**Cuadros de mando de administración de información y eventos de seguridad (SIEM)**

las herramientas de SIEM se basan en los registros para monitorear los sistemas y detectar amenazas de Seguridad.

Una herramienta de administración de información y eventos de seguridad, o SIEM, es una aplicación que recopila y analiza los datos de registro para monitorear las actividades críticas de una organización. Proporciona visibilidad en tiempo real, monitoreo y análisis de eventos y alertas automatizadas. También almacena todos los datos de registro en una ubicación centralizada.

Como las herramientas SIEM indexan y minimizan la cantidad de registros que un profesional de Seguridad debe revisar y analizar manualmente, aumentan la eficiencia y ahorran tiempo. Sin embargo, las herramientas de SIEM deben configurarse y personalizarse para satisfacer las necesidades de Seguridad únicas de cada organización. A medida que surgen nuevas amenazas y vulnerabilidades, las organizaciones deben personalizar continuamente sus herramientas de SIEM para garantizar que las amenazas se detecten y aborden rápidamente.

Las herramientas SIEM también se pueden usar para crear paneles. Es posible que haya encontrado paneles en una aplicación de su teléfono u otro dispositivo. Presentan información sobre tu cuenta o ubicación en un formato fácil de entender.

Por ejemplo, las aplicaciones meteorológicas muestran datos como la temperatura, las precipitaciones, la velocidad del viento y el pronóstico mediante tablas, gráficos y otros elementos visuales.

Este formato facilita la identificación rápida de los patrones y tendencias meteorológicas, para que puedas estar preparado y planificar tu día en consecuencia.

Al igual que las aplicaciones meteorológicas ayudan a las personas a tomar decisiones rápidas e informadas basadas en datos, los paneles de SIEM ayudan a los analistas de seguridad a acceder rápida y fácilmente a la información de seguridad de su organización en forma de tablas, gráficos o tablas.

Por ejemplo, un analista de Seguridad recibe una alerta sobre un intento de inicio de sesión sospechoso. El analista accede a su panel de SIEM para recopilar información sobre esta alerta. Mediante el panel de control, el analista descubre que se han realizado 500 intentos de inicio de sesión en la cuenta de Ymara en un lapso de cinco minutos. También descubren que los intentos de inicio de sesión se realizaron desde ubicaciones geográficas fuera de la ubicación habitual de Ymara y fuera de su horario de trabajo habitual. Al usar un panel, el analista de Seguridad pudo revisar rápidamente las representaciones visuales de la cronología de los intentos de inicio de sesión, la ubicación y la hora exacta de la actividad, y luego determinar si la actividad era sospechosa.

Además de proporcionar un resumen completo de los datos relacionados con la seguridad, los paneles de SIEM también proporcionan a la parte interesada diferentes métricas. Las métricas son atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software.

Los paneles de SIEM se pueden personalizar para mostrar métricas específicas u otros datos que sean relevantes para los diferentes miembros de una organización. Por ejemplo, un analista de Seguridad puede crear un panel que muestre las métricas para supervisar las operaciones empresariales diarias, como el volumen del tráfico de red entrante y saliente.

**Puntos clave**

Las herramientas SIEM desempeñan una importante Función en el Monitoreo de los Datos de una organización. Como analista de seguridad de nivel básico, es posible que monitorice los paneles SIEM como parte de sus tareas diarias. Investigar regularmente los nuevos desarrollos de la tecnología SIEM le ayudará a crecer y a adaptarse a los cambios en el Campo de la ciberseguridad. La computación en la nube, la integración SIEM-aplicación y la automatización son sólo algunos de los avances que los profesionales de la seguridad pueden esperar en la evolución futura de las herramientas SIEM.