RAPID7

SOLUTION BRIEF

Streamlining Vulnerability Management: Pairing InsightConnect with InsightVM

Improve how your team discovers, prioritizes, and addresses vulnerabilities.

With the continuously evolving threat landscape, it's more important than ever to address critical vulnerabilities quickly—before they're exploited by attackers. The problem? Security teams have a backlog of work, and the number of manual steps, decisions, and processes required to push a single vulnerability from discovery to remediation or containment can cause audible groans.

With targeted automation, you can reduce friction, remove (or at least simplify) repetitive processes, and drive the high performance necessary to collaborate and close vulnerabilities more efficiently.

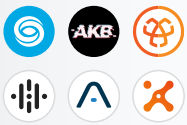
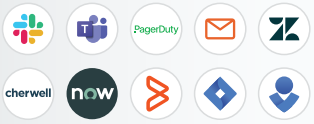
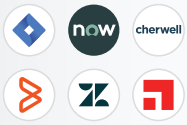
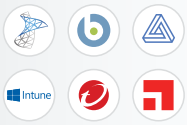
> **Automation is the only way we can keep up with vulnerabilities. There is just no other way we could do it with our infrastructure.**
>
> Rapid7 Insight Platform Customer

Key Benefits of Using InsightConnect with InsightVM

- ✓ Streamline communication with security, IT, application development, and other teams
- ✓ Continuously update asset inventories for maximum visibility
- ✓ Accelerate visibility of critical vulnerabilities and the potential impact
- ✓ Quickly prioritize and communicate remediation activities
- ✓ Streamline remediation tasks to improve IT and security productivity
- ✓ Enable efficient validation of remediation and patching
- ✓ Improve and ease cross-functional collaboration by leveraging preferred communication channels and systems

InsightConnect, Rapid7's SOAR solution, enables your team to automate many types of vulnerability management tasks in conjunction with InsightVM, Rapid7's vulnerability management solution:

- Group and assign tickets to specific internal stakeholders based on asset groups
- Verify successful patching via chat commands
- Updating CMDB configuration items (CIs) based on InsightVM asset discoveries
- Streamline exception management and IT information requests
- Notify and stage patches for newly discovered and critical vulnerabilities
- Immediately protect vulnerable assets that can't be immediately patched with mitigating controls such as firewall updates, endpoint quarantines, and increased security monitoring

Vulnerability Management Requirements	Example InsightConnect Workflow	Some Supporting Integrations
Visibility and context on assets across a hybrid environment (cloud/on-premises)	Integrate with a CMDB or the corporate directory to share data when new assets are discovered as a result of a scan	
Assess vulnerability exposure and risk continuously	Incorporate data from threat intelligence feeds to enrich vulnerability discoveries and aide in prioritizing remediation activity.	
Communicate vulnerability exposure and risk continuously	Leverage existing enterprise systems and processes such as Chatops and ITSM systems to notify and collaborate on critical vulnerabilities	
Analyze and prioritize critical vulnerabilities and coordinate response plan	Automatically create, assign, and update remediation tasks in the organization's ITSM to understand current security posture and remediation progress or friction points.	
Mitigate vulnerabilities during exposure period	Apply mitigation measures or mitigating controls to high risk assets during the period of exposure	
Remediate, patch, and validate	Group, stage and deploy patches in test environments and communicate production patch deployment status via Slack or Microsoft Teams	

insightCloudSec | insightIDR | ThreatCommand | insightVM

insightAppSec | insightConnect | Security Services

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

Support

Customer Portal | Call +1.866.380.8113