Mandiant

SPLUNK ENTERPRISE SECURITY

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is remote capable.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login	`/services/auth/login`
Search	`/services/search/jobs/export` This API uses exec_mode set to blocking to run the query.
Search for notables	Step 1: `/services/search/jobs/export using `| rest /services/saved/searches | where <titles of correlation searches that produced notable events>`` Step 2: After getting the list of notable events, we hit the following two for each notable that matched our query: • Retrieve parser for the notable query ◦ `/services/search/parser` • Use parsed notable to search for base events with the Search API call.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access Splunk.
2. Port for Splunk communications (default is 8089).
3. Identify whether the protocol is HTTP or HTTPS for connections to the Splunk port.

4. Identify or create credentials to access Splunk. Read permissions are required.
5. Identify the field name mappings for the following:
    a. Source IP
    b. Destination IP
    c. Source Port
    d. Destination Port
    e. Event Signature ID
    f. Event Name
    g. Event Source Host

    > There could be multiple field names, depending on log sources and configurations.

6. Verify that the Splunk account has the following capabilities enabled:
    - accelerate_search
    - edit_search_schedule_window
    - export_results_is_visible
    - get_metadata
    - get_typeahead
    - list_accelerate_search
    - list_inputs
    - list_metrics_catalog
    - pattern_detect
    - request_remote_tok
    - rest_apps_view
    - rest_properties_get
    - rest_properties_set
    - run_collect
    - run_mcollect
    - schedule_rtsearch
    - search
    - User is set to the GMT/UTC timezone

Configuration

TO ADD THE SPLUNK ES INTEGRATION

> The %ACTOR_IPS% variable can be used in all queries. This variable improves event matching.

1. Go to Settings > Integrations.
2. Click Add Integration > Splunk ES.
3. Enter information for the Host, Port, Protocol, Username, and Password or API Token.
4. Set the Authentication Method (defaults to Token with Bearer Token, Basic, and Token+Cookie as additional options).
    a. The Token method authenticates by logging in and creating a session token, not by using a token that you provide to the Validation Platform.
    b. The Bearer Token method authenticates over HTTP without requiring the Username and Password values. Bearer tokens are permanent unless they are revoked or given an expiry time by a Splunk system administrator.
    c. Basic Authentication Use Case: Your Splunk instance is behind a proxy and there's the possibility of requests

hitting different search heads; if you were using token authentication, the token created by logging into one search head would not work for requests on another search head.

If you are using a load balancer, try using Token+Cookie for the authentication type. Otherwise, verify that the credentials are correct.

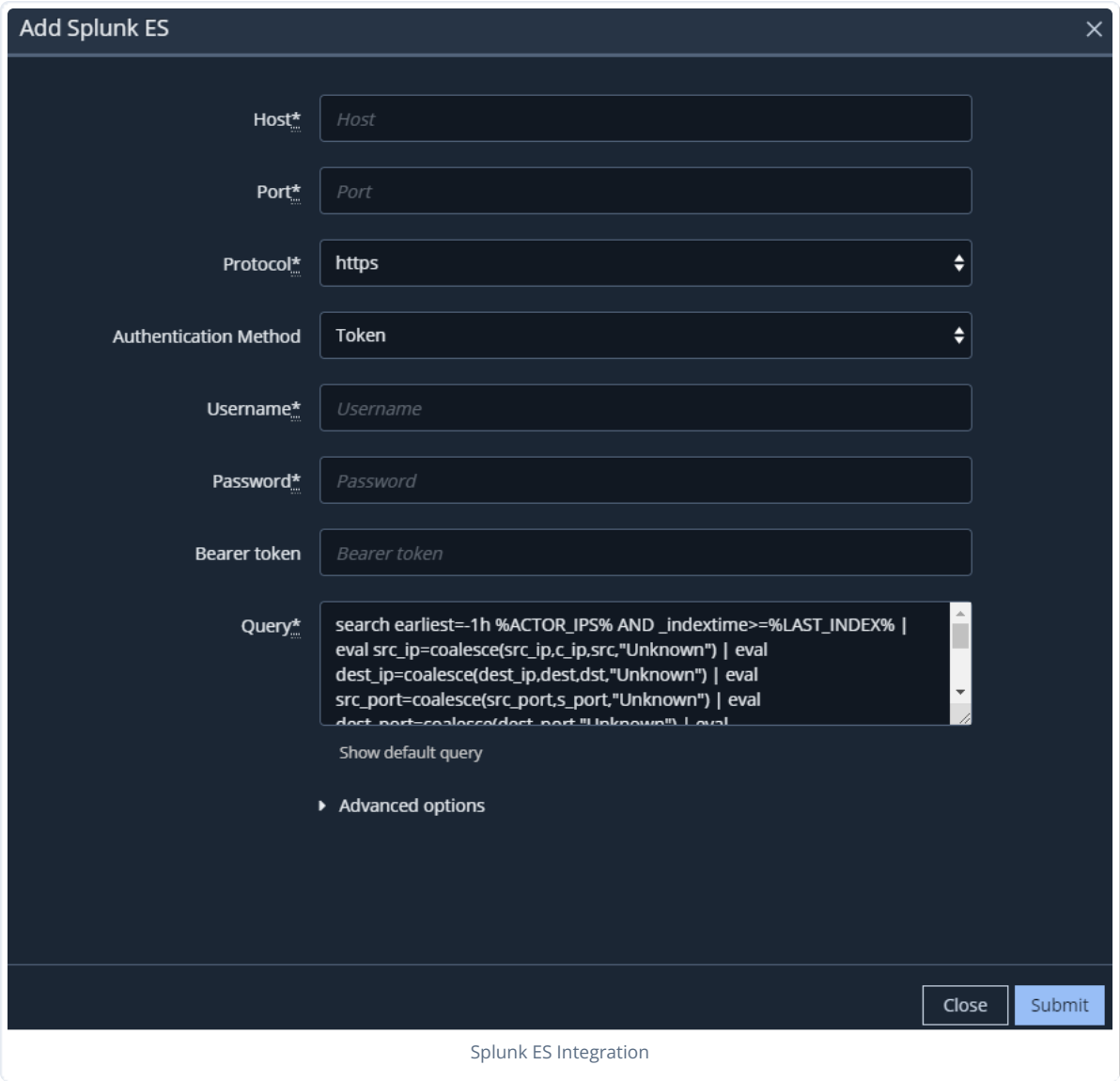
5. Review and update the Query to include instance-specific field names, sources, data types, and other customization.

   This Integration supports the following variables inside queries:

Variable	Description
%ACTOR_IPS%	IP addresses of Actors used to run an Action.
%DOMAINS%	Domain names queried in recent DNS Actions.
%SENDERS%	Email addresses and user names of senders in recent email Actions.
%RECIPIENTS%	Email addresses and user names of recipients of recent email Actions.
%HOST_CLI_ACTOR_IPS%	IP addresses of Actors that recently ran a Host CLI Action.
%HOST_CLI_ACTOR_HOSTNAMES%	Hostname of Actors that recently ran a Host CLI Action.
%LAST_INDEX%	The start time for the query window.

The default queries can be viewed by clicking Show default query.

The query includes information that allows event matching based on any file hashes included in an Action.



Splunk ES Integration

6. Expand Advanced options.
7. (Optional) Update Query time (minutes) and Delay time (minutes).

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

8. (Optional) Enter the App Namespace to use for requests for this Splunk integration.

9. Update Correlation Query as necessary.

- Depending on your Splunk ES environment, some searches for base events require additional manipulation to correctly match against Security Validation Actions. You can add **search replacement** strings that rewrite parts of the Correlation Query when searching for a notable event's base event or events.
- %HOST_CLI_ACTOR_IPS% and %HOST_CLI_ACTOR_HOSTNAMES%, which correspond to any Actor IP addresses or hostnames that were recently used to run Host CLI Actions, can be used in this query. If no Actors were included, the variables in the query are replaced with an empty set of parentheses. This substitution is necessary to prevent errors when the query runs.
- See **Correlated Events (https://docs.mandiant.com/home/correlated-events)** for information about how the Validation Platform matches correlated events to a Job Action.

10. (Optional) Select **Pre-Process Event Correlation**.
11. (Optional) Select **Auto-generate tstats drilldown searches** .

When base events and their corresponding notable events come from correlation searches that use the tstats command, a programmatic drilldown search is needed for the Validation Platform to identify them. If the Auto-generate tstats drilldown searches option is enabled, values from notable events are automatically added to a new search that finds the correct base events. When base events are identified, the corresponding notable event is correlated to a Job.

12. (Optional) Select **Add additional filters to tstats to improve performance** .
13. (Optional) Enter rules in Include subsearches in tstats drilldown for these rules (comma separated). This field lets you tell the platform which rules should also be applied to the tstats drilldown (by default, subsearches are only applied to the base search).
    Example: `RULE_123,RULE_456`
14. (Optional) Enter rules in **Add actor info to base event searches for these notable rules only (comma separated)**. This field lets you define which notable base event queries should be modified to add known actor info before running.
15. (Optional) Select **Add actor info to all base event searches** . When selected, this option will override the previous field and modify all notable base event queries to add known actor info before running.
16. (Optional) Select Enable query for Malicious DNS Actions and configure the Query. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
17. (Optional) Select >Enable query for Email Actions and configure the Query. This query will only be used when you run Email Actions.
18. (Optional) Select Enable query for Host CLI Actions and configure the Query. This query will only be used when you run Host CLI Actions.

If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

19. (Optional) For Timeout for Query Requests (seconds), enter how much time to allow before the query times out. This timeout applies to all queries that you configure for this integration.
20. (Optional) Add **Search replacements** for the Correlation Query.

> The Validation Platform uses Splunk ES base events to accurately match Actions against notable events in Splunk ES. If base events cannot be identified, notable events will not be correlated to Security Validation Actions. Search replacements are applied to base event searches to prevent failed searches and misidentification of notable events.

a. Under **Regex**, enter a Ruby-compatible regular expression (regex) that matches notable event fields from the Correlation Query. As an example, your Correlation Query might search for the following source and destination IP addresses in notable events:
`search src=10.10.0.* dest=10.10.0.*`
A matching regex pattern search would be:
`search (src=[\d.*]+ dest=[\d.*]+)`

b. Under **Replacement**, refer to the captured groups in your regex and add any notable event fields that will help identify base events. Use `\<number>` to refer to the captured groups in your regex, starting at `\1` for the first captured group. Use `%{field_name}` to list notable event fields that you want to be searched. The field name used inside the brackets will automatically return the value identified in the event search. Field names used must exactly match the field name used in notable events. You might use a unique field name shared between your Splunk ES notable events and their corresponding base event. For example, if you know that your Splunk ES notable events share the unique field name "signature" with their corresponding base event, you could include it in your replacement. Using the regex pattern and field name "signature" would look like:
`search \1 signature="%{signature}"`
After entering the regex pattern and replacement pair, the modified search in Splunk ES would be:
`search src=10.10.0.* dest=10.10.0.* signature="Example event"`

Regex	Replacement
search (src=[\d.*]+ dest=[\d.*]+)	search \1 signature="%{signature}"

An example search replacement

21. (Optional) Select Discover network devices automatically.
22. Modify the Query Interval (seconds) and Event Time Adjustment (seconds), if necessary.
23. (Optional) Assign a Name.
24. (Optional) Choose Yes to save suspicious events.
25. Click Submit.

Splunk ES Integration - Advanced Options

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

SAML is not supported.

Verify connectivity

TO VERIFY CONNECTIVITY TO SPLUNK ES

Click Test to verify that:

- The Director can communicate with Splunk on the port and protocol specified.
- The User credentials are working.

If there is an issue running the test, a message identifies the specific cause of the error, helping pinpoint the settings you need to review.

Run a Malicious or Captive DNS Action and then review the last run query to verify:

- The custom DNS query works as expected (if configured).

Troubleshooting Jobs

If events are missing when running Jobs, check the integration's last query. It contains the specific query and errors that occurred when the query was run. In addition, it can provide status information when events for a Job are being processed.