**Herramientas comunes de ciberseguridad**

**Log:** Un **registro** es un registro de los eventos que se producen en los sistemas de una organización. Entre los ejemplos de registros relacionados con la seguridad se incluyen los registros de empleados que inician sesión en sus ordenadores o acceden a servicios basados en la web. Los registros ayudan a los profesionales de la seguridad a identificar las vulnerabilidades y posibles infracciones de seguridad.

Las primeras herramientas que analizaremos son las herramientas de administración de información y eventos de seguridad, o herramientas SIEM. Una herramienta **SIEM** es una aplicación que recopila y analiza los datos de registro para monitorear las actividades críticas de una organización. El acrónimo S-I-E-M puede pronunciarse como «sim» o «parece», pero usaremos «sim» en todo este programa. Las herramientas SIEM recopilan información en tiempo real o instantánea y permiten a los analistas de Seguridad identificar posibles infracciones a medida que ocurren.

Imagine tener que leer páginas y páginas de registros para determinar si hay alguna amenaza de Seguridad. Según la cantidad de datos, puede tardar horas o días. Las herramientas de SIEM reducen la cantidad de datos que un analista debe revisar al proporcionar alertas para tipos específicos de riesgos y amenazas.

A continuación, repasemos ejemplos de herramientas SIEM de uso común: Splunk y Chronicle.

**Splunk** es una plataforma de análisis de datos y **Splunk Enterprise** ofrece soluciones SIEM. **Splunk Enterprise** es una herramienta autohospedada que se utiliza para retener , analizar y buscar los datos de registro de una organización.

Otra herramienta de SIEM es **Google Chronicle**. **Chronicle** es una herramienta SIEM nativa de la nube que almacena datos de Seguridad para su búsqueda y análisis. Nativo en la nube significa que Chronicle permite la entrega rápida de nuevas funciones.

Otras herramientas clave que utilizará en su función de analista de Seguridad, y que tendrá la oportunidad práctica de utilizar más adelante en el programa, son los manuales de estrategias y los analizadores de protocolos de red.

Un **manual** de estrategias es un manual que proporciona detalles sobre cualquier acción operativa, como la forma de responder a un incidente. Los manuales, que varían de una organización a otra, guían a los analistas sobre cómo gestionar un incidente de Seguridad antes, durante y después de que se produzca. Los manuales pueden referirse a las revisiones de Seguridad o cumplimiento, la administración del acceso y muchas otras tareas organizativas que requieren un proceso documentado de principio a fin.

Otra herramienta que puede usar como analista de Seguridad es un **analizador de protocolos de red (sniffers de paquetes)**, también llamado rastreador de paquetes. Un rastreador de paquetes es una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red. Entre los analizadores de protocolos de red más comunes se incluyen **tcpdump** y **Wireshark**.