EFFECTIVENESS GAUGES OVERVIEW

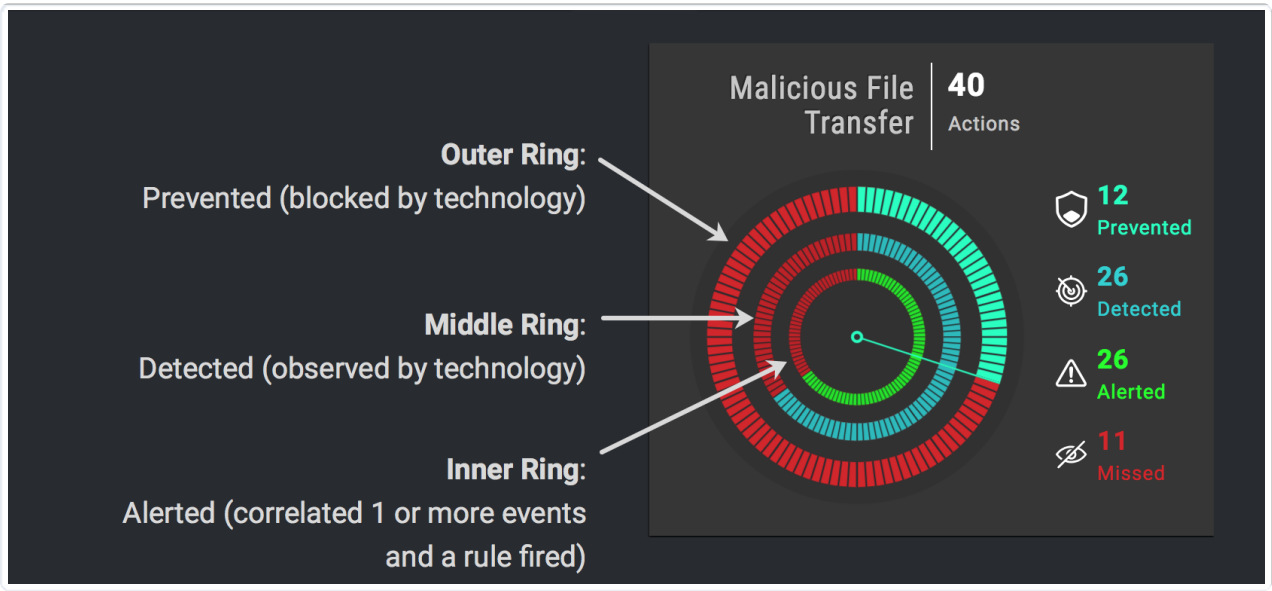
The Effectiveness Gauges provide a visual overview of Job Action results and their related Security Technologies. Each gauge allows you to drill down to detailed information on the results. You can view the Effectiveness Gauges by selecting **Analyze > Gauges**.

> If the Validation Platform cannot relate a security technology to an Action that was prevented or detected, an unknown category is created. A process workflow is attached to this category. Use this workflow to identify potential issues with the configuration of your security stack by reviewing Jobs and Events that are currently unrelated to a defined security technology.

Understand Effectiveness Gauges

To visualize the initial information, the Gauge Effectiveness page contains one or more Gauges that represent the four possible outcomes when an Action is run:

- Prevented - The outer ring
- Detected - The middle ring
- Alerted - The inner ring
- Missed - Not represented in the Gauge



Explanation of Gauge Rings

Additional details regarding the Actions and the security technologies involved is available by clicking on a Gauge or clicking **Expand All Details** to display the details section for all Gauges. The Gauge details pane includes the following information:

- Title bar that contains the name of the Gauge, the total number of Actions that were run, and buttons that allow you to switch between the count and percentage.
- The following four sections: Actions that were Prevented, Detected, Logged, and Alerted.
- Each section includes all technologies that were identified by the integrations.
    - If there are multiple instances of a security technology, the host information is included.
    - If a security technology is identified for which the platform has no logo, a standard logo is used.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- When a Job Action is prevented or detected but did not match a known security technology, it is captured in an "other" category, represented by 3 white circles, that have additional drill-down capabilities. See **Effectiveness Validation Process (EVP)** **(https://docs.mandiant.com/home/msv-evp)** for details on how to work with these Actions.

Authentication & Authorization Gauge Details - Security Technologies' performance

- By default, the Gauges pull information for all dates and zones in the system, and display Malicious File Transfer, Data Exfiltration, Authentication & Authorization, and Command & Control Communications. You can configure this to include the dimensions, zones, and time range you are interested in.
- When you use the Zones filter, results include all Actions that match the destination Actor.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.