RAPID7

Investigating suspected false positives

Table of Contents

Troubleshooting Prerequisites

1. Is the InsightVM Security Console fully updated?

- The latest release notes can be found at https://docs.rapid7.com/release-notes/insightvm/
- To find the running product version on your console:
  - i. Administration > Global and Console Settings section > Administer > General tab.

2. Are the InsightVM Scan Engines fully updated?

- The latest release notes can be found at https://docs.rapid7.com/release-notes/insightvm/
- To find the running product version on each of your Scan Engines:
  - i. Administration > Scan Options section > Engines heading > manage.

3. For findings from an agent-based assessment, is the asset's Insight Agent on the latest version?

- The latest release notes can be found at https://docs.rapid7.com/release-notes/insightagent/
- To find the agent version on a particular asset:
  - i. Data Collection Management > Agents heading > Query Builder field.
  - ii. Search for the asset by hostname, IP address, or unique agent ID if known (Query Builder can assist you as you type).
  - iii. Results table will show the asset's agent version and status.

4. Are your configured scan credentials working properly with the correct permissions/privileges on the assets in question?

- Microsoft Windows
  - i. Protocol: SMB/CIFS (required), Remote PowerShell/WinRM (optional)
  - ii. https://docs.rapid7.com/insightvm/authentication-on-windows-best-practices
  - iii. https://docs.rapid7.com/insightvm/using-powershell-with-your-scans

- **Linux/UNIX and other UNIX-like systems (Apple macOS, HP-UX, IBM AIX, Cisco IOS, VMware ESXi, Juniper JunOS, etc.)**

  i. Protocol: SSH

  ii. https://docs.rapid7.com/insightvm/authentication-on-unix-and-related-targets-best-practices/

- **Scan Assistant**

  i. Option if there are no configured credentials for the asset(s) in question.

  ii. Microsoft Windows and Linux only

    - Supported Microsoft Windows versions:

      - https://docs.rapid7.com/insightvm/scan-assistant-combined#supported-windows-platforms

    - Supported Linux distributions:

      - https://docs.rapid7.com/insightvm/scan-assistant-combined#linux-distributions-by-service-manager-and-package-manager

  iii. https://docs.rapid7.com/insightvm/scan-assistant

5. Is the asset showing the suspected false positive finding reachable over the network from your deployed Scan Engines?

False Positive Investigations Summary

1. Run troubleshooting scan with successful authentication.
2. Generate XML Export 2.0 report.
3. Open support case with Rapid7 Support.

False Positive Investigations Steps

Much of the process is automated using the False Positive Investigations tool built into InsightVM.

1. Navigate to the asset in InsightVM.

2. If the asset has an Insight Agent installed and running, collect the Agent Log through the *Data Collection Management page*.

3. Check if the asset's scan history indicates it has only undergone agent-based assessment (i.e., no Scan Engine scans).

   a. If the asset has never been scanned by your Scan Engines, then there is a possibility that the asset exists outside your network and the *False Positive Investigations* tool will be unable to properly reassess the asset with your configured credentials.

   b. For confirmed agent-only assets, after collecting the agent logs (see step 2), skip to step 9.

4. In the Vulnerabilities table, locate the vulnerability suspected of being a false positive finding.

5. In the Investigations column, click the *Investigate* link.

6. In the Vulnerability Investigations dialogue, the process will be summarized. Click the *Investigate* button to begin the rescan.

   a. The default scan template, *Full Audit Enhanced Logging without Web Spider*, will be used.

7. Once the rescan is completed, click the *Review* link.

8. If the scan results produce the same suspected false positive finding as previous assessments, then it should be reported to Rapid7 using the *Send Results* link.

   a. This will automatically send an XML Export 2.0 report and the scan's data to Rapid7.

9. Collect any other items of interest that would help to explain why you suspect the asset has a false positive finding such as screenshots of Windows Registry values, command-line output, installed patches, hotfixes, and software, users and groups, etc. NOTE: the more visual aids you provide the easier it will be for Rapid7 to assist you.

10. Open a case with Rapid7 Support (Product: InsightVM) and attach:

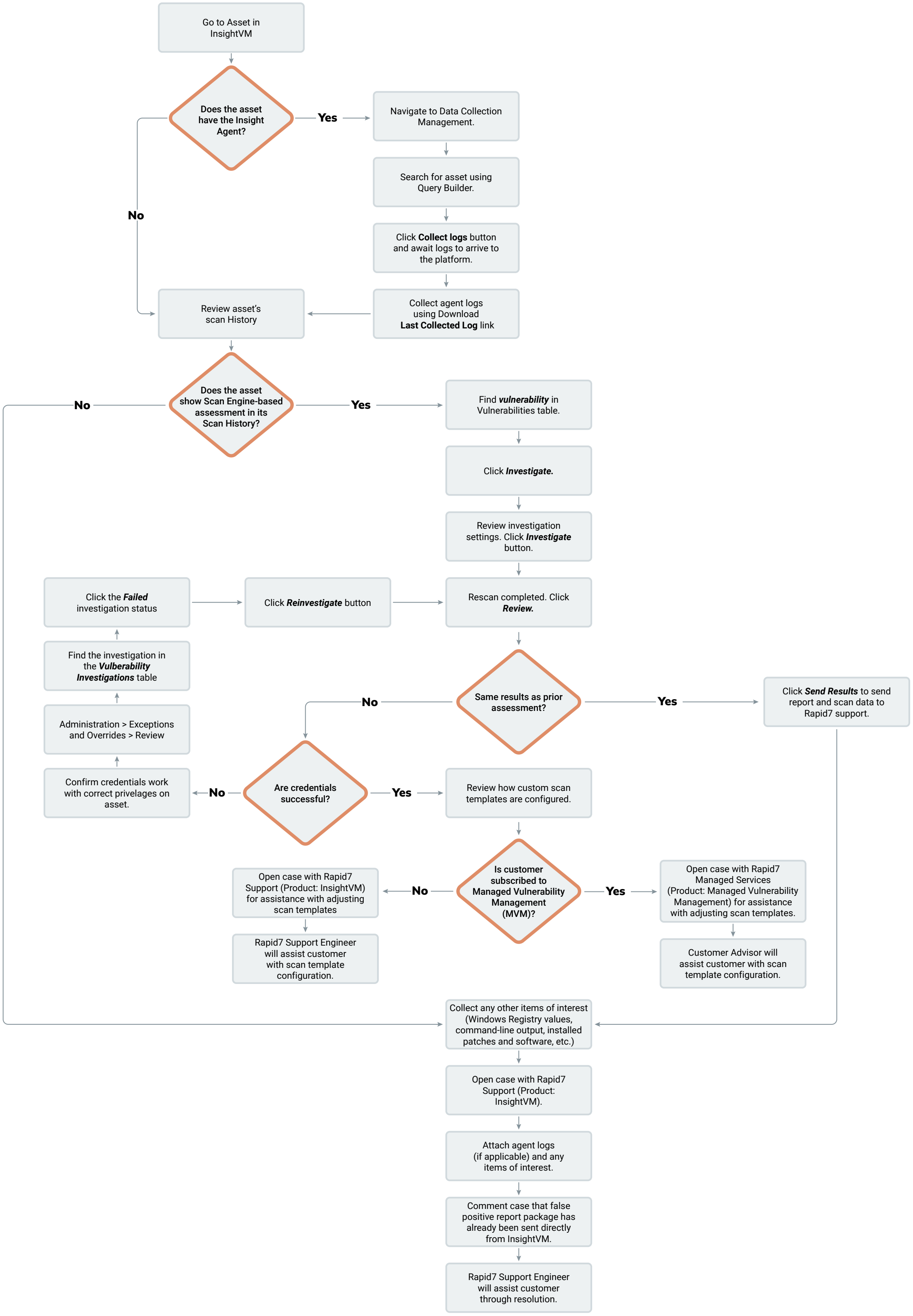
    a. Agent logs (if available)

    b. Other items of interest (see step 8).

11. In the support case, document which specific vulnerabilities you suspect are a false positive and be sure to indicate that you have already submitted a false positive report package directly from InsightVM

12. Once a Rapid7 Support Engineer has reviewed the case, they will communicate with you regarding next steps. Should their review confirm a false positive situation with InsightVM's vulnerability check logic, Rapid7's internal teams will coordinate to evaluate a fix.

False Positive Investigations Workflow



Go to Asset in InsightVM

Does the asset have the Insight Agent?

Yes

Navigate to Data Collection Management.

Search for asset using Query Builder.

Click **Collect logs** button and await logs to arrive to the platform.

Collect agent logs using Download **Last Collected Log** link

No

Review asset's scan History

Does the asset show Scan Engine-based assessment in its Scan History?

Yes

Find ***vulnerability*** in Vulnerabilities table.

Click ***Investigate.***

Review investigation settings. Click ***Investigate*** button.

Rescan completed. Click ***Review.***

Same results as prior assessment?

Yes

Click ***Send Results*** to send report and scan data to Rapid7 support.

No

Are credentials successful?

No

Confirm credentials work with correct privelages on asset.

Administration > Exceptions and Overrides > Review

Find the investigation in the ***Vulberability Investigations*** table

Click the ***Failed*** investigation status

Click ***Reinvestigate*** button

Yes

Review how custom scan templates are configured.

Is customer subscribed to Managed Vulnerability Management (MVM)?

No

Open case with Rapid7 Support (Product: InsightVM) for assistance with adjusting scan templates

Rapid7 Support Engineer will assist customer with scan template configuration.

Yes

Open case with Rapid7 Managed Services (Product: Managed Vulnerability Management) for assistance with adjusting scan templates.

Customer Advisor will assist customer with scan template configuration.

No

Collect any other items of interest (Windows Registry values, command-line output, installed patches and software, etc.)

Open case with Rapid7 Support (Product: InsightVM).

Attach agent logs (if applicable) and any items of interest.

Comment case that false positive report package has already been sent directly from InsightVM.

Rapid7 Support Engineer will assist customer through resolution.

Situations with Single or Multiple Suspected False Positives on One or More Assets

If you suspect multiple false positives (single or multiple unique vulnerabilities) across many assets, the investigations process will be more involved. But it will lead to a similar outcome as the previous process for a single suspected false positive on a single asset. Depending on the number of suspected false positive vulnerability findings and the number of assets involved, you will need to select a representative sample of the assets for investigation.

1. Once you have selected a sample of assets, run through the playbook as described above for each asset.
   a. You do not need to run an investigation for each unique false positive finding per asset; **only run a single investigation per asset**. If the situation involves multiple potential false positive findings, simply pick a single vulnerability on the asset to start the investigation. The XML Export 2.0 report and the asset's scan data will cover all vulnerabilities including the other vulnerabilities you suspect are false positives on the asset.

2. In step 8 of the playbook, make sure to collect any other items of interest (screenshots of Windows Registry keys and values, installed patches and software, configuration file content, etc.) **for each asset you performed an investigation against**. Make sure these files are clearly marked by asset name and IP address and attach them to the case as indicated in step 9.

3. In step 10 of the playbook, note the names of each asset an investigation was performed on. Additionally, indicate by title which specific vulnerabilities you suspect are false positives along with your reasoning as to why these are being incorrectly reported by InsightVM.

Note: when you suspect multiple false positive vulnerabilities on one or more assets, and you list those vulnerabilities accordingly, Rapid7 Support will collaborate with you to investigate each specific vulnerability listed in a sequential manner until all suspected false positive findings are resolved. Once a Rapid7 Support Engineer has reviewed the case, they will communicate with you regarding next steps. Should the review confirm a false positive with InsightVM's vulnerability check logic, Rapid7's internal teams will coordinate to evaluate any fixes.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/