento	Capacitar y entrenar a todo el personal involucrado en el uso y gestión de la plataforma, incluyendo el personal de seguridad, TI y otras áreas relevantes.
Monitoreo y mejora continua	Monitorear continuamente el desempeño de la plataforma y sus componentes, para identificar oportunidades de mejora y asegurar que la plataforma siga siendo efectiva en la prevención y gestión de incidentes de seguridad.

Tabla 10: Estrategia Threat Intelligence
Fuente: Elaboración propia

6.2. Descripción del Caso de Uso

Para describir nuestro caso de uso tomamos como referencia la arquitectura mostrada en la figura 15, considerando que para esta demostración de análisis trataremos un caso de ***Phisinhg***:

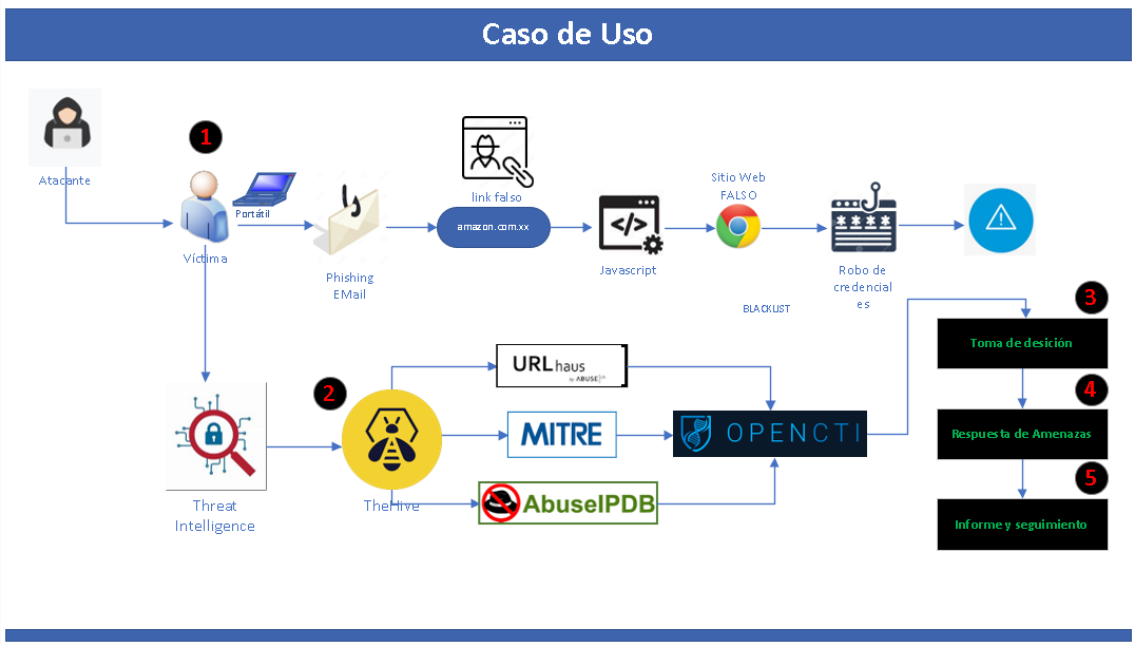


Figura 15: Arquitectura del Caso de Uso
Fuente: Elaboración propia

Descripción:

- **Nombre del caso de uso:** Análisis de phishing utilizando la plataforma OpenCTI y TheHive.
- **Actores:** Analista de seguridad

Este caso de uso describe el proceso de análisis de phishing utilizando la plataforma OpenCTI y los conectores TheHive, Mitre y AbuseIPDB. El objetivo principal es identificar y analizar direcciones IP y/o correos electrónicos de phishing para detectar posibles amenazas y tomar medidas correspondientes.

Flujo básico:

- El proceso inicia cuando el usuario informa al analista de seguridad de un correo sospechoso que ha llegado a su buzón.
- El analista de seguridad recibe dicho correo electrónico sospechoso de phishing, para lo cual crea un caso en la plataforma TheHive, el mismo que luego se encargará de generar alertas y estas se verán reflejado en la plataforma OpenCTI.

- OpenCTI utiliza el conector TheHive para buscar el correo electrónico en su base de datos de casos anteriores y correlacionar la información relevante.
- El analista revisa los resultados obtenidos de TheHive para identificar patrones similares o indicadores de compromiso (IOC).
- Así mismo, gracias a la integración del conector Mitre, busca en la base de datos de Mitre ATT&CK Framework información relacionada con los IOC identificados.
- Adicional, OpenCTI utiliza el conector AbuseIPDB para verificar la reputación de las direcciones IP asociadas al correo electrónico.
- El analista revisa los resultados de AbuseIPDB para evaluar el nivel de confianza y peligro asociado a las direcciones IP.
- Basándose en los resultados de los pasos anteriores, el analista realiza un análisis detallado del correo electrónico de phishing, identificando posibles técnicas utilizadas, intenciones maliciosas y posibles medidas de mitigación.

Flujos alternativos:

Si no se encuentran resultados relevantes en TheHive, el analista puede realizar un análisis manual adicional del correo electrónico utilizando otras herramientas de análisis de phishing disponibles. Si no se encuentran IOC relacionados en Mitre, el analista puede ampliar la búsqueda utilizando otras fuentes de información o realizar un análisis manual de las técnicas de phishing identificadas.

Requisitos previos:

Acceso a la plataforma OpenCTI y los conectores TheHive, Mitre y AbuseIPDB. Correo electrónico de phishing para analizar.

Requisitos posteriores:

Informe detallado del análisis de phishing, que incluye IOC identificados, técnicas utilizadas, intenciones maliciosas y posibles medidas de mitigación. Posibles acciones de respuesta y mitigación, como bloqueo de direcciones IP, informes a proveedores de servicios de correo y educación de usuarios.

Extensiones:

Si deseamos robustecer o enriquecer el análisis, se puede Integrar con herramientas adicionales de análisis de phishing, como herramientas de **sandboxing** para análisis de archivos adjuntos o herramientas de análisis de

URL (trabajo que se encarga el conector **URLhaus**) para evaluar la seguridad de enlaces incluidos en el correo electrónico.

Esta descripción del caso de uso proporciona una visión general del proceso de análisis de phishing utilizando OpenCTI y los conectores TheHive, Mitre y AbuseIPDB, identificando los pasos clave y los resultados esperados. Los detalles específicos de configuración y funcionalidades adicionales se pueden incluir según los requisitos y el alcance del proyecto de tesis.

Aquí las herramientas indicadas en el punto anterior, determinarán si contiene algún tipo de amenaza para procesarla y poder tomar una decisión.

- **Toma de decisiones:** Con la información recopilada a través de OpenCTI y sus herramientas de complemento, el equipo de seguridad puede tomar una decisión informada sobre cómo responder a la amenaza. Por ejemplo, pueden decidir bloquear el remitente, el dominio o la dirección IP, o pueden decidir enviar el correo electrónico sospechoso a cuarentena.
- **Respuesta a la amenaza:** Si se decide que la amenaza es real, el equipo de seguridad puede utilizar TheHive para crear una tarea y asignarla a un miembro del equipo para que la investigue. El miembro del equipo puede utilizar OpenCTI y sus complementos para recopilar más información sobre la amenaza y tomar medidas para remediar la situación.
- **Informes y seguimiento:** Una vez que se ha investigado y respondido a la amenaza, el equipo de seguridad puede utilizar TheHive para generar informes y realizar un seguimiento de la amenaza para asegurarse de que no vuelva a ocurrir en el futuro.

Esto proporciona una respuesta coordinada y rápida a los incidentes de phishing, y también ayuda a proporcionar una visibilidad completa del panorama de amenazas.

En síntesis, al utilizar una plataforma de OpenCTI integrada con TheHive y componentes como los mencionados en el primer punto, genera que el equipo de seguridad de una organización pueda analizar y responder a posibles amenazas de phishing de manera eficaz y eficiente.

6.3. Prueba de Concepto

La implementación de una plataforma de Threat Intelligence tiene como objetivo centralizar y gestionar la información de inteligencia de amenazas, así como facilitar la detección y respuesta a incidentes de seguridad. OpenCTI actúa como un repositorio central para almacenar y analizar la información de inteligencia, mientras que TheHive proporciona una interfaz de gestión de incidentes y coordinación de respuesta.

Pasos de la prueba de concepto:

a) **Preparación del entorno virtual:**

- Configura y preparar el ambiente de prueba desde un servidor o máquina virtual creada en **Virtual Box 7.0**[7], importante establecer las configuraciones óptimas en recursos RAM, y espacio en disco para el correcto funcionamiento e instalación del sistema operativo (**Ubuntu 22.02**[8]) para alojar los contenedores y soporte las plataformas (OpenCTI, TheHive).

b) **Preparación entorno Docker, Docker Compose y Portainer:**

- Descargar e Instalar las herramientas **Docker y Docker-Compose**[9]**,** desde el sitio oficial, estos permitirán posteriormente implementar las pilas de las plataformas OpenCTI y TheHive.
- Asi mismo se necesitará de la herramienta **Portainer**[10] que servirá como gestor de administración de las plataformas.
- Verifica que los contenedores se hayan iniciado correctamente utilizando el comando docker ps.

c) **Implementación plataforma OpenCTI Docker:**

- Desde Portainer, crear una nueva pila (Stack) y nombrarla como "**opencti**".
- Desde el repositorio oficial en **GitHub OpenCTI Docker** encontrar el archivo . docker-compose.yml, copiar el contenido y pegarlo en el editor de la pila creada.
- Del mismo repositorio Github OpenCTI Docker ingreso al archivo "**env.sample"** copio el contenido y genero las respectivas variables de entorno como se indica en el ejemplo.
- Configurar los parámetros de instalación, como la dirección IP, el puerto, el token, URL, y los UUID respectivos en los que se ejecutará OpenCTI.
- Levantar la pila.

.

d) **Implementación plataforma TheHive:**

[7] https://download.virtualbox.org/virtualbox/7.0.8/VirtualBox-7.0.8-156879-Win.exe
[8] https://ubuntu.com/download
[9] https://docs.docker.com/engine/install/ubuntu/
[10] https://docs.portainer.io/start/install-ce/server/docker/linux

- Desde Portainer, crear una nueva pila (Stack) y nombrarla como "**thehive**".
- Desde el repositorio oficial en **GitHub TheHive** encontrar el archivo . docker-compose.yml, copiar el contenido y pegarlo en el editor de la pila creada.
- Configurar los parámetros de instalación, como la dirección IP, el puerto, el token, URL, y los UUID respectivos en los que se ejecutará TheHive.
- Actualizar la pila.

e) Configuración de la integración (conectores):

- Accede a la interfaz web de OpenCTI y TheHive utilizando un navegador web.
- Inicia sesión en ambas plataformas con las credenciales de administrador.
- Desde GitHub OpenCTI ingresamos a **Conectores**[11]**.**
- Luego ingresamos al tipo de conector **"external-import"**
- Ingresamos al conector **TheHive** abrimos el archivo docker-compose.yml y copiamos su contenido.
- Desde Portainer, en el editor de la pila de OpenCTI, al final del código agregamos el código copiado del paso anterior.
- Configuramos los parámetros respectivos como la dirección IP, APIKEY y el puerto correspondiente.
- Actualizar la pila y listo se ha realizado la integración.
- Repetiremos todos estos pasos indicados, para cada uno de los conectores URLhause y MITRE.

f) **Configuración de Enriquecimiento:**

- Finalmente enriqueceremos conocimiento a la plataforma OpenCTI con conectores de tipo **"internal-enrichment".**
- Ingresamos al conector **AbuseIPDB** abrimos el archivo docker-compose.yml y copiamos su contenido.
- Desde Portainer, en el editor de la pila de OpenCTI, al final del código agregamos el código copiado del paso anterior.
- Configuramos los parámetros respectivos como la dirección IP, APIKEY y el puerto correspondiente.

[11] https://github.com/OpenCTI-Platform/connectors

- Actualizar la pila y listo se ha realizado la integración de enriquecimiento.

g) Configuración de casos TheHive:

- Desde la plataforma **TheHive**, creamos nuestra empresa y un primer usuario que será aquel que nos permita generar los casos, observables y los IoC.
- De forma automática, estas alertas se verán reflejados desde la plataforma OpenCTI gracias a la integración realizada.
- Una vez completo todos los pasos anteriores se obtiene como resultado la funcionalidad de nuestra **plataforma de Inteligencia de Amenazas** (Threat Intelligence) con OpenCTI y TheHive.

h) Simulación Phishing:

- Implementada la plataforma se obtiene la muestra del correo electrónico que se sospecha de phishing para utilizar en la prueba. Desde TheHive, creamos internamente un caso para simular esta situación.
- Gracias a la integración de los conectores de **TheHive y Mitre** para realizar consultas y búsquedas relacionadas con los correos electrónicos cargados, se verifican que los resultados se correlacionen adecuadamente y proporcionen información útil para el análisis.
- A continuación, **AbuseIPDB** gracias a su conector se encarga de verificar la reputación de las direcciones IP asociadas a los correos electrónicos de phishing. Evalúa que los resultados reflejen de manera precisa la confiabilidad y riesgo asociados a las IP.
- Del mismo modo, **URLhause** como plataforma colaborativa recopila y comparte información sobre URLs maliciosas enriqueciendo su análisis, es decir, enlaces que dirigen a sitios web que contienen contenido malicioso, como malware, phishing o estafas en línea.
- **Análisis y generación de informes:** OpenCTI, realiza un análisis detallado de los correos electrónicos de phishing utilizando la información recopilada de TheHive, Mitre URLhause y AbuseIPDB. Identifica indicadores de compromiso, técnicas utilizadas y posibles medidas de mitigación. Finalmente, desde **OpenCTI** se genera informes que documenten los resultados y hallazgos del análisis.
- **Evaluación de la efectividad y eficiencia:** Evaluamos la efectividad y eficiencia de la solución propuesta en términos de detección de phishing, correlación de información, rapidez en la obtención de resultados y utilidad de los informes generados.

- **Documentación y conclusiones:** Se elabora un informe de prueba de concepto que resuma los resultados obtenidos, las conclusiones alcanzadas y las recomendaciones para la implementación de la solución a gran escala.

La prueba de concepto en este caso permitirá demostrar la capacidad de las herramientas y su integración para detectar y analizar eficazmente correos electrónicos de phishing, proporcionando información valiosa para la toma de decisiones de seguridad. Además, se evalúa la interoperabilidad de las herramientas y su adecuación para cumplir con los requisitos y objetivos establecidos en el caso de uso.

7. Implementación

7.1. Despliegue Docker, Docker-Compose y Portainer

Preparación del entorno: Para esta demostración se implementó dentro de una máquina virtual Ubuntu 22.02 donde se configuró un entorno en el que se puedan desplegar las tecnologías necesarias para la Prueba de Concepto, utilizando una arquitectura basada en contenedores, este proceso lo realizamos basándonos en el sitio oficial de Docker.

	Docker Standalone	Docker Compose	Portainer
Función	Empaquetar aplicaciones en contenedores con todas las dependencias También aisla sus ambientes sin afectar al sistema host.	Admite definir múltiples contenedores que se ejecutan juntos como una aplicación. Facilita la colaboración en equipo al definir aplicaciones.	Ofrece una interfaz gráfica para la gestión de contenedores, redes y volúmenes de Docker.
Instalación del entorno	https://docs.docker.com/engine/install/ubuntu/	https://docs.docker.com/compose/install/linux/	https://docs.portainer.io/start/install/server/docker/linux

Tabla 11: Tecnología Docker, Docker Compose y Portainer.
Fuente: Elaboración propia

Una vez instalado, desde el navegador ingresamos a Portainer mediante la dirección: **https://192.168.1.49:9443**

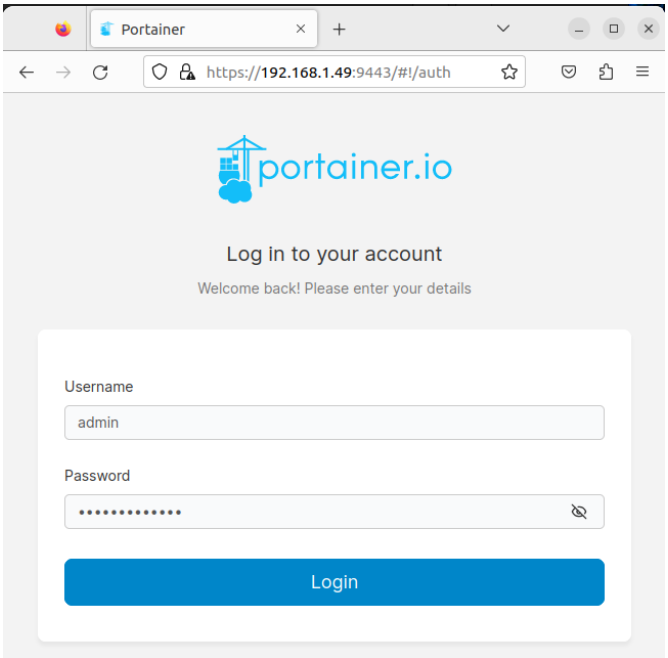


Figura 16: Acceso a Portainer
Fuente: Elaboración propia

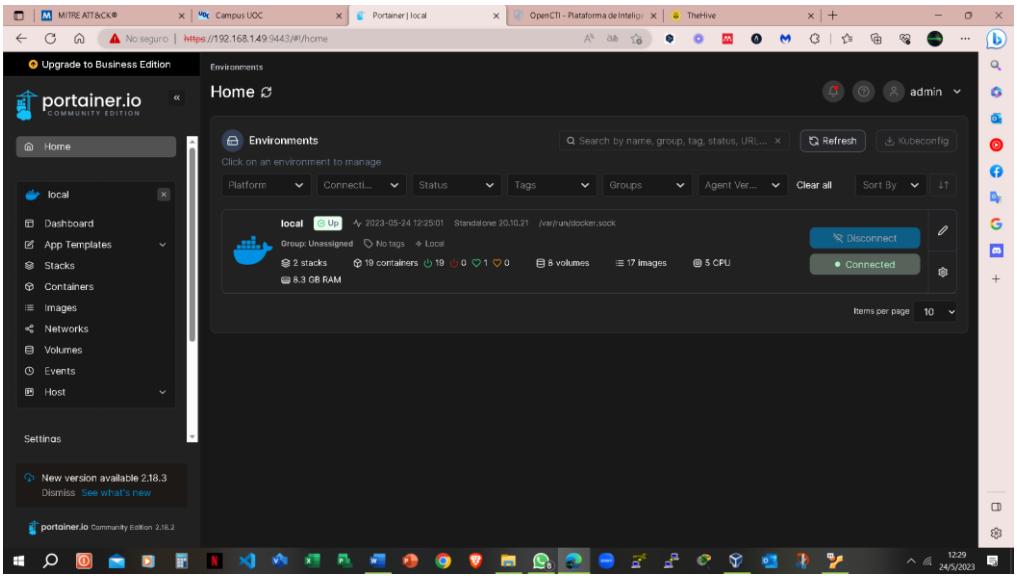


Figura 17: Interfaz Portainer
Fuente: Elaboración propia

- **Despliegue de los servicios:** una vez levantada la plataforma **Portainer** y su dockerización respectiva**,** se deben desplegar los servicios necesarios para la Prueba de Concepto.

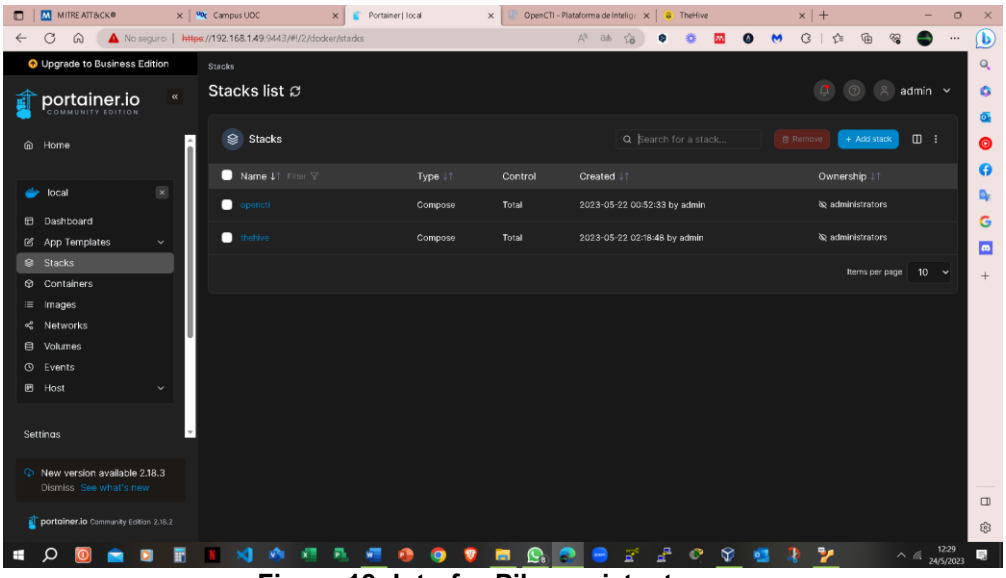


Figura 18: Interfaz Pilas existentes
Fuente: Elaboración propia

En este caso, se desplegó dos plataformas: la principal **OpenCTI** y complementando con **TheHive.** Para lo cual creamos un nuevo Stack con el nombre **Opencti.**

7.2. Implementación Plataforma OpenCTI

Para el despliegue se siguió los pasos que se encuentra en la respectiva documentación de su GitHub oficial de OpenCTI[12].

[12] https://github.com/OpenCTI-Platform/docker/blob/master/docker-compose.yml

De alli tomados el archivo “**docker-compose.yml”** y copiamos el contenido para posteriormente pegarlo dentro del editor del Stack OpenCTI que se ha creado como se indica en la figura 19.

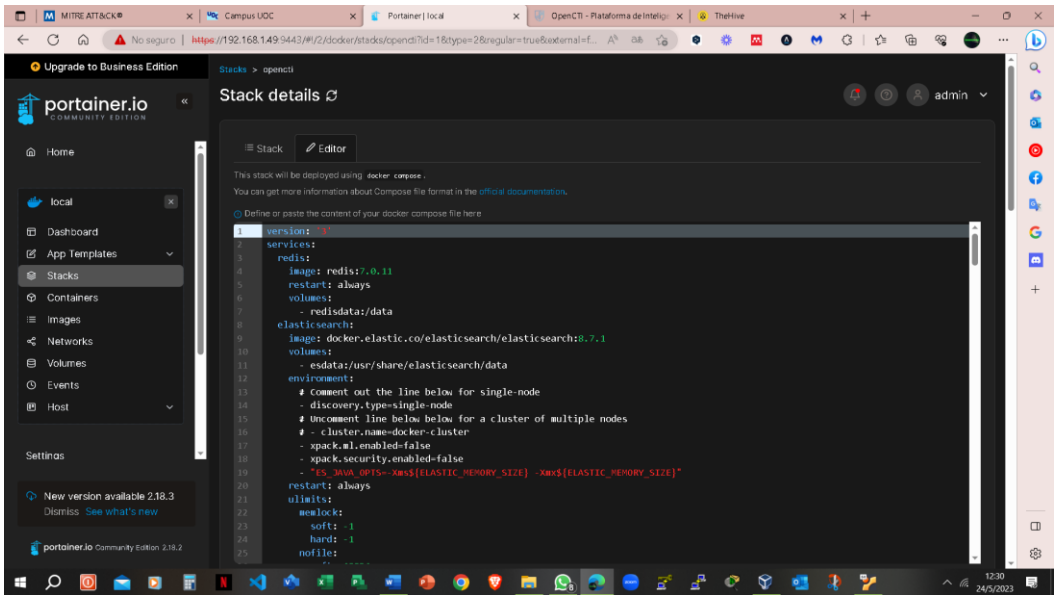


Figura 19: Archivo docker-compose OpenCTI
Fuente: Elaboración propia

- De modo similar, se debe configurar todas las **Variables de Ambiente**[13] con sus parámetros respectivos como se muestra en la figura 20:

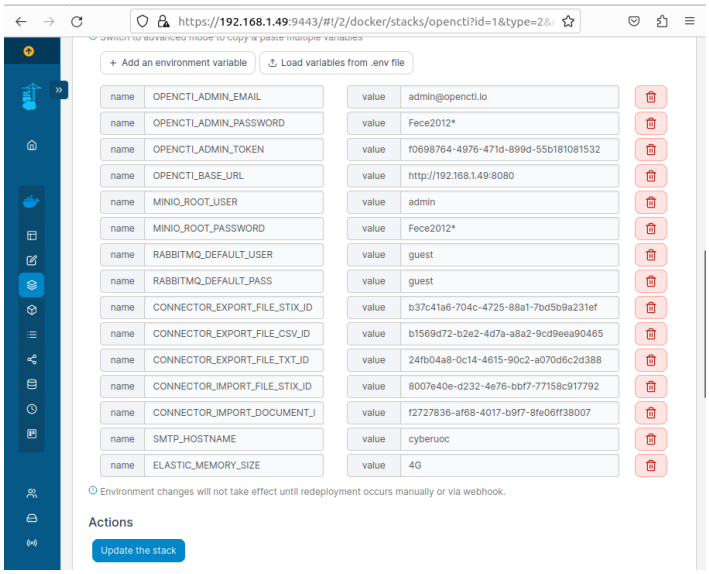


Figura 20: Variables de Entorno OpenCTI
Fuente: Elaboración propia

- Por último, se da clic en el botón de “**Update Stack**”.

[13] https://github.com/OpenCTI-Platform/docker/blob/master/.env.sample

- Si es satisfactorio, se verifica desde un navegador ingresando a la url: **192.168.1.49:8080** donde solicitará el usuario y contraseña que se asignó en la configuración de las variables de entorno.

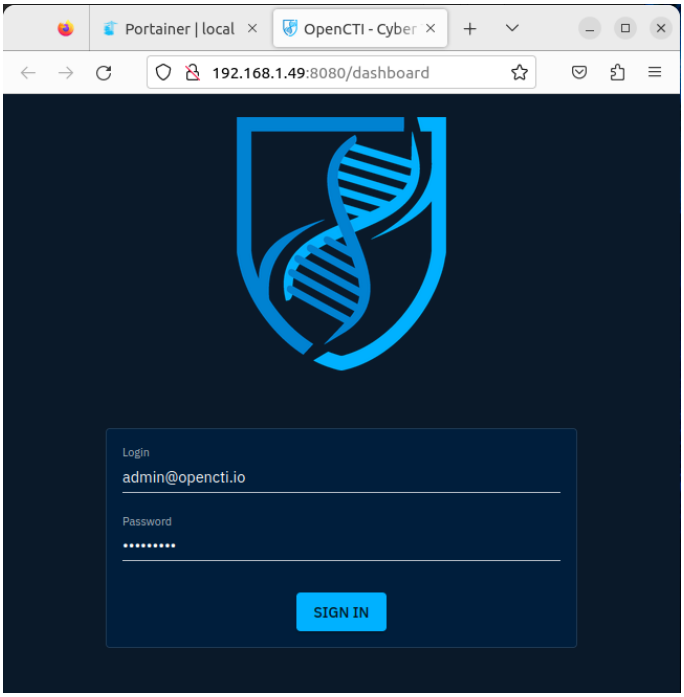


Figura 21: Logueo plataforma OpenCTI
Fuente: Elaboración propia

Luego de ingresar las credenciales se mostrará la interfaz de la plataforma OpenCTI, normalmente estará vacía en virtud que aún no se ha enriquecido con información para su análisis.

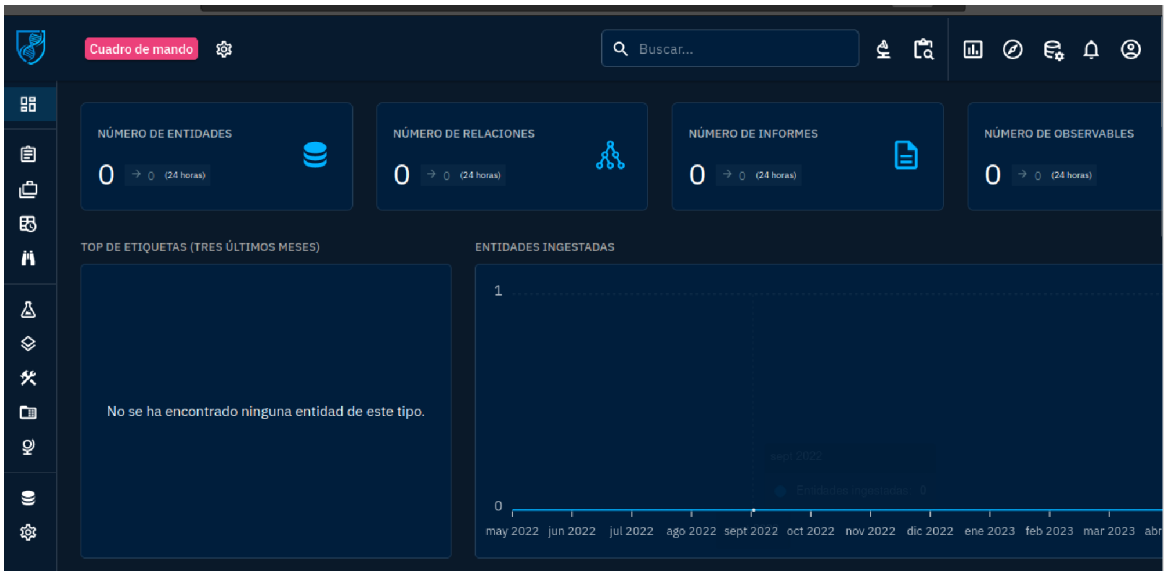


Figura 22: Interfaz OpenCTI
Fuente: Elaboración propia

7.3. Implementación Plataforma TheHive

Creamos una nueva Pila (Stack) y la denominamos **thehive**, luego desde el sitio web TheHive[14], abrimos el archivo **docker-composer.yml** y copiamos su contenido para pegarlo dentro de la pestaña Editor

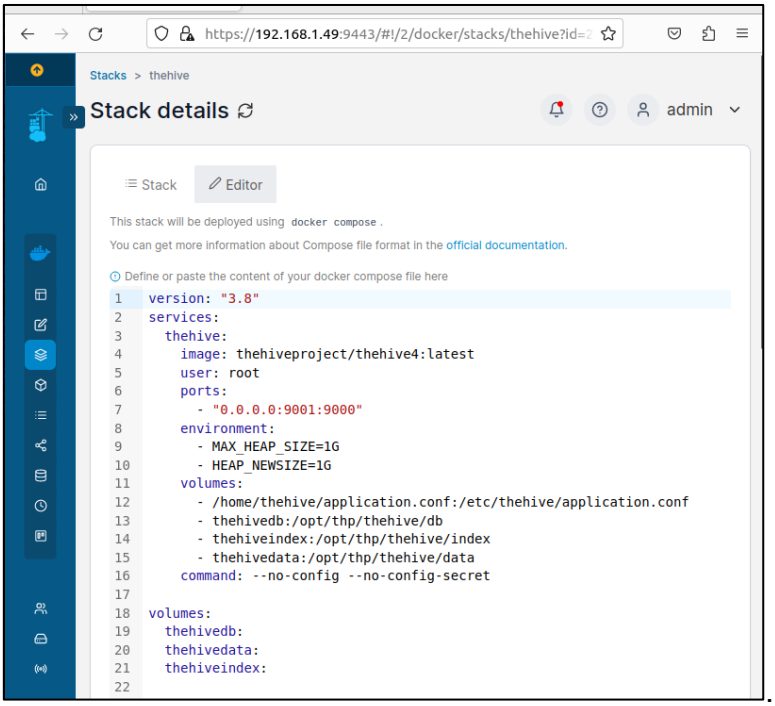


Figura 23: Archivo docker-compose TheHive
Fuente: Elaboración propia

Por último, se da clic en el botón "**Update Stack**".

Si es satisfactorio, se verifica desde un navegador ingresando a la url: **192.168.1.49:9001** donde solicitará el usuario y contraseña

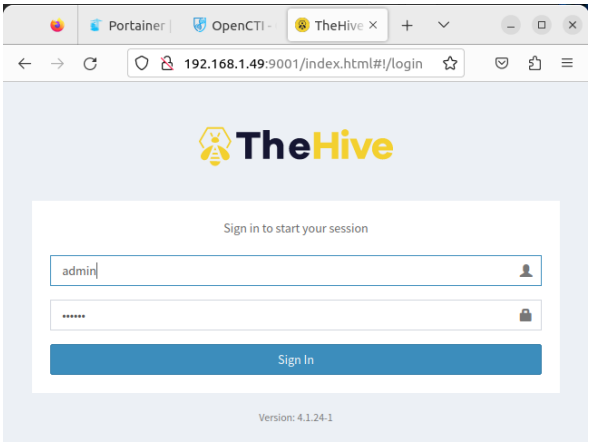


Figura 24: Logueo plataforma TheHive
Fuente: Elaboración propia

[14] https://docs.strangebee.com/thehive/setup/installation/docker/

Una vez que ingresamos a la plataforma, creamos una nueva empresa y un nuevo usuario, datos que posteriormente nos servirá para integrar desde un conector de OpenCTI.

Asi mismo, desde esta plataforma se ofrece herramientas para asignar tareas, compartir información, colaborar en tiempo real y realizar un seguimiento del progreso de los incidentes.

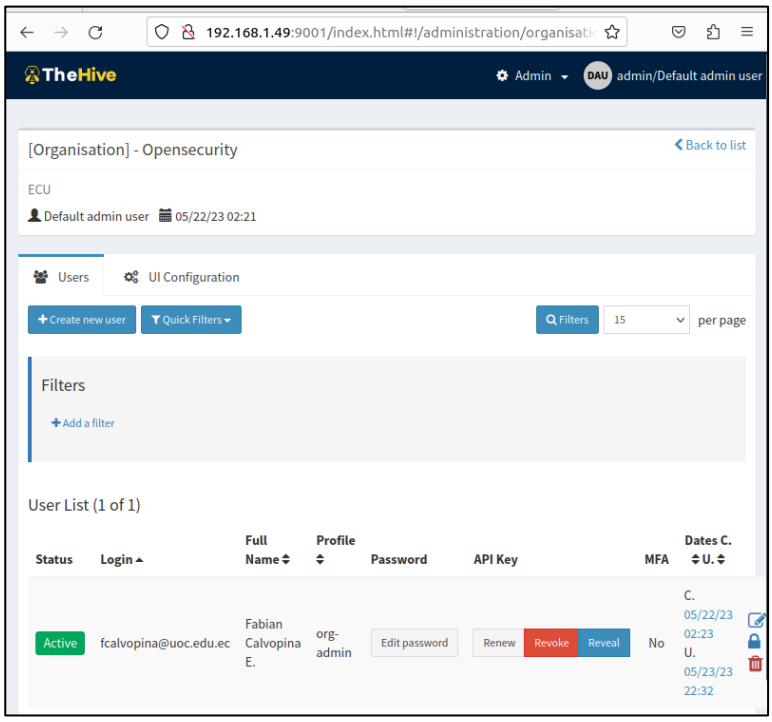


Figura 25: Interfaz Plataforma TheHive
Fuente: Elaboración propia

Creación de casos en TheHive

- Nos logueamos con el usuario creado, **fcalvopina@uoc.edu.ec**
- Creamos un nuevo Caso
- El proceso se encuentra en el Anexo del documento.

7.4. Implementación de Conectores.

De acuerdo con nuestra simulación, los componentes (open-source) que hemos contemplado más apropiados y que están relacionados con amenazas de phishing para OpenCTI son: **Mitre, URLHaus, TheHive y AbuseIPDB**

Conector	Definición	Función
MITRE ATT&CK	Un marco de referencia de tácticas y técnicas de ataque	Permite a los investigadores y analistas de seguridad clasificar y entender mejor los diferentes tipos de **ataques** cibernéticos, para desarrollar medidas de defensa efectivas.
URLhaus	Una base de datos de URLs maliciosas	Proporciona una lista actualizada de **URLs** maliciosas y distribuidas a través de botnets,

		para su uso en la prevención y detección de ataques de phishing y malware.
TheHive	Integración con otras herramientas y servicios de seguridad, con el objetivo de automatizar y agilizar la respuesta a incidentes.	Puede conectarse a diferentes fuentes de información, como sistemas de detección de intrusiones (IDS/IPS), antivirus, SIEM, entre otros. Permite recopilar y centralizar datos relevantes sobre eventos de seguridad y amenazas.
AbuseIPDB	Una base de datos de direcciones IP maliciosas	Este conector permitirá enriquecer la información proporcionando una lista actualizada de direcciones **IP maliciosas reportadas** por la **comunidad** de seguridad cibernética, para su uso en la prevención y detección de ataques.

Tabla 12: Conectores OpenCTI
Fuente: Elaboración propia

Cada uno de estos conectores lo encontramos dentro del repositorio GitHub de OpenCTI de donde se tomará el contenido respectivo de estos archivos y se añadirá al final del compose del Stack OpenCTI:

- **Implementar conector TheHive:** se copia el contenido respectivo **docker-compose.yml** y se lo añadirá al final del código de la pila dentro del editor del Stack de OpenCTI. Aquí configuramos API KEY, URL, TOKEN, ID, Organización.

```
229   connector-thehive:
230     image: opencti/connector-thehive:5.7.6
231     environment:
232       - OPENCTI_URL=http://opencti:8080
233       - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
234       - CONNECTOR_ID=6bb335e0-1d9f-4c2b-a464-fd42c138df5f
235       - CONNECTOR_TYPE=EXTERNAL_IMPORT
236       - CONNECTOR_NAME=TheHive
237       - CONNECTOR_SCOPE=thehive
238       - CONNECTOR_CONFIDENCE_LEVEL=80 # From 0 (Unknown) to 100 (Fully trusted)
239       - CONNECTOR_UPDATE_EXISTING_DATA=false
240       - CONNECTOR_LOG_LEVEL=info
241       - THEHIVE_URL=http://192.168.1.49:9001
242       - THEHIVE_API_KEY=d+4rFDLwpNtMf+Z6dBe62QkZz9zdhNSo
243       - THEHIVE_CHECK_SSL=false
244       - THEHIVE_ORGANIZATION_NAME=Opensecurity
245       - THEHIVE_IMPORT_FROM_DATE=2021-01-01T00:00:00 # Optional
246     restart: always
247     depends_on:
248       - opencti
```

- **Implementar conector AbuseIPDB:** se copia el contenido respectivo **docker-compose.yml** y se lo añadirá al final del código de la pila dentro del editor del Stack de OpenCTI. Aquí configuramos principalmente el API KEY, URL y TOKEN.

```
      - opencti
  connector-abuseipdb:
    image: opencti/connector-abuseipdb:5.7.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=f81df518-0e16-4bc8-8a7d-f5b80108fab6
      - CONNECTOR_TYPE=INTERNAL_ENRICHMENT
      - CONNECTOR_NAME=AbuseIPDB
      - CONNECTOR_SCOPE=IPv4-Addr
      - CONNECTOR_AUTO=true
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
      - ABUSEIPDB_API_KEY=671e441738d8a5a7355c3729d85e21c91b08d1ac1e36835a06292dbc2b13e6d8259efe611ef93678
      - ABUSEIPDB_MAX_TLP=TLP:AMBER
    restart: always
    depends_on:
      - opencti
```

- **Implementar conector URLhaus:** se copia el contenido respectivo **docker-compose.yml** y se lo añadirá al final del código de la pila dentro del editor del Stack de OpenCTI. Aquí configuramos: ID, URL y TOKEN.

```
  connector-urlhaus:
    image: opencti/connector-urlhaus:5.7.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=9fcb34ab-bcd9-4623-8b1c-c4cec7b2e237
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - "CONNECTOR_NAME=Abuse.ch URLhaus"
      - CONNECTOR_SCOPE=urlhaus
      - CONNECTOR_CONFIDENCE_LEVEL=40 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_UPDATE_EXISTING_DATA=false
      - CONNECTOR_LOG_LEVEL=info
      - URLHAUS_CSV_URL=https://urlhaus.abuse.ch/downloads/csv_recent/
      - URLHAUS_IMPORT_OFFLINE=true
      - URLHAUS_CREATE_INDICATORS=true
      - URLHAUS_THREATS_FROM_LABELS=true
      - URLHAUS_INTERVAL=3 # In days, must be strictly greater than 1
    restart: always
    depends_on:
      - opencti
```

- **Implementar conector MITRE:** se copia el contenido respectivo **docker-compose.yml** y se lo añadirá al final del código de la pila dentro del editor del Stack de OpenCTI. Aquí configuramos: ID, URL y TOKEN.

```
  connector-mitre:
    image: opencti/connector-mitre:5.7.6
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=14ea3c29-2b21-4f74-b28c-1ee70ec27fd1
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - "CONNECTOR_NAME=MITRE Datasets"
      - CONNECTOR_SCOPE=tool,report,malware,identity,campaign,intrusion-set,attack-pattern,course-of-action,x-m
      - CONNECTOR_CONFIDENCE_LEVEL=75
      - CONNECTOR_UPDATE_EXISTING_DATA=false
      - CONNECTOR_RUN_AND_TERMINATE=false
      - CONNECTOR_LOG_LEVEL=info
      - MITRE_INTERVAL=7 # In days
    restart: always
    depends_on:
      - opencti
```

8. Conclusiones y Trabajo Futuro

8.1. Conclusiones

Finalmente podemos indicar que luego de haber implementado todas y cada una de las herramientas y recursos indicados, se cuenta con nuestra plataforma de inteligencia de amenazas, de tal forma que al abrir OpenCTI, se mostrará la información respectiva de los casos ingresados en TheHive enriquecido con los datos de colaboración que proporcionan los diferentes conectores integrados.

Con esto podemos decir que:

- La integración de OpenCTI y TheHive permite una mejor gestión de incidentes al facilitar la recopilación, análisis y correlación de información de inteligencia de amenazas. Esto agiliza el proceso de detección, respuesta y mitigación de incidentes de seguridad, lo que resulta en una mayor eficiencia operativa.

- Al enriquecer la información de inteligencia de amenazas con datos adicionales provenientes de fuentes como Mitre y AbuseIPDB, se obtiene una visión más completa de los ataques y se mejora la capacidad de detección y respuesta ante amenazas, incluyendo el phishing.

- La integración de estas plataformas proporciona a los analistas de seguridad una visión contextualizada de los incidentes, con información detallada sobre indicadores de compromiso, tácticas utilizadas por los atacantes y datos de reputación de IP. Esto permite una mejor toma de decisiones en la respuesta a los incidentes.

- La integración entre OpenCTI y TheHive fomenta la colaboración y la comunicación entre los equipos de seguridad ya que los analistas pueden compartir información de forma más eficiente, asignar tareas, dar seguimiento al progreso y documentar las acciones tomadas, lo que contribuye a una respuesta coordinada y efectiva ante los incidentes.

- Mediante la retroalimentación de información adicional o actualizada a OpenCTI, se enriquece la inteligencia de amenazas y se mejora la capacidad de detección y respuesta en futuros incidentes. Esto promueve la mejora continua de la seguridad y la adaptación a nuevas y emergentes amenazas cibernéticas.

8.2. Trabajo Futuro

TheHive y OpenCTI pueden integrarse con otras herramientas de seguridad, como **SIEM** (Security Information and Event Management) y **SOAR** (Security Orchestration, Automation, and Response) para proporcionar una solución de seguridad integral y completamente automatizada que pueda proteger contra una amplia gama de amenazas cibernéticas, incluyendo el phishing.

Puntualmente, como parte de trabajos futuros que complementen a esta investigación, se considere la integración de OpenCTI y TheHive con una plataforma **SOAR** para aprovechar la automatización y orquestación de tareas de seguridad. En virtud que una plataforma SOAR permite crear flujos de trabajo automatizados para la detección y respuesta a incidentes, incluyendo la ejecución de acciones de mitigación basadas en la inteligencia de amenazas recopilada en OpenCTI. Esto optimizaría la capacidad de respuesta a amenazas, reduciendo el tiempo de reacción y mejorando la eficiencia operativa.

9. Bibliografía

Alam, Bhusal, D., Park, Y., & Rastogi, N. (2022). *CyNER: A Python Library for Cybersecurity Named Entity Recognition*. arXiv.org.

Al-Shaer, E., & Zhang, N. (2019). *Cyber Threat Intelligence Sharing and Analysis. In Cybersecurity: The Insights You Need from Harvard Business Review* (pp. 113-131). Harvard Business Review Press.

Belyaev, E., Guschin, A., & Paramonov, V. (2020). *OpenCTI: Open source platform for cyber threat intelligence management. In Proceedings of the 2020* IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 1380-1383.

Canas, J. M., Garcia, R., Santos, J. M., & Martín, E. (2021). *Expanding MISP and OpenCTI with MISP modules to integrate with other cyber threat intelligence sources*. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 126-133.

CIBERCI. (2022). *(362) Ciclo de vida del Threat Intelligence: de la reactividad a la proactividad - Hesaul Sánchez. - YouTube*. https://www.youtube.com/watch?v=zU0VWP6GV50

Ciberseguridad.com. (2021). *Inteligencia de amenazas, todo lo que debes saber*. Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas. https://ciberseguridad.com/guias/prevencion-proteccion/inteligencia-amenazas/

Conti, M., Dehghantanha, A., & Dargahi, T. (2018). *Inteligencia de amenazas cibernéticas: desafíos y oportunidades*. https://link.springer.com/chapter/10.1007/978-3-319-73951-9_1

Create "search history" drop down in main search bar, unique to each user · Issue #2925 · OpenCTI-Platform/opencti · GitHub. (s/f). Recuperado el 8 de marzo de 2023, de https://github.com/OpenCTI-Platform/opencti/issues/2925

Cybervie. (2020). Inteligencia de amenazas cibernéticas | Guía para principiantes - CYBERVIE. *Blog*. https://www.cybervie.com/blog/cyber-threat-intelligence-beginners-guide/

Cyware Unveils New Threat Response Docker to Empower Security Community with Open-Source Threat Intelligence Technologies: Free Open-Source Threat Intelligence Tool Will Allow Users to Automate and Orchestrate Key Threat Intelligence Tasks. (2021, May 11). PR Newswire https://www.proquest.com/wire-feeds/cyware-unveils-new-threat-response-docker-empower/docview/2524731938/se-2

Daniele, J. (2021). Inteligencia de amenazas cibernéticas - DNC | Proveedor de servicios de seguridad gestionados | MSSP | Toronto, Canadá. *DNC CYBERSECURITY*. https://dncybersecurity.com/insights/cyber-intelligence/

Dincer, B., & Karabacak, B. (2021). An Investigation into the Integration of Threat Intelligence Platforms and Security Information and Event Management Systems. In 2021 5th International Conference on Computer Science,

Engineering and Applications (ICCSEA) (pp. 1-6). IEEE.

Equipo Flaspoint. (2021). *Las cinco fases del ciclo de vida de Threat Intelligence | Punto de inflamación*. Blog. https://flashpoint.io/blog/threat-intelligence-lifecycle/

Filigran. (2022). *GitHub - OpenCTI-Platform/opencti: Open Cyber Threat Intelligence Platform*. github. https://github.com/OpenCTI-Platform/opencti

Ferrill, T. (2023). 10 dark web monitoring tools. *CSO (Online),* https://www.proquest.com/trade-journals/10-dark-web-monitoring-tools/docview/2778314434/se-2

Kaspersky. (2023). ¿Qué es la inteligencia de ciberamenazas? Definición y explicación. *Centro de recursos*. https://latam.kaspersky.com/resource-center/definitions/threat-intelligence

Níquel, K. (2018). Using ATT&CK to Advance Cyber Threat Intelligence — Part 1 | by Katie Nickels | MITRE ATT&CK® | Medium. *MITRE*. https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-1-c5ad14d59724

OpenCTI. (2021). OpenCTI: An open source platform to manage threat intelligence. Recuperado el 29 de marzo de 2023, de https://www.opencti.io/

OpenCTI: una plataforma de inteligencia de amenazas de código abierto para la ciberseguridad en el sector público" por J. Jiménez et al. (2021) en la Revista de Tecnologías de la Información y las Comunicaciones: http://www.scielo.org.co/scielo.php?pid=S2256-50352021000200009&script=sci_abstract

OpenCTI: una plataforma de inteligencia de amenazas de código abierto para la colaboración en la comunidad de ciberseguridad" por J. Portela et al. (2020) en la Revista de Ingeniería de Sistemas y Tecnología: https://dialnet.unirioja.es/servlet/articulo?codigo=7583479

Papaioannou, F. (2021). *Threat Intelligence Platforms Evaluation* [Dissertation, ProQuest Dissertations Publishing]. https://doi.org/10.26267/unipi_dione/769

Palacin. (2021). *Practical threat intelligence and data-driven threat huntingx* : **Practical** threat intelligence and data-driven threat hunting : a hands-on guide to threat hunting with the ATT&CK framework and open source tools / Valentina Palacin. Packt Publishing, Limited.

Pérez, J. E., García, E., & García-Teodoro, P. (2021). OpenCTI-based cyber threat intelligence platform for malware analysis. Journal of Information Security and Applications, 61, 102973.

Reyes-Rodriguez, J. A., González-Cabrera, D., & Valenzuela, A. M. (2021). Implementación de una plataforma de inteligencia de amenazas de código abierto utilizando OpenCTI y MISP. In Actas del XVI Congreso de la Sociedad Española de Sistemas de Información (págs. 425-432).

Rosa, R. Batista, R. Gonçalves, J. Martins y F. Branco, "Cyber Threat Intelligence Architecture for Applied Cybersecurity Scenarios: PhD Thesis Proposal in

Web Science and Technology," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9820152.

Stojkovski, B. (2021). *¿Qué hay en una plataforma de intercambio de inteligencia de amenazas cibernéticas? | Conferencia Anual de Aplicaciones de Seguridad Informática*. https://dl.acm.org/doi/abs/10.1145/3485832.3488030

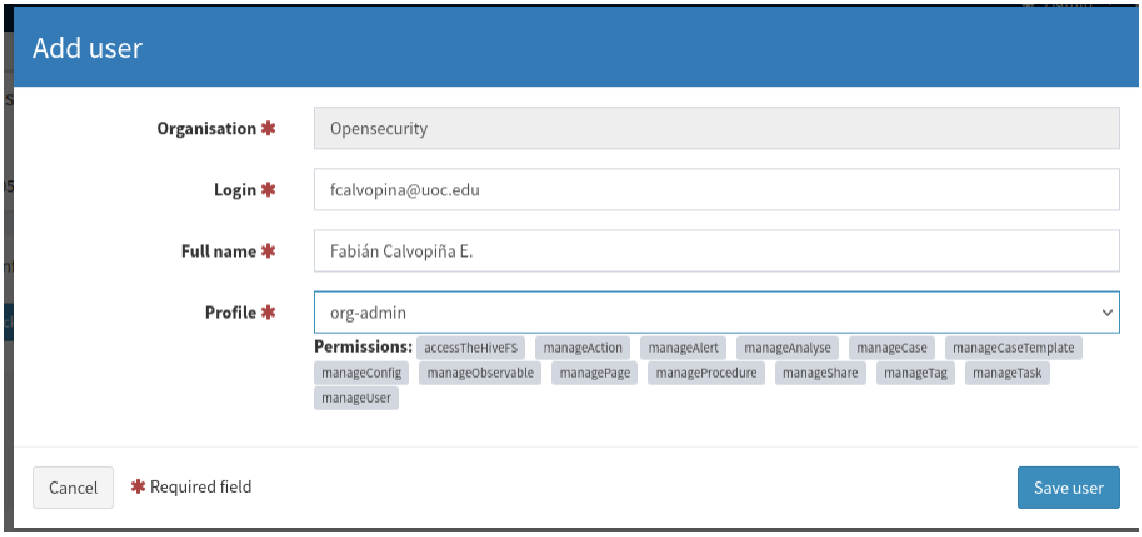
Slay, J., & Hall, J. (2019). *Cyber Threat Intelligence and the Mitigation of Advanced Persistent Threats. En Advanced Persistent Security* (pp. 155-176). Springer, Cham.

TheHive. (2021). *GitHub - TheHive-Project/TheHive: TheHive: a Scalable, Open Source and Free Security Incident Response Platform*. github. https://github.com/TheHive-Project/TheHive

United Kingdom : Reducing Installation Time for Open Source Threat Intelligence Platform, OpenCTI. (2022, Aug 18). MENA Report https://www.proquest.com/wire-feeds/united-kingdom-reducing-installation-time-open/docview/2703734240/se-2

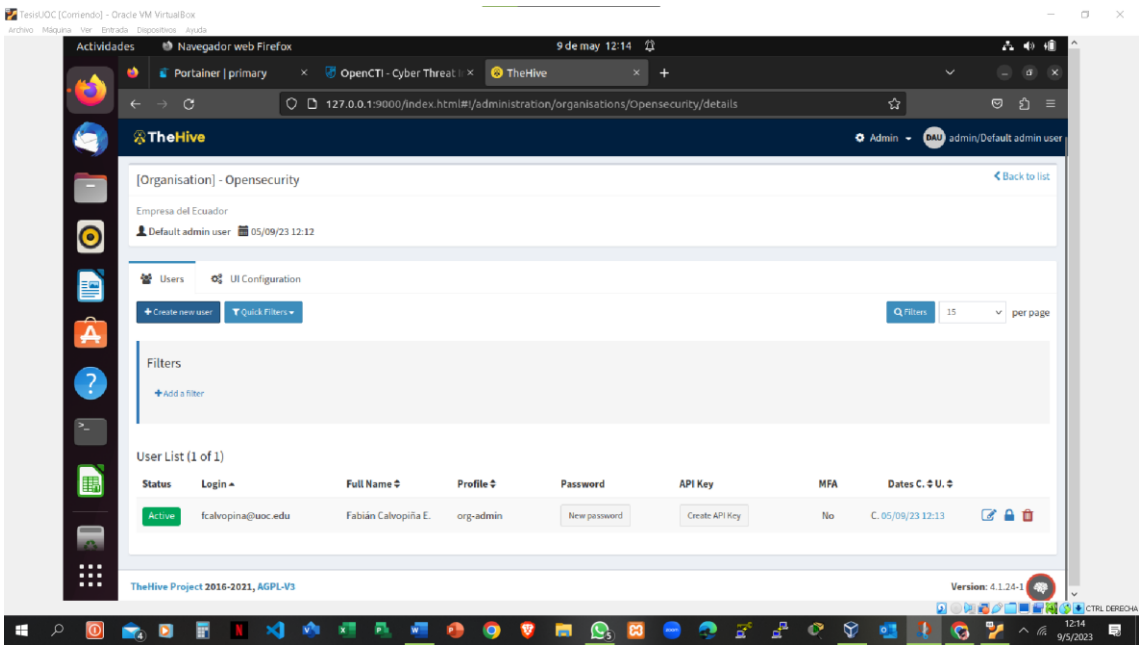
10. Anexos

- **Proceso crear casos en TheHive:**



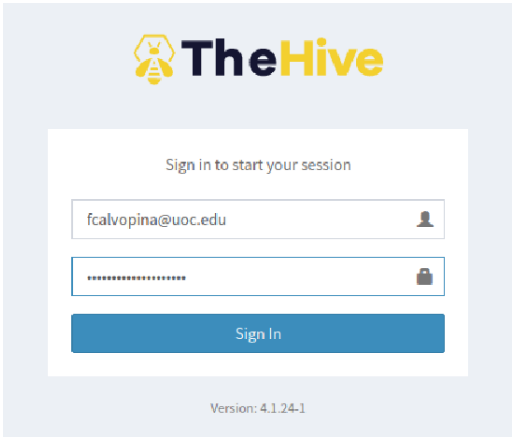
Añadir Usuario

- Creamos un password nuevo
- Generamos el APIKEY: `tEIl5kMKOHKL29izIz57WJEGO42gLJlA`
- Este ApiKey lo debemos asignar dentro del código del conector TheHive conjuntamente con el nombre de la organización y actualizar la pila.

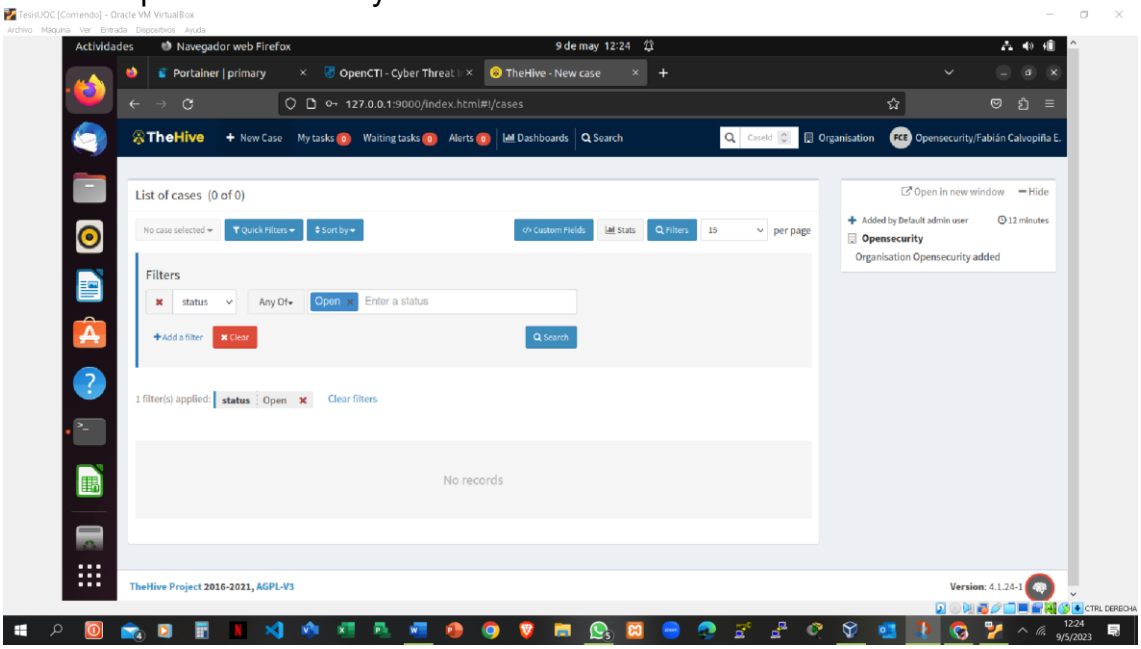


Usuario fcalvopina creado

Ahora cerramos la sesión y nos logueamos con el nuevo usuario creado:



- Desde nuestro usuario ya podemos crear nuevos casos para las respectivas alertas y observables.

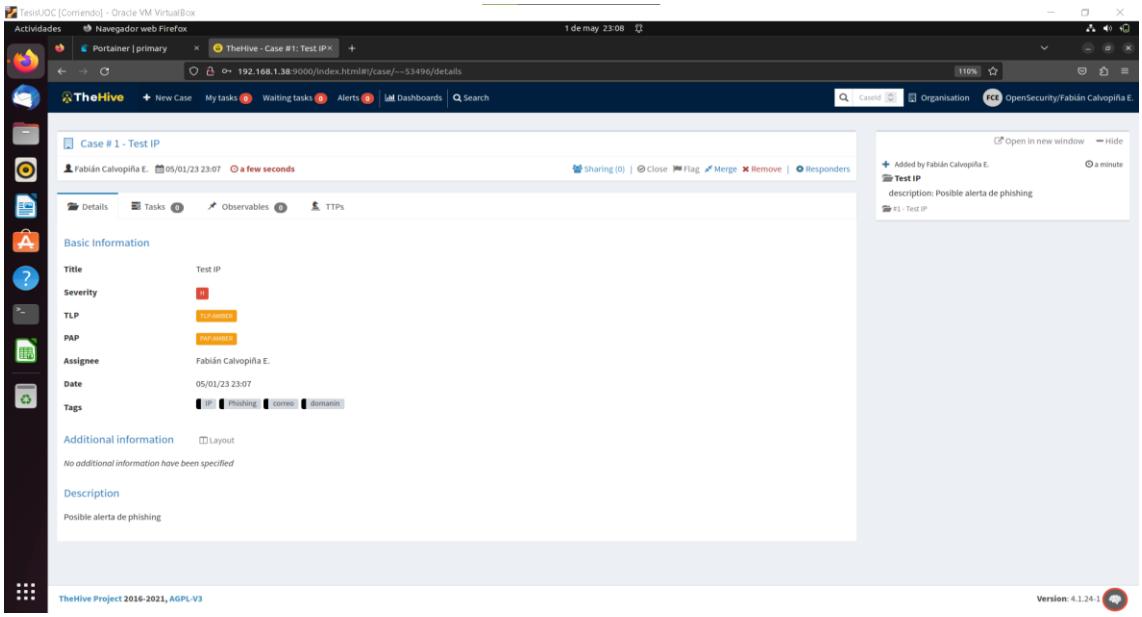


Logueo de Usuario fcalvopina

- De este modo estamos integrando la herramienta TheHive dentro de nuestra plataforma OpenCTI y se podrá visualizar los casos ingresados desde TheHive.

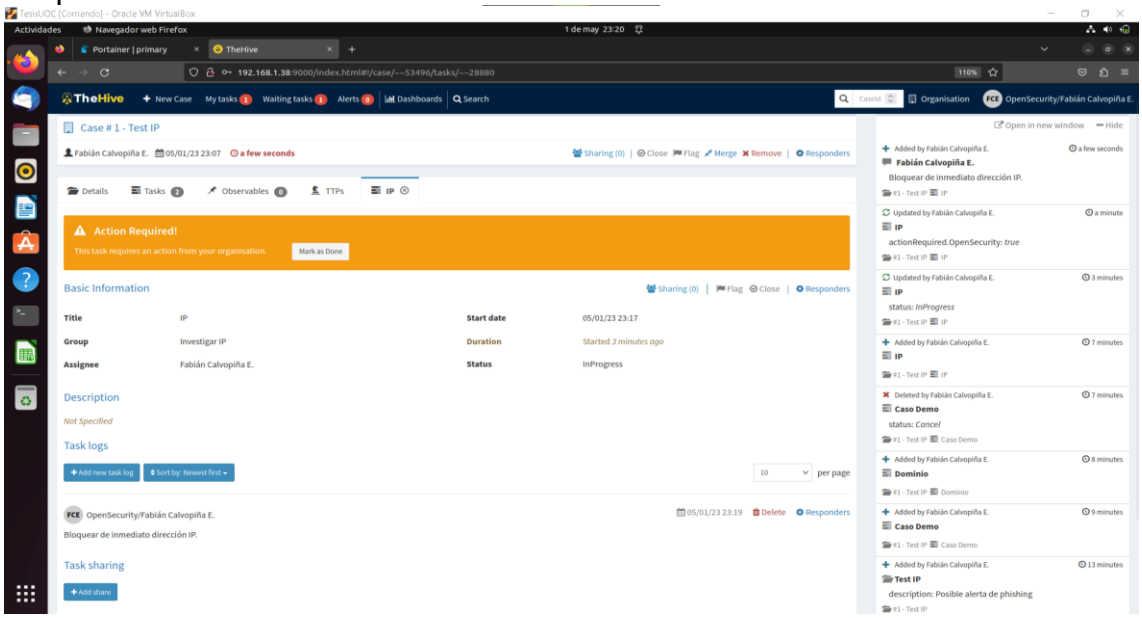
Por el momento vamos a crear un par de casos de ejemplo como prueba de test y para explicar el proceso:

Creación de casos:

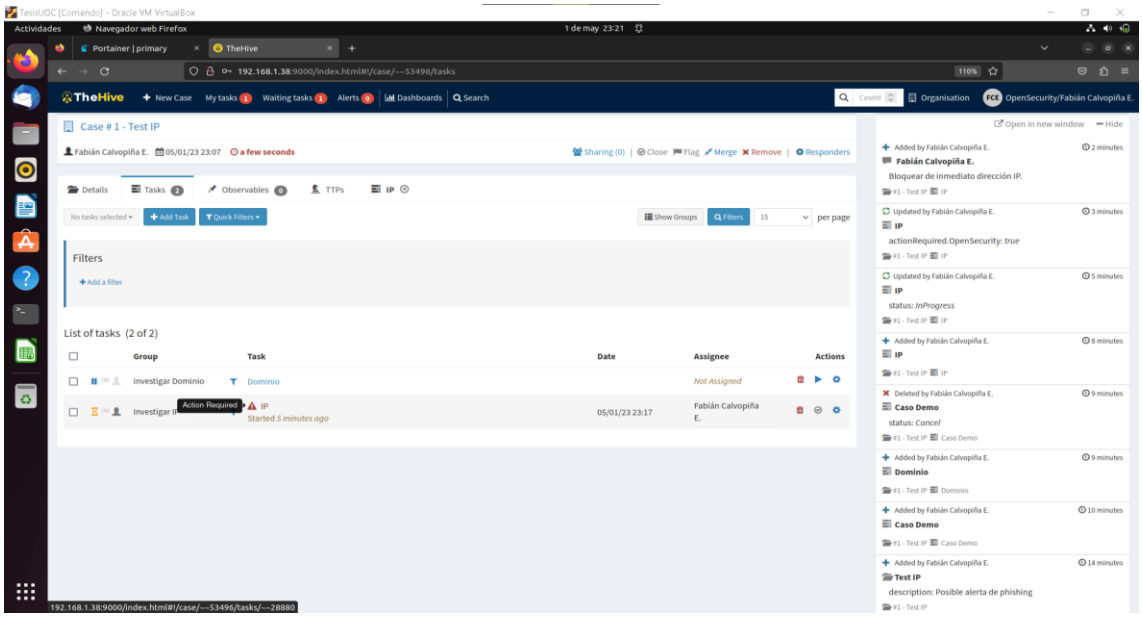


Añadimos nuevo caso

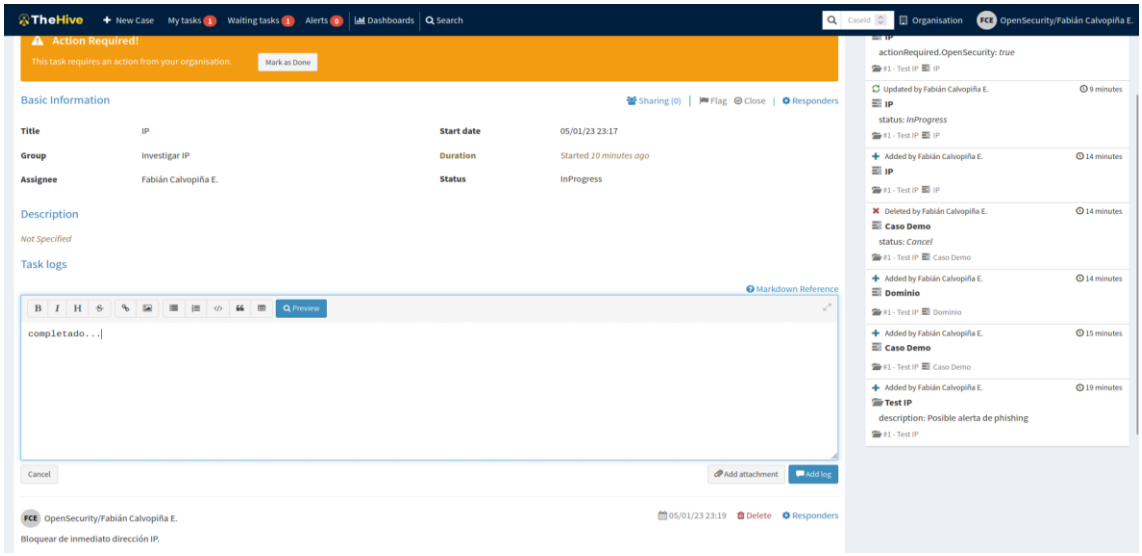
Requerir una acción:



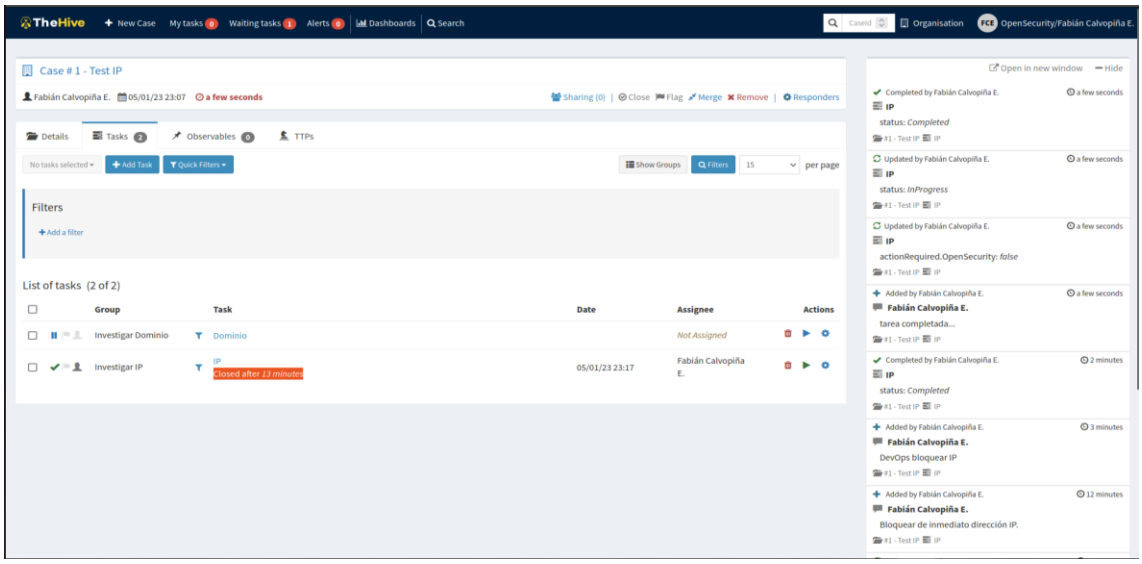
Verificamos en Tareas que ahora tenemos un aviso (alerta) del requerimiento creado en el paso anterior.



Si quiero puedo compartir la tarea con el equipo DevOps para poner en lista negra una dirección IP específica en el firewall.

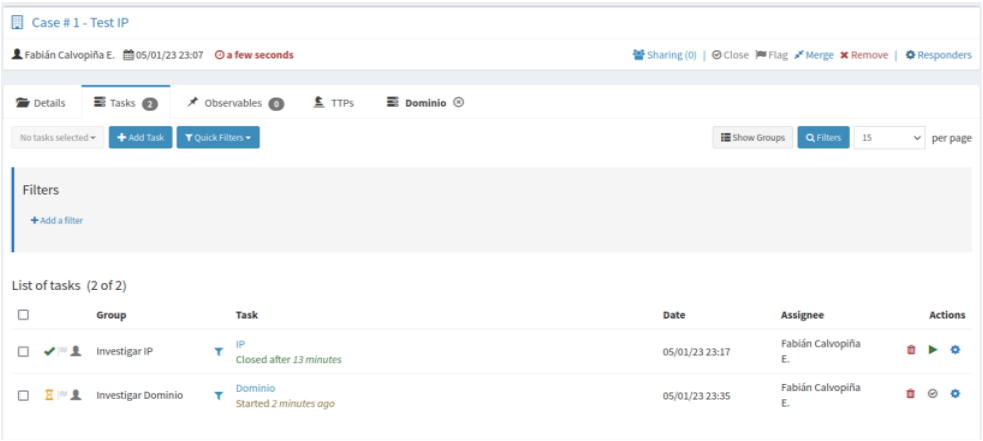


Con lo cual luego del completar la Tarea, puedo Cerrar la misma:

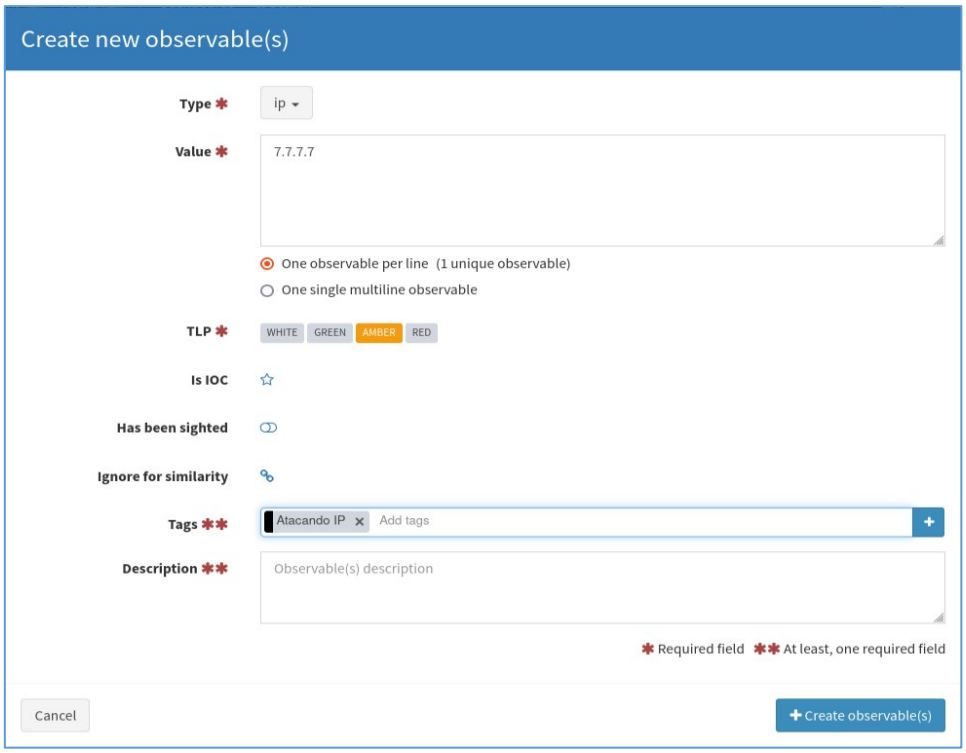


Ahora, un segundo usuario puede dar clic en **Start (play)** para apoyar a la otra tarea del **dominio**.

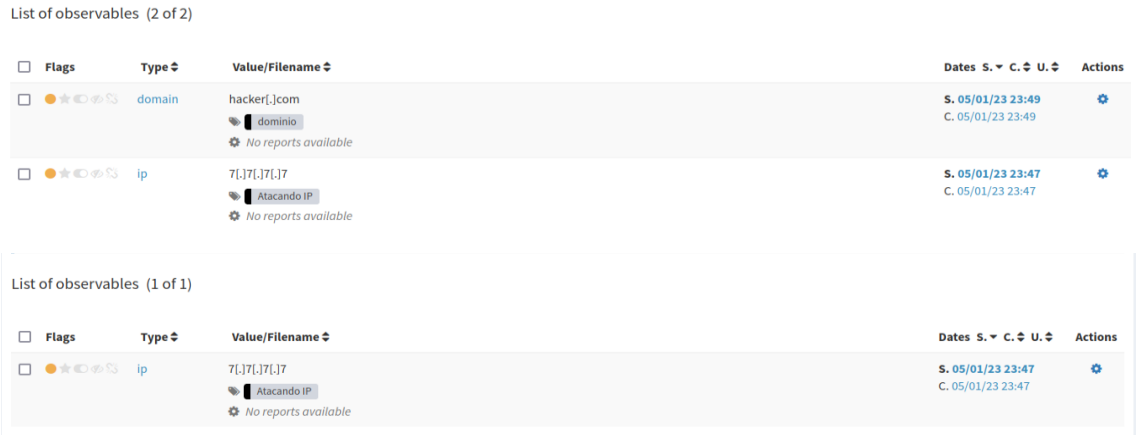
Podemos mirar que ahora la una tarea se encuentra completada y cerrada y los dos usuarios pueden trabajar en la Tarea faltante que forma parte del caso # 1.



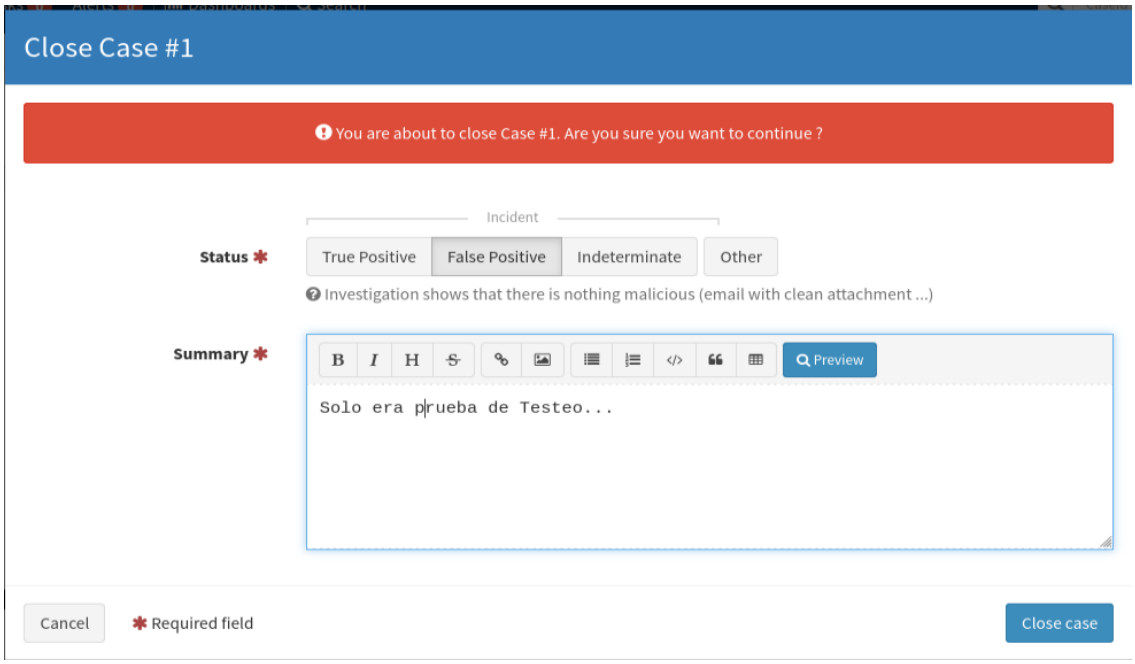
Vamos ahora a crear los **OBSERVABLES** :

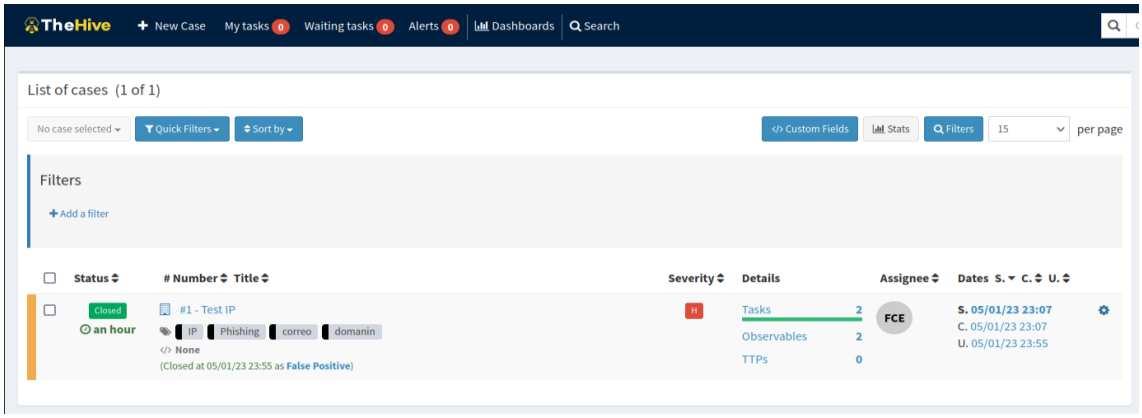


Entonces los observables creados se agregan:

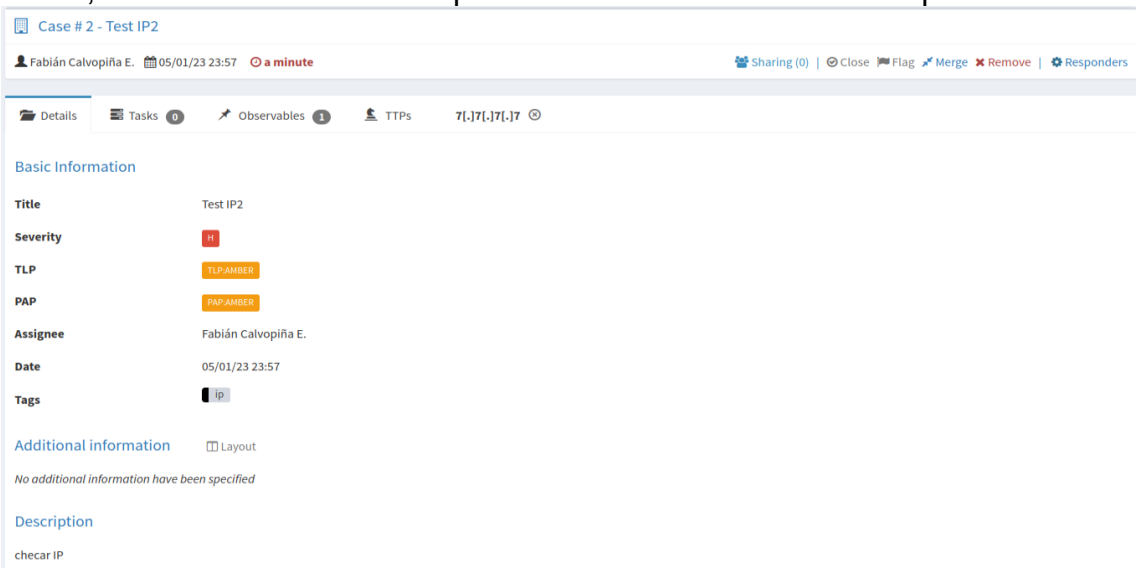


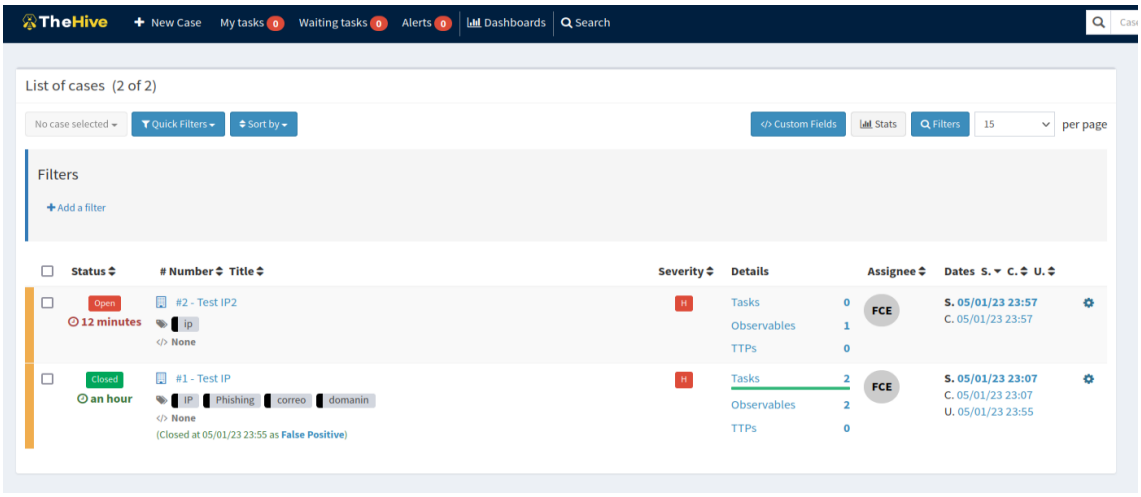
Una vez que se han cerrado todas las tareas, se puede cerrar el **Caso** y llenamos los datos de Status.



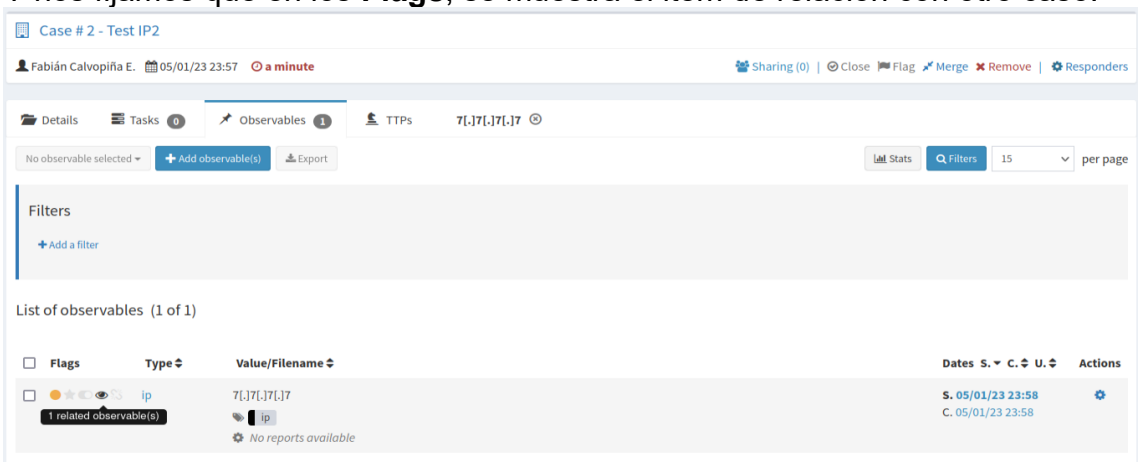


Ahora, creamos un nuevo caso para continuar con el análisis de prueba:

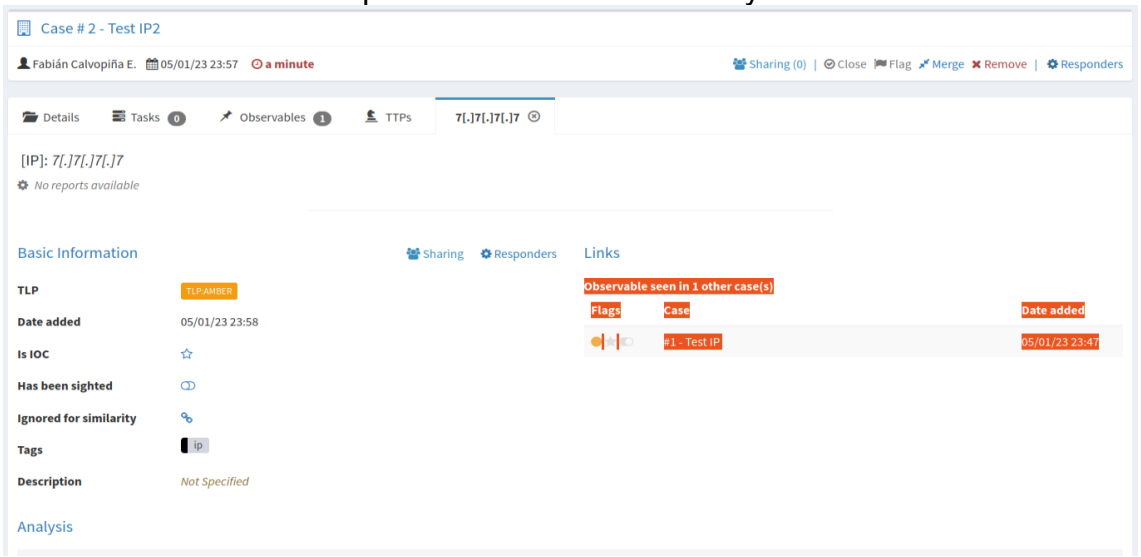




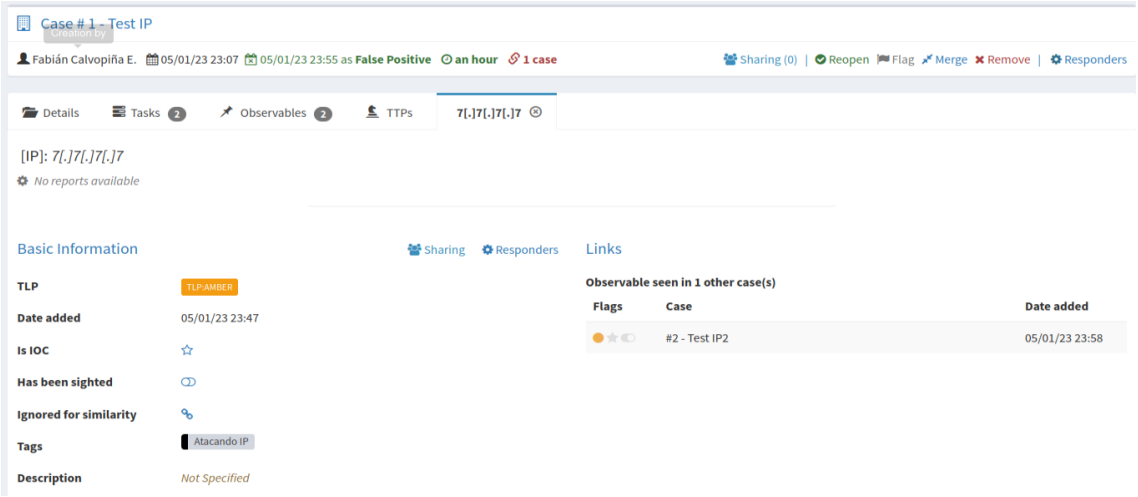
Y nos fijamos que en los **Flags**, se muestra el item de relación con otro caso:



Revisamos en el detalle que efectivamente la alerta ya se vió en otro caso:

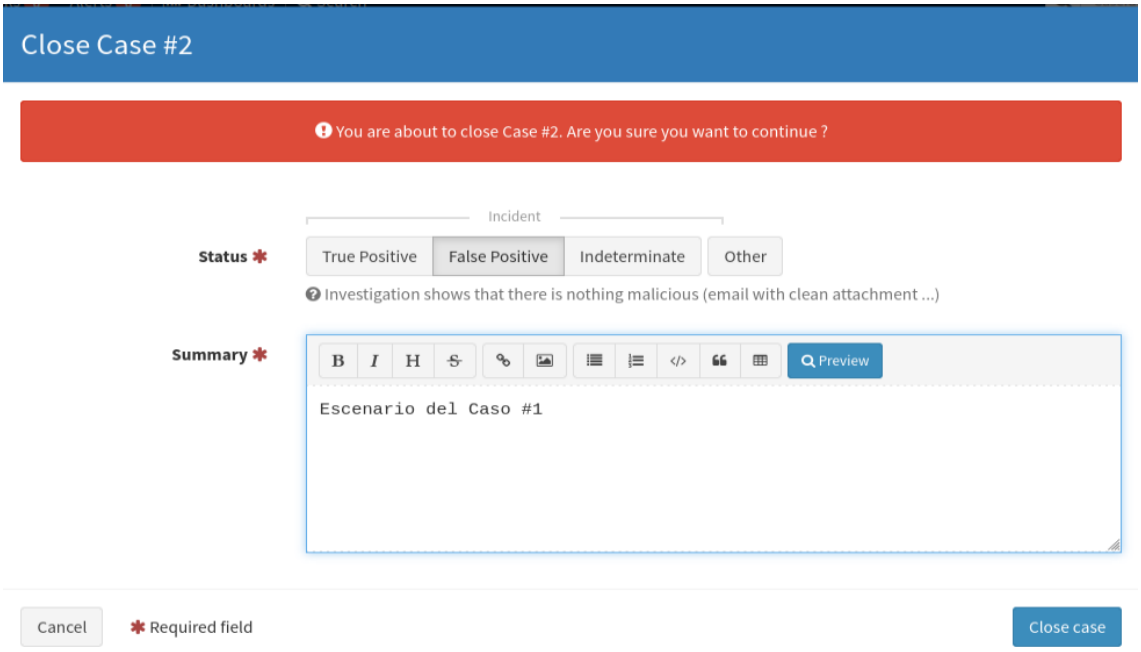


Podemos comprobar que si se vió en el Caso #1 que se creó anteriormente:

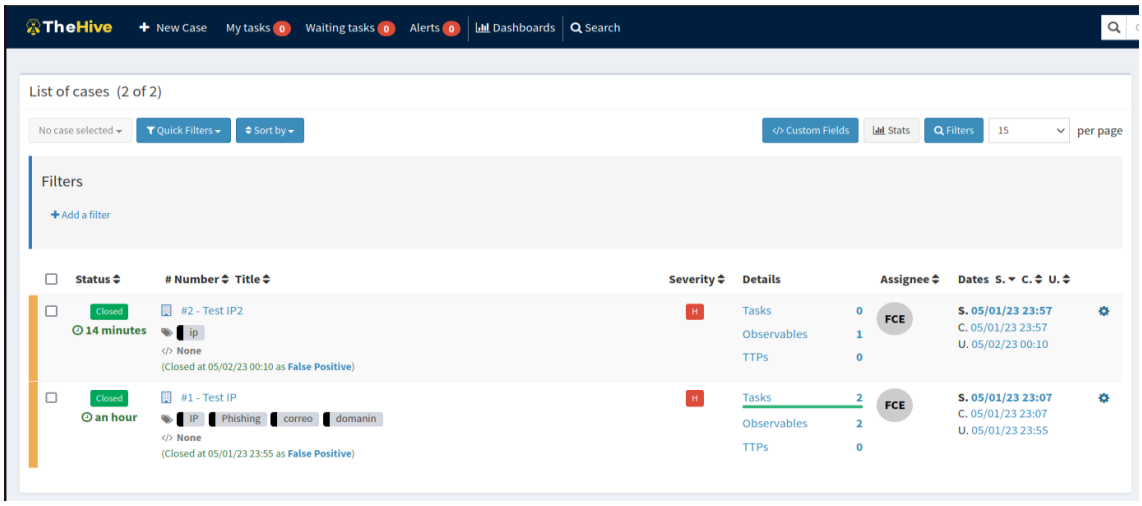


Con esta información, se replica instantáneamente en todos los usuarios sin necesidad de avisarles, ya que los diferentes observables se vinculan en todos los casos analizados.

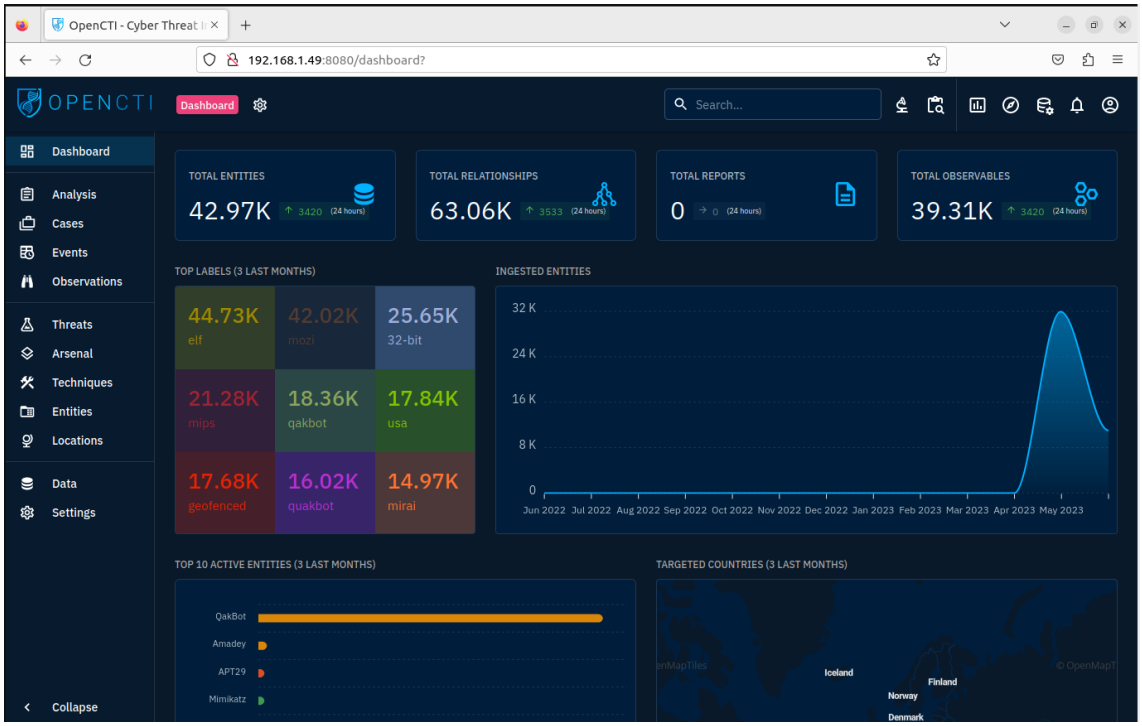
Cerramos el caso 2:



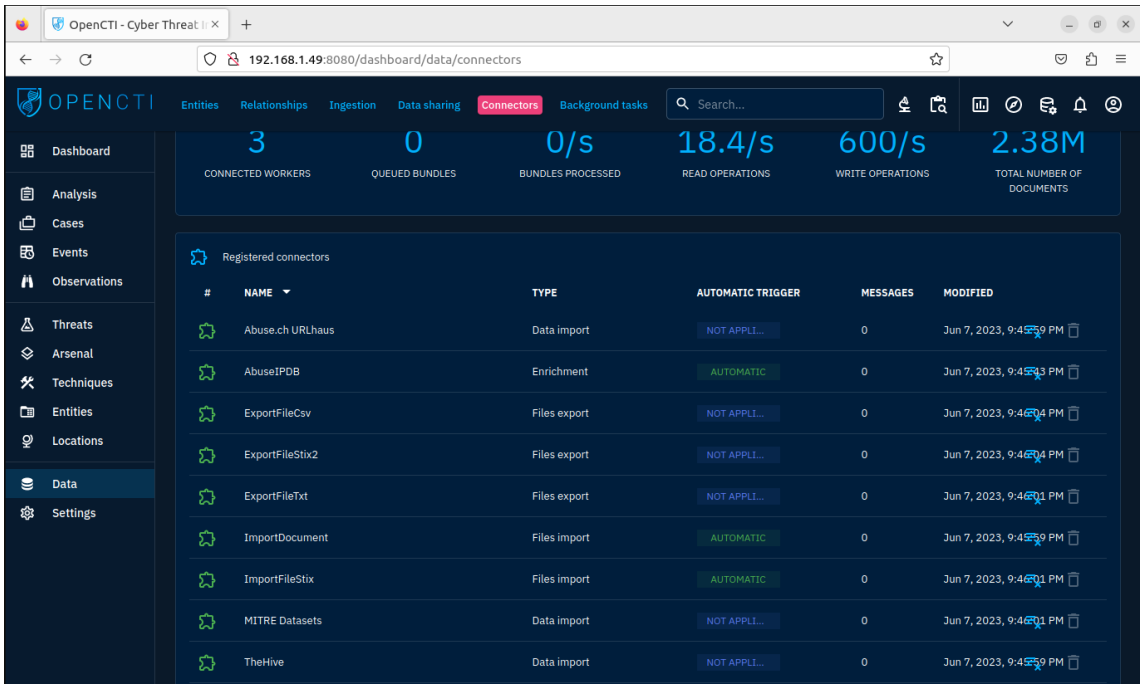
De este modo es como se manejará el proceso que involucra crear los casos y/o observables desde TheHive.



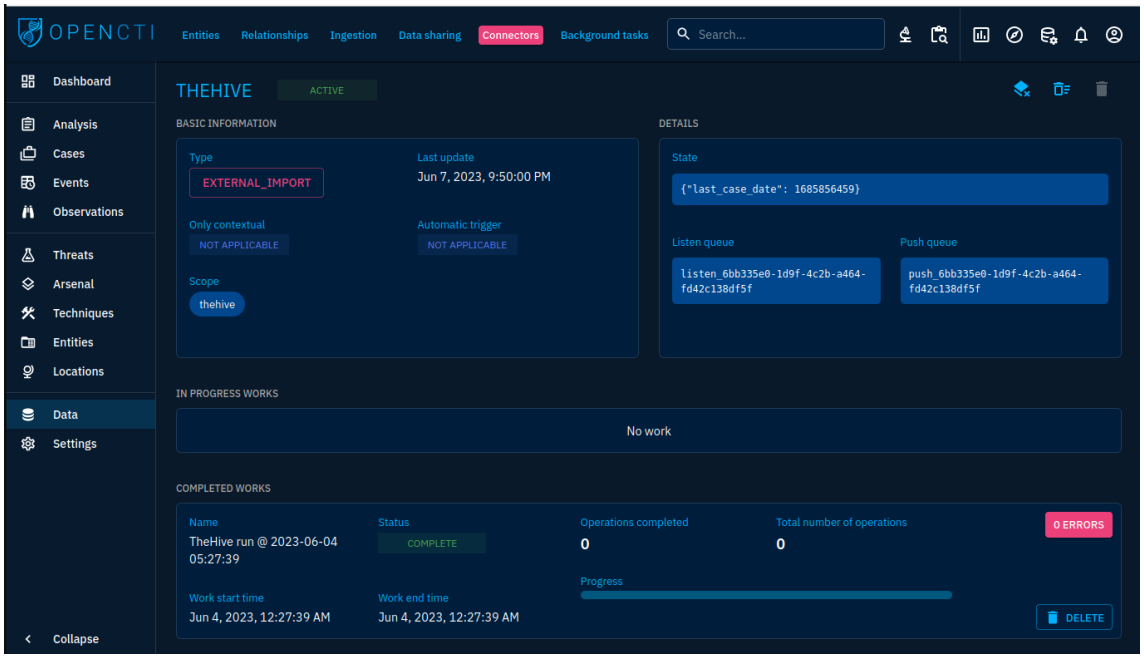
Integración en plataforma OpenCTI con información desde TheHive y sus conectores



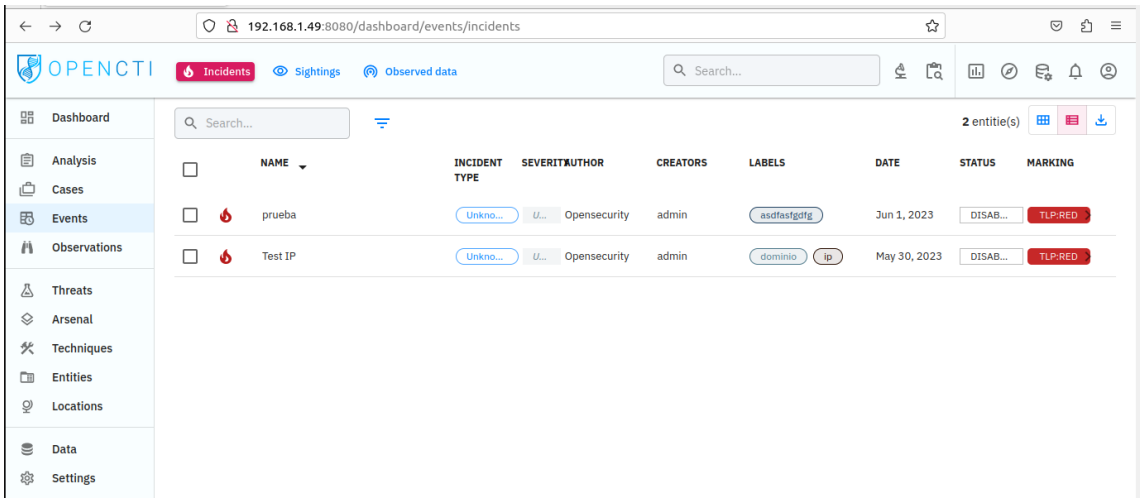
Conectores Integrados en OpenCTI:



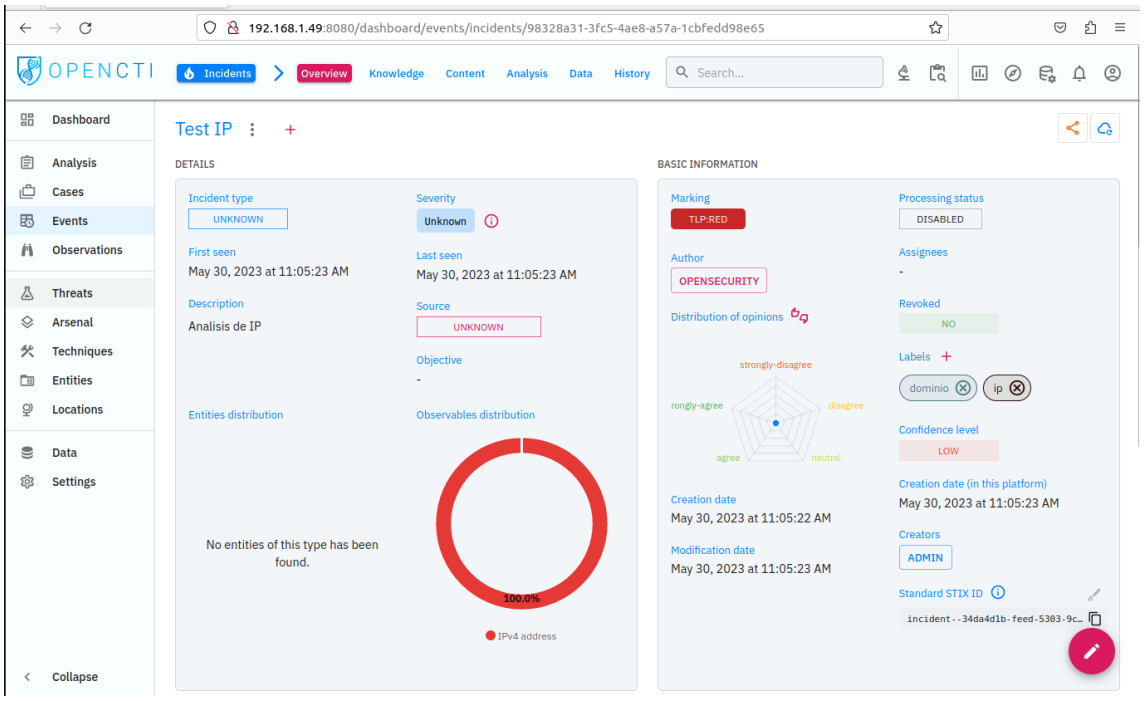
Conector TheHive



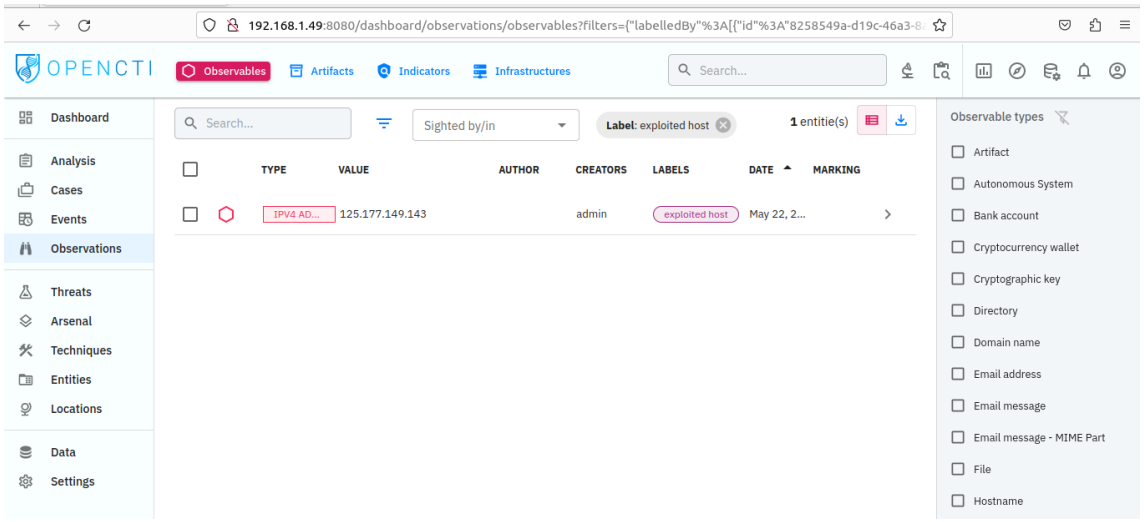
Carga de casos ingresados en TheHive:



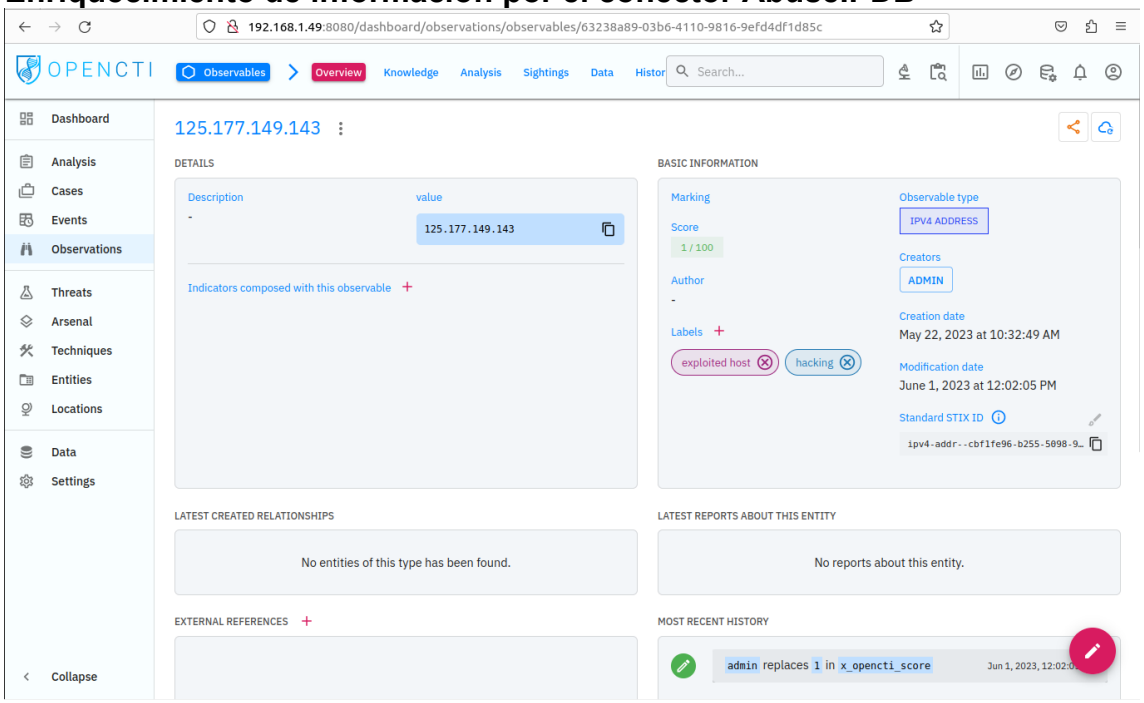
Revisión de incidente:

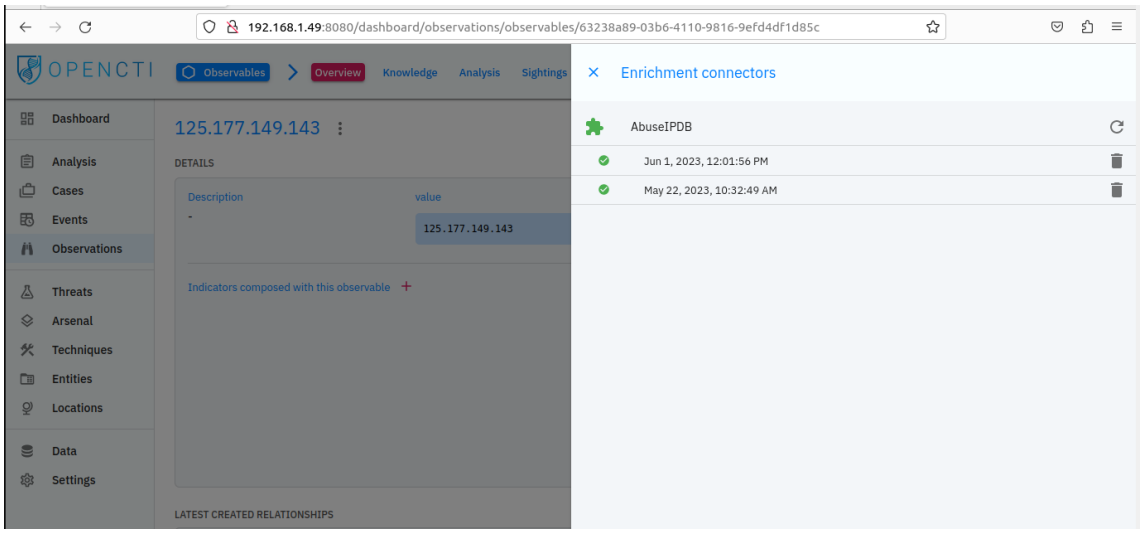


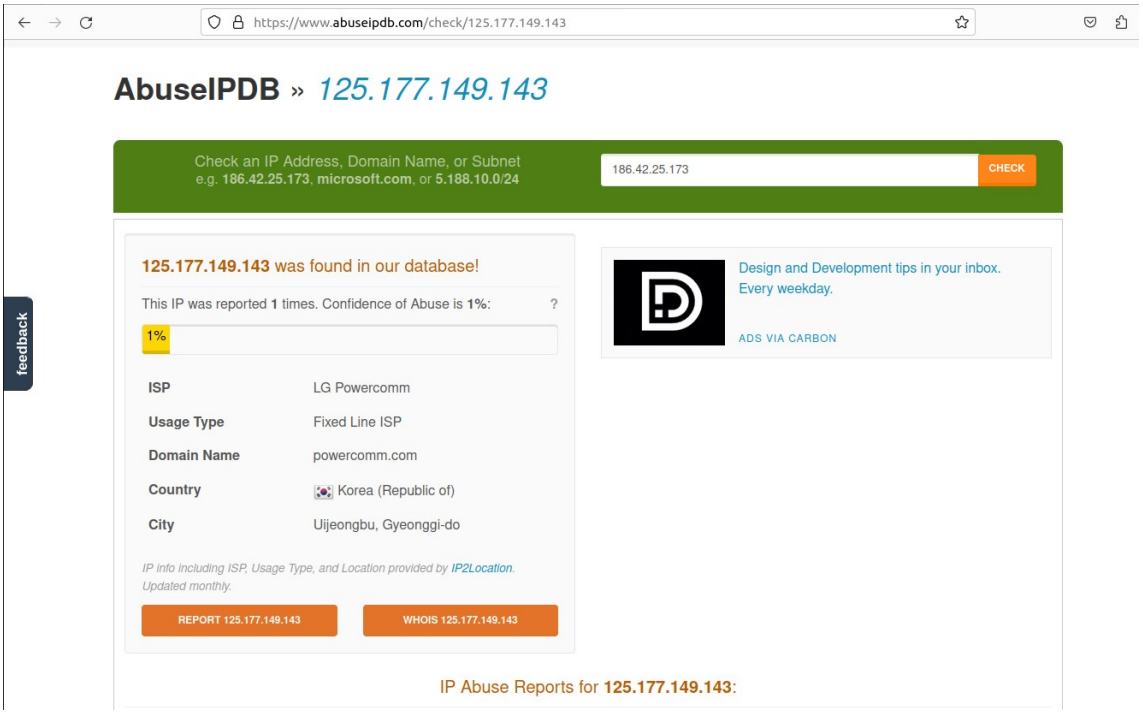
Observables:



Enriquecimiento de información por el conector AbuseIPDB






https://www.abuseipdb.com/check/125.177.149.143
AbuseIPDB » 125.177.149.143
Check an IP Address, Domain Name, or Subnet
e.g. 186.42.25.173, microsoft.com, or 5.188.10.0/24
186.42.25.173
CHECK
feedback
125.177.149.143 was found in our database!
This IP was reported 1 times. Confidence of Abuse is 1%:
1%
ISP
LG Powercomm
Usage Type
Fixed Line ISP
Domain Name
powercomm.com
Country
Korea (Republic of)
City
Uijeongbu, Gyeonggi-do
IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.
REPORT 125.177.149.143
WHOIS 125.177.149.143
Design and Development tips in your inbox.
Every weekday.
ADS VIA CARBON
IP Abuse Reports for 125.177.149.143: