EVENT FILTER RULES

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

The Security Validation platform captures all events its integrations see when Jobs are run. Some of these events may just be noise or not directly related to the test you're running, so you don't want them to be counted towards the results of the Job. To assist you with excluding these events, the platform includes Integration Event Filter Rules.

An overview of the functionality includes:

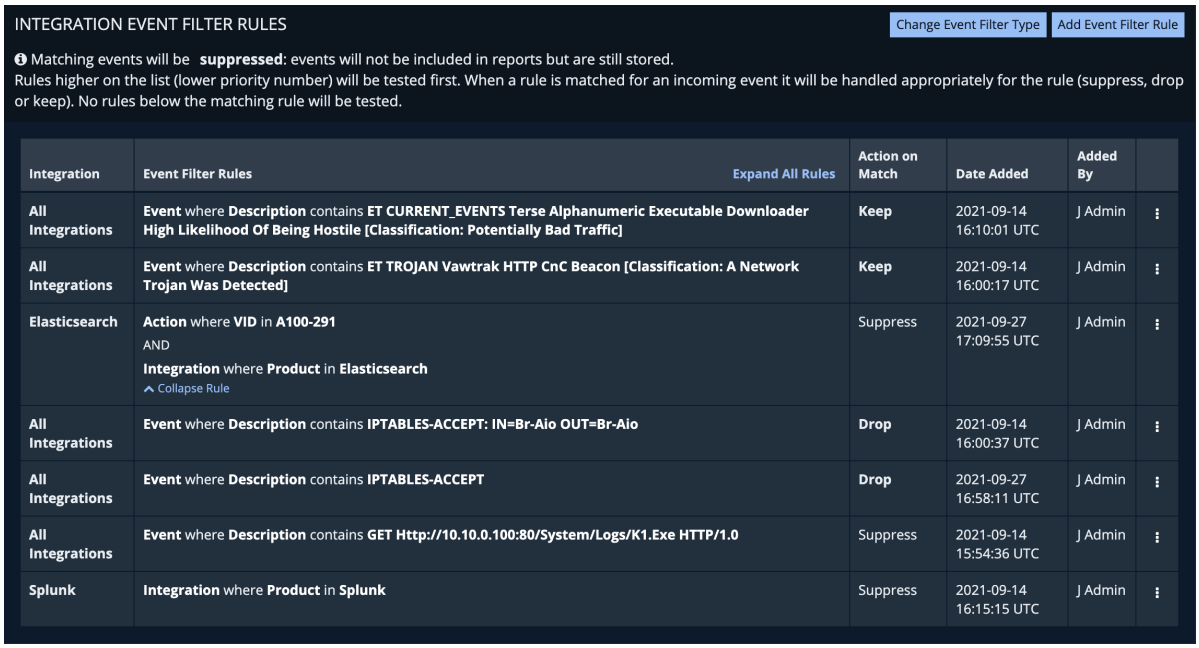
- The platform will have a default filter type that's automatically applied to all Filter Rules you create - suppressed or dropped are the two options.
- Individual Filter rules can be configured to override the platform's default Action. In addition to having suppressed and dropped as options, you can also configure the rule to Keep specific events.
- The filter rules are displayed in the order they are applied when a Job is run, which is configured when creating and editing the rules.
- The Job Results include a section for each Action that displays which Event filter rules were applied and what action that rule completed.

Viewing all Event Filter Rules

There are several places in the Director where you can view Event Filter Rules. However, the only place you can see them all and what order they run is in the Event Filter Rules Table on the Integrations page.

If an Event Filter Rule is bolded, it means the Event Filter Type is manually set and does not use the global Event Filter Type.

To view all Event Filter Rules configured for your environment, go to **Settings** > **Integrations**.



Event Filter Rules table

Important Definitions

When creating event filter rules, you configure them to use one of three types: suppress, drop, or keep.

Term	Definition	Examples of when to use
Suppress	Events will not be included in reports but are still stored	You want to see the events when you view the Job Action, but you do not want it to count towards the Job Action's pass / fail / detected information.
Drop	Events are discarded and not stored	There is no need to track the specific events when running tests.
Keep	Events will remain associated to the Job Action	If you want events to remain and you have other event filter rules that would either suppress or drop them. For example, you have an Event Filter Rule that suppresses events for an Action type but you want the events to remain for specific Actions.

Required Permissions

The ability to view, create, and edit Event Filter Rules and the ability to manually drop Events from Jobs is controlled by several system-level permissions, as described in the following table.

Event & Event Filter Rules Permissions

Action	Required Permission	Roles with the permission by default
Create / Edit Event Filter Rules	Settings - Edit	System Admin, Power User
View Event Filter Rules	Settings - View	System Admin, Power User, Users
Drop / Suppress Events directly from Job Results	Integration Events - Edit	System Admin

Mandiant

How the Director processes Event Filter Rules

Event Filter rules run against new Jobs only, not Jobs that have run in the past. Once an event is filtered by a rule, the results will not change for that event, regardless of other rules that run or of any changes you make to the filter rule. Changing an Event Filter Rule during the event matching window will only impact events that have not already been processed.

Event Filter Rules are also applied in a specific order - the order of the rules in the Integration Event Filter Rules table determines the order the rules are processed. Knowing this gives you some general best practices to follow when considering your ordering:

- Order rules so specific rules run before general ones
  Example 1: Keep a specific event for a type of Action before suppressing the same event for other Action types
- Example 2: Suppress events with a specific description before suppressing events for different instances of an integration
- If you create a rule that keeps events, because it's important those events are always associated with Job Actions, those rules need to run first
  Example: When testing your environment for a specific type of Action, you may want to keep all Events for that Action type, including events that are dropped by a rule further down in the list

Event Suppression can also filter events. This filtering works at the level of the Director where Integration Events are matched with Job Actions that are responsible for them. Most feature-specific events are affected by event suppression because they all create Director-level events. Note that events that have been filtered out through of the the event filter types do not show up when creating monitors. For more information, see **Reassigning, Suppressing, and Dropping Events from Jobs (https://docs.mandiant.com/home/msv-reassigning-suppressing-and-dropping-events)**.

If you have many rules, instead of using the rule's arrows to move it, use the Insert Above or Insert Below option on another rule to move it.