**Explore las herramientas de administración de información y eventos de seguridad (SIEM)**

Las herramientas SIEM auto alojadas requieren que las organizaciones instalen, operen y mantengan la herramienta utilizando su propia infraestructura física, como la capacidad del servidor. Estas aplicaciones son entonces gestionadas y mantenidas por el departamento de TI de la organización, en lugar de por un proveedor externo. Las herramientas SIEM auto alojadas son ideales cuando una organización debe mantener el control físico sobre los datos confidenciales.

Alternativamente, las herramientas SIEM alojadas en la nube son mantenidas gestionadas por los proveedores de SIEM, lo que las hace accesibles a través de Internet. Las herramientas SIEM alojadas en la nube son ideales para organizaciones que no quieren invertir en crear y mantener su propia infraestructura.

O bien, una organización puede optar por utilizar una combinación de herramientas SIEM auto alojadas y alojadas en la nube, lo que se conoce como una solución híbrida. Las organizaciones pueden elegir una solución SIEM híbrida para aprovechar las ventajas de la nube y, al mismo tiempo, mantener el control físico sobre los datos confidenciales.

Splunk Enterprise, Splunk Cloud y Chronicle son herramientas SIEM comunes que muchas organizaciones utilizan para ayudar a proteger sus datos y sistemas.

Comencemos hablando de Splunk.

Splunk es una plataforma de análisis de datos y Splunk Enterprise proporciona soluciones SIEM. Splunk Enterprise es una herramienta auto alojada que se utiliza para retener, analizar y buscar datos de registro de una organización para proporcionar información de seguridad y alertas en tiempo real. Splunk Cloud es una herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorizar datos de registro. Splunk Cloud es útil para organizaciones que ejecutan entornos híbridos o sólo en la nube, donde algunos o todos los servicios de la organización están en la nube.

Por último, está Chronicle de Google. Chronicle es una herramienta nativa de la nube diseñada para retener, analizar y buscar datos. Chronicle proporciona supervisión de registros, análisis de datos y recopilación de datos. Al igual que las herramientas alojadas en la nube, las herramientas nativas de la nube también son mantenidas y gestionadas en su totalidad por el proveedor. Pero las herramientas nativas de la nube están diseñadas específicamente para aprovechar al máximo las capacidades de la computación en la nube, como la disponibilidad, flexibilidad y escalabilidad.

Dado que los Agentes de amenaza mejoran con frecuencia sus estrategias para comprometer la confidencialidad, integridad y disponibilidad de sus objetivos, es importante que las organizaciones utilicen una variedad de herramientas de seguridad para ayudar a defenderse de los ataques.

Anteriormente, usted aprendió acerca de varias herramientas que son utilizadas por los miembros del equipo de Ciberseguridad para Monitorear e Identificar posibles amenazas a la Seguridad, Riesgos y Vulnerabilidades. En esta lectura, aprenderá más sobre las herramientas de ciberseguridad de código abierto y propietarias más comunes que puede utilizar como profesional de la ciberseguridad.

**Herramientas de código abierto**

Las herramientas de código abierto suelen ser de uso gratuito y pueden resultar fáciles de utilizar. El Objetivo de las herramientas de código abierto es proporcionar a los usuarios software construido por el público de forma colaborativa, lo que puede resultar en que el software sea más seguro. Además, las herramientas de código abierto permiten una mayor personalización por parte de los usuarios, lo que da lugar a una gran variedad de nuevos servicios creados a partir del mismo paquete de software como Servicio.

Los ingenieros de software crean proyectos de código abierto para mejorar el software y ponerlo a disposición de cualquiera que desee utilizarlo, siempre que se respete la licencia especificada. El código fuente de los proyectos de código abierto está fácilmente a disposición de los usuarios, así como el material de Entrenamiento que los acompaña. Tener estas fuentes fácilmente disponibles permite a los usuarios modificar y mejorar los materiales del proyecto.

**Herramientas propietarias**

Las herramientas patentadas son desarrolladas y propiedad de una persona o empresa, y los usuarios suelen pagar una cuota por su uso y Entrenamiento. Los propietarios de las herramientas propietarias son los únicos que pueden acceder al código fuente y modificarlo. Esto significa que, por lo general, los usuarios tienen que esperar a que se realicen actualizaciones del software y, en ocasiones, pueden tener que pagar una cuota por dichas actualizaciones. Por lo general, el software propietario permite a los usuarios modificar un número limitado de funciones para satisfacer las necesidades individuales y de la organización. Algunos ejemplos de herramientas propietarias son Splunk® y las herramientas SIEM de Chronicle.

**Conceptos erróneos comunes**

Existe la idea errónea de que las herramientas de código abierto son menos eficaces y su uso no es tan seguro como el de las herramientas propietarias. Sin embargo, los desarrolladores llevan años creando materiales de código abierto que se han convertido en estándares del sector. Aunque es cierto que los agentes de amenaza han intentado manipular las herramientas de código abierto, como estas herramientas son de código abierto en realidad es más difícil que las personas con intenciones maliciosas consigan causar daño. La amplia Exposición y el acceso inmediato al código fuente por parte de usuarios y profesionales bienintencionados e informados hace que sea menos probable que se produzcan problemas, porque pueden solucionarlos en cuanto se identifican.

**Ejemplos de herramientas de código abierto**

En materia de Seguridad, hay muchas herramientas en uso que son de código abierto y están comúnmente disponibles. Dos ejemplos son Linux y Suricata.

1. **Linux**

Linux es un sistema operativo de código abierto ampliamente utilizado. Le permite adaptar el sistema operativo a sus necesidades mediante una interfaz de línea de comandos. Un **sistema** operativo es la interfaz entre el hardware de la computadora y el usuario. Se utiliza para comunicarse con el hardware de una computadora y gestionar aplicaciones de software.

Existen múltiples versiones de Linux para realizar tareas específicas. Linux y su interfaz de línea de comandos se tratarán en detalle, más adelante, en el programa de certificación.

1. **Suricata**

Suricata es un software de análisis de redes y detección de amenazas de código abierto. El software de análisis de redes y detección de amenazas se utiliza para inspeccionar el Tráfico de red para identificar comportamientos sospechosos y generar registros de datos de red. El software de Detección encuentra la actividad de usuarios, computadoras o direcciones IP (Protocolo de Internet) para ayudar a descubrir posibles amenazas, riesgos o vulnerabilidades.

Suricata fue desarrollado por la Fundación Abierta para la Seguridad de la Información (OISF). La OISF se dedica a mantener el código abierto del proyecto Suricata para garantizar que sea gratuito y esté a disposición del público. Suricata se utiliza ampliamente en el sector público y privado, y se integra con muchas herramientas SIEM y otras herramientas de Seguridad. También se hablará de Suricata con más detalle más adelante en el programa.

**Puntos clave**

Las herramientas de Código abierto se utilizan ampliamente en la profesión de la ciberseguridad. A lo largo del programa de certificación, tendrá múltiples oportunidades para conocer y explorar más a fondo tanto las herramientas de código abierto como las propietarias.

**Utilice herramientas SIEM para proteger a las organizaciones**

Anteriormente, conoció las herramientas de administración de información y eventos de seguridad (SIEM) y algunos cuadros de mando SIEM. También aprendió sobre las diferentes amenazas, riesgos y vulnerabilidades que puede experimentar una organización. En esta lectura, aprenderá más sobre los datos del panel SIEM y cómo los profesionales de la ciberseguridad utilizan esos datos para identificar una posible amenaza, riesgo o vulnerabilidad.

**Splunk**

Splunk ofrece diferentes opciones de herramientas SIEM: Splunk® Enterprise y Splunk® Cloud. Ambas permiten revisar los datos de una organización en cuadros de mando. Esto ayuda a los profesionales de la seguridad a gestionar la infraestructura interna de una organización mediante la recopilación, búsqueda, supervisión y análisis de los datos de registro de múltiples fuentes para obtener una visibilidad completa de las operaciones diarias de una organización.

Revise los siguientes paneles de Splunk y sus propósitos:

1. **Panel de postura de seguridad**

El panel de Postura de seguridad está diseñado para los centros de operaciones de seguridad (SOC). Muestra las últimas 24 horas de los eventos y tendencias notables relacionados con la seguridad de una organización y permite a los profesionales de la Seguridad determinar si la infraestructura y las políticas de Seguridad están funcionando según lo diseñado. Los analistas de seguridad pueden utilizar este panel para supervisar e investigar las amenazas potenciales en tiempo real, como la actividad de red sospechosa que se origina desde una dirección IP específica.

1. **Panel de resumen ejecutivo**

El panel de resumen ejecutivo analiza y supervisa la salud general de la organización a lo largo del tiempo. Esto ayuda a los Equipos de Seguridad a mejorar las medidas de Seguridad que reducen el Riesgo. Los analistas de Seguridad podrían utilizar este tablero para proporcionar estadísticas de alto nivel a las partes interesadas, como generar un resumen de los incidentes de seguridad y las tendencias durante un período de tiempo específico.

1. **Panel de revisión de incidentes**

El cuadro de mandos de revisión de incidentes permite a los analistas identificar los patrones sospechosos que pueden producirse en caso de incidente. Ayuda resaltando los elementos de mayor riesgo que necesitan una revisión inmediata por parte de un analista. Este cuadro de mandos puede ser muy útil porque proporciona una cronología visual de los acontecimientos que conducen a un incidente.

1. **Panel de análisis de riesgos**

El tablero de análisis de riesgos ayuda a los analistas a identificar el riesgo para cada objeto de riesgo (por ejemplo, un usuario específico, una computadora o una dirección IP). Muestra los cambios en la actividad o el comportamiento relacionados con el riesgo, como el inicio de sesión de un usuario fuera de las horas normales de trabajo o un tráfico de red inusualmente alto desde una computadora específica. Un analista de Seguridad podría utilizar este panel para analizar el impacto potencial de las vulnerabilidades en los recursos críticos, lo que ayuda a los analistas a priorizar sus esfuerzos de mitigación de riesgos.

**Chronicle**

Chronicle es una herramienta SIEM de Google nativa de la nube que retiene, analiza y busca datos de registro para identificar posibles amenazas a la seguridad, riesgos y vulnerabilidades. Chronicle le permite recopilar y analizar datos de registro en función de:

* Un recurso específico
* Un nombre de dominio
* Un usuario
* Una dirección IP

Chronicle proporciona múltiples tableros que ayudan a los analistas a Monitorear los registros de una organización, crear filtros y alertas, y rastrear nombres de dominio sospechosos.

Revise los siguientes tableros de Chronicle y sus propósitos:

1. **Panel de estadísticas empresariales**

El panel de información estadística de la empresa destaca las alertas recientes. Identifica nombres de dominio sospechosos en los registros, conocidos como Indicadores de compromiso (IOC). Cada resultado se etiqueta con una puntuación de confianza para indicar la probabilidad de una amenaza. También proporciona un nivel de gravedad que indica la importancia de cada amenaza para la organización. Un analista de seguridad podría utilizar este panel para monitorizar los intentos de inicio de sesión o de acceso a los datos relacionados con un recurso crítico -como una aplicación o un sistema- desde ubicaciones o dispositivos poco habituales.

1. **Panel de ingestión de datos y salud**

El panel de ingestión de datos y salud muestra el número de registros de eventos, las fuentes de registro y las tasas de éxito de los datos que se están procesando en Chronicle. Un analista de Seguridad podría utilizar este panel para asegurarse de que las fuentes de registro están correctamente configuradas y que los registros se reciben sin errores. Esto ayuda a garantizar que se abordan los problemas relacionados con los registros para que el equipo de Seguridad tenga acceso a los datos de registro que necesita.

1. **Cuadro de mando de coincidencias de COI**

El cuadro de mandos de coincidencias COI indica las principales amenazas, riesgos y vulnerabilidades para la organización. Los profesionales de la Seguridad utilizan este tablero para observar los nombres de dominio, las direcciones IP y los COI de los dispositivos a lo largo del tiempo con el fin de identificar tendencias. Esta información se utiliza después para dirigir el enfoque del equipo de seguridad hacia las amenazas de mayor prioridad. Por ejemplo, los analistas de Seguridad pueden utilizar este panel para buscar actividad adicional asociada a una alerta, como el inicio de sesión de un usuario sospechoso desde una ubicación geográfica inusual.

1. **Panel principal**

El cuadro de mandos principal muestra un resumen de alto nivel de la información relacionada con la actividad de ingestión de datos, alertas y eventos de la organización a lo largo del tiempo. Los profesionales de la Seguridad pueden utilizar este panel para acceder a una cronología de los eventos de seguridad -como un pico de intentos fallidos de inicio de sesión- para identificar las tendencias de las amenazas a través de las fuentes de registro, los dispositivos, las direcciones IP y las ubicaciones físicas.

1. **Panel de detecciones de reglas**

El panel de detecciones de reglas proporciona estadísticas relacionadas con los incidentes de mayor incidencia, gravedad y detecciones a lo largo del tiempo. Los analistas de Seguridad pueden utilizar este tablero para acceder a una lista de todas las alertas activadas por una regla de detección específica, como una regla diseñada para alertar cada vez que un usuario abre un archivo adjunto malicioso conocido de un correo electrónico. A continuación, los analistas utilizan esas estadísticas para ayudar a gestionar los incidentes recurrentes y establecer tácticas de mitigación para reducir el nivel de riesgo de una organización.

1. **Panel general de inicio de sesión de usuario**

El cuadro de mandos general del inicio de sesión de los usuarios proporciona información sobre el comportamiento de acceso de los usuarios en toda la organización. Los analistas de Seguridad pueden utilizar este panel para acceder a una Lista de todos los eventos de inicio de sesión de los usuarios para identificar actividades inusuales de los usuarios, como el inicio de sesión de un usuario desde varias ubicaciones al mismo tiempo. A continuación, esta información se utiliza para ayudar a mitigar las amenazas, los riesgos y las vulnerabilidades de las cuentas de usuario y las aplicaciones de la organización.

**Claves**

Las herramientas SIEM proporcionan paneles que ayudan a los profesionales de la Seguridad a organizar y centrar sus esfuerzos en materia de Seguridad. Esto es importante porque permite a los analistas reducir el riesgo identificando, analizando y remediando los elementos de mayor prioridad de manera oportuna. Más adelante en el Programa, tendrá la oportunidad de practicar el uso de diversas características y comandos de las herramientas SIEM para realizar consultas de búsqueda.