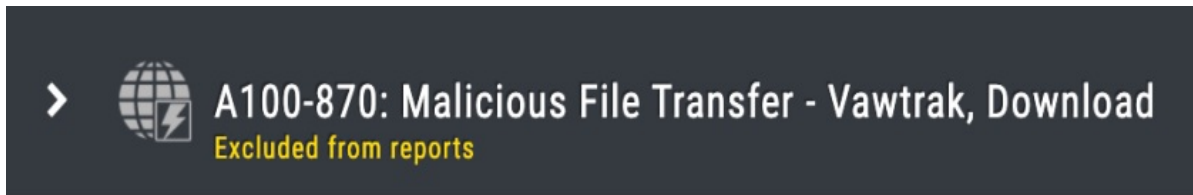


REASSIGN, SUPPRESS, AND DROP EVENTS FROM JOBS

Excluding Actions from Reports

When the Action menu is expanded, you can choose to exclude that Action from all reporting metrics if you have the Jobs - View permission. Excluded Actions still appear in Job Results and can be included in reporting again using the same menu.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b96445d5e3e714b3b87/n/action-excluded-from-reporting.png>)

An Action that has been excluded from reporting displays a message identifying its status

Reassigning, Suppressing, and Dropping Events



IMPORTANT: Reassigning, suppressing, and dropping events from Job Actions will impact the detected result and could impact the pass/fail result.

To improve the context already provided by automatic event attribution, you can suppress or drop events from a Job Action or relocate events to another Action in the Job. Using **Modify Events**, you can tailor a Job Results page to focus on a particular security technology's events, eliminate white noise, or correct a misleading automatic event attribution. For example, if you're configuring one of five security technologies, you could delete all events that weren't related to the security technology you're configuring.

If there are one or more events associated with a Job, the **Modify Events** option is available. When selected, you can select one or more events and then suppress them, drop them, or move them to a different Action.

Permissions required: Event - Edit permission, which is disabled for all Validation Platform User Groups by default.

EVENTS (26)

elastic (10.10.10.6) Suppress 2 Events Drop 2 Events Move 2 Events Cancel

Timestamp	Source IP	Dest IP	Message	Count	Host			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.10.6	10.10.0.100	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile	2	verodin-aiosnort			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.10.6	10.10.0.100	ET CURRENT_EVENTS Possible Malicious Macro DL BIN May 2016 (No UA)	2	verodin-aiosnort			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.20.100	10.10.10.6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile	2	verodin-aiosnort			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.10.6	10.10.0.100	ET INFO Executable Download from dotted-quad Host	2	verodin-aiosnort			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.20.100	10.10.10.6	ET CURRENT_EVENTS Possible Malicious Macro DL BIN May 2016 (No UA)	2	verodin-aiosnort			
<input type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.20.100	10.10.10.6	ET INFO Executable Download from dotted-quad Host	2	verodin-aiosnort			
<input checked="" type="checkbox"/> 2020-07-01 14:22:33 UTC	10.10.20.100	10.10.0.100	GET http://10.10.0.100:80/system/logs/k1.exe HTTP/1.0	2	verodin-aioprivoxy			

[Show All Raw](#) [View Event Details](#)

Selecting Events to remove or move to another Action

Reassign events between Actions

1. Expand the Events section in an Action.
2. Click **Modify Events** in the top right corner.
3. Select the events.
4. Click **Move <number selected> Events**.
5. Select a destination from the available list of Actions.
6. Enter the reason for relocating the events.
7. Click **Move Events**.

Move Integration Events ✕

You are about to move 1 events from **Job Action 59**, please select a destination Action.

Destination

Group 1: Malware Activity

- A100-267: Malicious File Download - Bartalex Download
- A100-867: Command and Control - Bartalex, Instruction Retrieval
- A100-870: Malicious File Transfer - Vawtrak, Download
- A100-871: Command and Control - Vawtrak, Instruction Retrieval

Group 2: Lateral Recon & Movement

- A100-140: Scanning Activity - Nmap, Database Port Scan
- A100-566: Information Gathering - MS-SQL, Database Account Information Dump
- A100-056: Remote Desktop Protocol Traffic

Group 3: PII Data Exfill

- A100-170: ICMP Tunnel-based Exfil/Upload of PII Data

Reason for Moving

Events assigned incorrectly

Cancel Move Events

Moving Integration Events from one Action to another

Suppress or Drop Events from Job Results

Events that are suppressed are still associated with the Job with the record being maintained in the database. Events that are dropped are removed from the database so specific event information will not be available.





1. Expand the Events section in an Action.
2. Click **Modify Events**.
3. Select the events.
4. Click **Suppress Events** or **Drop Events**.
5. Click **OK** when prompted. The events are moved from the Events to the appropriate tab in the Suppressed and Dropped Events table, as shown here.

Suppressed and Dropped Events

There were 32 Events suppressed or dropped for the Integration of this Job Action. [Hide Filtered Events \(32\)](#)

Matching events will be **suppressed: events will not be included in reports but are still stored. Change this setting on the [Integrations](#) page.**

Suppressed by a Rule (2) Dropped by a Rule (29) Dropped by User (1)

Integration where Host in Splunk - 10.10.10.7							
Timestamp	Source IP	Dest IP	Message	Count	Host		
2021-09-14 16:05:13 UTC	10.10.20.100	10.10.10.6	ET INFO Executable Download from dotted-quad Host [Classification: A Network Trojan was detected]	1	snort		
2021-09-14 16:05:13 UTC	10.10.10.6	10.10.0.100	ET INFO Executable Download from dotted-quad Host [Classification: A Network Trojan was detected]	1	snort		

Show All Raw

Suppressed and Dropped Events



If there are events you are suppressing or dropping from more than one Job, you may want to create an event filter rule instead. For full details on Event filter Rules, see [Event Filter Rules](https://docs.mandiant.com/home/event-filter-rules) (<https://docs.mandiant.com/home/event-filter-rules>).