UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Programa de Apoyo al Egreso para Alumnos con Práctica Profesional Supervisada

TÍTULO: Malware Information Sharing Platform y su integración a CERTUNLP

AUTOR: Pablo Germán Maddalena Kreff

DIRECTOR/A ACADÉMICO: Paula Venosa

DIRECTOR/A PROFESIONAL: Mateo Durante

CARRERA: Licenciatura en Sistemas

RESUMEN

La investigación aplicada se centra en la investigación e implementación de una plataforma que permite compartir indicadores de compromiso entre organizaciones. El objetivo principal es mejorar la colaboración y la comunicación entre las organizaciones, permitiendo un intercambio eficiente de información relevante.

Palabras Claves

cert, ciberseguridad, malware, indicadores de compromiso, ciberamenazas

Conclusiones

Para mejorar la postura de ciberseguridad de una organización, implementar MISP es un gran acierto. Sincronizar con otras comunidades las instancias de MISP y compartir eventos, correlacionar sus atributos y aportar a las organizaciones, tanto la propia como ajenas por medio de MISP es sumamente valioso.

Trabajos Realizados

En la búsqueda de mejora en el CERTUNLP, se ha encontrado que en el campo de la inteligencia de amenazas había un terreno para seguir trabajando para dar con alguna plataforma que reúna las características que puedan satisfacer las necesidades. Se implementó MISP y se sincronizó con instancias de otras organizaciones.

Trabajos Futuros

Integrar con otras plataformas, incorporar módulos e incluso incrementar las fuentes de información en el CERTUNLP. Por otra parte, MISP como tal tiene varios puntos para seguir mejorando.

Fecha de la presentación: DICIEMBRE 2023

Palabras Claves **2**
Marco Conceptual **2**
Introducción 2
CERTUNLP 3
Objetivo 4
Trabajo realizado **4**
Investigación 5
Implementación de la plataforma 21
Pruebas 28
Conclusiones 29
Líneas de posibles trabajos futuros **30**
Integraciones de MISP 30
Mejoras en Fuentes de Información 31
Mejoras sobre MISP 31
Bibliografía **33**

Palabras Claves

csirt, cert, ciberseguridad, malware, indicadores de compromiso, ciberamenazas

Marco Conceptual

El marco conceptual abarca una breve introducción al estado actual de la ciberseguridad así como al contexto donde se realizan las actividades en el CERTUNLP y su rol en el ámbito de la Universidad Nacional de La Plata (UNLP). Se incluye también en esta sección el objetivo para utilizar MISP como herramienta de inteligencia de amenazas.

Introducción

Internet ha revolucionado la forma en que nos comunicamos y compartimos información. Sin embargo, con esta revolución también han surgido nuevos desafíos en términos de seguridad. Aquí es donde entra en juego la ciberseguridad, que se ocupa de proteger nuestros sistemas, redes y aplicaciones de ciberataques.

A medida que los ciberdelincuentes se vuelven más sofisticados, la necesidad de una defensa proactiva se vuelve cada vez más crítica. Aquí es donde la inteligencia de amenazas juega un papel crucial. La inteligencia de amenazas implica la recopilación y análisis de información sobre amenazas potenciales para ayudar a las organizaciones a prevenir o mitigar los ciberataques.

En este contexto, herramientas como MISP (Malware Information Sharing Platform) pueden ser extremadamente útiles. MISP es una plataforma de código abierto para compartir, almacenar y correlacionar indicadores de compromisos de ataques cibernéticos. Permite a las organizaciones compartir información de amenazas de manera eficiente y puede ayudar a mejorar la postura de seguridad general de una organización.

Numerosas universidades han sido víctimas de ciberataques. Con realizar simples consultas en motores de búsqueda web podremos listar varias noticias relacionadas, con lo cual es atinado pensar que son objetivos de cibercriminales.

La Universidad Nacional de La Plata, como organización, cuenta con el CeSPI y allí es donde se desenvuelven las actividades del CERTUNLP, siendo la locación en la cual MISP es implementado.

CERTUNLP

El Centro Superior para el Procesamiento de la Información (CeSPI) es una dependencia de la Universidad Nacional de La Plata. En él se realizan las tareas vinculadas con el diseño, desarrollo, mantenimiento, configuración y administración de los sistemas informáticos que brindan servicios a todas las comunidades de la UNLP. Dichos sistemas se encuentran integrados entre sí con el objetivo de intercambiar información, integrar funcionalidades y simplificar la experiencia del usuario.

En el CeSPI se desarrollan las actividades del CERTUNLP (Centro de Respuestas de Incidentes de Seguridad) de la Universidad Nacional de La Plata. Se conformó en el año 2007 y se presentó formalmente a la comunidad académica en el marco de las actividades de la semana de la seguridad en noviembre del 2008 en la UNLP y a partir de esa fecha continúa trabajando en forma ininterrumpida.

Los objetivos del CERTUNLP son:

- Minimizar incidentes de seguridad en la red de la UNLP que puedan afectar a usuarios internos y externos.

- Desarrollar herramientas y mecanismos adecuados para detectar y prevenir situaciones que afecten la seguridad de la información de los usuarios, redes y servicios de la UNLP.
- Interactuar con la comunidad de CSIRTs.
- Definir y promover buenas prácticas de ciberseguridad entre la comunidad universitaria y la sociedad en su conjunto.
- Investigar incidentes de seguridad; asesorar a instituciones, organismos públicos y/o privados de Argentina y otros países en la prevención y mitigación de dichos incidentes.

La misión del CERTUNLP es prevenir, detectar, gestionar, mitigar e investigar problemas e incidentes de seguridad, coordinando acciones para la protección de los usuarios y los servicios de la UNLP. Además, propiciar el uso y apropiación de las Tecnologías de la Información y Comunicación y los cambios sociales necesarios para su aprovechamiento, que contribuyan a mejorar las funciones de educación, investigación científica y tecnológica y extensión universitaria que desarrolla la Universidad Nacional de La Plata; aportando a una sociedad sostenible social y ambientalmente.

De forma cotidiana, en el CERTUNLP se usan herramientas en pos de cumplir con sus objetivos. Éstas herramientas se pueden complementar y mejorar relacionándolas con otras, al mismo tiempo que incorporan información.

Incorporar al MISP como herramienta de colaboración entre organizaciones, para compartir información de amenazas, poder analizarlas y automatizar procesos para combatirlas es de gran importancia. En la búsqueda de ese horizonte es donde apunta ésta investigación aplicada.

Objetivo

Como se ha planteado en la propuesta de la Práctica Profesional Supervisada, las líneas principales expuestas del trabajo son la investigación acerca de proyectos e implementaciones existentes de MISP hoy en día en diversas organizaciones alrededor del mundo. Asimismo ha planteado analizar funcionalidades y módulos complementarios de la plataforma; investigar sobre cómo se comparten los eventos en MISP en diferentes comunidades de confianza; a la vez de integrar MISP al CERTUNLP.

Trabajo realizado

Bajo la premisa de una búsqueda de mejora en el CERTUNLP, junto a sus propias herramientas y sus fuentes de información, se ha encontrado que en el campo de la inteligencia de amenazas había un terreno para seguir trabajando para dar con alguna plataforma que reúna las características que puedan satisfacer las necesidades a los efectos de incrementar la seguridad de la comunidad objetivo, y simultáneamente colaborar con otras organizaciones.

Durante meses de investigación, búsqueda de fuentes de investigación, alianzas con otras organizaciones, e implementación de la plataforma encontrada; se han podido lograr todos los objetivos que a priori se habían planteado.

Investigación

Antes de profundizar sobre MISP, es oportuno comprender el motivo por el cual MISP ha sido elegido entre otros productos de software, incluso de compañías de gran prestigio y ampliamente reconocidas. Primero que todo, la búsqueda se ha acotado al tener como preferencia al software open-source, por numerosas virtudes.

MISP entre otros

Al analizar las propuestas en soluciones de inteligencia de amenazas se han listado por diferentes criterios las herramientas existentes.

Herramienta	Costo	Open Source	Vigente
AlienVault OTX	Gratis [1]/ Pago	No	Sí
CIF	Gratis	Sí	No
CRITs	Gratis	Sí	No
EclesticIQ	Pago	No	Sí
Flashpoint	Pago	No	Sì
Harpoon	Gratis	Sí	Sí
IBM X-Force Exchange	Pago	No	Sí
Kaspersky Threat Intelligence	Pago	No	Sí
MISP	Gratis	Sí	Sí
OpenCTI	Gratis [2]/ Pago	Sí	Sí
Recorded Future	Pago	No	Sí
ThreatConnect Threat Intelligence Operations Platform	Pago	No	Sí
ThreatQuotient	Pago	No	Sí
Trellix Threat Intelligence	Pago	No	Si
Yeti	Gratis	Sí	Sí
ZeroFox	Pago	No	Sí

Figura 1ª Cuadro comparativo entre soluciones de Inteligencia de Amenazas
Se han pintado en verde los primeros criterios de búsqueda.

[1]Ofrece características limitadas de forma gratuita
[2] Edición gratuita “Community Edition” y de paga “Enterprise Edition”

Algunas de las herramientas sobre inteligencia de amenazas eran gratuitas y open-source, pero eran proyectos que no recibían actualizaciones, en algunos casos por años. Otras de estas herramientas no ofrecen una variedad de funciones, como la recopilación, el análisis y el intercambio de inteligencia de amenazas. Es por ello que se han ido decantando entre algunas propuestas: MISP; OpenCTI; Yeti y Harpoon.

Los cuatro proyectos tienen en común que publican su código fuente en GitHub, con lo cual podemos compararlos[3]

	MISP	OpenCTI	Yeti	Harpoon
Fundadores	Co Fundado por la Unión Europea	Filigran	N/A[4]	Etienne "Tek" Maynier
GitHub	https://github.com/MISP/MISP	https://github.com/OpenCTI-Platform/opencti	https://github.com/yeti-platform/yeti	https://github.com/Te-k/harpoon
Licencia	AGPL 3.0	Apache 2.0	Apache 2.0	GPL 3.0
Cantidad de contribuidores	213	70	50	12
Último lanzamiento	versión 2.4.178 (octubre 2023)	versión 5.11.13 (noviembre 2023)	versión 1.8.5 (febrero 2022)	N/A[5]
Lanzamientos publicados	100	137	11	N/A[6]
Puntaje[7]	4.7k	4.1k	1.5k	1.1k
Observadores[8]	276	119	95	50
Bifurcaciones[9]	1.3k	740	281	186

Figura 2ª Cuadro comparativo de los productos de software basados en GitHub

Según el cuadro comparativo podemos concluir que MISP y OpenCTI están mejor respaldados en cuanto a la trayectoria de sus fundadores frente a Yeti y Harpoon. Otras de las virtudes que tienen MISP y Open CTI es que son muy difundidos, aceptados y despiertan gran interés en la comunidad de desarrolladores, a la par que ofrecen funcionalidades adicionales y mejor integración. Ahora la decisión queda entre MISP y OpenCTI.

---

[3] Los datos del cuadro comparativo de GitHub se han tomado el día 11/11/2023
[4] La organización no publica sus miembros.
[5] Sin fecha disponible. No han diferenciado lanzamientos a lo largo del desarrollo.
[6] Sin cantidad disponible. No han diferenciado lanzamientos a lo largo del desarrollo.
[7] Se toma el valor de “Stars”, que representa la cantidad de usuarios que lo han marcado como favorito.
[8] Se toma el valor de “Watching”, que representa la cantidad de usuarios que reciben notificaciones específicas (discusiones).
[9] Se toma el valor de “Forks”, que representa la cantidad de bifurcaciones que se han realizado.

Diferencias entre MISP y OpenCTI (Community Edition)

Si bien MISP y OpenCTI ofrecen muchas características similares, existen algunas diferencias clave entre las dos plataformas que vale la pena considerar.

1) Modelado de entidades

Una de las diferencias entre MISP y OpenCTI es la forma en que manejan el modelado de entidades. MISP utiliza un conjunto predefinido de modelos de datos, lo cual significa que los usuarios de MISP deben adaptar sus datos a estos modelos predefinidos. Aunque esto puede limitar la flexibilidad, también puede simplificar el proceso de modelado de datos, ya que los usuarios no necesitan definir sus propios modelos. OpenCTI permite a los usuarios definir sus propios modelos de entidades. Esto brinda a los usuarios una mayor flexibilidad en la forma en que mapean y analizan sus datos de inteligencia de amenazas, aunque también puede requerir un mayor esfuerzo por parte de los usuarios para definir y mantener sus propios modelos. MISP usa el modelo de datos MISP y cuenta con conversores a STIX2 (y viceversa), mientras que OpenCTI usa STIX2, que está más dirigido a describir, Técnicas, Técnicas y Procedimientos (TTP), mientras que MISP se trata más de compartir Indicadores de Compromiso.

2) Integración

Tanto MISP como OpenCTI, ofrecen integración con una variedad de fuentes de datos y otras herramientas de seguridad. Sin embargo, MISP ofrece una gama más amplia de integraciones que OpenCTI, gracias en parte a su historia más larga y su base de usuarios más grande.

3) Comunidad

MISP tiene una comunidad de usuarios y colaboradores más grande que OpenCTI, lo que significa que tiene un grupo más grande de recursos y soporte disponible. Sin embargo, OpenCTI está aumentando rápidamente su base de usuarios y su comunidad, lo que podría cambiar en el futuro.

En conclusión, MISP es una plataforma flexible y escalable que puede ser utilizada por organizaciones de todos los tamaños. Es madura con una gama más amplia de integraciones y una comunidad de usuarios abundante. Su gran comunidad de usuarios y desarrolladores que pueden proporcionar apoyo y recursos, incluso ampliando sus funcionalidades con módulos y nuevas integraciones.

Análisis de MISP e Inteligencia de Amenazas

MISP es una plataforma de código abierto para compartir, almacenar y correlacionar indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidades o incluso información de contrainteligencia. MISP es utilizado hoy en día múltiples organizaciones no solo para almacenar, compartir y colaborar en indicadores de ciberseguridad y análisis de malware, sino también para utilizar los Indicadores de Compromiso y la

información para detectar y prevenir ataques, fraudes o amenazas contra infraestructuras TIC, organizaciones o personas. Un Indicador de Compromiso (IoC, por sus siglas en inglés) es cualquier rastro o evidencia que indique que se accedió sin autorización a un sistema de datos. Este tipo de evidencia se utiliza para reforzar la estrategia de ciberseguridad y robustecer los sistemas ante cualquier amenaza. Los indicadores de compromiso permiten identificar brechas de ciberseguridad y son elementos que ayudan a detectar actividades maliciosas.

Existen múltiples razones por las cuales una organización pueda utilizar MISP:

Compartir información de amenazas: MISP permite a las organizaciones compartir información sobre amenazas de seguridad de manera estructurada. Esto incluye indicadores de compromiso (IoCs), información sobre malware, tácticas, técnicas y procedimientos (TTPs), y más. Compartir esta información puede ayudar a otras organizaciones a defenderse contra amenazas similares.

Colaboración: MISP facilita la colaboración entre organizaciones y equipos de ciberseguridad. Puede utilizarse para coordinar la respuesta a incidentes, compartir conocimientos y mejorar la seguridad en conjunto.

Análisis de amenazas: MISP proporciona herramientas para el análisis de amenazas. Los analistas pueden utilizar la plataforma para correlacionar y analizar datos de amenazas, identificar patrones y tendencias, y tomar decisiones informadas sobre cómo defenderse contra amenazas.

Automatización: MISP permite la automatización de tareas de ciberseguridad. Puede integrarse con otras herramientas de seguridad para automatizar la recolección de información de amenazas, la actualización de reglas de detección y la respuesta a incidentes.

Inteligencia de amenazas: La plataforma también se utiliza para crear y mantener bases de datos de inteligencia de amenazas, lo que ayuda a las organizaciones a estar al tanto de las últimas amenazas y a tomar medidas proactivas para protegerse.

MISP posee una gran comunidad de usuarios que crean, mantienen y operan comunidades de usuarios u organizaciones que comparten información sobre amenazas o indicadores de ciberseguridad en todo el mundo. El proyecto MISP no mantiene una lista exhaustiva de todas las comunidades que confían en MISP, especialmente porque algunas comunidades usan MISP internamente o en privado. Cada comunidad puede tener reglas específicas para unirse a ellas.

Su amplia gama de funcionalidades y módulos complementarios lo hacen altamente adaptable a las necesidades particulares de cada organización. Además, su gran comunidad de usuarios y su enfoque en el intercambio de información lo convierten en una herramienta valiosa para mejorar la colaboración y el intercambio de información entre organizaciones confiables.

MISP es una herramienta de tipo Threat Intelligence, lo que implica el análisis y procesamiento de múltiples datos, tanto de las causas, los motivos, los objetivos y los comportamientos de los ataques llevados adelante por ciberdelincuentes. La inteligencia de amenazas, Threat Intelligence, es el resultado del enriquecimiento de los datos que se recopilan, procesan y analizan para comprender las causas, motivos, objetivos y comportamientos de ataque de los ciberdelincuentes. Por otro lado, la cacería de amenazas, Threat Hunting, se trata de una búsqueda proactiva de amenazas internas o externas que permite identificar las amenazas de ciberseguridad que acechan sin ser detectadas en la red de las organizaciones, incluso es posible identificar intrusos en la red que hayan evadido

defensas sin ser detectados. Threat Hunting tiene como objetivo al proceso continuo e iterativo centrado en la capacidad analítica humana de buscar actividades anormales en los activos de la organización que podrían significar compromiso, intrusión o exfiltración de los datos de una organización. Este proceso, que parte de la idea de que el atacante ya obtuvo acceso a los sistemas de la organización, se realiza monitoreando la red y los distintos elementos que conforman la misma.

Threat Intelligence y Threat Hunting son dos enfoques diferentes para aumentar las defensas de ciberseguridad de una organización contra atacantes. Ambas aportan valiosos resultados en la estrategia de ciberseguridad de las organizaciones, y si bien son dos metodologías completamente diferentes, al complementarse pueden generar resultados aún más valiosos.
El Threat Hunting basado en Inteligencia de amenazas parte desde hashes, direcciones IP, dominios y/o artefactos[10] proporcionados principalmente por plataformas de Threat Intelligence, como es MISP, ya sea de fuentes abiertas o privadas, pudiendo exportar desde estas plataformas una serie de alertas para que sean introducidas de forma automática en soluciones como los SIEM[11]/SOAR[12] en formato de expresión de información estructurada sobre amenazas (STIX [3]) o intercambio automatizado de confianza de información de inteligencia (TAXII [4]).

Structured Threat Information eXpression (STIX) es un lenguaje estandarizado que utiliza un léxico basado en JSON[13] para expresar y compartir información sobre amenazas en un formato legible y coherente. Permite el intercambio de información sobre ciberamenazas entre los sistemas bajo una sintaxis común para que los usuarios puedan describir las amenazas.

Figura 3ª Uso de STIX para compartir indicadores
Traducido de documentación de STIX

[10] Registro o huella creada a partir de tecnologías digitales.
[11] SIEM (Security Information and Event Management), es un sistema para la gestión de la información sobre seguridad y gestión de eventos basado en diferentes logs (registros).
[12] SOAR (Security Orchestration, Automation, and Response), es un sistema que aprovecha datos de diversas herramientas relacionadas con la ciberseguridad para responder incidentes.
[13] JSON (JavaScript Object Notation) es un formato de texto simple que forma parte del sistema de JavaScript ,que se deriva de su sintaxis, para el intercambio de datos.

STIX 2.1 define 18 Objetos de Dominio STIX (SDOs). Los usados en la Figura 3ª son:

Icono	Significado
	Vulnerabilidad: Un error en el software que un pirata informático puede utilizar directamente para obtener acceso a un sistema o red.
	Indicador: Contiene un patrón que se puede utilizar para detectar actividad cibernética sospechosa o maliciosa.
	Campaña: Una agrupación de comportamientos adversarios que describe un conjunto de actividades o ataques maliciosos (a veces llamados oleadas) que ocurren durante un período de tiempo contra un conjunto específico de objetivos.
	Actor de amenaza Personas, grupos u organizaciones reales que se cree que operan con intenciones maliciosas.

Íconos y significados traducidos y tomados de la documentación oficial de STIX

Trusted Automated Exchange of Intelligence Information (TAXII) es un protocolo de aplicación para intercambiar CTI[14]a través de HTTPS[15].
TAXII define una API RESTful (un conjunto de servicios e intercambios de mensajes) y un conjunto de requisitos para los Clientes y Servidores de TAXII. Como se muestra a continuación, TAXII define dos servicios principales para respaldar una variedad de modelos comunes de uso compartido:

1) Colecciones: una colección es una interfaz para un repositorio lógico de objetos CTI proporcionado por un servidor TAXII que permite a un productor alojar un conjunto de datos CTI que pueden ser solicitados por los consumidores: los clientes y servidores TAXII intercambian información en un modelo de solicitud-respuesta.

2) Canales: mantenido por un servidor TAXII, un canal permite a los productores enviar datos a muchos consumidores y a los consumidores recibir datos de muchos productores: los clientes TAXII intercambian información con otros clientes TAXII en un modelo de publicación-suscripción.

[14] Cyber Threat Intelligence
[15] Hyper Text Transfer Protocol Secure

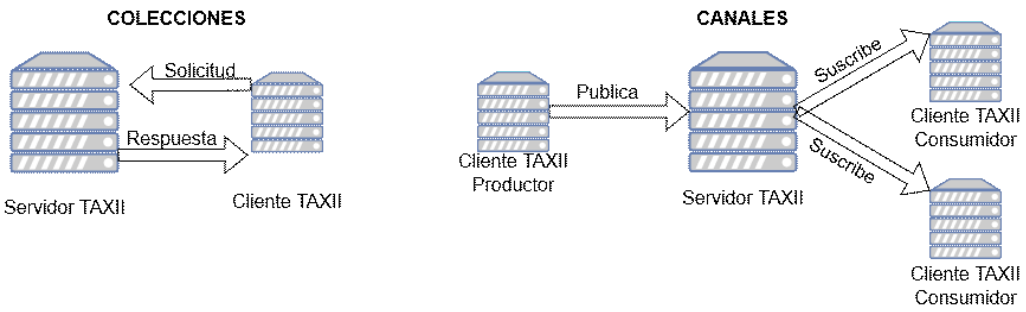


Figura 4ª Uso de los dos modelos de TAXII : Colecciones y Canales
Traducido de la documentaciòn de TAXII

STIX y TAXII son estándares independientes. STIX no depende de un método de transporte específico y se puede usar TAXII para transportar información y datos que no sean STIX. Aunque al utilizarse juntos, STIX/TAXII forman un marco para compartir y utilizar la información sobre amenazas, creando una plataforma de código abierto que permite a los usuarios buscar en registros que contienen detalles de vectores de ataque, como direcciones IP maliciosas, firmas de malware y agentes de amenazas.

Una vez que los sistemas de Threat Hunting basados en Threat Intelligence fueron alimentados con todos estos IoC, se puede investigar la actividad previa y posterior a la ocurrencia de los eventos para identificar cualquier compromiso de los activos apoyándose de otras herramientas y estándares de la industria existentes. MISP soporta el uso de STIX y TAXII, con lo cual facilita la integración y comunicación con otras plataformas y servicios.

Conceptos de MISP

Es necesario comprender algunos conceptos básicos de MISP:

- Todos los datos de malware ingresados en MISP se componen de objetos de eventos.
- Los eventos son contenedores de información vinculada contextualmente, a partir de un incidente, un informe de seguridad o un análisis de actores de amenazas
- Los eventos contienen atributos con indicadores.
- Los indicadores contienen un patrón que se puede utilizar para detectar sospechas o actividad maliciosa.
- Los IoC son un subconjunto de indicadores.
- Cada evento solo puede ser editado directamente por los usuarios del creador original de la organización. Sin embargo, si otra organización quisiera modificar un evento con información adicional sobre un evento, o si desean corregir un error en un atributo, pueden crear una propuesta.
- Las propuestas pueden ser aceptadas por el creador original.
- Las propuestas se pueden enviar a otro servidor, lo que permite a los usuarios instancias conectadas para proponer cambios que, de ser aceptados, pueden ser posteriormente rechazado.
- Se puede establecer la privacidad de la organización informante.
- MISP tiene una funcionalidad para delegar la publicación y eliminar el vínculo entre la información compartida y su organización. Se puede delegar la publicación a otra organización. La otra organización puede asumir la propiedad de un evento y proporcionar pseudoanonimato para la organización inicial.

MISP usa objetos que pueden ser utilizados por otra herramienta para compartir información. Los objetos MISP se suman a los atributos MISP para permitir combinaciones avanzadas de atributos. La creación de estos objetos y sus atributos asociados se basan en casos de uso reales de ciberseguridad y prácticas existentes en el intercambio de información. Los objetos simplemente se comparten como cualquier otro atributo en MISP incluso si las otras instancias de MISP no tienen la plantilla del objeto. En otras palabras, los objetos MISP son contenedores para agrupar atributos relacionados contextualmente. Los objetos permiten a los analistas agrupar atributos relacionados y describir las relaciones que existen entre los puntos de datos en un evento de amenaza[16].

En MISP, un evento es una unidad estructurada de información de amenazas. Los eventos pueden incluir información como nombres de host maliciosos, enlaces, direcciones IP y *hashes*[17]. Una de las características más poderosas de MISP es la correlación automática entre eventos relacionados.

La correlación en MISP es una forma de encontrar relaciones entre atributos e indicadores de malware o campañas de ataques. La correlación ayuda a los analistas a detectar grupos de actividades similares y rotar de un evento a otro.

Por otra parte, MISP usa *Galaxy Cluster*, que es un método simple para expresar un objeto grande en el que se pueden adjuntar eventos o atributos. *Galaxy Cluster* es un grupo que puede estar compuesto por uno o más elementos. Los elementos se expresan como valores-clave. Hay vocabularios predeterminados disponibles en Galaxy Cluster, pero se pueden sobrescribir, reemplazado o actualizado como desee. Los grupos y vocabularios existentes se pueden utilizar tal cual o como una plantilla. La distribución MISP se puede aplicar a cada grupo para permitir una distribución limitada o más amplia.
esquema de distribución.
Así mismo, en MISP se hace uso de etiquetas, que son una forma simple de adjuntar una clasificación a un evento o atributo. La clasificación debe ser utilizada globalmente para ser eficiente.

Uso de MISP por parte de diferentes organizaciones vinculadas a la ciberseguridad.

Hay diferentes comunidades de MISP, que van desde el sector financiero hasta organizaciones CSIRT. Las hay tanto de tipo públicas como privadas, y es por ello que como cada comunidad tiene sus propias reglas uno es libre de ponerse en contacto con ellas a los fines de compartir información.

Algunas de la organizaciones que usan MISP son: CERT-FR; CIRCL; CSIRT Americas Network; CSSA; CiviCERT; ColCERT; Danish MISP Community; CSIRT-PONAL; MISP-LEA; NATO; PISAX y X-ISAC.

Por contraparte, MISP también se ofrece como servicio de instancia. También hay comunidades que comparten la información bajo pago para entornos empresariales. Algunas de las organizaciones que ofrecen sus servicios son:

---

[16] Es el problema que potencialmente puede ocurrir si se aprovecha una debilidad de un sistema
[17] Es el resultado de un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

- CUDESO: Instalación y configuración a medida de servidores MISP. Módulos de contextualización y enriquecimiento. Soporte para la integración y automatización de MISP en el flujo de trabajo de gestión de incidentes. Talleres de capacitación y mejores prácticas del MISP.
- ESET: Acceso al servidor MISP de ESET. Servicio de feed que consta de información APT [18] producida por la investigación de ESET. En general, la fuente es una exportación del servidor MISP interno de ESET. Todos los datos que se comparten también se explican con mayor detalle en los informes APT.
- The DFIR Report: Servicio de fuentes de amenazas mediante su instancia MISP, a la que se puede acceder a través de la web, API o MISP Sync.

Con lo expuesto, es notable la cantidad de organizaciones ya sean públicas, privadas, gratuitas o pagas que pertenecen y dan soporte a la comunidad de MISP.

Manejo de información en MISP

Existe una gran comunidad de usuarios de MISP que crean, mantienen y operan comunidades de usuarios u organizaciones que comparten información sobre amenazas o indicadores de ciberseguridad en todo el mundo. El proyecto MISP no mantiene una lista exhaustiva de todas las comunidades que dependen de MISP, especialmente que algunas comunidades usan MISP interna o privadamente.
MISP integra una funcionalidad llamada *feed* que permite obtener eventos MISP directamente desde un servidor sin acuerdo previo. Dos fuentes OSINT (*CIRCL OSINT Feed* y por otro lado *Botvrij.eu OSINT feed*) se incluyen de forma predeterminada en MISP y se pueden habilitar en cualquier instalación nueva.El formato con el que se comparten es JSON, tal como se puede ver en los *feeds* de http://www.botvrij.eu/data/feed-osint/ y https://www.circl.lu/doc/misp/feed-osint/

Dependiendo del sector al que pertenezca cada organización, la información a compartir va a diferir. MISP se usa en el sector financiero, incluidos bancos, instituciones financieras y organizaciones de procesamiento de pagos; en CSIRTs; organizaciones gubernamentales; Global Security Exchange (GSX); Internet eXchanges Points (IXP); e incluso relacionado a la salud y las ciberamenazas como el caso de COVID-19 MISP Community (https://covid-19.iglocska.eu/)

Una parte importante de MISP es su capacidad para utilizar taxonomías para clasificar y etiquetar eventos y atributos.

Una taxonomía en MISP es un conjunto de etiquetas predefinidas que se utilizan para clasificar y categorizar eventos y atributos. Las taxonomías pueden ser creadas por los usuarios o importadas desde fuentes externas. Las taxonomías proporcionan una forma estandarizada de describir la información en MISP, lo que facilita el intercambio y la correlación de datos entre diferentes organizaciones. Esta información también se puede calificar usando el método de Admiralty Scale (también conocido como NATO System) para evaluar la confiabilidad de una fuente y la credibilidad de una información de inteligencia recopilada. Consiste en una notación de dos caracteres.

La confiabilidad de una fuente se evalúa basándose en una evaluación técnica de su capacidad o, en el caso de fuentes de Inteligencia Humana, su historial. La notación utilizada se comprende entre la A y la F.

[18] Advanced Persistent Threat

La credibilidad de un elemento se evalúa en función de la probabilidad y los niveles de corroboración de otras fuentes. La notación que se utiliza es un código numérico entre 1 y 6.

Estas referencias del NATO System están basadas en el documento *Human Intelligence Collector Operations*[19].

Confiabilidad de la Fuente		Credibilidad de la Información	
A	Completamente confiable: Sin duda de autenticidad, confiabilidad o competencia; tiene un historial de total confiabilidad	**1**	Confirmado por otras fuentes: Confirmado por otras fuentes independientes; lógico en sí mismo; Consistente con otra información sobre el tema.
B	Generalmente confiable: Duda menor sobre autenticidad, confiabilidad o competencia; tiene un historial de información válida la mayor parte del tiempo	**2**	Probablemente cierto: No confirmado; lógico en sí mismo; consistente con otra información sobre el tema.
C	Bastante confiable: Duda sobre la autenticidad, confiabilidad o competencia, pero ha proporcionado información válida en el pasado.	**3**	Posiblemente cierto: No confirmado; razonablemente lógico en sí mismo; de acuerdo con alguna otra información sobre el tema
D	Generalmente no confiable: Dudas significativas sobre la autenticidad, confiabilidad o competencia, pero ha proporcionado información válida en el pasado.	**4**	Dudoso: No confirmado; posible pero no lógico; ninguna otra información sobre el tema.
E	No confiable: Falta de autenticidad, confiabilidad y competencia; historial de información no válida	**5**	Improbable: No confirmado; no es lógico en sí mismo; contradicho por otra información sobre el tema.
F	La confianza no se puede juzgar: No existe ninguna base para evaluar la confiabilidad de la fuente.	**6**	La credibilidad no se puede juzgar: No existe base para evaluar la validez de la información.

Figura 5ª Tabla de valores de confiabilidad de la fuente y credibilidad de la información.

Las taxonomías en MISP proporcionan una forma estandarizada y estructurada de clasificar y categorizar eventos y atributos, lo que facilita el intercambio y análisis de información sobre amenazas.

Un evento en MISP es una colección de información relacionada con una amenaza o incidente de seguridad. Un evento puede contener múltiples atributos, que son piezas individuales de información,

[19] Documento del ejército de los Estados Unidos sobre las operaciones de recolección de inteligencia humana, identificado como FM 2-22.3 (FM 34-52).

como direcciones IP, hashes de archivos, nombres de dominio, etc. Los eventos pueden ser etiquetados con etiquetas de taxonomía para proporcionar información adicional sobre el contexto y la naturaleza del evento.

MISP utiliza el Protocolo de Semáforo (TLP) para clasificar y compartir información sensible mientras se mantiene el control sobre su distribución. El Protocolo de semáforo (TLP) (v2.0) se creó para facilitar un mayor intercambio de información potencialmente confidencial y una colaboración más efectiva. El intercambio de información ocurre desde una fuente de información hacia uno o más destinatarios. Se utiliza para indicar los límites de intercambio que deben aplicar los destinatarios.

Código	Cuándo utilizarlo
TLP:RED	Se debe utilizar cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.
TLP:AMBER	Se debe utilizar cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.
TLP:GREEN	Se debe utilizar cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.
TLP:CLEAR	Se debe utilizar cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.

Figura 6ª Códigos y uso de TLP
Fuente: INCIBE [5]

FIRST sólo considera válidas las etiquetas recién mencionadas, aunque MISP agrega en una taxonomía que incluye etiquetas adicionales para compatibilidad con versiones anteriores que ya no están validadas por FIRST SIG[20].

Fuentes de información

Las fuentes de información son recursos que se utilizan para obtener datos. Pueden brindar datos incluso que no sean del todo fidedignos. La fuente de información puede ser interna o externa y se la clasifica en:

Fuentes primarias: Son aquellas más cercanas posible al evento que se investiga, es decir, con la menor cantidad posible de intermediaciones.
Fuentes secundarias: Se basan en las primarias y les dan algún tipo de tratamiento, para proponer nuevas formas de información.

Hoy en día abunda información y se encuentra poco ordenada y poco jerarquizada, haciendo que mucho de ella se pierda entre información de poco valor, que de tanto repetirse ha ido perdiendo necesario contexto. Por esta razón, poder identificar las fuentes fidedignas y pertinentes es más necesario que nunca.

[20] Los grupos de interés especial existen para proporcionar un foro donde los miembros de FIRST puedan discutir temas de interés común para la comunidad de respuesta a incidentes.

MISP ordena y estandariza la información además de que se puede complementar con el Proyecto Cerebrate para evitar información no fidedigna. En el caso del CERTUNLP, se ha sincronizado con instancias de MISP, las cuales podrán ser fuentes de información, así como el CERTUNLP podría ser fuente de información de las demás instancias. Las organizaciones con las que se han sincronizado son:

ARIU Asociación Redes de Interconexión Universitaria	La Asociación de Redes de Interconexión Universitaria cuenta con su servicio de CSIRT.
BA CSIRT	BA-CSIRT, es el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires. Se dedica a asistir y concientizar tanto a la ciudadanía como al Gobierno de la Ciudad de Buenos Aires en diversos temas relacionados al uso seguro y responsable de las tecnologías.Gestiona incidentes de seguridad.
CSIRT-NQN	Maneja y centraliza los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública difundiendo información con el fin de neutralizarlos en forma preventiva o correctiva. Actúa como repositorio de toda la información sobre incidentes de seguridad, herramientas y técnicas de defensa.
OEA | OAS	La Organización de los Estados Americanos fue fundada con el objetivo de lograr en sus Estados Miembros, un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia. Se basa en sus principales pilares que son la democracia, los derechos humanos, la seguridad y el desarrollo.

Figura 7ª Organizaciones sincronizadas con MISP del CERTUNLP

Correlación en MISP

Siendo que tenemos fuentes externas de información, con la cual MISP se alimenta, también podemos tener fuentes internas correlacionando los datos de los cuales ya se ha alimentado. La correlación es una característica principal en este proceso.

Las correlaciones en MISP son una manera de encontrar relaciones entre atributos. La correlación ayuda en la detección de grupos de actividades similares y vinculadas de un evento a otro.

Cuando el volumen de datos de una instancia MISP crece, el número de correlaciones puede crecer demasiado, sin embargo hace que mejore la detección de amenazas. Es básicamente una manera de que MISP indique que existe cierto valor en más de un evento.

La correlación se realiza a nivel de atributo. Pero debido a que los atributos están encerrados en un evento, también están representados a nivel de eventos.

Hay tres maneras en que MISP informa de correlaciones:

1. En el índice de eventos
2. En la página de detalle del caso
3. Junto a los atributos que causan la correlación

Siendo que la correlación genera nuevos datos que son creados por el vínculo entre atributos de eventos distintos, conlleva a un crecimiento de los recursos donde esté instanciado MISP, podría ser un limitante en alguna organización o incluso si la correlación no es de interés o no agrega ningún valor real para la organización donde se esté implementado MISP. También podría pasar que la correlación sea de interés pero solamente para valores específicos, excluyendo otras correlaciones. Es por ello que existen distintas opciones para deshabilitar parcial o totalmente la correlación.

Por atributo

La correlación en MISP se hace en segundo plano, y se puede evitar que se lleve a cabo la correlación para ciertos atributos. Cuando se añaden atributos, ya sea manualmente, por lotes o a través de la importación de texto libre, existe la opción de anular la correlación automática.

Deshabilitando la correlación a nivel de atributo solo deshabilita la correlación para el atributo específico que se agrega o edita, con lo cual esta acción no deshabilita el motor de correlación MISP para otros atributos u otros eventos.

Por evento

En lugar de desactivar la correlación por atributo, también se puede desactivar la correlación a nivel de eventos. Activando la opción *MISP.allow_disabling_correlation*, se deshabilitan todas las correlaciones para un evento específico.

Excluir valores para correlación

Se puede excluir la correlación en valores específicos con las entradas de exclusión de correlación. Con ello se puede agregar una lista de valores de atributos para los que no desea que se lleve a cabo ninguna correlación; e incluso borrar correlaciones ya existentes.

Correlación completamente desactivada

Se puede desactivar completamente el índice de correlación de MISP activando *MISP.completely_disable_correlation*.

Respecto al rendimiento de la correlación, en algunos casos el sistema podría tener recursos suficientes para hacer frente a la correlación, pero todavía experimenta la lentitud al iniciarla. Esto se

puede deber a que se está mostrando el número de correlaciones en la página del índice de eventos. Cuando las correlaciones no están en caché, significa que se les solicita cada vez que se accede a la página del índice de eventos. Se puede mejorar el rendimiento de esto en la página del índice de eventos deshabilitando *MISP.showCorrelationsOnIndex.*

Esta acción no deshabilita la correlación. Sólo evita que las correlaciones se puedan mostrar en la página del índice de eventos, es decir, todavía se tiene acceso a todas las correlaciones en la página de detalles del evento y en la lista de atributos.

Sincronización entre servidores

En MISP se pueden tener dos formas de sincronización entre servidores.

1. Por medio de instancias MISP conectadas entre sí.
2. Desde un enlace, por medio del consumo de feeds.

1)Una vez que se ha establecido un acuerdo con una fuente de información, la organización que otorga el acceso para poder conectarnos a su feed deberá:

1. Crear una Organización en la instancia de MISP (Instancia_MISP/admin/organisations/add).
2. Crear un usuario SyncUser con el usuario Administrador y asignarlo a la Organización creada (Instancia_MISP/admin/users/add).
3. Ingresar a la instancia de MISP con el usuario SyncUser
4. Obtener el JSON con los datos para poder conectarse con la instancia de MISP en Create Sync Config (Instancia_MISP/servers/createSync)
5. La otra organización deberá ingresar el JSON a la lista de sus servidores (Instancia_MISP/servers/import).

Nota: “Instancia_MISP” es el dominio donde se encuentra instanciado MISP

Los pasos expuestos sólo son una vía de sincronizar instancias de MISP entre otras. Otra forma es agregar un servidor agregando campo a campo los valores que la organización te pueda proveer. Incluso se también se podría suministrar al correo electrónico de la organización a la cual se dará acceso la clave para ingresar a la interfaz web y administrar su propio acceso bajo credenciales para el ingreso.

2)Los feeds son recursos remotos o locales que contienen indicadores que se pueden importar automáticamente a MISP a intervalos regulares. Los feeds se pueden estructurar en formato MISP, formato CSV o incluso formato de texto libre. Puede importar fácilmente cualquier URL local o remota para almacenar los datos en su instancia MISP. Las descripciones de feeds también se pueden compartir fácilmente entre diferentes instancias de MISP, ya que puede exportar una descripción de feed como JSON e importarla nuevamente en otra instancia de MISP.

Control de accesos a las fuentes de información de consumo y generadas

Existen diversas configuraciones que se pueden establecer para el control de la información que se puede consumir, también como la que se puede compartir.

- Métodos de sincronización habilitados:
    - Push: Permitir la carga de eventos y sus atributos. Sólo los eventos que coincidan con las reglas de inserción dadas se enviarán al servidor.
    - Pull: Permitir la descarga de eventos y sus atributos desde el servidor. Solo se extraerán los datos que coincidan con las reglas de extracción dadas.
    - Push Sightings: Si está marcado, los avistamientos (*Sightings*) también se permitirán cargar.
    - Caching Enabled: Permitir el almacenamiento en caché del servidor remoto.
    - Push Galaxy Clusters:Permite la carga de Galaxy Clusters
    - Pull Galaxy Clusters:Permite la descarga de Galaxy Clusters

Las reglas de carga (*Push*) y descarga (*Pull*) permiten establecer filtrados para los datos (basados en etiquetas y en organizaciones).

Creación de eventos

MISP está compuesto de eventos. Son los que se comparten entre organizaciones. Pueden ser creado por los investigadores de ciberseguridad del CERTUNLP o bien ser consumidos desde otras organizaciones. Los eventos están compuestos de:

- Date: fecha del reporte del evento
- Distribution: Dependiendo del evento, se podrá configurar si distribución.
- Threat Level: Nivel de amenaza, pudiendo ser:
    - Alto: APT[21] malware sofisticado o zero-day[22].
    - Medio: APT malware.
    - Bajo: malware masivo.
    - Sin definir: Autodescriptivo, sin definir.
- Analysis: Establece la etapa actual del análisis, pudiendo ser inicial, en proceso o completo. Desde que se publica el informe, se supone que el análisis está completo.
- Event Info: Nombre o título del evento.
- Extends Event : No es obligatorio, su uso es para ampliar un evento existente.

Atributos de eventos

Los eventos podrán tener diferentes atributos asociados, los cuales se dividen en:

---

[21]Amenaza persistente avanzada es un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque.

[22] Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes.

- Category: es la categoría del atributo, es decir, qué aspecto del malware describe este atributo. Esto podría significar los mecanismos de persistencia del malware o la actividad de la red, etc.
- Type: Mientras que las categorías determinan qué aspecto de un evento están describiendo, el Tipo explica por qué medios se describe ese aspecto. Por ejemplo, la dirección IP de origen de un ataque, una dirección de correo electrónico de origen o un archivo enviado a través de un archivo adjunto pueden describir la entrega del payload [23]de un malware. Estos serían los tipos de atributos con la categoría de entrega de payload.
- Distribution: permite controlar quién podrá ver este atributo. La distribución se hereda por atributos: gana la configuración más restrictiva.
- Value: El valor real del atributo, ingrese datos sobre el valor según lo que sea válido para el tipo de atributo elegido. Por ejemplo, para un atributo de tipo ip-src (dirección IP de origen), 11.11.11.11 sería un valor válido.
- Contextual comment: puede agregar algunos comentarios de contexto al atributo que no se utilizarán para la correlación, sino que servirán como un campo puramente informativo.
- For Intrusion Detection System: esta opción permite que el atributo se utilice como firma IDS [24]al exportar los datos NIDS, a menos que la lista de permitidos lo anule. Si no se establece el indicador IDS, el atributo se considera información contextual y no debe utilizarse para la detección automática.
- Batch import: si hay varios atributos del mismo tipo para ingresar (como por ejemplo una lista de direcciones IP), es posible ingresarlos todos en el mismo campo de valor, separados por un salto de línea entre cada línea. Esto permitirá que el sistema pueda crear líneas separadas para cada atributo.

Distribución de eventos

La información generada y a la cual puede consumir cada organización estará relacionada a la distribución que tendrá un evento. A modo de ejemplo práctico, los pasos son:

- Crear un evento: desde el menú Events Actions/Add Event, o desde el menú principal Home, y en el menú lateral pulsar sobre Add Event.

En la página de creación del evento, en Distribution

- Opciones de distribución:
    - Your organization only: El evento sólo será visible para los usuarios de tu organización.
    - This community only: El evento será visible para todas las organizaciones en tu comunidad MISP.
    - Connected communities: El evento será visible para tu comunidad y todas las comunidades que estén conectadas a la tuya.
    - All communities: El evento será visible para todas las comunidades.
    - Sharing group: Permite especificar un grupo de compartición personalizado (desde Administration/Server Settings & Maintenance/ MISP/live)

[23] Parte del código del malware que realiza la acción maliciosa en el sistema.
[24] El Sistema de Detección de Intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

Implementación de la plataforma

Se han instalado[25] tres instancias de MISP en el CERTUNLP, bajo la premisa de tener entornos aislados entre instancias en las fases de prueba, con lo cual, al momento de consumir y/o generar información con otras organizaciones, las instancias no se comuniquen entre sí.

Recomendaciones técnicas

Previo a la instalaciones, se ha optado por el uso de máquinas virtuales[26] bajo la recomendación de distribución del Proyecto MISP, es decir, la distribución más estable y más reciente de Ubuntu, como es actualmente la versión 22.04 LTS.

Los recursos asignados a una instancia MISP dependen en gran medida de cómo se utilizará la instancia. El número de usuarios, los datos ingeridos, los puntos de datos utilizados, el número de eventos, el número de correlaciones y el uso de la API son todos parámetros que deben considerarse al dimensionar su instancia.

Desde una perspectiva de hardware, los requisitos de MISP son bastante humildes, un servidor web con 2 núcleos y 8-16 GB de memoria debe ser suficiente. Mucho de ella depende del conjunto de datos y el número de usuarios con los que esté tratando.

También depende de la correlación de los datos, por el consumo de memoria y cómputo intensivo. Para un alto grado de relación de correlación, es conveniente reducir esto con una mejor gestión de los datos (indicador de correlacionar en los atributos) o aumentando la memoria y la CPU disponibles;
El número de muestras y archivos adjuntos afectan directamente al uso del disco;
la cantidad de usuarios concurrentes afectan el uso de la memoria y la utilización de CPU, especialmente si tiene una lista de usuarios de API que preguntan con frecuencia MISP; así como el número de alimentaciones y servidores remotos en caché y mantenidos en memoria también aumentará los requisitos de memoria del sistema. La cantidad de registros, actividades y la longevidad del servidor puede aumentar los requisitos del disco tanto en la base de datos como el conjunto de archivos de registro local.

La base de datos principal del MISP se basa en MariaDB. El uso de SSD es muy recomendable para garantizar una baja latencia, y garantizar un acceso eficiente a la base de datos.

Módulos y vinculación con software existente

Al implementar MISP, en vez de tratarlo como una plataforma aislada, se puede complementar e integrar a otras. Existe variedad de plataformas que pueden interactuar, acoplarse y enriquecer a

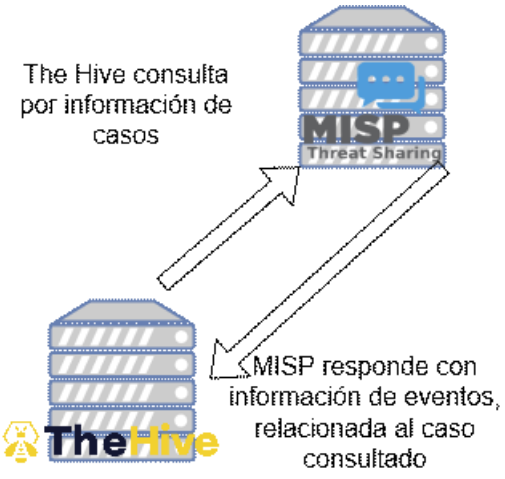
[25] ENISA[6], CSIRT de Chile [7] y CERT.br [8] han documentado la instalación y configuración lo cual ha sido de ayuda en esta etapa.
[26] Máquina con componentes virtuales

MISP, al igual que MISP puede ser fuente de consulta de otras. Es importante comprender algunas de ellas para profundizar el valioso rol de MISP.

TheHive [9] es una plataforma escalable de respuesta a incidentes de seguridad, estrechamente integrada con MISP , diseñada para facilitar a los *SOC*[27], *CERT* [28] y cualquier profesional de seguridad de la información que se enfrente a incidentes de seguridad que deben investigarse y actuar con rapidez.

Se destacan tres pilares:

1) Colaborar: Permite que varios analistas de SOC y CERT elaboren investigaciones simultáneamente. Gracias a la transmisión en vivo incorporada, la información en tiempo real relacionada con casos, tareas, observables e indicadores de compromisos nuevos (o existentes) está disponible para todos los miembros del equipo. Las notificaciones especiales permiten manejar o asignar nuevas tareas y obtener una vista previa de nuevos eventos y alertas de MISP de múltiples fuentes, como informes de correo electrónico, proveedores de CTI y SIEM. Luego pueden importarlos e investigarlos de inmediato.
2) Elaborar: Se pueden crear casos y tareas asociadas utilizando un motor de plantillas simple pero potente. Puede agregar métricas y campos personalizados a sus plantillas para impulsar la actividad de su equipo, identificar el tipo de investigaciones que toman mucho tiempo y buscar automatizar tareas tediosas a través de paneles dinámicos. Los analistas pueden registrar su progreso, adjuntar pruebas o archivos importantes, agregar etiquetas e importar archivos ZIP protegidos con contraseña que contengan malware o datos sospechosos sin abrirlos.
3) Actuar: Permite agregar observables a cada caso que o importarlos directamente desde un evento MISP o cualquier alerta enviada a la plataforma; así como clasificarlos y filtrarlos. Se puede aprovechar de Cortex con sus analizadores para obtener información valiosa, acelerar la investigación y contener amenazas. Aprovechando las etiquetas, IOCs, e identificando observables vistos anteriormente en virtud de alimentar la inteligencia sobre amenazas. Una vez que se han completado las investigaciones, se puede exportar los IOC a instancias MISP.



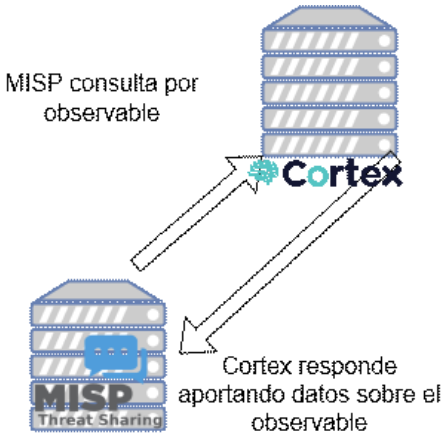
The Hive maneja casos, basados en alertas levantadas, sobre la gestión de incidentes, con lo cual es de gran importancia consultarle a MISP sobre sus casos. A los efectos, MISP analizará los eventos relacionados al caso de The Hive. Siendo que MISP se conecta a otras organizaciones se puede detectar un incidente que ya se ha producido en otras organizaciones para abordarlo de la mejor manera posible.

[27] Security Operations Center
[28] Computer Emergency Response Team

Cortex[10] analiza los observables como direcciones IP y de correo electrónico, URL, nombres de dominio, archivos o hashes. Estas operaciones se pueden automatizar y enviar grandes conjuntos de observables desde TheHive o MISP. Cuando se utiliza junto con TheHive, Cortex facilita en gran medida la fase de contención gracias a sus funciones de Respuesta Activa.

Se destacan tres pilares:

1) Escribir: Posee un amplio conjunto de analizadores , así como también permite crear analizadores o respondedores propios utilizando cualquier lenguaje de programación compatible con Linux e incluso compartirlos. También puede consultar simultáneamente varias instancias MISP.
2) Conectar: TheHive puede conectarse a instancias de Cortex y observables como también desencadenar respuestas activas. Si bien se puede utilizar Cortex como producto independiente también puede interactuar con otros productos, como MISP, a través de su API REST o mediante Cortex4py.
3) Ejecutar: Cortex incorpora analizadores para servicios, como por ejemplo VirusTotal, Joe Sandbox, DomainTools, PassiveTotal, Google Safe Browsing, Shodan y Onyphe. Los analizadores Cortex también se pueden consultar desde MISP para enriquecer los eventos y ampliar la cobertura de sus investigaciones.



De esta manera una instancia de MISP genera una consulta por un observable a Cortex, que procesa la consulta devolviendo y aportando datos sobre el observable consultado. Esta acción es definida como “enriquecer observables”.

Otra plataforma que puede alimentar MISP para el análisis de observables es el proyecto Intel Owl [11]. También de código abierto y es una excelente alternativa a Cortex por su buena integración a MISP.

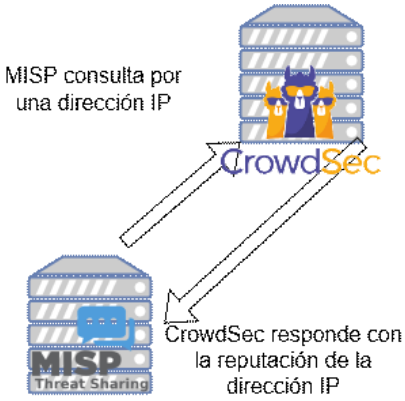
MISP se puede complementar con herramientas que permitan tomar acciones automatizadas para proteger la comunidad objetivo a la vez que se beneficia de más información. CrowSec, inspirada en Fail2ban[29], es una de esas herramientas.

CrowdSec[12] es una herramienta de seguridad colaborativa y de código abierto que aprovecha el poder de la multitud. Analiza comportamientos, responde a ataques y comparte señales en toda la comunidad. MISP por medio de un módulo adicional puede hacer uso de CrowdSec CTI, que distribuye inteligencia de reputación de IP, lo que permite a los equipos de SOC y a los analistas de seguridad obtener datos altamente seleccionados sobre intentos, orígenes y tendencias de intrusión.

Se destacan en 4 pilares:

1) Conocer al atacante: CrowdSec CTI aprovecha las decenas de miles de usuarios de CrowdSec para centralizar, seleccionar y redistribuir datos de usuarios y aplicaciones de la vida real.
   La mayoría de los CTI utilizan honeypots para recopilar datos sobre amenazas cibernéticas. CrowdSec CTI se centra en datos de usuarios reales, en todo el mundo, operando una gran variedad de servicios y aplicaciones para proporcionar datos precisos. Los usuarios de CrowdSec se encuentran en más de 180 países y tienen cientos de casos de uso diferentes, lo que brinda un contexto preciso para cada ataque.CrowdSec CTI opera dos bases de datos: *Smoke*, que contiene datos sin procesar de nuestros usuarios, y *Fire*, con datos rigurosamente filtrados sobre IP especialmente peligrosas.
2) Sus dos bases de datos: Información muy precisa y detallada. Los usuarios de CrowdSec comparten millones de señales diariamente, lo que permite recopilar una gran cantidad de información sobre cada dirección IP. Cada dirección IP compartida brinda información sobre el tipo de ataque, momento y caso de uso, permitiendo evaluar la agresividad de cada dirección IP. CrowdSec enriquece esos datos con recursos de terceros para añadir información como país de origen, sistema autónomo, etc. Los datos de reputación se actualizan con frecuencia para garantizar que reflejen el ciclo de vida de una dirección IP.
3) Conjuntos de datos estrictamente seleccionados: Los falsos positivos, los datos obsoletos o las bases envenenadas aumentan la fatiga de las alertas y proporcionan información poco fiable para tomar decisiones. CrowdSec CTI está diseñado para garantizar que solo se compartan con los usuarios datos de alta confianza. Cada usuario que contribuye obtiene una puntuación de reputación basada en la antigüedad y la contribución. Cuanto mayor sea la reputación, mayor será el valor que el algoritmo de curación dará a los datos proporcionados por el usuario. CrowdSec opera su propia red de honeypots. Los datos del usuario se correlacionan con los datos de los honeypots para garantizar la homogeneidad. La base de datos de *Smoke* expone datos no seleccionados para enriquecer los equipos de SOC o los datos de los analistas. La base de datos de *Fire* proporciona datos seleccionados para que los firewalls los consuman directamente para bloquear preventivamente las IP agresivas.

[29] Fail2ban es una aplicación para la prevención de intrusos en un sistema, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta.



Dada una instancia de MISP, al tener una dirección IP como valor de un atributo por el cual se quiere consultar su reputación, la instancia de MISP consulta a CrowdSec, que responderá con la reputación asociada a la dirección IP consultada.

Sabiendo la importancia del origen de la información con la cual MISP se nutre, puede ser integrado con el Proyecto Cerebrate.

Cerebrate [13] es una plataforma de código abierto destinada a actuar como proveedor confiable de información de contacto y orquestador de interconexión para herramientas de seguridad, incluyendo a MISP.
Entre sus características, tiene un repositorio avanzado para gestionar personas y organizaciones; almacén de claves para cifrado público y firma de claves criptográficas (por ejemplo, PGP);un modelo de sincronización distribuida donde se pueden interconectar múltiples instancias de Cerebrate entre organizaciones y/o departamentos; la gestión de personas y sus afiliaciones a cada organización. El desarrollo central del software está dirigido por el equipo central de MISP y especialmente por el equipo que trabaja en CIRCL.

MISP puede consultar a una instancia de Cerebrate a los fines de obtener información confiable y autenticar la fuente de información.

MISP además puede alimentar otra reconocida plataforma de seguridad, de manera tal que pueda ser fuente de información. Es el caso de Wazuh, donde puede enriquecer sus alertas automatizando las identificaciones de IOC con su integración de MISP con Wazuh.

Wazuh [14] es una plataforma gratuita y de código abierto que unifica protección XDR y SIEM para endpoints y cargas de trabajo en la nube (cloud workloads). Protege worksloads a través de ambientes propios (on-premise), virtualizados, en contenedores o basados en la nube. La Protección XDR activa de las amenazas modernas, proporciona a los analistas correlación y contexto en tiempo real. Las respuestas activas son granulares y abarcan la corrección en el dispositivo para que los puntos finales se mantengan limpios y operativos. Su solución de Security Information and Event Management (SIEM) proporciona monitoreo, detección y alertas de eventos e incidentes de seguridad.

Wazuh se basa en cuatro pilares:

1. Seguridad de los endpoints (Evaluación de configuración;Detección de malware y Monitoreo de integridad de archivos)
2. Inteligencia de amenazas (Caza de amenazas; Análisis de datos de registro y Detección de vulnerabilidades)
3. Operaciones de seguridad (Respuesta de incidentes; Cumplimiento normativo e Higiene TI[30])
4. Seguridad en la nube (Seguridad de contenedores; Manejo de la postura[31] y Protección de Cloud workloads)

Wazuh se integra con soluciones de terceros que mejoran las capacidades de búsqueda de amenazas. Estas integraciones permiten consolidar datos de diversas fuentes y automatizar la detección y respuesta a amenazas. Wazuh se integra perfectamente con plataformas populares de código abierto como MISP. Esta integración permite a los usuarios comparar la telemetría [32]con fuentes de inteligencia sobre amenazas, mejorando la detección y la respuesta a las amenazas.

Al promover el intercambio de información entre equipos de seguridad experimentados, estas integraciones fomentan una estrategia de defensa colectiva, mejorando la eficacia del proceso general de búsqueda de amenazas.

Con todos los módulos expuestos, podemos destacar la flexibilidad de MISP para ser integrado en un sistema; generando consultas a otras plataformas y también ser fuente de consultas, para el manejo de inteligencia de amenazas.

La figura 8ª representa a MISP integrado a las herramientas y plataformas mencionadas, poniendo a disposición información lista para ser consumida; a la par que se nutre y mejora la defensa contra las ciberamenazas. MISP posee un rol fundamental en la conexión entre las plataformas de la propia organización y va más allá al compartir información con otras organizaciones.

---

[30] Proceso de identificar continuamente activos, riesgos y vulnerabilidades en los endpoints y corregirlos
[31] Gestión para proteger las cargas de trabajo en entornos de nube al identificar riesgos de seguridad y garantizar el cumplimiento de los estándares regulatorios.
[32] Recopilación y análisis de datos de registro de los endpoints monitoreados, aplicaciones y dispositivos de red.

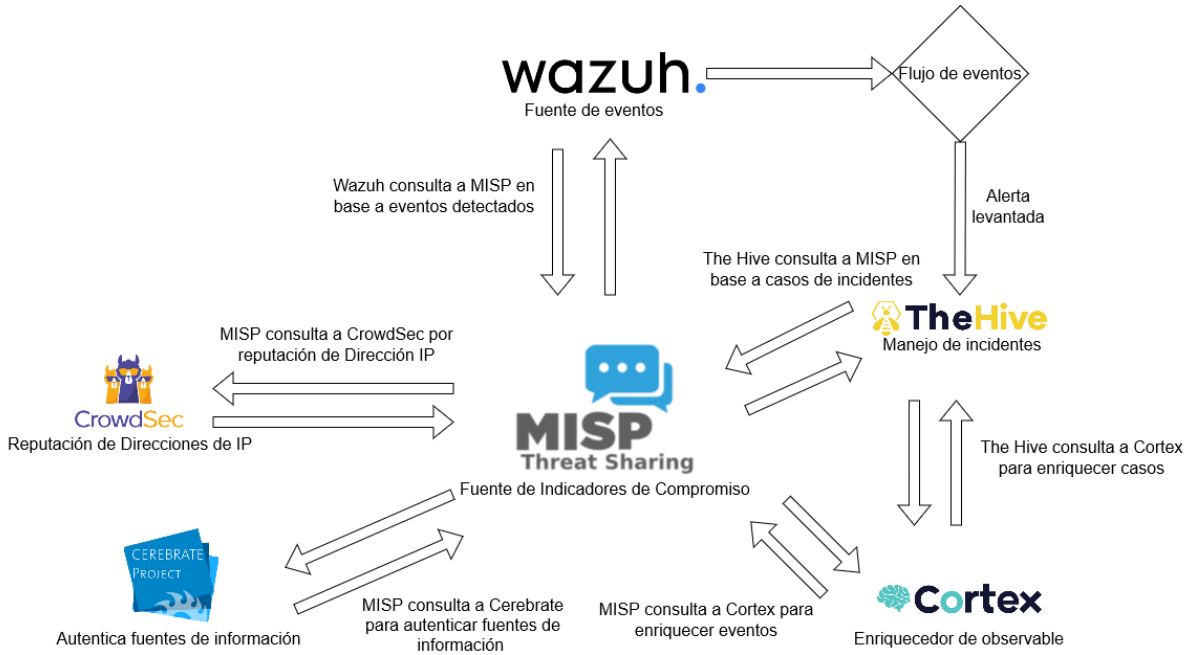


Figura 8ª Diagrama de integración de MISP

Integración a CERTUNLP

Aclaración: Con motivos de resguardar información en el uso de tecnologías, aplicaciones, plataformas y fuentes de información, este apartado ha sido redactado con fines de asegurar su privacidad.

Al haber elegido a MISP entre otras plataformas, su flexibilidad y fácil integración ya era conocida. Es por ello que frente al manejo de incidentes de ciberseguridad con NGEN y con las comunidades afines al CERTUNLP se decidió incorporar MISP en la escena de la inteligencia de amenazas.

NGEN [15] es un sistema para la gestión de incidentes de seguridad, destinado a distintos tipos de CSIRTs. El CERTUNLP lo utiliza en su misión diaria de la gestión de incidentes. Nació como un sistema de gestión de incidentes desarrollado para su uso en el ámbito de trabajo del CSIRT de la Universidad Nacional de La Plata, y fue liberado posteriormente como software libre.

Los eventos de ciberseguridad son enriquecidos mediante IntelMQ, hoy en día integrado a NGEN y que también puede ser integrado a MISP.

IntelMQ [16] es una solución de código abierto para equipos de seguridad de TI para recopilar y procesar fuentes de seguridad. Es una iniciativa impulsada por la comunidad llamada IHAP (Proyecto de automatización de manejo de incidentes) que fue diseñada conceptualmente por CERT/CSIRT europeos durante varios eventos de InfoSec. Su objetivo principal es brindar

a los servicios de respuesta a incidentes una manera fácil de recopilar y procesar inteligencia sobre amenazas, mejorando así los procesos de manejo de incidentes de los CERT.

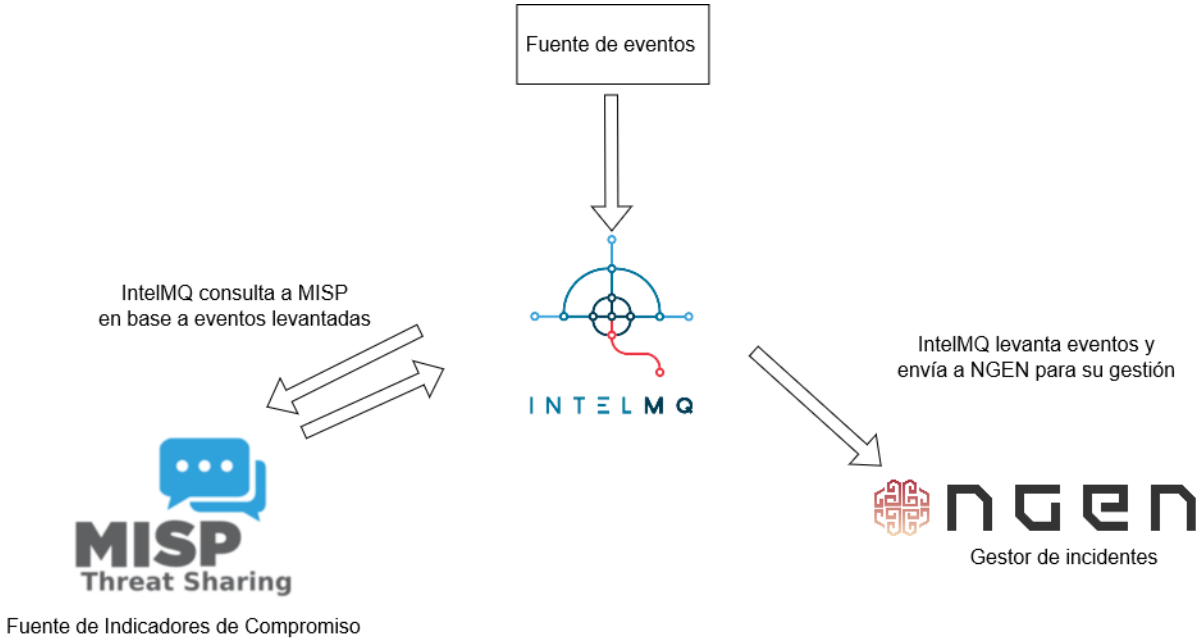


Figura 9ª MISP integrado al CERTUNLP

La figura 9ª nos muestra la integración de MISP al CERTUNLP, incluyendo las interacciones entre sus elementos, es decir, las solicitudes y respuestas entre plataformas.

Pruebas

Luego de la etapa de investigación y análisis, se han realizado diversas pruebas que abarcan desde la implementación de tres instancias, sus configuraciones de seguridad; configuraciones de funcionalidad; envío de correo electrónico, creación de eventos, hasta la sincronización con otras instancias por fuera del CERTUNLP.

Configuraciones

Se han realizado instalaciones desatendidas de MISP, configurando los parámetros con los valores en concordancia con la infraestructura y prácticas de ciberseguridad propias del CERTUNLP.

Se han encontrado algunos inconvenientes, mencionados en el apartado del documento de *Aportes a MISP*, relacionado con configuraciones de servidores SMTP [33]y de Redis[34], que fueron subsanados antes de su puesta en producción.

[33]Protocolo Simple de Transferencia de Correo, utilizado para el intercambio de correo electrónico
[34] Motor de base de datos en memoria

Consumo de información de prueba

A los fines de probar el consumo de información de prueba, se ha logrado satisfactoriamente por medio de *CIRCL OSINT Feed.* Una vez consumida la información, se ha podido listar en la instancia de MISP que la ha consumido y se ha agregado una tarea asincrónica que se encarga de consumir nueva información en tiempos regulares.

Generar información de prueba

Se han creado eventos con distintas opciones de distribución, con atributos de prueba. Además se hizo uso del etiquetado TLP. Por defecto las etiquetas de TLP vienen desactivadas en MISP. Para ello en el listado de taxonomías se selecciona *Enable* y luego se activan las etiquetas TLP que se quieran usar.

Problemas encontrados

Aclaración: Con motivos de resguardar información de otras organizaciones, este apartado ha sido redactado con fines para asegurar su privacidad.

Previo al pase a producción, se han encontrado diversos problemas durante las pruebas. Al momento de sincronizar MISP con otra organización, e incluso entre distintas versiones pero aún así compatibles, se han obtenido errores que no eran muy descriptivos.

Al haber varias formas de agregar un servidor, ya sea con un JSON, o copiando manualmente los valores propios de un servidor, al no haber una única forma fue causante de interpretaciones al momento de la sincronización.

También ha pasado que alguna instancia al crear una organización, un usuario y asignar el usuario a la organización, cuando se generaba el JSON para compartir los datos y dar lugar a la sincronización, los datos del JSON no eran congruentes con la vinculación entre organización y usuario.

Por último, dentro de las especificaciones de parámetros MISP OpenApi, no se ha podido configurar el uso del servidor SMTP, con lo que se ha configurado manualmente, logrando satisfactoriamente el envío de correos electrónicos por parte de MISP.

Conclusiones

Al momento de adentrarse o profundizar la postura de ciberseguridad de una organización, implementar MISP como plataforma de inteligencia de amenazas basada en indicadores de compromisos es un gran acierto. Sincronizar con otras comunidades las instancias de MISP y compartir eventos, correlacionar sus atributos y aportar a las organizaciones, tanto la propia como ajenas por medio de MISP es sumamente valioso.

Siendo una plataforma de código abierto y respaldada por la Unión Europea, y usada por varios países por fuera de ésta; junto a numerosas organizaciones gubernamentales, empresas privadas, y CSIRTs/CERTs.

Líneas de posibles trabajos futuros

MISP es una plataforma reconocida en las comunidades de ciberseguridad; con lo cual tiene abundantes módulos para integrar con otras plataformas e incluso incrementar las fuentes de información en el CERTUNLP. Por otra parte, MISP como tal tiene varios puntos para seguir mejorando.

Integraciones de MISP

En base al trabajo realizado, puede ser de puntapié para seguir investigando e implementando integraciones tanto de los módulos existentes como otros a implementar, que han sido mencionados a lo largo de ésta investigación.

Mejorar la integración de IntelMQ

Para ésta práctica, IntelMQ genera consultas a MISP. Se podría integrar en sentido contrario, siendo que MISP haga consultas a IntelMQ.

Mejorar la integración con NGEN

Para ésta práctica, MISP se integra a NGEN por medio de IntelMQ. Esto podría mejorar si fuera NGEN que haga consultas a MISP y viceversa, de forma directa.

Mejorar la integración con Cortex

Para esta práctica, MISP se ha vinculado con Cortex con analizadores de prueba. Se podría mejorar al agregar analizadores para tener mayor cantidad y calidad de fuentes de información para enriquecer los eventos.

Integrar Cerabrate Proyect a MISP

Se podría mejorar la seguridad en las fuentes de información por medio de Cerabrate Proyect, que fue analizado oportunamente en la investigación de ésta práctica.

Integrar CrowdSec a MISP

Se podría integrar CrowdSec como fuente de información de direcciones de IP detectadas como amenaza. Una alternativa podría ser integrarlo como analizador en Cortex.

Mejoras en Fuentes de Información

Se podría proyectar la sincronización de MISP con otras fuentes de información que participan en el CERTUNLP y colaboran dentro de la red de confianza. Algunas de ellas son:

Organización	Descripción
lacnic	La función de LACNIC es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región. LACNIC contribuye al desarrollo de Internet en la región mediante una política activa de cooperación. Promueve y defiende los intereses de la comunidad regional y colabora en generar las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico de América Latina y el Caribe.
metaredTIC by universia	MetaRed es un proyecto colaborativo que conforma una red de redes de responsables de Tecnologías de la Información y la Comunicación (TICs) de IES Iberoamericanas, tanto públicas como privadas, con el objetivo de compartir mejores prácticas, casos de éxito y realizar desarrollos tecnológicos colaborativos.
SHADOWSERVER	The Shadow Server Foundation es una organización de seguridad sin fines de lucro que trabaja de manera altruista entre bastidores para hacer que Internet sea más seguro para todos. Recopila datos sobre amenazas, envía informes de solución diarios y cultiva sólidas relaciones recíprocas con proveedores de redes, gobiernos nacionales y autoridades policiales. Sacamos de la sombra las actividades maliciosas y las vulnerabilidades de las que se puede abusar, aceleramos su remediación y ayudamos a proteger mejor Internet.

Mejoras sobre MISP

Se pueden desarrollar mejoras desde el punto de vista del consumo de recursos, de algoritmos de correlación, de la misma seguridad de los datos criptográficos, la detección y mitigación de información errónea, la desinformación; entre otras que se destaca a continuación:

Aportes a MISP

Premisa: Durante el proceso de instalación se informan algunos errores que podrían ser tratados. Por otro lado, algunas configuraciones de Redis no se han implementado de forma correcta, lo cual conlleva a errores que deja sin servicio a la plataforma.

Mejora: analizar los causantes de los errores y corregirlos.

Análisis de correlación MISP y mejora del modelado de complejidad de algoritmos.

Premisa: Los usuarios de MISP frecuentemente experimentan problemas de rendimiento cuando utilizan la función de correlación. Esto a menudo conduce a una depuración manual de consultas que requiere mucho tiempo, acompañada de ajustes en los algoritmos de correlación existentes.

Mejora: Se podría intentar realizar un análisis de complejidad en profundidad de los motores de correlación actuales. Este análisis ayudará a optimizar la utilización del hardware para una correlación más efectiva. Con este modelo, se pueden obtener especificaciones precisas para componentes de hardware como discos, RAM y CPU para dimensionar su hardware con precisión. Además, se podría planear realizar un seguimiento con mejoras en los algoritmos de correlación existentes.

Análisis y mejoras de la integridad de los datos criptográficos.

Premisa: En marzo de 2022, se introdujo el concepto de eventos protegidos para firmar criptográficamente eventos, evitando la manipulación de datos. La distribución de materiales criptográficos se realiza mediante Cerebrate .

Mejora: Se podría analizar en profundidad estos mecanismos, seguido de un examen de los ataques criptográficos y la propuesta de posibles soluciones o mejoras.

Detección y mitigación de información errónea y desinformación

Premisa: La herramienta complementaria, Cerebrate, proporciona una descripción general de los contribuyentes a MISP mediante verificación criptográfica. Sin embargo, el riesgo de desinformación dentro de las comunidades de MISP sigue estando siempre presente, y los usuarios malintencionados difunden información falsa.

Mejora: Se podría evaluar los mecanismos actuales, como las listas de advertencia y las listas de no admisión en MISP. También se podría realizar un estudio detallado de la información errónea y las técnicas de desinformación que potencialmente podrían afectar a las comunidades de MISP, así como del desarrollo de contramedidas apropiadas.

Herramientas de análisis comunitario

Premisa: MISP facilita el intercambio de numerosos tipos de objetos dentro de una comunidad de intercambio.

Mejora: Si bien algunas características proporcionan estadísticas básicas sobre el uso de estos objetos dentro de una comunidad determinada, se podría analizar exhaustivamente estas estadísticas, evaluar sus ventajas y limitaciones e introducir métodos automatizados novedosos para obtener conocimientos más profundos sobre las comunidades MISP, con un especial énfasis en los aspectos de intercambio de información.

Calificación de la comunidad MISP

Premisa: En el rico entramado de comunidades de intercambio de información de MISP, reside una gran cantidad de conocimientos y datos analíticos que ofrecen valiosos vistazos a las diversas capacidades de las organizaciones involucradas en compartir inteligencia sobre amenazas.

Mejora: Se podría buscar evaluar algoritmos y metodologías que puedan evaluar y calificar de forma autónoma a las organizaciones dentro de una comunidad MISP. Sus resultados tienen el potencial de una integración perfecta en MISP o Cerebrate, permitiendo compartir capacidades organizativas calculadas y calificaciones en toda la comunidad. Estas calificaciones pueden, a su vez, desempeñar un papel fundamental en la calificación y validación de la información generada por estas organizaciones participantes. Los resultados pueden luego integrarse en MISP para calificar la inteligencia producida por las organizaciones calificadas.

Bibliografía

[1] Sitio oficial de MISP https://www.misp-project.org/
[2] Sitio oficial del CERTUNLP https://www.cert.unlp.edu.ar/
[3] Documentación de STIX https://oasis-open.github.io/cti-documentation/stix/intro
[4] Documentación de TAXII https://oasis-open.github.io/cti-documentation/taxii/intro
[5] Documentación de TLP por INCIBE https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp
[6] Documentación de soporte de MISP por ENISA
https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-training-modules-and-tb.pdf
[7] Documentación de soporte de MISP por CSIRT de Chile
https://www.csirt.gob.cl/reportes/an2-2020-21/
[8] Documentación de soporte de MISP por CERT.br https://www.cert.br/misp/
[9] The Hive Project https://thehive-project.org/
[10] Documentación de integración entre MISP y Cortex
https://thehive-project.github.io/Cortex-Analyzers/analyzers/MISP/
[11] Sitio oficial de IntelOwl https://intelowlproject.github.io/

[12] Documentación de integración entre MISP y CrowdSec
https://docs.crowdsec.net/docs/next/cti_api/integration_misp/
[13] Sitio oficial de Cerebrate Project https://cerebrate-project.org/
[14] Sitio oficial de Wazuh https://wazuh.com/use-cases/threat-hunting/#threat-intelligence
[15] N-GEN https://github.com/CERTUNLP
[16] Documentación de integración entre MISP e IntelMQ
https://intelmq.readthedocs.io/en/latest/user/MISP-Integrations.html