Own your risk with
Vulcan Cyber
and Red Hat Insights

In today's complex IT landscape, enterprises face an overwhelming number of vulnerabilities, often struggling to identify and fix them before they are exploited. Delayed remediation leaves systems exposed, threatening business operations, and increasing the risk of costly security breaches.

> *60% of breaches involve vulnerabilities that could have been patched but weren't addressed in time* (Ponemon Institute).   **Did you know?**

Security teams need a proactive, unified solution to correlate, prioritize, and remediate vulnerabilities across their environments to help mitigate critical risks in time. This is where enabled integration of Vulcan Cyber and Red Hat Insights comes in.

A more seamless integration for effective exposure management

Vulcan Cyber collaborated with Red Hat insights to provide businesses with a holistic view of exposure risk across all attack surfaces and asset types.

Red Hat Insights takes the first step by offering visibility into common vulnerabilities and exposures (CVEs) and configuration issues. Vulcan Cyber then takes it a step further by integrating findings from additional scanners and enriching them with threat intelligence and business context, transforming them into actionable, prioritized tasks for R&D and IT teams.

How it works

1. **Connect Red Hat Insights to Vulcan Cyber:** The Red Hat Insights connector enables a more seamless sync between the two platforms, automatically ingesting vulnerability data from your Red Hat Insights system into the Vulcan Cyber ExposureOS.

2. **Prioritize and assess risk:** The Vulcan Cyber ExposureOS automatically evaluates the vulnerabilities discovered by Red Hat Insights, considering the risk they pose based on real-world threat intelligence and your unique business context.

3. **Automate remediation:** Once prioritized, the Vulcan Cyber ExposureOS automates remediation tasks through your ticketing system (e.g., Jira, ServiceNow) and provides asset owners with the most efficient fixes to apply, such as patches or configuration changes.

4. **Continuous monitoring:** Keep track of remediation progress and easily communicate risk data across teams by leveraging the Vulcan Cyber ExposureOS advanced reporting and dashboards.

Collect Red Hat data | Enrich and prioritize findings | Fix critical vulnerabilities

Better together: Empowering security and IT teams

- **End-to-end risk management:** Gain complete visibility into your exposure risk and effectively mitigate critical vulnerabilities across the attack surface.

- **Reduce MTTR:** Empower teams to address vulnerabilities more quickly to shorten the loop from identification to remediation and minimize the exposure window.

- **Prioritize based on real-world risk:** Identify the vulnerabilities that matter most to your business and allocate remediation efforts where they are most needed.

- **Collaborate more seamlessly:** Bridge the gap between security and IT teams by embedding remediation tasks directly into the tools they already use.

Take the next step in your exposure management journey

Vulcan Cyber and Red Hat Insights go beyond just identifying risks—we help you take a proactive and unified approach by prioritizing and automating the remediation of critical vulnerabilities across all your attack surfaces.

By harnessing Red Hat Insights' deep visibility into host vulnerabilities, paired with the Vulcan Cyber holistic view, intelligent risk scoring, and automated workflows, your teams will be empowered to resolve issues faster, enhance collaboration between security and IT teams, and ultimately reduce the risk of security breaches.

In today's fast-evolving threat landscape, where time-to-remediation is critical, this integration provides an indispensable advantage. To experience firsthand how this solution can elevate your exposure management strategy, schedule a demo today.

See Vulcan Cyber and Red Hat Insights in action >>

VULCAN.