Mandiant

UNDERSTANDING JOB RESULTS

When Actions, Sequences, Evaluations, or Monitors are run, they become Jobs. You can view Jobs and their results in a number of ways.

You can also generate HTTP/HTTPS or syslog notifications to send to a specified destination that ingests machine data, such as Splunk or Elasticsearch, by selecting the Notification Formats menu option.

You can access these Job features by going to the Jobs menu on the navigation bar.

The Validation Platform supports parallel Job execution, with the following limitation:

- When an Actor is involved in multiple Jobs, the Jobs will be queued in the order they are received.

This limitation means any Actors queued for Job one will be unavailable to Job two until Job one is complete, therefore queuing all Job two Actions. Jobs may contain one or more Job Actions, which involve up to two Actors.

The Job Results provides information on how your security controls handle tests based on **Actions** (https://docs.mandiant.com/home/msv-actions), **Sequences, and Evaluations** (https://docs.mandiant.com/home/msv-sequences-evaluations). The information is displayed in three main sections:

- **Job Overview**
- **Group Details**
- **Action Details**

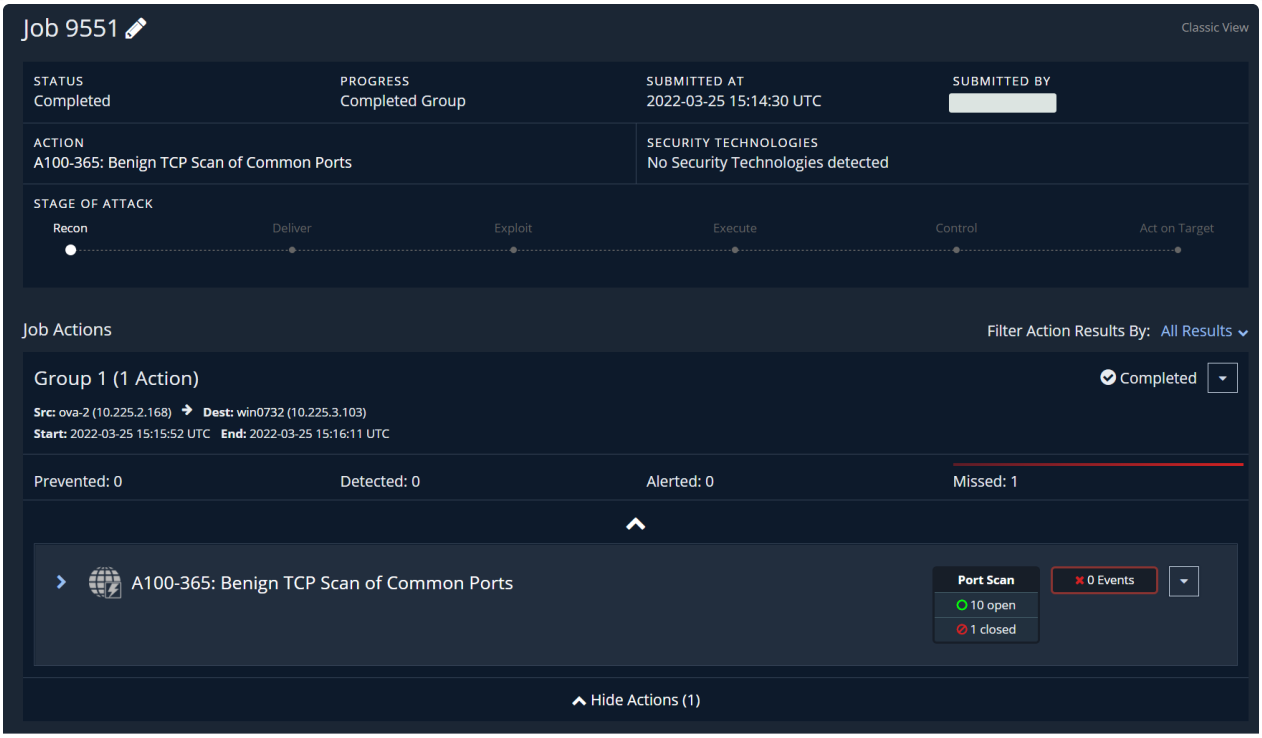
To help you understand your Job results, this article provides overviews and details about the information available within each section.

For more information, see the following Job Result Tasks and Features articles:

- **Adding Notes and Attachments to Jobs** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs)
- **Viewing Events** (https://docs.mandiant.com/home/viewing-events)
- **Printing the Job Results** (https://docs.mandiant.com/home/printing-the-job-results)
- **Viewing Job Debug Results** (https://docs.mandiant.com/home/viewing-job-debug-results)

NOTE: The Job Results page was updated in version 4.3.0.0. If you need to access the previous version for any reason, use the **Classic View** link. Information for that view can be found in **Understanding Job Results - Classic View** (https://docs.mandiant.com/home/msv-understanding-job-results-classic-view).

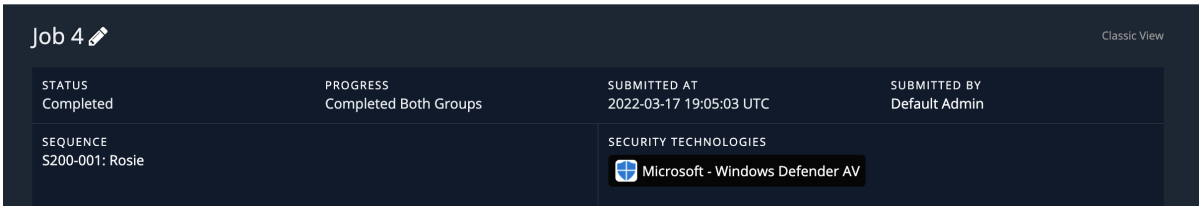
Job Overview



Job Results

The Job Overview section contains general information about the Job. This includes:

- Job ID/Name
- Status
- Progress - If the Job is still running, errored, completed, etc.
- Time the Job was submitted and by whom
- Name (and VID if applicable) of the Action, Sequence, Evaluation, or Monitor that was run
- Security technologies seen (that had events fire) when the Job ran



General Details for the Job Results

- Job Results
  - For Jobs that contain a Sequence or Evaluation, you see three interactive charts: Status by Action, Summary of Results, and Stage of Attack

Job Results charts for a Sequence

- In the Status by Action, Port Scan Actions are excluded from pass/fail but are reflected in a slice in the donut chart.
- Following the Stages of Attack bar chart, you see the number of Port Scan Actions that were excluded from the results.

- For Jobs that contain a single Action, you see a list of possible Stages of Attack with the stage associated to the Job highlighted. The summary results aren't shown here because they duplicate information shown in the Group details.

Job Results for single Action

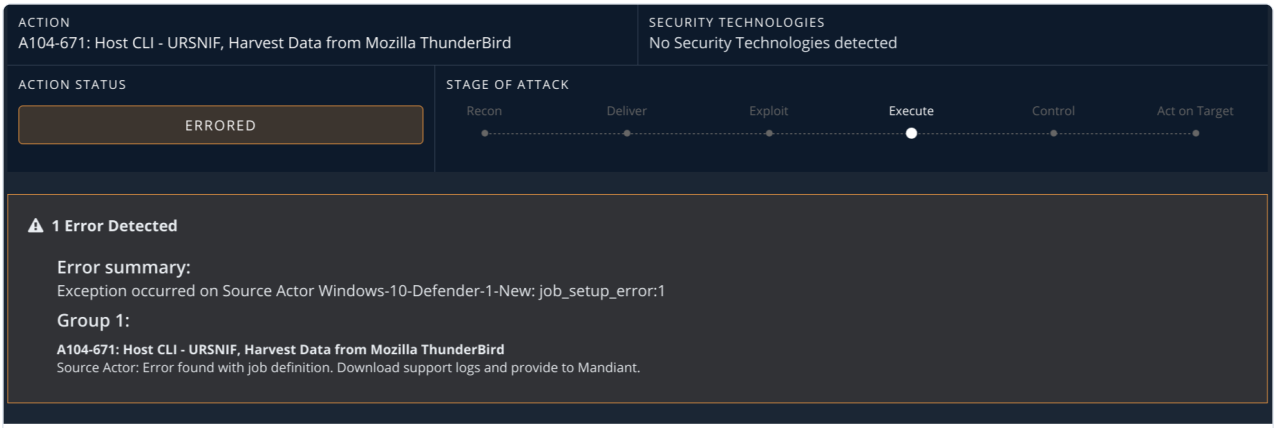
If you look at the Job Results header, there are actions you can complete regarding the entire Job. These actions include:

- Exporting the Job Results
- Navigating to the other Job Results

Job Results page menu

Viewing Reason for Job Failure or Error

When a Job fails, you see **Action Status** as *ERRORED* along with messages indicating the reason or reasons for the failure. These messages provide assistance with troubleshooting failed Jobs.



Job Failure Message

Group Details

Each Job Results has one or more Groups, which will have one or more Actions. The list of the Actions in a group is collapsed by default. Information that is visible by default includes:

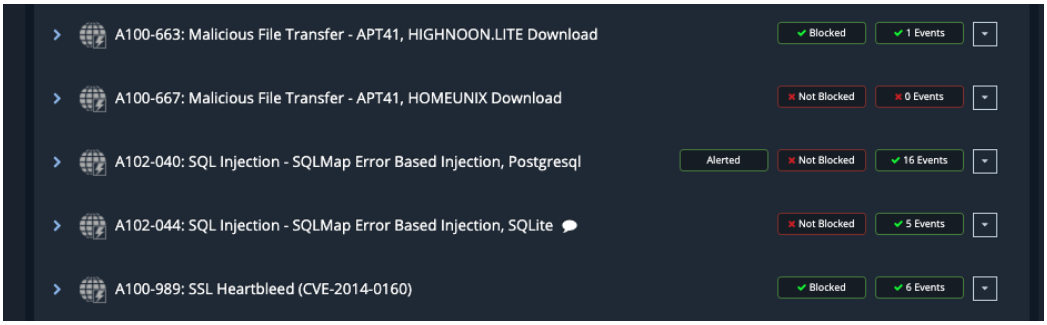
- Group Name and count of Actions
- Group completion status
- Actor or Actors assigned to the Group and any security technologies installed on those Actors

> If you are watching the results populate as the Job runs, you may notice the source and destination addresses update at the end of the Job. When an Action is running, Security Validation only knows the Actor Interface addresses. Security Validation might also know the destination address that the source needs to use, such as when an AWS Actor is behind a NAT in AWS so its NIC IP is different from the external IP you use to reach it. In cases where the source Actor is going through a NAT, Verodin doesn't know the external address of that NAT until the destination Actor sees it and returns its info upon completing the Job Action.

- User Profile or Friendly Name used for the Group (when applicable)
- The language if it is not English
- Start and end times, which may differ from the Job Submitted time
- Security Technology icons for the security technologies that detected the Job Actions in that Group
- Prevented, Detected, Alerted, and Missed overview

Alert Flags

When an alert is generated against an Action, an alert flag displays on the Job Status page, next to the Blocked / Not Blocked boxes. This indicator makes it easy to see which Action generated the alert, without having to search through all of the events.



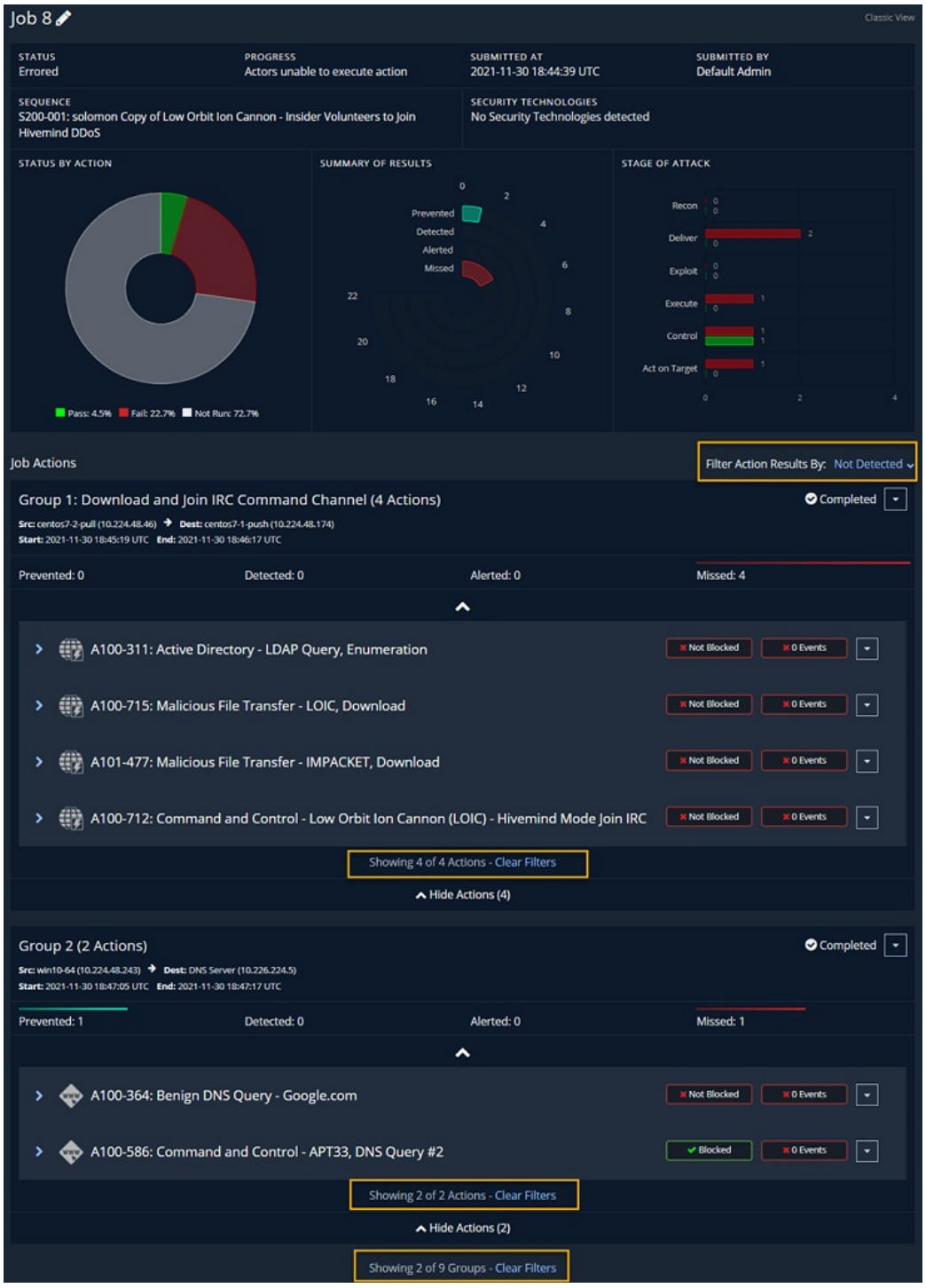
Alert Flags on Job Status Page

You can filter the displayed Job results by result type using a drop-down list in the Job Actions area. This filter drop-down list includes the following filtering options:

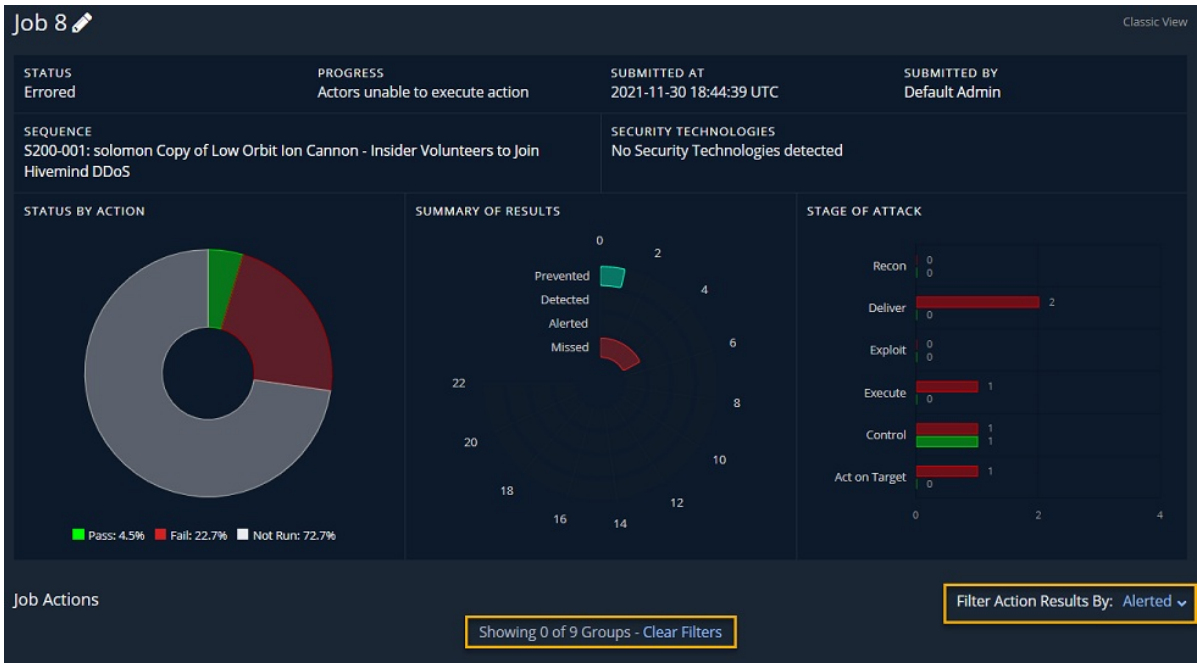
- **All Results** (select this option for no filtering)
- **Not Alerted**
- **Not Detected**
- **Not Prevented**
- **Prevented**
- **Detected**
- **Alerted**
- **Missed** (this result type indicates that Job Actions were not prevented AND not detected AND not alerted AND not errored)
- **Errored**

> All of the result type filtering options should not include Job Actions that have not completed, such as those that are actively running, have a "not run" status, or are in a queue to be run.

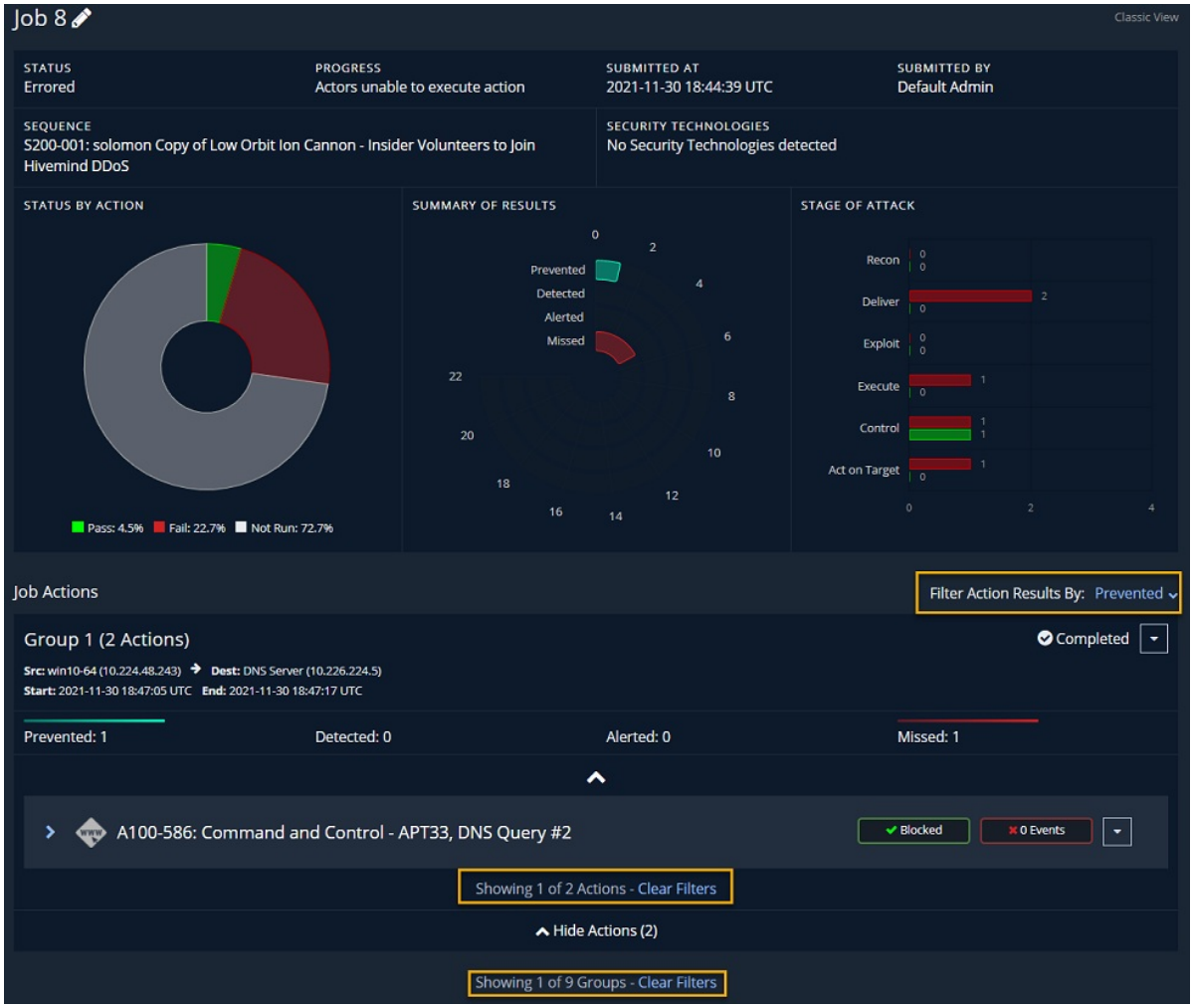
When you apply these filters, the Job Actions in each group display by result type.



Results of the Not Detected filter



Results of the Alerted filter



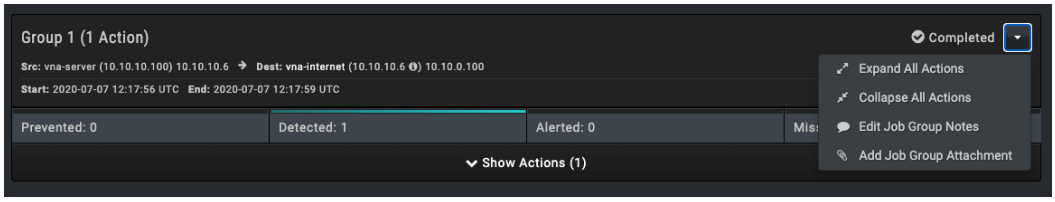
Results of the Prevented filter

When you apply a result type filter, the following displays below each list of Actions and Groups:

- Showing `X` of `Y` Job Actions/Groups (for example, Showing `2` of `2` Actions/Showing `2` of `9` Groups)
- **Clear Filters** (this is a link that resets to the All Results filter)

An expandable menu to the right of the Group completion status lets you:

- Expand all Actions
- Collapse all Actions
- **Edit Job Group notes** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs#Job)
- **Edit Job Group attachments** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs#Job2)



Job Group heading expandable menu

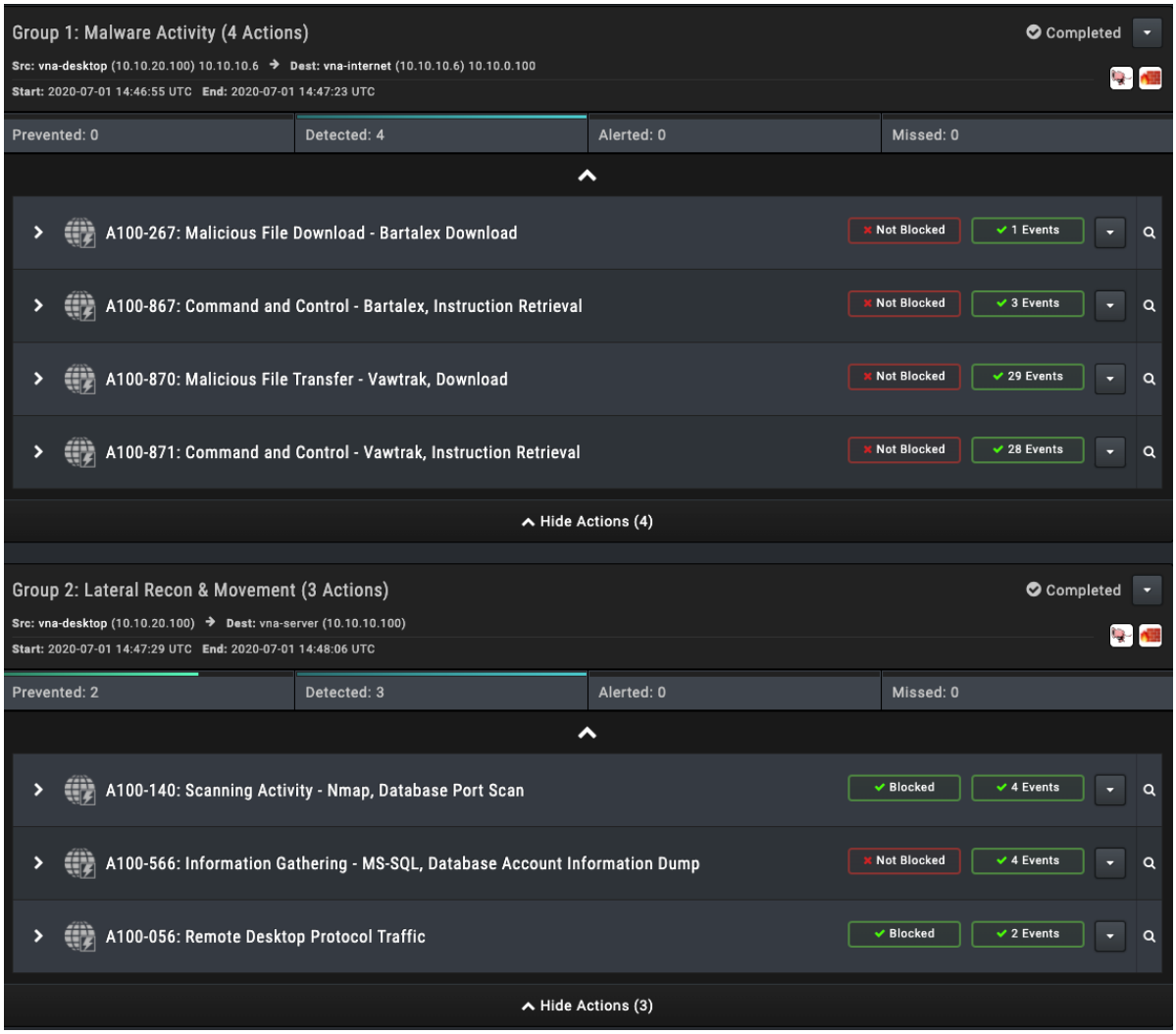
There's also a Show Actions option which will expand the Group to display basic Action information for each Action in the group:

- Action VID and name (can be clicked to view the Action details)
- Blocked cell that shows Blocked / Not Blocked /Alerted
  When the Action is blocked, hovering over the cell provides additional details.

  > DNS Actions are marked as blocked if they timeout during Job execution.

- Events cell that indicates the detection information, which either shows 0 Events or a Count of Events
  - When there are Events, this cell can be clicked to see the event details.
  - The outline of the cell changes color based on status: **blue** - event timeframe is open, **green** - events fired, **red** - no events
  - While the event matching timeframe is active, hovering over the cell displays how much time remains in the event timeframe
- An Info cell, which may have icons and buttons (see **Action's Info Cell** for more details)

The Group level also includes an option to expand or collapse all Action details.



Jobs Group heading

Action's Info Cell

Each Action has an Info Cell. This cell is located to the right of the Action menu. contains details for the icons and buttons you may see in this cell.

Job Action Info Icons

Icon	Title	Description
	Suspicious Events	If events were logged that might match the Action but could not be 100% related. When an event cannot be matched to a Job Action, a Suspicious Event is logged.
	Debug	A magnifying glass to view the Action logs, when they are available The magnifying glass will only appear if you have enabled Show Debug Links for Jobs (option is listed in User Preferences, access by going to **User** > **User Preferences** or if ?debug is added to the end of the job results url.

Icon	Title	Description
⚠	Block page - no block rule	A clickable triangle to indicate if there was a Block HTTP page that came up and if there is a Block rule in place for that page. The triangle is yellow if no block rule, white if there is a block rule.
⚠	Block page - block rule	

Action Details

Each Action in a Group can be expanded to show additional information about the Action and the Job results for that Action. When the Action is expanded additional details are displayed. When applicable, there is a section that provides the following Job details:

- Runtime parameters tied to the Job Action
- Security technologies that detected the Job Action
- Proxy used
- Email addresses used
- Host CLI variables (when applicable)
- Warnings generated when the Action ran (such as a Suspicious Events warning you can click on to jump to the Suspicious Events page).

After this static section, there are two types of expandable sections: information about the **Job Action results** and information about the **Action** itself.

Job Action result sections

- **Events** (https://docs.mandiant.com/home/viewing-events)
- **Port Scan Results** (when applicable)
- **CLI Log Output** (when applicable)
- Protected Theater Screenshots (when applicable)

  Actions that are run as System or use Bash Shell do not have screenshots.

  This section opens a new window and cannot be included when printing the Job Results.

- Conversations (when **Pull Connection Log for Protected Actor** is enabled in the Protected Theater settings)

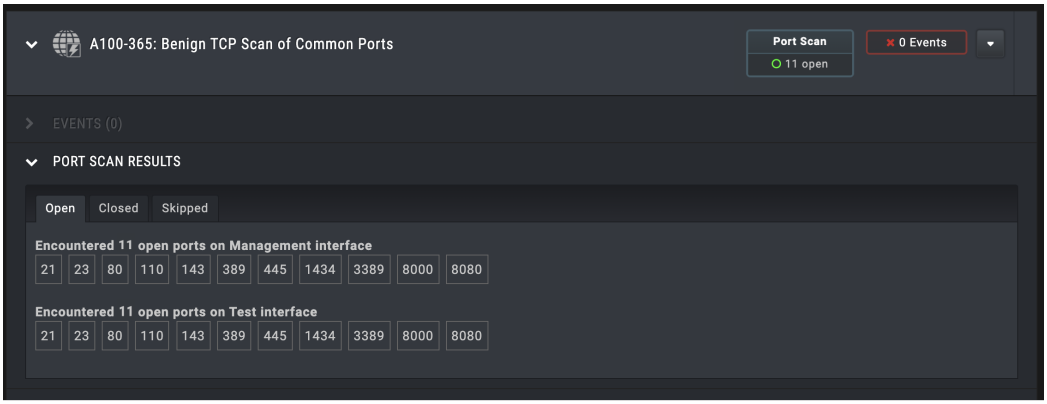
  This section opens a new window and cannot be included when printing the Job Results.

- **Email Log** (when applicable)
- **Captive IOC Results** (always displays for Captive IOC URL Actions and displays for Captive IOC PCAP Actions if the safe URL check fails)

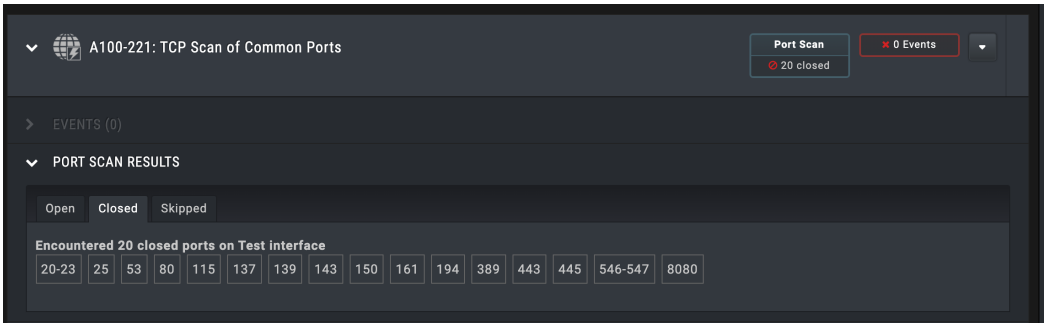
Port Scan Results

The Port Scan Results section shows Ports that were Open, Closed, and Skipped in separate tabs. Each tab includes areas

for each interface that was tested.



Port Scan results



Port Scan Results - multiple interfaces

Host CLI Action sections

When a Job includes a Host CLI Action (and some Protected Theater Actions), there are specific sections included:

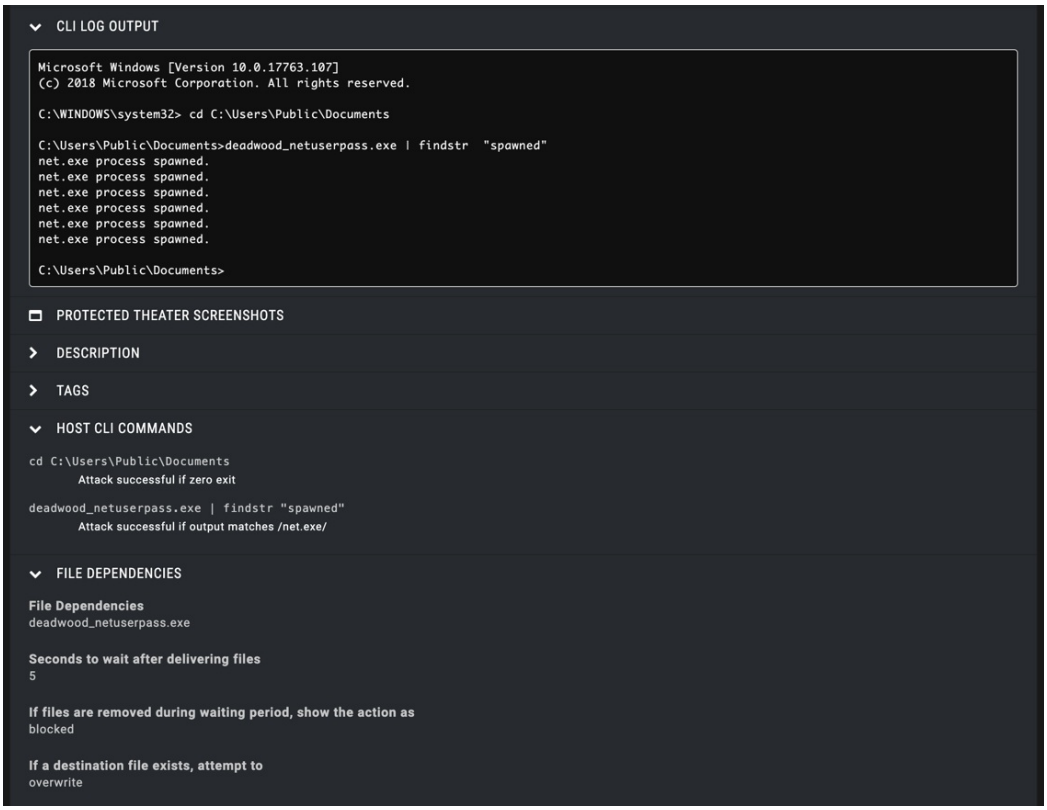
- Host CLI Commands: Lists the commands included in the Action and information for handling those files when the Action runs.
- CLI Log Output: Documents what occurred on the system when the Action ran.

  If you are running Host CLI Actions on a Windows environment where a double-byte character language is the primary language, you may see that the CLI Log Output may not display correctly. Enabling the **Host CLI Actions - Force Windows Code Page to English** advanced setting will resolve the issue and force command outputs to display in English. This ensures that the Job Results for these Actions are accurate after being processed by Security Validation. See Advanced Settings in the Security Validation *Admin Guide* for more information.

- File Dependencies: Lists files that are part of the Action and information for handling those files when the Action runs.

  This section is available for all file-based Actions.

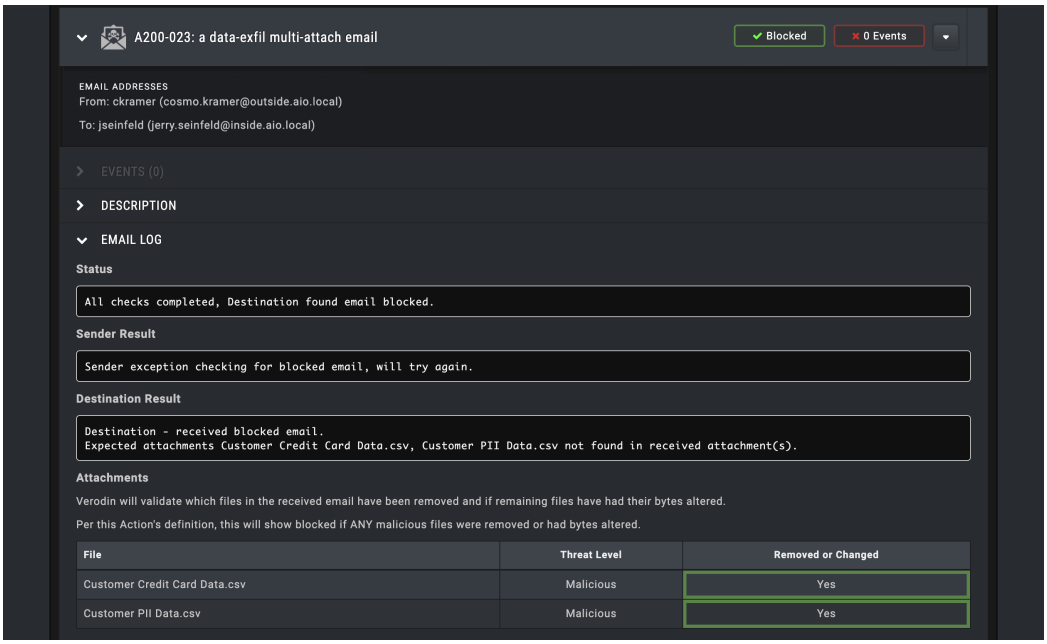
Having this information together in the Job makes it easy to share the results with other departments and analysts if the Job results aren't what is expected or if you are trying to optimize your security controls.



Host CLI sections for a Job

Email Log

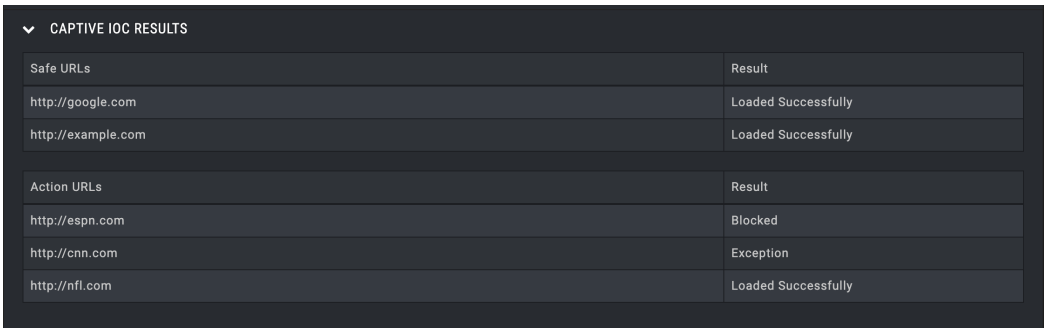
The Email Log section provides an overall status, Sender and Destination results, and details on what happened to attached files.



Email Log section for a Job

Captive IOC Results

The Captive IOC Results section displays for Captive IOC URL Actions and Captive IOC PCAP Actions if the safe URL check fails. This section may contain two tables: Safe URLs and Action URLs. Each table provides details on what occurred with the URL when the Action ran.



Captive IOC Results section for a Job

Action detail sections

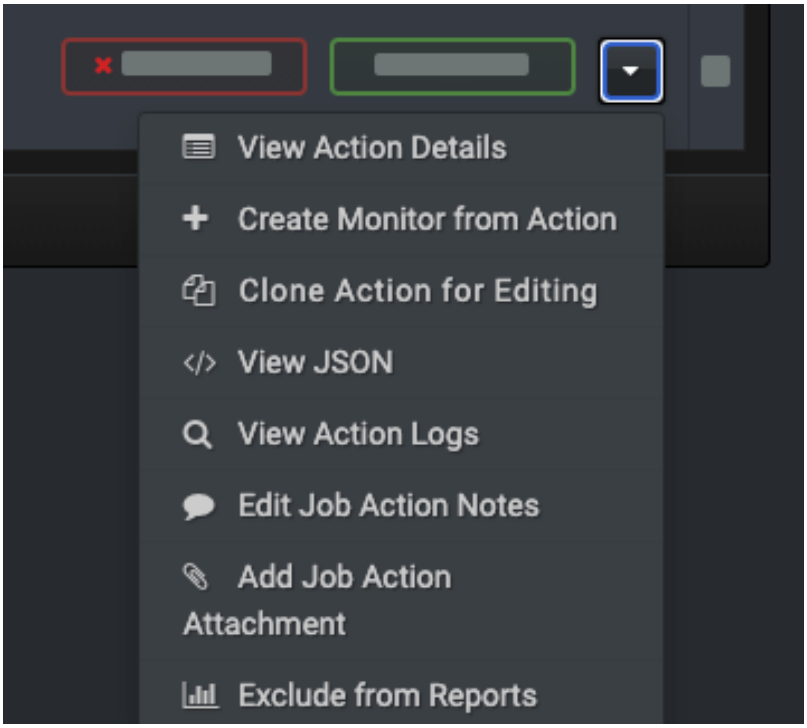
- Description
- Tags
- Dimensions
- Action-type specific sections (**Host CLI Commands, File Dependencies**)
- **Job Notes** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs)
- **Job Attachments** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs)
- Common Detection Alerts
- **PCAP Captures** (when applicable)

There is also an expandable Action-specific menu to the right of the Blocked / Not Blocked status and count of Events generated. For each Action you can:

- View the Action Details
- Create a Monitor (refer to **Monitors / Advanced Environmental Drift Analysis (AEDA)** (https://docs.mandiant.com/home/monitors-advanced-environmental-drift-analysis-aeda) for more information)

  If a Job Action has been disabled, this option does not appear.

- Clone the Action
- Edit the Action (user-created Actions only)
- View the JSON for the Job Results for the Action
- View the Action logs (when debug is enabled)
- **Manage Job Group notes** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs#Job)
- **Manage Job Group attachments** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs#Job2)
- Exclude the Action from reporting



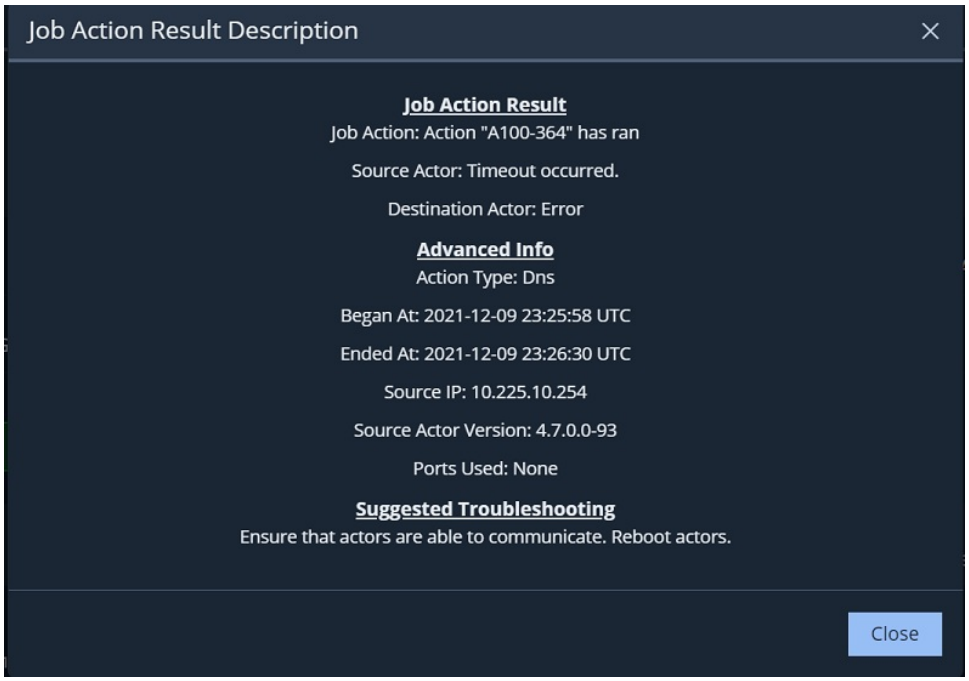
A Job Action's expandable menu

Viewing Action Summary for Blocked / Not Blocked Status

You can view additional information about why an Action resulted in a Blocked or Not Blocked status by clicking the green Blocked / red Not Blocked status box.

TO VIEW ACTION SUMMARY FOR BLOCKED / NOT BLOCKED STATUS

1. Go to **Jobs** > **Job Status**.
2. In the Jobs Status list, locate the Job for which you want more detailed information for Blocked / Not Blocked status.
3. In the Job Actions area, locate the Action with the Blocked / Not Blocked status you want to view and click the box for Blocked / Not Blocked.
   A pop-up description box displays that contains detailed information about why the Action was blocked or not blocked.

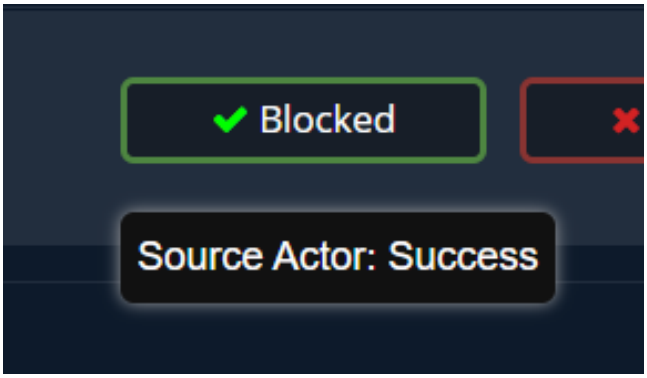


Job Action Description

From this pop-up you can see information about why an Action was blocked or not blocked, such as:

- Why it was blocked / not blocked
- Time the Action was run
- md5sum mismatch - file wasn't in the same form on one side or the other
- Password for an email account expired
- Connection was refused
- Connection was reset

When you hover your mouse over the Blocked / Not Blocked status box, a tooltip shows the job result status, as shown in the following figure.



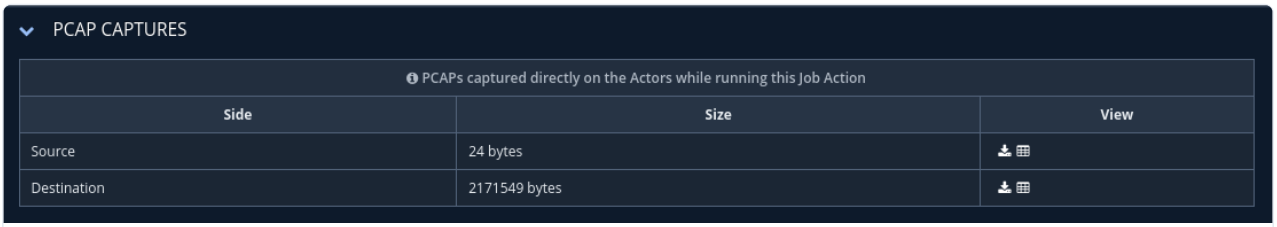
Blocked Status Tooltip

PCAP Captures

When you run a network Action with **PCAP Capture Enabled**, the results appear in this section. You see where the traffic originated and terminated, and the size of the packets. You can download the PCAP report for offline viewing or open it using the built-in viewer.

For PCAP captures to work, one or more Network Actors in the Action must be deployed as a virtual appliance:

- For a PCAP capture from the source side, you need to select a Network Actor appliance as the source.
- For a PCAP capture from the destination side, you need to select a Network Actor appliance as the destination.
- If you want PCAPs on both sides, a Network Actor needs to be selected for both source and destination.
- Endpoint Actors do not work with PCAP captures.



PCAP Captures in Job Results

Incompatible Status

When a Host CLI Action is requested and the script does not find the conditions necessary to continue the exploit, the Job is not run. Additionally, a status of Incompatible is reported within the Job Actions details. One example yielding this result would be running a Host CLI Action with an Endpoint Actor that is not supported by the Action.

Jobs identified as Incompatible are excluded from reports.