Mandiant

USING 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)**.

Event Filter Rules should be setup when first configuring your Director and when you add or modify your security controls. You may also want to configure new rules when you are troubleshooting issues in your environment and when you start testing new use cases (Action Types).

Events on Jobs that come directly from Endpoint Products cannot have rules created around them. Instead, you will need to suppress or drops those events when reviewing the Job.

Eliminate "noise" events

By default, the pass / fail rules for Jobs consider a Job Action that was either Blocked or Detected to have passed. If your security controls are sending Events that don't indicate that the Job Action was actually detected, you're getting a false positive. Setting up Event Filter Rules to drop those events will give you a more clear picture of the security of your environment. This could include keeping events for some types of Actions but suppressing those same events for other Action Types because they aren't pertinent. For example, suppressing Network Events for Host CLI Actions.

Isolate Integrations

There are several reasons you might want to isolate an integration:

- You have an Integration that contains multiple products, such as ePO, and you don't want to see event IDs for modules that don't relate to your detection.
- You have the same Integration on multiple hosts and they are not receiving the same events. So, you suppress events from one or more so you can focus on the host that you suspect is misconfigured.
- You are comparing integrations to gain a perspective on how each of them are working.
- Events from some security controls are only going into one integration and not the other.