MANAGING SECURITY TECHNOLOGIES

Security platforms and solutions are an important part of Security Validations and are identified several ways, including during installation of Actors or running Actions and having the events identified by the Integrations. Once they are identified, they are displayed on the map, are seen in the events section of Job Actions, and can be reported on.

Note: If you're working with AWS security technologies, they appear on the network map per region, which is a slightly different behavior than other security technologies. For example, if an event comes in for a GuardDuty integration setup in us-east-1, a GuardDuty icon should pop up on the map. Likewise, if an event comes in for a separate region (for example, us-east-2), a second GuardDuty icon should appear on the map.

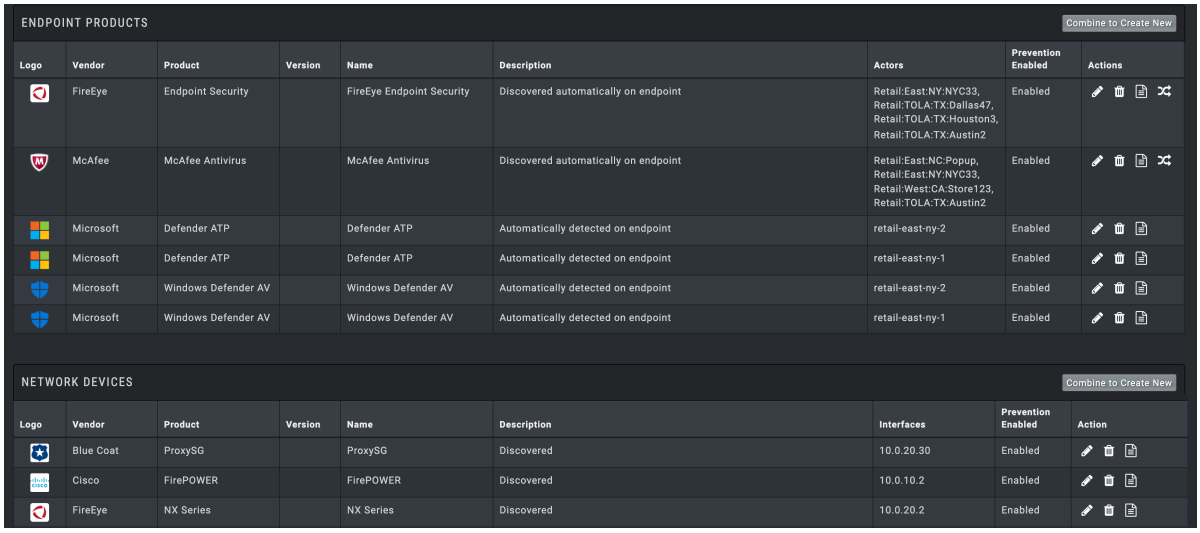
There are two main areas where you can review and manage the Security Technologies identified in your system (or definitions provided by Mandiant):

- **Security Technologies Page**
- **Security Technology Settings Page**

Security Technologies Page

The Security Technologies page displays a list of security platforms or solutions identified through the platform's integrations. On this page, you can edit and delete the security technologies, and you can view the activity log.

TIP: If your security technology wasn't identified, you may need to create a custom definition. This can be done by manually creating a definition, or by working through the Unknown Security Technologies Workflow, a part of **Effectiveness Validation Process (EVP)** **(https://docs.mandiant.com/home/msv-evp)**.



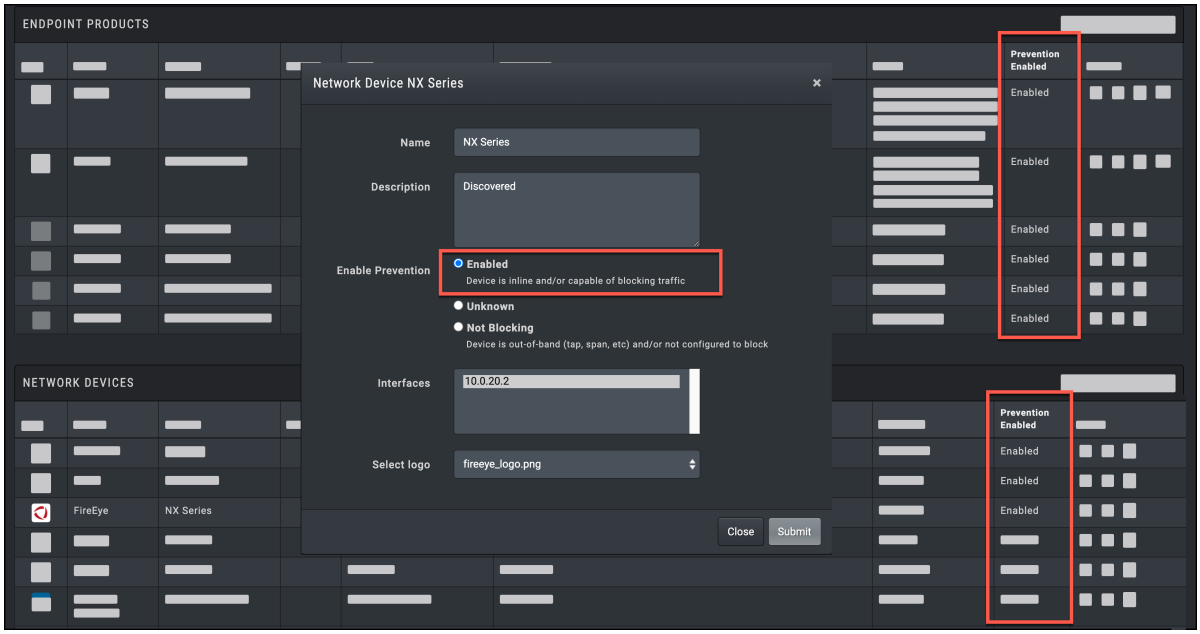
Security Technologies page

Security Technology Prevention Settings

When you edit a security technology, a configuration option defines if the device is used for Prevention. By default, all endpoint security technologies list Prevention as Enabled and network security technologies list Prevention as Unknown. On initial installation, go to **Environment > Security Technology** and review and update the Prevention configuration for

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

each Security Technology that your organization uses to Prevent Attack behaviors.



Security Technology Prevention setting

Until you make this configuration change on your security technologies, the platform cannot relate Job Actions that were Prevented to specific security technologies. When Job Actions are correctly related to security technologies, the Gauge details on the Gauge page are more complete.

Combining Multiple Instances of a Security Technology

If you have multiple security devices (network or endpoint) you'd like to combine so they only show up once in reporting and on the map, you can do that on the Security Technology page. For example, the environment shown below shows our Firewall and IDS technologies identified on several interfaces. The first instance of the Firewall is a combined version, as is the IDS.

TO COMBINE SECURITY TECHNOLOGIES

1. Go to **Environment** > **Security Technologies**.
2. Identify security technologies you want to combine in either the Endpoint Devices or the Network Devices table.
3. Click **Combine to Create New**.
4. Select two security technologies from the table. You know they are selected because they change color. Then click **Submit**. The table will refresh and the security technologies will be combined in one row, with both interfaces listed.

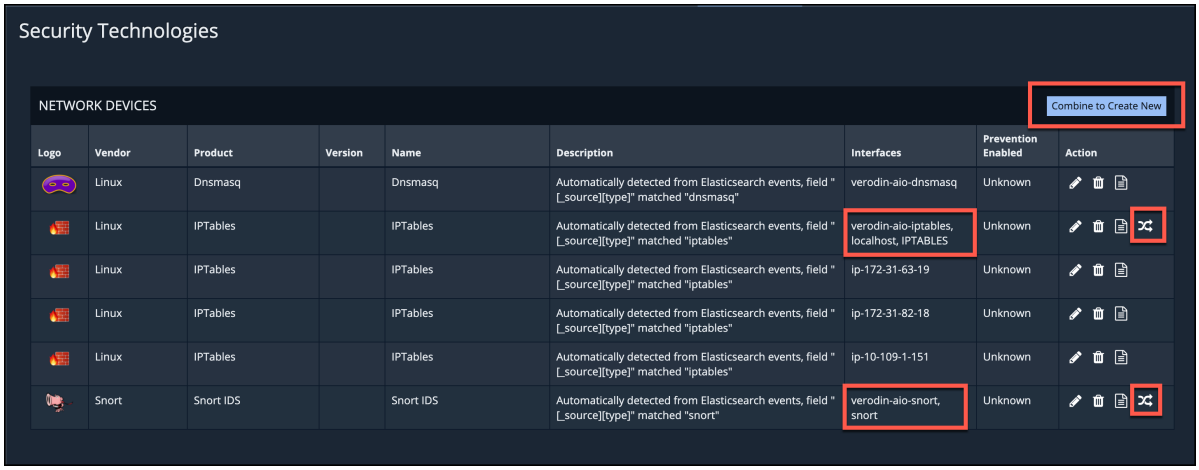
TO SEPARATE SECURITY TECHNOLOGIES

If you want the security technologies to display separately on the map and in reporting, you can separate the ones you combined.

1. Go to **Environment** > **Security Technologies**.
2. Identify the security technology you want to separate and from its Action menu, select **Separate**.
3. From the Device window, select one or more interfaces and click **Move to new device**. Then click **Submit**. The table will refresh and there will be a new line in the table for the separated security technologies.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

TIP: When separating security technologies, it will only create one new security technology. For example, if you have a security technology with three interfaces and you want to separate them, you will need to complete this procedure twice.



Security Technology combined

Deleting a Security Technology

If you have removed a security device from your environment, you may want to remove it from the map. To do this, you would delete the security technology.

NOTE: When you delete a Security Technology, it is disabled in the database instead of being removed. This allows historic information, such as Jobs, Job Actions, and Events, to be maintained in the database for retrieval.

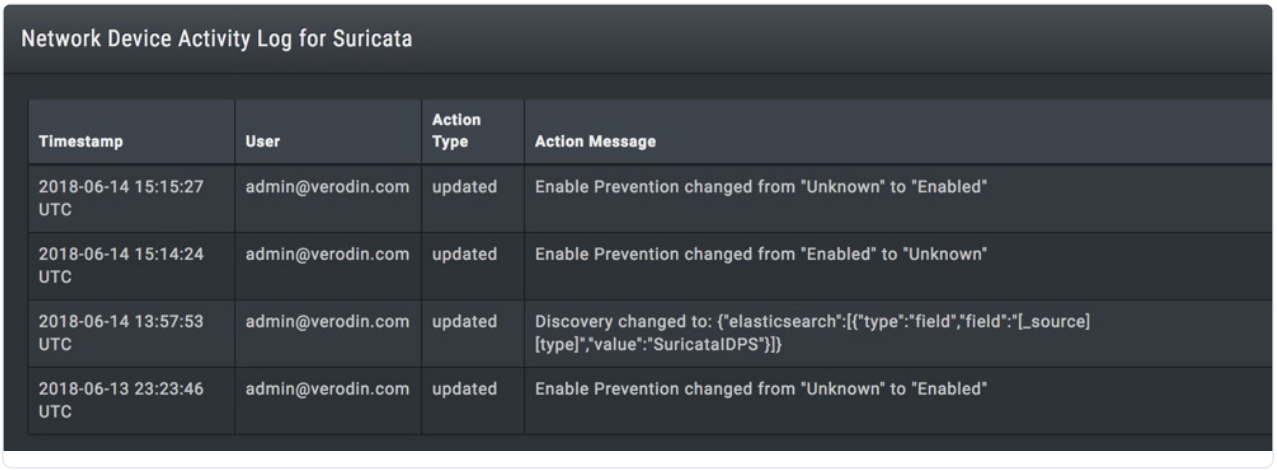
TO DELETE SECURITY TECHNOLOGIES

1. Go to **Environment** > **Security Technologies**.
2. Identify the security technology you want to remove from the map and from its Action menu, select **Delete**.
3. Click OK to confirm. The table will refresh and the security technology will be removed from the table.

Activity Log

All modifications to the Security Technology definitions are recorded, whether done from the Security Technology page or from the Create New Security Technology page. This allows you to identify when a security technology definition is changed and who made that change. To view the change, click **Environment** > **Security Technologies** Environment, then click the Activity Log icon for the security technology you want to see.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Network Device Activity Log for Suricata

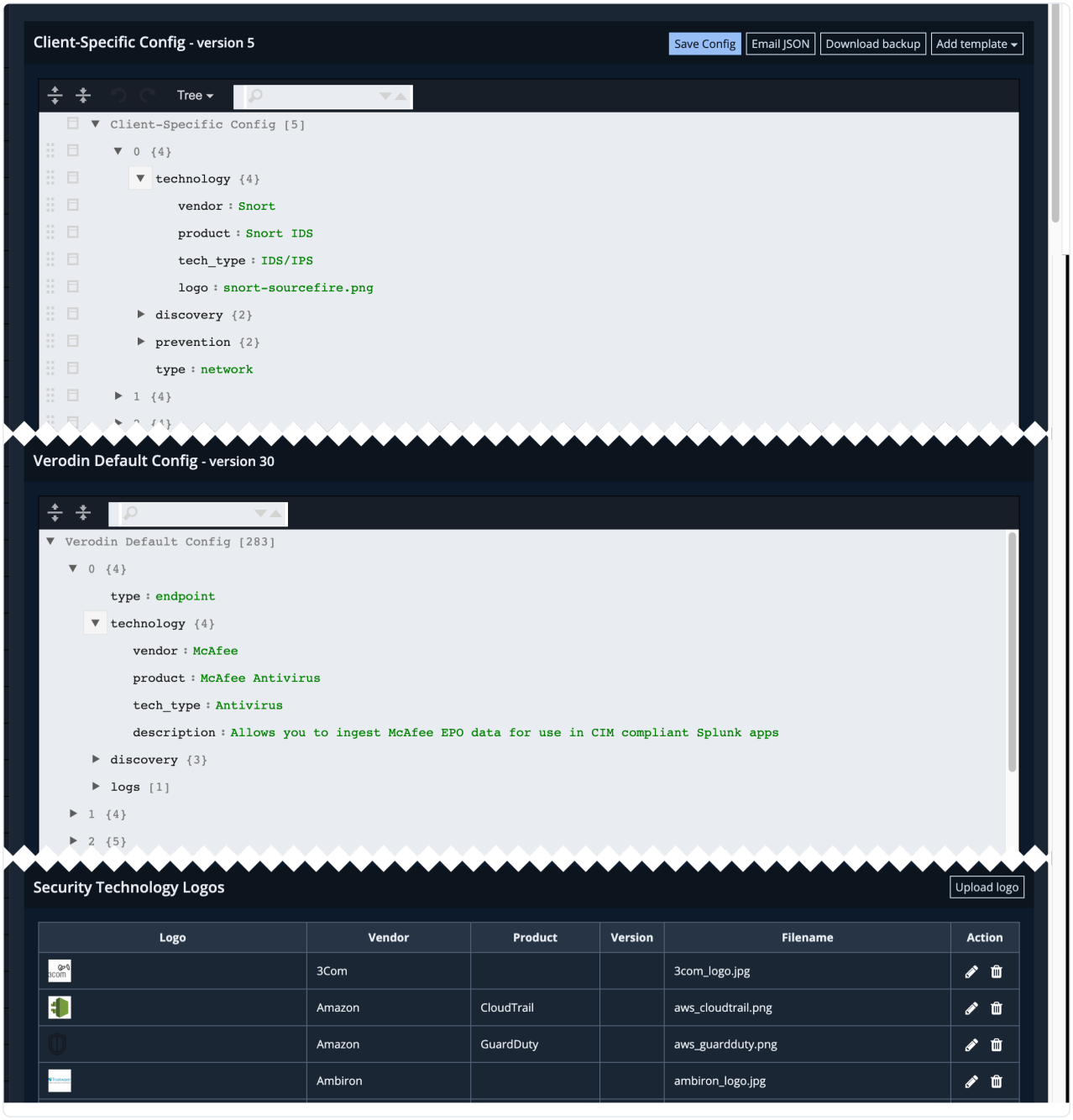
Timestamp	User	Action Type	Action Message
2018-06-14 15:15:27 UTC	admin@verodin.com	updated	Enable Prevention changed from "Unknown" to "Enabled"
2018-06-14 15:14:24 UTC	admin@verodin.com	updated	Enable Prevention changed from "Enabled" to "Unknown"
2018-06-14 13:57:53 UTC	admin@verodin.com	updated	Discovery changed to: {"elasticsearch":[{"type":"field","field":"[_source][type]","value":"SuricataIDPS"}]}
2018-06-13 23:23:46 UTC	admin@verodin.com	updated	Enable Prevention changed from "Unknown" to "Enabled"

Audit log showing changes to the Suricata Security Technology

Security Technologies Settings Page

The Security Technologies Settings page is where you view and create rules for identifying security technologies in your environment and add logos for the security technologies. To access this page, go to **Settings** > **Director Settings**. Then select **Security Technologies**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Security Technologies settings

When jobs are processed, the platform examines the events culled from integrations and compares the fields to the security technology definitions. The Validation Platform comes pre-populated with definitions for the common security technologies. The technologies that are identified are populated in the Security Technologies tables under **Environment > Security Technologies**. Their logos will also appear on the map.

If you have a security technology that the Validation Platform does not have a definition for, you can create new rules. If you are comfortable working with JSON, you can write these in the Client-specific Config area of this page. If you do not

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

want to write it out using JSON and you have a Job with events that don't have a defined security technology, you can also use the EVP process. This can be started from Job Results or from the Gauges. See **Creating New Security Technology Definitions** for more information.

Network Security Technology Definitions

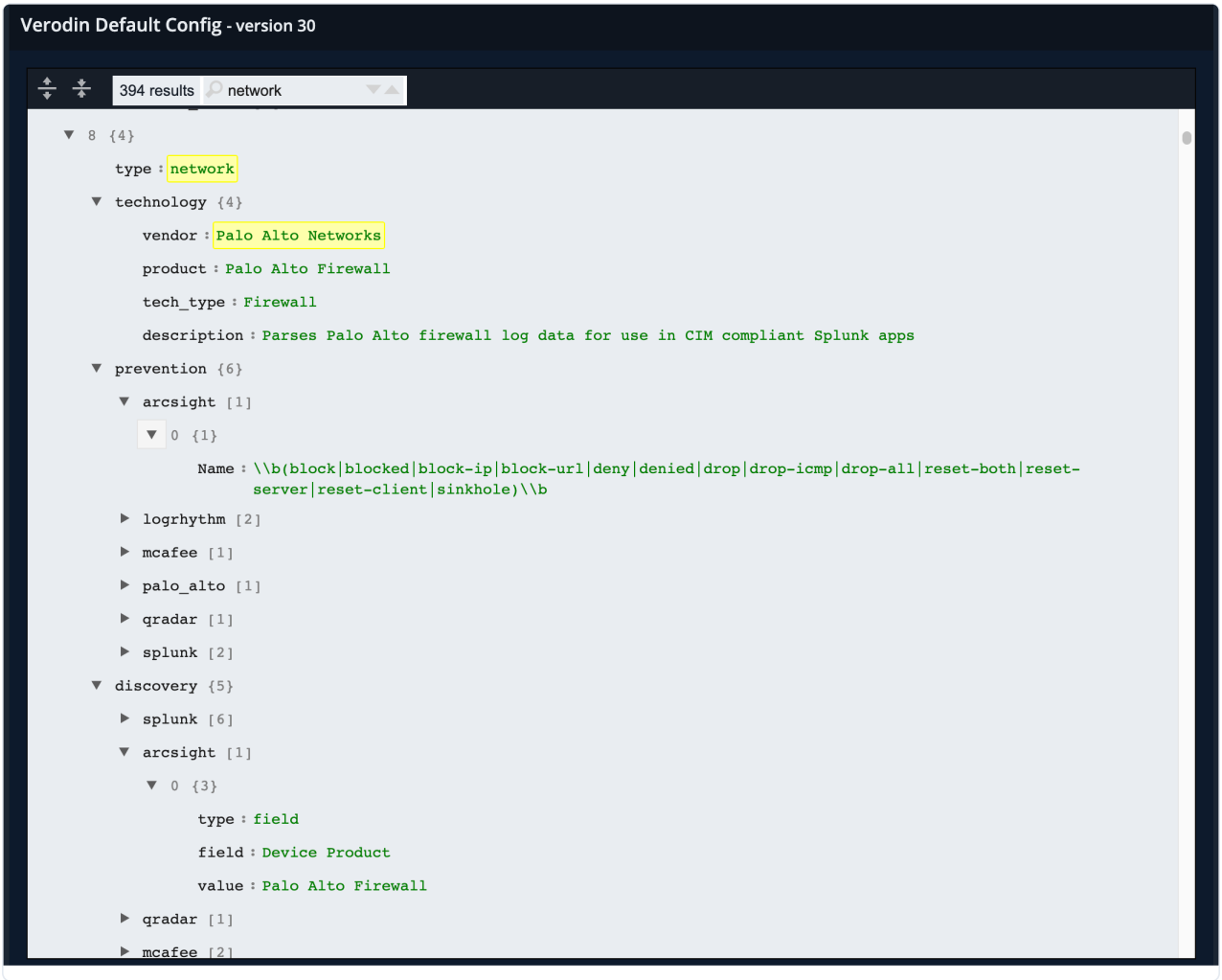
The network security technology definitions include the following sections.

- Technology:
  - Entry that provides overview details of the security technology, such as vendor, product, security technology type, and optional entries like description, logo, and version
- Prevention:
  - Entry that populates if prevention is possible for that technology
  - Entries that show how integrations know that the security technology blocked a behavior or attack

    NOTE: This section is optional.
- Discovery:
  - Entries that represent how integrations identify or discover the security technology, which include the following:
    - type: How integrations identify the security technology (this will always be "field")
    - field: Name of the field where the information comes from
    - value: Value in the field

The following figure shows an example of one of the Validation Platform's pre-configured network security technology definitions.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Example of a Network Security Technology Definition

Endpoint Security Technology Definitions

Endpoint security technology definitions include the following sections:

- Technology:
  - Entry provides overview details
- Discovery:
  - Entries that represent how the security technology is discovered. This includes the type, which is how the integrations identify the security technology (this could be file_exists, directory_exists, service_exists, or program installed).

    NOTE: Additional fields will be included based on how the "type" field is populated.
- Logs:
  - Entry identifies the log type and source that the Validation Platform pulls events from and lists any logs on the operating system where events could be found.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

This determines where we look for host events on an Actor when running Host CLI Actions. This can come from Windows event logs or a flat log file. In the config, a logs item must have a `type` key that can be either `event_log` or `file`. Depending on the type value, we require different additional fields.
For `event_log` type items:

- `value`: this is the log name, for example, "Application" or "Security"
- `filter`: this is a dictionary with a single key `source`, which is a list of log source values to filter by. The log source value corresponds to the Name attribute of the System Provider field in Windows event logs. There's an example of this later in this section.

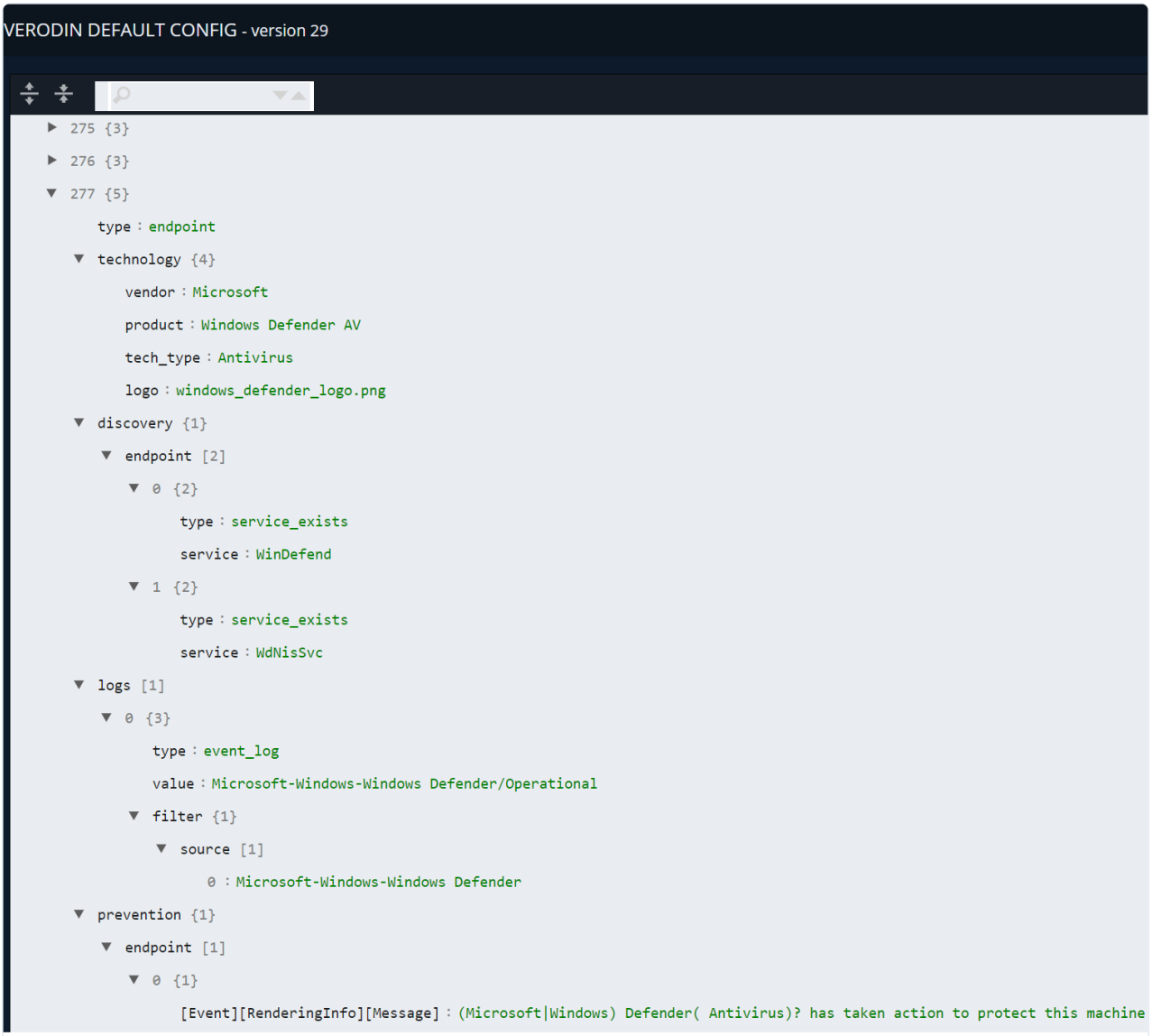
- For `file` type items:
  - `value`: this is the filepath of the log file to check
  - `regex`: a multi-line Python-compatible regex used to parse log entries. Named groups must use the syntax `(?P<group name>)`. We will respect the following list of group names in the regex, although you can include additional ones, if appropriate:
    - computer
    - message
    - src_log_file
    - log_name
    - event_id
    - category
    - event_type
    - user
    - opcode
    - keywords

- Prevention:
  - Entries that represent how the Validation Platform knows the security technology blocked a behavior or attack

> **NOTE:** This section is optional.

An example of one of the Validation Platform's pre-configured endpoint security technology definitions is available in .

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Example of an Endpoint Security Technology Definition

Creating New Security Technology Definitions

If you have a security technology that the Validation Platform does not have a definition for, or for which information is missing, you can manually add the security definition. This can be for a new security technology or to add information to an existing technology. If you are comfortable working with JSON, you can write these in the Client-specific Config area of this page.

If you do not want to write it out using JSON and you have a Job with events that don't have a defined security technology, you can also use the EVP process, which includes using existing events and the forms that are part of EVP. You can create new network and endpoint security technology definitions using the template in the Security Technology settings by switching the text to the other option. You can use the parsed event to populate the definitions. See **Effectiveness Validation Process (EVP) (https://docs.mandiant.com/home/effectiveness-validation-process-evp)** for more information.

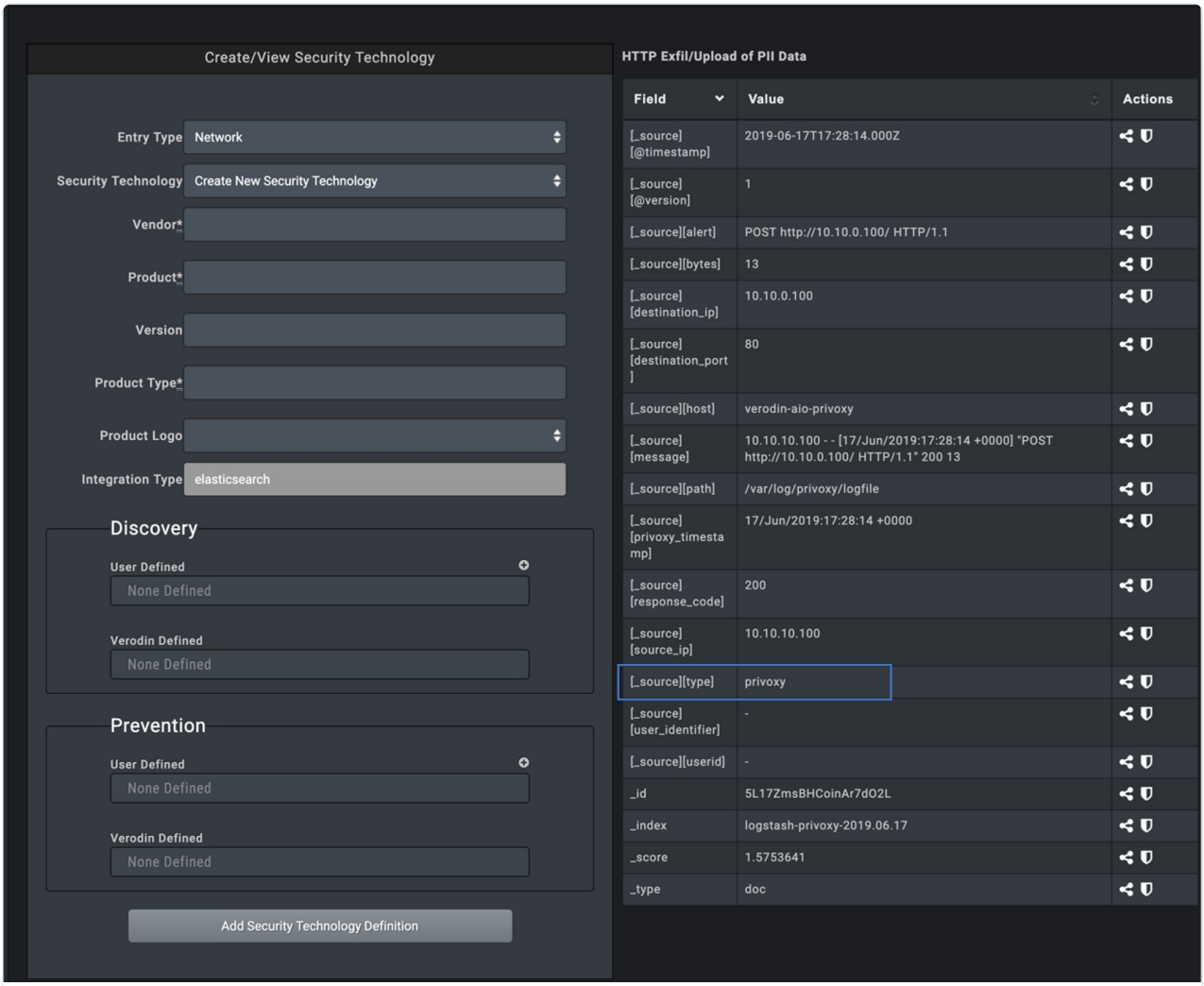
For example, you can add definitions for how the integrations discover the security technology (represented by the icon) or how the integrations identify when the security technology prevented/blocked a test (represented by the

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

icon).

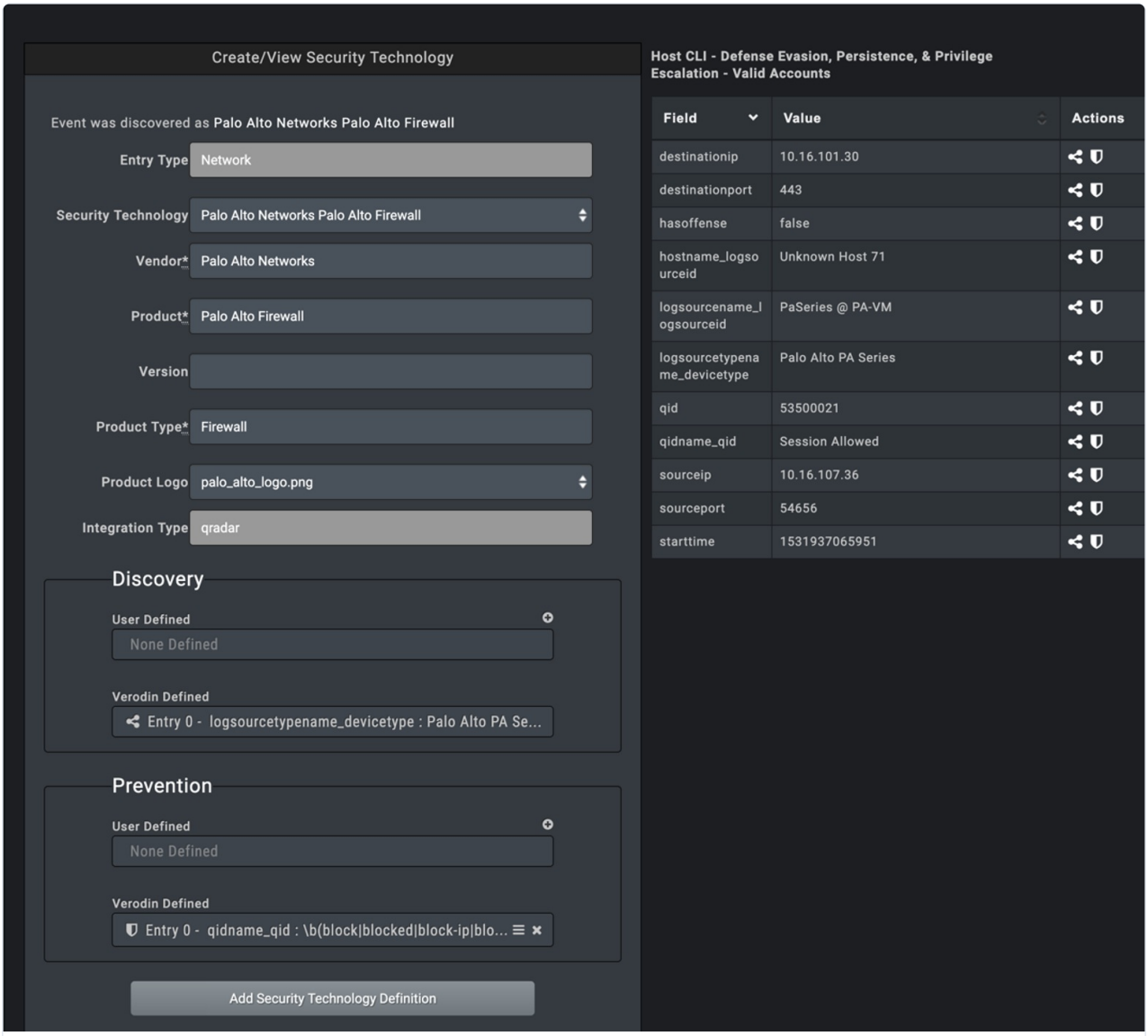
Access this form by clicking on one of the following options:

- The security technology icon (or +) from an event in a Job
- The unknown technology process for the Gauges
- The filtered Jobs list for the MITRE Dashboard



unpopulated form

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



populated form

As customers send us their custom definitions, we will review and integrate them into the pre-defined definitions as appropriate.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.