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:

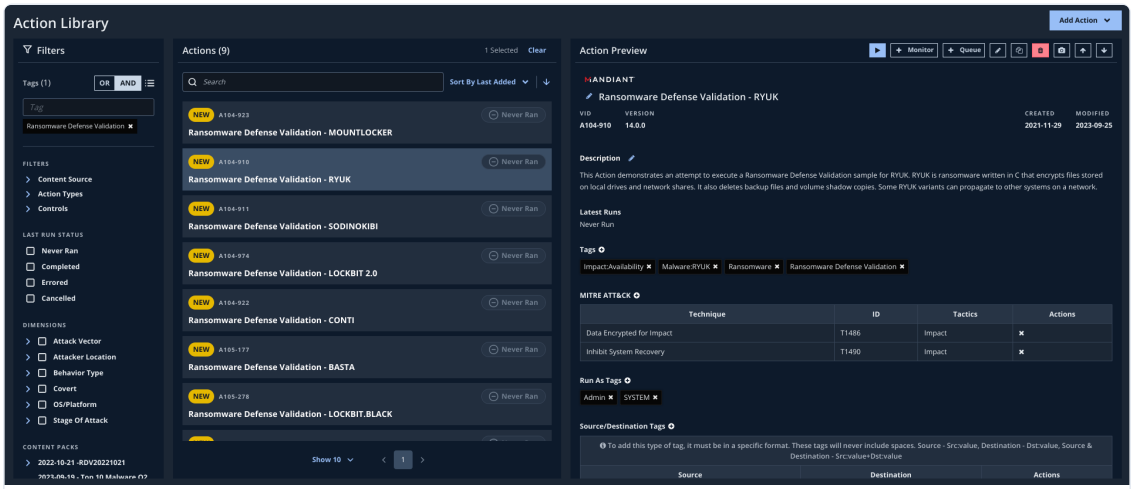
1. **Select and Run Actions from the Action Library** that cover Ransomware Defense Validation (RDV) workflows.
2. **Generate a Ransomware Validation Report**.

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

Video Overview

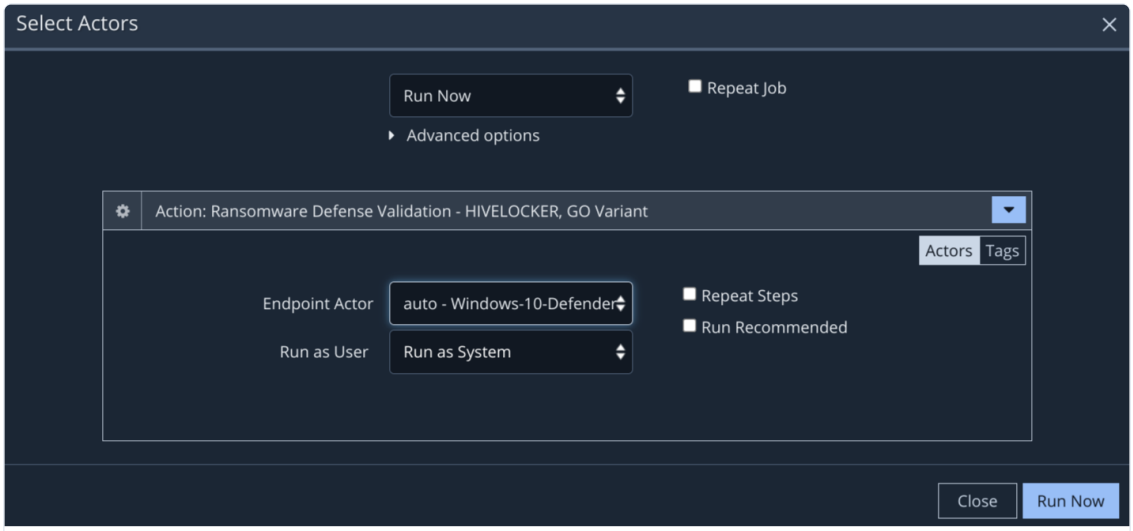
Run RDV Actions

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.



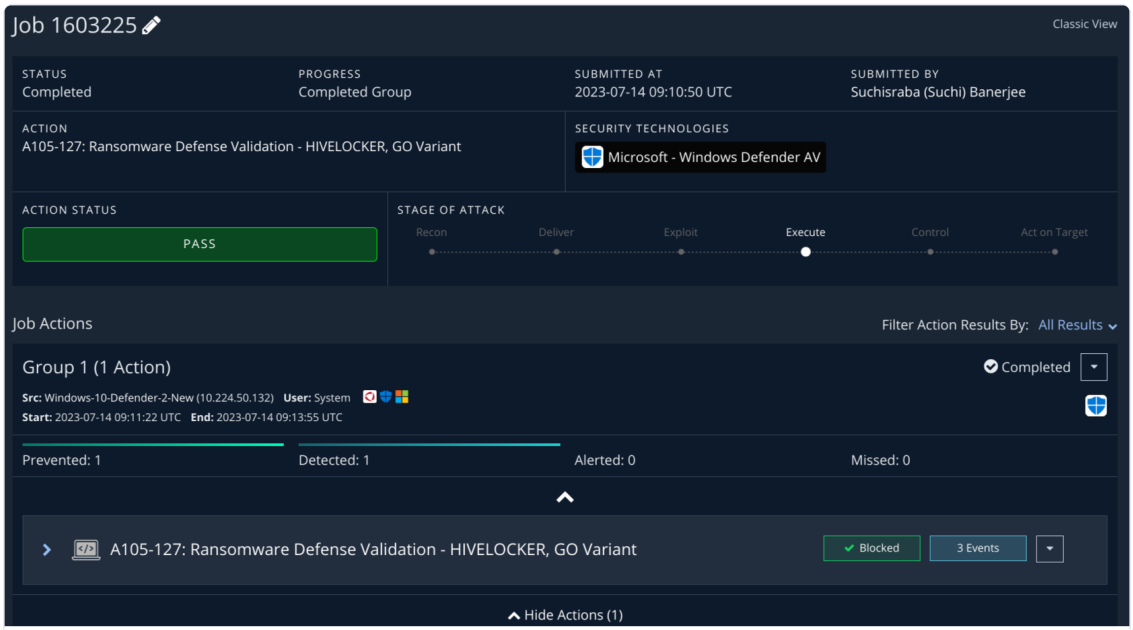
Action Library with Ransomware Defense Validation-tagged Content

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.