SOLUTION BRIEF

# Automated External Threat Intelligence for Continuous Vulnerability Management

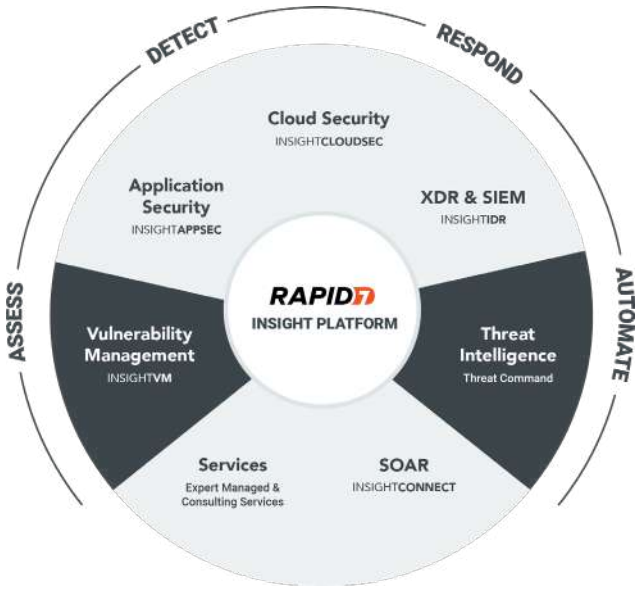
## Rapid7 Threat Command Vulnerability Risk Analyzer + InsightVM

Security teams are inundated with many more vulnerabilities and alerts than they can possibly address. A mandatory component of an effective cyber defense is a prioritized and automated response to threats relevant to your organization, which is precisely what the integration of Rapid7's Threat Command Vulnerability Risk Analyzer and InsightVM delivers.

The traditional Common Vulnerability Scoring System (CVSS) lacks valuable context, including hacker motivation, intentions, and readiness to exploit vulnerabilities. Since all vulnerabilities cannot and should not be remediated at the same time, automated prioritization of critical vulnerabilities is essential.

### Integration Benefits

- **Visibility:** Continuously monitor assets and associated vulnerabilities.
- **Speed:** Instantly assess risk from emerging vulnerabilities and improve patching cadence.
- **Assessment:** Eliminate blind spots with enhanced vulnerability coverage.
- **Productivity:** Reduce time security analysts spend searching for threats by 75% or more.
- **Prioritization:** Focus on the vulnerabilities that matter most.
- **Automation:** Integrate CVEs enriched with threat intelligence into existing security stack.
- **Simplification:** Rely on intuitive dashboards for centralized vulnerability management.



## Features and Capabilities

- Automated risk-based CVE patching prioritization
- Accelerated patch management vs. legacy resource-intensive process
- Continuous CVE assessment for instant adjustments to ensure risk score accuracy
- Visibility into vulnerabilities being exploited in the wild and linked to adversarial campaigns targeting the organization
- Read the Vulnerability Risk Analyzer Data Sheet (link to rebranded version) to learn more.

The VRA + IVM integration merges the capabilities of two foundational pillars of the Rapid7 Insight platform and offers customers complete visibility into assets and prioritized vulnerabilities across the organization. IVM scans, detects, and helps customers prioritize vulnerability mitigation based on technical and open-source parameters, while VRA provides valuable context based on threat intelligence.

Security teams get relevant, risk-scored CVEs enriched with external threat intelligence, leveling up the vulnerability patch management process. This integration enables IVM customers to instantly sync vulnerabilities and prioritize CVE patching based on risk severity.

### Threat Command Vulnerability Risk Analyzer

VRA instantly assesses risk from emerging vulnerabilities by delivering real-time external threat intelligence surrounding organization-specific CVEs, supplemented by a proprietary risk-based prioritization score. VRA automatically enriches CVEs with valuable context and prioritizes vulnerability criticality, eliminating the guesswork of manually determining which CVEs should be patched first. Security practitioners can assess the external risk posed from every CVE and patch vulnerabilities based on relevance.

**VRA is a bridge connecting objective critical data with contextualized threat intelligence.**

Read the **Vulnerability Risk Analyzer Solution Brief** to learn more.

### InsightVM

Rapid7 IVM enables you to stay one step ahead of bad actors by providing clarity into where risk is present across your ecosystem, as well as visibility into the actions required to prioritize and remediate those vulnerabilities.

With this deep and accurate understanding of your risk, you can better prepare and align technical teams for prioritization through remediation.

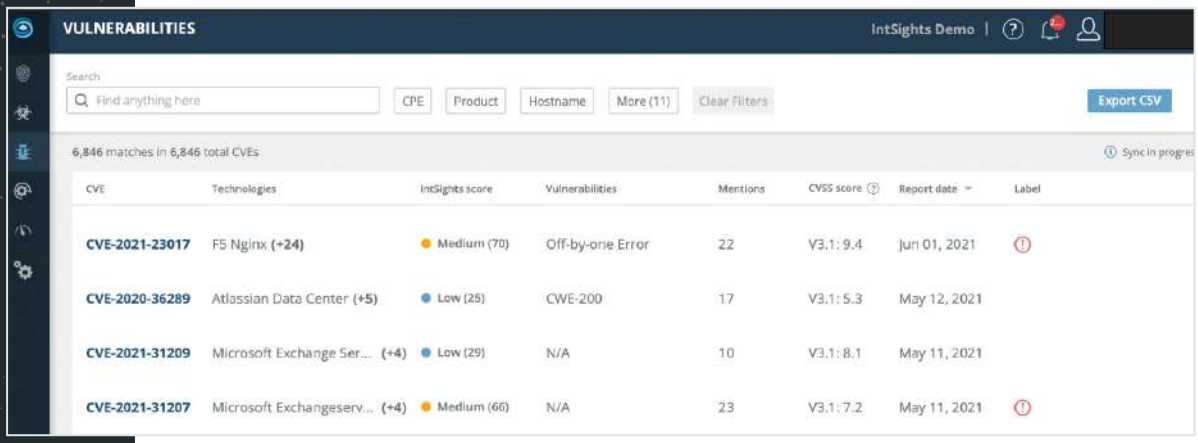
### Integration Overview: How It Works

Vulnerability Risk Analyzer continuously pulls CVE and host data from InsightVM. Robust enrichment data allows users to review and filter relevant clear, deep, and dark web intelligence from specific sources and by risk score for granular CVE risk assessment.

Prioritization scores are calculated by measuring several factors, including trends and findings from both non-malicious actors (security experts, IT personnel) as well as hackers and malicious actors (dark web, hacker forums, social media, etc.). Each CVE description includes a trendline showing the level of activity over time. Exploits for CVEs and the actual code snippets used to leverage the CVE are displayed, giving security teams visibility into how attackers exploit the vulnerability.

Additionally, users can leverage Rapid7 threat intelligence by tapping into our TIP Threat Library and Investigation module. WIth these tools, cyber threats are translated into IOCs that can be used to detect, block, and mitigate threats in your environment.

The VRA integration with InsightVM provides customers with complete visibility into assets and vulnerabilities across the organization's attack surface.




## Get Started Today

First, integrate your IVM account so that you can import CVEs to the Threat Command VRA.

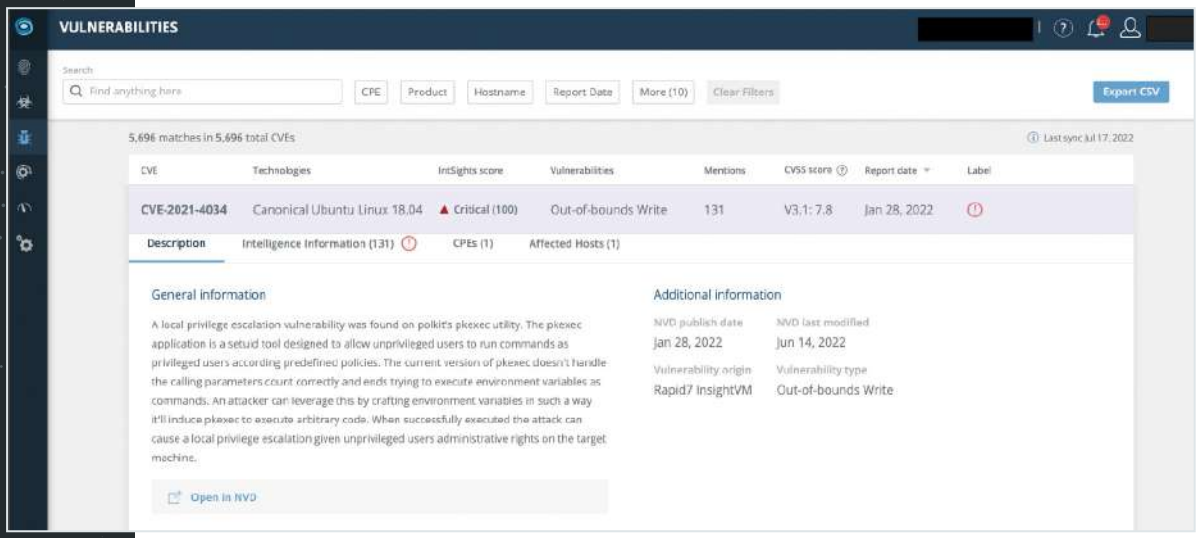
**InsightVM customers: Login to your IVM account and follow these steps:**

1. From the platform, click on the **Settings** icon > **API Keys**.
2. From the **Organization Key** tab, click on the **New organization key** button.
3. Type a user-defined name for the API key.
4. Copy the API key.

**To import CVEs to the VRA module, follow these steps:**

1. From the platform, select **Automation > Integrations**.
2. From the **Integrations** window, click **Cloud**.
   Click **Add new device**.
3. Type a user-defined name for the device.
4. For the **Device type**, select **Rapid7 InsightVM**.
5. Type in your InsightVM API key token along with the Region in which your data is physically stored.
   It is recommended to click **Test Credentials** to ensure that the key and region are valid.
   If the key or region is not valid, a message is displayed.
6. Click Add.

Once the connection is established, VRA will continuously pull relevant CVEs from your IVM instance. CVE data imported from IVM will display in the **Risk Analyzer > Vulnerabilities** page.




## About Rapid7

With Rapid7 (NASDAQ: RPD), security and IT professionals gain the clarity and confidence they need to protect against risk and drive innovation. Rapid7 analytics transform data into answers, eliminating blind spots and giving customers the insight they need to securely develop and operate today's sophisticated IT infrastructures, networks, and applications.

Rapid7 solutions include vulnerability management, penetration testing, application security, incident detection and response, SIEM and log management, and offers managed and consulting services across its portfolio.

To learn more about Rapid7 or get involved in our threat research, visit **www.rapid7.com**.

PRODUCTS

insightCloudSec | insightIDR | Threat Command

insightVM | insightAppSec | insightConnect

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

SUPPORT

Customer Portal | Call +1.866.380.8113

RAPID7