Mandiant

UNDERSTANDING PASS/FAIL RULES

When you're talking about Security Validation and the terms passed and failed, you must consider the context before you know what those terms actually mean. Specific context includes:

- Jobs / Actions Passing / Failing
  - Special case 1: Email Actions
  - Special case 2: Malicious DNS Query Actions
  - Special case 3: Host CLI Actions
  - Special case 4: Cloud Validation Actions
- **Monitors Passing / Failing** **(https://docs.mandiant.com/home/msv-how-passfail-is-determined-for-monitors)**
- **Operational Readiness tests Passing / Failing** **(https://docs.mandiant.com/home/msv-operational-readiness)**

Pass / Fail: Jobs and Actions

When you run an Action, which we call a Job Action, the Validation Platform identifies whether the Action is blocked and/or detected. The platform uses that information to determine if the Job Action passed or failed. By default, if the Job Action is blocked or detected, it receives a "Pass" score. However, the platform is configurable, allowing you to update the pass/fail definitions to better reflect your organization's needs. There are three types of pass/fail rules you can create:

- **VID Rules**: Defining requirements for a specific Action
- **Dimension Rules**: Defining requirements that are applied to all Actions that are assigned the selected dimensions (Attack Vector, Attacker Location, Behavior Type, Covert, OS/Platform, & Stage of Attack)
- **Default Rule**: The rule that is applied to Actions that are not impacted by a VID or Dimension rule

For each of these rules, you have the following options to choose from to define the pass criteria:

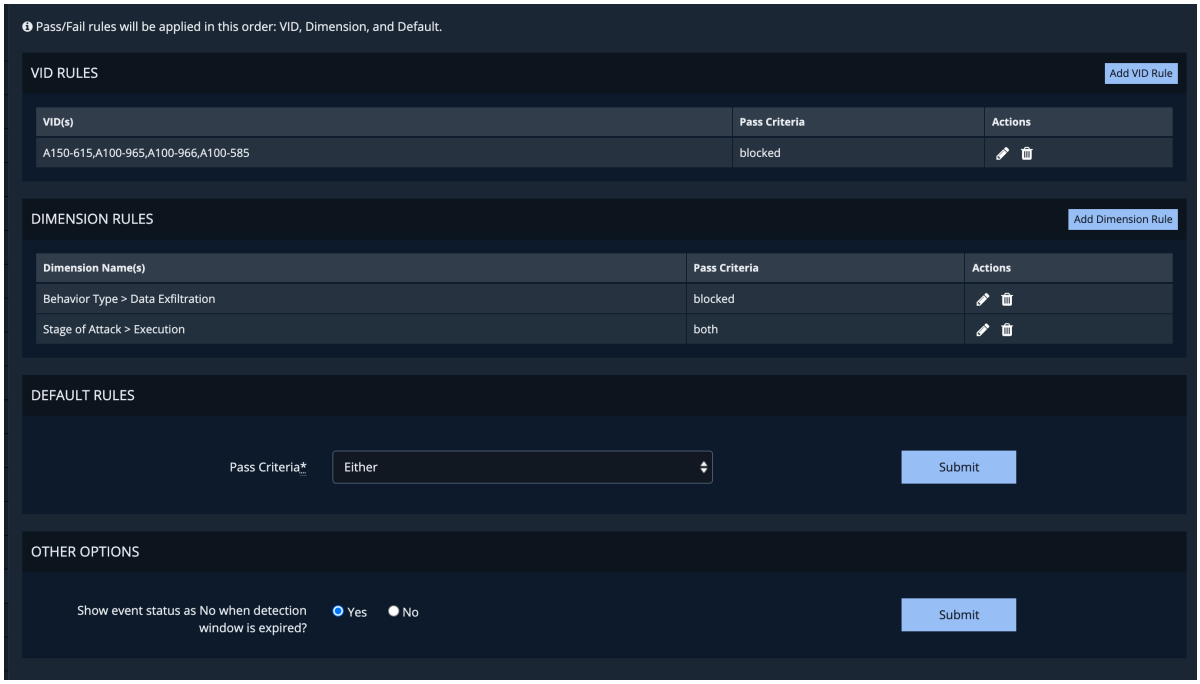
- Either
- Blocked
- Detected
- Both

A Job Action will only have one pass/fail rule applied to it. The platform applies the rules from most specific (VID rules) to most general (the Default rule). For example, if there is a VID and Dimension Rule that impacts a Job Action, the VID rule is used to determine the pass/fail results for the Job. Here are details and explanations for each type of Rule.

Type of Rule	Order / Priority	Example
VID	1	Use when you want to apply specific Pass criteria for an individual Action. • Example: you've created a custom Action that should always be blocked. • Example: you've updated your security requirements for PowerShell execution and you want to your PowerShell Actions to be blocked. • Example: You are waiting on an environment change and you want an Action to fail until it is blocked.
Dimension	2	Configure a Dimension Rule if you have specific requirements for a type of Action. • Example: if your security program says all attempts of Data Exfiltration should be blocked, you can create a Dimension rule to support that.

Type of Rule	Order / Priority	Example
Default	3	Update the default definition as your organization's security posture improves. • Use **Either** when first starting out, or if you're security program is young. • As your security program progresses, you may want to update this to require the Action to be **Blocked** to be considered passed. • You can also require that an Action be **Both** Detected and Blocked for the Job to pass, but verify that your security controls always detect (create an event) when they block something.

TIP: If you need to maintain historic pass/fail information and have AEDA, configuring Monitors is another way to define expected results for Actions.



Pass/Fail Settings page

To Review, Add, or Update the Pass/Fail Rules

1. Launch the Director.
2. Go to **Settings > Director Settings**.
3. Select **Pass/Fail**.
4. Review the existing rules, create or update rules, or set the desired event status.

   IMPORTANT: Any updates you make to the pass/fail rules impacts all Jobs, not just future Jobs. For example, if you update the default rule so a Job Action must be Detected to pass, all jobs that have been run will be reviewed and updated based on their detection status.

5. (Optional) Change the **Show event status as No when detection window is expired?** setting to modify the event status that is attached to an Action that is detected as expired.

Mandiant

Email Rules / Actions

When you run an Email Action, you're testing the response of your email security controls. For Security Validation to understand what the responses mean, and thus determine if the Job Action passes or fails, you must setup **Email Rules (https://docs.mandiant.com/home/msv-email-rules)**. These tell the platform what responses mean the Action was blocked, and thus if the Job Action passes or fails.

Malicious DNS Query Actions

Security Validation doesn't know how to interpret blocked results for Malicious DNS Query Actions without user input. **Creating Rules for Malicious DNS Query Actions (https://docs.mandiant.com/home/msv-dns-servers-settings)** is how you configure the system to identify what Actions should be blocked, leading to the final pass/fail determination.

Host CLI Actions and Cloud Validation Actions

These Actions includes scripts to have certain actions performed on systems. As such, you must build in what your expected blocked conditions are. Otherwise, Security Validation won't know if the Job Action passes or fails.