**Registros**

Archivo de los eventos que se producen en los sistemas de una organización, entre los cuales se incluyen

* Inicios de sesión de los empleados en sus ordenadores
* Accesos a servicios basados en la web

Los registros ayudan a los profesionales de la seguridad a identificar las vulnerabilidades y posibles infracciones de seguridad

**Herramientas SIEM**Una herramienta SIEM (administración de información y eventos de seguridad) es una aplicación que recopila y analiza los datos de registro para monitorear las actividades criticas de una organización, recopilan información en tiempo real o instantánea y permiten a los analistas de Seguridad identificar posibles infracciones a medida que ocurren, algunos tipos de estas herramientas son:

1. **Splunk**: es una plataforma de análisis de datos y Splunk Enterprise ofrece soluciones SIEM
2. **Chronicle**: plataforma de operaciones de seguridad desarrollada por Google que ayuda a las organizaciones a detectar, investigar y responder a amenazas cibernéticas. Se describe como una plataforma SIEM (Security Information and Event Management) nativa de la nube, que se basa en la infraestructura de Google Cloud para ofrecer capacidades de análisis y búsqueda de datos de seguridad a gran escala. 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.

Tambien se podrán usar herramientas como es un analizador de protocolos de red , 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*
* *Wireshark*

**Manuales de estrategias**

Es un manual que proporciona detalles sobre cualquier acción operativa, como por ejemplo cómo responder a un incidente de seguridad. Las organizaciones suelen tener varios manuales de estrategias que documentan los procesos y procedimientos que deben seguir sus equipos. Los manuales de estrategias varían de una organización a otra, pero todos tienen un propósito similar: guiar a los analistas a través de una serie de pasos para completar tareas específicas relacionadas con la Seguridad. Se pueden seguir 2 tipos de manuales cuanso se trabaja en un caso forense

1. *Libro de jugadas de la cadena de custodia:* la cadena de custodia es el proceso de documentación de la posesión y el control de las pruebas durante el ciclo de vida de un incidente. Como analista de seguridad que participa en un análisis forense, trabajará con los datos informáticos que fueron violados. Usted y el equipo forense también tendrán que documentar quién, qué, dónde y por qué tiene las pruebas recogidas. Las pruebas son su responsabilidad mientras estén en su posesión. Las pruebas deben mantenerse seguras y rastreadas. Cada vez que se trasladen las pruebas, deberá informarse de ello. Esto permite que todas las partes implicadas sepan exactamente dónde están las pruebas en todo momento.
2. *Manual de protección y preservación de evidencias:* proteger y preservar evidencias es el proceso de trabajar adecuadamente con evidencias digitales frágiles y volátiles. Así, como analista de seguridad, es fundamental comprender que son las pruebas digitales frágiles y volátiles y por que existe un procedimiento. A medida que siga este Manual de estrategias, consultará el Orden de volatilidad, que es una secuencia que describe el orden de los datos que deben conservarse del primero al último. Da prioridad a los Datos volátiles, que son aquellos que pueden perderse si el dispositivo en cuestión se apaga, independientemente del motivo. Mientras se lleva a cabo una investigación, una gestión inadecuada de las pruebas digitales puede comprometer y alterar dichas pruebas. Cuando las pruebas se gestionan de forma inadecuada durante una investigación, ya no pueden utilizarse. Por esta razón, la primera prioridad en cualquier investigación es preservar adecuadamente los datos. Puede preservar los Datos haciendo copias y llevando a cabo su investigación utilizando esas copias.

**La programación en la ciberseguridad**

Las organizaciones pueden usar la programación para crear un conjunto específico de instrucciones para que una computadora ejecute tareas. La programación permite a los analistas completar tareas y procesos repetitivos con un alto grado de precisión y eficiencia. También ayuda a reducir el riesgo de errores humanos y puede ahorrar horas o días en comparación con la realización manual del trabajo. Además de esto, se utiliza un S.O especifico y relacionado llamado:

*Linux:* es un sistema operativo de código abierto o disponible públicamente y se basa en una línea de comandos como interfaz de usuario principal. Linux en sí mismo no es un lenguaje de programación, pero sí permite el uso de comandos basados en texto entre el usuario y el sistema operativo.

*SQL:* siglas de Lenguaje de Consulta Estructurado. SQL es un lenguaje de programación que se utiliza para crear interactuar y solicitar información de una base de datos. Una base de datos es una colección organizada de información o datos. Puede haber millones de puntos de datos en una base de datos. Por lo tanto, un analista de seguridad de nivel básico utilizaría SQL para filtrar los puntos de datos y recuperar información específica.

*Python:* es utilizado para realizar tareas repetitivas y lentas que requieren un alto nivel de detalle y precisión

**Vulnerabilidad web**

Una vulnerabilidad web es un fallo único en una aplicación web que un agende de amenaza podría explotar mediante el uso de código o comportamiento malicioso, para permitir el acceso no autorizado, el robo de datos y la implementación de software malicioso para permitir el acceso no autorizado, el robo de datos y la implementación de software malicioso

**Sistema de detección de intrusiones**

Es una aplicación que monitoriza la actividad del sistema y alerta sobre posibles intrusiones. El sistema escanea y analiza los paquetes de red, que transportan pequeñas cantidades de datos a través de una red. La pequeña cantidad de datos facilita el proceso de detección para que un IDS identifique posibles amenazas a los datos sensibles. Otros sucesos que un IDS puede detectar pueden ser robos y accesos no autorizados

**Encriptación**

Hace que los datos sean ilegibles y difíciles de descifrar para un usuario no autorizado; su principal objetivo es garantizar la confidencialidad de los datos privados, es el proceso de convertir datos de un formato legible a un formato codificado criptográficamente, la cual consiste en convertir el texto plano en texto cifrado seguro

**Pruebas de penetración**

Las pruebas de penetración, también denominadas pen testing, son el acto de participar en un ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. Es una evaluación de riesgos exhaustiva que puede evaluar e identificar las amenazas externas e internas, así como los puntos débiles.