WORKING WITH UNCATEGORIZED PREVENTED ACTIONS

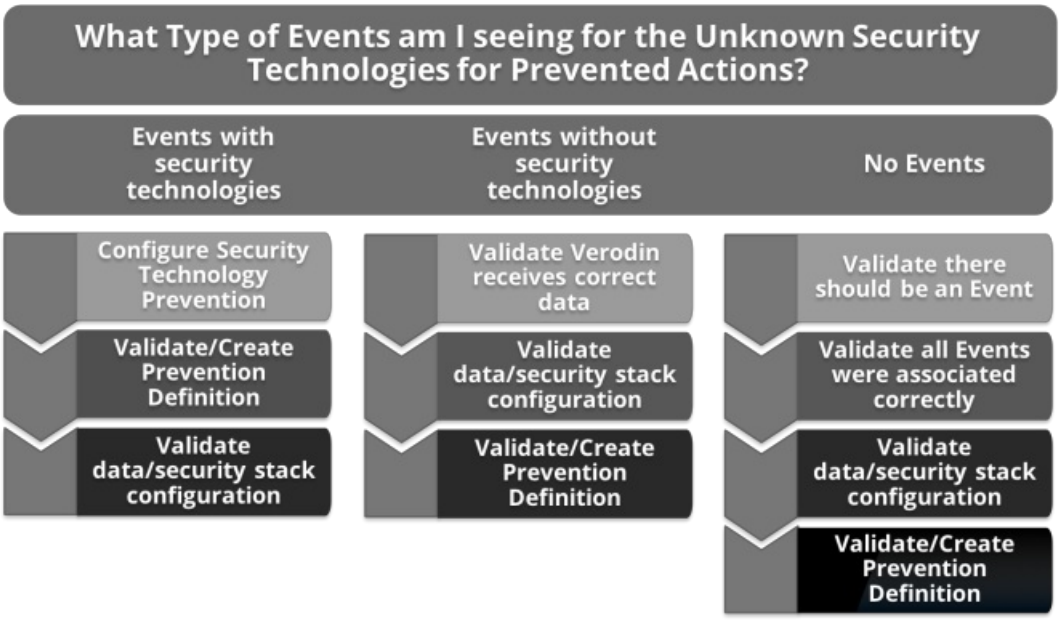
There are many reasons why the Validation Platform may have Job Actions that were prevented but not tied to a specific Security Technology:

- The security technologies may be configured to not generate events when an Action is blocked
- The default security technology definitions in the Validation Platform do not contain the necessary information to allow the integration to identify the security technology
- There may be configuration issues that prevent an event from being related to a Job
- There may be configuration issues in the security stack that prevent events from being generated

What information you see in the Job Events for these uncategorized Actions determines your workflow. T he following sections walk you through the workflow using example use cases. Resolving these issues will continue to improve your security posture.

Keep in mind that as you work through these unknowns, it is possible you will not be able to clear them all out, specifically when events are not generated.

IMPORTANT: When you add or edit security technology definition and prevention information, the changes have to be processed, so the updates to the Jobs, Events, and Gauges may not display immediately.



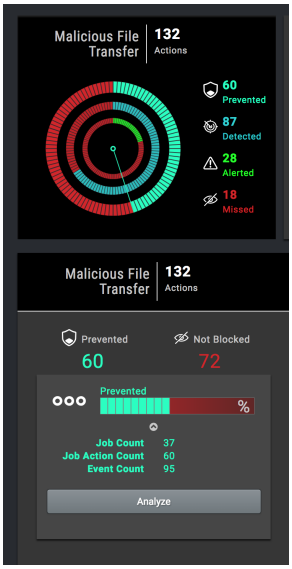
Workflow for Resolving Prevented Unknown Security Technology Actions

Events available – provides blocked info

Network Technologies

Consider the details for the Malicious File Transfer Gauge. There are 60 Job Actions that were Prevented but none of them were associated with a technology.

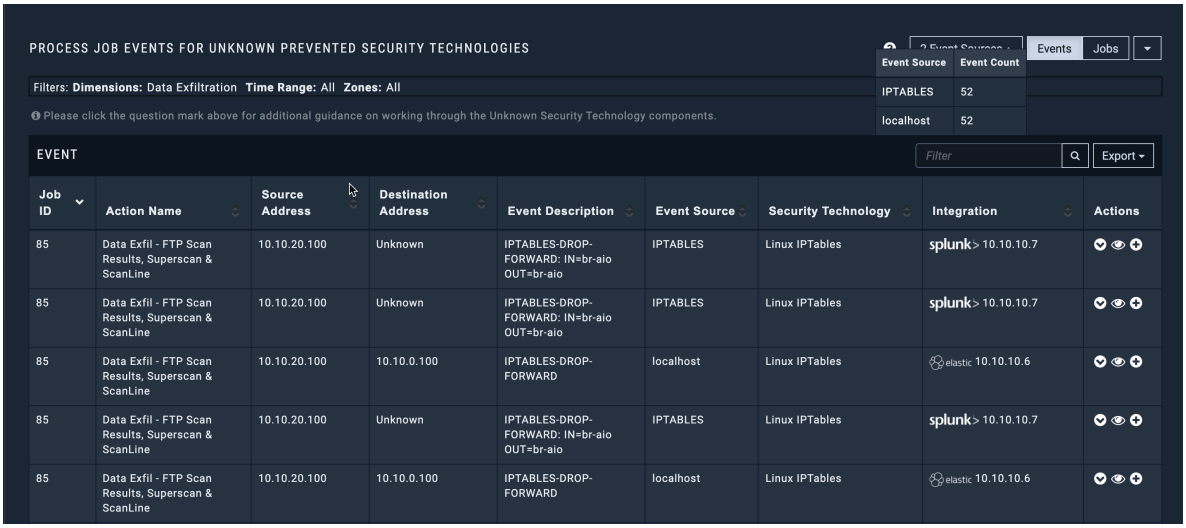
MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Malicious File Transfer Unknown Prevent Gauge Details

To research this, click on Analyze to display the Process Job Events specific to the Detected Events in the unknown security technology category for malicious file transfers. From here, you can start your analysis using the Events listed, or switch over to the Process Job Actions view. On the Process Actions view, review the Events Action by Action, with the ability to filter the list to only include Actions with events, Actions with suspicious events, or Actions with no events.

In this case, you decide to start with the Events list, sorting by each of the columns to identify any information that will help identify the security technology or the blocking event. Once you sort by the description field, you see there are Palo Alto events that have a description of blocked. This gives you enough information to check the security technology definition and potentially add in the prevention information, which you can do by clicking **Add Security Technology**.

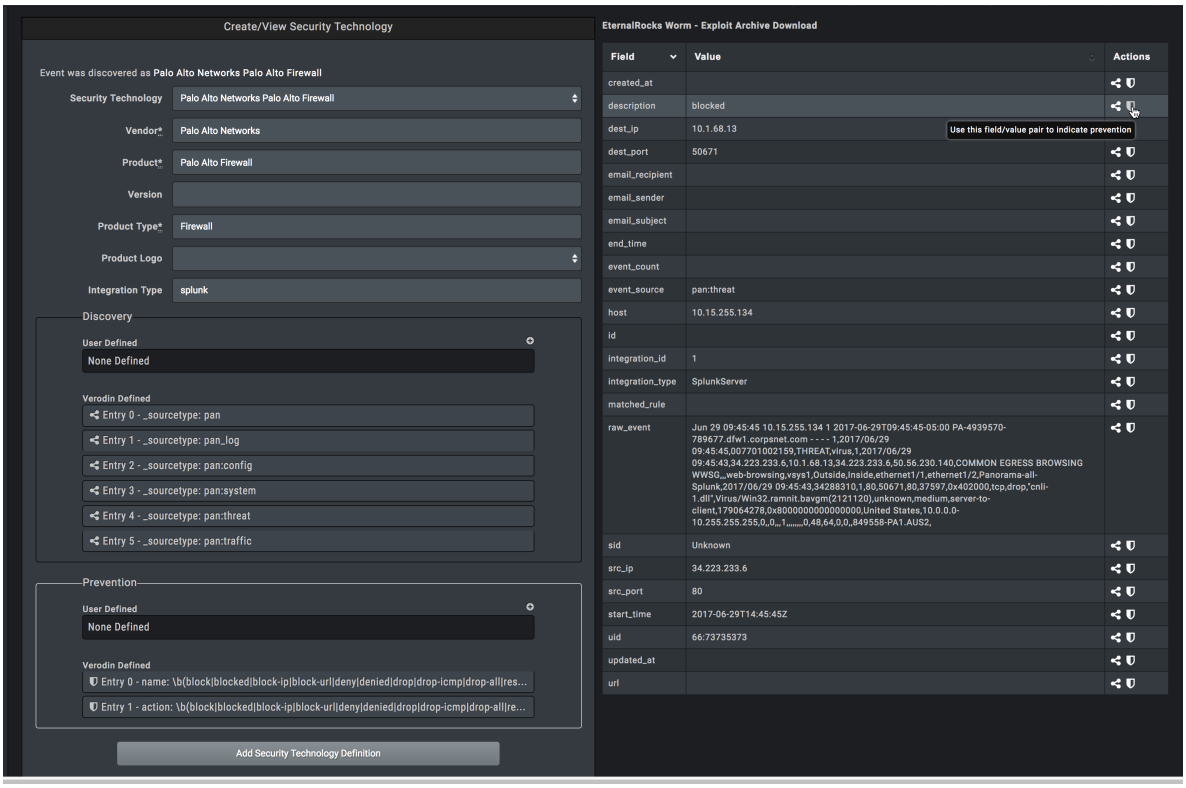


The Process Job Events page sorted by Event Description

Since the technology was already defined, this page prepopulates with the platform-provided information, as well as any user-provided information. You can see the Validation Platform defined some prevention information but did not include

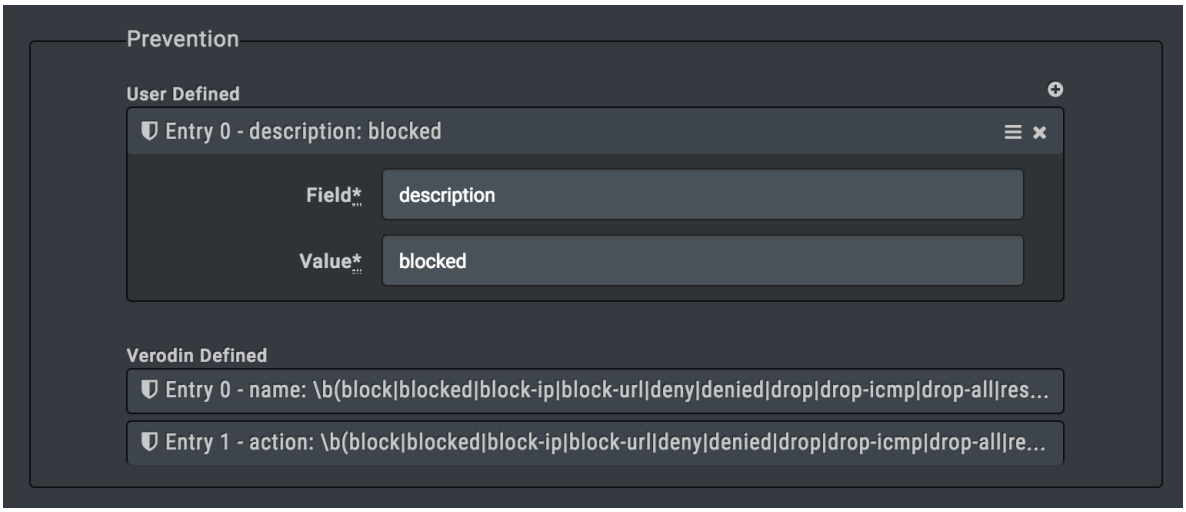
MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

the description field. Since the description field contains pertinent information, you add that to the definition by clicking **Add Prevention Info** for the description field.



Add Prevention info to Security Definition

When you do this, it adds an entry to the User Defined Prevention section, which when expanded, shows the specific field and value included.

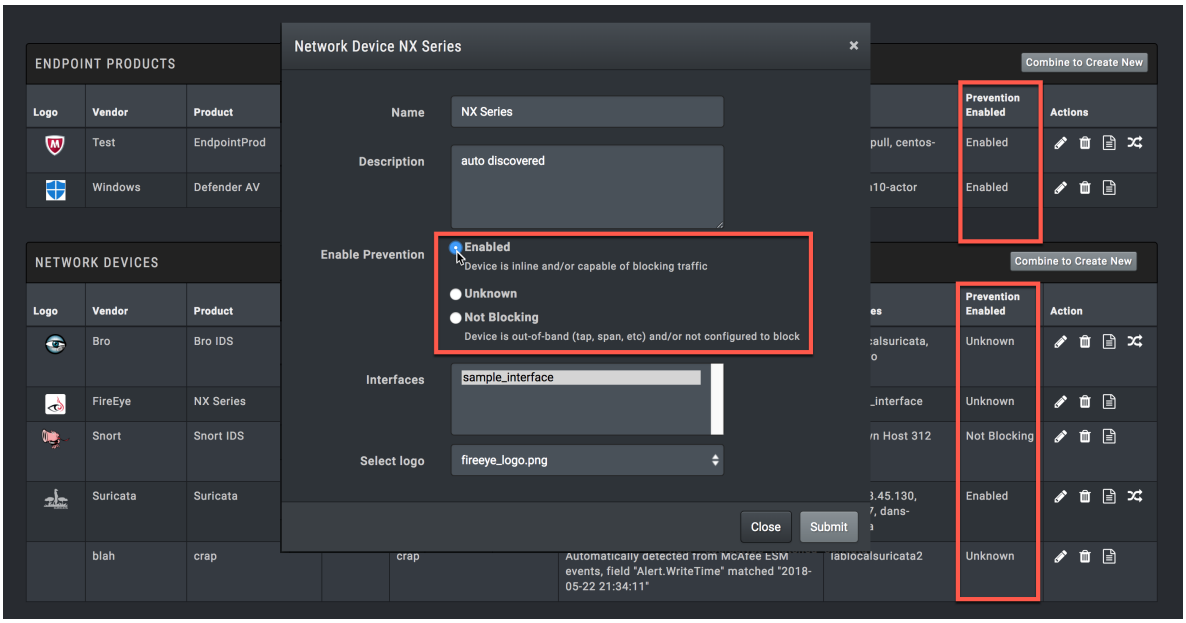


User-defined Prevention field expanded showing the information added

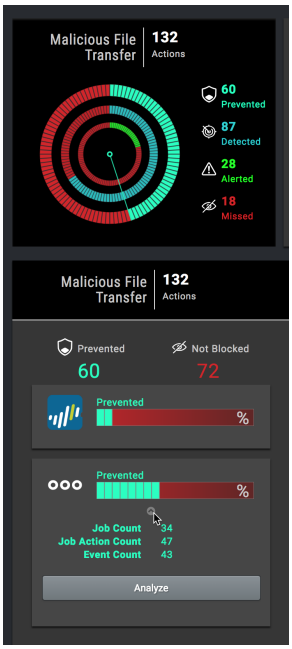
After saving your changes, the Security Technology page in the Environment section displays so you can verify Palo Alto

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

has Prevention Enabled. In this case, it is not, so you edit the security technology to enable it.



Security Technology page - enabling Prevention for Palo Alto



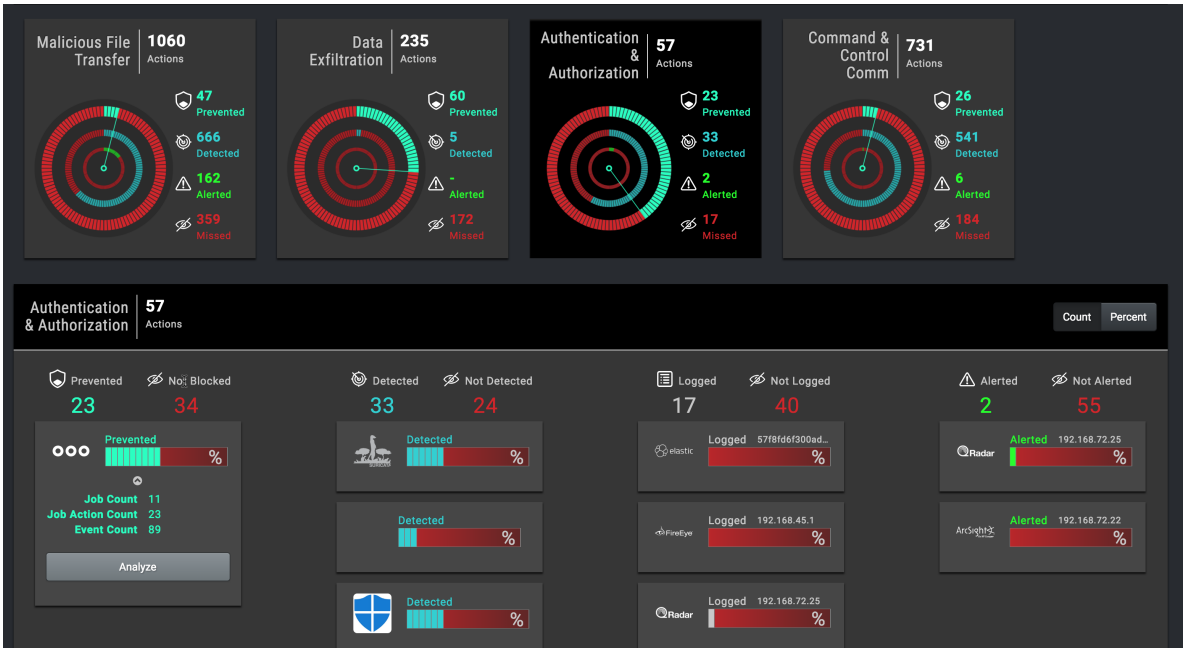
Malicious File Transfer after Prevention defined and enabled

Then, switch to the Gauge page and refresh it. When the changes are process, the Gauge details for Malicious File Transfer will show Actions associated with Palo Alto and the number of unknown Actions will have decreased.

Endpoint Technologies

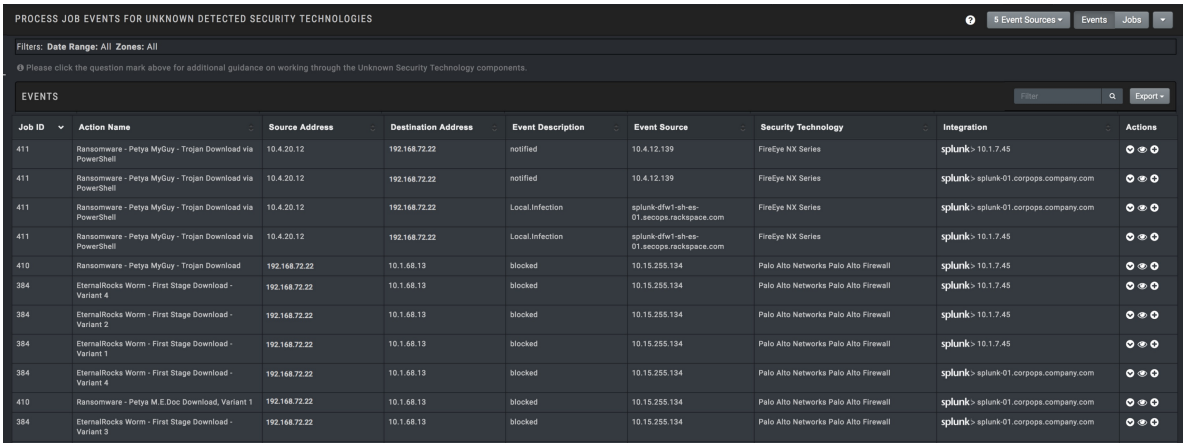
Consider the details for the Authentication & Authorization Gauge. There are 23 Job Actions that were Prevented but none of them were associated with a technology.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Authentication & Authorization Unknown Prevented

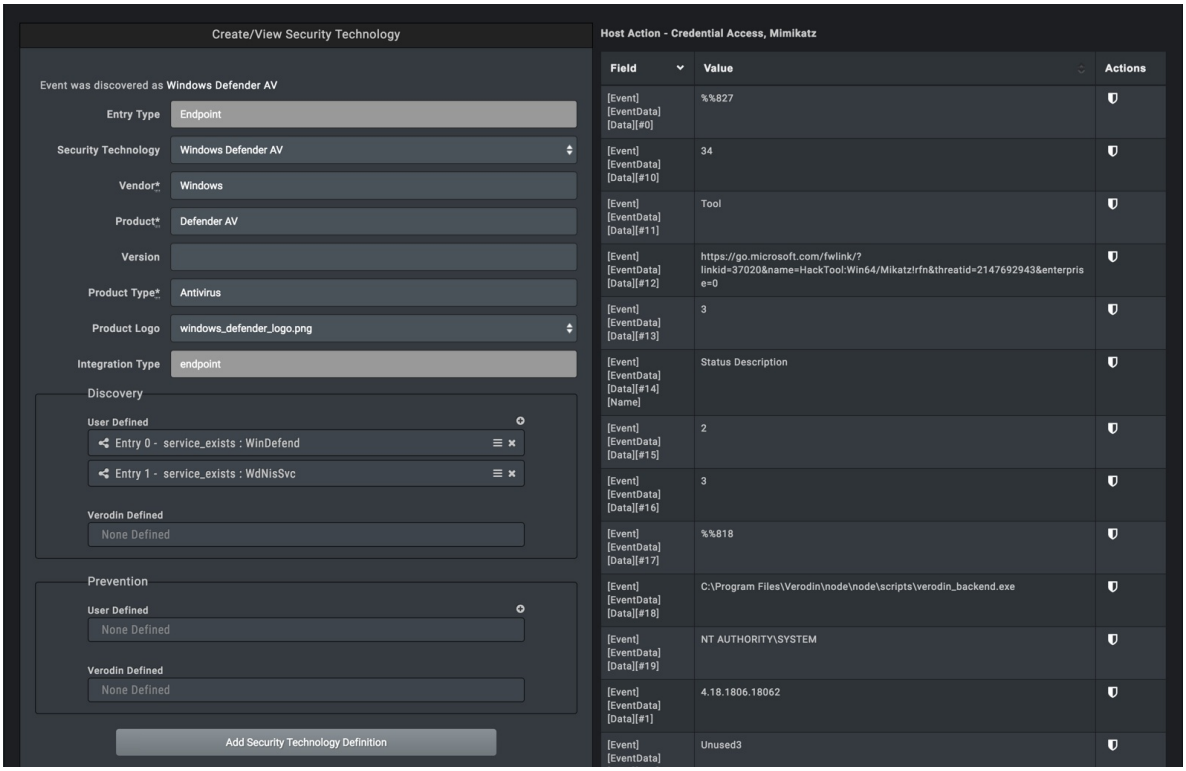
To research this, click **Analyze** to bring up the EVP page, which has the Process Job Events and Process Job Actions views specific to the Prevented Events in the unknown security technology category for Authentication & Authorization. From here, switch the Jobs Actions view to start your analysis. Expand one of the Actions and click **Events** to see the Event details. Immediately you can see that these are Endpoint events, the events are associated to Microsoft® Windows® Defender, and that there's information in the Message field that shows that Windows Defender prevented the Action. Hover over Add a new Security Technology and see that Windows Defender has prevention enabled, so now you need to add the rule so the Actions are related to it.



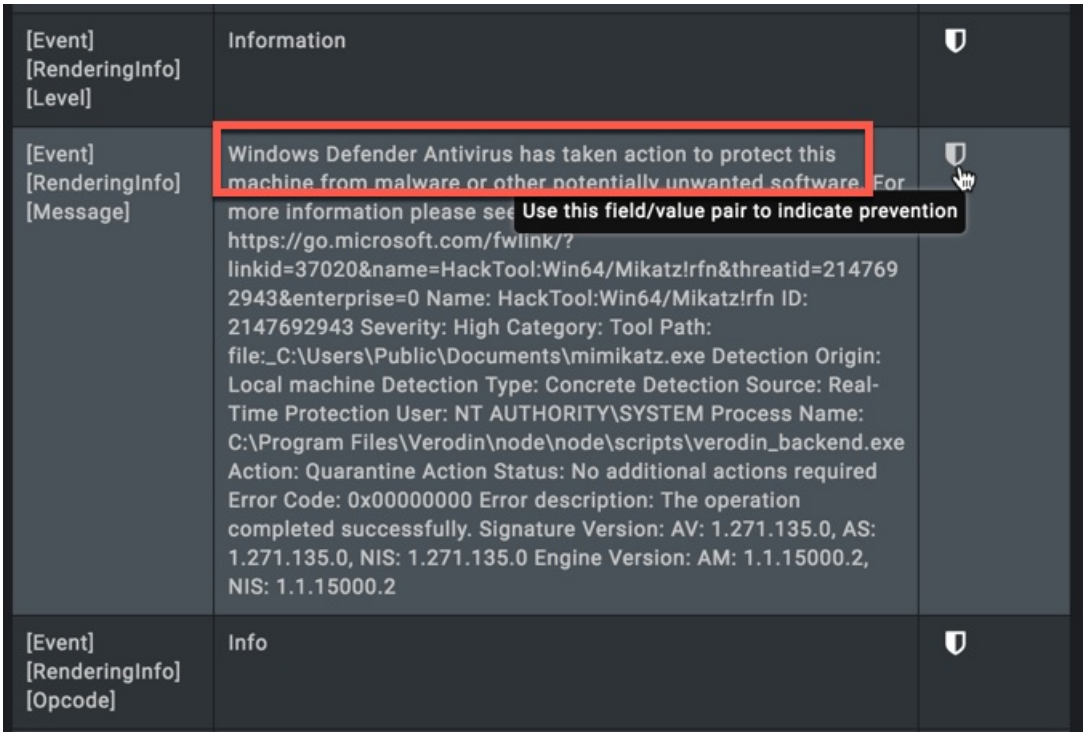
The Process Job Action view showing Events for one of the Actions

Since the technology was already defined, this page prepopulates with the current definition and rules. Notice that this page is different, with the available information field names different than what you saw for the network security devices. The Add to Detection option also isn't available in the Actions field.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Create/View Screenshot for Windows Defender

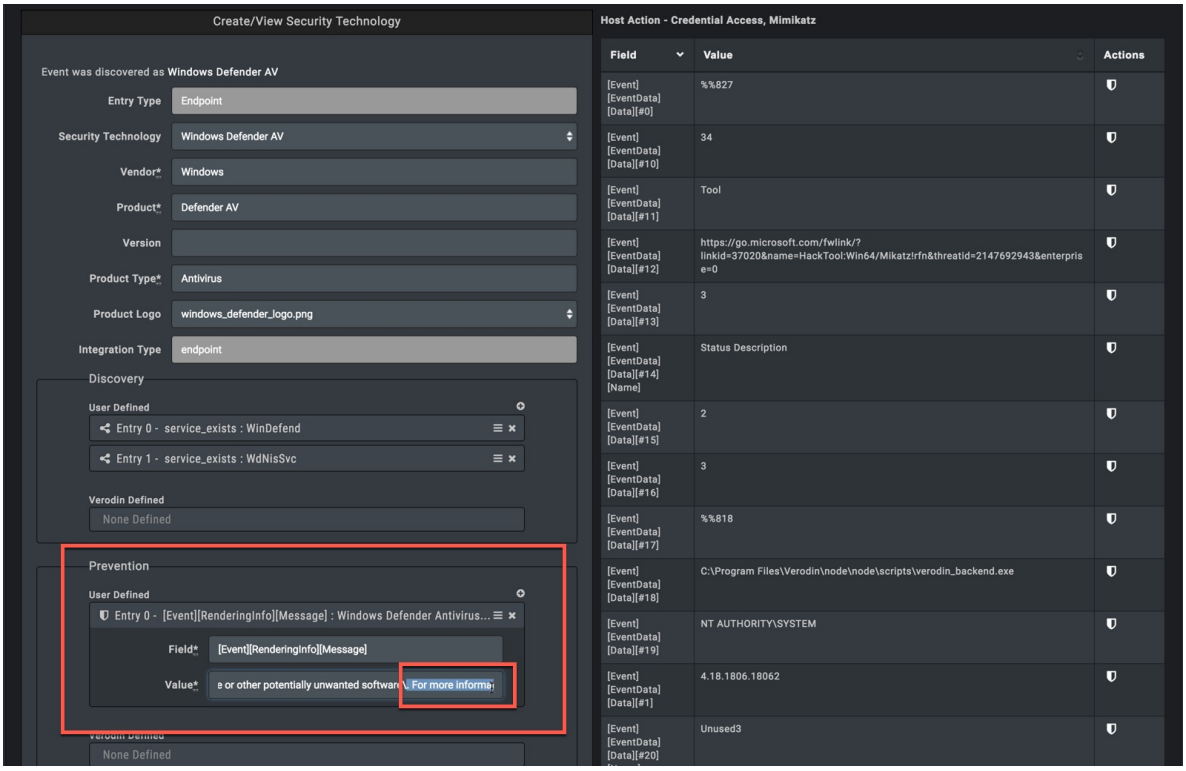


Windows Defender Field containing prevention info

You look for the message field and realize it contains extra information. Click **Add to Prevention** to create the user-

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

defined Prevention rule fields, and then edit the field to contain only enough detail so the Validation Platform can identify the Action has being prevented by Windows Defender.



Create/View Security Technology highlighting the prevention definition

After you save the rule, the Validation Platform updates its configuration and when the changes are processed, you see the unknown category in the Gauges has greatly reduced and Windows Defender is now listed as a technology that prevented Actions.

IMPORTANT: When you add or edit security technology definition and prevention information, the changes have to be processed, so the updates to the Jobs, Events, and Gauges may not display immediately.

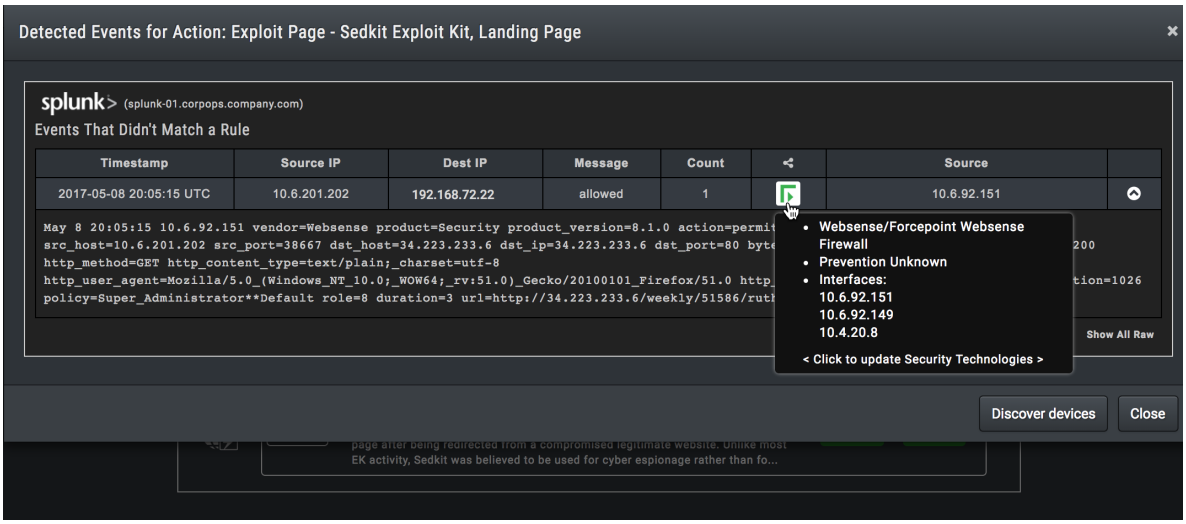
MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Authentication & Authorization details now includes Windows Defender

Event Available – No Blocked info

Consider Job ID 23 for Reconnaissance Attacks with unknown prevented security technologies. Here you see that the Action was Blocked and there was one Event. Reviewing the Event, you see that it:

- Is identified as an Event tied to Forcepoint
- Was not related to a Splunk rule, so no Alert was fired
- The message field is allowed



Processed Jobs Actions for Reconnaissance Attacks with Job ID 23 expanded

At this point you know that the only Event generated indicates the Action was allowed and was not blocked. So now you need to investigate to determine:

- Were all Events generated that should have been generated?

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

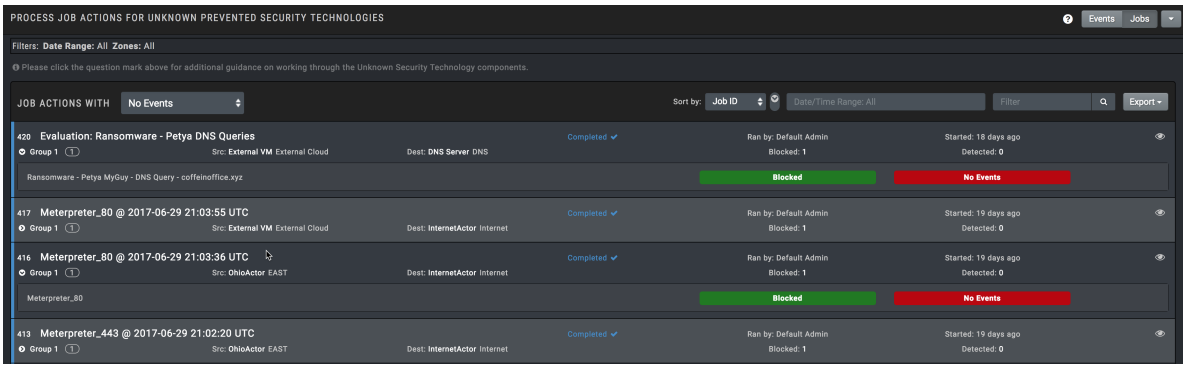
- Is there a configuration issue in the security stack that caused Splunk to believe the Action was blocked when it really was not, since the only Event associated with the Action says it was actually allowed?
- Is there a configuration issue that populated the event information incorrectly?

After you complete the investigation and resolve configuration issues within the stack, rerun the Job to see what the Validation Platform tells you. If there is only one Event that now shows as blocked but is still not related to a security technology from the prevention side, you have additional information to use to continue through the workflow, potentially creating the security technology definition and adjusting the security technology configuration the same way you did in the previous use case.

Once you have addressed the root of the issue, you may decide to delete the original Job since it may not contain valid data. The information in the original Job will not change, regardless of the configuration changes you make, so it will continue to be included under the Unknown prevented category.

No Events Available

Consider the Command and Control Actions with unknown security technologies. Of the 34 Jobs run, 12 of them do not have any Events associated with them.



Processed Jobs Actions - Command & Control Comm Attacks showing no Events

Since there are no Events, you need to look at the security stack to identify the issue. Some common troubleshooting questions could include

- For the Actions run, should there have been Events created?
- If Events should have been created, what security technologies are in the security stack that should have created the Events?
- Was the security technology that was responsible for generating the events down when the Action was run?
- Is there a configuration issue in the security stack that prevented the event from being generated and/or seen by the Validation Platform?
- Are the integration configurations in the Validation Platform set up correctly to capture the required information?

As mentioned earlier, it is possible that there will not be events generated and thus the Validation Platform cannot identify the security technologies. If you resolve an issue in your security stack, re-run the Jobs. When you re-run the Jobs and Events are found, the Events are either associated with the security technology, or you will have the event information in the Validation Platform to assist you with further troubleshooting. If Events are found, you may choose to delete the original Job since it contains invalid data now that the issue is resolved.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

NOTE: There is an Audit Log that allows you to see information around Job deletion

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.