Mandiant

TESTING RANSOMWARE DEFENSE CONTROLS

This documentation walks you through prerequisites, configuration, and running of Ransomware Defense Validation content for your Security Validation environment. Using the results, you can build comprehensive reports that provide granular details about how protected you are from ransomware.

Get Started with Ransomware Defense in Security Validation

Ransomware Defense Validation (RDV), available for both Mandiant Advantage Security Validation (MA-SV) and Mandiant Security Validation (MSV), delivers a “low touch," safe, and continuous test of whether your security controls can prevent the latest ransomware. It leverages Mandiant’s incident response experience and world-class threat intelligence to provide visibility into your security controls’ ability to alert on or block prevalent ransomware.

Prerequisites

Before you start using RDV, you need to meet the following criteria:

- Actors that are used to run RDV content must be on release 4.12.0.0 or later
- MSV only: The Director must be on release 4.12.0.0 or later
- Have a content pack license and obtain the latest RDV content pack from **Content Pack Downloads (https://docs.mandiant.com/home/msv-content-packs#rdv-packs)**
- Have exclusions established so that the appropriate files are added to your allow list:
  - **Windows Defender: Establish Exclusions (https://docs.mandiant.com/home/msv-windows-defender-establish-exclusions)**
  - **CrowdStrike: Exclusions & Local Logs (https://docs.mandiant.com/home/rdv-crowdstrike-setup)**

RDV Benefits

RDV for Security Validation allows you to run Jobs with RDV content and present the results of those Jobs in Report Builder using special panels. Once you've met the prerequisites, you gain access to the following features:

- **RDV content**: Repurposes actual ransomware and controls it so it can be executed safely. Safely leveraging actual ransomware from likely and prevalent attackers enables authentic and accurate testing of your endpoint security controls in your actual production environment.
- **RDV panels in Report Builder**: Panels in Report Builder that represent summaries and results of any RDV Jobs in a granular fashion. These can also present links to Threat Actors and further details about Ransomware campaigns (MA-SV only).

See **Use Security Validation for Ransomware Defense Validation (https://docs.mandiant.com/home/msv-check-ransomware-exposure-rdv)** for more information.

Check Ransomware Exposure using Security Validation

Security Validation provides a platform for evaluating your security controls in the face of new **ransomware (https://en.wikipedia.org/wiki/Ransomware)**. The incident response experience and threat intelligence of Mandiant can provide insight of your security controls' ability to alert or block prevalent ransomware attacks.

To verify and substantiate your security measures against ransomware, you can do the following:

1. **Select and Run Actions from the Action Library** that cover Ransomware Defense Validation (RDV) workflows.

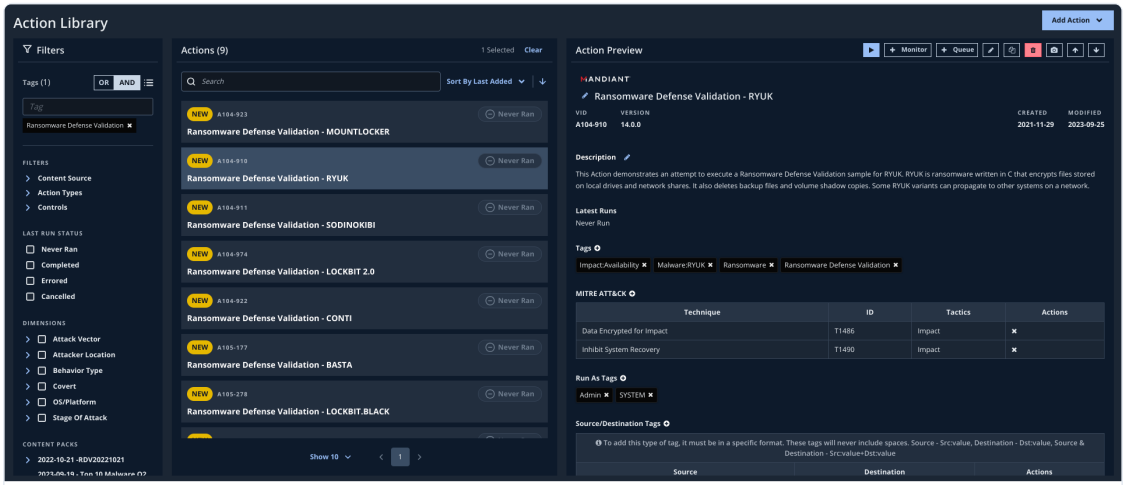
2. **Generate a Ransomware Validation Report**.

All RDV content is tagged with the `Ransomware Defense Validation` system tag.

Video Overview

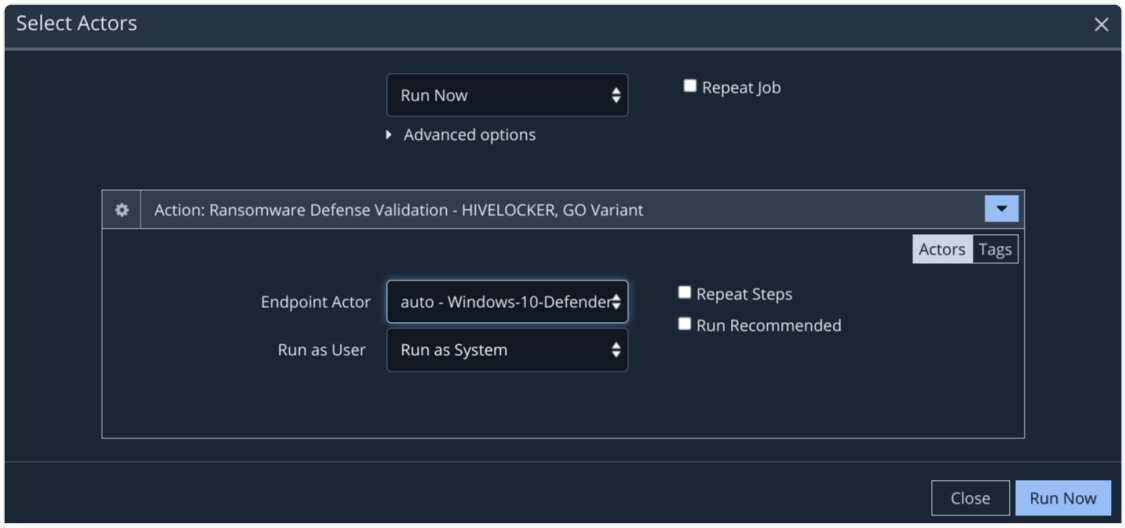
Run RDV Actions

1. Go to **Library > Actions** to open the respective **Actions Library** page.
2. On the **Actions Library** page, add `Ransomware Defense Validation` as a tag to filter on the RDV content.
3. Get a list of ransomware Actions available in the library.



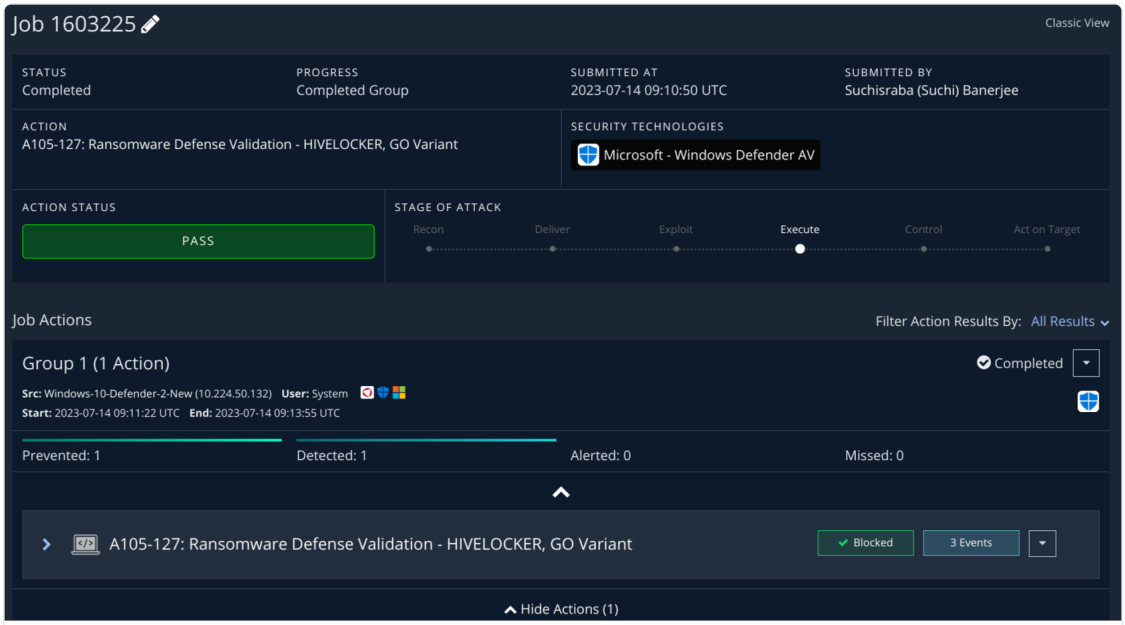
Action Library with Ransomware Defense Validation-tagged Content

4. Select the Action that you want to run and then click **Run**.
5. Select **Actors**.
   - For this example, we'll use a Windows Actor for the **Endpoint Actor**.
   - If needed for your specific Actor, you can change the **Run as User** entry, but it is not required.



Select Actors

6. Click **Run Now** or **Schedule**. When you click Run Now or at the Scheduled time, a Job is created and the Action runs. If you clicked **Run Now**, the Job Results page shows the status and results when the Job completes.



Example of a Completed Job for an RDV Action

7. Repeat the preceding steps if you want to run more ransomware validation Actions.

To learn more about security content and Jobs, refer to **Security Content & Jobs** (https://docs.mandiant.com/home/msv-sc-jobs).

Create a Ransomware Validation Report

After checking your environment for ransomware exposure using the provided Actions, you can use these high-level steps that guide you to the ransomware-specific content widgets that you can add to a report. For more guidance on preparing comprehensive reports, see **Security Validation Reports** (https://docs.mandiant.com/home/msv-reports).

1. Go to **Analyze > Reports**.
2. Click **Create New Report**.
3. Optional: Update the time range and add rules, then click **Continue**.
4. Add one or both of the Ransomware components (**Ransomware Results** and **Ransomware Summary**), which are listed under the **Layout/Structure** section of the **Panel Library**.

The following screenshot shows an example of the **Ransomware Results** and **Ransomware Summary** content widgets after they're added to a report. Two ransomware families, HIVELOCKER and LOCKBIT 2.0, are selected.