Search methods with SIEM tools

So far, you've learned about how you can use **security information and event management (SIEM)** tools to search for security events such as failed login attempts. Remember, SIEM is an application that collects and analyzes log data to monitor critical activities in an organization. In this reading, you'll examine how SIEM tools like Splunk and Chronicle use different search methods to find, filter, and transform search results.

Not all organizations use the same SIEM tool to gather and centralize their security data. As a security analyst, you'll need to be ready to learn how to use different SIEM tools. It's important to understand the different types of searches you can perform using SIEM tools so that you can find relevant event data to support your security investigations.

Splunk searches

As you've learned, Splunk has its own querying language called **Search Processing Language (SPL)**. SPL is used to search and retrieve events from indexes using Splunk's Search & Reporting app. An SPL search can contain many different commands and arguments. For example, you can use commands to transform your search results into a chart format or filter results for specific information.

Splunk Cloud's search page.

Here is an example of a basic SPL search that is querying an index for a failed event:

index=main fail

- *index=main*: This is the beginning of the search command that tells Splunk to retrieve events from an *index* named *main*. An index stores event data that's been collected and processed by Splunk.
- *fail*: This is the search term. This tells Splunk to return any event that contains the term *fail*.

Knowing how to effectively use SPL has many benefits. It helps shorten the time it takes to return search results. It also helps you obtain the exact results you need from various data sources. SPL supports many different types of searches that are beyond the scope of this reading. If you would like to learn more about SPL, explore Splunk's Search Reference

.

Pipes

Previously, you might have learned about how piping is used in the Linux bash shell. As a refresher, piping sends the output of one command as the input to another command.

SPL also uses the pipe character | to separate the individual commands in the search. It's also used to chain commands together so that the output of one command combines into the next command. This is useful because you can refine data in various ways to get the results you need using a single command.

Here is an example of two commands that are piped together:

index=main fail| chart count by host

- *index=main fail*: This is the beginning of the search command that tells Splunk to retrieve events from an *index* named *main* for events containing the search term *fail*.
- |: The pipe character separates and chains the two commands *index=main* and *chart count by host*. This means that the output of the first command *index=main* is used as the input of the second command *chart count by host*.
- *chart count by host*: This command tells Splunk to transform the search results by creating a *chart* according to the *count* or number of events. The argument *by host* tells Splunk to list the events by host, which are the names of the devices the events come from. This command can be helpful in identifying hosts with excessive failure counts in an environment.

Wildcard

A **wildcard** is a special character that can be substituted with any other character. A wildcard is usually symbolized by an asterisk character *. Wildcards match characters in string values. In Splunk, the wildcard that you use depends on the command that you are using the wildcard with. Wildcards are useful because they can help find events that contain data that is similar but not entirely identical. Here is an example of using a wildcard to expand the search results for a search term:

*index=main fail**

- *index=main*: This command retrieves events from an *index* named *main*.
- *fail**: The wildcard after *fail* represents any character. This tells Splunk to search for all possible endings that contain the term *fail*. This expands the search results to return any event that contains the term *fail* such as “failed” or “failure”.

Pro tip: Double quotations are used to specify a search for an exact phrase or string. For example, if you want to only search for events that contain the exact phrase *login failure*, you can enclose the phrase in double quotations "*login failure*". This search will match only events that contain the exact phrase *login failure* and not other events that contain the words *failure* or *login* separately.

Chronicle searches

In Chronicle, you can search for events using the Search field. You can also use Procedural Filtering to apply filters to a search to further refine the search results. For example, you can use Procedural Filtering to include or exclude search results that contain specific information relating to an event type or log source. There are two types of searches you can perform to find events in Chronicle, a Unified Data Mode (UDM) Search or a Raw Log Search.



Chronicle's home page.

Unified Data Model (UDM) Search

The UDM Search is the default search type used in Chronicle. You can perform a UDM search by typing your search, clicking on “Search,” and selecting “UDM Search.” Through a UDM Search, Chronicle searches security data that has been ingested, parsed, and normalized. A UDM Search retrieves search results faster than a Raw Log Search because it searches through indexed and structured data that’s normalized in UDM.



Chronicle's home page.

A UDM Search retrieves events formatted in UDM and these events contain UDM fields. There are many different types of UDM fields that can be used to query for specific information from an event. Discussing all of these UDM fields is beyond the scope of this reading, but you can learn more about UDM fields by exploring Chronicle's UDM field list

. Know that all UDM events contain a set of common fields including:

- **Entities**: Entities are also known as nouns. All UDM events must contain at least one entity. This field provides additional context about a device, user, or process that’s involved in an event. For example, a UDM event that contains entity information includes the details of the origin of an event such as the hostname, the username, and IP address of the event.
- **Event metadata**: This field provides a basic description of an event, including what type of event it is, timestamps, and more.
- **Network metadata**: This field provides information about network-related events and protocol details.
- **Security results**: This field provides the security-related outcome of events. An example of a security result can be an antivirus software detecting and quarantining a malicious file by reporting "virus detected and quarantined."

Here’s an example of a simple UDM search that uses the event metadata field to locate events relating to user logins:

metadata.event_type = “USER_LOGIN”

- *metadata.event_type = “USER_LOGIN”*: This UDM field *metadata.event_type* contains information about the event type. This includes information like timestamp, network connection, user authentication, and more. Here, the event type specifies *USER_LOGIN*, which searches for events relating to authentication.

Using just the metadata fields, you can quickly start searching for events. As you continue practicing searching in Chronicle using UDM Search, you will encounter more fields. Try using these fields to form specific searches to locate different events.

Raw Log Search

If you can't find the information you are searching for through the normalized data, using a Raw Log Search will search through the raw, unparsed logs. You can perform a Raw Log Search by typing your search, clicking on “Search,” and selecting “Raw Log Search.” Because it is searching through raw logs, it takes longer than a structured search. In the Search field, you can perform a Raw Log Search by specifying information like usernames, filenames, hashes, and more. Chronicle will retrieve events that are associated with the search.

Pro tip: Raw Log Search supports the use of regular expressions, which can help you narrow down a search to match on specific patterns.

Key takeaways

SIEM tools like Splunk and Chronicle have their own methods for searching and retrieving event data. As a security analyst, it's important to understand how to leverage these tools to quickly and efficiently find the information you need. This will allow you to explore data in ways that support detecting threats, as well as rapidly responding to security incidents.

Resources for more information

Here are some resources should you like to learn more about searching for events with Splunk and Chronicle:

- Splunk’s Search Manual
- on how to use the Splunk search processing language (SPL)
- Chronicle's quickstart guide

- on the different types of searches

Revision #1
Created 2023-11-04 10:01:23 UTC by naruzkurai

Updated 2023-11-04 10:01:34 UTC by naruzkurai