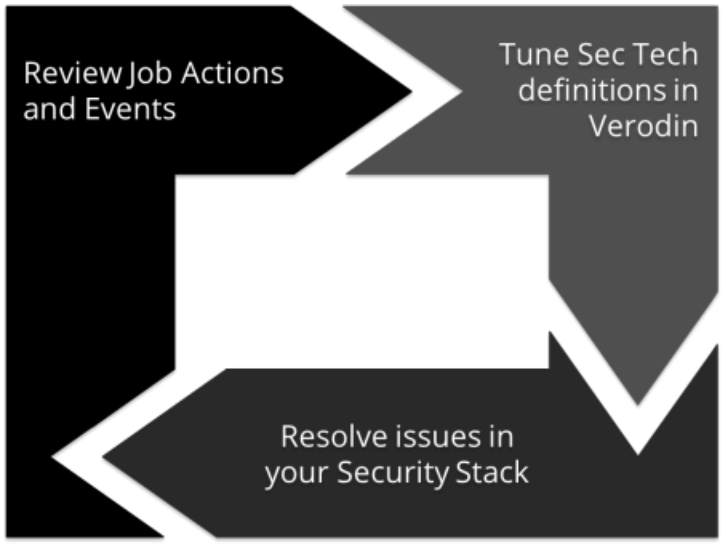
EFFECTIVENESS VALIDATION PROCESS (EVP) OVERVIEW

When Job Actions are not related to security technologies, you are not able to see the full security posture of your network. Part of Security Validation's Effectiveness Validation Process (EVP) is addressing this lack of visibility into the network and addressing these Actions. In general, the process is straightforward.



Workflow for handling Actions not related to a Security Technology

Use the process:

- As part of your initial implementation after running a base set of Security Content
- After you add new systems to your security stack
- At regular intervals, coinciding with your change control

This process helps you:

- Fine-tune the Validation Platform to help you instrument the entire defensive stack
- Identify correlation issues with your SIEM
- Identify missing information in Events
- Identify other configuration issues that may be present

Start the workflow from the Gauge page by selecting a gauge to view its details. Then expand the Unknown Security Technology Category (●●●) for Prevented or Detected. From here, click Analyze to open the EVP Workflow page.

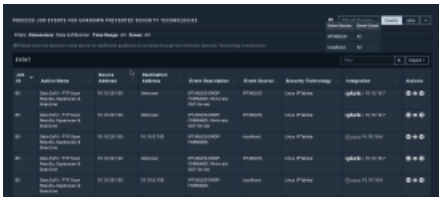
The EVP Workflow page has two Views; Process Job Events and Process Job Actions. The Process Job Actions view is similar to the standard Job Status page. However, these two views automatically filter the information, displaying:

- Job Actions and Events that have Actions that are not related to a security technology
- Job Actions and Events that are part of the dimension you have selected, either through the Gauge page or using the standard filter options available at the top of the page

Both Views include the standard filter, accessed from the top of the page. If you view the filter, the only dimension selected is the dimension of the gauge where you selected **Analyze**. The filter also includes the date and zone filters from the gauges. You can further filter this data, limiting the zones or shortening the time range, for example. Clicking **Reset**

Filter returns you to the initial filter, with one dimension selected and the initial time range and zones.

The Process Job Events View includes a Source Summary list that dynamically shows which Sources have Events that aren't related to security technologies. When you expand the list, it shows the specific sources and the count of Events not related to a security technology. Clicking a source automatically filters the list of Events to show only events from that source. If you use this filter option, return to the list and choose **Clear Filter** to show all sources again.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b89445d5e3e714b3b1b/n/mft-process-job-events.png)

Process Job Events page for Unknown Security Technologies

The Process Job Actions view can be further filtered to show only Actions with events, suspicious events, and with no events. All users can view these pages, including all available details regarding the specific Actions, blocked status, and Events. However, only Power Users and Administrators can complete any required tuning in the platform.

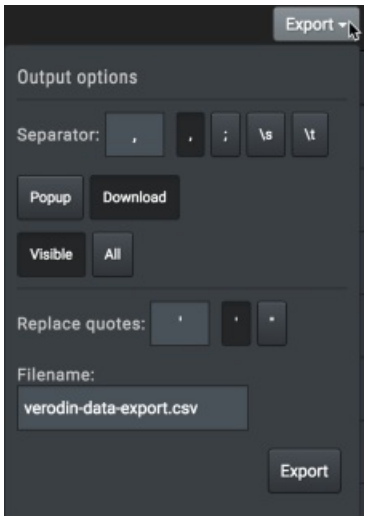
(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880bbb445d5e3e714b3c77/n/mft-process-job-actions1.png)

Process Job Actions page for Unknown Security Technologies with filter options

Both the Process Job Events and Actions pages have export to CSV capabilities. By default, the export downloads the visible rows using a comma as a delimiter but can be changed.

NOTE: Job Actions often have commas in the names. If you plan on working with the CSV file in a spreadsheet program such as Microsoft Excel, consider using the semicolon as the delimiter during export.

For best results, import your CSV file into Excel or similar spreadsheet program, confirm the delimiter (e.g., comma, semi-colon) and use single-quotation marks as the text qualifier during import.



Export Menu

When viewing the Events for a specific Action (on either the Process Jobs Action page or the Job page), you will now see a Security Technology column. This column shows the Security Technology that was identified or include the Add Security Technology icon. Hovering over the icon provides additional information about the Security Technology and displays the prevention configuration. Clicking the icon displays the Create/View Security Technology page.

NOTE: The Security Technology icon or Add Security technology icon also appears next to each raw event. This allows you to populate the Create/View Security Technology form with the desired event when multiple events are grouped together.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b88445d5e3e714b3b19/n/mft-process-job-actions-events.png)

Event Details showing the identified Security Technology and prevention info

The Create/View Security Technology form allows you to:

- Create a new Security Technology definition
- View the definition for an existing Security Technology
- Add user-defined definitions for both prevention and detection
- View all available information for the Event you were viewing when you opened the page

There are two versions of the form; one for network security technologies and one for endpoint security technologies. The version of the form controls which security technologies appear in the list and determines if you can add both Discovery and Prevention rules (Network) or Prevention only (Endpoint).

When viewing an existing Security Technology, the JSON information that you would see in the Security Technology Settings page is pulled in. Security Technology rules you add using the form can be viewed, changed, and deleted on the Security Technology Settings page.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b79445d5e3e714b3ab7/n/create-view-sec-tech-palo-network.png)

The Create/View Security Technology form showing Network technology

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880b79445d5e3e714b3ab5/n/create-view-endpoint.png)

The Create/View Security Technology form showing Endpoint technology

NOTE: Discovery for Endpoint Security Technologies is not configured based on a field and value pair in the event. Currently the discovery can only be set up using the Security Technology setting page by adding the information directly to the json.