seemplicity

Remediation Planning Efficiency Assessment

Building a remediation plan often involves more planning than meets the eye – especially as an organization scales in size and structure. For many organizations, it's one of the most difficult aspects of vulnerability management because of communication gaps, conflicting priorities, and resource constraints between security and development teams. When building a formal remediation plan, it is helpful to evaluate areas of ownership, notable platforms and tools in play, and any bottlenecks. The end goal should be an efficient, process-focused approach to vulnerability remediation that can sustain the volume and velocity of security findings the organization receives.

Take this 2-minute assessment to understand the efficiency and maturity of your organization's remediation efforts.

1. How does your organization collect vulnerability testing tool findings?

- **A** We use a manual CSV download.
- **B** We use an API to collect vulnerability findings.
- **C** We have a fully integrated platform to collect and ingest findings.

2. How does your organization correlate vulnerability findings with each other?

- **A** We manually correlate findings
- **B** We have our testing tools partially integrated into a vulnerability management platform
- **C** We have a fully integrated vulnerability management platform that we solely work from

3. How do you prioritize vulnerability findings?

- **A** Prioritization is ad-hoc and varies by team.
- **B** We have a basic prioritization framework.
- **C** We use a comprehensive, automated prioritization system.

---

4. How do you identify the remediation owner for each vulnerability?

- **A** Owners are identified manually.
- **B** Owners are identified using a semi-automated process.
- **C** We have an automated system that identifies owners based on predefined criteria.

---

5. How is communication with the remediation owner handled?

- **A** Communication is via manual channels (e.g., spreadsheets, email and/or instant messaging).
- **B** We use a combination of formal and informal communication methods.
- **C** Communication is managed through an integrated platform with automated notifications.

---

6. How do you monitor the status of remediation tickets?

- **A** Status is tracked manually in spreadsheets.
- **B** We use a basic ticketing system with limited automation.
- **C** We have an advanced system with real-time monitoring and automated updates.

---

7. Who is responsible for updating and closing remediation tickets?

- **A** No clear ticket owners, ad-hoc.
- **B** Security teams.
- **C** Remediation teams/ developers

---

8. How do you validate successful remediation?

- **A** We manually validate and close tickets after the next vulnerability scan
- **B** Our vulnerability management platform validates the remediation and we close the ticket
- **C** Our vulnerability management platform validates the remediation and automatically closes the ticket

---

9. How do you ensure consistency across the remediation process?

- **A** We don’t. Sometimes remediation plans are created, other times the work just gets done.
- **B** We have basic remediation planning in place, so there’s some level of consistency.
- **C** We create detailed remediation plans using consistent and repeatable processes.

Recommendations

Low Efficiency

MOSTLY “As”

Your current processes will benefit from significant improvement. Here are some steps to enhance your efficiency:

- Look for ways to integrate your security testing tools into a vulnerability management platform to streamline the collection of vulnerability findings.
- Develop a basic prioritization framework.
- Automate the delivery of remediation workflow requests.
- Transition from informal, ad-hoc communication to formal, process-driven communication methods.
- Clearly define remediation ticket ownership and responsibility.
- Implement a basic system for ticket tracking and monitoring.
- Begin automating some parts of your remediation processes, such as vulnerability correlation or prioritization, to ensure consistency.

Medium Efficiency

MOSTLY “Bs”,
OR A MIX OF “As” & “Bs”

You have a good foundation, but there's room for improvement. Consider the following steps for greater efficiency:

- Move towards a platform integrated with testing tools that can consolidate vulnerability findings.
- Establish a set of criteria, based on technical and business context, to automatically prioritize vulnerabilities.
- Upgrade to a fully automated system for assigning remediation owners.
- Utilize more structured communication workflows with automated notifications.
- Implement an advanced ticketing system with continuous monitoring.
- Clearly determine who is responsible for each remediation task by leveraging automation.
- Further develop your remediation planning to ensure repeatable and consistent processes.

High Efficiency

MOSTLY “Cs”,
OR A MIX OF “Bs” & “Cs”

Your processes are highly efficient. Here are some recommendations to further enhance your efficiency by leveraging AI:

- Use AI to enhance your automated prioritization system, enabling more precise identification of critical vulnerabilities.
- Implement AI technology to intelligently assign remediation owners based on data-driven analysis for greater precision and accuracy.
- Apply AI in your communication workflows for actionable recommendations based on historical data, allowing for proactive remediation efforts.
- Use AI to tailor remediation plans based on business context and remediation team workloads

Ready to take your remediation planning to the next level?

SCHEDULE A DEMO

Let Seemplicity do all of the heavy lifting.

Schedule a demo with Seemplicity to get a better understanding of where your processes currently stand and how to make them more efficient with process automation and workflow integration that gets you ahead of risk, eliminates process busy work, and drives team engagement.