HOW TO TRACK

VULNERABILITY DATA & REMEDIATION WORKFLOW

NETSPI™

INTRO

Vulnerability data must be tracked to ensure remediation – otherwise software vulnerabilities may fall through the cracks and leave your organization exposed to a data breach or other cyber security attacks. Most vulnerability data comes from scanners, but the most important vulnerability data often comes from humans, specifically penetration testers. In this whitepaper on vulnerability management tools, we provide you with guidance on how to effectively track your vulnerability data and remediation workflow.

NETSPI™

Several Non-Optimized Tools are Commonly Used for Tracking Vulnerabilities and Remediation Status.

Each has Significant Limitations:

Excel and SharePoint: Companies often use Excel or SharePoint to track the remediation status of vulnerabilities from a central list of penetration testing and scanner findings. Typically, dozens of users comb through thousands of vulnerabilities in a single spreadsheet. Tracking vulnerability remediation this way presents huge challenges, because spreadsheet tools are not designed to help manage such complicated data sets and team collaboration. The information in a spreadsheet is easily overwritten or marked improperly. The accuracy of the data is questionable, making vulnerability management reporting difficult.

JIRA: Alternately, some companies use JIRA for tracking software vulnerabilities, which helps ensure that best-practice processes are followed. Unfortunately, most organizations have many JIRA instances across multiple development environments. Distributing the results across many JIRA instances leads to an inability to effectively report on the data. Storing the results in a central JIRA system has advantages, but getting stakeholders to take the time to login and review the findings in a different system than they use daily can be difficult.

ServiceNow: Some companies attempt to use ServiceNow to track vulnerabilities on the networking side, which has the advantage of more robust ticketing. Unfortunately, some of the same data ingestion challenges exist, and you lose the fidelity of having all of the vulnerabilities in a single place.

Home-built: Other companies use custom vulnerability management tracking systems that connect to other internal systems. While these vulnerability management tracking tools work, home-built tools are difficult to maintain and often are maintained less formally than other normal development efforts, because vulnerability management tracking tools are not the company's core business. Such in-house remediation tracking systems are often databases with a minimal user interface, and not fully optimized for the purpose.

BEST PRACTICES CHECKLIST:
Vulnerability Management Tracking Systems

VULNERABILITY TRACKING REQUIRES A SYSTEM FOR MANAGING REMEDIATION WORKFLOWS THAT CAN HANDLE THESE SEVEN TASKS:

- [ ] Ingestion of various data formats with flexible normalization
- [ ] Reviewing of normalized data for changes and modifications as needed
- [ ] Distribution of normalized data to various external systems
- [ ] Tracking the data distributed externally to keep a central listing up to date
- [ ] Ensuring policy is adhered to across the various systems where the data vulnerability remediation is tracked
- [ ] Sending notifications and keeping humans involved in the process, especially when vulnerability remediation is overdue
- [ ] Reporting on the outcome of vulnerabilities by group, business unit, or globally across the organization

AS A RESULT, A CHECKLIST FOR ORCHESTRATING VULNERABILITY MANAGEMENT TASKS TO ASSURE TIMELY, PRIORITIZED REMEDIATION SHOULD INCLUDE THESE SIX CAPABILITIES:

- [ ] Serve as a central clearinghouse of vulnerability data
- [ ] Automate many steps of the remediation process
- [ ] Coordinate multiple processes based on the organization's internal structure and environment
- [ ] Integrate with many systems via an API
- [ ] Define a workflow with decision points based on data-based criteria
- [ ] Notify key users when something is not right

Make sure any vulnerability management tool you consider checks these six boxes before you try it.

NETSPI™

ABOUT NETSPI

About Resolve™

NetSPI Resolve™ is a world-class penetration testing execution and delivery system for vulnerability management tracking and more. Resolve correlates all vulnerability data across your organization into a single view, so you can find, prioritize, and fix vulnerabilities faster.

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest healthcare companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve™ platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster. Follow us on LinkedIn, Twitter, and Facebook.