seemplicity

Ultimate Guide: Scalable Remediation Plans

Strategies for Rapid Risk Reduction

GUIDE

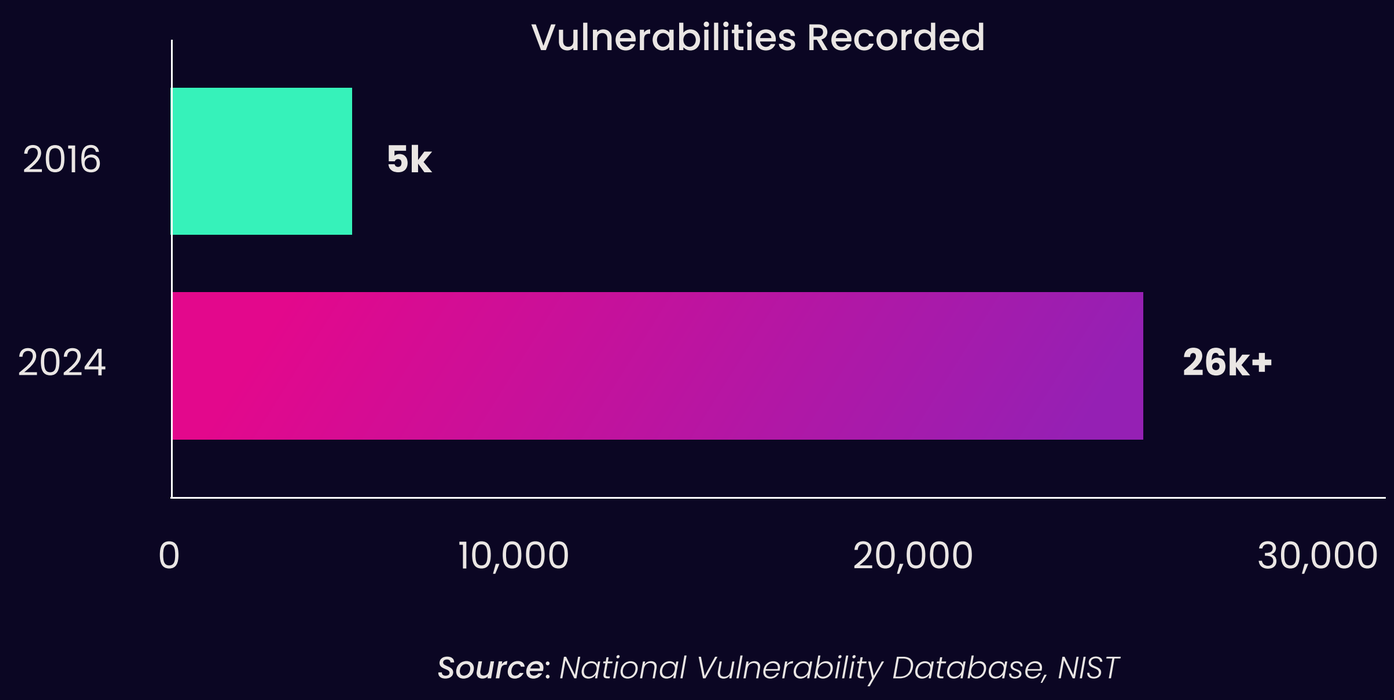
Introduction

Organizations face an unprecedented volume of vulnerabilities. According to the National Vulnerability Database (NVD), over 26,000 vulnerabilities were recorded in 2024 alone, a significant increase from the 5,000 reported in 2016. This sharp rise illustrates the growing frequency of risks that organizations must navigate. As security environments become more intricate, the need for a structured and effective remediation plan has never been more critical.

Common Vulnerabilities and Exposures

26k+

vulnerabilities recorded in 2024.



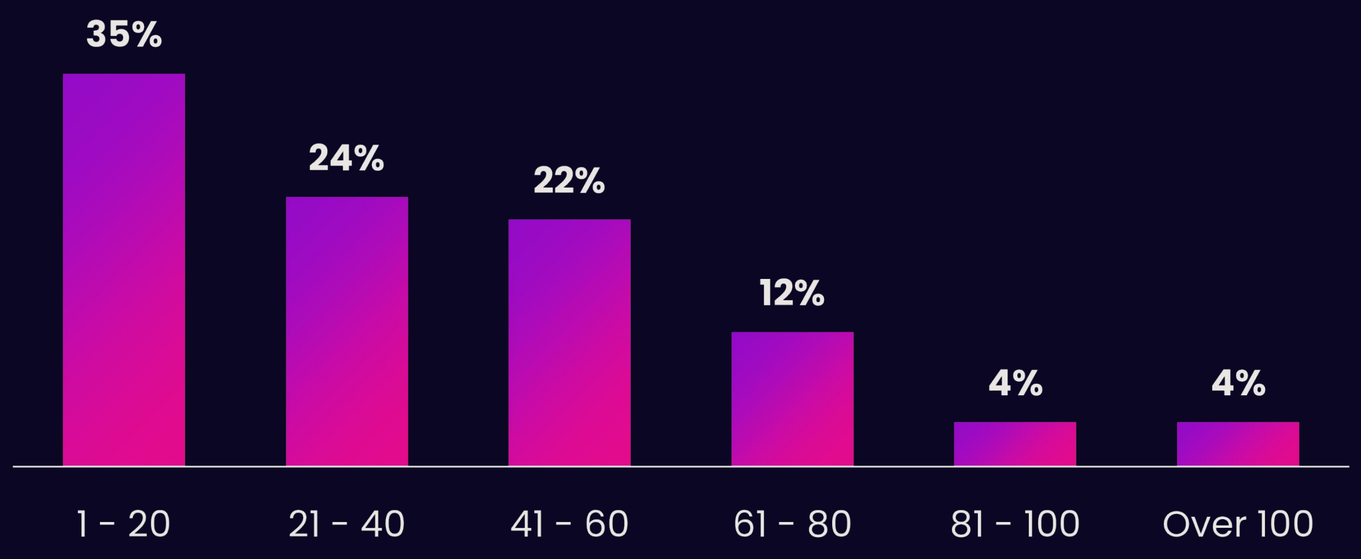
***Source**: National Vulnerability Database, NIST*

A well-structured remediation plan serves as a roadmap for organizations to manage and mitigate these vulnerabilities consistently and effectively. It ensures that security teams can systematically identify, prioritize, and address the most critical risks, safeguarding their operations and maintaining business continuity. Relying on ad hoc remediation operations is no longer adequate and is not only inefficient but also unsustainable. Without a structured plan, security teams are left grappling with an overwhelming number of vulnerabilities, leading to delays in remediation.

The challenges are further compounded by the diverse and siloed nature of security tools employed by organizations. With an average of 38 different security product vendors in use, data consolidation and prioritization become daunting tasks. This fragmentation creates gaps in visibility, slowing down the remediation process and hindering effective risk management.

Number of Security Product Vendors

On average, organizations are using **38 different security product vendors.**



***Source**: The 2024 Remediation Operations Report, Seemplicity*

A scalable remediation plan not only streamlines remediation operations but also ensures remediation processes can handle large volumes of vulnerabilities without compromising speed or efficacy. By addressing vulnerabilities in a timely and efficient manner, organizations can reduce their threat exposure and maintain a proactive approach to risk management.

This guide will walk you through the essential components of an effective vulnerability remediation plan, providing actionable insights to help your organization enhance and scale its remediation operations and stay ahead in the ever-changing cybersecurity landscape.

What Is A Remediation Plan?

A remediation plan is a structured approach to identifying, prioritizing, assigning, and resolving vulnerabilities within an organization's digital infrastructure. It provides a systematic framework that ensures vulnerabilities are addressed consistently and effectively, minimizing risk and enhancing overall security posture.

At its core, a remediation plan guides security, operations and development teams through the process of mitigating risks. It allows teams to focus on the most critical risks first, ensuring that resources are allocated where they are needed most.

A well-designed remediation plan must be scalable so that organizations can manage and mitigate risks efficiently as they grow. As the number of vulnerabilities and findings increase, a scalable plan ensures that remediation operations are adaptive and remain effective. Scalability allows security teams to systematically reduce their threat exposure and maintain a proactive approach to risk management, despite growing complexities and demands.

Challenges In Scaling A Remediation Plan

Organizations often start with a remediation plan that works well enough for their initial needs. However, as the organization grows, scaling this plan to meet the demands of a larger, more complex attack surface often proves challenging. Strategies that may have been effective - or at least sufficient - on a smaller scale can become significant obstacles as organizations expand, leading to inefficiencies and gaps in the remediation process.

One of the main challenges security teams face in scaling their remediation plan is a heavy reliance on manual efforts, such as using spreadsheets and best guesses to track and prioritize vulnerabilities and assign remediation ownership. While this may work in a smaller environment, as the organization grows these methods quickly become unsustainable.

Resource constraints further exacerbate the issue. As the volume of vulnerabilities increases, the resources available - particularly in terms of manpower - do not always keep pace. Security teams that were once able to manage the remediation process manually find themselves overwhelmed by the sheer volume. The heavy reliance on manual efforts is futile in a larger organization as there simply aren't enough personnel to handle the increased workload.

Compounding those challenges is the lack of automation and integration. A deficiency in automated tools further exacerbates the reliance on personnel, whereby the security team has to manually sift through findings from multiple sources. In large organizations, it's impossible to maintain a comprehensive and up-to-date view of the organization's security posture, leading to ineffective remediation efforts.

Consequences Of Ad-Hoc Remediation

A lack of scalability often results in fragmented and inconsistent remediation processes across the organization. Failing to implement a structured remediation plan means vulnerabilities are managed in an ad-hoc manner, leading to a lack of cohesion and standardization. This fragmentation not only reduces the effectiveness of remediation efforts but also increases the risk of security gaps, as there is no unified approach to managing and mitigating vulnerabilities. This presents a host of issues, such as slower response times and missed vulnerabilities, which compromise the organization's security posture, efficiency and overall resilience.

One of the most notable consequences is delayed remediation. Without a structured plan, it's extremely difficult to address vulnerabilities in a timely manner. It takes organizations an average of 5 days to identify and notify the remediation owner, creating a dangerous window of opportunity for attackers. As the number of unaddressed vulnerabilities grows, so does the risk to the organization, creating a snowball effect that can be difficult to reverse.

Average Remediation Time by Company Size

On average, organizations take **5 days** to identify the remediation owner, determine the ticketing system and board, open the ticket, and notify the remediation owner.

Avg. Remediation Days by Company Size	Overall Days	Up to 1,000 Employees	1,000-9,999 Employees	10,000+ Employees
Identify remediation owner, ticketing system and board	3.26	2.71	3.56	3.28
Open ticket and notify remediation owner	2.44	2.94	2.6	1.69
Total Process Time Average Days	**5,7**	**5,65**	**6,16**	**4,97**

Source: *The 2023 State of Risk Reduction, Dark Reading*

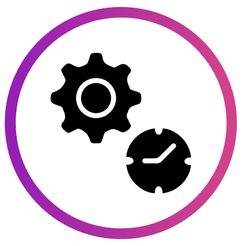
Additionally, organizations that lack a structured plan tend to allocate their already-limited resources inefficiently. Security teams may spend excessive time addressing low-priority issues or duplicating efforts, which not only wastes valuable resources but also delays the remediation of more critical vulnerabilities. Without clear guidelines and prioritization criteria, efforts become scattered, leading to inefficiencies that can cripple the organization's ability to respond effectively to threats.

A lack of tracking and reporting is another consequence of relying on ad-hoc remediation efforts. In The absence of a well-established tracking mechanism, organizations lack visibility into the status of remediation efforts, making it difficult to assess progress and ensure that vulnerabilities are being addressed effectively. To do so, security teams have to chase down the remediation owner, which is a further waste of time and effort.

This lack of visibility can also impede regulatory compliance as organizations may struggle to ensure they're in line with requirements. The absence of detailed records and reporting capabilities can also lead to significant problems during future audits, exposing the organization to potential penalties.

A Remediation Plan - An Overview

Building a vulnerability remediation plan requires a clear understanding of its core components. These components serve as the foundation upon which effective and scalable remediation operations are developed.



WHAT

The VM team would manually parse findings data and assemble tickets per each remediation team's specifications around ticket format, ticketing frequency, supplemental vulnerability information, and SLA time. The VM team needed to automate these specifications to save both time and manual labor.

WHERE

Once vulnerabilities have been identified, it is important to determine where they exist within the organization's extended IT ecosystem. This includes pinpointing the exact location of each vulnerability, whether it resides in on-premises servers, employee devices, cloud environments, or within a codebase. Knowing the precise location of vulnerabilities allows for more targeted and efficient remediation efforts by providing context for the subsequent **Who** and **How** steps.

WHO

Assigning ownership and responsibilities is a critical aspect of the remediation process. Effective remediation requires clear delineation of roles, ensuring that the right teams are tasked with addressing the appropriate vulnerabilities.

HOW

The final component of a remediation plan involves establishing the method of remediation. This includes defining the steps necessary to resolve each vulnerability, from initial identification through to validation. The "how" of remediation also encompasses collaboration among teams, ensuring that efforts are coordinated and that progress is monitored in real-time.

Building A Remediation Plan

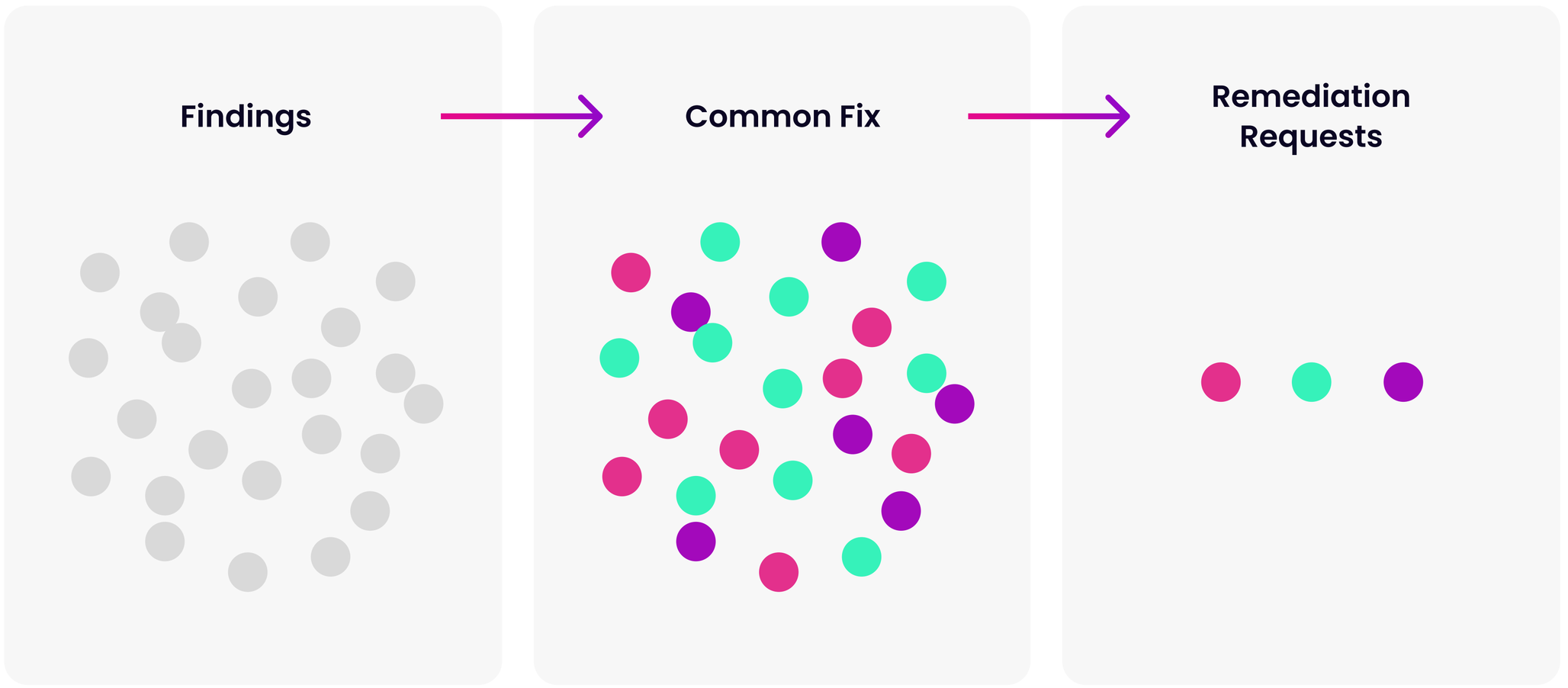
WHAT | Identifying What Needs to be Remediated

The foundation of any remediation plan begins with a clear and precise identification of what needs to be remediated. With a never-ending backlog of findings, organizations must prioritize effectively to ensure that their remediation efforts are focused on the most critical risks.

The process of identifying what needs to be remediated starts with establishing a set of criteria for prioritization. This criteria should be tailored to the specific needs and risk profile of the organization, considering both the business context and the technical severity of each vulnerability. Common criteria include the severity score (such as CVSS), the type of asset affected, Service Level Agreements (SLAs), and the potential business impact. For instance, vulnerabilities affecting mission-critical systems or those exposed to external threats should be given higher priority. By applying consistent criteria across all findings, organizations can effectively compare vulnerabilities and prioritize them based on their relative risk.

Another key aspect of this process is aggregation. In many cases, multiple findings may be related to the same underlying vulnerability. By aggregating these findings into a single remediation item, organizations can streamline their efforts, focusing on fixes that address multiple issues simultaneously. This not only expedites the remediation process but also enhances the overall impact by reducing redundancy and ensuring that resources are used efficiently.

> Leveraging automated tools enables security teams to quickly filter through the noise, identify the most pressing vulnerabilities, and focus on reducing risk.



Automation must play a role in the identification process. Given the volume of findings generated by modern security tools, often including duplications, manually sifting through data to determine what needs to be remediated is not only time-consuming and prone to error, but it also strains already-limited resources. Automation can also assist in the enrichment of vulnerability data, providing additional context that aids in more accurate prioritization.

This systematic approach not only enhances the effectiveness of vulnerability management but also positions the organization to respond swiftly and decisively to risks, no matter the complexity and volume of findings. It also ensures that remediation efforts are easily scalable, remaining efficient and effective regardless of how large the organization becomes.

WHERE | Determining the Location of Vulnerabilities

Once an organization has identified what needs to be remediated, the next step is determining where these vulnerabilities are located. Understanding the precise location of each vulnerability is essential for developing an effective and scalable remediation strategy.

> **A vulnerability's location not only influences its priority level, but also dictates how it will be addressed and who will be responsible for the remediation efforts.**

Vulnerabilities can exist across a wide range of environments within an organization, from on-premises servers and employee devices to cloud-based infrastructure and lines of code. As organizations grow, the complexity of these environments increases, and manual methods of tracking vulnerability locations become untenable. Different teams will be responsible for different environments, and understanding the vulnerability's location will quickly inform who needs to remediate it, ensuring they get notified without delay.

Each of these environments presents unique challenges and requires specific approaches to remediation. For example, vulnerabilities found in cloud environments may necessitate different remediation techniques and tools compared to those found in on-premises systems. Similarly, vulnerabilities in production systems might demand immediate attention, whereas those in development or staging environments could be addressed on a different timeline. As the organization scales, these challenges multiply, making it essential to have a robust, automated system in place for tracking and managing the location of vulnerabilities across diverse environments.

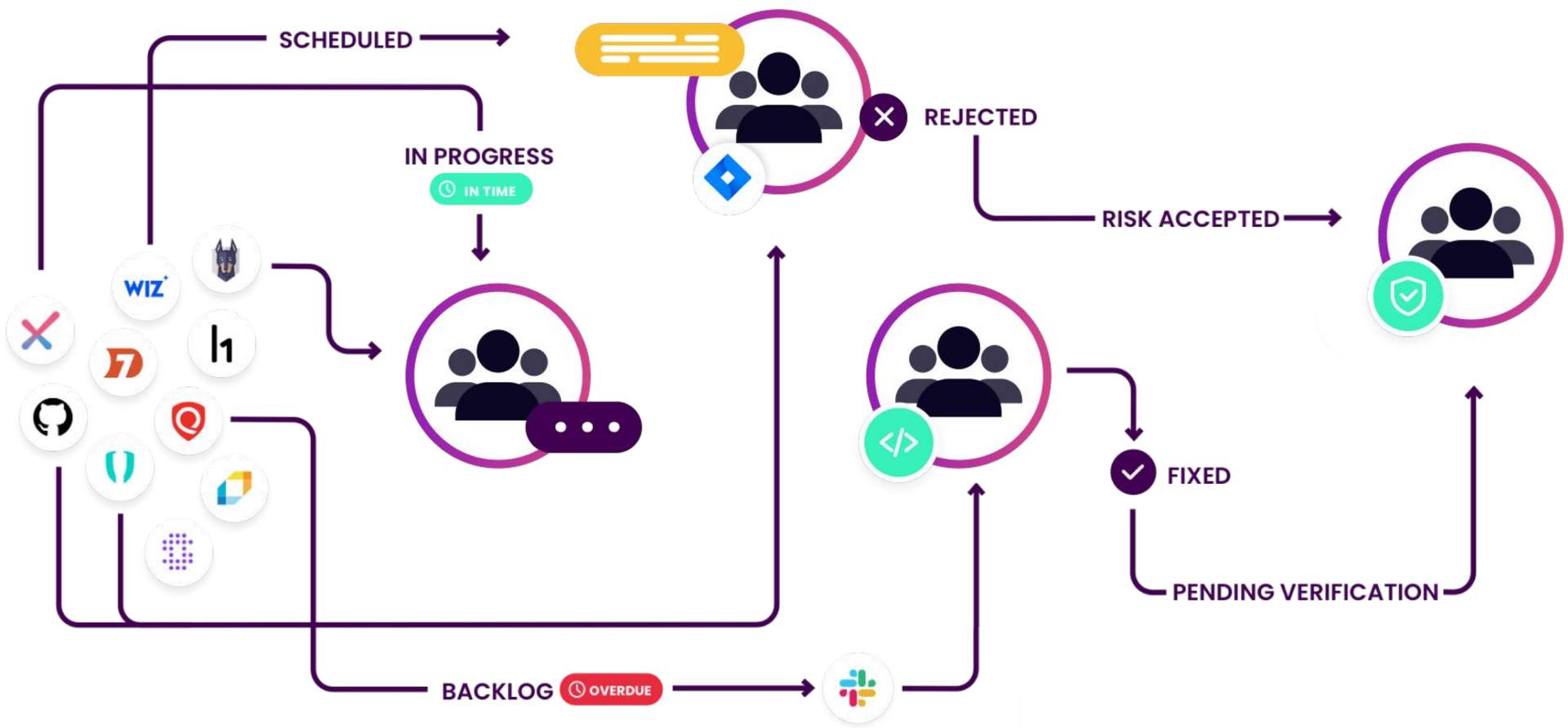
Misidentifying the location of a vulnerability can lead to ineffective remediation efforts, leaving critical systems exposed to potential threats. To avoid this, organizations should employ automated tagging and tracking systems that can accurately map vulnerabilities to their respective assets. These automated systems not only increase accuracy but also save time and resources by reducing the need for manual data entry and cross-referencing. Integrating these systems with a Configuration Management Database (CMDB) further enhances accuracy, enabling security teams to maintain up-to-date records of where vulnerabilities reside within the infrastructure.

By accurately mapping vulnerabilities to their respective environments, organizations can enhance the precision and efficiency of their remediation efforts. This approach is particularly important as the organization grows, ensuring that the scalability of the remediation plan is maintained. Automation in tracking and mapping allows security teams to manage large-scale environments without losing sight of critical details.

WHO | Assigning Ownership and Responsibilities

An essential aspect of a remediation plan is ensuring that each identified vulnerability is assigned to the right person or team through structured workflows. Without this, vulnerabilities can fall through the cracks, leading to delays in remediation and increased risk.

Assigning Ownership



Understanding the organizational hierarchy is the first step in assigning ownership. This involves using a CMDB or otherwise mapping out the various teams, departments, and individuals who are responsible for different aspects of the organization's security infrastructure. In large organizations, maintaining an accurate and up-to-date map of these responsibilities is significantly more challenging but also more critical. By knowing who is responsible for what, security teams can avoid the inefficiencies of manually identifying the relevant remediation owner each time a vulnerability is discovered. For instance, vulnerabilities in cloud infrastructure should be routed directly to the cloud security team, while issues within application code may be best handled by the application security team or specific people within the development team.

Historical data can also play a valuable role in determining ownership. Reviewing past remediation efforts can help identify which teams or individuals have successfully handled similar issues before. This historical insight allows for more efficient routing of tasks. Leveraging this data ensures that tasks are assigned to the most capable individuals or teams, enhancing both speed and effectiveness.

Workflows are another critical component in assigning ownership. Using the organizational hierarchy and historical data helps develop well-designed workflows that route remediation tasks to the appropriate owners in the correct sequence. These workflows can also incorporate organizational preferences, such as routing tasks through specific platforms like JIRA, to align with how teams already operate. Automation significantly improves the consistency and scalability of these workflows, allowing organizations to handle large volumes of vulnerabilities efficiently and effectively.

By leveraging organizational hierarchy, historical data, and automated workflows, organizations benefit from structured and scalable remediation operations that minimize risk and maximize security outcomes. This approach ensures that no matter the size of the organization, vulnerabilities are addressed with the same level of diligence and effectiveness, maintaining the integrity of the overall security posture.

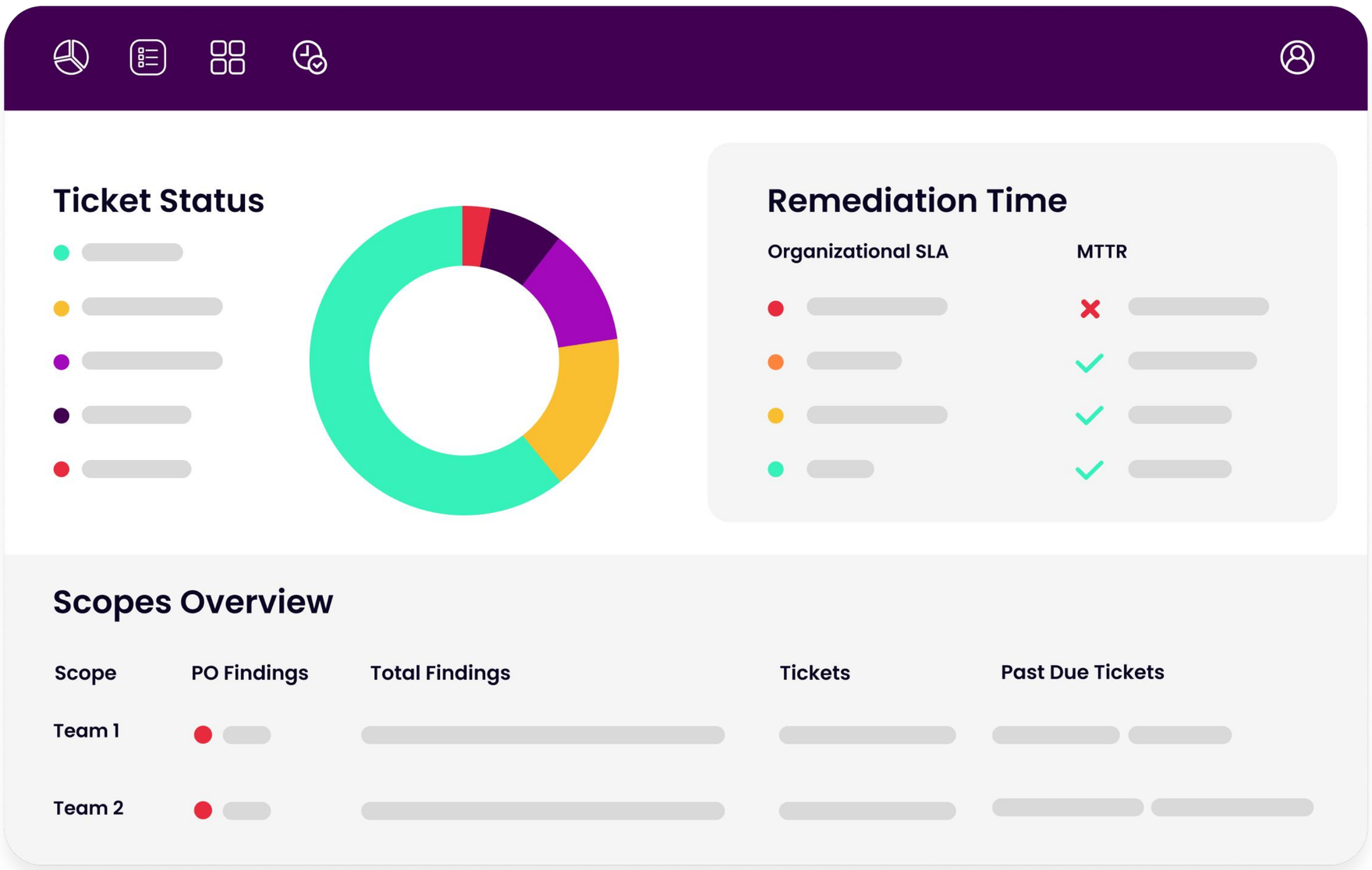
> **Assigning ownership involves ensuring that the assigned teams have the necessary context and information to execute remediation efforts effectively.**

HOW | Establishing the Method of Remediation

The final component of a scalable vulnerability remediation plan is establishing a clear and effective method for remediation. This begins with gathering comprehensive vulnerability information, which includes understanding the nature of the vulnerability, its severity, and its potential impact on the organization. Sources such as the Common Vulnerability Scoring System (CVSS), Exploit Prediction Scoring System (EPSS), and Known Exploited Vulnerabilities (KEV) lists from CISA and VulnCheck provide valuable context that can guide remediation efforts. This information helps remediation teams prioritize their actions and apply the most appropriate fixes, whether that involves deploying a patch, reconfiguring systems, or implementing compensating controls.

Collaboration is another aspect of the remediation method, particularly in larger organizations where a number of stakeholders are involved in the remediation process. Vulnerability remediation requires the coordinated efforts of multiple people across multiple teams, each responsible for different parts of the remediation process. Clear, continuous communication and collaboration are essential to keeping remediation operations aligned and on track. Automation tools can facilitate this collaboration by providing ongoing updates on remediation progress, ensuring that all involved parties are informed and can act without delay. This not only improves efficiency but also reduces the risk of miscommunication or duplication of efforts.

Remediation Reporting



Validation is the final step in the remediation process. Simply applying a fix does not guarantee that the vulnerability has been fully resolved. It is essential to validate that the remediation efforts have been successful and that the vulnerability no longer poses a threat. This can be achieved through a combination of ticketing systems and scanning tools. Closing a remediation ticket typically requires confirmation that the vulnerability is no longer detectable by security scanners. Automated validation processes can streamline this step, reducing the likelihood of human error and ensuring that remediation efforts are consistently validated.

This structured approach enhances the organization’s ability to respond swiftly and effectively to risks, thereby reducing time to remediation. This not only strengthens the overall security posture but also ensures that vulnerabilities are addressed with the same rigor and efficiency, regardless of the organization's size or complexity.

Key Takeaways And Next Steps

A well-structured and scalable vulnerability remediation plan is not just a best practice but a critical necessity. The complexity and volume of vulnerabilities that organizations face demand a systematic approach to remediation operations, one that ensures the most critical threats are addressed promptly and effectively. By following the steps outlined in this guide—identifying what needs to be remediated, determining where vulnerabilities reside, assigning clear ownership and responsibilities, and establishing a precise method of remediation—organizations can significantly enhance their security posture and reduce their overall risk.

The key to success lies in the integration of these components into a cohesive, scalable process. Each step in the remediation plan builds upon the previous one, creating a robust framework that enables security teams to respond to threats with speed and precision. The use of automation throughout this process not only reduces the likelihood of human error, but also increases efficiency and scalability, ensuring that vulnerabilities are consistently identified, prioritized, and resolved no matter the organization's size.

As organizations continue to navigate the challenges of a dynamic threat environment, the ability to rapidly adapt and refine remediation operations will be essential. Regularly reviewing and updating remediation plans, incorporating feedback from past experiences, and leveraging the latest tools and technologies, such as Artificial Intelligence (AI), will help maintain the effectiveness of these efforts. Ultimately, a strong and scalable remediation plan is a key element of a broader security strategy that empowers organizations to protect their critical assets and maintain business continuity in the face of ever-changing threats.

By implementing the strategies and best practices outlined in this guide, organizations can move from a reactive to a proactive approach to exposure management. This shift not only strengthens defenses but also positions the organization to better anticipate and mitigate future risks, ensuring long-term resilience and security.