Mandiant

ACTION DETAILS IN JOB RESULTS

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)

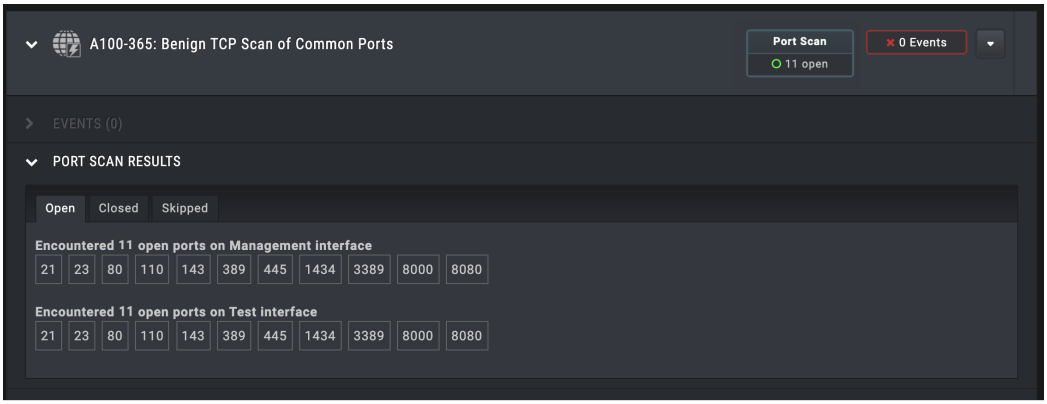
  

  This section opens a new window and cannot be included when printing the Job Results.

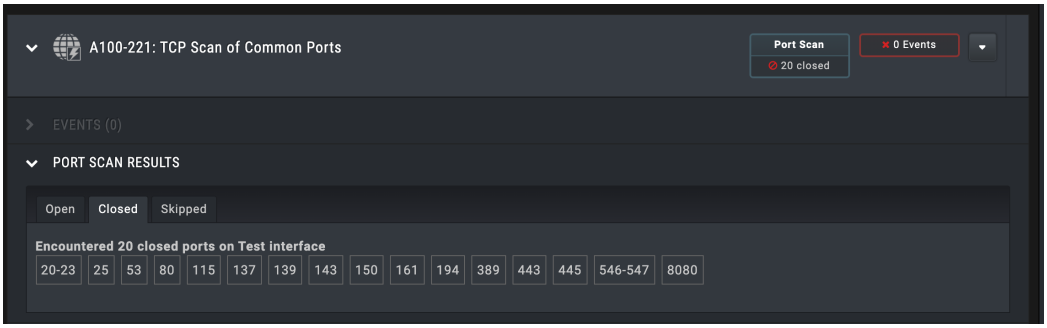
- **Email Log** (when applicable)
- **Captive IOC Results** (always displays for Captive IOC URL Actions and displays for Captive IOC PCAP Actions if the safe URL check fails)

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:

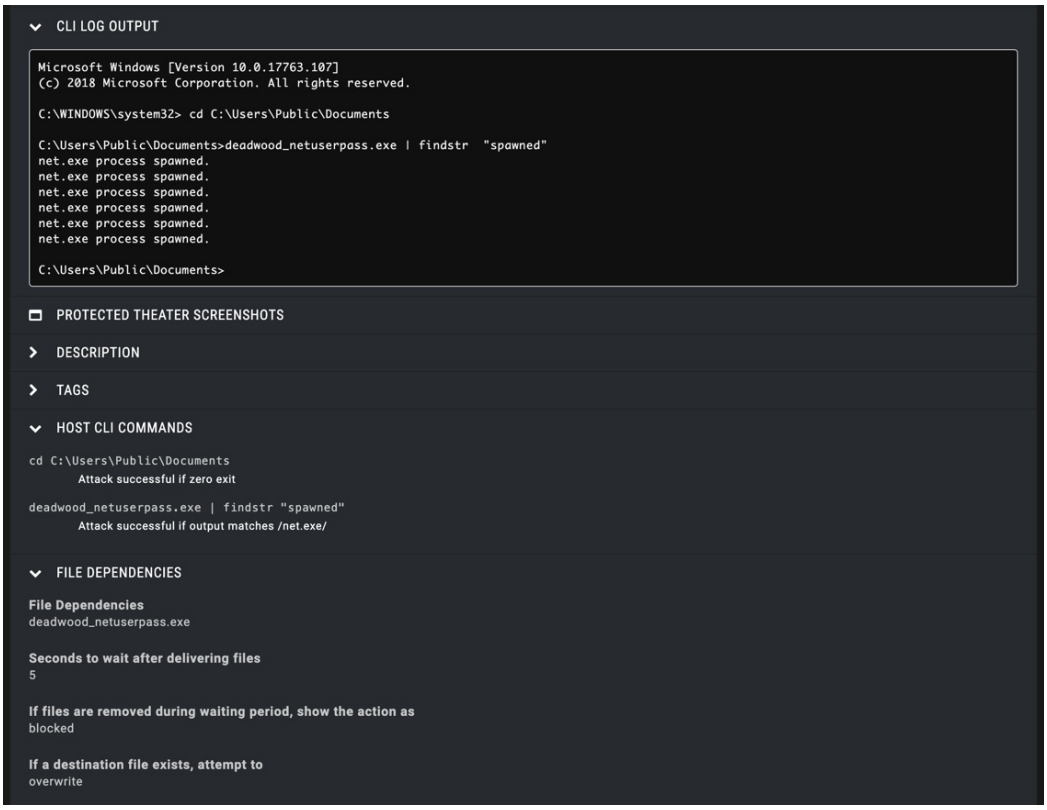
- Host CLI Commands: Lists the commands included in the Action and information for handling those files when the Action runs.
- CLI Log Output: Documents what occurred on the system when the Action ran.

> 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.

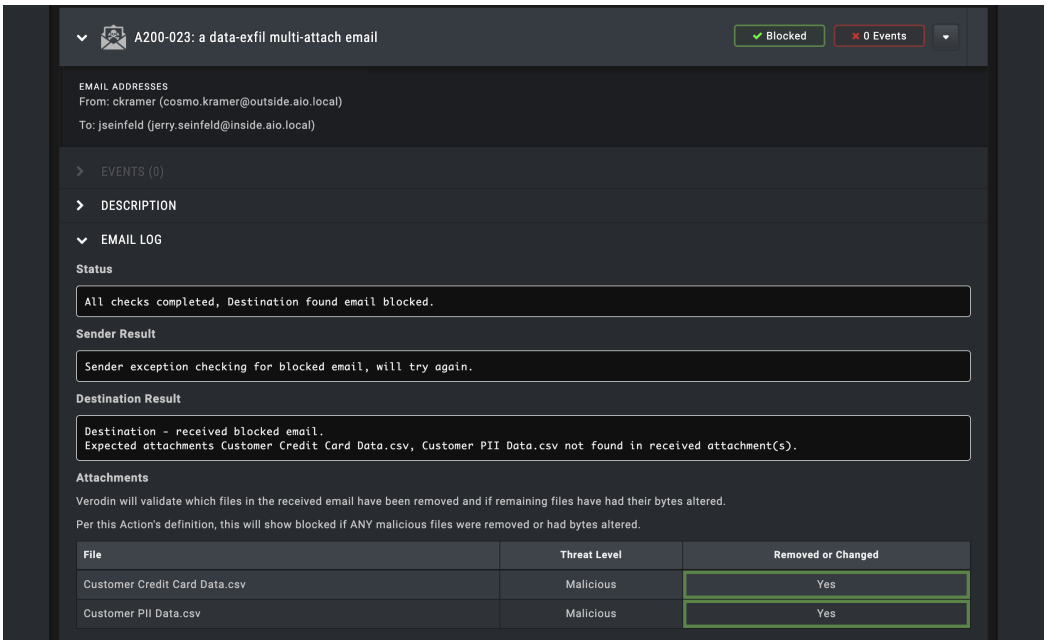
Having this information together in the Job makes it easy to share the results with other departments and analysts if the Job results aren't what is expected or if you are trying to optimize your security controls.



Host CLI sections for a Job

Email Log

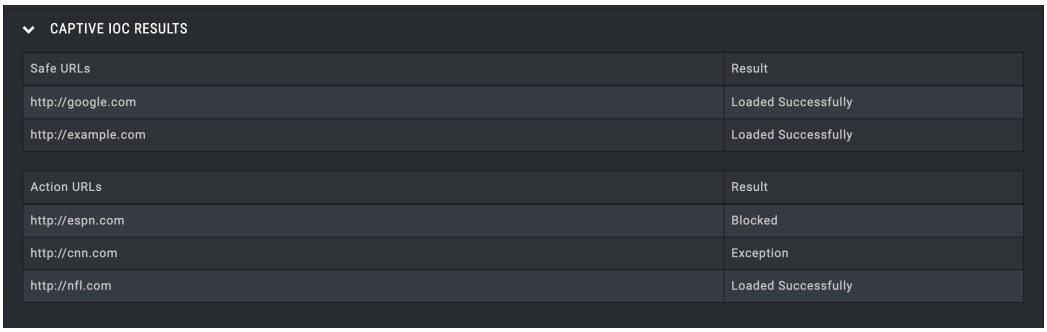
The Email Log section provides an overall status, Sender and Destination results, and details on what happened to attached files.



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

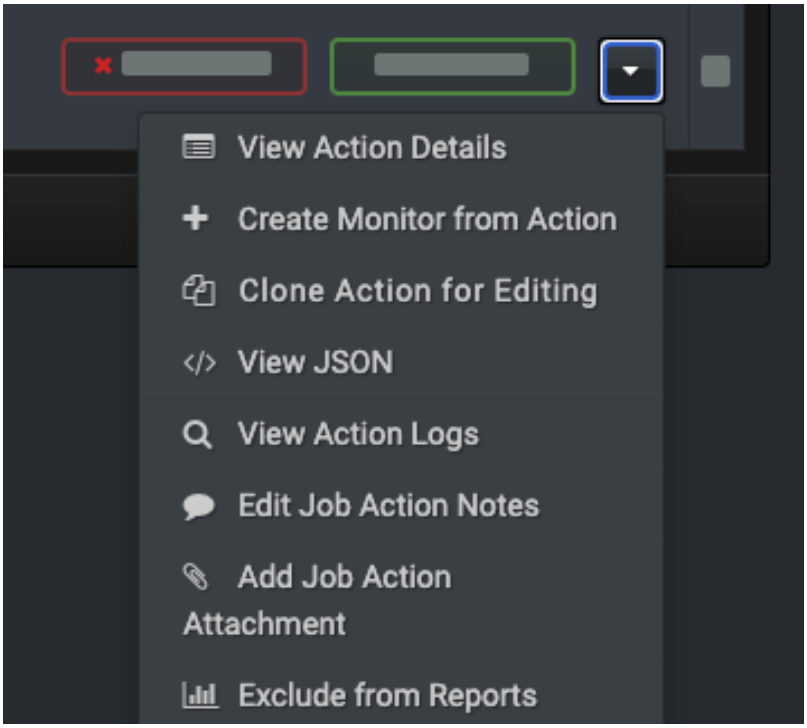
- Description
- Tags
- Dimensions
- Action-type specific sections (**Host CLI Commands, File Dependencies**)
- **Job Notes** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs)
- **Job Attachments** (https://docs.mandiant.com/home/adding-notes-and-attachments-to-jobs)
- Common Detection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



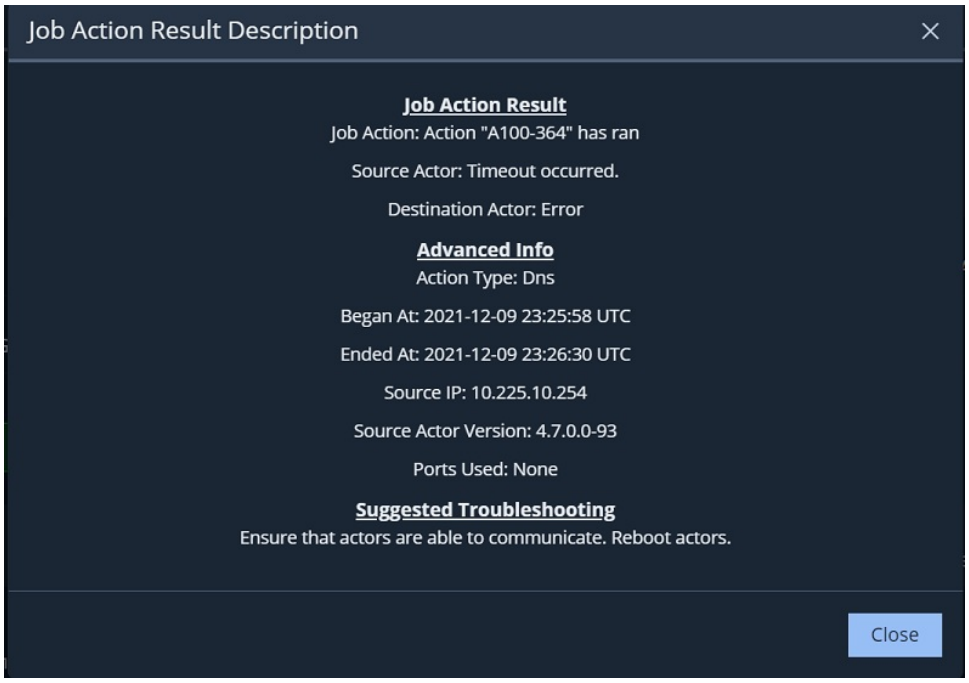
A Job Action's expandable menu

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.

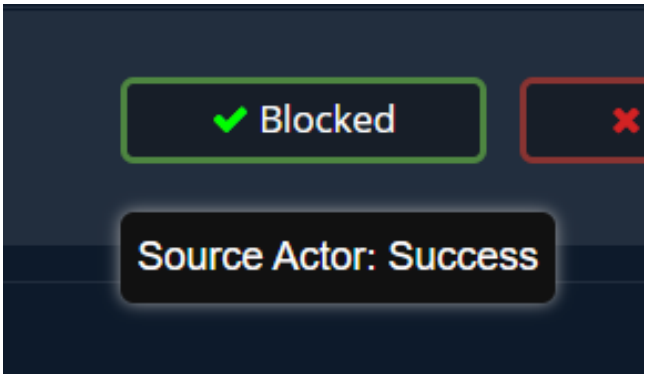


Job Action Description

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.



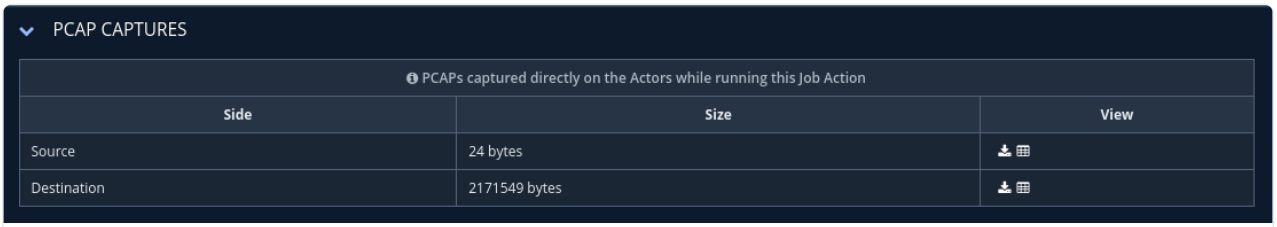
Blocked Status Tooltip

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.