UNIVERSIDAD DE BUENOS AIRES

Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

TESIS

Demostración del uso de una solución NG-SIEM

Autor:

Yaquemet Varela, Alvaro Octavio

Tutor:

Pagola, Hugo

Mayo 2021

Cohorte 2020

Control del documento

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	21/11/2020	Versión Inicial	Alvaro Yaquemet	Hugo Pagola
2.0	21/4/2021	Versión beta	Alvaro Yaquemet	Hugo Pagola
3.0	24/4/2021	Entrega Final	Alvaro Yaquemet	Hugo Pagola

Índice

1. Introducción 5
1.1 Reto de Seguridad 8
1.2 Objetivo 8
1.3 Objetos de Estudio 8
1.4 Alcance 8
2. Marco Teórico 9
2.1 SIEM 9
2.2 NG-SIEM 10
2.3 Detección de anomalías 11
2.4 SOAR 11
2.5 Inteligencia de la amenaza 12
2.6 Framework MITRE ATT&CK 13
3. Análisis sobre Casos de Uso de un NG-SIEM 14
3.1 Casos de Uso genéricos 16
3.1.1 Acceso no autorizado (hacking) 16
3.1.2 DDoS 17
3.1.3 Malware 18
3.1.4 Phishing 20
3.1.5 Anomalías 22
3.1.6 Análisis Forense 23
3.1.7 Fuga de información 23
3.1.8 Vulnerabilidad expuesta 24
3.1.9 Aumento de Amenaza 25
3.1.10 Hunting 25
3.1.11 Business Email Compromise (BEC) 26
3.2 Casos de uso basados en MITRE ATT&CK 27
T1031 - Modify Existing Service 28
T1036 - Masquerading 28
T1044 - File System Permissions Weakness 28
T1047 - Windows Management Instrumentation 29
T1053 - Scheduled Task/Job 29
T1070 - Indicator Removal on Host 29
T1073 - DLL Side-Loading 30
T1086 - Powershell 30
T1099 - Timestomp 30

T1130 - Install Root Certificate 31
T1204 - User Execution 31
T1218 - Signed Binary Proxy Execution 32
3. Etapa de Implementación 33
3.1 Laboratorio 33
3.2 Arquitectura y configuración 34
3.3 Herramientas 35
3.3.1 Security Onion 35
3.3.2 The Hive 36
3.3.3 Cortex 37
3.3.4 Synapse 40
3.3.5 MISP - Malware Information Sharing Platform 41
3.3.6 AIL - Analysis of Information Leaks 42
3.3.7 Caldera 44
3.3.8 Agentes 46
4. Alinear los casos de uso a la topología planteada 50
4.1 MISP - IDS: 50
4.2 The Hive - AIL 51
4.3 The Hive - Cortex 52
4.4 The Hive 54
4.5 Wazuh - Sysmon 56
4.6 Testeo de integración por API 57
4.7 Configuración de las reglas a monitorearse 57
4.7.1 Sysmon 57
4.7.2 BZAR - Zeek 57
4.7.3 Wazuh 58
5. Control y monitoreo 59
5.1 Implementación de Dashboards 59
5.1.1 Dashboard - Detección y métricas de certificados. 60
5.1.2 FIM - Monitoreo de alteración de objetos 61
5.1.3 Dashboard - Detección y métricas para SSL 61
5.1.4 Dashboard - Control de Endpoints 62
5.1.5 Dashboard - Control de perímetro 62
5.1.6 Dashboard - Control de tráfico sospechoso 62
5.1.7 Trafico por país y catalogación de IOCs 63
5.1.8 CTI - Comunicación con IOCs 63

5.2 Generación de reportes 64
5.2.1 Métricas - Flujo de Tareas del análisis automatizado 64
5.2.2 Métricas - Gestión de Incidentes 65
6. Metodología de trabajo 66
6.1 Análisis manual de Alertas 66
6.2 Análisis de comportamiento 67
6.3 Obtención de indicadores sobre rangos amplios de tiempo 67
6.4 Informe de incidentes 67
7. Análisis de resultados 68
8. Conclusiones 69
9. Bibliografía 70
10. Glosario 72
11. Anexo A 76
12. Anexo B 77
13. Anexo C 79

1. Introducción

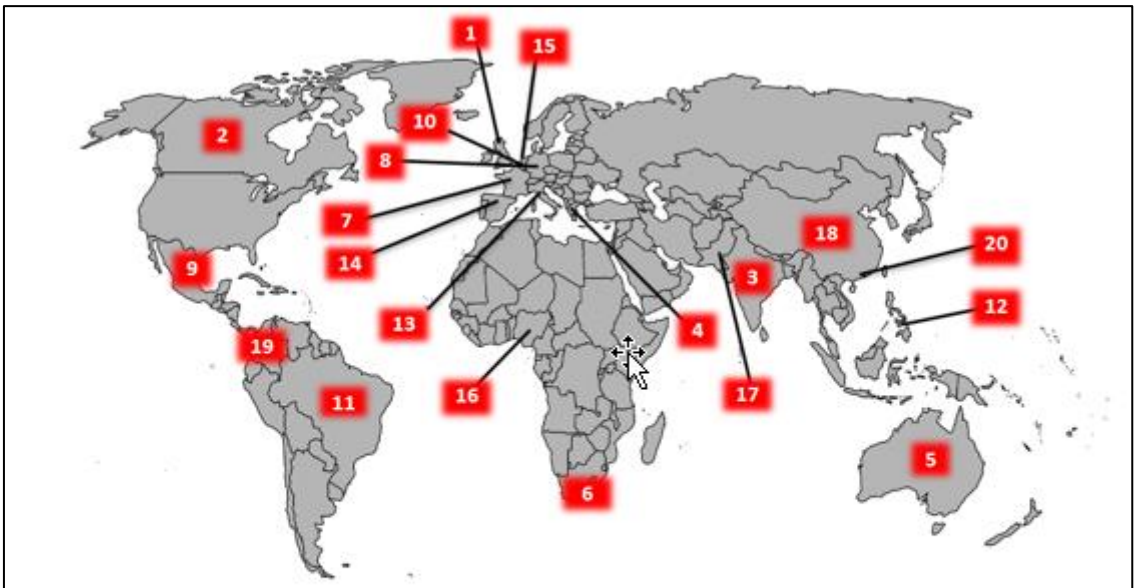
La tecnología e información son un pilar indispensable e indiscutido para la operatoria de los negocios dado el contexto en el que vivimos. Junto a ello, podemos identificar riesgos asociados a la productividad en conjunto a la eficacia y eficiencia. Para promover sus facultades, es necesario preservarlas. Lo que significa que, al ser unos de los activos más importantes requieren garantizar una adecuada concientización y control para su continuidad.

Las amenazas cibernéticas han evolucionado, no sólo a nivel de potencialidad, sino también en su ofuscación y proliferación. Durante los últimos años, han existido grandes brechas digitales en organizaciones de primer nivel, ya sea, por 0days, amenazas no identificadas o salvaguardas no aplicadas, entre otros.

Un ejemplo claro de ello es el informe de IC3 [1] donde se expone claramente amenazas tales como fraudes por correo electrónico (U$D1.8 billones) y Ransomware (U$D 29.1 millones) estos últimos han aumentado considerablemente, produciendo grandes pérdidas económicas.

En el último Ransomware Threat Report de Palo Alto Networks [2], manifiestan que el valor del rescate promedio pagado por organizaciones en Canadá, EEUU y Europa aumentó de U$D115.123 en 2019 a U$D312.493 en 2020, un 171% de incremento. Además, el rescate más alto ha sido duplicado de 5 millones a 10 millones de dólares en tan sólo un año. Es para destacar que las demandas de rescate de MAZE fueron promedio U$D4.8 millones, un aumento significativo comparado con el promedio de U$D847.344 de todas las familias de Ransomware en 2020.

Muchos de los grupos cibercriminales han realizado filtraciones de datos, probablemente en un esfuerzo por presionar a organizaciones víctima para que paguen el rescate antes de una fecha límite.

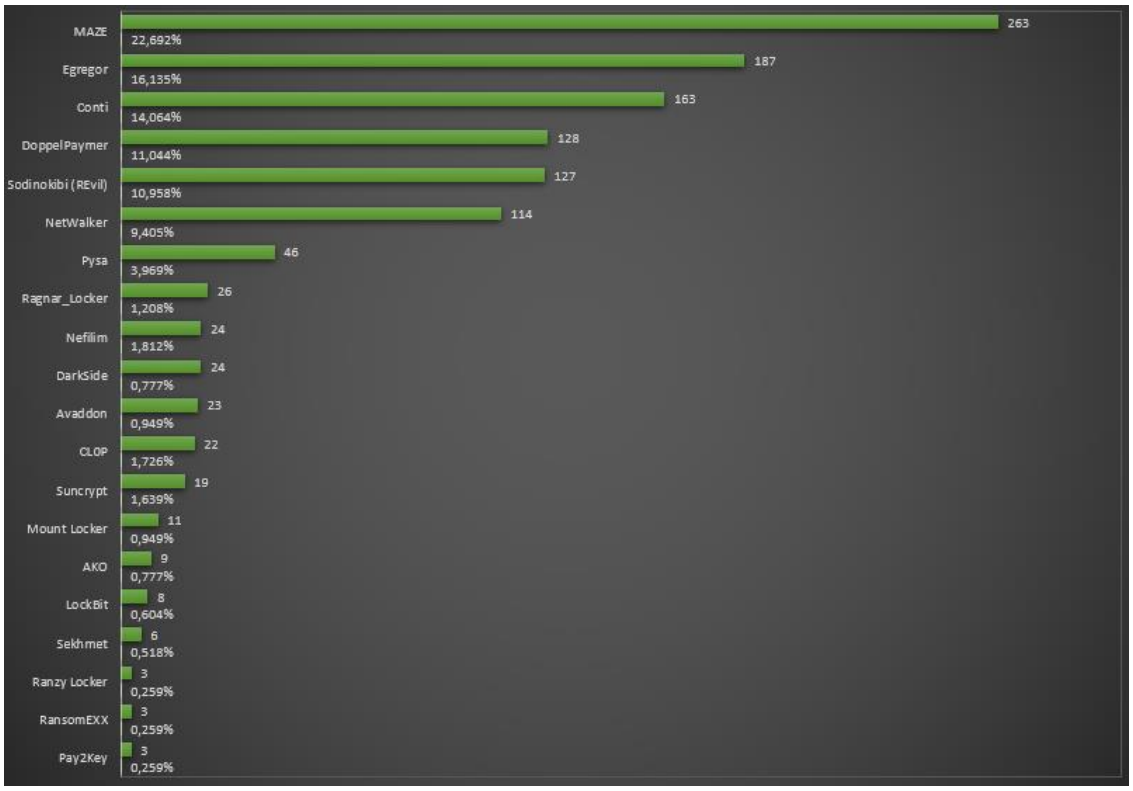


1. United Kingdom	216,633	6. South Africa	1,754	11. Brazil	951	16. Nigeria	443
2. Canada	5,399	7. France	1,640	12. Philippines	898	17. Pakistan	443
3. India	2,930	8. Germany	1,578	13. Italy	728	18. China	442
4. Greece	2,314	9. Mexico	1,164	14. Spain	618	19. Colombia	418
5. Australia	1,807	10. Belgium	1,023	15. Netherlands	450	20. Hong Kong	407

TOP 20 - Países víctimas - excluido Estados Unidos [1]

Las organizaciones invierten en ciberseguridad, pero las métricas muestran que están operando con supuestos que no coinciden con la realidad. Basado en M-Trends 2020 [3], el tiempo promedio que lleva una organización a descubrir que ha sido víctima de una violación de datos en 2019 es de 56 días; esto significa que un intruso podrá estar en la red durante casi 2 meses antes que se tenga noción sobre ello. Se puede ver una mejora notable comparado en 2011 con 416 días, aunque 56 días sigue siendo mucho tiempo. Las organizaciones que acentúan cierta mora en la respuesta ante incidentes son aquellas que siguen utilizando un enfoque tradicional de la seguridad para defender sus activos.

La mejor manera para combatir esta desconexión es validar la efectividad del programa de seguridad, a través de la evaluación continua y automatizada, optimizando y racionalizando los procesos críticos de negocio. Al enfrentarse a los atacantes del mundo real, los equipos de seguridad pueden evaluar su propia capacidad para detectar y responder a un escenario de atacante activo. Dicha gimnasia permitirá reducir los riesgos, identificándolos tempranamente para proteger no sólo los activos críticos sino también la reputación y el valor económico de la organización.



Organizaciones víctima de Ransomware - Publicado en DarkWeb

1.1 Reto de Seguridad

Es acertado considerar replantearse el modelo estratégico y de gestión de las operaciones de ciberseguridad, a través de lo evidenciado durante el trabajo, se demostrará cómo implementar infraestructura útil y viable (Open Source) junto al framework MITRE ATT&CK. Para identificar, clasificar y salvaguardar los negocios de la constante evolución de amenazas, avanzando hacia un enfoque predictivo y proactivo transformando las necesidades del negocio con la tecnología.

1.2 Objetivo

Implementar sistemas que permitan explorar y evaluar la red, mediante una solución NG-SIEM, demostrar las ventajas que presenta para la identificación y prevención proactiva de amenazas.

1.3 Objetos de Estudio

Next-Generation SIEM, Cyber Threat Intelligence, SOAR, MITRE ATT&CK Framework, Advanced Adversary Emulation, EDR, TTP, Ransomware.

1.4 Alcance

Se utilizarán soluciones Open Source, entre ellas se encuentra Security Onion, The Hive, Cortex, Sysmon, Wazuh, MISP, AIL, Caldera. También, se mostrarán las integraciones entre ellas y posibles usos en 4 equipos servidor de una misma red, para demostrar mediante 2 equipos cliente lo planteado.

2. Marco Teórico

En este capítulo se plasmarán una serie de conceptos que se consideran necesarios para la correcta comprensión del presente trabajo.

2.1 SIEM

Security Information and Event Management es una solución de software para monitoreo de seguridad informática que recopila y agrega datos de registros generados por distintas fuentes tales como Firewall, IDS, Antivirus, Base de Datos, etc.

Se encarga de otorgar información útil sobre las posibles amenazas de seguridad a las que se enfrenta una organización.

El objetivo final de un SIEM es que sea capaz de detectar, responder y neutralizar amenazas informáticas.

Hay varias razones para implementar un SIEM en una organización y entre ellas se destacan:

- Supervisión, gestión y retención de eventos 24x7
- Detección y respuesta ante amenazas
- Validación de la aplicación de políticas

Hoy en día, una solución de este tipo cumple con un modelo de seguridad tradicional donde se correlacionan eventos de distintos tipos de dispositivos con indicadores conocidos. Pero este tipo de SIEM no es lo mejor para detectar ataques desconocidos, comprender el comportamiento de una red y del usuario, analizar volúmenes masivos de datos en tiempo real y tomar medidas inmediatas para eliminar amenazas automáticamente antes de que dañen los sistemas de información de la organización.

2.2 NG-SIEM

Un SIEM de próxima generación brinda protección contra amenazas emergentes que no pueden detectarse con las formas y herramientas tradicionales de detección de amenazas.

La implementación de un NG-SIEM en una organización puede tener muchos beneficios, tales como respuesta inmediata de incidentes, menos alertas de falsos positivos, análisis del comportamiento de usuarios y del ciberespacio para realizar una priorización mejor informada.

Una solución NG-SIEM debe tener la capacidad de procesar grandes volúmenes de información y variedad de datos, así como correlacionarlos de manera oportuna. También debe permitir una integración más rápida en la infraestructura empresarial, incluir herramientas de visualización en tiempo real para comprender las actividades de alto riesgo. Debe ser capaz de proporcionar un marco flexible para detectar y priorizar escenarios de comportamiento significativos para el flujo de trabajo de las operaciones de ciberseguridad.

Características destacadas
Procesos y arquitectura estática mejorada con algunas características avanzadas
Tasa de alto rendimiento flexible y análisis en tiempo real
Integración con múltiples soluciones de ciberinteligencia
Utiliza aprendizaje automático e inteligencia artificial
Analiza en busca de ataques desconocidos, comportamiento del usuario, anomalías en la red, etc.
Facilita la automatización de alertas prioritarias, esto ayuda a utilizar el tiempo de manera eficiente
Puede analizar grandes volúmenes de datos

Recopilación extraída del manual del evaluador [4]

2.3 Detección de anomalías

Son eventos, comportamiento, patrones que son inusuales o sospechosos. Por ejemplo, si el comportamiento del usuario es inusual o sospechoso de su comportamiento habitual, podemos averiguarlo inmediatamente antes de que se convierta en una amenaza para la organización. Esta técnica se utiliza para detectar amenazas desconocidas.

2.4 SOAR

Security Orchestration Automation and Response ayuda a coordinar, ejecutar y automatizar tareas entre varias personas y herramientas. La orquestación de las operaciones de seguridad por medio de un SOAR facilita al NG-SIEM su uso para la toma de decisiones impulsado por Big Data, lo que permite a los equipos de seguridad tomar acciones mejor informados, esto significa menor cantidad de falsos positivos y por ende, mejor tiempo de respuesta ante incidentes.

Ayuda a estandarizar el análisis de incidentes y los procedimientos de respuesta. Entre sus usos, son prioridad la automatización de actividades de respuesta para las consolas de seguridad informática (EDR, Malware Sandbox, FW, Anti-DDoS, Email Security, etc.).

Características destacadas
Automatiza las tareas manuales repetitivas
Gestiona todos los aspectos del ciclo de vida de los incidentes de seguridad
Define el análisis de incidentes y los procedimientos de respuesta
Prioriza, estandariza y escala los procesos de respuesta de una manera coherente, transparente y documentada.
Identifica y asigna con rapidez y precisión niveles de gravedad de incidentes a las alertas de seguridad
Proporciona funcionalidades que facilitan la colaboración y el seguimiento entre equipos y miembros de equipo

Recopilación extraída del sitio oficial de Palo Alto Networks [5]

Beneficios:

- Mejora enormemente la postura de seguridad y la eficiencia operativa.
- Acelera la detección de incidentes de seguridad y los tiempos de respuesta; estandariza las acciones de respuesta.
- Admite la colaboración en tiempo real y las investigaciones no estructuradas.
- Aumenta la productividad de los analistas y centrándolos en mejorar la seguridad en lugar de realizar tareas manuales.
- Aprovecha las inversiones en tecnología de seguridad existentes.

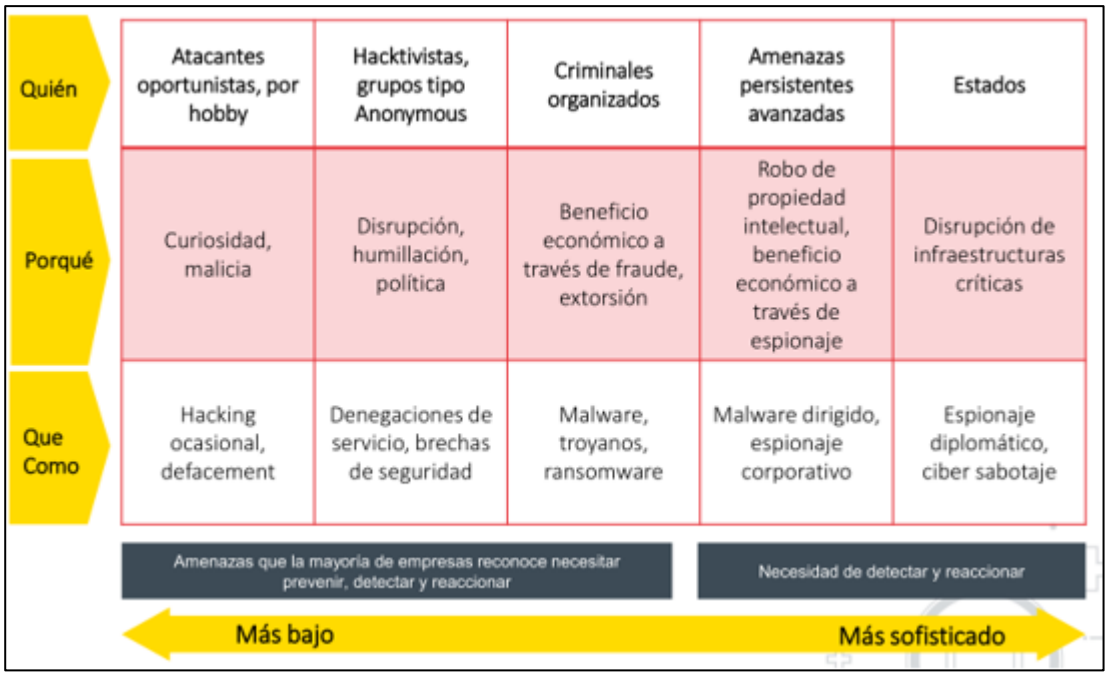
2.5 Inteligencia de la amenaza

El centro de Tecnologías Emergentes de la Universidad Carnagie Mellon, la define como: “La adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye a la toma de decisiones”. Es decir, que intenta procesar datos convirtiéndolos en información para de esa manera se genere conocimiento que permita tomar acción mejor informados.

Al otorgar contexto, por medio de información externa nos permite contar con mayor visibilidad respecto a amenazas emergentes. Esto ayuda a estar al tanto de ciberataques.

Inteligencia de la amenaza viable:

- Oportuna: aborda los problemas que suceden en el momento o por suceder.
- Precisa: tiene que ser representativo a la acción analizada.
- Procesable: ser rige de estándares para la normalización.
- Relevante: Su contenido tiene que ser de valor (adaptado) para el negocio.



Ciberactores - Motivaciones ¿Quién, por qué, que? [6]

2.6 Framework MITRE ATT&CK

Es un marco de inteligencia de amenazas que proporciona estructuras que promueven una amplia comprensión de cómo actúan los atacantes, las habilidades que usan, dotándonos de conocimientos clave para intentar frenar ciberataques en etapas tempranas [7].

El mismo se compone de tácticas, técnicas y procedimientos:

Acceso inicial, ejecución, persistencia, escalamiento de privilegios, evasión de defensas, acceso a credenciales, descubrimiento, movimiento lateral, recolección, comando y control, exfiltración e impacto.

Cada táctica contiene al menos una técnica que describe el comportamiento del atacante.

3. Análisis sobre Casos de Uso de un NG-SIEM

La respuesta ante incidentes requiere una cautelosa preparación, así como la capacidad de identificar, contener y recuperarse de ciberataques.

Existen varios estándares y pautas de respuesta ante incidentes. Los más famosos son NIST 800-61 Rev. 2 “Computer Security Incident Handling Guide”, ISO 27035:2016 “Information Security incident management”, SANS “Incident Response Process”.

Ahora, paso a describir cada uno y resumir los enfoques propuestos en etapas definidas para respuesta de incidentes.

La ISO 27035: 2016, trata fundamentalmente sobre redes y sistemas, no aborda otras formas de información, como propiedad intelectual, patentes, conocimiento, etc. La norma ISO 27035 propone cinco fases:

- Planificar y preparar
- Detección y notificación
- Evaluación y decisión
- Respuesta
- Lecciones aprendidas

El proceso de respuesta a incidentes de SANS se centra más en un acontecimiento basado en malware típico software evento y fue desarrollado especialmente para la respuesta ante incidentes basada en computadoras en lugar de incidentes de seguridad de la información. El proceso SANS IR consta de seis etapas:

- Preparación
- Identificación
- Contención
- Erradicación
- Recuperación
- Lecciones aprendidas

La guía NIST 800-61 Rev.2 es de los estándares más detallados que existen abiertos al público. Describe más profundamente el proceso de respuesta ante incidentes.

Según el documento del NIST, hay cuatro etapas principales de respuesta a incidentes:

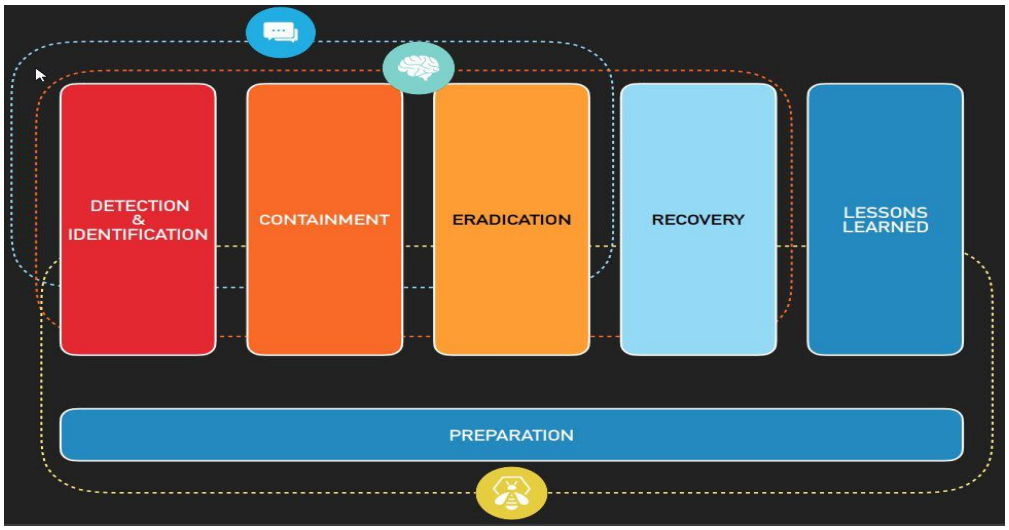
- Preparación
- Detección y análisis
- Contención, erradicación y recuperación
- Actividad posterior al incidente

Debe quedar claro que no existe un patrón de oro para planificar la respuesta ante incidentes de ciberseguridad. A raíz de ello, es que las distintas industrias han llegado al punto de estar en desacuerdo sobre cuál sería el mejor enfoque.

Los casos de uso están enfocados en las mejores prácticas para afianzar la metodología de trabajo en respuesta ante incidentes, como así también para la unificación de criterios de acuerdo con las tecnologías, procesos e implicancias que existiesen.

Para ello, se confeccionaron en The Hive unas plantillas personalizables como base para dar respuesta ante incidentes. El analista puede agregar tareas particulares a los casos, según la necesidad.

Es posible que determinadas tareas no apliquen a todos los incidentes.



Metodología de trabajo con The Hive Project [8]

Dichas plantillas pueden complementarse y enriquecerse con el tiempo a medida que el equipo vaya adquiriendo la experiencia necesaria.

3.1 Casos de Uso genéricos

3.1.1 Acceso no autorizado (hacking)

[IDEN] RI1: Identificar los sistemas afectados: IP interna, IP externa, sistema operativo (Windows, Linux), tipo de servicio (Web, Correo, VPN, etc.), software vulnerado (Apache, Tomcat, JBoss, Exchange, DNS bind, etc.).

[IDEN] RI2: Realizar un respaldo o copia del servidor afectado, para posterior análisis forense.

[IDEN] RI3: Recolectar los archivos de log del sistema operativo (Visor de Eventos en caso de Windows o /var/log/* en caso de Linux).

[IDEN] RI4: Buscar en los eventos del SIEM hacia/desde la IP externa e interna del servidor afectado.

[IDEN] RI5: Revisar internamente si existe un análisis de vulnerabilidades del perímetro reciente para detectar posibles vulnerabilidades existentes. Si no existe, coordinar un análisis de vulnerabilidades.

[CONT] RC2: En el caso de acceso del atacante, coordinar análisis forense para descartar/confirmar movimientos laterales y persistencia.

[ERR] RE1: Si se confirma una vulnerabilidad expuesta, identificar si está presente en otros servidores para mitigarla.

[LECC] RL1: Lecciones aprendidas: ¿Qué faltó para detectar la vulnerabilidad? ¿Qué faltó para detectar el acceso no autorizado?

3.1.2 DDoS

IDEN] RI1: Casos de DDOS:

- Aumento de tráfico de entrada en los enlaces Internet, producto del ataque el uso del enlace supera el 80% de su capacidad.
- Uso excesivo de CPU en los servidores, lo que afecta el tiempo de respuesta para atender a los clientes válidos.
- Uso excesivo de CPU en el firewall perimetral al procesar las políticas de acceso. Este tipo de ataques pueden durar varios días, incluso semanas.

[IDEN] RI2: Identificar sistemas afectados: Si estamos ante un ataque volumétrico, afectará a todos los servicios que utilizan dicho enlace. Si el ataque

sólo afecta un servicio, debemos enfocarnos en los equipos involucrado en dicho servicio.

[IDEN] RI3: Identificar el tipo de ataque, por ejemplo: protocolo utilizado por la mayoría del tráfico (ICMP, UDP, TCP), puertos que son objeto del ataque (HTTP, HTTPS, DNS, NTP, etc.).

[CONT] RC1: Evaluar acciones de mitigación: Arbor on premise, Arbor Cloud, CloudFlare, etc.

[LECC] RL1: Lecciones aprendidas: ¿Cuánto tiempo nos demoramos en saber que estábamos ante un ataque DDoS? ¿Pudimos contener el ataque con las tecnologías ya implementadas?

3.1.3 Malware

[IDEN] RI1: Se detecta presencia de posible código malicioso en servidor o estación de trabajo.

[IDEN] RI2: Identificación del sistema afectado: Por medio de un análisis rápido (triage) identificar el tipo de infección: gusano, Ransomware, etc. Indicar datos del sistema afectado, fecha y hora de detección, una foto que contenga los datos del archivo como: nombre, tamaño, fecha del sistema, etc.

[IDEN] RI3: Extraer muestras de los archivos maliciosos para análisis. Si se trata de un script o archivo Word (vbs, powershell, docx, xlsx) realizar un análisis rápido para identificar confirmar la presencia de malware (este análisis debe ser realizado por un especialista). Si se trata de un archivo ejecutable calcular el MD5 o SHA256 y buscar en el sitio de Virus Total.

[IDEN] RI4: Identificar direcciones IP y nombres de dominio asociados con el malware (si existen)

[IDEN] RI5: Si es posible, configurar un scan para identificar la presencia y remover el malware.

[CONT] RC1: Enviar muestra del malware al proveedor antivirus para que genere antídoto.

[CONT] RC2: Cuando contemos con el antídoto se debe distribuir a todas las estaciones de trabajo.

[CONT] RC3: Proceder con el bloqueo de los IOCs a nivel perimetral.

[CONT] RC4: Si contamos con la tecnología que lo permite, aislar en forma remota las estaciones de trabajo afectadas. Si no tenemos la tecnología para aislarlas en forma remota, debemos contar con personal en sitio o al menos distribuir las instrucciones de cómo proceder ante un escenario de este tipo.

[CONT] RC5: A partir de los Indicadores de Compromiso (entradas del registro, nombre de servicios, hash de archivos, etc.) identificar otras estaciones de trabajo posiblemente infectadas.

[ERR] RC1: Si el malware aprovecha una vulnerabilidad, debemos aplicar el parche correspondiente para mitigarla.

[ERR] RC2: Cargar antídotos en solución antimalware.

[ERR] RC3: Si es necesario, ampliar la cobertura del software antimalware.

[LECC] RL1: Lecciones aprendidas: Si el malware se propaga vía ingeniería social, debemos reforzar la sensibilización de los usuarios. Si el malware aprovecha una vulnerabilidad de los sistemas, debemos revisar nuestra política de parcheo.

3.1.4 Phishing

[IDEN] RI1: Se detecta correo electrónico con posible Phishing o se observa en Internet sitio Web de phishing.

[IDEN] RI2: Obtener muestra del correo sospechoso o URL de sitio web.

[IDEN] RI3: Analizar correo electrónico. Se recomienda analizar los siguientes elementos: encabezado del correo, fecha y hora, dominio de origen, IP de origen, fecha de creación del dominio de origen, elementos dentro del cuerpo del mensaje: archivos, URL, IPs, dominios.

[IDEN] RI4: Analizar sitio web. El objetivo es identificar si corresponde a una suplantación de sitio verdadero.

[IDEN] RI5: Confirmar o descartar amenaza de phishing.

[IDEN] RI6: Identificar destinatarios que recibieron correo de phishing o correo similar: buscar por asunto, origen, contenido.

[IDEN] RI7: Extraer IOC (archivos, URL, dominios, IPs).

[IDEN] RI8: Buscar en log de firewall, proxy de navegación o en EDR accesos a los IOC identificados.

[CONT] RC1: Cambiar contraseñas a usuarios afectados por el phishing, activar doble factor de autenticación en caso de que el usuario no lo tuviese.

[CONT] RC2: Bloquear IOC en controles de navegación.

[CONT] RC3: Bloquear IOC en correo de entrada.

[ERR] RC1: Borrar correo electrónico que contiene el phishing de las casillas de los usuarios afectados.

[REC] RR1: Evaluar y definir fecha en la cual se eliminarán bloqueos de los IOCs informados.

[LECC] RL1: Lecciones aprendidas: Si se estima necesario, reforzar la sensibilización de los usuarios. ¿Cuál fue el control qué falló?

3.1.5 Anomalías

[IDEN] RI1: Se detecta anomalía de algún tipo, la puede detectar un analista o la puede informar un cliente.

[IDEN] RI2: Identificar el tipo de anomalía, cómo se detectó, su comportamiento, frecuencia, fecha y hora de comienzo. Tipos de anomalías: aumento de tráfico de red, intentos de acceso (login exitosos o fallidos), correo electrónico sospechoso, procesos sospechosos en servidor o estación de trabajo.

[IDEN] RI3: Anomalías de tráfico: obtener detalle de la anomalía, comportamiento, mecanismo de detección. Recolectar tráfico para posterior análisis (tcpdump o Wireshark).

[IDEN] RI4: Anomalías de accesos: obtener detalle de la anomalía, frecuencia, fecha de comienzo. Recolectar logs de sistemas para posterior análisis.

[IDEN] RI5: Correo electrónico anómalo: obtener detalle del correo electrónico, cantidad de correos similares, periodo en que llegaron los correos.

[IDEN] RI6: Procesos sospechosos: obtener nombre y ubicación de los procesos, fecha y hora de creación, es posible obtener direcciones IP y puertos asociados (conexiones), fecha del ejecutable.

[CONT] RC1: Resultados del análisis de la anomalía reportada.

[LECC] RL1: Lecciones aprendidas.

3.1.6 Análisis Forense

IDEN] RI1: Se solicita análisis forense, o se realiza análisis forense producto de una respuesta a incidente.

[IDEN] RI2: Indicar tipo de Forense: malware, robo de información, hacking, phishing.

[IDEN] RI3: Indicar antecedentes del incidente: fecha y hora, activos afectados, aplicaciones, usuarios.

[IDEN] RI4: Evidencia recolectada.

[IDEN] RI5: Resultados del análisis forense.

[CONT] RC1: Recomendaciones y conclusiones.

[CONT] RC2: Realimentar sistemas con IOC obtenidos.

[LECC] RL1: Lecciones aprendidas.

3.1.7 Fuga de información

[IDEN] RI1: Se sospecha de fuga de información.

[IDEN] RI2: Identificar el tipo de información y el repositorio de la información.

[IDEN] RI3: Indicar porqué se sospecha de la fuga

[IDEN] RI4: Obtener registros de acceso a la información

[IDEN] RI5: Resultados del análisis

[LECC] RL1: Lecciones aprendidas

3.1.8 Vulnerabilidad expuesta

[IDEN] RI1: Se identifica vulnerabilidad de alto riesgo expuesta a Internet

[IDEN] RI2: Identificar plataforma (sistema operativo, aplicación, versión)

[IDEN] RI3: Identificar impacto de la vulnerabilidad

[IDEN] RI4: Confirmar presencia de la vulnerabilidad

[CONT] RI1: Aplicar parcheo

[CONT] RI2: Confirmar mitigación de la vulnerabilidad

[LECC] RL1: Lecciones aprendidas

3.1.9 Aumento de Amenaza

[IDEN] RI1: Por medio de inteligencia de la amenaza se detecta aumento de amenazas.

[IDEN] RI2: Indicar fuente y descripción de la amenaza

[IDEN] RI3: Investigar riesgos y posibles mitigaciones

[LECC] RL1: Lecciones aprendidas

3.1.10 Hunting

[IDEN] RI1: Hunting periódico o a solicitud.

[LECC] RL1: Lecciones aprendidas.

3.1.11 Business Email Compromise (BEC)

[IDEN] RI1: Alerta de Información confidencial en Mercado Negro.

[IDEN] RI2: Indicar fuente y descripción de la amenaza

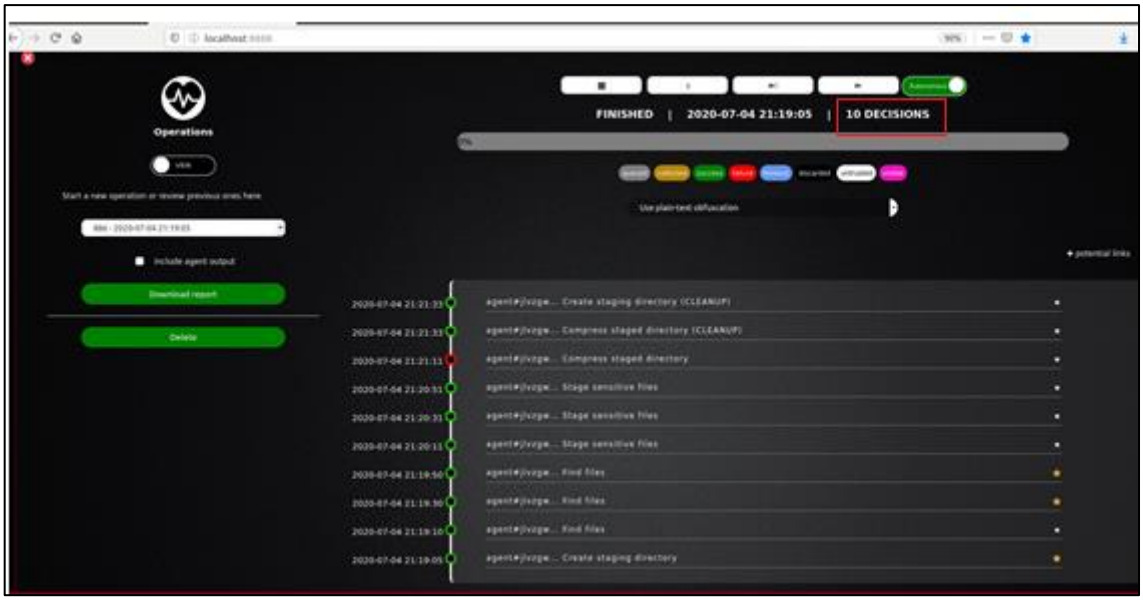
[IDEN] RI3: Investigar riesgos y posible mitigación

[LECC] RL1: Lecciones aprendidas

Idealmente, las tareas de respuesta ante incidentes deben planearse de antemano, integrarse con proyectos de seguridad y probar lo suficiente, practicando dichas tareas con equipos internos y externalizados. Lo esencial es saber y practicar las responsabilidades de antemano.

3.2 Casos de uso basados en MITRE ATT&CK

Se utilizó como base el framework de MITRE ATT&CK para emular una serie de ataques referidos a TTPs conocidos. Dicho framework, presenta una matriz dividida por columnas (Ver Anexo C), en la cual cada columna es una táctica (el porqué, el objetivo técnico) o técnica (el cómo, las acciones a realizar) que un posible atacante podría accionar para intentar una intrusión.

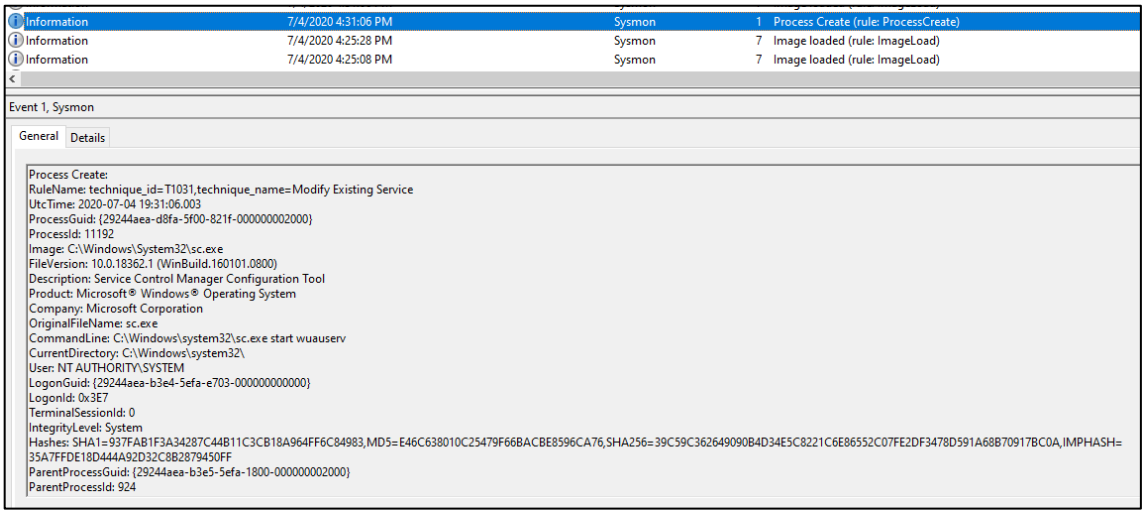


Cadena de ataque ejecutada con Caldera

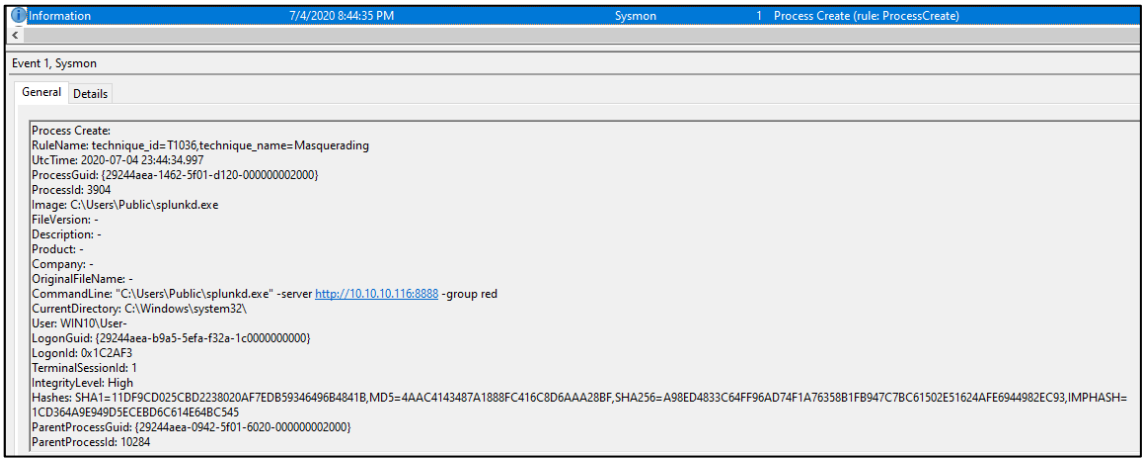
Dichas TTPs, desembocan en múltiples posibles escenarios que a su vez es posible establecer distintos casos de uso dependiendo del contexto, con lo cual esto prevé casos de uso adaptables al ejercicio de simulación que se requiera evaluar.

Detección de TTPs:

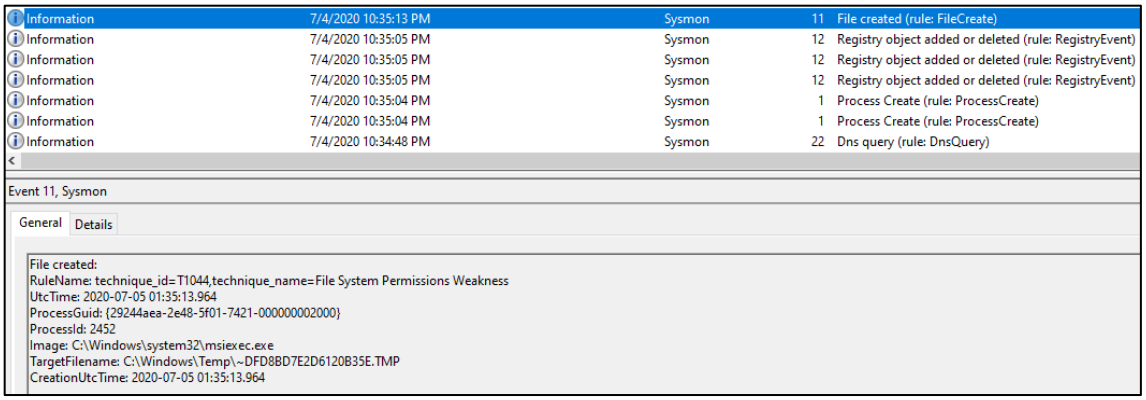
T1031 - Modify Existing Service



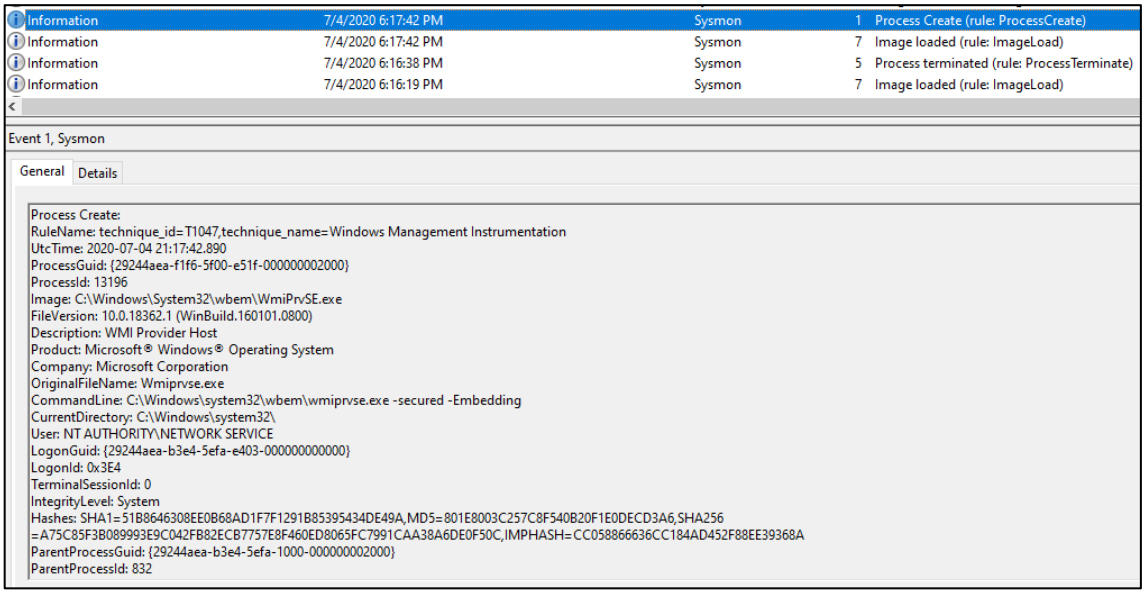
T1036 - Masquerading



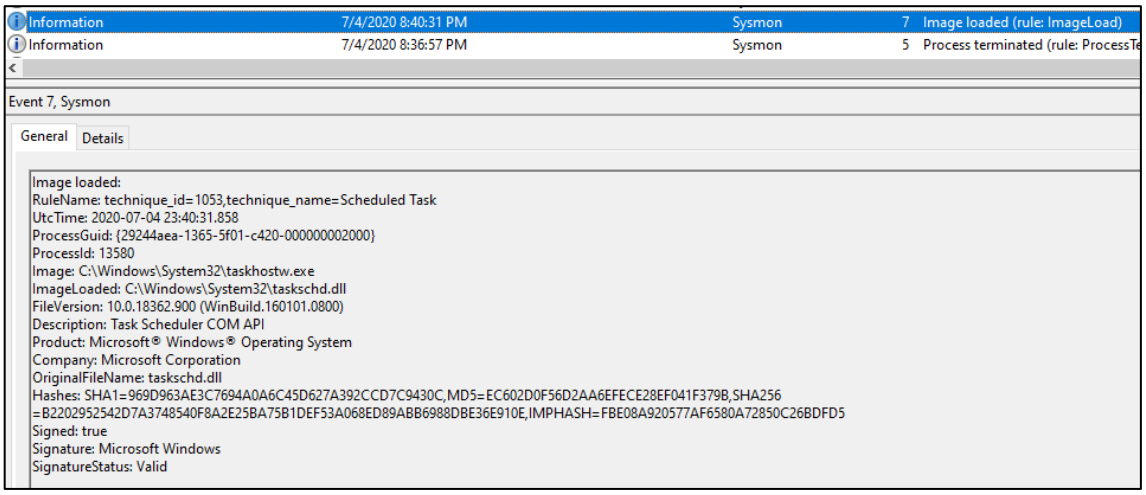
T1044 - File System Permissions Weakness



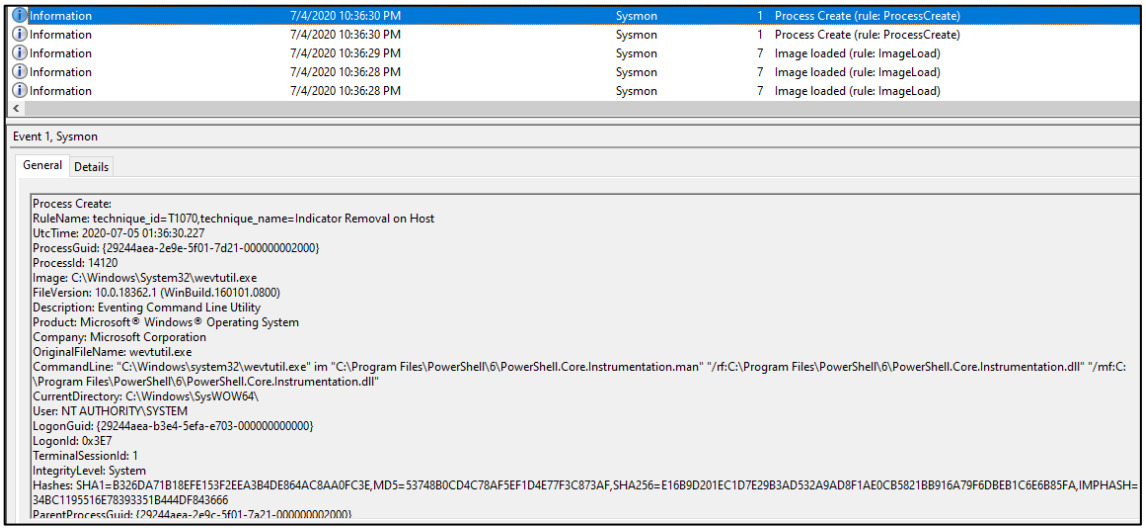
T1047 - Windows Management Instrumentation



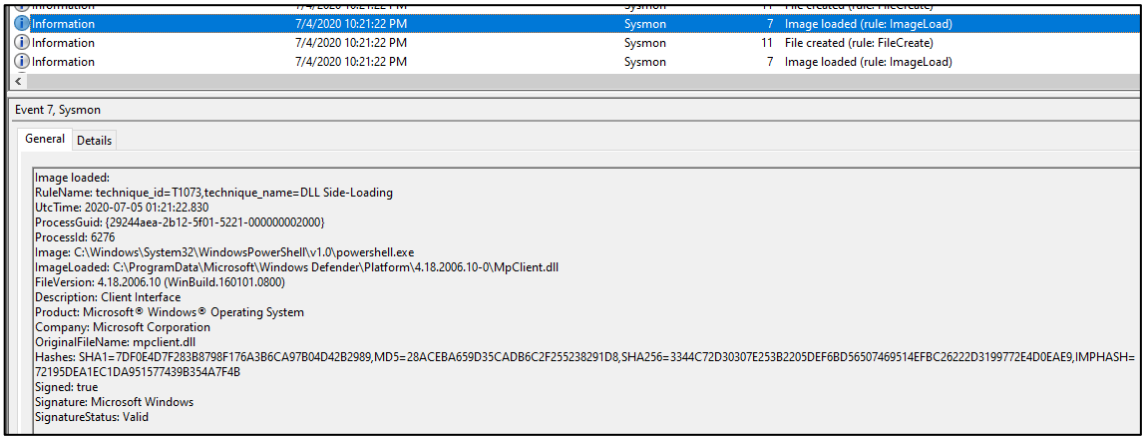
T1053 - Scheduled Task/Job



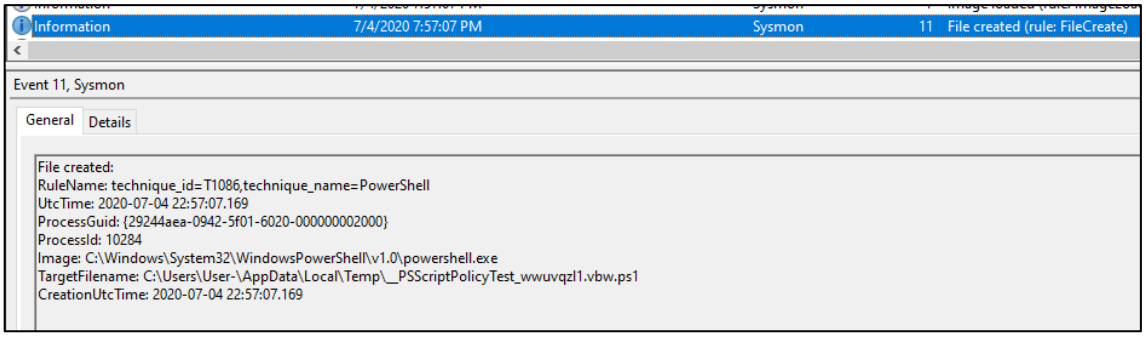
T1070 - Indicator Removal on Host



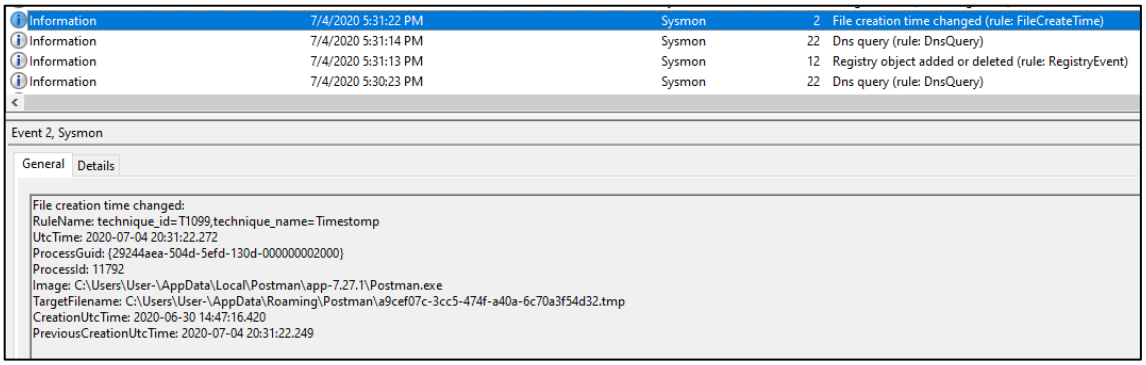
T1073 - DLL Side-Loading



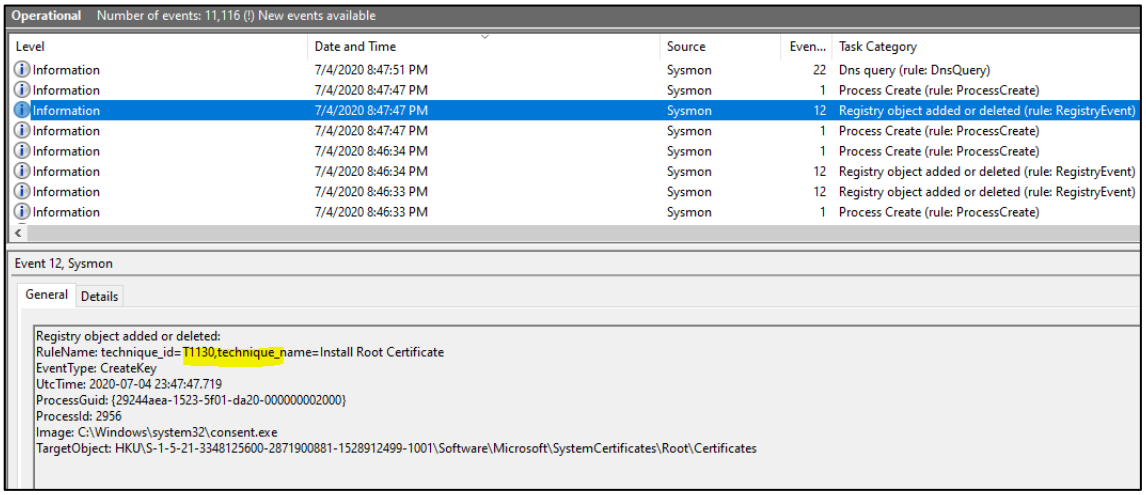
T1086 - Powershell



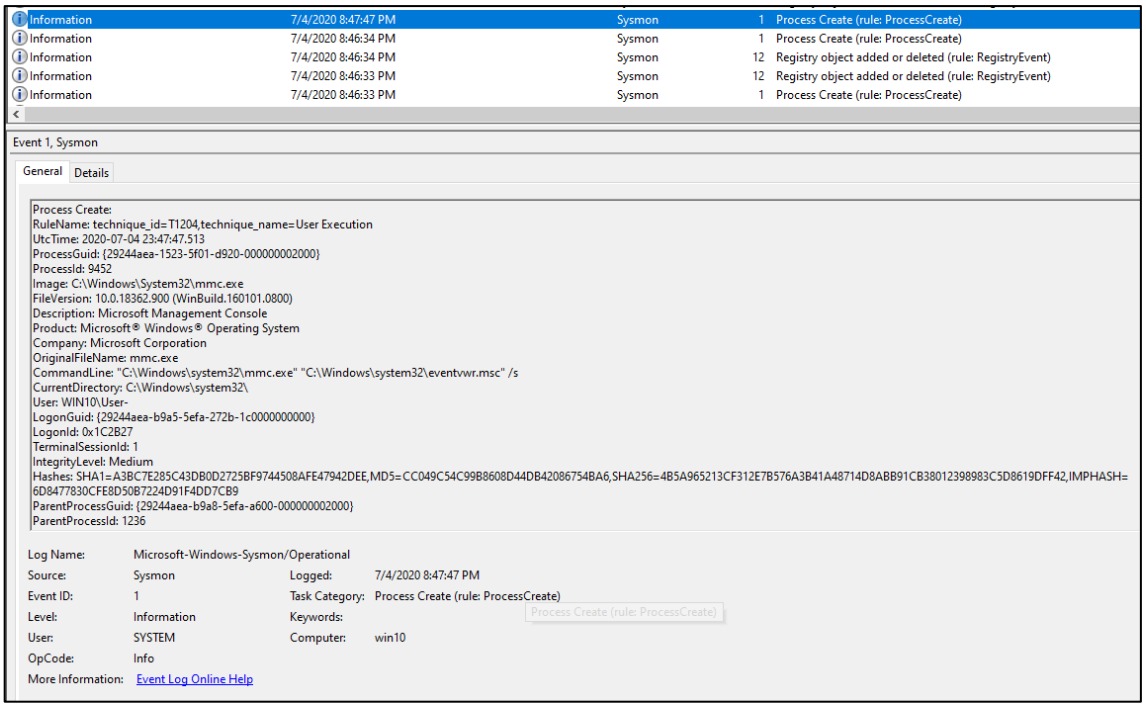
T1099 - Timestomp



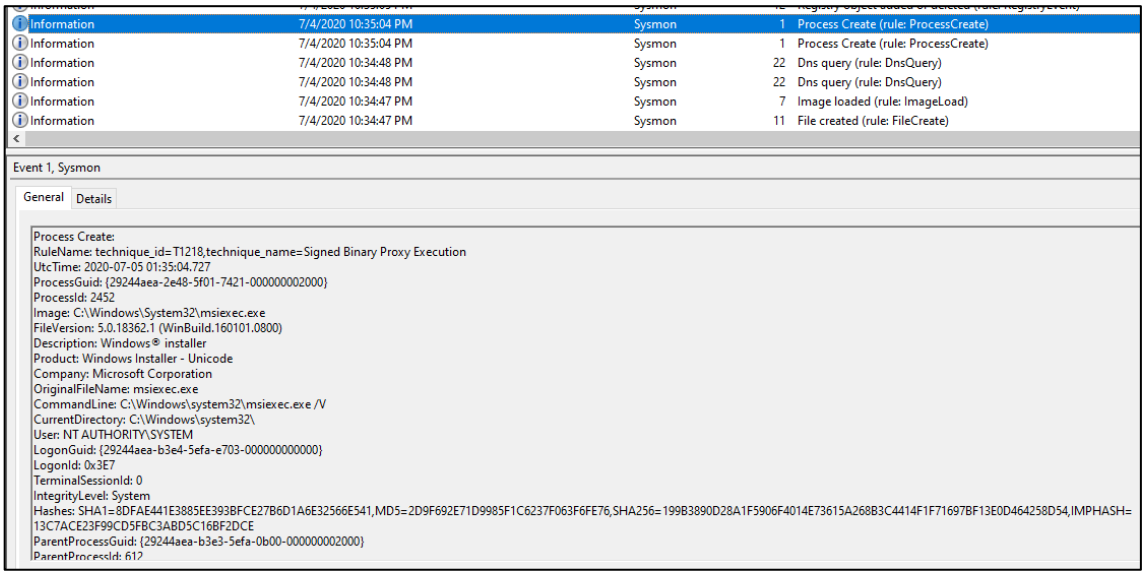
T1130 - Install Root Certificate



T1204 - User Execution



T1218 - Signed Binary Proxy Execution



3. Etapa de Implementación

3.1 Laboratorio

Para este análisis se trabajará con fuentes de datos del ambiente Windows y Linux/Unix.

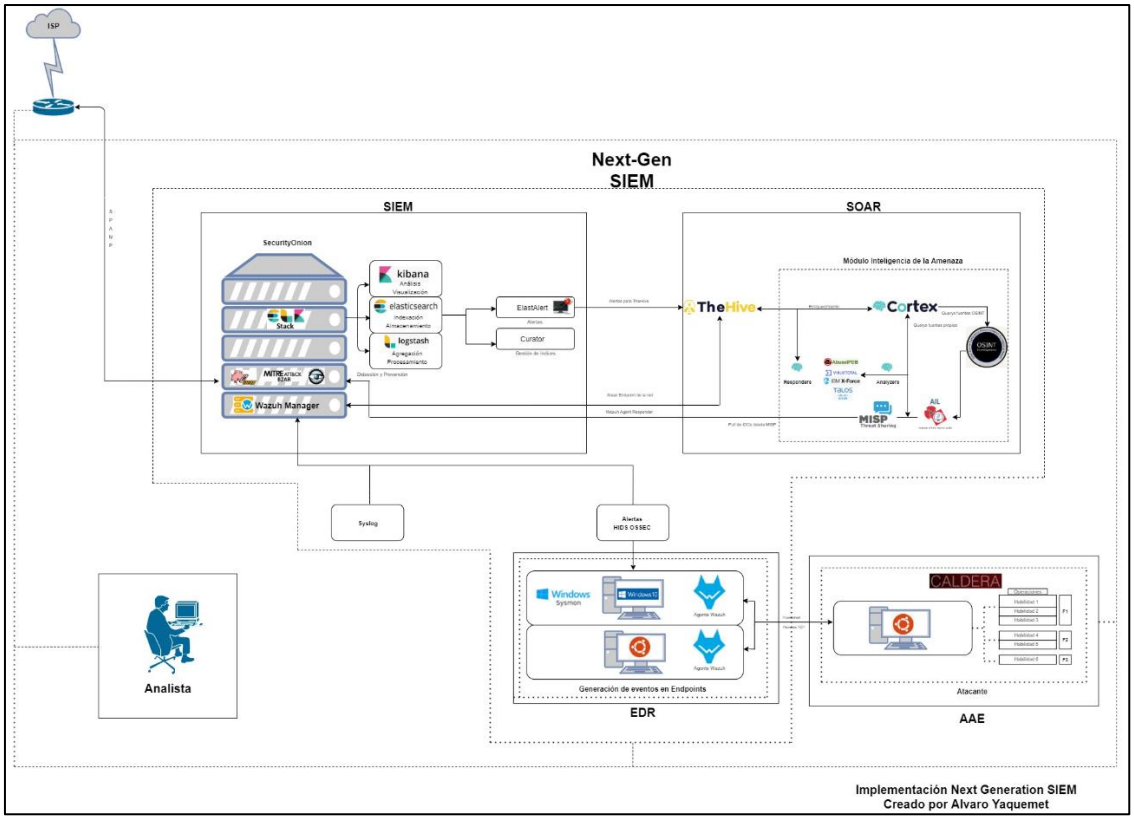
La configuración del laboratorio comienza con una computadora host con Proxmox 6.3-1. Hardware Custom (AMD 8 cores 16 threads, 64GB 3200 MHz DDR4). Dicha máquina corre 6 sistemas operativos virtualizados o “invitados” para la experimentación:

Hostname	IPv4	Rol	OS	CPU	RAM	Interface de red
pfSense	10.10.10.1	Router/ FW	FreeBSD/PFSense 2.4.5-RELEASE (amd64) CE	1	2048	WAN LAN SPANP
ngsiem	10.10.10.180	NG-SIEM	CentOS 7.7 (amd64)	6	16384	LAN SPANP
SOAR	10.10.10.170	CTI	Ubuntu 18.04 (amd64)	4	8192	LAN
MISP						
aae-purple	10.10.10.112	AAE	Ubuntu 18.04 (amd64)	2	8192	LAN
win10	10.10.10.140	Endpoint	Windows 10 Pro 64-bits	1	4096	LAN
ubuntu18	10.10.10.115	Endpoint	Ubuntu 18.04 (amd64)	1	4096	LAN

Cabe destacar que todas las máquinas están sincronizadas fecha y horario, recomendado por buenas prácticas. Por otro lado, se desactivó Windows Defender en su totalidad para no hacer interferencia durante la fase de ejecución de pruebas.

3.2 Arquitectura y configuración

Por medio de una evaluación de herramientas, se tuvo en cuenta que sea posible integrar múltiples sistemas y el grado de complejidad, si es por API nativa o no, y si el software posee una comunidad activa de soporte y casos de uso empíricos.



La configuración del laboratorio de pruebas consta de un pfSense como switch/FW que provee internet a la LAN, refleja todo el tráfico entrante y saliente a un puerto SPANP local que está conectado directamente a la interfaz enp0s8 del host ngsiem.

El host ngsiem, cuenta con Security Onion y un sensor IDS, ambos se configuraron como implementación Standalone durante el Wizard de instalación.

Para SOAR, se utiliza The Hive con Cortex y para CTI se implementó AIL-Framework (Analysis of Information Leaks) con MISP (Malware Information Sharing Platform) y Synapse para la integración con Office 365.

Como AAE (Advanced Adversary Emulation) la herramienta que provee MITRE llamada Caldera, donde se ejecutó una conexión reverse-tcp a los Endpoints.

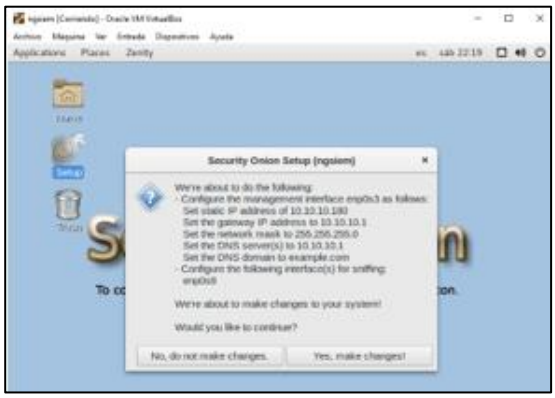
Luego dos equipos Endpoint, por un lado, un Ubuntu 18.04 y como segundo equipo de pruebas una máquina con Windows 10 v.2004 que tiene configurado Sysmon (SysInternalTools) donde se importó en la instalación un XML personalizado de configuración para detección de TTPs. Junto con el agente Wazuh que cumple 3 propósitos, FIM (File Integrity Monitoring), exportar los registros de Operaciones de EventViewer (Sysmon) y proveernos la ejecución de acciones automatizadas desde el SOAR llamadas “Responders” donde si identificamos que un equipo estuviese comprometido mediante un clic podríamos bloquear el tráfico malicioso, entre otras funcionalidades.

3.3 Herramientas

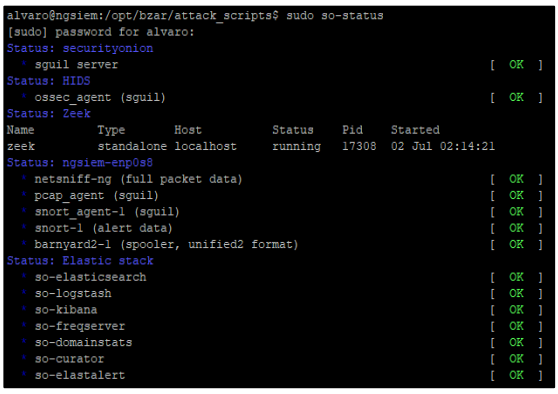
En base a mi experiencia y los conocimientos adquiridos durante la carrera, opté por la implementación de las soluciones de forma práctica, ya que, a efectos de la demostración cumple con los requisitos necesarios para la documentación del desarrollo de los casos de uso.

3.3.1 Security Onion

Se implementó la solución Security Onion en modalidad Standalone, ya que, para el uso de pruebas es lo más recomendado [9].



Wizard de instalación

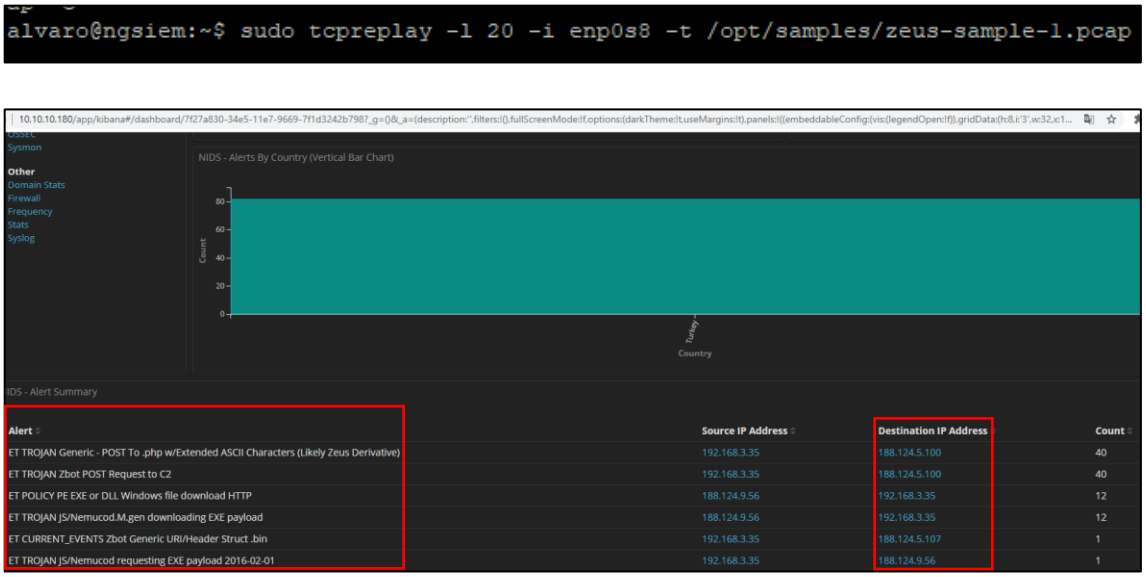


Servicios levantados

Cuenta con ELK para el análisis, almacenamiento, indexación y procesamiento de datos.

También con un servidor Wazuh, monitoreo de tráfico de red a través de Zeek para inteligencia de amenazas con las reglas de detección BZAR - MITRE [10] podríamos reconocer ataques oportunamente.

3.3.1.1 Prueba de funcionamiento IDS/IPS:



Detección de tráfico - Familia de Malware Zeus

3.3.2 The Hive

El foco para realizar inteligencia de amenazas efectiva es automatizar los procesos desde un principio, fundamentalmente las tareas relacionadas con datos, agregación, comparación, contextualización, etc. Cuando estos están bien implementados, los informes y alertas se realizan de manera ágil y eficaz para la toma de decisiones. De manera tal que se anticipen amenazas emergentes automatizando tareas de monitoreo y correlación de indicadores de compromiso, alimentando la información de reputación de comportamiento desde una visión madura del ciberespacio.

En primer lugar, Cortex-The Hive [11] es provisto como una solución autocontenida instalada como un único archivo docker-compose que corre sobre un servidor Linux.

A continuación, se describen los principales componentes del producto.

- Base de Datos: Cortex-The Hive utiliza una base de datos Cassandra 3.11 a donde se almacenan todos los datos.
- Búsqueda e Indexación: Un rápido motor de búsqueda ElasticSearch 7.9 brinda la capacidad de encontrar rápidamente cualquier dato residente, incluyendo observables, mensajes, investigaciones pasadas, y más.
- Software adicional: Un componente opcional que permite la integración con o365 Outlook es el software Synapse.

Dentro del mismo, se configuraron para atender los puertos:

5000 - Synapse

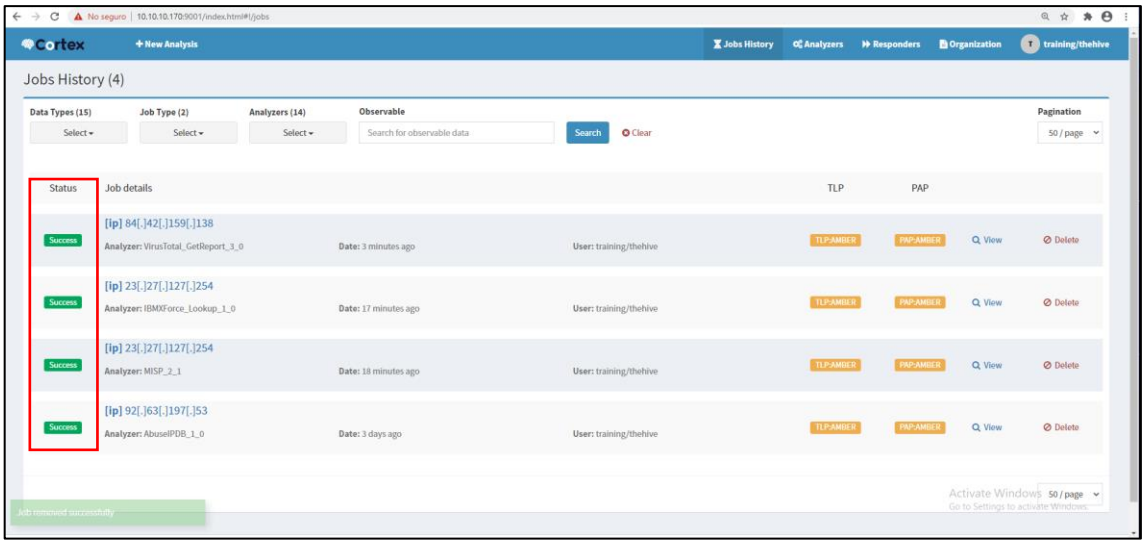
9000 - The Hive

9001 - Cortex

3.3.3 Cortex

Es una herramienta que se integró con The Hive para resolver un problema común que con frecuencia encuentran los profesionales de ciberseguridad. Se busca afianzar el uso de la inteligencia de amenazas, el análisis forense digital y agilizar la respuesta a incidentes.

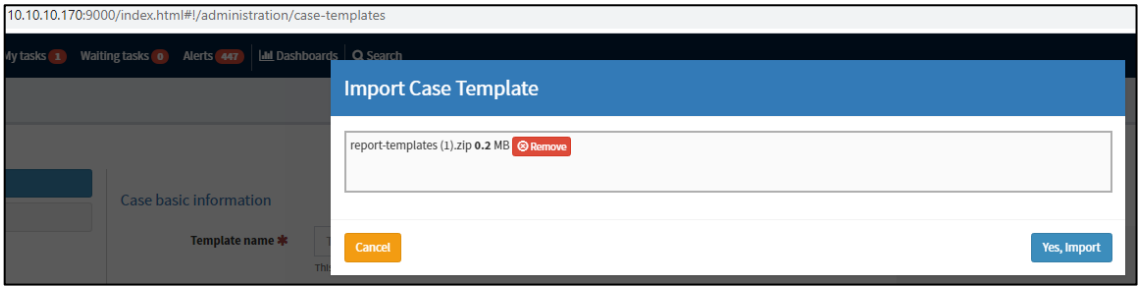
Por medio de la integración por API, se puede automatizar el análisis de observables (IP, e-mail, URL, nombres de dominio, hash, malware, etc.), incluso de forma masiva. (Ver Anexo A). Para dicho uso se debe tener en cuenta la reputación de feeds.

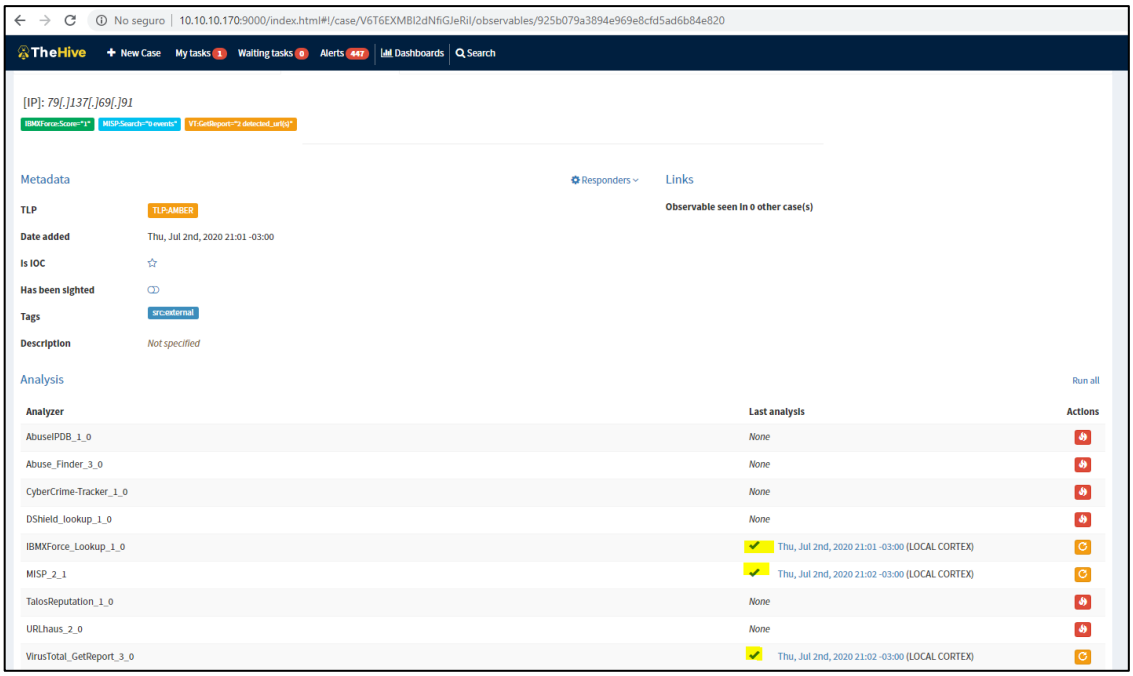


Analyzer - Salida Success de JOBs

Responders - Automatización con Wazuh

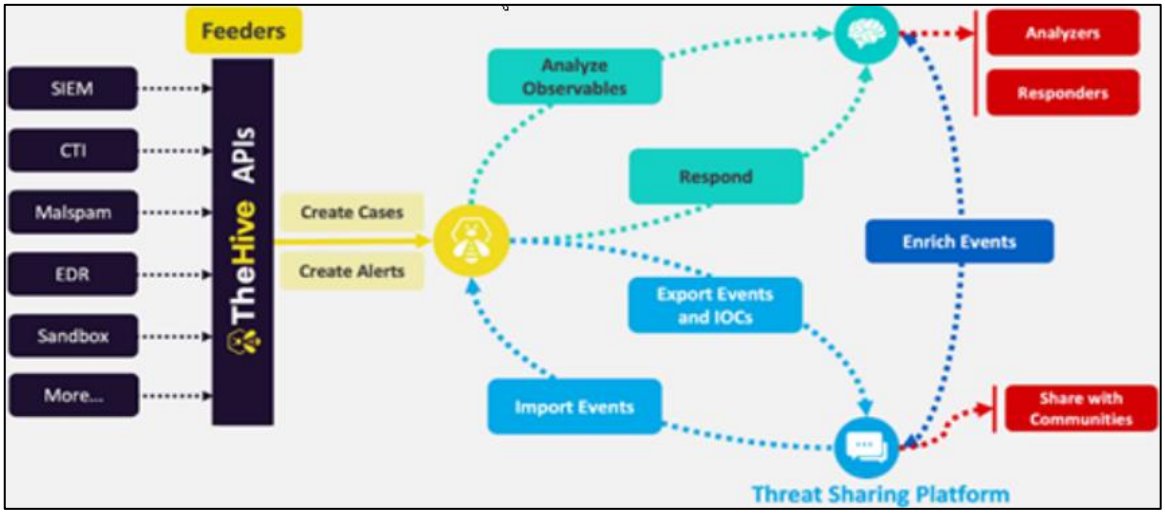
Por otro lado, se importaron plantillas para informes de incidentes de seguridad:



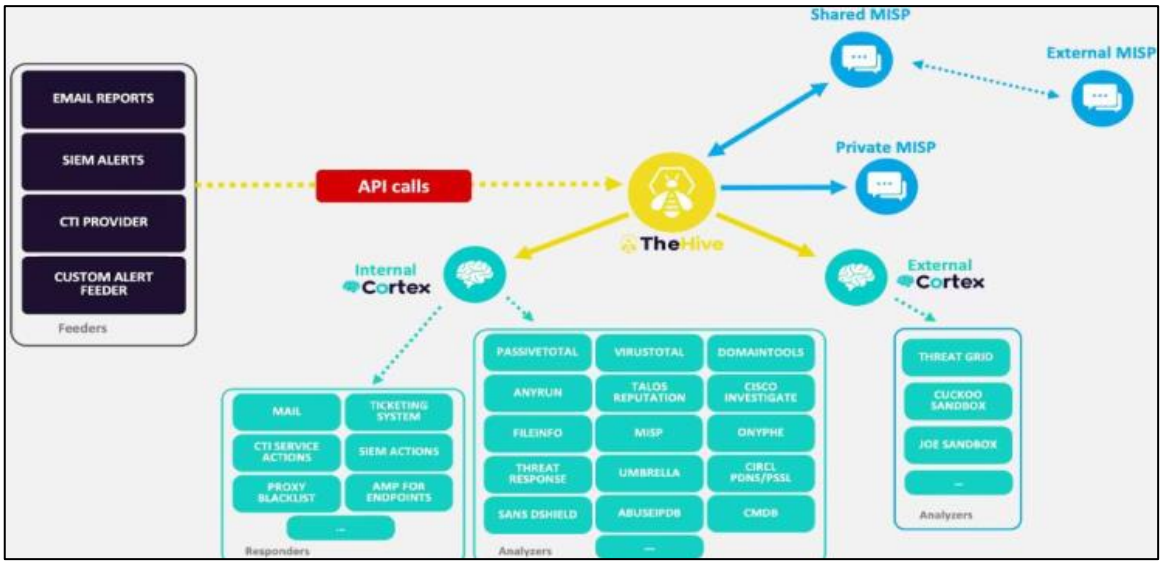


Resultados del IOC [79.137.69.91] analizado por 3 fuentes de CTI.

La funcionalidad que se busca es integrar las alertas generadas desde Security Onion para robustecer y clarificar el análisis sumando información de contexto y aplicando metodología de respuesta ante incidentes:



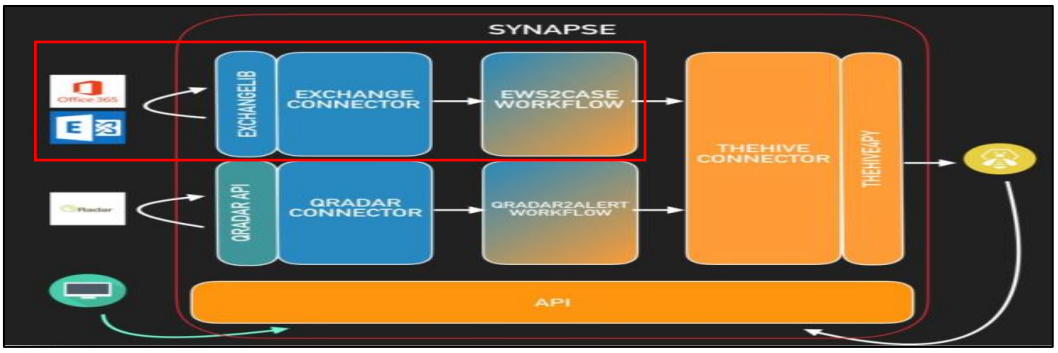
Motor de análisis y respuesta de observables [11]



Arquitectura e integración The Hive Project - MISP [11]

3.3.4 Synapse

Es un complemento que permite alimentar a The Hive por medio de múltiples fuentes de alertas a la vez [12]. En este trabajo, se integra con Office 365, para unificar el flujo de alertas y establecer la metodología de trabajo.



Tipos de alertas integradas:

- Alertas Perimetrales
- Alertas Endpoints
- Actividad Sospechosa múltiples fuentes.
- Alertas de Superación de Umbrales
- Alertas de indicadores de compromiso
- Alertas de seguridad de Distintos Canales

3.3.5 MISP - Malware Information Sharing Platform

Es una plataforma de intercambio de amenazas que ayuda a compartir, almacenar y correlacionar indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidades, entre otros [13].

La funcionalidad que se busca es integrar los datos almacenados en Security Onion con inteligencia de amenazas para que sea accesible y utilizable. En primer lugar, para dar visibilidad en los eventos y actividades de seguridad capturados por las herramientas de seguridad informática. Combinando y correlacionando IOCs y eventos se produce inteligencia genuina relevante para el negocio y así se otorga un panorama más amplio de amenazas.

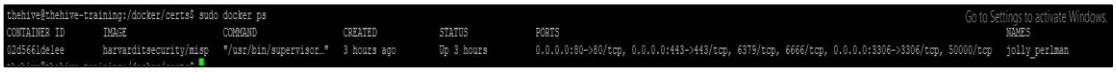
El aspecto crítico de la integración es entregar más inteligencia importante, específica, relevante y contextualizada del grupo cibercriminal correcto en el momento correcto según la matriz MITRE ATT&CK.

La solución se implementó con Docker [14]:

```
service docker start

git clone https://github.com/harvard-itsecurity/docker-misp.git

sudo docker run -it --rm -v /docker/misp-db:/var/lib/mysql harvarditsecurity/misp /init-db

sudo mkdir /docker/certs

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /docker/certs/misp.key -out /docker/certs/misp.crt

sudo docker run -it -d -p 443:443 -p 80:80 -p 3306:3306 -v /docker/certs:/etc/ssl/private -v /docker/misp-db:/var/lib/mysql harvarditsecurity/misp

 #!/bin/bash

 docker rmi harvarditsecurity/misp

 docker build \--rm=true --force-rm=true \

--build-arg MYSQL_MISP_PASSWORD=9s2hd.s-2/s\

--build-arg POSTFIX_RELAY_HOST=localhost \

--build-arg MISP_FQDN=10.10.10.170 \
```

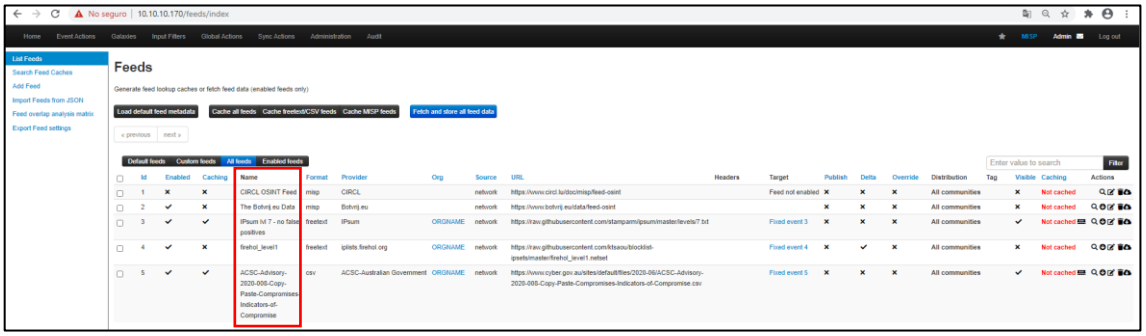
--build-arg MISP_EMAIL=alvaro@misp \

--build-arg MISP_GPG_PASSWORD=L.sjp*/¬sd3fr\



Servicios corriendo

3.3.5.1 Configuración de Feeds



Consola MISP

Se configuraron Feeds, que son fuente de intercambio de información de amenazas para retroalimentar la arquitectura de NG-SIEM.

3.3.6 AIL - Analysis of Information Leaks

Es un marco para analizar posibles filtraciones de información de fuentes de datos no estructuradas como Pastebin o servicios similares. Se utiliza para detección y prevención de fuga de datos. Dentro de sus características principales, posee integración con The Hive y MISP, durante la crawl phase rastrea de manera continua actividad en la DarkWeb, ya sean, claves de privadas, información de usuarios VIP, información confidencial de la organización [15].

Dicha herramienta se implementó como contenedor:

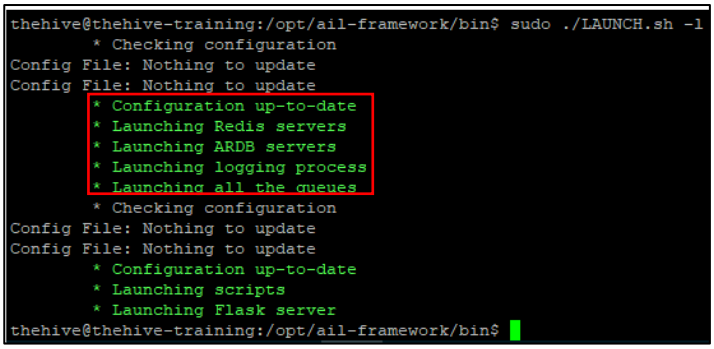
git clone https://github.com/ail-project/ail-framework.git

cd /opt/AIL-framework

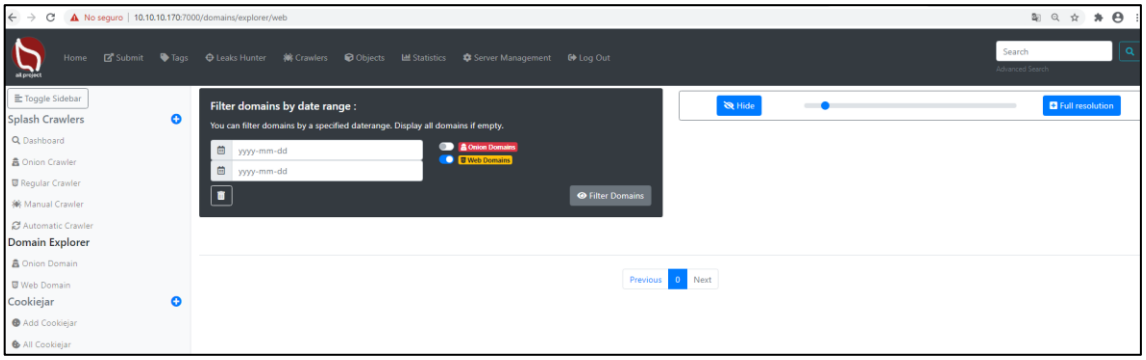
./installing_deps.sh

cd bin/

./LAUNCH.sh -l



Servicio levantado y funcionando



Añadiendo strings de posibles Data Leaks en DarkWeb.

3.3.7 Caldera

La mejor defensa es una defensa probada con anterioridad. Por dicho motivo es que se describirá la instalación y uso de la herramienta, basada en el framework MITRE ATT&CK y diseñada para simular de manera práctica y sencilla habilidades concretas que realizan los atacantes [16].

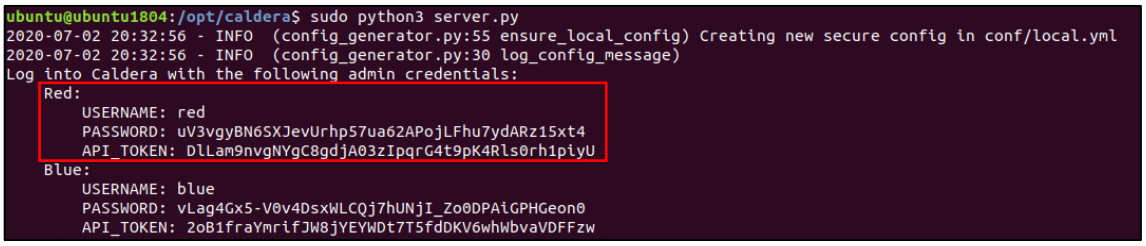
Funciona con un agente llamado 54ndc47 escrito en GoLang para compatibilidad multiplataforma, es el agente implementado en los Endpoints mediante la opción reverse-shell TCP.

Es altamente recomendable primero realizar la instalación de Go:

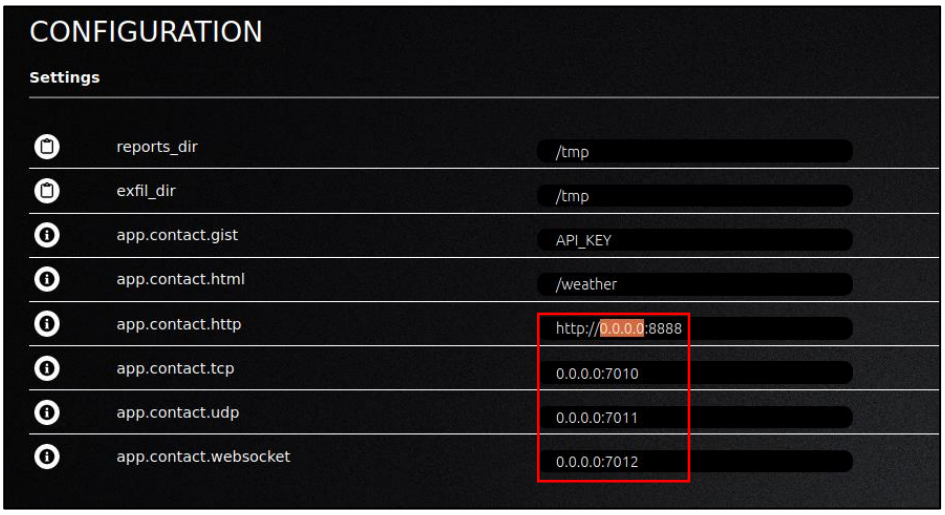
```
curl -O https://dl.google.com/go/go1.10.3.linux-amd64.tar.gz
tar xvf go1.10.3.linux-amd64.tar.gz
sudo chown -R root:root ./go
sudo nano ~/.profile
sudo mv go /usr/local
export GOPATH=$HOME/work
export PATH=$PATH:/usr/local/go/bin:$GOPATH/bin
export GOROOT=$HOME/go
export GOPATH=$HOME/work
export PATH=$PATH:$GOROOT/bin:$GOPATH/bin
source ~/.profile
```

Una vez hecho esto y corroborado, se puede instalar la herramienta:

```
git clone https://github.com/mitre/caldera.git --recursive --branch master
pip3 install -r requirements.txt
python3 server.py
```



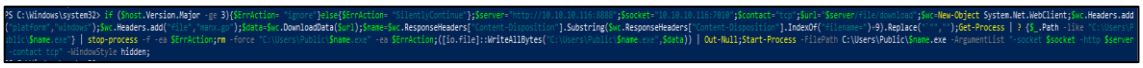
Activación exitosa de Caldera



Configuración de puertos

3.3.7.1 Conexión con máquinas victima

Primero se toma posesión de la víctima con Windows 10, para ello se ejecuta un script:



Ejecución de PSH y verificación de conexión exitosa

Luego, se lanza en el Endpoint Ubuntu el agente reverse-shell para comunicar via TCP con Caldera y realizar las pruebas entre Endpoints:

```
root@ubuntu1804:/home/ubuntu# server="http://10.10.10.116:8888";socket="10.10.10
.116:7010";contact="tcp";curl -s -X POST -H "file:manx.go" -H "platform:linux" $
server/file/download > manx.go;chmod +x manx.go;./manx.go -http $server -socket
$socket -contact $contact -v
[*] tcp outbound socket 10.10.10.116:7010, inbound at 6000
[+] TCP established for ubrihf
```

Ambas máquinas fueron tomadas, una vez hecho, se pasa a ejecutar acciones tales como TTPs.

Evidencia del lado del atacante.

El objetivo es probar y desarrollar análisis de detección basado en los datos generados por las configuraciones personalizadas en Sysmon y Wazuh.

La selección de habilidades se centrará en aquellas que se requieran para cumplir los casos de uso específicos, que se relacionan con actividades comunes en el proceso de intrusión, no obstante, la herramienta provee variaciones en el uso de las habilidades recomendadas.

3.3.8 Agentes

3.3.8.1 Instalación y configuración de Sysmon

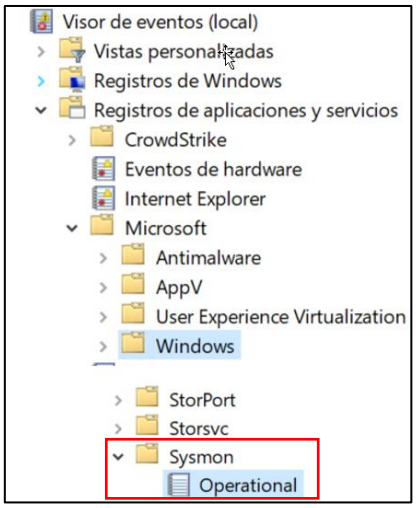
Se pretende utilizar una herramienta EDR libre desarrollada por Microsoft denominada Sysinternals Sysmon. Posee varias funciones, entre ellas colecciona información detallada sobre la actividad de sistema, creaciones de proceso, archivo, conexiones de la red, etc. por medio de un controlador de dispositivos y un servicio que se inicia en el proceso de arranque de manera que permite obtener un mayor trazado en plataformas Windows [17].

Para esto, se tomó como base el proyecto publicado en https://github.com/olafhartong/sysmon-modular. Se lo adaptó para segmentar por tácticas el archivo de configuración sysmonconfig.xml, para añadir algunos controles y excepciones en el visor de eventos de Windows. Dichos eventos serán enviados a Security Onion por medio de Wazuh para comprender cómo operan los intrusos y malware en la red.

```
C:\Users\User-\Desktop\Sysmon\Sysmon_Ejecutable>sysmon.exe -accepteula -i sysmonconfig.xml

System Monitor v11.10 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.30
Sysmon schema version: 4.32
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Servicio Sysmon corriendo y configurado

Luego, en la ubicación del Visor de Eventos se visualizan los Registros “Operacionales”:



3.3.8.2 Instalación y configuración de Wazuh

Es una solución que provee funcionalidades de monitoreo, detección y respuesta de incidentes [18]. Se utilizará para recopilar los registros del Visor de Eventos por medio de un canal cifrado y autenticado que serán enviados al host ngsiem.

En Security Onion se ejecuta:

/var/ossec/bin/manage_agents -a 10.10.10.140 -n win10

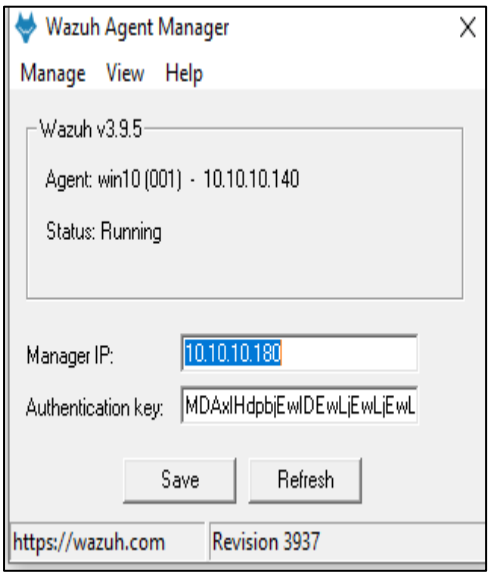
```
root@ngsiem:/home/alvaro# /var/ossec/bin/manage_agents -a 10.10.10.140 -n win10


****************************************
* Wazuh v3.9.5 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent:    * The IP Address of the new agent: Confirm add
ing it?(y/n): Agent added with ID 001.

manage_agents: Exiting.
root@ngsiem:/home/alvaro# /var/ossec/bin/manage_agents -l

Available agents:
   ID: 001, Name: win10, IP: 10.10.10.140
```

Alta de agente

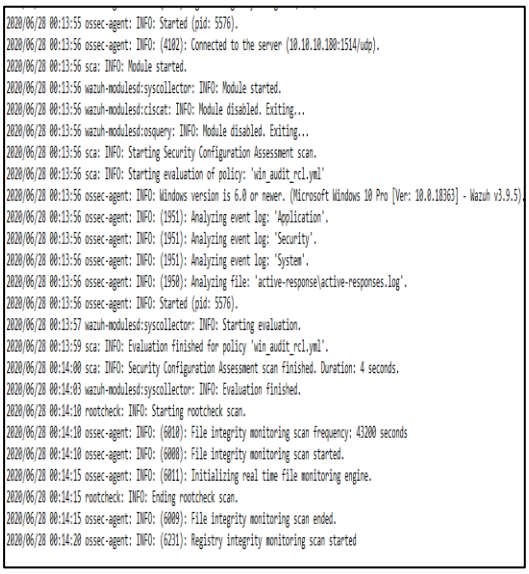
Luego tomamos la clave de autorización para cargarla en el agente posteriormente:

```
root@ngsiem:/home/alvaro# /var/ossec/bin/manage_agents -e 001

Agent key information for '001' is:
MDAxIHdpbjEwIDEwLjEwLjEwLjE0MCAlOWNlOTJjMDlmNDFmZDdmOTIyZDQ2ZDQwN2ZkMzQwMDg5MzIzNTY4ZjhmOTk4M2E2NzIxNzg5M2E1MGM5YTJk
```

En el Endpoint Windows10 validamos la instalación:



Ventana de registración



Eventos de inicialización

Desde el host ngsiem se corrobora la configuración de agentes:

```
root@ngsiem:/home/alvaro# /var/ossec/bin/agent_control -lc

Wazuh agent_control. List of available agents:
   ID: 000, Name: ngsiem (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: win10, IP: 10.10.10.140, Active
```

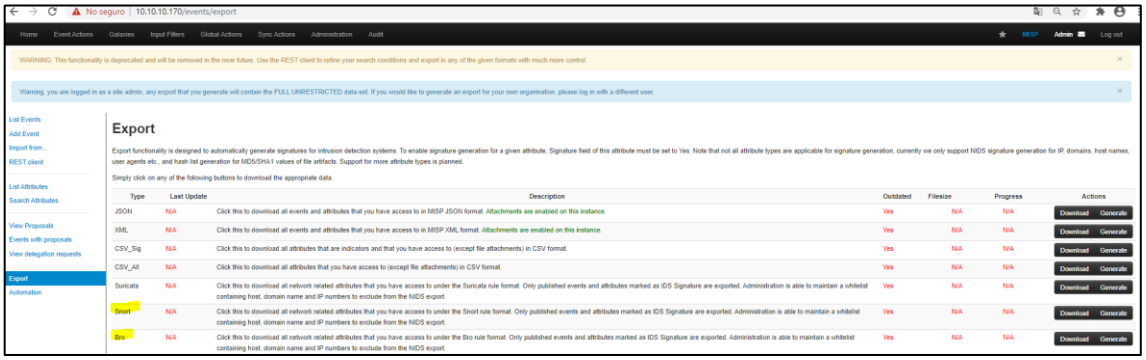
/var/ossec/bin/agent_control -lc

4. Alinear los casos de uso a la topología planteada

A continuación, se detallan las integraciones llevadas a cabo para la orquestación, automatización y control:

4.1 MISP - IDS:

En la consola de MISP, se generan las reglas de IDS y se sincronizan por medio de un script:



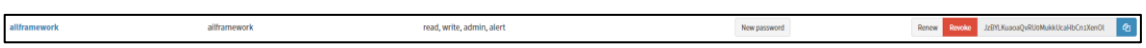
Ventana export Reglas IDS

Se ejecuta el script de integración MISP-Zeek:

```
============================================================
Welcome to the Security Onion MISP Import Wizard!
============================================================


What is the ip address of your MISP instance? [x.x.x.x]
10.10.10.170


What protocol should be used? [http/https]

For security, the protocol is set as https, by default.
Would you like to continue with this protocol? [yes/no]
no

Which protocol would you like to use? [http/https]
http
http
Please provide an API key to access a MISP instance.

You can find this information by navigating to:
https://your-misp-instance/events/automation


Would you like to configure NIDS rules for Snort/Suricata?

If so, please type YES below and press the ENTER key:

YES


Would you like to configure Intel data for Zeek?

If so, please type YES below and press the ENTER key:

YES

To confirm, we will configure the following:

NIDS Rules: /etc/nsm/rules/local.misp.rules
Zeek Intel: /opt/zeek/share/zeek/intel/misp-intel.dat
IP: 10.10.10.170
Protocol: http
API Key: (redacted)


If you would like to continue, please type YES below and press the ENTER key:
YES

Configuring...

Restarting: Zeek
stopping zeek ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/site ...
removing old policies in /nsm/bro/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
starting zeek ...
Restarting: ngsiem-enp0s8

Configuring Pulledpork...

If manually running this script, ensure that /usr/sbin/rule-update is run afterwards.

That's all folks!
```

4.2 The Hive - AIL

Se crea un usuario para integración en The Hive y se exporta la clave API en AIL:



Generación de usuario para integración.

```
thehive@thehive-training:/opt/ail-framework/configs/keys$ cat theHiveKEYS.py
the_hive_url = 'http://10.10.10.170:9000'
the_hive_key = 'JzBYLKuaoaQvRU0MukkUcaHbCnlXenOl' # The Hive auth key can be found on the The Hive web interface under the User Management
the_hive_verifycert = False
```

Configuración de API en AIL

Integración The Hive con AIL-Framework

4.3 The Hive - Cortex

La integración de dichas herramientas viene embebida en la imagen que se utilizó para esta prueba de concepto, no obstante, se añadieron funcionalidades: https://github.com/The Hive-Project/Cortex-Analyzers configurando 152 analyzers y 19 responders para automatizar tareas de análisis y respuesta a incidentes.

Edición del archivo /etc/application.conf:

analyzer {

Directory that holds analyzers

path = [

"/opt/Cortex-Analyzers/analyzers",

]

fork-join-executor {

Min number of threads available for analyze

parallelism-min = 2

Parallelism (threads) ... ceil(available processors * factor)

parallelism-factor = 2.0

Max number of threads available for analyze

```
parallelism-max = 4
}
}
responder {
# Directory that holds responders
path = [
"/opt/Cortex-Analyzers/responders",
        ]
fork-join-executor {
# Min number of threads available for analyze
parallelism-min = 2
# Parallelism (threads) ... ceil(available processors * factor)
parallelism-factor = 2.0
# Max number of threads available for analyze
parallelism-max = 4
}
}
## ANALYZERS
#
analyzer {
# Absolute path where you have pulled the Cortex-Analyzers repository.
#path = ["/opt/Cortex-Analyzers/analyzers"]
urls = ["https://dl.bintray.com/The Hive-project/cortexneurons/analyzers.json"]

# Sane defaults. Do not change unless you know what you are doing.
fork-join-executor {

# Min number of threads available for analysis.
parallelism-min = 2
# Parallelism (threads) ... ceil(available processors * factor).
parallelism-factor = 2.0
# Max number of threads available for analysis.
parallelism-max = 4
```

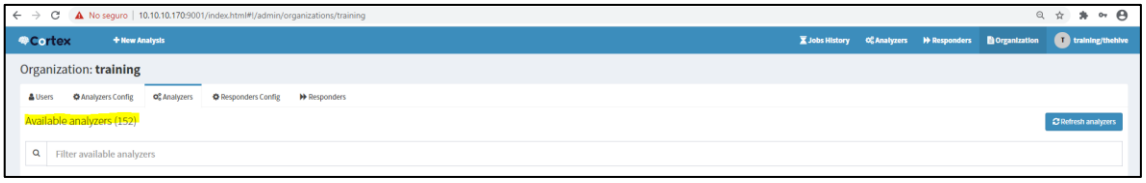
}

}

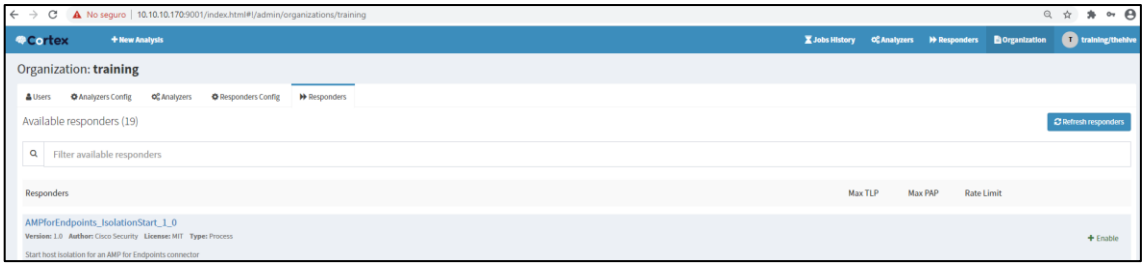
responder {

path = ["/opt/Cortex-Analyzers/responders"]

}



Cantidad de analizadores disponibles



Cantidad de responders disponibles

4.4 The Hive - ElastAlert

Se configuró a través de ElastAlert el envió de reglas matcheadas IDS-MISP a The Hive

El comando para testear la configuración de alertas es:

sudo so-elastalert-test /etc/elastalert/elastalert_config.yaml

misp-nids-hive.yaml

Elastalert rule to forward IDS alerts generated by MISP NIDS rules from Security Onion

to a specified The Hive instance.

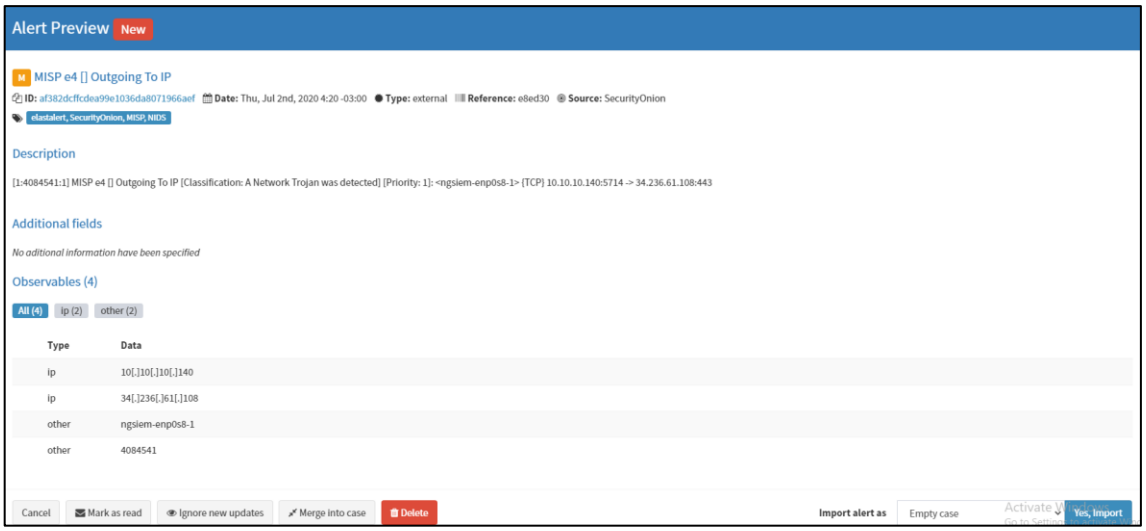
#

es_host: 10.10.10.180

es_port: 9200

name: MISP NIDS Rule Match

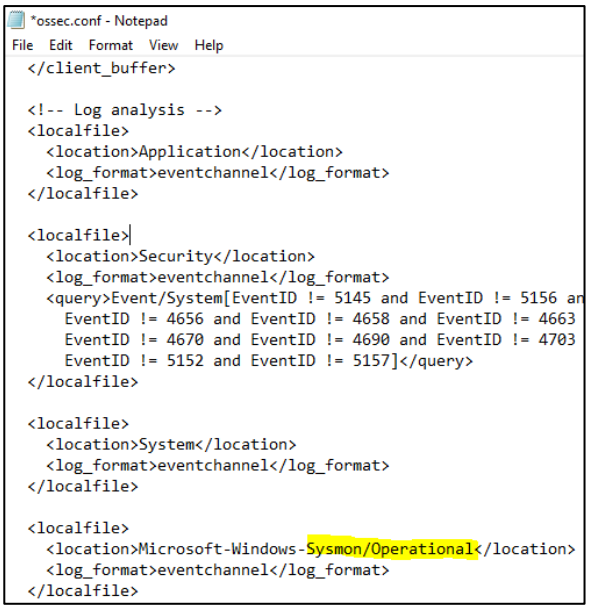
```
type: frequency
index: "*:logstash-ids*"
num_events: 1
timeframe:
    minutes: 1
filter:
 - query:
    query_string:
     query: "alert: MISP"
alert:
- "hivealerter"
hive_connection:
    hive_host:  http://10.10.10.170:9000
    hive_apikey: f2+cLlZVNuI6/wHBO/UA+97DpRSrWavu
hive_alert_config:
    title: '{match[alert]}'
    type: 'external'
    source: 'Security Onion'
    description: '{match[message]}'
    severity: 2
    tags: ['elastalert, Security Onion, MISP, NIDS']
    tlp: 3
    status: 'New'
    follow: True
hive_observable_data_mapping:
    - ip: '{match[source_ip]}'
    - ip: '{match[destination_ip]}'
    - other: '{match[interface]}'
    - other: '{match[sid]}'
```



Visualización de alerta en The Hive - Nuevo Incidente de seguridad

4.5 Wazuh - Sysmon

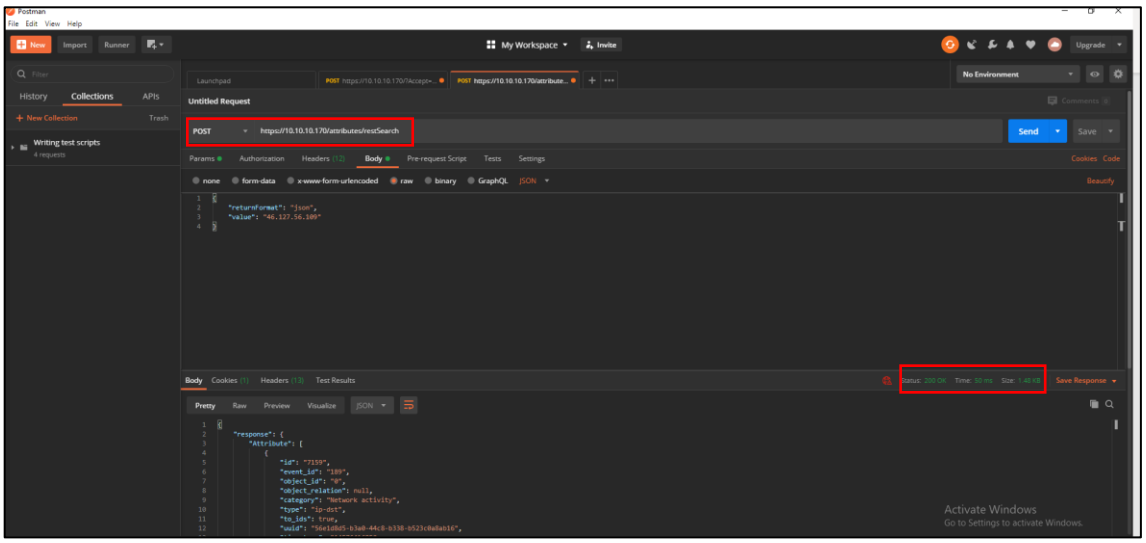
Se edita el archivo de configuración del agente Wazuh para que tome los registros Operacionales del Visor de Eventos de Windows:



4.6 Testeo de integración por API

Las integraciones fueron testeadas con la herramienta Postman [19], la cual se utiliza, sobre todo, para consumir, depurar y realizar pruebas de API REST, monitorizarlas, simularlas, etc.

En la imagen siguiente, por medio de un POST obtenemos una salida válida, de esta forma podemos decir que la API está respondiendo:



4.7 Configuración de las reglas a monitorearse

4.7.1 Sysmon

Para la obtención de registros relacionados con la matriz de MITRE, se configuraron las reglas de monitoreo según el alcance que tiene Sysmon de acuerdo con la matriz de MITRE ATT&CK [20].

4.7.2 BZAR - Zeek

Se importaron y cargaron reglas referentes al framework MITRE ATT&CK:

```
alvaro@ngsiem:/opt/bzar/attack_scripts$ ls
bzar_config_options.bro  bzar_files.bro        bzar_smb_report.bro
bzar_dce-rpc_consts.bro  bzar_smb1_detect.bro  dpd.sig
bzar_dce-rpc_detect.bro  bzar_smb2_detect.bro  __load__.bro
bzar_dce-rpc_report.bro  bzar_smb_consts.bro   main.bro
```

Importación de reglas https://github.com/mitre-attack/bzar

```
Rule Stats...
        New:-------56
        Deleted:---14280
        Enabled Rules:----20319
        Dropped Rules:----0
        Disabled Rules:---9222
        Total Rules:------29541
```

Carga de reglas

4.7.3 Wazuh

Configuración Monitoreo de Integridad de Archivos (FIM):

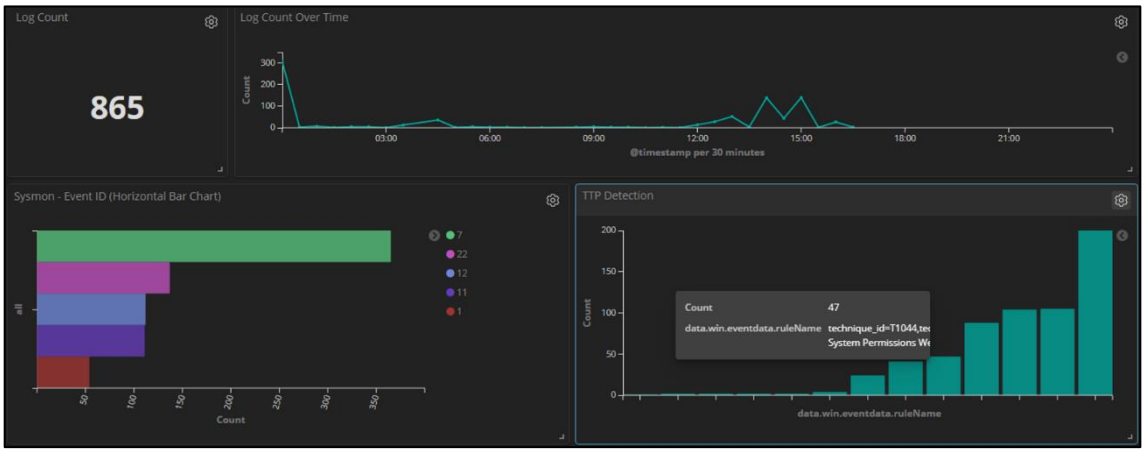
```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->

   <frequency>6000</frequency>

  <directories check_all="yes" realtime="yes" report_changes="yes">C:\Users\User-\Documents\BaseDeClientesVIP</directories>
```

Control tiempo real de modificación en directorio “BaseDeClientesVIP”

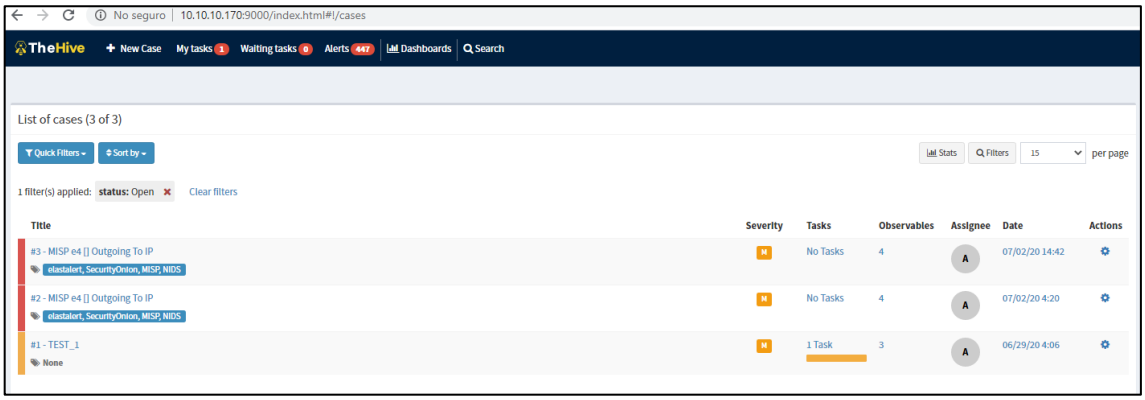
5. Control y monitoreo

5.1 Implementación de Dashboards

Por medio de un Dashboard en Kibana, podemos apreciar las reglas que se correlacionaron para tener métricas sobre las posibles TTPs detectadas tanto en Endpoints (Sysmon/Wazuh) como perímetro (BZAR - Zeek).

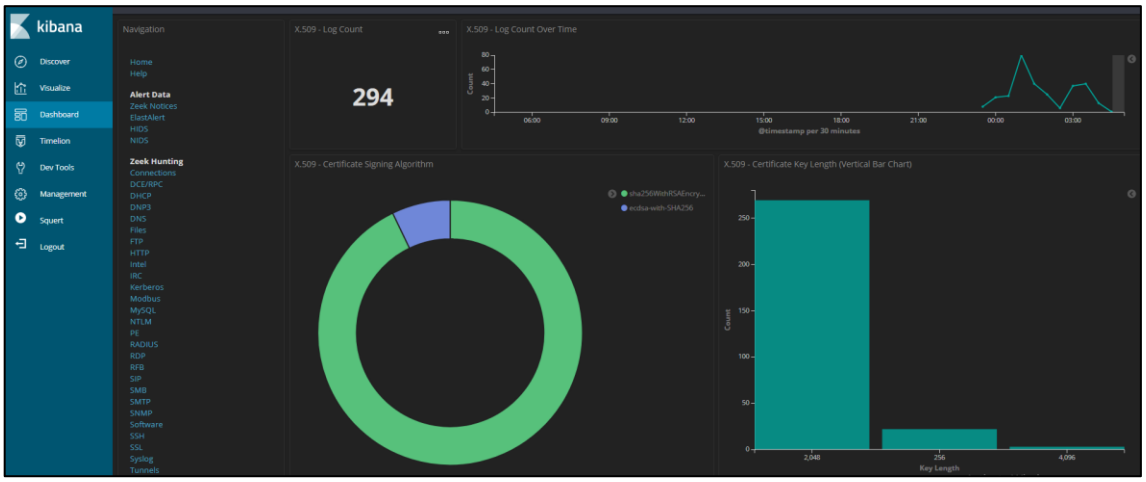


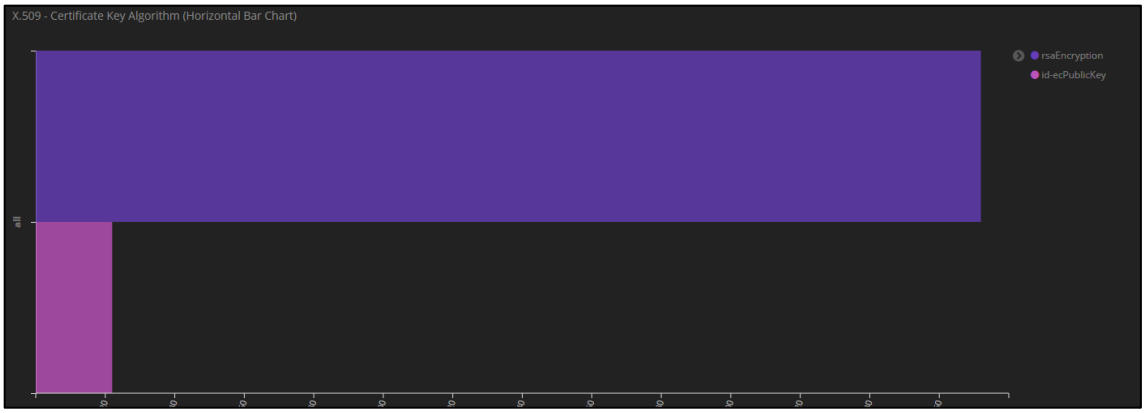
Desde The Hive se visualizan las alertas generadas por ElastAlert sobre los eventos correlacionados en Security Onion:



Gestión de incidentes de seguridad por medio de casos

5.1.1 Dashboard - Detección y métricas de certificados.





X.509 - Certificate Subject

Subject	Count
CN=*.rfihub.com,O=ZETA GLOBAL CORP.,L=New York,ST=New York,C=US	16
CN=*.adnxs.com,O=AppNexus\, Inc.,L=New York,ST=New York,C=US	13
CN=settings-win.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US	12
CN=smartscreen.microsoft.com	12
CN=*.rubiconproject.com,O=The Rubicon Project\, Inc.,L=Los Angeles,ST=California,C=US	9
CN=www.github.com,O=GitHub\, Inc.,L=San Francisco,ST=California,C=US	9
CN=*.githubassets.com,O=GitHub\, Inc.,L=San Francisco,ST=California,C=US	8
CN=*.msedge.net	7
CN=getpostman.com	7
CN=*.pstmn.io	6

X.509 - Certificate Issuer

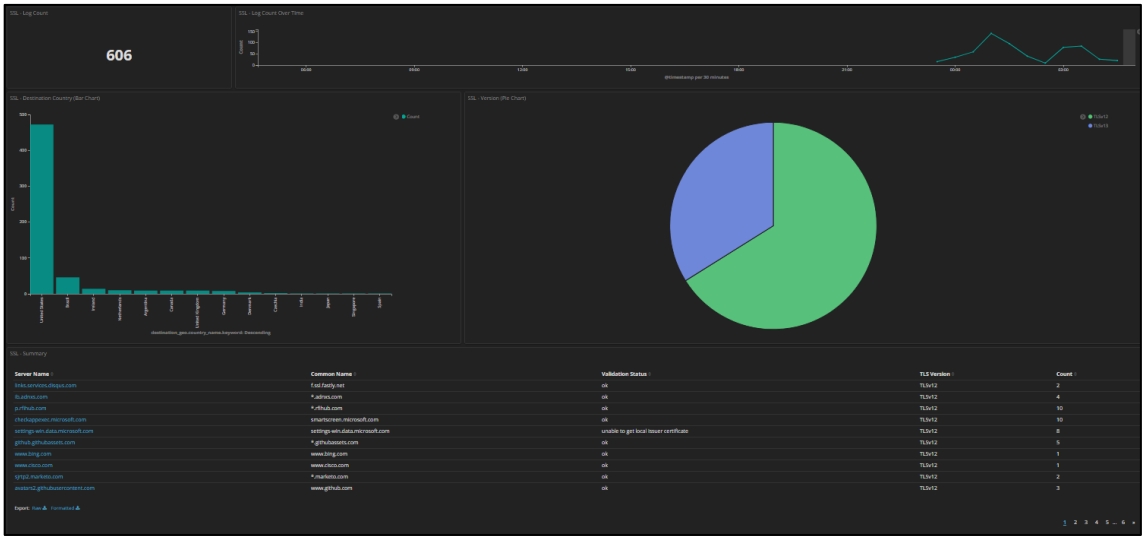
Issuer	Count
CN=DigiCert SHA2 Secure Server CA,O=DigiCert Inc,C=US	58
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	52
CN=DigiCert SHA2 High Assurance Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US	30
CN=Microsoft Secure Server CA 2011,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US	18
CN=Microsoft IT TLS CA 1,OU=Microsoft IT,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US	17
CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US	16
CN=DigiCert ECC Secure Server CA,O=DigiCert Inc,C=US	13
CN=GlobalSign CloudSSL CA - SHA256 - G3,O=GlobalSign nv-sa,C=BE	11
CN=Microsoft IT TLS CA 4,OU=Microsoft IT,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US	9
CN=Microsoft IT TLS CA 2,OU=Microsoft IT,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US	7

5.1.2 FIM - Monitoreo de alteración de objetos

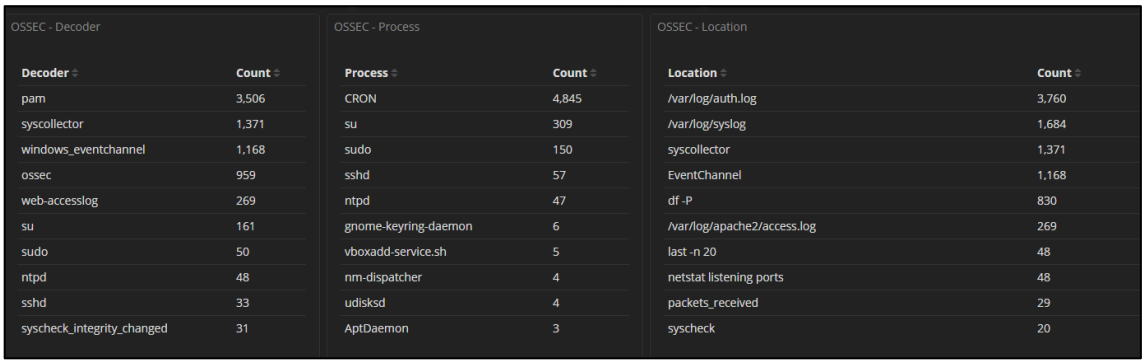
agent.name	win10
alert_level	7
classification	"Bad word" matching
decoder.name	syscheck_integrity_changed
description	Integrity checksum changed.
event_type	ossec
full_log	File 'c:\users\user-\documents\basedeclientesvip\nuevocliente.txt' checksum changed. Size changed from '45' to '19' Old md5sum was: 'd5deb93d8d49064c4db7a469c7028b5c' New md5sum is : '07595f5f9879d34e9ab9dd7a32de319d' Old sha1sum was: '12481e7f32a1724f135712e861069e3b7c2fc7a1' New sha1sum is : 'e7d24a73b34849e490308036661322c136772e2d' Old sha256sum was: '64d271b477cd8efa00b6b6f38a39b4dbf6d1a93fca6b5ed9044b3cffed9af5c0' New sha256sum is : 'aab907e35a7cbe7f2773eefa3df9be3238b60535ce340739c83c6710b0d92a1e' Old modification time was: 'Tue Jul 7 14:18:30 2020', now it is 'Tue Jul 7 14:20:28 2020' < hugo_pagola < javier_vallejos < hugo_pagola --- > borrado de clientes

En la imagen se aprecia, cómo se realizó borrado de contenido en un documento “nuevocliente.txt” y se verifica la variación del hash.

5.1.3 Dashboard - Detección y métricas para SSL



5.1.4 Dashboard - Control de Endpoints



OSSEC - Decoder

Decoder	Count
pam	3,506
syscollector	1,371
windows_eventchannel	1,168
ossec	959
web-accesslog	269
su	161
sudo	50
ntpd	48
sshd	33
syscheck_integrity_changed	31

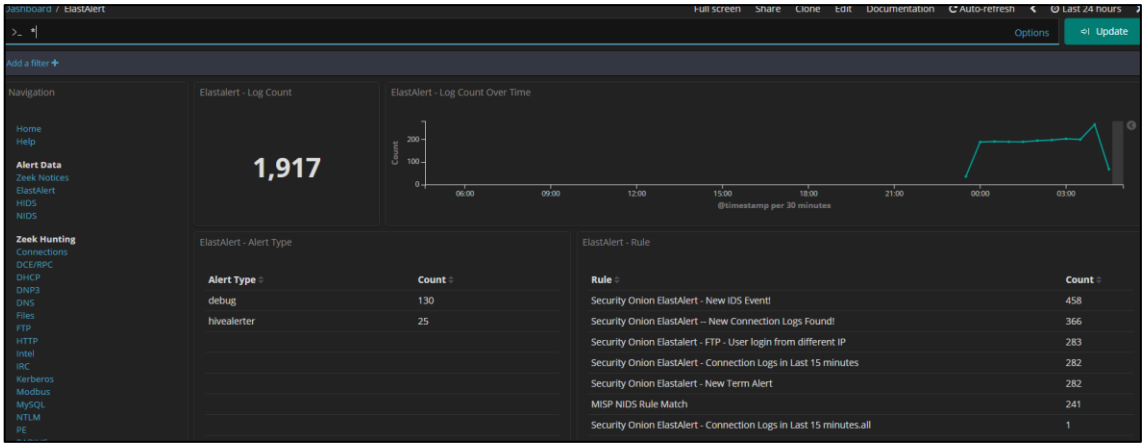
OSSEC - Process

Process	Count
CRON	4,845
su	309
sudo	150
sshd	57
ntpd	47
gnome-keyring-daemon	6
vboxadd-service.sh	5
nm-dispatcher	4
udisksd	4
AptDaemon	3

OSSEC - Location

Location	Count
/var/log/auth.log	3,760
/var/log/syslog	1,684
syscollector	1,371
EventChannel	1,168
df -P	830
/var/log/apache2/access.log	269
last -n 20	48
netstat listening ports	48
packets_received	29
syscheck	20

5.1.5 Dashboard - Control de perímetro



Navigation

Home
Help

Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS

Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE

Elastalert - Log Count

1,917

ElastAlert - Log Count Over Time

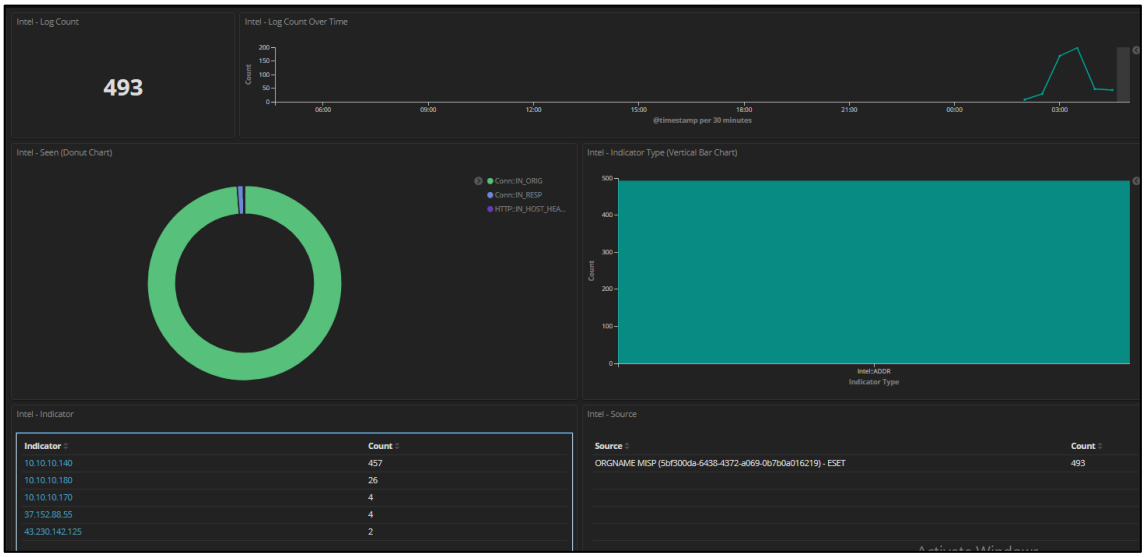
ElastAlert - Alert Type

Alert Type	Count
debug	130
hivealerter	25

ElastAlert - Rule

Rule	Count
Security Onion ElastAlert - New IDS Event!	458
Security Onion ElastAlert -- New Connection Logs Found!	366
Security Onion Elastalert - FTP - User login from different IP	283
Security Onion ElastAlert - Connection Logs in Last 15 minutes	282
Security Onion Elastalert - New Term Alert	282
MISP NIDS Rule Match	241
Security Onion ElastAlert - Connection Logs in Last 15 minutes.all	1

5.1.6 Dashboard - Control de tráfico sospechoso



Intel - Log Count

493

Intel - Log Count Over Time

Intel - Seen (Donut Chart)

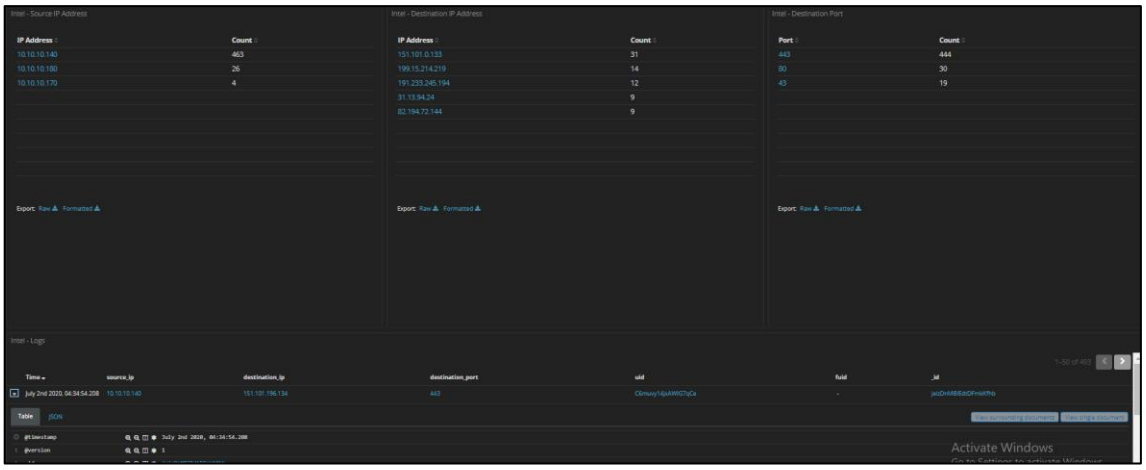
Intel - Indicator Type (Vertical Bar Chart)

Intel - Indicator

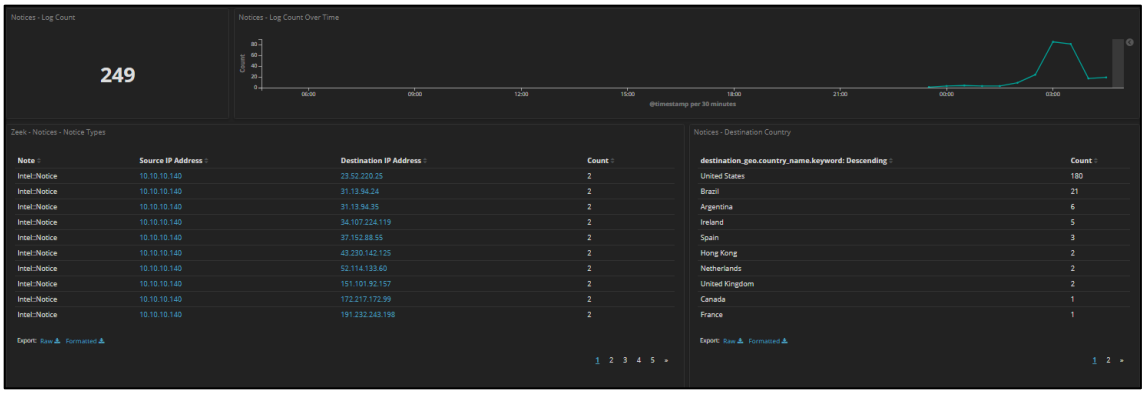
Indicator	Count
10.10.10.140	457
10.10.10.180	26
10.10.10.170	4
37.152.88.55	4
43.230.142.125	2

Intel - Source

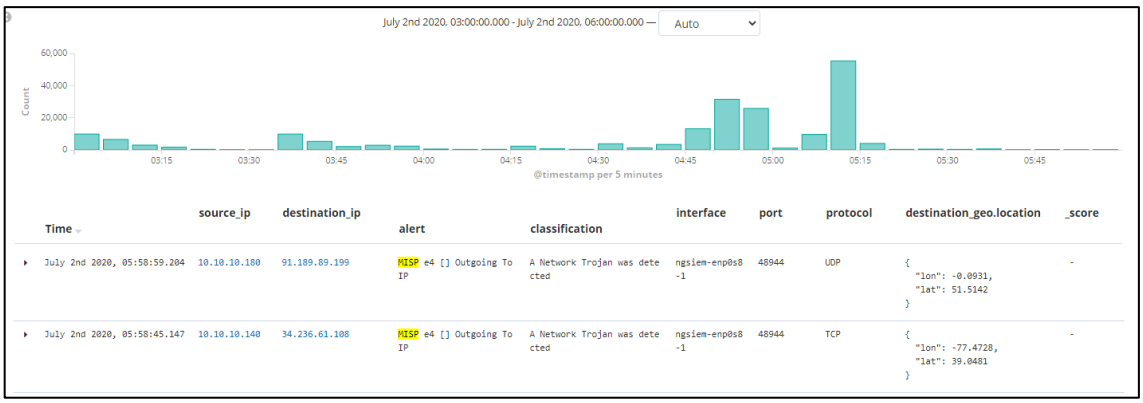
Source	Count
ORGNAME MISP (5bf300da-6438-4372-a069-0b7b0a016219) - ESET	493



5.1.7 Trafico por país y catalogación de IOCs



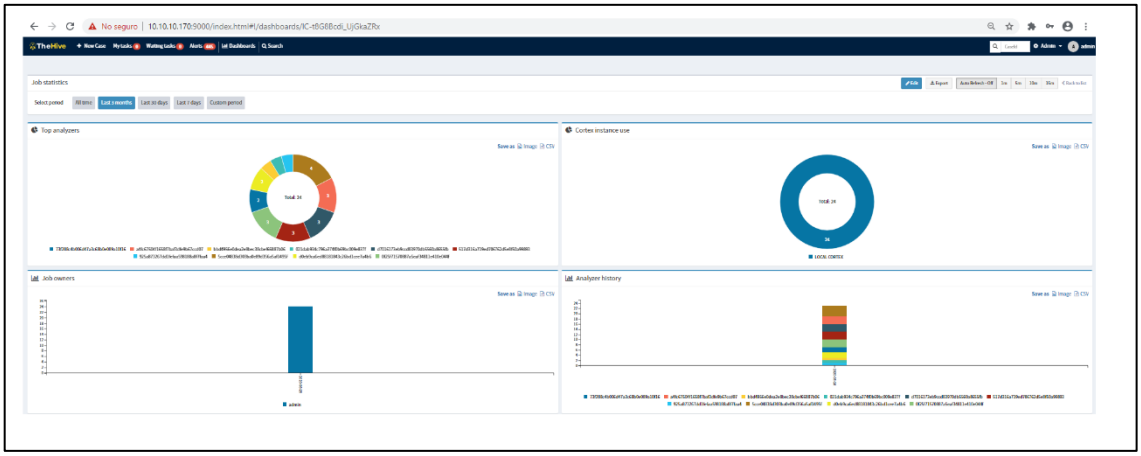
5.1.8 CTI - Comunicación con IOCs

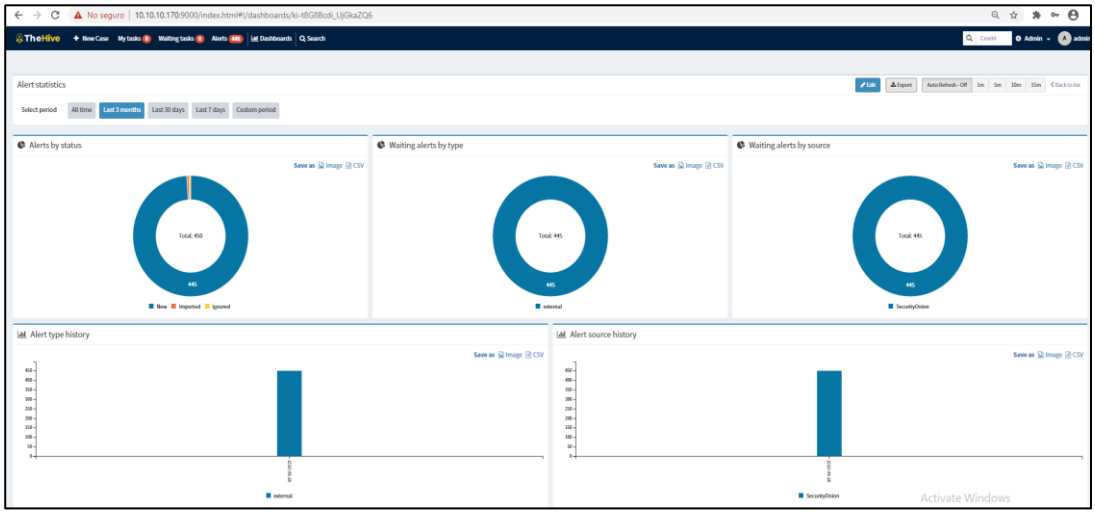


Luego de correlacionar indicadores de compromiso con los registros de las fuentes de eventos, se puede reflejar en el Dashboard la existencia de tráfico permitido con destino reportado por actividades maliciosas.

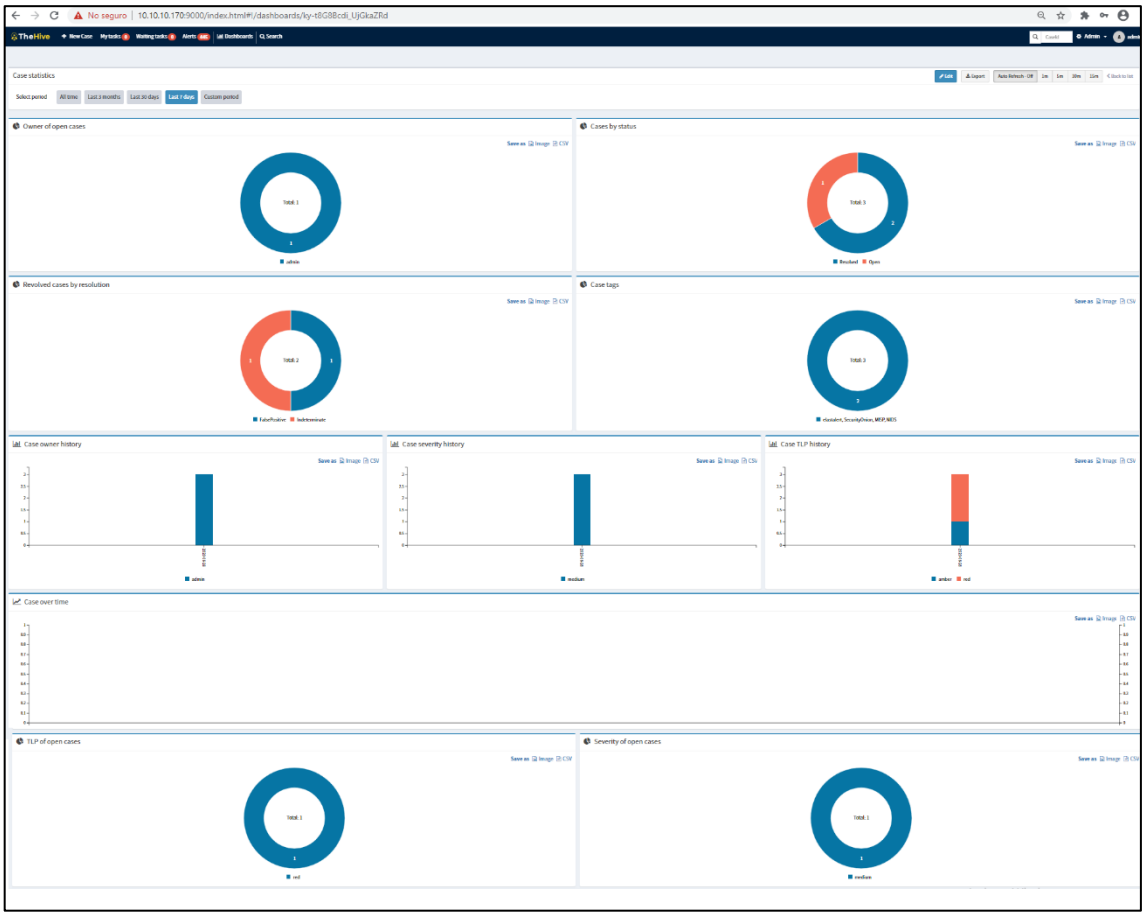
5.2 Generación de reportes

5.2.1 Métricas - Flujo de Tareas del análisis automatizado





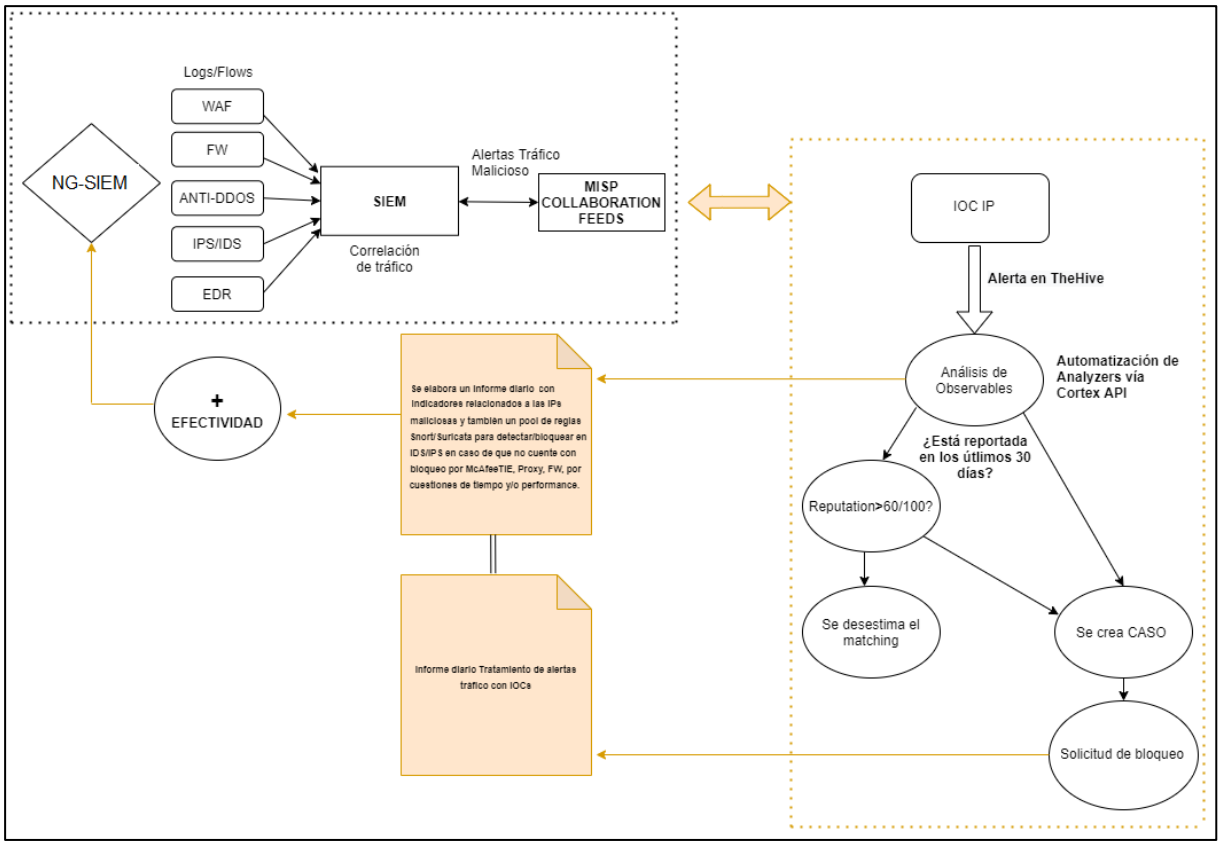
5.2.2 Métricas - Gestión de Incidentes



6. Metodología de trabajo

6.1 Análisis manual de Alertas

El análisis manual de alertas se realiza por medio de las herramientas implementadas como SOAR, retroalimentándose bidireccionalmente con feeds integrados de inteligencia de la amenaza.



Flujo de trabajo NG-SIEM

6.2 Análisis de comportamiento

Como dato de entrada, tenemos los registros y alertas en tiempo real. Los mismos se investigan manualmente, a través de incidentes generados automáticamente por SOAR. También, se puede realizar el análisis por medio de Dashboards armados específicamente para detección de comportamiento anómalo basado en probabilidad y estadística.

6.3 Obtención de indicadores sobre rangos amplios de tiempo

Por medio de los eventos gestionados en la solución NG-SIEM, es posible obtener información valiosa analizando largos períodos de tiempo. Se elaboran y optimizan Dashboards, de forma tal que sea posible analizar desde “lo macro” las distintas alertas que se generaron en un rango de tiempo definido. Puede ser para todas las unidades de negocio, buscando tendencias de vectores de ataque como así también encontrar similitudes de indicadores de compromiso, definir cadena de ataques y manipular la severidad de los indicadores proporcionados entre unidades de negocio.

6.4 Informe de incidentes

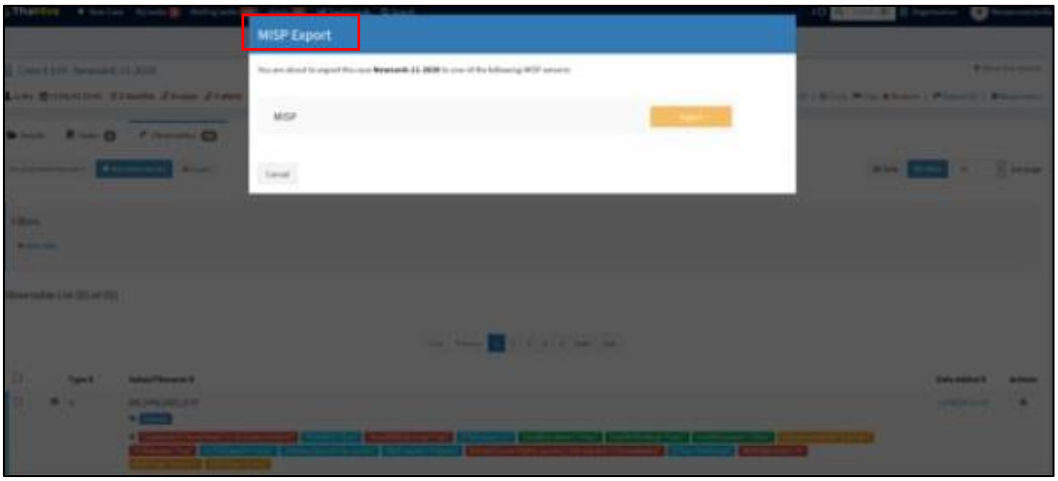
El informe de incidente es el documento que expone las observaciones, tareas y resultados que se identifican con el incidente. El mismo debe tener:

- Qué sucedió
- La cronología del acontecimiento
- Clasificación y priorización del incidente
- Una lista de activos afectados
- El impacto del incidente en la organización
- Las decisiones que se tomaron para la contención, el análisis y la erradicación.
- Los resultados de un análisis de la causa raíz de por qué pudo haber ocurrido el incidente.

7. Análisis de resultados

Tras haber analizado los distintos inputs, tales como alertas manuales de severidad alta, estadísticas de comportamiento, indicadores suministrados por terceros, se realiza la gimnasia de la tarea de ciber inteligencia. Para dar como resultado, la elaboración de nuevos indicadores de compromiso, importando los mismos a la plataforma MISP para ser compartidos. Generando a partir de entonces nuevos bloqueos automáticos e indicadores propios de naturaleza maliciosa comprobada.

Finalmente, el intercambio de información recíproco con distintas organizaciones puede ayudar a que el mismo incidente no vuelva a suceder.



Export de IOCs hacia MISP para compartir información de amenazas

8. Conclusiones

El trabajo proporciona una visión general a alto nivel de los componentes necesarios para una plataforma de Next-Generation SIEM, así como también provee una visión realista, aunque simplista, sobre cómo utilizar la solución para detectar, analizar y responder a la dificultad que presentan las amenazas avanzadas.

También el desarrollo sobre como instalar, configurar y operar las distintas herramientas en un entorno de pruebas.

La dificultad de realización y utilización de esta solución es relativamente baja. Con una buena configuración de las herramientas, se podría descubrir indicadores de riesgo iniciales en Endpoints/perímetro y utilizarlos como punto de partida en la investigación de incidentes. La herramienta Caldera, es de gran utilidad a la hora de probar las soluciones de seguridad; así como para comprender mejor cómo se ejecutan algunas técnicas.

En conjunto con SOAR se demostró cómo mejorar la eficiencia en la gestión y construcción de informes de seguridad acordes a las mejores prácticas, resolviendo los incidentes de manera ágil.

Cada punto de la infraestructura tiene puntos débiles y fuertes. Si optamos por las herramientas adecuadas para monitorear la mayor cantidad de vectores de ataque posibles, podemos cubrir la matriz de MITRE ATT&CK. Las lecciones aprendidas en las investigaciones de seguridad se pueden utilizar para descubrir nuevos indicadores, por medio de la correlación entre los registros de infraestructura y los del módulo de ciber inteligencia. De manera tal, que se haga foco en los riesgos relevantes y así mejorar la postura de seguridad.

9. Bibliografía

[1] «Internet Crime Report 2020» [En línea]. Disponible en: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [Consultada el: 18-dic-2020].

[2] «2021 Unit 42 Ransomware Threat Report» [En línea]. Disponible en: https://www.paloaltonetworks.com/resources/research/unit42-ransomware-threat-report-2021 [Consultada el: 20-nov-2020].

[3] «FireEye Mandiant - Mtrends-2020» [En línea]. Disponible en: https://content.fireeye.com/m-trends/rpt-m-trends-2020 [Consultada el: 20-nov-2020].

[4] «An Evaluator's Guide to NextGen SIEM - Barbara Filkins» [En línea]. Disponible en: https://www.sans.org/reading-room/whitepapers/logging/paper/38720 [Consultada el: 20-nov-2020].

[5] «What is SOAR» [En línea]. Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-soar [Consultada el: 15-mar-2021].

[6] «Threat Intelligence - Desde qué hasta cómo lo hago» [En línea]. Disponible en: https://incibe.es+cybercamp17 [Consultada el: 20-nov-2020].

[7] «MITRE ATT&CK» [En línea]. Disponible en: https://attack.mitre.org [Consultada el: 20-nov-2020].

[8] «Lisbon Conference - TheHive Project» [En línea]. Disponible en: http://docs.thehive-project.org/resources/Keynotes/TLP-WHITE-Bsides_Lisbon2018-TheHive_Cortex_MISP.pdf [Consultada el: 20-nov-2020].

[9] «Security Onion» [En línea]. Disponible en: https://Security Onionsolutions.com [Consultada el: 20-nov-2020].

[10] «BZAR - MITRE ATT&CK» [En línea]. Disponible en: https://github.com/mitre-attack/bzar [Consultada el: 20-nov-2020].

[11] «The Hive Project» [En línea]. Disponible en: https://The Hive-project.org [Consultada el: 20-nov-2020].

[12] «Synapse - a Meta Alert Feeder for The Hive» [En línea]. Disponible en: https://www.github.com/The Hive-Project/Synapse [Consultada el: 20-feb-2021].

[13] «MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing» [En línea]. Disponible en: https://www.misp-project.org [Consultada el: 20-nov-2020].

[14] «Docker» [En línea]. Disponible en: https://docs.docker.com [Consultada el: 20-nov-2020].

[15] «AIL Framework - Analysis Information Leak framework» [En línea]. Disponible en: https://github.com/CIRCL/AIL-Framework [Consultada el: 20-nov-2020].

[16] «MITRE CALDERA» [En línea]. Disponible en: https://github.com/mitre/caldera [Consultada el: 20-nov-2020].

[17] «Microsoft Sysmon» [En línea]. Disponible en: https://docs.microsoft.com/enus/sysinternals/downloads/sysmon [Consultada el: 20-nov-2020].

[18] «Wazuh - The Open Source Security Platform» [En línea]. Disponible en: https://wazuh.com [Consultada el: 20-nov-2020].

[19] «Postman - The Collaboration Platform for API Development» [En línea]. Disponible en: https://www.postman.com [Consultada el: 20-feb-2021].

[20] «MITRE CAR - Cyber Analytics Repository» [En línea]. Disponible en: https://car.mitre.org/sensors/sysmon_11.0 [Consultada el: 20-feb-2021].

10. Glosario

Crawl Phase: La fase de rastreo implica navegar por la DarkWeb, seguir enlaces, enviar formularios e iniciar sesión cuando sea necesario, para catalogar contenido y rutas. Presenta una variedad de desafíos para crear un mapa preciso de posibles riesgos para activos de la información.

DDoS: Ataque de denegación de servicio distribuido. Una variación de DoS. En un ataque DDoS el tráfico malicioso entrante proviene de múltiples orígenes. Pueden ser más potentes y difíciles de mitigar.

ELK: Elasticsearch+Logstash+Kibana. Esta combinación Open Source da como resultado el producto ELK, que combina la capacidad de Logstash (una pila dinámica enriquecida con plugins, para ingestar datos), la velocidad de búsqueda de Elasticsearch (motor para almacenar, buscar y analizar grandes volúmenes de datos en tiempo real) y la interfaz de Kibana (interfaz gráfica web encargada de la visualización mediante distintos diagramas y gráficos)

Exploit Kits: Son paquetes de código malicioso que suelen aprovechar varios vectores de ataque para explotar vulnerabilidades conocidas o no.

0day: Se denomina vulnerabilidad de día 0 a los bugs encontrados que aún no están reportados o no tienen una cobertura por parte de los fabricantes de tecnología de seguridad informática o una salvaguarda a disposición de la comunidad.

IOC: son datos forenses que identifican actividades potencialmente maliciosas en un sistema o red. Las organizaciones pueden detectarlos y actuar rápidamente para evitar ataques durante sus primeros estadíos.

Reputación de feeds: Se denomina a la probabilidad de ocurrencia negativa sobre el negocio que posee un IOCs.

SPAN Port: Básicamente es un puerto configurado en el switch que obtiene una duplicación del tráfico para utilizarlo en un IDS y ejecutar controles sin afectar la disponibilidad de la red interna.

Malware: es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

Incidentes de exfiltración de datos: Hace referencia a cuando una organización reconoce que fue atacada y vulnerada junto a sus posibles activos de información, puede ser medido o no.

TTPs: Técnicas, Tácticas y Procedimientos catalogadas por la matriz de MITRE ATT&CK.

Amenazas persistentes avanzadas: ataques dinámicos que evaden las herramientas de seguridad informática tradicionales por su naturaleza sigilosa. Suelen estar controladas de forma remota.

CTI: Ciberinteligencia de la amenaza es un concepto de colección de información de acuerdo con las tendencias actuales respecto de amenazas de ciberseguridad.

Ransomware: código malicioso que impide o limita el acceso de los usuarios a su sistema, ya sea bloquear la pantalla o cifrando archivos hasta que se pague un rescate.

Observables: Son los registros y otros datos que se crean para evaluar indicador de ataque que pueden ser analizados para añadir inteligencia a los motores de correlación.

HTTP: Protocolo de transferencia de hipertexto. Un protocolo utilizado para servir contenido web desde un servidor a un cliente.

HTTPS: Protocolo de transferencia de hipertexto seguro. Extensión de HTTP que utiliza SSL o TLS para cifrar la comunicación.

IP: Protocolo de Internet. Un protocolo de red que divide el tráfico en paquetes. Los dispositivos se identifican mediante direcciones IP.

IDS: Sistema de detección de intrusos. Un producto de hardware y software que analiza la información de una computadora o una red de computadoras para identificar posibles brechas de seguridad.

IPS: Sistema de Prevención de Intrusión. Similar a un IDS, pero un IPS también es capaz de detener la brecha de seguridad identificada, por ejemplo, bloqueando la conexión de red maliciosa.

LAN: Red de área local. Una red informática que conecta dispositivos capaces de funcionar en red dentro de un área limitada, como una residencia o una escuela.

MitM: Hombre en el ataque de Medio. Un ataque en el que el atacante se coloca en secreto entre dos o más partes que se están comunicando. El atacante puede intentar alterar las comunicaciones o recopilar datos.

SIEM: Información de seguridad y gestión de eventos. Un software o un dispositivo que es capaz de analizar y correlacionar grandes cantidades de eventos de seguridad casi en tiempo real. Los productos SIEM maduros también son capaces de generar alertas y visualizar datos relacionados con la seguridad.

SOAR: Ayuda a organizar, ejecutar y automatizar tareas entre varias personas y herramientas de seguridad. Además, estandariza el análisis de incidentes y los procedimientos de respuesta.

Docker: Una plataforma abierta para desarrollar, enviar y ejecutar aplicaciones que permite empaquetar proyectos con todas sus dependencias únicamente necesarias en un simple binario, de forma aislada al resto de aplicaciones que puedan convivir en una misma máquina.

Docker-Compose: Es una herramienta para definir y ejecutar aplicaciones Docker multicontenedor que permite simplificar el uso de Docker a partir de archivos YAML, de esta manera se simplifica la creación de contendores que se relacionen entre sí, conectarlos, habilitar puertos, volumenes, etc.

Apache Cassandra: Un software de base de datos de denominación NoSQL que permite el manejo masivo de datos, de una manera escalable, tiene capacidad lineal de escalar. Posee conceptos muy innovadores como el soporte multi-data center o la comunicación P2P entre nodos.

11. Anexo A

Catálogo de Integraciones con feeds para inteligencia de la amenaza

Las integraciones vía API de SOAR con las diferentes fuentes de información permite orquestar inteligencia de la amenaza; con el fin de automatizar tareas de análisis.

A continuación, se enumeran algunas de las integraciones probadas:

ThreatIntell-Feeds	Necesita suscripción
DShield	No
UrlScan	No
URLHaus	No
MISP	No
AbuseIPDB	No
AlienvaultOTX	No
SinkDB	No
Shodan	Sí
NERD	Sí
VirusTotal	Sí
PassiveTotal	Sí

12. Anexo B

Tags

El objetivo de los tags es agrupar los casos por tipo, ir obteniendo estadísticas y utilizar el lenguaje común para la elaboración de reportes.

MITRE ATT&CK - Tácticas:

TA0001: ACCESO INICIAL

TA0002: EJECUCIÓN

TA0003: PERSISTENCIA

TA0004: ESCALAMIENTO DE PRIVILEGIOS

TA0005: EVASIÓN DE DEFENSAS

TA0006: ACCESO A CREDENCIALES

TA0007: DESCUBRIMIENTO

TA0008: MOVIMIENTO LATERAL

TA0009: RECOLECCIÓN

TA0010: EXFILTRACIÓN

TA0011: COMANDO Y CONTROL

TA0012: IMPACTO

Otras:

MALWARE: Código malicioso

HACK: Hacking, defacement, acceso no autorizado

DDOS: Denegación de servicio (Distribuido o no)

PHISHING: Phishing

ANOMALIAS: Anomalías

FORENSE: Análisis forense

FUGA: Fuga de Información

VULNS: Vulnerabilidad expuesta

AMENAZA: Aumento de la amenaza

HUNTING: Tareas de Hunting

13. Anexo C

Matriz MITRE ATT&CK

Última Edición - octubre 2020.