FORTINET
NSE Training Institute

NSE 2 SOAR Scripts—Spanish Version

¡Hola! En esta clase, veremos de qué se trata la orquestación de seguridad, automatización y respuesta o SOAR. En la industria de la seguridad, se suele hablar mucho de la SOAR. Por eso, no solo es importante saber qué es, sino que también hay que estar al tanto de los retos y los problemas que aborda la SOAR. Pero, antes de eso, veamos los aspectos básicos.

¿Qué es la SOAR? La SOAR unifica todas las demás herramientas de la pila de seguridad en flujos de trabajo definidos, que pueden ejecutarse automáticamente. Es decir, la SOAR le permite a su equipo de seguridad obtener una mayor eficiencia al automatizar los procesos repetitivos manuales.

Hoy en día, la automatización es muy importante en el mundo de la seguridad, ya que los equipos están desbordados. A medida que se diseñan nuevas herramientas para hacer frente al dinámico panorama de amenazas, los analistas que utilizan dichas herramientas deben alternar entre una y otra para llevar a cabo sus tareas diarias.

Una tarea muy frecuente en el día a día es la respuesta ante alertas. Cuantas más herramientas de seguridad hay, más alertas se presentan. Para ocuparse de ellas, existe una serie de procesos manuales y de cambios de contexto; es decir, se cambia de una herramienta a otra. Al haber más alertas diarias a las que responder, se puede dedicar menos tiempo a cada una, lo que aumenta la probabilidad de cometer errores. La degradación del rendimiento como resultado de una avalancha de alertas se denomina "**fatiga de alertas**".

Una forma obvia de reducir la fatiga de alertas consiste simplemente en contratar más analistas. Sin embargo, como los conocimientos de ciberseguridad no abundan, lo cierto es que no hay suficientes analistas calificados. Entonces, si contratar más analistas no es viable, ¿cómo se puede eliminar la fatiga de alertas? Es fácil: con la SOAR.

Como se mencionó antes, la SOAR unifica las herramientas de la pila de seguridad. Al extraer datos de todas estas fuentes, la SOAR reduce los cambios de contexto con los que tienen que lidiar los analistas. Así, los analistas pueden ejecutar los procesos de investigación usuales directamente desde la interfaz de origen. Además, estos procesos pueden traducirse de forma manual o automática a un manual de estrategias, en el que se enumeran los pasos como en el diagrama de flujo. Estos pasos pueden repetirse bajo demanda. El manual garantiza que se sigan todos los pasos del procedimiento de operaciones estándar. También proporciona datos exactos acerca de lo que se hizo y de cuándo y quién lo hizo. Esta capacidad se llama "orquestación y automatización".

Otra capacidad fundamental de la SOAR es la investigación. Cuando aparece una alerta sospechosa, los equipos pueden realizar tareas de investigación, como recurrir a fuentes de información sobre amenazas para verificar la reputación o consultar en un sistema de gestión de la información de seguridad o SIM, para conocer eventos relacionados desde dentro de la plataforma de SOAR. La información recopilada durante la investigación permitirá determinar los pasos necesarios para la mitigación. Luego, como la SOAR es una mesa de trabajo que unifica todas las herramientas de seguridad, también es posible llevar a cabo los pasos para la mitigación desde la plataforma de SOAR. Por ejemplo, a través de esta plataforma se puede bloquear el tráfico proveniente de una dirección IP maliciosa mediante su *firewall* o eliminar un correo electrónico de suplantación de identidad (*phishing*) desde el servidor de correo electrónico. Al incorporar procesos estándares en los manuales de estrategias, es posible eliminar los procesos repetitivos manuales, que insumen mucho tiempo, mediante la automatización a la velocidad de la máquina. La automatización libera a los analistas y les permite dedicar más tiempo a investigar alertas críticas.

Cuando implementa la SOAR en su ecosistema, no solo centraliza los procesos de respuesta ante incidentes, sino que optimiza toda una operación. Como resultado de la optimización, se obtienen respuestas mejoradas a la velocidad de la máquina, lo que permite a los equipos potenciar la colaboración y administrar mejor la incesante ola de alertas. Esto es así porque, mediante la SOAR, los usuarios pueden asignar alertas a distintos analistas o equipos en diferentes etapas del proceso de respuesta. A su vez, los usuarios asignados pueden agregar información a la alerta a medida que trabajan en ella, de modo que, más adelante, quienes se refieran a dicha alerta tendrán un contexto adicional para la investigación.

hora detallaremos qué son los manuales de estrategias. Los equipos utilizan los manuales de estrategias, a veces llamados "flujos de trabajo", para responder a todas las alertas o los incidentes de la misma manera. Los manuales de estrategias trabajan en conjunto con los equipos de seguridad y siguen los mismos pasos que normalmente seguiría un analista para responder a un incidente. Los manuales ejecutan las tareas repetitivas, como compilar datos en un informe o enviar correos electrónicos, y pueden pausarse cuando se requiere supervisión humana, como al implementar un bloqueo en el firewall. Los manuales de estrategias son la clave de la capacidad de automatización de la SOAR, ya que permiten a los equipos ofrecer respuestas más veloces y unificadas y, al mismo tiempo, mantener el proceso bajo el control de una persona. En definitiva, al utilizar un manual de estrategias se pueden obtener menores probabilidades de error y una carga de trabajo reducida para los analistas.

Las investigaciones sobre el correo suplantación de identidad son uno de los casos de uso más frecuentes de la SOAR entre los clientes. Sin esta plataforma, los analistas pasarían mucho tiempo investigando el remitente de un correo de suplantación de identidad y los indicadores clave ubicados en el encabezado o en el cuerpo del mensaje. Este tipo de investigaciones implica destinar mucho tiempo a ingresar dominios y URL en una plataforma de información sobre amenazas. Si los analistas determinan que un correo electrónico es dañino, deben dedicar aún más tiempo a investigar el servidor de correo electrónico y consultar el sistema de SIM, a determinar quién recibió el correo y quién lo abrió, a eliminarlo, etcétera. Con un manual de estrategias para investigar los correos de *phishing*, los pasos iniciales de la investigación se siguen automáticamente, apenas se informa acerca del correo. De este modo, el analista solo recibe alertas sobre los correos que son sospechosos según el manual de estrategias. Cuando el analista confirma que un correo electrónico informado requiere otra acción, el manual de estrategias puede realizar consultas adicionales en el sistema de SIM, eliminar el correo de la bandeja de entrada de todos los usuarios, enviar un correo que informe a todos los usuarios las medidas tomadas y brindar consejos útiles sobre qué hacer en caso de recibir correos similares en el futuro.

Hasta aquí, una introducción a la SOAR: qué es, qué problemas resuelve y qué beneficios ofrece. El producto de SOAR de Fortinet se llama FortiSOAR™ e incluye todas estas características y más.

Gracias por su tiempo. No olvide responder las preguntas.