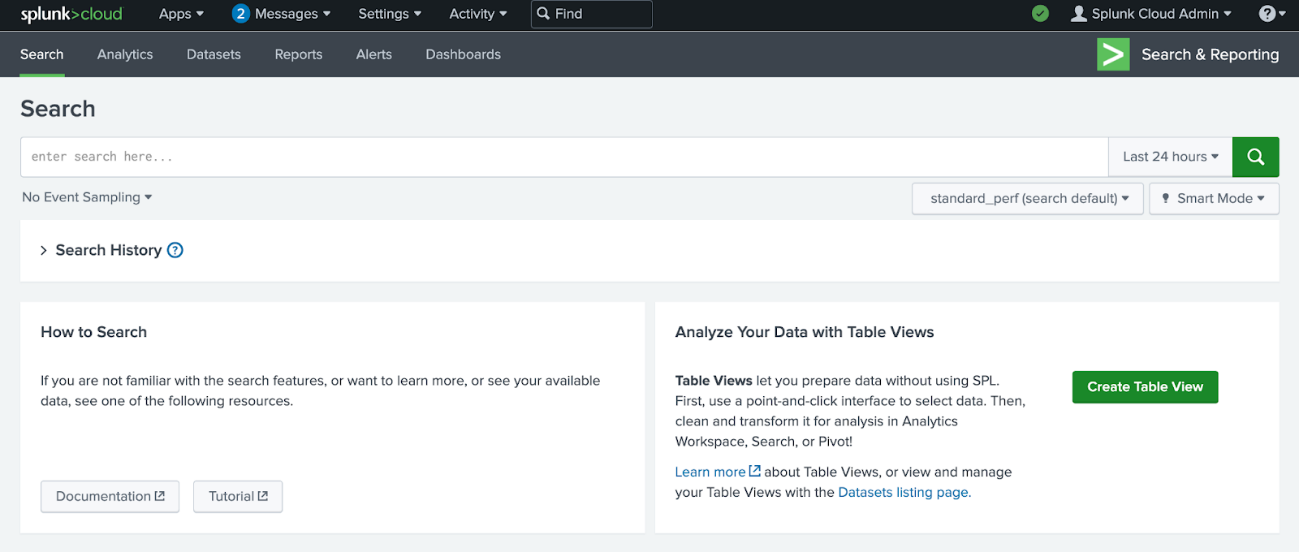
**Métodos de búsqueda con herramientas SIEM**

Anteriormente, aprendiste a usar las **herramientas de gestión de eventos e información de seguridad (SIEM)** para detectar eventos de seguridad, como intentos fallidos de inicio de sesión. SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización. En esta lectura, verás cómo herramientas SIEM, como Splunk y Chronicle, utilizan diferentes métodos de búsqueda para encontrar, filtrar y transformar los resultados de búsqueda.

No todas las organizaciones utilizan la misma herramienta SIEM para recopilar y centralizar sus datos de seguridad, por lo cual tendrás que aprender a usar varias de ellas. Entender los diferentes tipos de búsquedas que puedes llevar a cabo con estas herramientas es muy importante para encontrar datos de eventos relevantes que respalden tus investigaciones de seguridad.

**Búsquedas de Splunk**

Como has aprendido, Splunk tiene su propio lenguaje de consulta, denominado **Search Processing Language (SPL)** (lenguaje de procesamiento de búsqueda**)** que se utiliza para buscar y recuperar eventos de índices mediante la aplicación de búsqueda e informes de la herramienta. Una búsqueda SPL puede contener muchos comandos y argumentos diferentes. Por ejemplo, puedes usar comandos para transformar los resultados de búsqueda en un formato de gráfico o filtrar los resultados para obtener información específica.



Este es un ejemplo de una búsqueda SPL básica que está consultando un índice para un evento fallido:

**index=main fail**

* **index=main**: Es el comienzo del comando de búsqueda que le dice a Splunk que recupere eventos de un **index** (índice) llamado **main**.
* **fail**: Es el término de búsqueda. Le dice a Splunk que devuelva los eventos que contengan el término **fail**.

Saber cómo usar el SPL de manera efectiva tiene muchos beneficios. Ayuda a acortar el tiempo que se tarda en devolver los resultados de búsqueda y también a obtener los resultados exactos que necesitas de varias fuentes de datos. El SPL admite muchos tipos diferentes de búsquedas que no se incluyen en esta lectura. Si quieres conocer más sobre SPL, puedes consultar la [Referencia de búsqueda de Splunk](https://docs.splunk.com/Documentation/Splunk/9.0.2/SearchReference/UnderstandingSPLsyntax).

**Pipe**

Es posible que ya conozcas cómo se utiliza el comando pipe en Bash de Linux. A modo de repaso, el comando pipe envía la salida de un comando como entrada a otro comando.

SPL también utiliza la barra vertical o pleca **|** para separar los comandos individuales en la búsqueda y para encadenar comandos juntos, de forma tal que la salida de un comando se combine en el siguiente comando. Esto es útil porque te permite refinar los datos de varias maneras para obtener los resultados que necesitas, con un solo comando.

Aquí podrás observar un ejemplo de dos comandos separados por una pleca:

**index=main fail| chart count by host**

* **index=main fail**: Es el comienzo del comando de búsqueda que le dice a Splunk que recupere eventos de un **index** (índice) llamado **main** para eventos que contienen el término de búsqueda **fail**.
* **|**: La pleca separa y encadena los dos comandos **index=main**y **chart count by host**. Esto significa que la salida del primer comando *index=main* se usa como la entrada del segundo comando **chart count by host**.
* **chart count by host**: Este comando le dice a Splunk que transforme los resultados de búsqueda creando un **chart** (gráfico) de acuerdo con el **count** (recuento) o la cantidad de eventos. El argumento **by host** le dice a Splunk que enumere los eventos por host, que son los nombres de los dispositivos de los que provienen los eventos. Este comando puede ser útil para identificar hosts con recuentos excesivos de errores en un entorno.

**Comodín**

El **comodín** es un carácter especial que se puede sustituir por cualquier otro. Se suele simbolizar con un carácter de asterisco **\***. Los comodines coinciden con los caracteres en los valores de una cadena. En Splunk, el comodín que uses depende del comando con el que lo estés usando. Los comodines son útiles porque pueden ayudar a encontrar eventos que contienen datos similares, pero no completamente idénticos. A continuación, verás un ejemplo de uso de un comodín para expandir los resultados de búsqueda de un término de búsqueda:

**index=main fail\***

* **index=main**: Este comando recupera eventos de un **index** (índice) llamado **main**.
* **fail\***: El comodín después de **fail** representa cualquier carácter. Le dice a Splunk que busque todas las terminaciones posibles que contengan el término **fail**. Esto expande los resultados de búsqueda y devolverá eventos que contengan el término **fail**, como "failed" o "failure".

**Consejo profesional**: Las comillas dobles se utilizan para especificar la búsqueda de una frase o cadena exacta. Por ejemplo, si solo quieres buscar eventos que contengan la frase exacta **login failure** (error de inicio de sesión), puedes colocar la frase entre comillas dobles **"login failure"**. Esta búsqueda coincidirá solo con eventos que contengan la frase exacta **login failure** y no con otros eventos que contengan las palabras **failure** o **login** por separado.

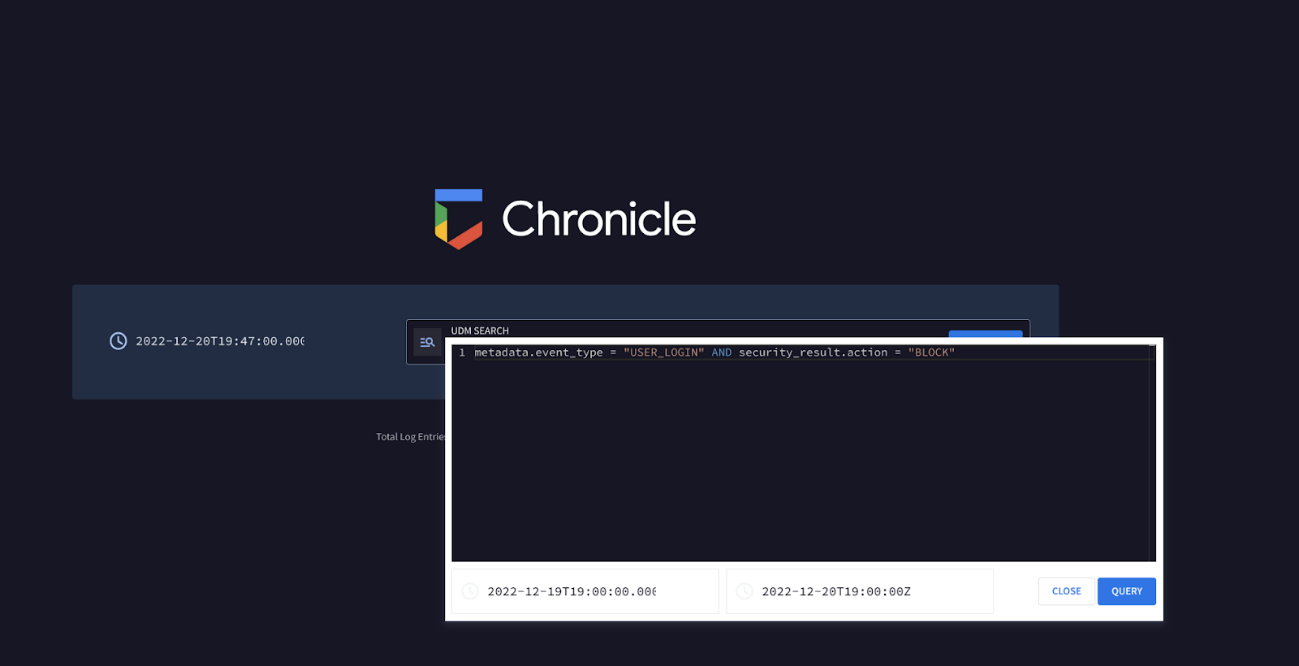
**Búsquedas en Chronicle**

En Chronicle, puedes buscar eventos en el campo Search (Buscar) y, además, utilizar el menú Procedural Filtering (proceso de filtrado) para aplicar filtros y refinar aún más los resultados de búsqueda. Por ejemplo, puedes usarlo para incluir o excluir resultados de búsqueda que contengan información específica relacionada a un tipo de evento o una fuente de registro. Hay dos tipos de búsqueda que puedes realizar para encontrar eventos en Chronicle: una búsqueda de modelos de datos unificados (UDM) o una búsqueda de registro sin procesar.



**Búsqueda de modelos de datos unificados (UDM)**

Es el tipo de búsqueda predeterminado que se utiliza en Chronicle. Para hacer una búsqueda UDM, debes escribir lo que quieres buscar, hacer clic en "Search" (Buscar) y seleccionar "UDM Search" (Búsqueda UDM). Con este tipo de búsqueda, Chronicle busca datos de seguridad que se hayan ingerido, analizado y normalizado. Una búsqueda UDM recupera los resultados de búsqueda más rápido que una búsqueda de registro sin procesar, porque busca en datos indexados y estructurados que están normalizados en UDM.



Una búsqueda UDM recupera eventos formateados en UDM, que contienen campos UDM. Hay muchos tipos diferentes de campos UDM que se pueden usar para consultar información específica de un evento. En esta lectura no los analizaremos todos, pero si deseas obtener más información, puedes consultar la [lista de campos UDM de Chronicle](https://cloud.google.com/chronicle/docs/reference/udm-field-list). Todos los eventos UDM contienen un conjunto de campos comunes que incluyen:

* **Entidades**: Se las conoce también como sustantivos. Todos los eventos UDM deben contener al menos una entidad. Este campo brinda contexto adicional sobre un dispositivo, usuario o proceso que está involucrado en un evento. Por ejemplo, un evento UDM que contiene información de entidad incluye los detalles del origen de un evento, como el nombre de host, el nombre de usuario y la dirección IP del evento.
* **Metadatos del evento**: Brinda una descripción básica de un evento, incluidos el tipo de evento, las marcas de tiempo y demás.
* **Metadatos de red**:Proporciona información sobre eventos relacionados con la red y detalles del protocolo.
* **Resultados de seguridad**:Indica el resultado relacionado con la seguridad de los eventos. Un ejemplo de un resultado de seguridad puede ser un software antivirus que detecta y pone en cuarentena un archivo malicioso e informa: "virus detectado y en cuarentena".

A continuación, podrás ver un ejemplo de una búsqueda UDM simple que utiliza el campo de metadatos de eventos para localizar eventos relacionados con los inicios de sesión de los usuarios:

**metadata.event\_type = “USER\_LOGIN”**

* **metadata.event\_type = “USER\_LOGIN”**: El campo UDM **metadata.event\_type** contiene información sobre el tipo del evento. Esto incluye información como marca de tiempo, conexión de red, autenticación de usuario y demás. Aquí, el tipo de evento especifica **USER\_LOGIN**, que busca eventos relacionados con la autenticación.

Si usas solo campos de metadatos, puedes comenzar rápidamente a buscar eventos. Mientras sigues practicando la búsqueda en Chronicle con UDM Search, irás encontrando más campos. Prueba usar estos campos para realizar búsquedas específicas con el fin de localizar diferentes eventos.

**Búsqueda de registros sin procesar**

Si no puedes encontrar la información que necesitas en los datos normalizados, puedes usar una búsqueda de registros sin procesar, que te permitirá buscar en los registros sin analizar. Para realizar una búsqueda de registros sin procesar, deberás escribir lo que quieres buscar, hacer clic en "Search" (Buscar) y seleccionar "Raw Log Search" (Búsqueda de registro sin procesar). Buscar en registros sin procesar, lleva más tiempo que una búsqueda estructurada. En el campo Search (Buscar), puedes hacer una búsqueda de registro sin procesar si especificas información, como nombres de usuario, nombres de archivo, hashes y demás. Chronicle recuperará los eventos asociados con la búsqueda.

**Consejo profesional**: La búsqueda de registro sin procesar admite el uso de expresiones regulares, lo que puede ayudarte a acotar una búsqueda para que coincida con patrones específicos.

**Conclusiones clave**

Las herramientas SIEM, como Splunk y Chronicle, tienen sus propios métodos para buscar y recuperar datos de eventos. Como analista de seguridad, es importante comprender cómo aprovechar estas herramientas, para encontrar la información que necesitas de manera rápida y eficiente. Esto te permitirá explorar los datos para detectar amenazas y responder rápidamente a los incidentes de seguridad.

**Recursos para obtener más información**

Si deseas obtener más información sobre la búsqueda de eventos con Splunk y Chronicle, puedes consultar los siguientes recursos:

* [Manual de búsqueda de Splunk](https://docs.splunk.com/Documentation/Splunk/9.0.1/Search/GetstartedwithSearch) sobre cómo utilizar el lenguaje de procesamiento de búsqueda Splunk (SPL)
* [Guía de inicio rápido de Chronicle](https://cloud.google.com/chronicle/docs/review-security-alert) sobre los diferentes tipos de búsquedas