Microsoft Security Copilot Plugin Guide - Splunk

Plugin overview

Splunk is a software platform that specializes in the analysis and visualization of machine-generated data, delivered as both a SaaS and on-premises solution. It is widely adopted by security operation centers (SOCs) for its powerful search capabilities, real-time data monitoring, and extensive alerting system.

The integration of Splunk into the Microsoft Security Copilot allows users to:

1. Search for Splunk events in a given index
2. Search for Splunk:
    a. Fired Alert(s)-**
    b. Saved Search(es)*
    c. Saved Search History*
    d. Saved Search Suppression State
    e. Search Job(s)-what is running/has run
    f. Alert Actions*
    g. Search Job Results
3. Create Splunk Search Jobs
4. Acknowledge Splunk Saved Searches
5. Dispatch Splunk Saved Searches
6. Create Splunk Saved Search Jobs
7. *NL to SPL-schema on read*
8. *Data retrieval*
9. *SPL against indexes*

Connect to Splunk

Prerequisites

1. Access to a Splunk Cloud instance. We currently do *not* support on-premises Splunk instances. The Self-hosted VM on cloud is also not supported.
2. A Splunk native ID with permissions to create and manage data inputs and API tokens. As of now we only support Basic auth
3. Access to Security Copilot, with permissions to connect plugins
4. Available Splunk API quota

Splunk setup

Allow-list Microsoft egress IP addresses for your region:

West US - 20.118.147.178

East US - 20.12.121.160

Canada Central - 20.104.47.255

Commented [DL1]: Could we add a note somewhere here that we don't support on-premise Splunk instances currently?

Canada East - 20.175.42.154

North Europe - 4.208.18.201

West Europe - 20.23.162.142

UK West - 20.254.153.164

UK South - 20.108.235.187

Australia Southeast - 20.70.94.38

Australia East - 20.167.110.23

Japan East - 20.27.134.98

Japan West - 104.214.147.156

Brazil South - 4.228.22.87

In your Splunk Cloud instance, Navigate to Server Settings

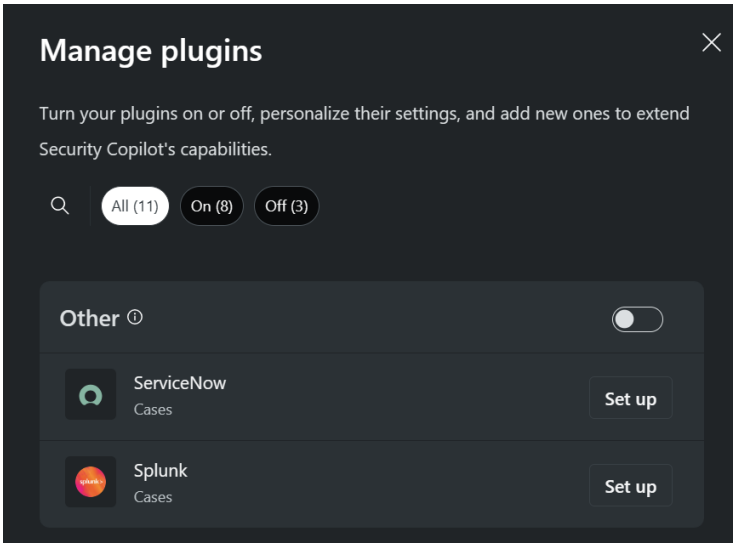
Use Case	Feature	Port	Description
Search head API access	search-api	8089	Grants access for customer subnets to Splunk search head api (applies to automated interfaces)
HEC access for ingestion	hec	443	Allows customer's environment to send HTTP data to Splunk indexers.
Indexer ingestion	s2s	9997	Allows subnets that include UF or HF to send data to Splunk indexers.
SH UI access	search-ui	80/443	Grant explicit access to search head UI in regulated customer environments.
IDM UI access	idm-ui	443	Grant explicit access to IDM UI in regulated customer environments.
IDM API	idm-api	8089	Grant access for add-ons that require an API. (Allows add-ons to send data to Splunk Cloud Platform.)

Tip: For general guidance getting data from TCP and UDP ports, see Getting Data In.

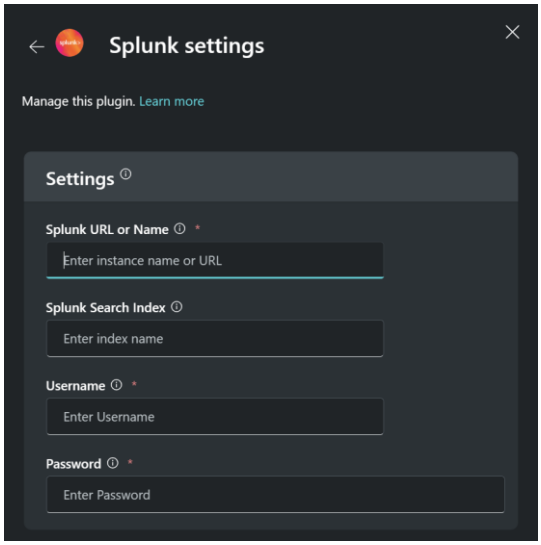
Security Copilot connection

1. Access Security Copilot at https://securitycopilot.microsoft.com/ and ensure you are authenticated.
2. Click the connect icon in the lower left corner of the screen.

3. Locate Splunk under the “Other” section and click “Set up”.



4. Enter the credentials:



a. Here is what each of the credential values mean:

Setting name	Description	Example

Splunk URL or Name	This is the URL or hostname of the Splunk server. It is used to connect to the Splunk instance for data ingestion and querying. Go to the service's portal to find the name or URL (for example, Contoso or www.contoso.service.com). Include the Splunk management port number if it's not the default port (8089). SSL must be enabled on the Splunk instance for communications to work. See here for more information: Configure TLS certificates for inter-Splunk communication - Splunk Documentation	medeina-splunk-test.eastus.cloudapp.azure.com
Splunk Search Index	Splunk index that should be used for search requests. This is the name of the index in Splunk where the data will be stored and searched. It is used to organize and retrieve data in Splunk.	main or security

5. Click "Save" to complete the setup.
   NOTE: Currently, the system does not validate your credentials when you save your settings. If they are not correct, you will see an error later when Security Copilot attempts to run a Splunk skill.
6. Close the plugins window.

Getting started

Tips for effective prompting

Security Copilot operates primarily with natural language prompts. When you query information from Splunk, you will submit a prompt that will guide Security Copilot to select the Splunk skillset and invoke the proper skill.

When you word your prompt, **ensure you mention Splunk as the preferred source of your search**; Security Copilot can connect to several systems that look up information, and it benefits from guidance on which source you prefer.

Example prompt for Splunk Search Job skills

- List all of my splunk search jobs

Commented [DL2]: SSL must be enabled on the splunk instance for communications to work, worth a call out I think

Commented [DL3R2]: Would be worth linking this as well: https://docs.splunk.com/Documentation/Splunk/9.1.1/Security/ConfigTLSCertsS2S

Example prompts for Splunk Alert skills

- Show me my Splunk alert actions
- Show me splunk fired alerts
- Show me the splunk fired alert 'test'
- Show me my Splunk alert actions

Example prompts for Splunk Search skills

- Show me splunk saved searches
- Give me details for the saved search 'Errors in the last hour'
- What's the suppression state for saved search 'Errors in the last hour'

Example prompts for SearchSplunkEvents

*Specifying an index in the query overrides the index specified in the config

- Show me all Splunk events for the index
- What splunk events in the botsv3 index show traffic hitting
- Show me splunk information for index devtutorial
- Show me splunk information for index botsv3
- Show me splunk information for index botsv3 that mentions 127.0.0.1 and abungst-l

Commented [DL4]: Would be good to note that specifying an index in the query overrides the index specified in the config

Plugin capabilities reference

Normally, Security Copilot will select and invoke the appropriate skill based on your prompt, but it is also possible to invoke the skills directly by typing "/" in the prompt bar and providing the necessary inputs.

In either case, it can be helpful to know which skills are available and how they are designed to operate.

Skill name	Skill behavior
Search Job skills - GetSplunkSearchJobResults - GetSplunkSearchJobs - CreateSplunkSearchJob	A Splunk search job is a specific execution of a search. When you run a search, Splunk creates a search job and assigns it a unique search ID. This job retrieves the event data that matches the search criteria within a specified time range. **CreateSplunkSearchJob** creates a new search job in Splunk. - **Required inputs:** Search query **GetSplunkSearchJobResults** retrieves the results of a specific search job. - **Required inputs:** Search job ID - **Optional inputs:** Response data format **GetSplunkSearchJobs** retrieves a list of all search jobs. - **Optional inputs:** Response data format

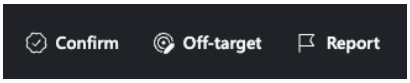
Alert skills - GetSplunkSavedSearchSuppressionState - GetSplunkFiredAlerts - GetSplunkAlertActions - GetSplunkFiredAlert	Splunk alert skills refer to the ability to create alerts in Splunk. Alerts are actions that are triggered when a search produces results that meet certain conditions. These alerts can be used to monitor your data and send notifications when specific conditions are met. **GetSplunkSavedSearchSuppressionState** retrieves the suppression state of a saved search. - **Required inputs:** Name of saved search - **Optional inputs:** Response data format **GetSplunkFiredAlert** retrieves a specific fired alert. - **Optional inputs:** o Name of fired alert o Response data format **GetSplunkFiredAlerts** retrieves a list of all fired alerts. - **Optional inputs:** Response data format **GetSplunkAlertActions** retrieves a list of all alert actions. - **Optional inputs:** Response data format
Search skills - GetSplunkSavedSearches - GetSplunkSavedSearch - GetSplunkSavedSearchHistory - CreateSplunkSavedSearch - DispatchSplunkSavedSearch - AcknowledgeSplunkSavedSearch	Splunk search skills use Splunk's Search Processing Language (SPL) to search your data. These skills are used to locate and perform actions on saved Spluknk searches. **GetSplunkSavedSearches** retrieves a list of all saved searches. - **Optional inputs:** Response data format **GetSplunkSavedSearch** retrieves a specific saved search. - **Required inputs:** Name of saved search - **Optional inputs:** Response data format **GetSplunkSavedSearchHistory** retrieves the history of a specific saved search. - **Required inputs:** Name of saved search - **Optional inputs:** Response data format **CreateSplunkSavedSearch** creates a new saved search. - **Required inputs:**

	○ Name of saved search ○ Search query **DispatchSplunkSavedSearch** dispatches a specific saved search. - **Required inputs:** Name of saved search - **Optional inputs:** Response data format **AcknowledgeSplunkSavedSearch** acknowledges a specific saved search. - **Required inputs:** Name of saved search - **Optional inputs:** Response data format
SearchSplunkEvents	Splunk events are individual records or logs that are returned by a search. An event is a single log entry and contains a timestamp and one or more fields. The fields provide specific information about the event, such as the event source, host, or any other relevant data. **SearchSplunkEvents** searches for specific events in Splunk. - **Required inputs:** ○ **Index**: Specifies the index to search for Splunk events. Example: 'botsv3' ▪ Specifying an index in the query overrides the index specified in the config - **Optional inputs:** ○ **Earliest**: Specifies the earliest time to search for Splunk events in the form of time units or date times. Time units are 's', 'm', 'h', 'd', and 'mon'. Date times must be in the format MM/DD/YYYY:hh:mm:ss. Examples are '-1d' and '10/15/2019:20:00:00' ○ **Latest**: Specifies the latest time to search for Splunk events in the form of time units or date times. Time units are 's', 'm', 'h', 'd', and 'mon'. Date times must be in the format MM/DD/YYYY:hh:mm:ss. Examples are '-1d' and '10/15/2019:20:00:00' ○ **Sort**: Specifies the field to sort the results by. Example: 'time'

	○ **EventCount**: Number of Splunk events to return. ○ **Severity**: Severity for Splunk events in the 'notable' index only. Must be one of: 'low', 'medium', 'high', 'critical', 'informational', 'unknown' ○ **Filters**: Specifies filters based on field and value criteria in the form of a space-separated - '<field_1>=<value_1> <field_2>=<value_2>'. Values can use wildcard patterns (e.g. *test*). If no field is specified for a field-value pair then '_raw' should be used. Examples are 'host=abungst-l dest_ip=*127.0.0.1*' and '_raw=*test*'

Providing feedback

Your feedback on Security Copilot generally, and the Splunk integration specifically, is vital to guide current and planned development on the product. The optimal way to provide this feedback is directly in the product, using the feedback buttons at the bottom of each completed prompt:



We recommend “Confirm” when the result matches expectations, “Off-target” when it does not, and “Report” when the result is harmful in some way.

Whenever possible, and especially when the result is “Off-target”, please write a few words explaining what we can do to improve the outcome. This also applies when you expected Security Copilot to invoke a Splunk skill, but another skill was selected instead.