Optimizing Exposure Management: RidgeBot® Validates and Prioritizes InsightVM Findings

Executive Summary

The fast-evolving threat landscape combined with increasing organizational and technological intricacies create an exceedingly complex environment that leaves organizations vulnerable to attack. Combining leading security tools—such as Rapid7 InsightVM's asset scanning, extensive vulnerability database, and vulnerability detection with Ridge Security RidgeBot's automated exploitation and validation—continuously probe the resilience of your assets to identify the highest priority vulnerabilities that pose an active breach risk to your organization.

The integration draws together Rapid7's expert research and data-rich resources of the latest vulnerabilities with RidgeBot's automated continuous vulnerability validation to provide a dashboard of insightful, actionable, accurate and timely threat intelligence to your SecOps team.

The Challenge

Attack surfaces continue to expand dramatically due to increasing adoption of cloud workloads and data storage, a significant WFA workforce, virtualization of the network perimeter, and evermore sophisticated cybercriminals and attack resources. To stay a step ahead of the bad actors, you require an adaptive, automated ecosystem of specialized security tools integrated into an operational interface for immediate visibility and situational awareness to maximize rapid SecOps response and action.

Joint Solution Description

The integration of Rapid7's vulnerability scanning with RidgeBot's automated exploitation strengthens your cybersecurity threat intelligence. The combined solution leverages the capabilities of Rapid7's vulnerability scanning driven by its extensive and continually updated databases, with RidgeBot's active exploitation validation to distil out the highest urgency real risks among the detected vulnerabilities.

Rapid7 InsightVM scans your assets and provides a list of the vulnerabilities identified. RidgeBot® receives this detailed list and proceeds to exploit these vulnerabilities to prioritize the active risk that each one poses. A proportion of the theoretical vulnerabilities may be minor or inconsequential, but the successfully exploitable ones pose a real risk to your assets. With this information, your SecOps team can immediately focus on—and remediate—the most perilous vulnerabilities to have the highest impact, in the shortest time, using the least resources, to best protect your assets.

Solution Components

Ridge Security RidgeBot®

Security validation AI agent that continuously probes and validates your network and assets. Results prioritize exploitable vulnerabilities and provide remedial steps.

Rapid7 InsightVM

Vulnerability management capabilities to assess vulnerabilities using its extensive and continually updated databases. Provides comprehensive management capabilities to gain asset visibility, track your patch schedule, and report on threat intelligence.

Solution Benefits

- **High-impact Remediation and Reporting**
  Provide better IT tools to understand active risk. Speed up remediation with automation and track remediation progress with dashboards and reports. Gain higher precision by focusing on critical exploitable vulnerabilities that must be addressed promptly.

- **Compliance with Policy and Regulatory Requirements**
  Automated, repeatable assessment of your assets against industry benchmarks.

- **Reduce Business Risk**
  Use intelligence from Rapid7 research labs to identify internet-facing assets and vulnerabilities. The integration helps to:

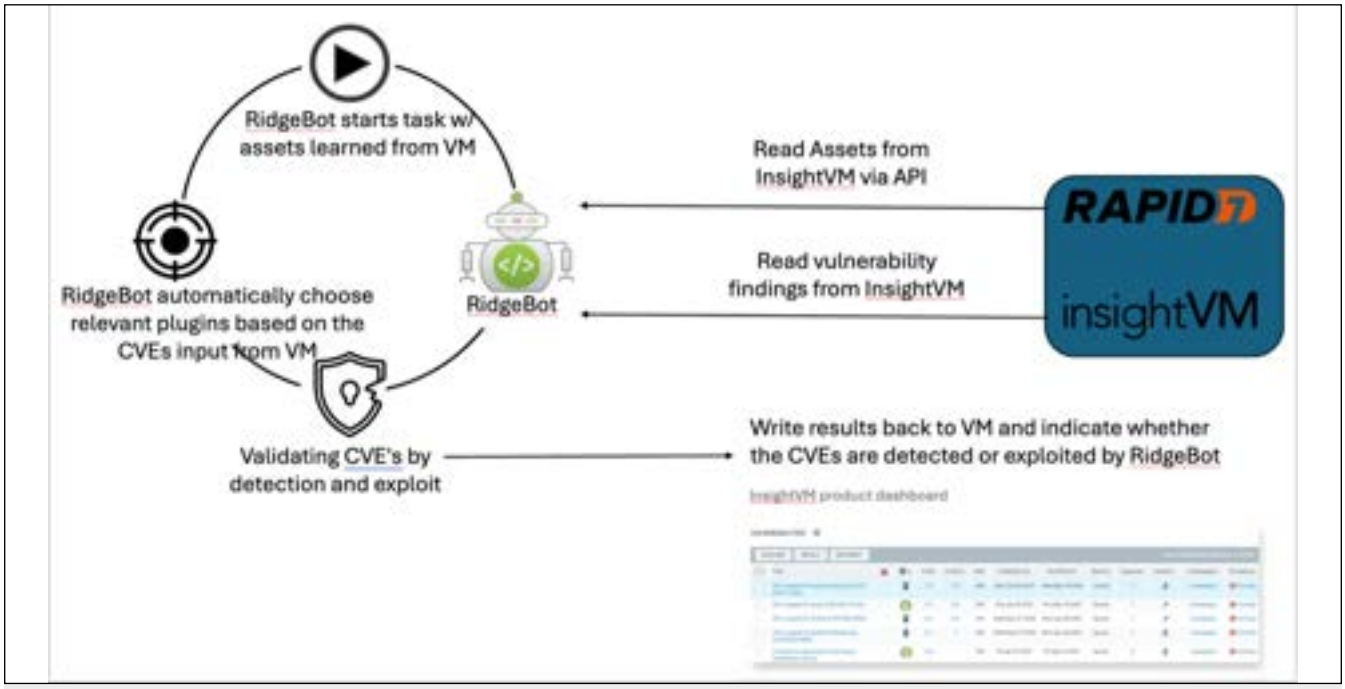
  - Transform raw data into actionable intelligence to enable your SecOps team to make quicker and better-informed decisions.
  - Provide a comprehensive view of your organization's security posture.
  - Provide clarity into how detected vulnerabilities translate into business risk and which ones are most likely to be targeted by attackers.

- **Streamline Vulnerability Management**
  Gain expanded visibility into your IT assets. Discover and prioritize active critical vulnerabilities for remediation. By integrating RidgeBot® exploitation with Rapid7 scanning, vulnerabilities detected can be tested for exploitability in real-time, immediately distinguishing between theoretical vulnerabilities and those that pose a real risk.

- **Cost and Efficiency**
  The integration automates the flow of information—RidgeBot® can automatically initiate exploitation tests based on the latest vulnerability scan results. By default, the integration uses non-impactful plugins to exploit vulnerabilities, ensuring no disruption of enterprise environments. You can optionally enable impactful plugins for more thorough probing in environments where needed. By verifying which vulnerabilities are actively exploitable, RidgeBot® helps reduce the time and resources spent on false positives and minor risks.

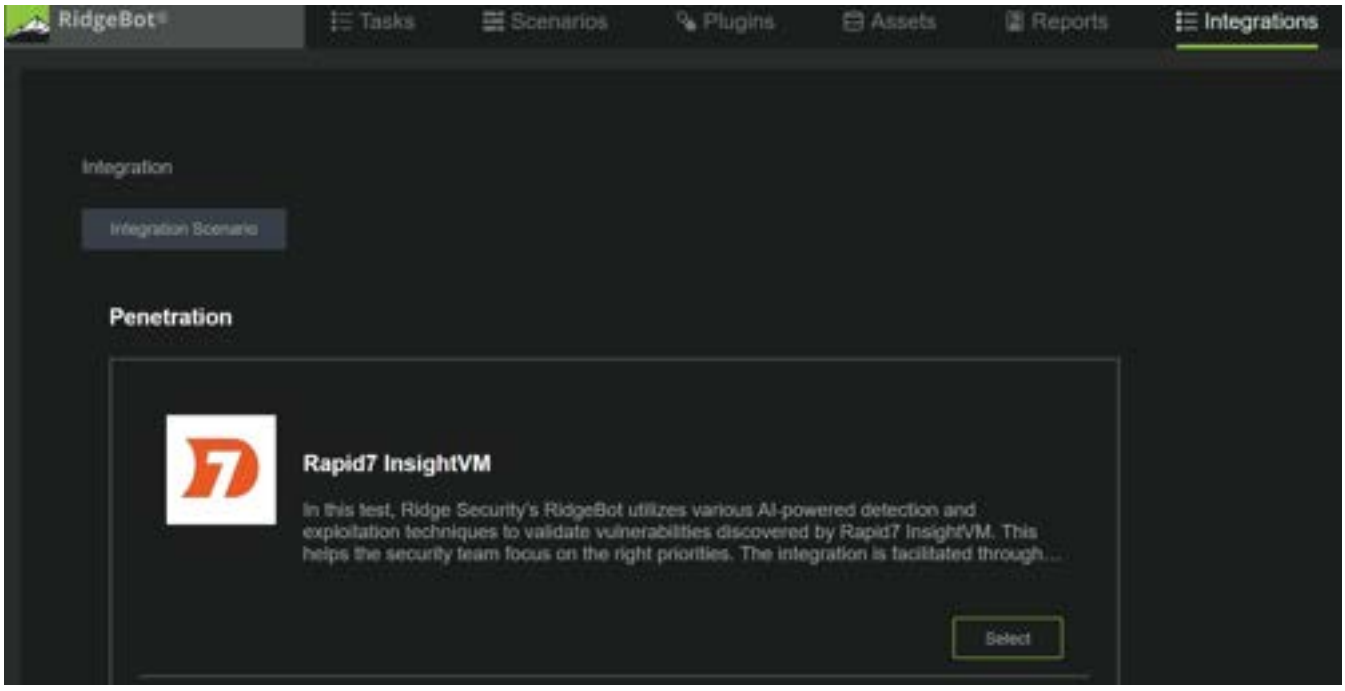
Joint Solution Integration

Ridge Security RidgeBot® facilitates automated vulnerability scanning and exploitation by creating a task to run on the Rapid7 InsightVM server, and then importing the results of identified vulnerabilities. RidgeBot® can then immediately attempt to exploit these vulnerabilities to provide your SecOps team with a prioritized list of the highest risk items to be remediated.



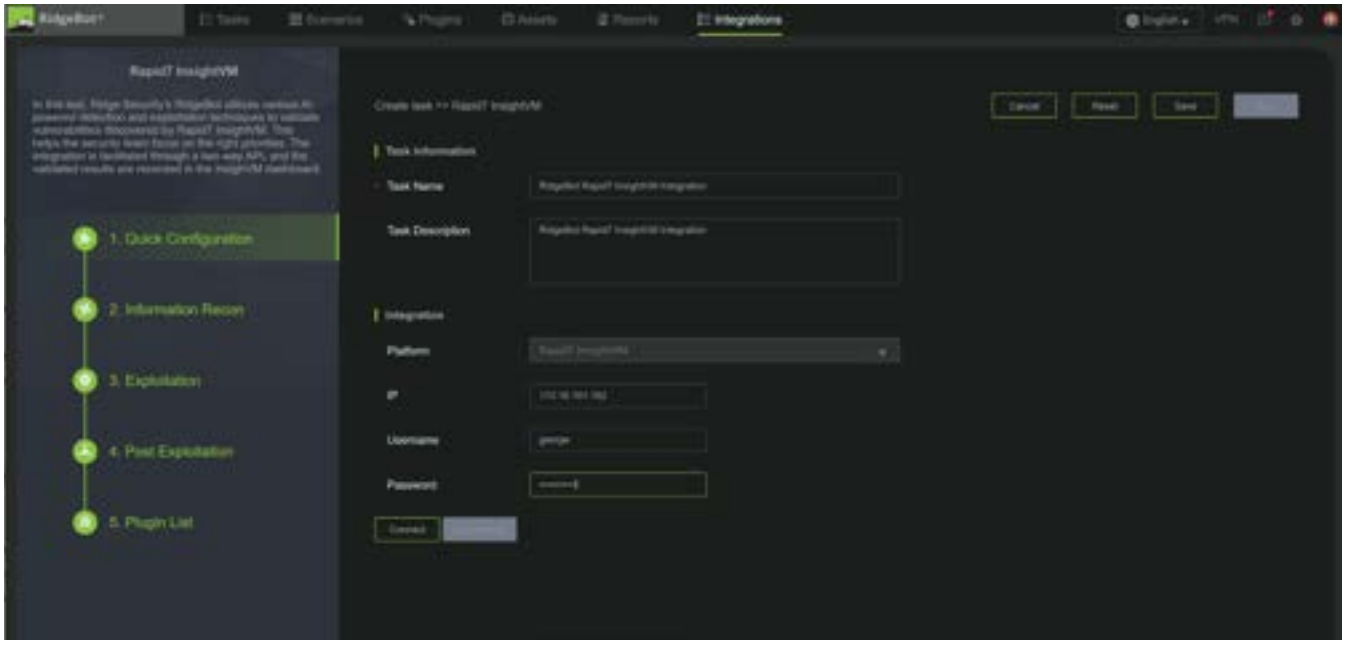
Integrating Rapid7 InsightVM Scanning with RidgeBot® Vulnerability Exploitation

From the RidgeBot® UI, choose the Rapid7 InsightVM integration.

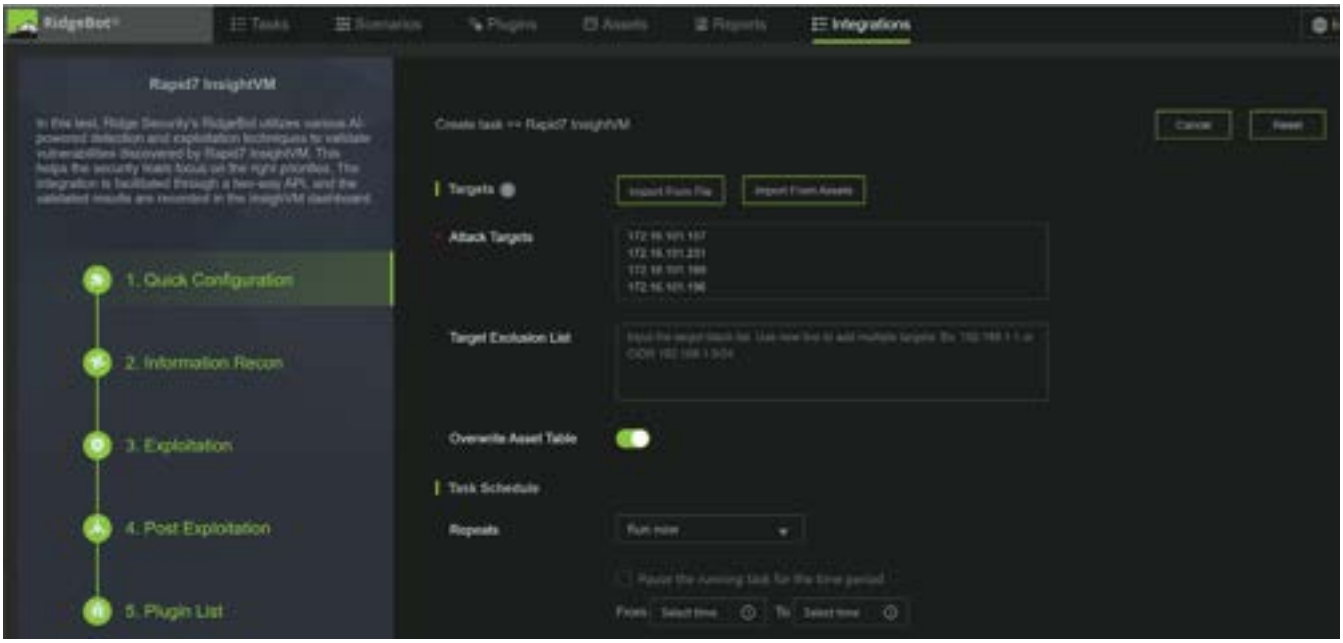


Configure the Rapid7 InsightVM server IP address, user name and authorization credentials, then select “Connect”.

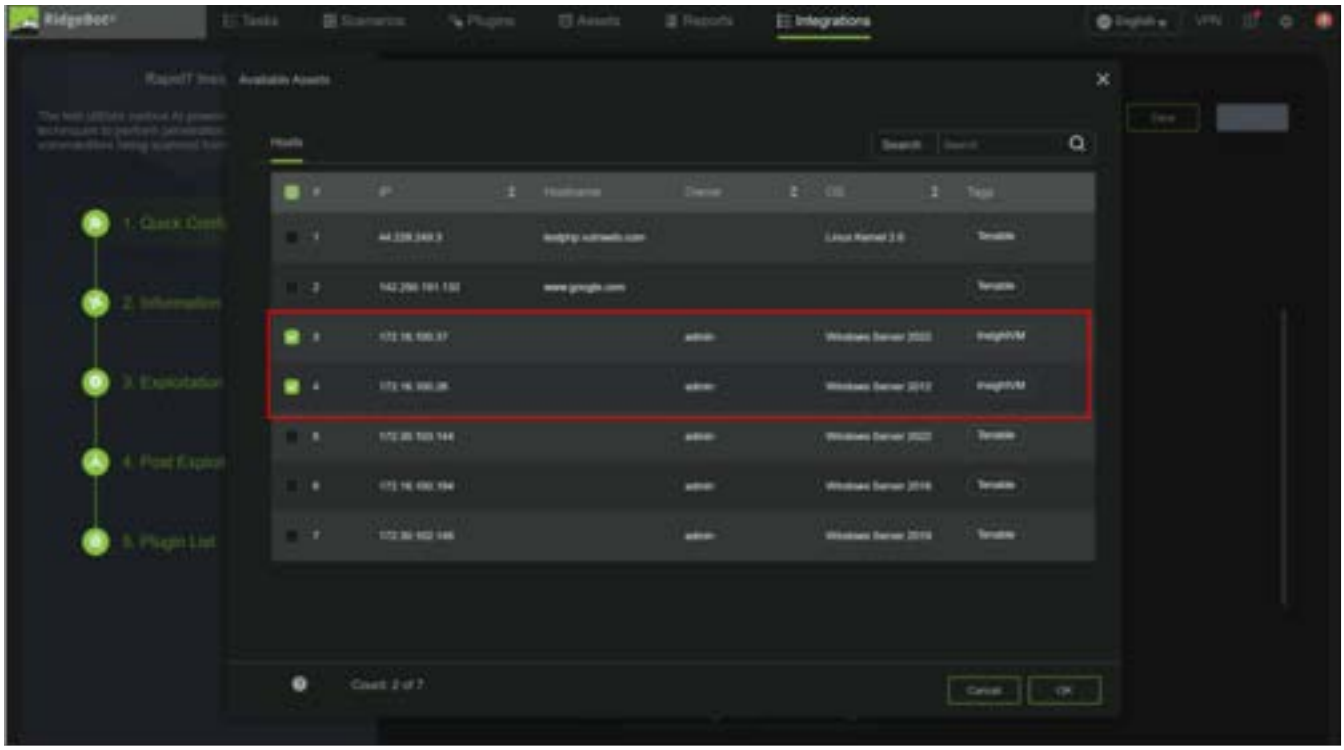
Once authenticated, you can also click the “Synchronize” button to collect the latest assets and vulnerabilities discovered by Rapid7 InsightVM.



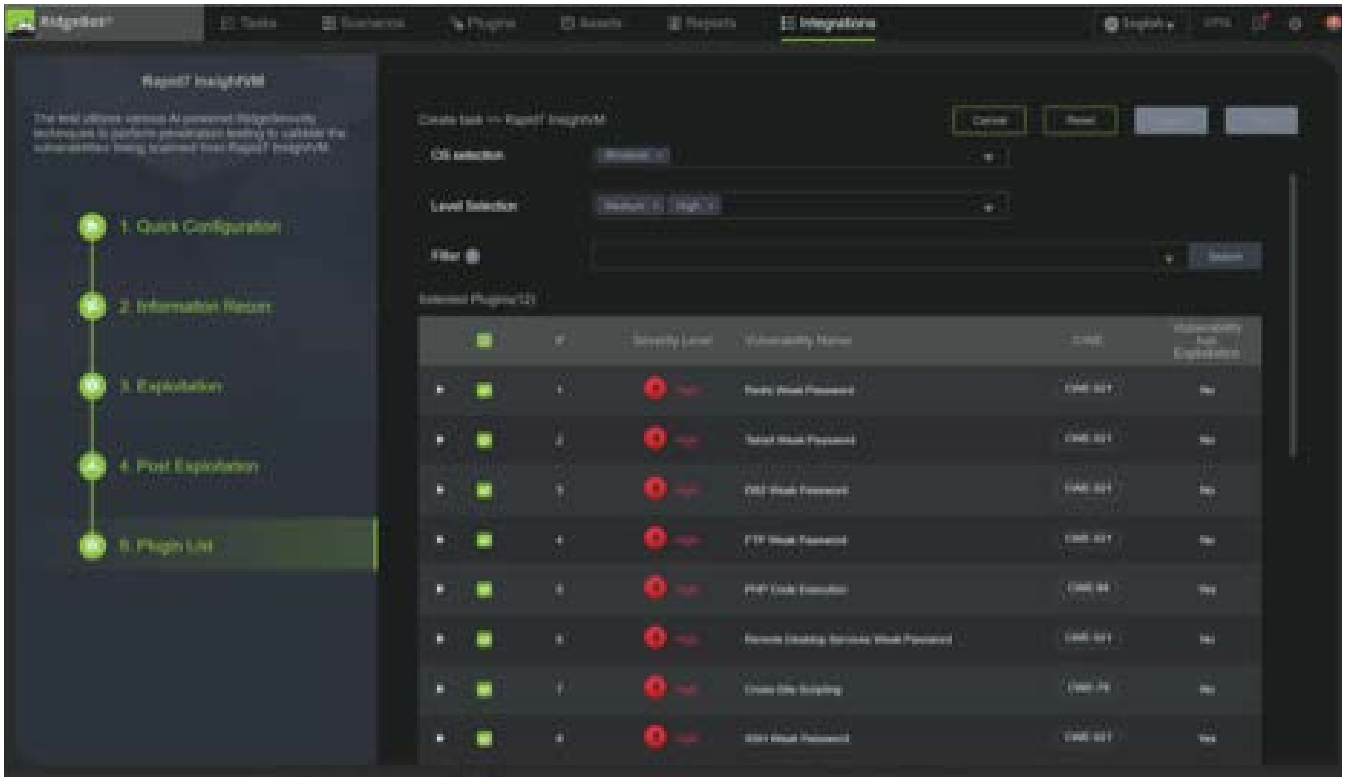
On the next screen, you can click the “Import From Assets” button to import a view of all assets discovered by Rapid7 scanning.



On the next screen, you can select the asset targets to be validated by RidgeBot®.

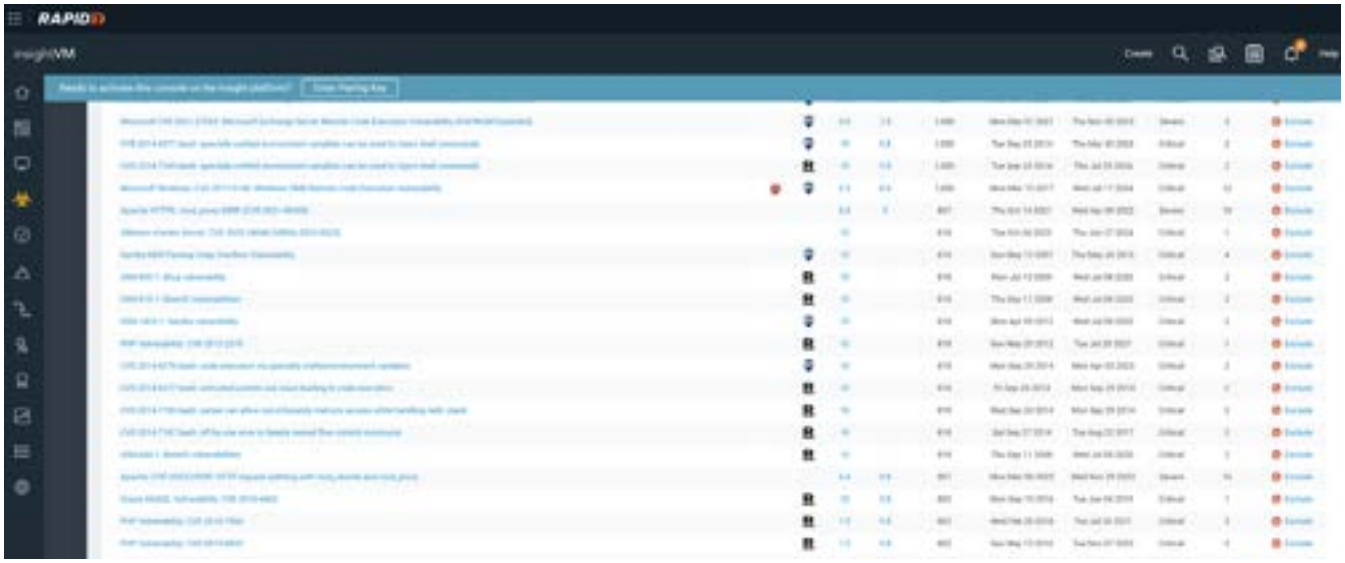


RidgeBot® automatically picks plugin groups based on the vulnerabilities discovered by Rapid7.



Once the RidgeBot®/Rapid7 integration task is started, you can see task status and progress in the task view pane.

When RidgeBot® completes its exploitation task, you can generate and download a report. The vulnerability validation results are also automatically exported back to the Rapid7 InsightVM server for display.



Joint Use Cases

With RidgeBot® integration with Rapid7, you can automate asset scanning, vulnerability identification, and vulnerability exploitation to quickly gain visibility into a prioritized list of the highest impact remedial actions to take to immediately lower your business risk.

About Ridge Security RidgeBot®

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity solutions designed to protect organizations from advanced cyber threats. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation. With a focus on automation, intelligence, and actionable insights, Ridge Security enables security teams to proactively defend against and respond to evolving cyber challenges.