Mandiant

SPLUNK INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Splunk to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Splunk to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

Splunk 8.x-9.x (API V1)

API	Usage
`/auth/login`	Authentication
`/search/jobs`	Querying Splunk for events
`/search/parser`	Querying Splunk for events

Splunk 10.x (API V1)

The integration uses the Splunk SDK, which internally calls the API.

API	Usage
`/auth/login`	Authentication
`/services/server/info`	Retrieving server information
`/search/v2/jobs`	Querying Splunk for events
`/search/v2/jobs/<id>/results`	Getting results of a specific search job
`/search/v2/parser`	Parsing a search string

Supported Versions

- Splunk 8.x-9.x (API V1)
- Splunk 10.x (API V2)

Before You Begin

To configure this integration, you need:

- The hostname of your Splunk instance
- A valid username and password or a Splunk Bearer Token for a user with permissions to use the API endpoints described in the previous step

Authentication

The integration supports both basic and token-based authentication methods.

Basic Authentication

To use basic authentication, collect the username and password of a user that has permission to query the data you would like to use with Mandiant.

Token-Based Authentication

To use an Authentication Token, follow these steps:

1. Log in to the Splunk platform instance as an administrator, or a user that has permission to manage token settings
2. From the system bar, select **Settings > Tokens**
3. Click **Enable Token Authentication**. Token authentication is enabled immediately, and there is no need to restart the instance.

Create a Splunk Authentication Token

1. From the system bar, click **Settings > Tokens**
2. Click **New Token**. The **New Token** dialog box appears
3. In the **New Token** dialog, enter the Splunk platform user that you want to create the token for in the **User** field
4. Enter a short description of the token purpose in the **Audience** field.
5. Optionally define token expiration. In the **Expiration** drop down list, select one of **Absolute Time** or **Relative Time**
    a. If you selected Absolute Time,
        i. Enter a valid date into the first field
        ii. Enter a valid 24-hour time in the second field

    b. If you do not select Absolute Time,
        i. Enter a string that represents the duration after the current time you want the token to be valid for. For example, if you want the token to expire in 30 days, enter +30d

6. Optionally define **Not Before** settings. From the drop-down, select one of **Absolute Time** or **Relative Time**.
    a. Repeat the steps taken for the **Expiration** control. The **Not Before** time can **not** be in the past, nor can it be later than the **Expiration** time.

7. Click **Create**. The **New Token** window updates the **Token** field to display the token value
8. Copy the value of the **Token** field and paste it to a safe location for use in the integration configuration. **NOTE:** The token value cannot be viewed again after you close the window
9. Click Close

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Splunk**.

    
    You can add this as either a Direct or Remote Integration.

3. Choose your preferred environment:
    - **8.x-9.x** for API V1
    - **10.x** for API V2

4. Enter a meaningful **Integration Name**.
5. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** **(https://docs.mandiant.com/home/msv-proxy-rules)**.

6. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
7. For the **Host**, enter the hostname of your Splunk instance.
8. Enter a **Port** value. The default is **8089**.
9. Optional: Enter a **Namespace** value, if needed. The namespace is the user/app context for accessing a resource.
10. From the **SplunkAuthTypesV1** or **SplunkAuthTypesV2** drop-down, choose a token or basic authorization method, depending on what you use in your environment.
11. Enter the **Username** and **Password** for the account that can use API endpoints.
12. Enter the **Bearer Token** value, if one was generated.
13. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
14. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
15. Optional: Add or remove **Queries** and **Correlation Queries**, as needed. Default values are provided for **IP Query**, **DNS Query**, **Email Query**, and **Hostname Query**.
16. Optional: Check **Enable ES Correlation Query** and configure ES correlation queries, as needed.
17. Optional: Check **Enable Correlation Query** and configure correlation queries, as needed.
18. Optional: Modify the **Page Size** value for requests to the upstream server. The default is **500**.
19. Optional: Modify the **Query Max Time** value to change the maximum run time to run a query before finalizing. The default is **300**.
20. Optional: If you enabled ES correlation queries, check **Use Special Tstats Logic** and **Add Filters Conditions To Tstats**.
21. Optional: Configure additional fields, such as **Subsearch In Tstat Rules** and **Include Actor Info For Rules**. Point to ⓘ to access more information.
22. Optional: For API V2, enable **Search Risk Notables** if you want to search for risk-based notables and correlate to original events.

    When activated, the integration first queries the dedicated Risk Index to correlate notables. The integration then automatically performs a secondary search to retrieve and correlate the original, raw source event associated with each risk finding. This double correlation ensures you have complete, validated evidence for every risk notable.

23. Optional: If you enabled ES correlation queries, configure **Search Replacements**.

    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.

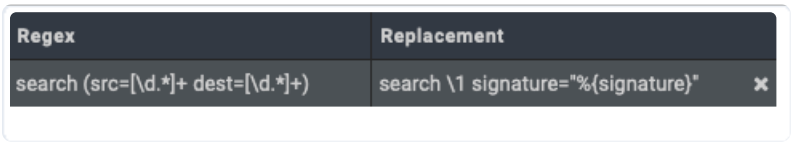
    a. Under **Regex**, enter a Ruby-compatible regular expression (regex) that matches notable event fields from the Correlation Query. As an example, your Correlation Query might search for the following source and destination IP addresses in notable events:
    `search src=10.10.0.* dest=10.10.0.*`
 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



An example search replacement

24. Optional: **Check Apply to Drilldown**.
25. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

26. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    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.

    b. Update **Query Interval** (seconds).
    c. Configure correlation queries:
        i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
        ii. Modify the **Correlation Query Interval**, if necessary (minutes).
    d. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    e. Select **Save Suspicious Events**.
    f. Modify the **Event Time Adjustment** (seconds). The default is **0**.

g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

27. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

> 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 document describes the steps required to integrate Splunk with the Mandiant Security Validation (MSV) Platform.

This integration is remote capable.

API Calls

The following API calls are used when integrating with MSV Platform.

Purpose	Call
Login	`/services/auth/login`
Search	`/services/search/jobs/export`  This API uses exec_mode set to blocking to run the query.

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:

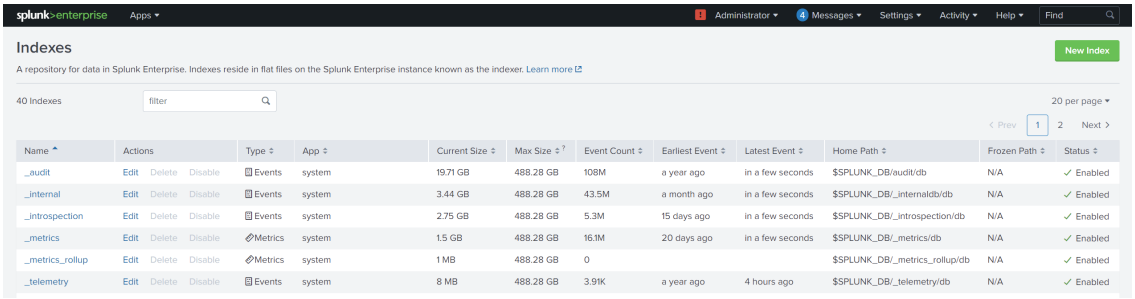
a. Source IP
b. Destination IP
c. Source Port
d. Destination Port
e. Event Signature ID
f. Event Name
g. Event Source Host

> 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

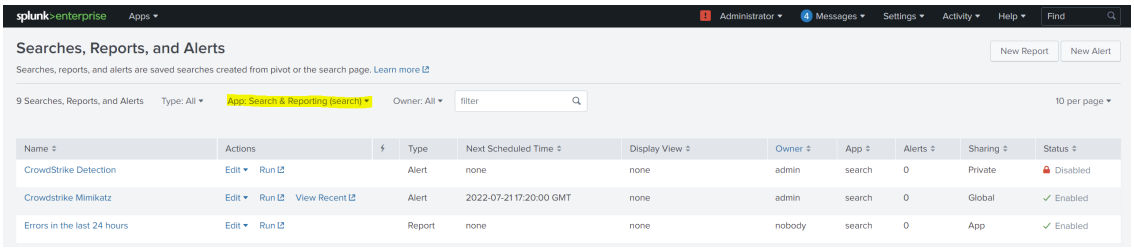
Create Alert conditions within Splunk

1. Create an index to store the alert. **Settings > Indexes > New Index**. Fill in the name of the index.



Splunk Indexes

2. Create an alert by going to: **Settings > Searches, Reports, and Alerts**. Do this step in the **Search & Reporting (search) app**. Select **New Alert**.



Splunk Searches, Reports, and Alerts

3. On the **New Alert** page, enter the following:

> Creating a Crowdstrike alert for demo purposes which is triggered whenever Splunk sees the `event.FileName=mimikatz.exe` and `action=blocked`

   a. **Name**: `Crowdstrike Mimikatz`
   b. **Search**: `index="crowdstrike" AND action="blocked" AND "event.FileName"="mimikatz.exe"`
   c. **Alert Type**: Scheduled

> This step sets up the alert search to run every `15min`

      i. **Run on Cron Schedule**

   d. **Time Range**: `Last 15 minutes`

> This setting should match your Cron schedule to avoid duplicating alerts.

   e. **Cron Expression**: `*/15 * * * *`
   f. **Expires**: `24 Hours` (default)
   g. **Trigger Conditions**:
      i. **Trigger alert when**: Number of Results is greater than 0

> Whenever it's detected, an alert is triggered.

      ii. **Trigger**: For each Result
      iii. **Throttle**: Unchecked

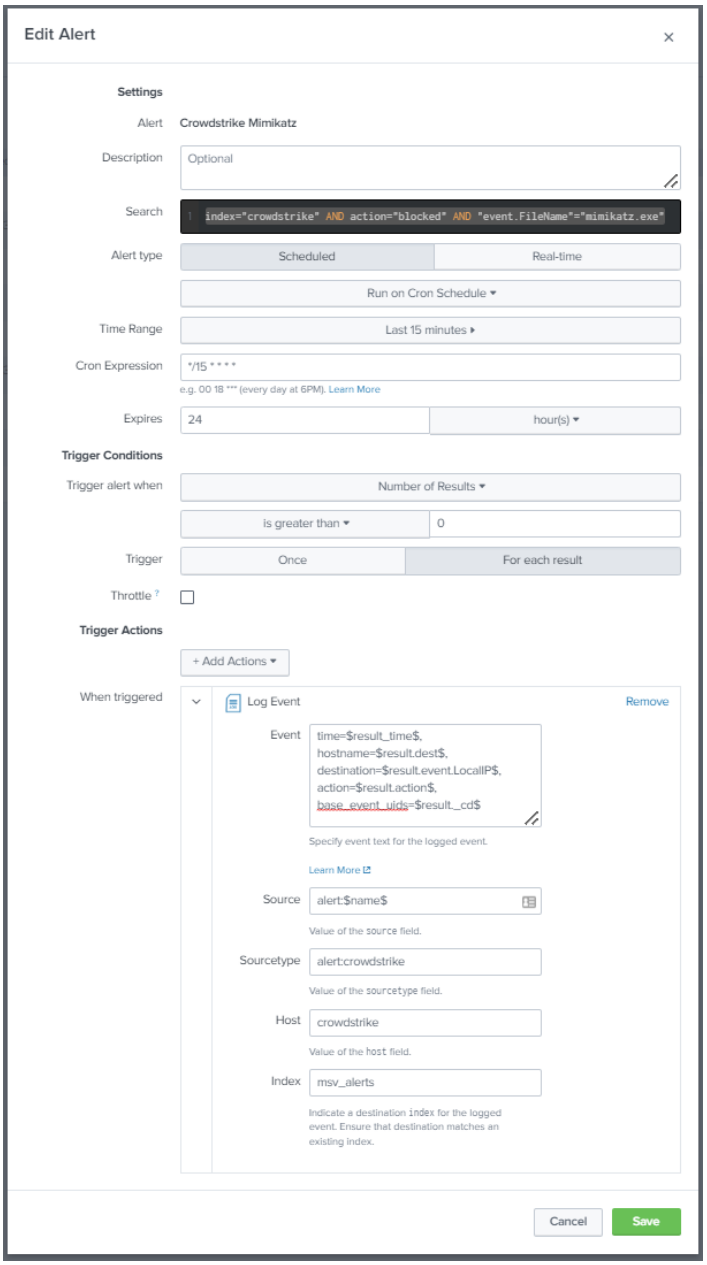
   h. **Trigger Actions**:
      i. **When triggered**: Log Event
      ii. **Event**: Do not hesitate to add other fields if necessary, but it is the basic information that is required. In particular, the `base_event_uids=$result._cd$` that will link to the base event for MSV to match it.

```
time=$result_time$,
hostname=$result.dest$,
destination=$result.event.LocalIP$,
action=$result.action$,
base_event_uids=$result._cd$
```

         - `$result.[field from source event]$` are the fields to match.

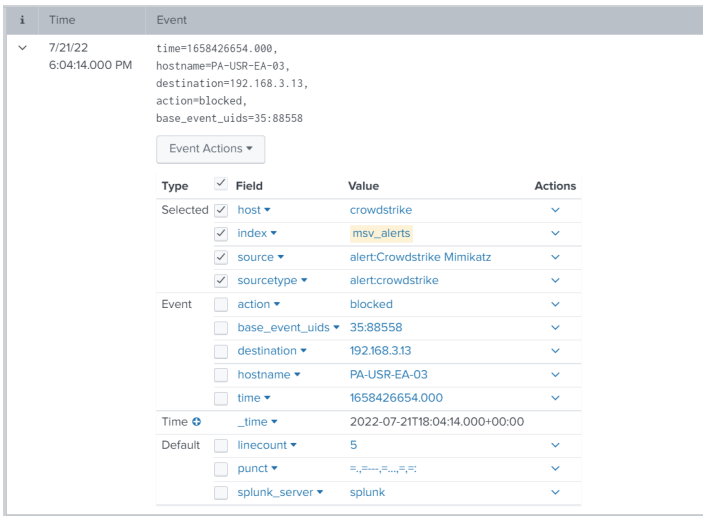
      iii. **Source**: `alert:$name$` The name of the event in the alert index
      iv. **Sourcetype**: `alert:crowdstrike` The source type of the event in the alert index

v. **Host**: `crowdstrike` The name of the Host in the alert index
vi. **Index**: `msv_alerts` The name of the index that was created in **Step 1**.



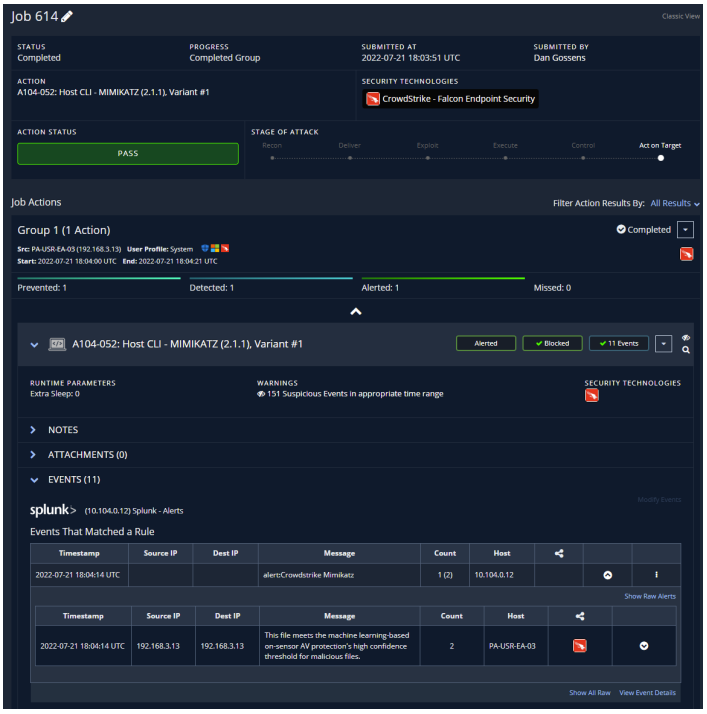
Splunk Edit Alert

For corresponding MSV setup, refer to the **enabling Correlation Query** section. The following is an example of an alert that has been triggered:



Splunk Triggered Alert

The Action which triggered this alert:



Action for the Alert

Add the Splunk 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**.
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 Security 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.

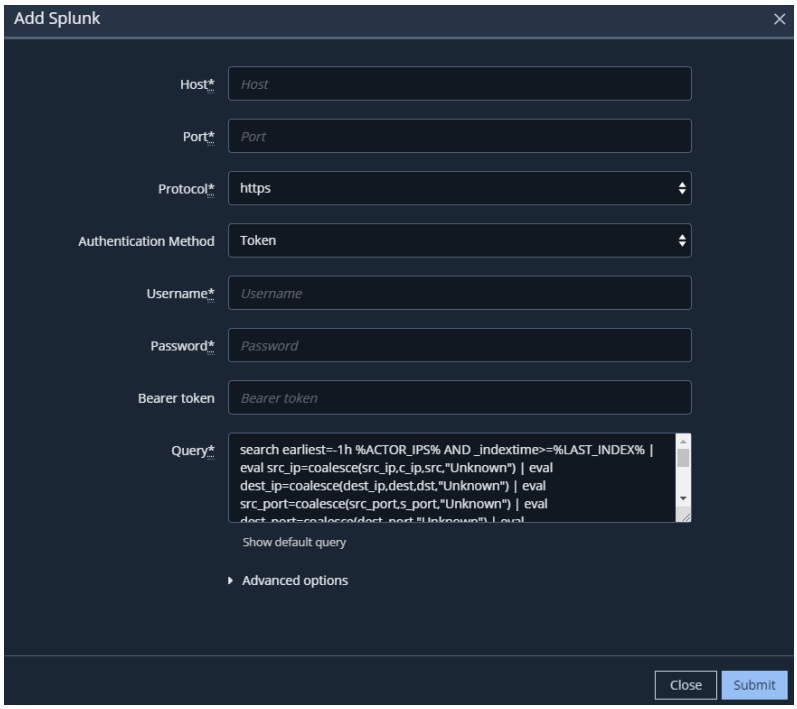
    > If you are using a load balancer, try using Token+Cookie for the authentication type. Otherwise, verify that the credentials are correct.

5. Review and update the **Query** to include instance-specific field names, sources, data types, and other customizations.
   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 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) 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.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
10. (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 substitutes the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

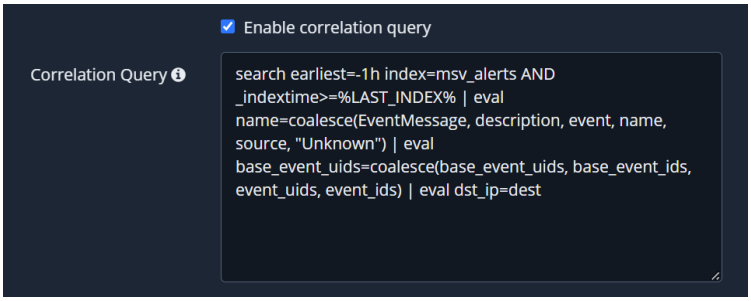
11. (Optional) Select **Pre-Process Event Correlation**.
12. (Optional) Select **Enable correlation query** and fill in the pertinent information from the alert that was created in Splunk to set up MSV to search for the Splunk alerts.

> Correlation queries let the Security Validation Platform recognize Splunk summary indexes as alerts in Job Action results. To build and use a Correlation Query on the platform, you must have a summary index. Correlation alerts populate this summary index. Use the name of the index in the integration's Correlation Query.
>
> In the index, each row must contain a property for base event UIDs. The property should be an array of _cd values from the base events to which the alert is correlating.
> _cd is an internal property to Splunk and does not show up by default, but it does exist by default in every index row. If your base_event_uids are stored as a string separated by commas, you can split your query by adding ' `| eval base_event_uids = split(base_event_uids, ",")` ' to the end of it. See the **Splunk documentation (https://docs.splunk.com/Documentation/Splunk/8.1.0/Knowledge/Setupsummaryindexes)** for information on creating summary indexes.

- In the Correlation Query, replace CHANGE_ME_CORRELATION_INDEX with the name of your populated index in Splunk.

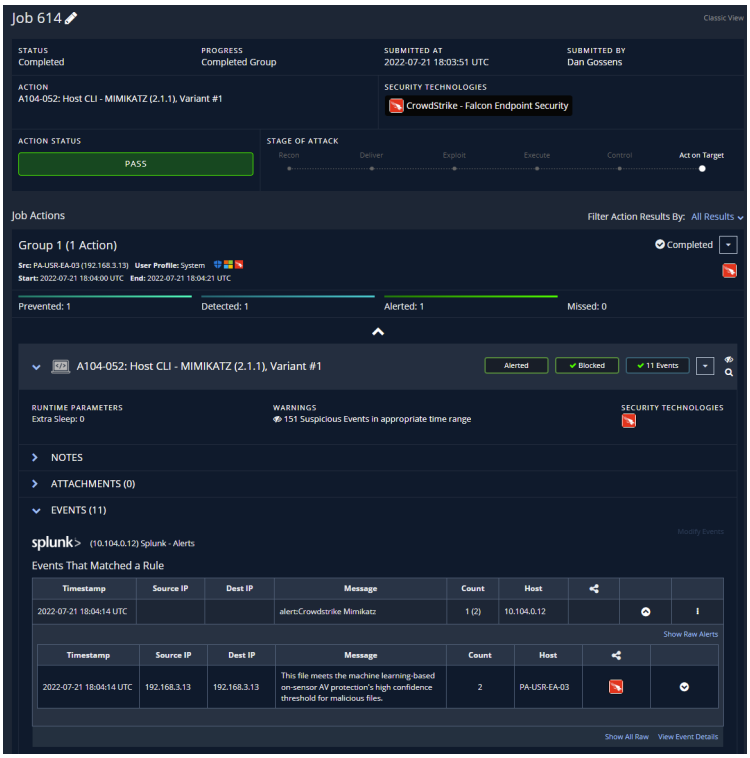
> See **Correlated Events (https://docs.mandiant.com/home/correlated-events)** for information about how the Security Validation Platform matches correlated events to a Job Action.

> For further assistance configuring the Correlation Query to work with a summary index, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.



Correlation Query

- After the 15-minute runtime, you see that the alert correlated to the original Action run.



Correlated Action

13. (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.
14. (Optional) Select **Discover network devices automatically**.
15. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
16. (Optional) Assign a **Name**.
17. (Optional) Choose **Yes** to save suspicious events.
18. Click **Submit**.

Splunk 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)**.

Verify Connectivity to Splunk

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 when running the test, a message identifies the specific cause of the error, helping to identify 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.