

SOC (Security Operations Center)

Módulo 5 – Herramientas



SECURITY ORQUESTATION, AUTOMATION AND RESPONSE - EJERCICIOS

Sheila Fernández Cisneros – 12/07/2024



Tarea 1:

El SOAR es una herramienta que nos permite gestionar y responder a incidentes de seguridad de una manera más eficiente y automatizada. Imagina que nuestro SOAR tiene ya configurados los conectores para recibir los datos de nuestro SIEM y trabajar con ellos.

Para automatizar lo mejor posible las alertas que nos llegan, el encargado del proyecto propone realizar como primer paso un enriquecimiento de las entidades del incidente (ver cuáles pueden ser maliciosas en base a feeds de inteligencia). Sin embargo, no tenemos aún hechas integraciones con plataformas de terceros. A continuación, se presentan una serie de opciones de plataformas de terceros disponibles en el Marketplace, ¿cuál/cuáles de estas crees que pueden ser útiles para lo que se pide? Explica el motivo.

The screenshot shows a grid of 12 marketplace items, each with a title, icon, version, certification status, and a brief description. The items are arranged in three rows of four:

- AbuseIPDB** (v3.0) - Certified: Leverage the AbuseIPDB threat intelligence API with this integration.
- Active Directory** (v34.0) - Certified: Microsoft Active Directory Integration facilitates the centralized management and synchronization of Windows user accounts with Security Center's administrator and cardholder accounts.
- AirTable** (v14.0) - Certified: Airtable can store information in a spreadsheet that's visually appealing and easy-to-use, but it's also powerful enough to act as a database that businesses can use for customer-relationshi...
- Alexa** (v5.0) - Certified: The Alexa Web Information Service (AWIS) offers a platform for creating innovative Web solutions and services based on Alexa's vast information about web sites.
- Microsoft Intune** (v2.0) - Certified: Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile...
- Microsoft Teams** (v20.0) - Certified: Microsoft Teams is a platform that combines workplace chat, meetings, notes, and attachments Quick Guide: you must first register your app at Microsoft App Registration Portal. Configur...
- mimecast** - Certified: Mimecast Cloud cybersecurity services for email, data, and web provides your organization with archiving and continuity needed to prevent compromise.
- MISP** (v29.0) - Certified: MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threat about cyber security incidents.
- unshorten.me** - Certified: Unshorten.me is a free service to Un-Shorten the URLs created by URL shortening services. Unshorten.me can un-shorten URLs created by different services like goo.gl (Google), fb.me...
- urlscan.io** - Certified: urlscan.io is a service to scan and analyse websites.
- URLVoid** (v10.0) - Certified: URLVoid is a service that analyzes a website through multiple blacklist engines and online reputation tools to facilitate the detection of fraudulent and malicious websites.
- Vanilla** - Vanilla provides a modern customer community platform to organizations who want to improve customer service, increase advocacy, and strengthen brand loyalty.
- virusTotal** (v35.0) - Certified: VirusTotal is a service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content. VirusTotal aggregates many antivirus products and online scan engines t...

Para el enriquecimiento de las entidades del incidente y la verificación de su potencial maliciosidad utilizando feeds de inteligencia, varias de las plataformas de terceros disponibles en el Marketplace pueden ser especialmente útiles.

- **AbuseIPDB**

- **Motivo:** Esta plataforma es especialmente útil para verificar la reputación de direcciones IP. Si un incidente involucra una IP sospechosa, AbuseIPDB puede proporcionar información sobre si esa IP ha sido reportada por actividades maliciosas, como spam o ataques de hacking.



- **Mimecast**

- **Motivo:** Mimecast proporciona servicios de seguridad para correos electrónicos. Si el incidente involucra un correo electrónico sospechoso, Mimecast puede ayudar a verificar la seguridad del correo y detectar posibles amenazas de phishing o malware adjunto.

- **MISP**

- **Motivo:** MISP es una herramienta de código abierto que, como su nombre indica, permite analizar, gestionar y compartir información relacionada con muestras de malware. Es una plataforma compartida de inteligencia de amenazas que puede ser muy útil para obtener información detallada sobre indicadores de compromiso.

- **urlscan.io**

- **Motivo:** Esta plataforma permite analizar y escanear URLs para determinar si son seguras o maliciosas. Es especialmente útil si el incidente involucra enlaces sospechosos, permitiendo verificar si esos enlaces están asociados con sitios fraudulentos o con malware.

- **URLVoid**

- **Motivo:** Similar a urlscan.io, URLVoid permite escanear un sitio web con múltiples motores y herramientas de reputación en línea. Esto facilita la detección de sitios web fraudulentos y maliciosos.

- **VirusTotal**

- **Motivo:** VirusTotal es una herramienta esencial que permite verificar archivos, URLs, direcciones IP y dominios contra múltiples motores antivirus y herramientas de análisis de malware. Ofrece inteligencia de amenazas a través de su servicio VirusTotal Intelligence, incluyendo búsquedas avanzadas, estadísticas detalladas y tendencias de malware. También proporciona APIs para la integración en otras herramientas de seguridad y feeds de amenazas en tiempo real, lo que permite enriquecer incidentes y mejorar la capacidad de respuesta ante amenazas. Ofrece una vasta base de datos de indicadores de compromiso con la cual identificar rápidamente si una entidad es maliciosa.

Tarea 2:

Tenemos finalmente una integración hecha para enriquecer entidades que nos ofrece las siguientes acciones:



Add Comment To Entity	Get Related Domains
Add Vote To Entity	Get Related Hashes
Download File	Get Related IPs
Enrich Hash	Get Related URLs
Enrich IOC	Ping
Enrich IP	Search Entity Graphs
Enrich URL	Search Graphs
Get Domain Details	Search IOCs
Get Graph Details	Submit File

Imagina que te llega un incidente de seguridad relacionado con la detección de un archivo binario malicioso en un equipo del cliente.

- ¿Cuál/es de estas acciones deberíamos usar para enriquecer correctamente esta alerta?

Para enriquecer correctamente la alerta relacionada con la detección de un archivo binario malicioso en un equipo del cliente, se podrían utilizar las siguientes acciones:

1. **Enrich Hash:** Esta acción se podría usar para obtener información adicional sobre el hash del archivo malicioso. Esto puede proporcionar datos sobre si el archivo ha sido detectado anteriormente y su reputación en diversas bases de datos de malware.
2. **Get Related Hashes:** Esta acción puede ayudar a identificar otros hashes relacionados con el archivo malicioso, lo cual puede ser útil para detectar variantes del mismo malware.
3. **Enrich IOC:** Esta acción se puede usar para obtener información adicional sobre el Indicador de Compromiso (IOC) relacionado con el archivo binario malicioso. Esto puede incluir detalles sobre la naturaleza del IOC y su contexto en campañas de ataque conocidas.



4. **Submit File:** Si tienes el archivo binario, puedes enviar el archivo para análisis adicional. Esto puede proporcionar información detallada sobre el comportamiento del archivo y su clasificación.

Los pasos a seguir podrían ser los siguientes:

1. **Enrich Hash:** Primero, obtener información sobre el hash del archivo.
2. **Get Related Hashes:** Investigar si hay otros hashes relacionados que puedan indicar variantes del malware.
3. **Enrich IOC:** Ampliar la información sobre cualquier IOC asociado con el archivo malicioso.
4. **Submit File:** Si es posible y seguro, enviar el archivo para un análisis más detallado.

Estas acciones proporcionarán una visión más completa del archivo malicioso y te ayudarán a tomar decisiones informadas sobre cómo manejar el incidente.

- **¿Crees que hay alguna acción más aparte de las aportadas por esta integración que sería buena incluir para enriquecer por completo las entidades de la alerta?**

A parte de las aportadas por el ejercicio, se podría considerar las siguientes acciones adicionales de inteligencia de amenazas.

- **Sandbox Analysis – Falcon Sandbox Analyze:** Ejecutar el archivo en un entorno seguro para observar su comportamiento.
- **Threat Intelligence Feeds – Xforce Get Hash Info:** Consultar fuentes de inteligencia de amenazas.
- **Revisión de Análisis Previos:** Verificar análisis previos en plataformas como VirusTotal.
- **Digital Signature Verification:** Analizar la firma digital del archivo.
- **Malware Databases:** Consultar bases de datos de malware.
- **Memory Analysis:** Realizar análisis forense de la memoria del sistema.
- **Disk Forensics:** Analizar el disco del sistema para buscar artefactos relacionados.
- **Behavioral Analysis Tools:** Utilizar herramientas para detectar comportamiento anómalo.

Estas acciones ayudarán a enriquecer por completo las entidades de la alerta, proporcionando un análisis exhaustivo y detallado de la amenaza detectada.

Tarea 3:



Uno de los problemas que tienen a menudo los analistas de seguridad es una gran volumetría de incidentes a los que hacer frente.

Una utilidad que ofrece el SOAR para hacer la respuesta a esta generación de alertas más eficiente es la de relacionar los nuevos casos generados con casos antiguos con los que puede guardar una estrecha relación, de manera que, si el nuevo caso presenta las mismas entidades que uno antiguo, se puede descartar y cerrar automáticamente.

Para ello el SOAR de Google Chronicle ofrece un bloque específico para playbooks llamado: “Get Similar Cases”. Este bloque por dentro tiene los siguientes parámetros:

Imagina que quieres que los casos de una determinada regla sean cerrados automáticamente si las IP externas coinciden con los de un caso antiguo (de la misma regla).

- **¿Cómo rellenarías los parámetros de esta acción?**

Para configurar el bloque “Get Similar Cases” en el SOAR de Google Chronicle para que los casos de una determinada regla sean cerrados automáticamente si las IP externas coinciden con los de un caso antiguo (de la misma regla), podemos llenar los parámetros de la siguiente manera:

1. **Choose Instance:** Seleccionar la instancia correspondiente que en este caso, parece que es “Shared_Siemplify_1”.



2. **Entities:** Seleccionar la opción “External IP” si está disponible o similar.
3. **Rule Generator:** Marcar esta opción y proporcionar el nombre de la regla específica que estás utilizando para generar los casos. Esto asegura que solo se consideren casos generados por la misma regla.
4. **Port:** Dejar esta opción sin marcar, ya que no tenemos esta información.
5. **Category Outcome:** Dejar esta opción sin marcar, ya que no es relevante para esta configuración.
6. **Entity Identifier:** Marcar esta opción para indicar que se deben utilizar identificadores de entidades (IP externas) para la comparación.
7. **Days Back:** Proporcionar el número de días atrás que deseas considerar para buscar casos similares. Esto depende de cuánto tiempo deseas retroceder para encontrar casos similares.
8. **Include Open Cases:** Marcar esta opción para incluir casos abiertos en la búsqueda.
9. **Include Closed Cases:** Marcar esta opción para incluir casos cerrados en la búsqueda.

- **¿Qué número crees que sería conveniente poner en Days Back?**

Un período de 30 días podría ser un buen punto de partida para configurar el parámetro **Days Back**. Este período suele ser suficiente para identificar patrones recurrentes de incidentes.

Aunque 30 días es un estándar común, la configuración ideal dependerá de la naturaleza y el volumen de alertas que recibe una organización. Algunas organizaciones pueden necesitar un período más corto o más largo basado en sus circunstancias específicas.

La frecuencia de alertas varía enormemente entre diferentes SOCs. Algunos SOCs manejan un alto volumen de alertas diariamente, mientras que otros reciben muy pocas.

Incluso si el volumen de alertas diarias es diferente, la frecuencia de recurrencia de alertas similares (por ejemplo, una vez a la semana) puede ser un factor común. Esto significa que, en este caso, el mismo período de días podría funcionar bien para ambos tipos de SOCs.

Es importante considerar la carga de trabajo y la capacidad de analizar grandes cantidades de datos. Un período más largo podría resultar en más datos a revisar, lo que puede ser manejable o no, dependiendo de los recursos y la infraestructura del SOC.

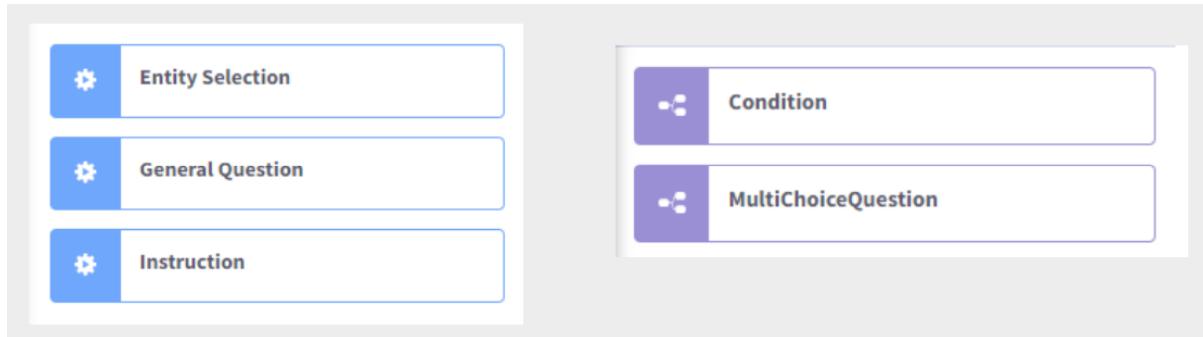
Por tanto, se podría decir que la elección de un período de 30 días para el parámetro **Days Back** es un buen punto de partida, pero debe ajustarse según las características específicas de la organización, incluyendo la frecuencia de alertas, la recurrencia de incidentes similares y la capacidad de análisis de datos del SOC.

Tarea 4:



Una vez tenemos hecho nuestro bloque para obtener los casos similares al anterior, obtendremos como salida un array que guardará el identificador de los casos similares al actual, tras ver que coinciden las IP externas. Si no hay ninguno que coincida, el array estará vacío.

- ¿Cuál de estas acciones crees que necesitaremos para continuar con el playbook?



Para continuar con el playbook después de obtener el array de casos similares, se continuará el playbook con la opción “**Condition**”.

La acción “Condition” se utilizará para evaluar si el array obtenido tiene elementos (es decir, si se encontraron casos similares) o está vacío.

Esta condición permitirá bifurcar el flujo del playbook dependiendo de si se encontraron casos similares o no.

- **Si el array no está vacío (es decir, se encontraron casos similares):** Se puede proceder a cerrar el caso actual o tomar otras acciones automatizadas basadas en la similitud de los casos.
 - **Si el array está vacío (es decir, no se encontraron casos similares):** Se puede continuar con el flujo normal de análisis y respuesta al incidente, posiblemente incluyendo más enriquecimiento de datos y análisis manual.
- **En caso de que nuestra acción de casos similares obtenga un array que no esté vacío, ¿con qué acción/acciones deberíamos de cerrar el playbook? A continuación se presentan una serie de opciones:**



Add Entity Insight	Close Case
Add General Insight	Create Entity
Add Tags To Similar Cases	Create Or Update Entity Properties
Add to Custom List	Get Connector Context Value
Assign Case	Get Scope Context Value
Attach Playbook to Alert	Get Similar Cases
Case Comment	Instruction
Case Tag	Investigation Details - Custom Action
Change Alert Priority	Is In Custom List
Change Case Stage	Mark As Important

En caso de que nuestra acción de obtener casos similares devuelva un array que no esté vacío, la acción que haríamos para cerrar el playbook sería “**Close Case**”. Esta acción cerrará el caso actual si se encuentran casos similares, evitando así duplicar esfuerzos y centralizando el manejo del incidente en el caso ya existente.

Pero si antes de cerrar el caso, se desea obtener los casos similares encontrados con **Get Similar Cases**, se podría añadir esta acción al flujo y luego cerrar el caso.

Tarea 5:

Se desea automatizar el proceso de enriquecimiento de direcciones IP, en el SOAR de chronicle, detectadas en incidentes de seguridad. El playbook se debe activar automáticamente al detectar una nueva IP relacionada con un incidente, consultar varias fuentes de información para obtener datos relevantes sobre la IP, procesar estos datos y tomar decisiones basadas en la reputación de la IP. Finalmente, debe generar alertas y reportes, e integrar los resultados con el sistema de SIEM/SOAR.



A continuación, se muestran diferentes bloques de chronicle que pueden servir para crear este playbook. Conéctelos de la manera que crea más apropiada para conseguir el propósito del enunciado, para ello puede utilizar una app web de dibujo de diagramas como draw.io.

Nota 1: los bloques indicados abajo son una guía y los fundamentales, puede proponer una solución con algún bloque más que cumpla con lo que se pide en el enunciado.

Nota 2: puede repetir los bloques si lo cree necesario.

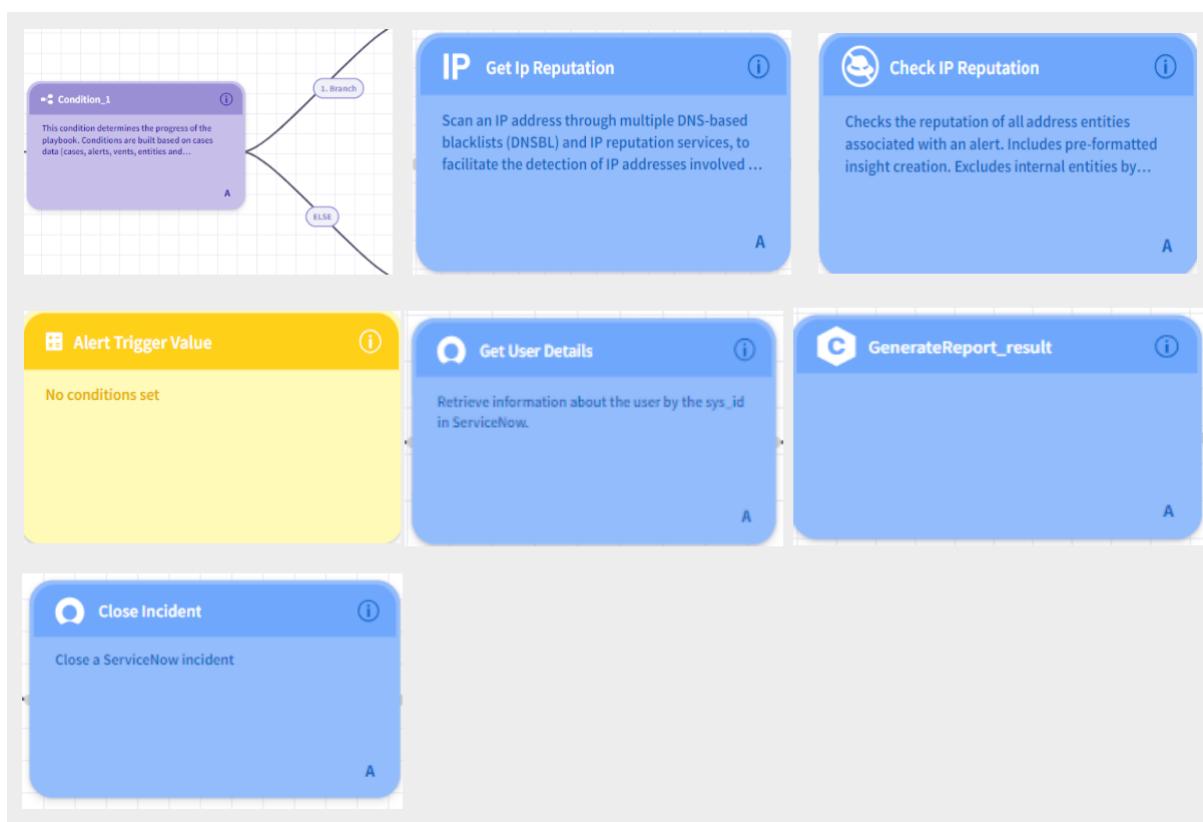
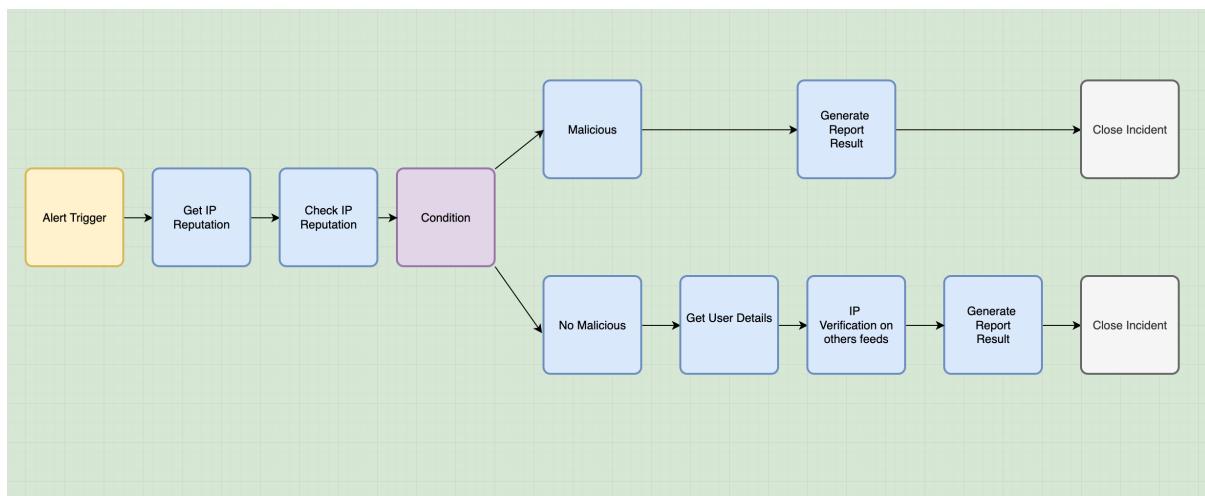


Diagrama del Playbook:



Flujo del Playbook:

1. **Alert Trigger:** Este bloque se activa automáticamente al detectar una nueva IP relacionada con un incidente.
2. **Get IP Reputation:** Consulta varias fuentes para obtener información sobre la reputación de la IP.
3. **Check IP Reputation:** Verifica la reputación de la IP utilizando múltiples servicios y excluye las IPs internas.
4. **Condition:** Evalúa si la IP es maliciosa o no basándose en la reputación obtenida.
 - o **Malicious:** Si la IP es maliciosa, se genera un reporte y se cierra el incidente.
 - o **No Malicious:** Si la IP no es maliciosa, se realizan pasos adicionales antes de cerrar el incidente.
5. **Para IPs Maliciosas:**
 - o **Generate Report Result:** Genera un reporte con los datos obtenidos sobre la IP.
 - o **Close Incident:** Cierra el incidente después de generar el reporte.
6. **Para IPs No Maliciosas:**
 - o **Get User Details:** Obtiene información adicional sobre el usuario asociado, si es necesario.
 - o **IP Verification on Other Feeds:** Verifica la IP en otras fuentes de inteligencia de amenazas para asegurar la reputación.
 - o **Generate Report Result:** Genera un reporte con los datos obtenidos.
 - o **Close Incident:** Cierra el incidente después de verificar la IP y generar el reporte.

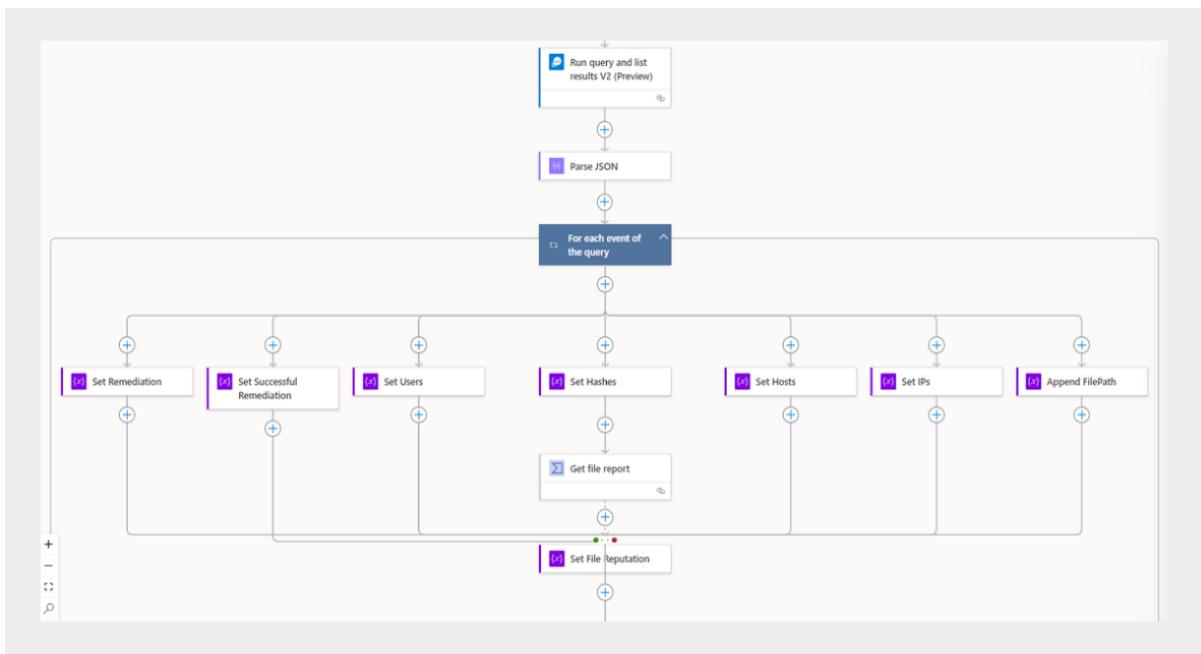


Tarea 6:

Una posible alternativa de automatización a los SOAR es una herramienta utilizada por Microsoft Sentinel conocida como “Logic Apps”.

Esta herramienta hace uso de playbooks para tratar las alertas de manera similar a como se hace en un SOAR. Además, puede usarse en conjunto con el SIEM de Sentinel, obteniendo los datos de cada incidencia y creando una respuesta automatizada.

En la siguiente imagen vemos un ejemplo de un bucle realizado en un playbook de la Logic App:



En este caso la acción ‘Parse JSON’ es la que obtiene todos los datos de la incidencia, los cuales se guardan posteriormente en variables para tratarlos.

- ¿Por qué hay un bucle For each y cuál crees que es su utilidad?

El **for each event of the query**, tal y como su nombre indica, iterará sobre los elementos de la lista obtenida por la consulta previa, de manera que cada elemento se procese de forma individual. De este modo, cada evento será analizado de forma separada, aplicándole las acciones específicas requeridas dependiendo del tipo de evento que sea.

- ¿Piensas que en este playbook se realiza un enriquecimiento tal y como el descrito en los ejercicios previos? En caso afirmativo, ¿qué entidad o entidades se están enriqueciendo?

Si. El enriquecimiento se ha realizado de las siguientes entidades:

- **Hashes:** Se está enriqueciendo la entidad “hashes” al obtener un reporte detallado del archivo y establecer su reputación.



- **IPs:** Se está identificando y estableciendo las direcciones IP relacionadas.
- **Hosts:** Se está identificando y estableciendo los hosts relacionados.
- **Users:** Se está identificando y estableciendo los usuarios relacionados.
- **FilePath:** Se está agregando la ruta del archivo relacionado con el evento.

Tarea 7:

Como ejercicio final, se propone pensar cuáles de estos incidentes de seguridad crees que sería posible automatizar de manera completa, es decir, recolección, trata de datos y resolución completa dentro del playbook, o cuáles deberían ser tratados por el analista antes de resolverse.

En caso de resolverlos de manera automática, indica también el tipo de resolución que les darías, si le enviarías un mensaje al cliente o los cerrarías directamente:

1. Un equipo ha tenido una conexión con un IoC (Indicator of Compromise) al navegar por la web.
2. Ataques de fuerza bruta contra un host de la organización.
3. Incidente de severidad media detectado por un EDR, como detección de un proceso irreconocido en el equipo.
4. Incidente de severidad alta/crítica detectado por un EDR, como la detección de un script malicioso, bloqueado por el EDR.
5. Incidente de severidad alta/crítica detectado por un EDR, como la detección de un script malicioso, pero no bloqueado por el EDR.
6. Ejecución de XSS (Cross Site Scripting) con petición HTTP exitosa.
7. Inicio de sesión a una cuenta de la organización desde países diferentes en un periodo muy corto de tiempo.
8. Operación sospechosa realizada en una aplicación de Office por un miembro de la organización.

Discusión de la automatización de los casos.

1. Un equipo ha tenido una conexión con un IoC (Indicator of Compromise) al navegar por la web.
 - **Resolución Automática:** Sí.
 - **Acción Automatizada:** Bloquear la URL/IoC, enviar un mensaje al cliente y cerrar el caso.



- **Justificación:** Las conexiones a IoCs conocidos pueden ser tratadas de manera automática bloqueando el acceso a esas URL y notificando al cliente sobre la acción tomada.

2. Ataques de fuerza bruta contra un host de la organización.

- **Resolución Automática:** Parcial.
- **Acción Automatizada:** Bloquear la IP atacante.
- **Intervención del Analista:** Revisar logs y patrones de ataque para asegurar que no hay una brecha mayor, realizar un análisis de las medidas de defensa, y ajustar las políticas de seguridad si es necesario.
- **Justificación:** Aunque se puede automatizar el bloqueo de la IP atacante, la naturaleza del ataque puede requerir una investigación más profunda para asegurarse de que no hay una brecha mayor.

3. Incidente de severidad media detectado por un EDR, como detección de un proceso irreconocido en el equipo.

- **Resolución Automática:** No.
- **Acción del Analista:** Analizar el proceso irreconocido para determinar si es benigno o malicioso, realizar una búsqueda de amenazas similares en otros sistemas, y ajustar las configuraciones del EDR para futuras detecciones.
- **Justificación:** Los procesos irreconocidos pueden ser benignos o maliciosos, y se necesita la intervención de un analista para determinar la naturaleza exacta del proceso.

4. Incidente de severidad alta/crítica detectado por un EDR, como la detección de un script malicioso, bloqueado por el EDR.

- **Resolución Automática:** No.
- **Acción del Analista:** Analizar el script bloqueado y su impacto potencial, revisar otros sistemas para detectar actividad similar, y actualizar las defensas para prevenir futuros incidentes.
- **Justificación:** Una alerta alta/crítica requiere de intervención inmediata y de un analista para analizar el script, mitigar daños y escalar el caso si es necesario aunque haya sido bloqueado por el EDR.

5. Incidente de severidad alta/crítica detectado por un EDR, como la detección de un script malicioso, pero no bloqueado por el EDR.

- **Resolución Automática:** No.
- **Acción del Analista:** Contener la amenaza de inmediato, analizar el script no bloqueado y su impacto, notificar a los equipos de respuesta para coordinación, y realizar un análisis forense para entender la penetración.



- **Justificación:** La detección de un script malicioso no bloqueado requiere una respuesta inmediata y detallada por parte de un analista para contener la amenaza y mitigar el riesgo.

6. Ejecución de XSS (Cross Site Scripting) con petición HTTP exitosa.

- **Resolución Automática:** No.
- **Acción del Analista:** Revisar los logs del servidor para determinar el alcance del ataque, identificar y neutralizar el código inyectado, y parchear la vulnerabilidad en la aplicación web.
- **Justificación:** Los ataques XSS pueden tener consecuencias graves y es necesario que un analista investigue el alcance del ataque y tome medidas correctivas.

7. Inicio de sesión a una cuenta de la organización desde países diferentes en un periodo muy corto de tiempo.

- **Resolución Automática:** Parcial.
- **Acción Automatizada:** Bloquear temporalmente la cuenta y notificar al usuario afectado.
- **Intervención del Analista:** Verificar la autenticidad de los inicios de sesión, investigar posibles compromisos de credenciales, y asesorar al usuario sobre pasos de seguridad adicionales.
- **Justificación:** Este comportamiento puede indicar un compromiso de la cuenta y requiere la intervención de un analista para confirmar y resolver el problema.

8. Operación sospechosa realizada en una aplicación de Office por un miembro de la organización.

- **Resolución Automática:** Parcial.
- **Acción Automatizada:** Detectar la operación sospechosa y generar una alerta inicial.
- **Intervención del Analista:** Analizar la operación sospechosa para determinar su naturaleza, realizar una auditoría de las actividades recientes del usuario, y, si es necesario, implementar medidas correctivas y de formación.
- **Justificación:** Las operaciones sospechosas en aplicaciones de Office pueden ser indicativas de un compromiso interno. Se puede automatizar la detección y la generación de una alerta inicial, pero un analista debe investigar la actividad para determinar si se trata de una amenaza real y tomar las acciones correctivas necesarias.