A modo de recuerdo, sabemos que un **registro** es un listado de los eventos que ocurren en los sistemas y redes de una organización. Hay 3 fuentes de registros comunes:

1. *Registro de firewall:* registro de las conexiones intentadas o establecidas para el trafico entrante de internet
2. *Registro de red:* registro de todos los ordenadores y dispositivos que entran y salen de la red
3. *Registro de servidor:* registro de eventos relacionados con servicios como sitios web, correos electrónicos o archivos compartidos. Se incluyen acciones como solicitudes de inicio de sesión, contraseña y nombre de usuario

Al monitorear los registros, los equipos de seguridad pueden identificar las vulnerabilidades y las posibles violaciones de datos

**Herramienta de Administración de Información y Eventos de Seguridad (SIEM):** aplicación que recopila y analiza los datos de registro para monitorear las actividades criticas de una organización. Proporciona visibilidad en tiempo real, monitoreo y análisis de eventos y alertas automatizadas. También amacena todos los datos de registro en una ubicación centralizada.   
Las herramientas, al indexar y minimizar la cantidad de registros que un profesional debe revisar y analizar manualmente, ahorran tiempo y aumentan la eficiencia. Sin embargo, estas deben configurarse y personalizarse para satisfacer las necesidades, debe ser continuamente, ya que siempre surgen nuevas amenazas y vulnerabilidades

Las herramientas a su vez, se pueden usar para crear paneles, como los que se puede encontrar en una aplicación que presenta información sobre tu cuenta o ubicación. 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 u otros elementos visuales. 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 todo lo anteriormente dicho, los paneles también proporcionan a la parte interesada diferentes métricas, las cuales 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

Las herramientas SIEM están evolucionando hacia soluciones en la nube (alojadas y nativas), gestionadas por proveedores y accesibles vía Internet, ofreciendo mayor disponibilidad, flexibilidad y escalabilidad. Con el crecimiento del IoT, aumentan la superficie de ataque y los datos a analizar. La incorporación de IA, machine learning y automatización (SOAR) permitirá una detección más precisa de amenazas, mejor visualización, almacenamiento optimizado y respuestas más rápidas, reduciendo la intervención manual. En el futuro, se espera una mayor integración y comunicación entre plataformas de ciberseguridad, aunque aún es un proceso en desarrollo.

Existen diferentes tipos de herramientas SIEM que las organizaciones pueden elegir:

* Herramientas autoalojadas: requieren que las organizaciones instalen, operen y mantengan la herramienta utilizando su propia infraestructura física, como la capacidad del servidor. Son ideales cuando una organización debe mantener el control físico sobre los datos confidenciales
* Herramientas alojadas en la nube: son mantenidas y gestionadas por losa proveedores de SIEM, lo que las hace accesibles a través de internet e ideales para organizaciones que no quieren invertir y crear su propia infraestructura, o por una organización que puede optar por utilizar una combinación de ambas, conocida como solución hibrida

Entre las herramientas mas comunes se destacan:

* ***Splunk:*** plataforma de análisis de datos y Splunk Enterprise proporciona soluciones SIEM. Esta es una herramienta autoalojada utilizada 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 utilizada para recopilar, buscar y monitorear datos de registro útil para las organizaciones que buscan entornos de soluciones hibridas o solo en la nube
* ***Chronicle (de Google):*** es una herramienta nativa de la nube diseñada para retener, analizar y recopilar datos, al ser nativa de la nube, está diseñada específicamente para aprovechar al máximo las capacidades de la computación en la nube, como la disponibilidad, flexibilidad y escalabilidad. Permite recopilar y analizar datos de registro en función de un recurso especifico, un nombre de dominio, un usuario y una dirección IP

**Herramientas de código abierto:** suelen ser gratuitas y fáciles de usar, su objetivo es proporcionar a los usuarios software creado por el publico de forma colaborativa, lo que puede hacer que el software sea más seguro, además permiten una mayor personalización por parte de los usuarios, algunos ejemplos son:  
**-Linux:** sistema operativo de código abierto

-**Suricata:** software de análisis de red y detección de amenazas de código abierto

**Herramientas propietarias:** son desarrolladas y propiedad de una persona o empresa, y los usuarios suelen pagar una cuota por su uso y formación. Los propietarios son los únicos que pueden acceder al código fuente y modificarlo, por lo que los usuarios en general deben esperar actualizaciones de software, lo que puede llevar a incluso el pago de una cuota, un ejemplo de estas son Splunk y Chronicle

Splunk ofrece distintos paneles:

* **Panel de postura de seguridad:** esta diseñado para los centros de operaciones de seguridad. Muestra las ultimas 24hs 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, sirve para investigar las amenazas potenciales en tiempo real, así como la actividad de red sospechosa
* **Panel de resumen ejecutivo:** analiza y supervisa la salud general de la organización a lo largo del tiempo, ayuda a mejorar las medidas de seguridad que reducen el riesgo
* **Panel 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
* **Panel de analisis de riesgos:** ayuda a los analistas a identificar el riesgo por cada objeto de riesgo (en un usuario especifico, una computadora por ejemplo). Muestra los cambios en la actividad o el comportamiento relacionado con el riesgo, como el inicio de sesión fuera de las horas normales del trabajo

Por otro lado, Chronicle proporciona multiples tableros que ayudan a los analistas a monitorear los registros de una organización, crear filtros y alertas, y rastrear nombres de dominios sospechosos:

* **Panel de estadísticas empresariales:** destaca las alertas recientes, identifica nombres de dominios sospechosos en los registros, conocidos como *Indicadores de Compromiso*. Cada resultado es etiquetado con una puntuación de confianza para indicar la probabilidad de una amenaza. Tambien proporciona un nivel de gravedad que indica la importancia de cada amenaza para la organización
* **Panel de ingestión de datos y salud:** muestra el numero de registros de eventos, las fuentes de registro y las tasas de éxito de los datos que se están procesando en Chronicle, se puede utilizar este panel para asegurarse que las fuentes de registro están correctamente configuradas y que los registros se reciben sin errores
* **Cuadro de mando de coincidencias (COI):** indica las principales amenazas, riesgos y vulnerabilidades para la organización. Este tablero se utiliza 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 es utilizada para dirigir el enfoque del equipo de seguridad hacia las amenazas de mayor prioridad
* **Panel 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, este panel se puede usar para acceder a una cronología de los eventos de seguridad para identificar las tendencias de las amenazas
* **Panel de detecciones de reglas:** proporciona estadísticas relacionadas con los incidentes de mayor incidencia, gravedad y detecciones a lo largo del tiempo, se puede usar para acceder a una lista de todas las alertas activadas por una regla de detección especifica, como una regla diseñada para alertar cada vez que un usuario abre un archivo adjunto malicioso conocido de un correo electrónico
* **Panel general de inicio de sesión de usuario:** proporciona información sobre el comportamiento de acceso de los usuarios en toda la organización, se puede utilizar para acceder a una lista de todos los eventos de inicio de sesión para identificar actividades inusuales en los usuarios