Definición de los conceptos de SIEM y SOAR

La protección del patrimonio digital, los recursos, los activos y los datos de una organización ante las infracciones y los ataques a la seguridad es un reto continuo y creciente. En el mundo empresarial hay multitud de trabajadores remotos, lo que crea vulnerabilidades de seguridad que los cibercriminales pueden aprovechar.

Contar con un conjunto de herramientas resistentes y eficaces estándar del sector puede ayudar a mitigar y evitar estos ataques. La administración de eventos e información de seguridad (SIEM) y la respuesta automatizada de orquestación de seguridad (SOAR) proporcionan conclusiones y automatización de seguridad que pueden mejorar la visibilidad de las amenazas y la respuesta a ellas en una organización.

¿Qué es la Administración de eventos e información de seguridad (SIEM)?

Un sistema SIEM es una herramienta que una organización utiliza para recopilar datos de todo el patrimonio, incluida la infraestructura, el software y los recursos. Realiza análisis, busca correlaciones o anomalías y genera alertas e incidencias.

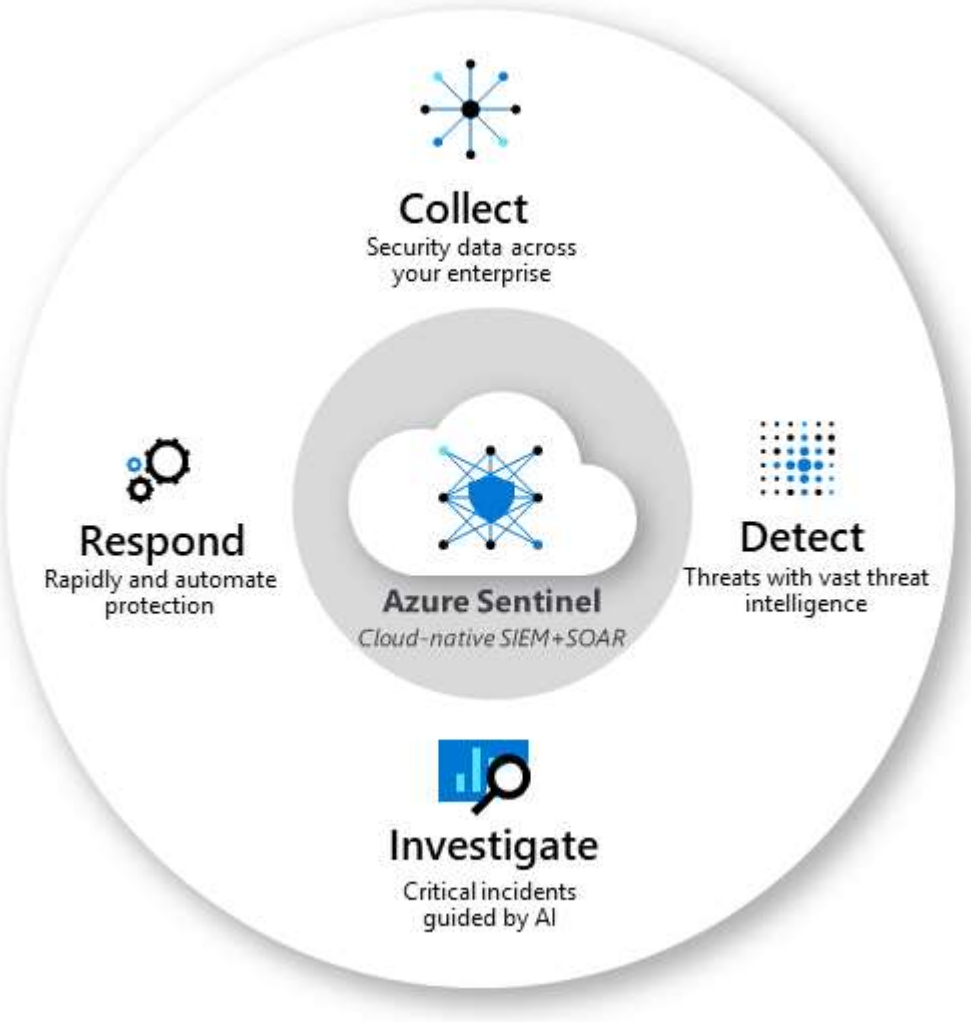
¿Qué es la respuesta automatizada de orquestación de seguridad (SOAR)?

Un sistema SOAR recibe alertas de muchos orígenes, como un sistema SIEM. El sistema SOAR desencadena entonces flujos de trabajo y procesos automatizados basados en acciones para ejecutar tareas de seguridad que mitiguen el problema.

A fin de proporcionar un enfoque completo para la seguridad, una organización debe usar una solución que adopte o combine las funcionalidades SIEM y SOAR.

Descripción de cómo Microsoft Sentinel proporciona administración contra amenazas integrada

La administración efectiva del perímetro de seguridad de red de una organización requiere la combinación adecuada de herramientas y sistemas. Microsoft Sentinel es una solución SIEM/SOAR escalable y nativa de la nube que ofrece análisis de seguridad inteligentes e inteligencia sobre amenazas en toda la empresa. Proporciona una única solución para la detección de alertas, la visibilidad de las amenazas, la búsqueda proactiva y la respuesta a las amenazas.



En este diagrama se muestra la funcionalidad de un extremo a otro de Microsoft Sentinel.

- **Recopile** datos a escala de nube de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.
- **Detecte** amenazas que antes no se abarcaban y reduzca los falsos positivos mediante un análisis y una inteligencia de amenazas sin precedentes.
- **Investigue** amenazas con inteligencia artificial (IA) y busque actividades sospechosas a gran escala, aprovechando el trabajo de ciberseguridad que ha realizado Microsoft durante décadas.
- **Responda** a los incidentes con rapidez con la orquestación y la automatización de tareas comunes de seguridad integradas.

Microsoft Sentinel ayuda a habilitar las operaciones de seguridad de un extremo a otro, en un centro de operaciones de seguridad (SOC) moderno. A continuación se enumeran algunas de las características clave de Microsoft Sentinel.

Conexión de Sentinel con los datos

Para incorporar Microsoft Sentinel, primero debe conectarse a los orígenes de seguridad. Microsoft Sentinel incluye varios conectores para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real. Se incluyen soluciones de Microsoft 365 Defender y orígenes de Microsoft 365, como Office 365, Azure AD y muchos más. Además, hay conectores integrados al amplio ecosistema de seguridad para soluciones que no son de Microsoft. También puede conectar los orígenes de datos mediante conectores de datos creados por la comunidad enumerados en el repositorio de Microsoft Sentinel en GitHub, o bien mediante los procedimientos de implementación genéricos para conectar el origen de datos a Microsoft Sentinel. Los vínculos a la información se incluyen en la sección Más información de la unidad de resumen y recursos.

Workbooks

Después de conectar los orígenes de datos a Microsoft Sentinel, puede supervisar los datos mediante la integración de Microsoft Sentinel con los libros de Azure Monitor. Verá un lienzo para el análisis de datos y la creación de informes visuales completos en Azure Portal. Mediante esta integración, Microsoft Sentinel le permite crear libros personalizados de todos los datos. También incluye plantillas de libro integradas que permiten obtener información rápidamente en los datos en cuanto se conecta con un origen de datos.

Análisis

Microsoft Sentinel usa el análisis para poner en correlación las alertas con los incidentes. Los incidentes son grupos de alertas relacionadas que, juntas, crean una posible amenaza procesable que se puede investigar y resolver. Con el análisis en Microsoft Sentinel, puede utilizar las reglas de correlación integradas tal y como están, o bien usarlas como punto de partida para crear otras propias. Microsoft Azure Sentinel también proporciona reglas de aprendizaje automático para asignar el comportamiento de red y buscar luego anomalías en los recursos. Estos análisis conectan los puntos, al combinar alertas de baja fidelidad sobre distintas entidades en posibles incidentes de seguridad de alta fidelidad.

Administración de incidentes en Microsoft Sentinel

La administración de incidentes permite administrar el ciclo de vida del incidente. Vea todas las alertas relacionadas que se agregan a un incidente. También puede evaluar las prioridades e investigar. Revise todas las entidades relacionadas del incidente y la información contextual adicional significativa para el proceso de evaluación de prioridades. Investigue las alertas y las entidades relacionadas para comprender el ámbito de la infracción. Desencadene cuadernos de estrategias en las alertas agrupadas en el incidente para resolver la amenaza detectada por la alerta. También puede realizar tareas de administración de incidentes estándar como cambiar el estado o asignar incidentes a individuos para su investigación.

Automatización y orquestación de seguridad

Puede usar Microsoft Sentinel para automatizar algunas de las operaciones de seguridad y hacer que el centro de operaciones de seguridad (SOC) sea más productivo. Microsoft Sentinel se integra con Azure Logic Apps, lo que permite crear flujos de trabajo automatizados, o cuadernos de estrategias, en respuesta a eventos. Un cuaderno de estrategias de seguridad es una colección de procedimientos que pueden ayudar a los ingenieros y analistas de SOC de todos los niveles a automatizar y simplificar las tareas y organizar una respuesta. Los cuadernos de estrategias son más adecuados para tareas únicas y repetibles, y no requieren ningún conocimiento de codificación.

Investigación

Las herramientas de investigación profunda de Microsoft Sentinel están actualmente en versión preliminar y le ayudan a conocer el ámbito de una posible amenaza de seguridad y a encontrar la causa principal. Elija una entidad en el gráfico interactivo para realizar preguntas concretas y, a continuación, explore en profundidad esa entidad y sus conexiones para llegar a la causa principal de la amenaza.

Búsqueda

Use las eficaces herramientas de búsqueda y consulta de Microsoft Sentinel, basadas en el marco MITRE (una base de datos global de tácticas y técnicas de adversarios), para buscar de forma proactiva amenazas de seguridad en todos los orígenes de datos de la organización, antes de que se desencadene una alerta. Una vez que ha descubierto qué consulta de búsqueda proporciona las conclusiones más valiosas sobre posibles ataques, también puede crear reglas de detección personalizadas basadas en la consulta y exponer esas conclusiones como alertas para los respondedores a los incidentes de seguridad.

Durante la búsqueda, puede crear marcadores de los eventos interesantes. El marcado de los eventos permite volver a ellos más tarde, compartirlos con otros usuarios y agruparlos con otros eventos correlacionados para crear un incidente de investigación convincente.

Cuaderno

Microsoft Sentinel admite cuadernos de Jupyter. Jupyter Notebook es una aplicación web de código abierto que le permite crear y compartir documentos que contienen código, ecuaciones, visualizaciones y texto narrativo dinámicos. Puede usar cuadernos de Jupyter en Microsoft Sentinel para ampliar el ámbito de lo que puede hacer con los datos de Microsoft Sentinel. Por ejemplo, realizar análisis que no están integrados en Microsoft Azure Sentinel, como algunas características de aprendizaje automático de Python, crear visualizaciones de datos que no están integradas en Microsoft Azure Sentinel, como escalas de tiempo personalizadas y árboles de proceso, o integrar orígenes de datos fuera de Microsoft Azure Sentinel, como un conjunto de datos local.

Comunidad

La comunidad Microsoft Azure Sentinel es un recurso muy eficaz para la detección y la automatización de amenazas. Los analistas de seguridad de Microsoft crean y agregan

constantemente nuevos libros, cuadernos de estrategias, consultas de búsqueda, etc., y los publican en la comunidad para que los pueda usar en el entorno. Puede descargar contenido de ejemplo del repositorio de GitHub privado de la comunidad para crear libros personalizados, consultas de búsqueda, cuadernos y cuadernos de estrategias Microsoft Azure Sentinel.

Presentación en vídeo de Microsoft Sentinel

En este vídeo, explorará algunas de las características clave disponibles en Microsoft Sentinel.

https://www.microsoft.com/es-mx/videoplayer/embed/RE4LHLR?postJsllMsg=true&autoCaptions=es-mx

Descripción de los costos de Sentinel

Microsoft Sentinel proporciona análisis de seguridad inteligente en toda la empresa. Los datos de este análisis se almacenan en un área de trabajo de Log Analytics de Azure Monitor. La facturación se basa en el volumen de datos ingeridos para su análisis en Microsoft Sentinel y almacenados en el área de trabajo de Log Analytics de Azure Monitor. Hay dos maneras de pagar por el servicio Microsoft Sentinel: reservas de capacidad y pago por uso.

- **Reservas de capacidad**: con las reservas de capacidad, se le factura una tarifa fija en función del nivel seleccionado, lo que permite un costo total predecible para Microsoft Sentinel.
- **Pago por uso**: con los precios de pago por uso, se le factura por gigabyte (GB) el volumen de datos ingeridos para el análisis en Microsoft Sentinel y almacenados en el área de trabajo de Log Analytics de Azure Monitor.

Para más información sobre los precios y una prueba gratuita de Microsoft Sentinel en un área de trabajo de Log Analytics de Azure Monitor, visite Precios de Microsoft Sentinel.