vicarius.io

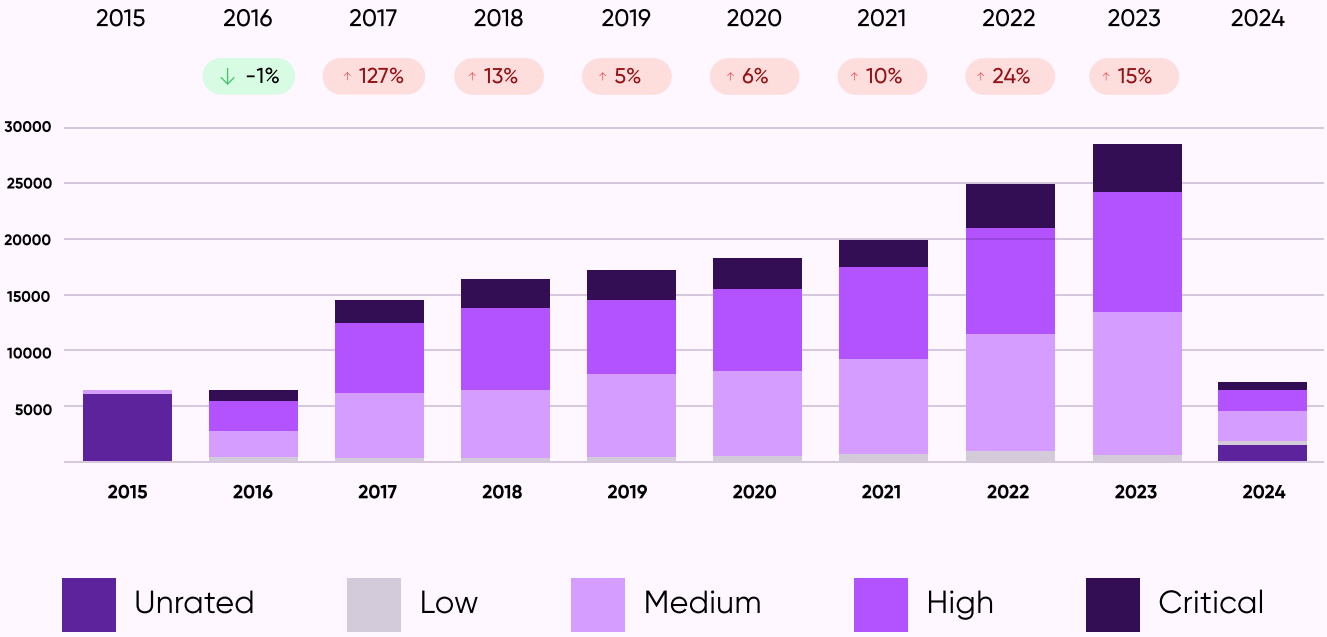
The 6-Step Framework

for a Remediation-Focused Approach To Vulnerability Management

1	2	3
4	5	6

Taking a Remediation-Focused approach to Vulnerability Management

Vulnerabilities are on the rise and so are exploits.



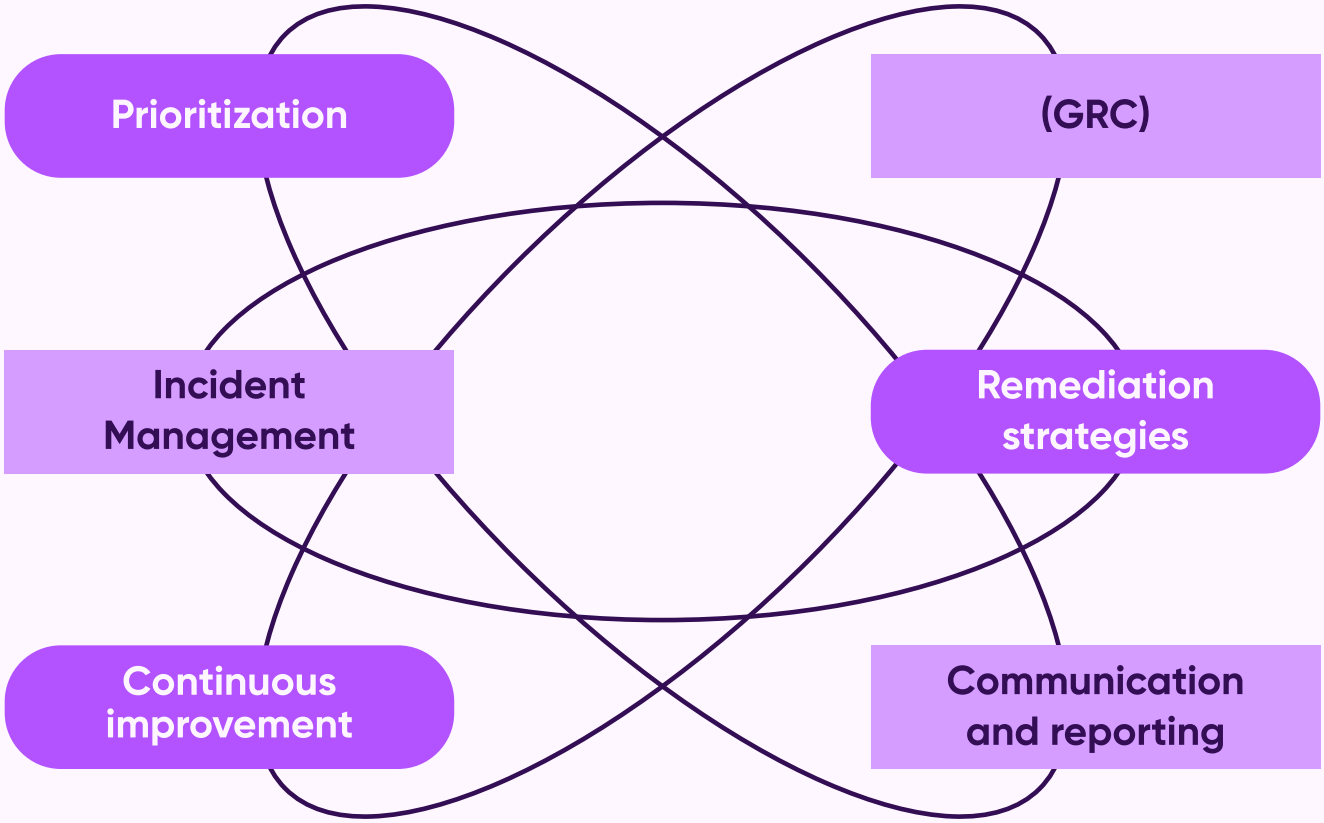
Given that the average Mean Time to Remediate (MTTR) for critical vulnerabilities often spans 60 to 150 days, the urgency for a shift towards a remediation-first mindset is apparent.

A Remediation-Focused approach to Vulnerability Management emphasizes proactive measures and rapid responses to vulnerabilities throughout the lifecycle of your VM program. This strategy pivots from simply identifying vulnerabilities to prioritizing and executing remediation swiftly, ensuring vulnerabilities are addressed before they can be exploited.

Source of chart: https://securityvulnerability.io/stats

Framework objective

To significantly reduce the organization's attack surface through a proactive, remediation-focused approach to Vulnerability Management.



[01] Governance, Risk Management, and Compliance (GRC)

Over 80% of the vulnerabilities exploited are ones for which a patch has been available for months (sometimes, even years!). Timely risk assessment and patch deployment within governance policies.

Governance integration

Detail the integration of Vulnerability Management into IT governance frameworks, like ITIL or COBIT, for strategic alignment.

Risk assessment techniques:

Incorporate risk assessment methodologies, such as FAIR or CVSS scoring, to quantify and prioritize vulnerabilities.

Compliance automation

Use compliance scanning tools and software that map findings directly to regulatory and framework controls (e.g., NIST, ISO).

[02] Threat analysis and prioritization

Scanning & Remediation

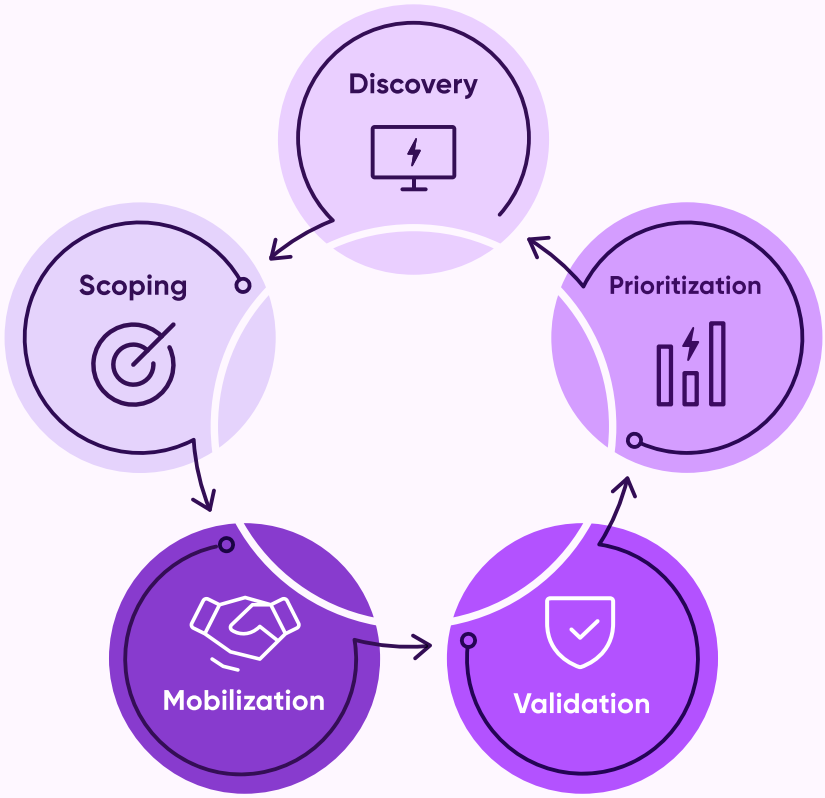
Don’t just just deploy scanning tools (e.g., Nessus, Qualys). Select and integrate tools that enhance remediation capabilities, such as automation tools that facilitate rapid patching and configuration changes.

Threat Intelligence

Integrate proactive threat intelligence to analyze past exploitations and forecast similar vulnerabilities across applications. This will help uncover vulnerabilities beyond publicly disclosed CVEs.

Automated prioritization

Use compliance scanning tools and software that map findings directly to regulatory and framework controls (e.g., NIST, ISO).



[03] Remediation strategies

Patch management

Use a mature Patch Management solution that can prioritize exploitable vulnerabilities and automatically or manually install all prioritized updates for which a patch is available across your OS and Apps.

Organizations utilizing automated patch management see patch application within an average of 30 days from release, in stark contrast to the 60 days or more for those without automation.

Configuration management and automation

Advocate for the use of configuration management tools to enforce security baselines and automate remediation tasks.

Vulnerability exceptions management

Implement a process for handling exceptions where immediate remediation isn't possible, including compensating controls. Enable patchless protection to keep your high-risk and vulnerable apps secure even when a patch has not been developed or deployed.

[04] Incident management and response

Rapid response with a remediation focus

Ensure incident response plans have a strong emphasis on immediate remediation actions to prevent further exploitation or spread.

Incident playbooks

Develop detailed incident response playbooks focused on specific vulnerability exploits, incorporating steps for containment, eradication, and recovery.

Security Information and Event Management (SIEM)

Utilize SIEM systems for real-time monitoring, detection, and automated response to incidents related to known vulnerabilities.

Learning for future remediation

Utilize SIEM systems for real-time monitoring, detection, and automated response to incidents related to known vulnerabilities.

[05] Communication and Reporting

Reporting with a purpose

Shift reporting focus towards metrics that highlight remediation effectiveness, such as Mean Time To Remediate, Remediation Success Rates, and Reductions in Repeat Vulnerabilities.

- Real time visibility
- IT assets inventory

Cultivating the remediation-focused culture

Cultivating the Remediation-Focused Culture: Regularly communicate the importance of a remediation-focused approach to all stakeholders, reinforcing its value and the role everyone plays in it.

[06] Continuous Improvement

Feedback for faster remediation

Encourage feedback loops specifically focused on improving the speed and efficiency of the remediation process.

Post-remediation testing

Establish procedures for validation testing post-remediation to ensure vulnerabilities are effectively neutralized.

Red team exercises

Conduct regular red team exercises or penetration testing to test the effectiveness of the remediation measures and the overall security posture.

Adapting processes for agility

Continually refine processes to remove bottlenecks in the remediation process, ensuring the organization can adapt quickly to new vulnerabilities.

Conclusion

Reinforce the critical importance of adopting a Remediation-Focused mindset across your organization, highlighting its impact on improving security resilience and reducing risk exposure.

Integrating a Remediation-Focused concept throughout the Vulnerability Management lifecycle not only aligns each element with proactive security measures but also fosters a cultural shift towards immediate action and resilience against threats. This holistic approach ensures that every part of the vulnerability management process contributes to a quicker, more effective response to vulnerabilities.

Happy Remediating!

---

vRx by Vicarius

The only consolidated platform for vulnerability remediation

Trusted by:

exabeam SAMSUNG DB SCHENKER Bupa Pizza Hut STARBUCKS COFFEE

vRx unifies all the different parts of Vulnerability Management - vulns discovery, prioritization, and remediation. Our platform is designed to help teams remediate vulns faster and smarter.

Vuln Discovery

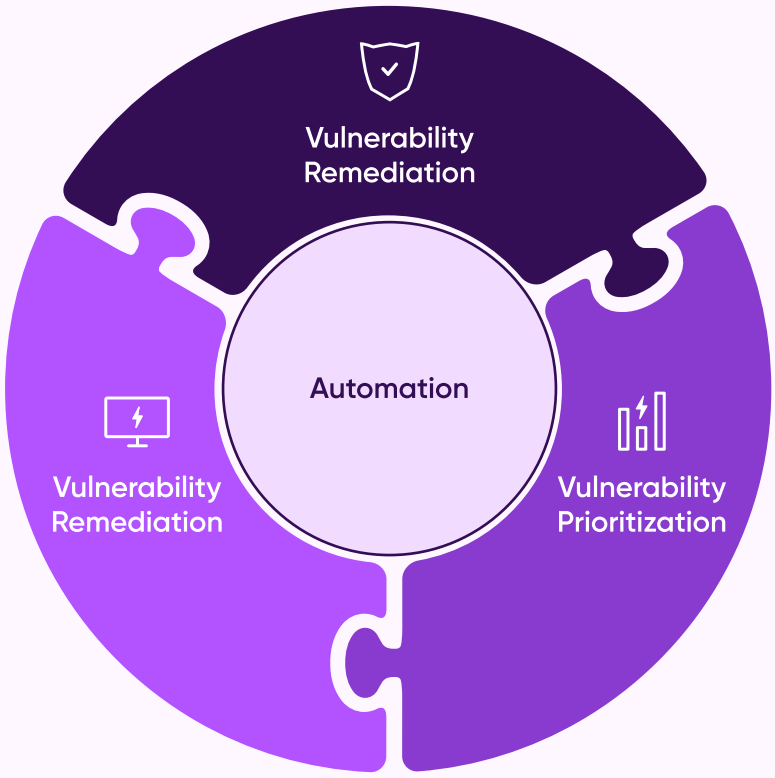
Beyond CVEs, vRx analyzes your OS, softwares, and inventory to identify the root cause of a vulnerability. This allows us to recommend remediation strategies for the root cause whenever it appears in your environment.

Vuln Prioritization

Using xTags, vRx creates contextual analysis that highlights the largest threats, so you can confidently prioritize risk remediation.

Vuln Remediation

vRx's Recommended Action Engine provides real-time suggestions for detected vulnerabilities, allowing you to take quick action and mitigate business risk. Real-Time Patch Management lets you close security gaps at a moment's notice or schedule patch installations across your apps, OS, and assets. When there is no patch available, vRxs Patchless Protection™ tool secures high-risk apps rapidly and blocks incoming exploitation attempts using proprietary in-memory protection.



See if vRx can support your remediation goals - start your free trial