Nucleus

# FIXING THE **BROKEN** VULNERABILITY MANAGEMENT PROCESS

A NUCLEUS SECURITY WHITEPAPER

# UNPATCHED VULNERABILITIES **CAUSE ONE-THIRD** OF BREACHES.

Effective, timely, and efficient vulnerability management (VM) is imperative to preventing cyberattacks, as approximately one in every three breaches is caused by an unpatched vulnerability. For example, the now infamous Equifax hack, which resulted in compromised personal data of over 143 million people, can be traced back to an unpatched version of Apache Struts.

Vulnerabilities take shape beyond patches as well, and keeping every device and application correctly configured and up to date across an enterprise environment can take Herculean effort. Significant advances in technology, particularly cloud computing, Internet of Things (IoT) devices, and mobile, have led to an explosion in vulnerability data. In 2019, over 17,000 new common vulnerabilities and exposures (CVEs) were published, up from 6,447 in 2016.

In addition to new vulnerabilities, existing ones can leave organizations open to compromise if they are not promptly addressed, as in the case of Equifax. Vulnerabilities can also be re-introduced while making configuration changes, or if devices and apps are mismanaged on the enterprise network.

If new and existing vulnerability data is not properly tracked and managed, dangerous vulnerabilities can fall through the cracks.

# BROKEN VM PROCESSES **PLAGUE** ORGANIZATIONS.

Many organizations are using outdated, highly inefficient, and time consuming VM processes that leave security personnel struggling to keep up. Numerous research studies conclude that the average mean time to patch (MTTP) is between 60 to 150 days, and about one-quarter of vulnerabilities remain unpatched for over a year. A study by the Ponemon Institute found that the average organization has a backlog of 57,555 identified vulnerabilities. Further, of organizations that reported having been breached in the past two years, 42% told Ponemon that when the breach occurred a known vulnerability had not been patched, even though a patch was available.

**60-150**

Average Mean Time (days) to Patch Vulnerabilities

**57,555**

Average Backlog of Identified Vulnerabilities

**42%**

Breaches Occuring via Vulnerability with Available Patch

Vulnerability scanners are highly efficient at discovering vulnerabilities, but they are not designed to help organizations manage or prioritize vulnerabilities. They output large volumes of raw data that lacks any asset or business context. This data doesn't provide security personnel with any actionable insights on its own. For it to be useful within a mature vulnerability management program, the data must be combined with other sources of vulnerability information. Additionally, the typical organization uses many disparate tools for vulnerability scanning, issue tracking, and alerting, making it extremely difficult to obtain a single view into current open vulnerabilities or compile reports on remediation efforts.

*Vulnerability scanners are highly efficient at discovering vulnerabilities, but they are not designed to help organizations manage or prioritize vulnerabilities.*

Historically, there was no way to consolidate vulnerability scans from different scanning tools, prioritize risk decisions, automate triage activities, and track and report vulnerability status at scale, leaving organizations with no choice but to cobble together their own solutions, including:

**Excel and Other Spreadsheet Software.** Spreadsheets are fantastic accounting tools; for vulnerability management, *not so much*. Because they don't scale, they cannot handle extremely large, highly complex data sets. Information must be added and updated through manual data entry, an inefficient and highly error-prone process, particularly in very large organizations, where dozens of people may be maintaining the list. Information may be entered incorrectly, deleted, or overwritten, which throws the accuracy of the data into question. Spreadsheets also don't maintain a usable version history, which is needed for compliance reporting. Finally, they do nothing to help organizations analyze vulnerability data and prioritize critical patches.

**SIEMs and BI Tools.** Security information and event management (SIEM) systems and business intelligence (BI) solutions are good tools for producing dashboards that give security personnel an "at a glance" view of the organization's most common and most critical vulnerabilities. However, this is woefully insufficient for vulnerability management in large enterprises, because SIEMs and BI solutions do not:

- Incorporate asset metadata for custom risk scoring
- Customize prioritization on business context
- Group assets and vulnerabilities based on custom properties
- Allow for changes to vulnerability status, such as accepting the risk of a vulnerability (e.g., an exception)

**Ticket/Task Tracking Systems, such as JIRA.** A task tracking system may seem like a logical choice for vulnerability management. However, many organizations run multiple instances of ticket tracking systems; sharing results across all of these instances complicates reporting and results in duplicates. Additionally, since every single vulnerability is not an action item for every single team, incorporating vulnerabilities into a ticketing system clutters it with "noise." Some organizations attempt to solve these problems by storing vulnerability data in one, central instance, but that means personnel must log in to a different system than the one they use for other tasks. Finally, ticketing systems do not allow for automated tracking of vulnerabilities over time; when a vulnerability is closed within the ticketing system, the status is not fed back into the vulnerability tracking register.

*"Homegrown" VM solutions tend to be clunky, time-consuming, and expensive to maintain.*

**Proprietary, In-House Software.** "Homegrown" vulnerability management solutions tend to be clunky, consisting of little more than a database with a primitive user interface. They're difficult, time-consuming, and expensive to maintain, especially considering that any time developers must spend maintaining the vulnerability management system is time they cannot spend on internal projects that drive the business forward.

Additionally, in-house solutions almost never meet the needs of the organization. They rarely scale sufficiently to meet increasing demand. They also tend to be purpose-built by one dedicated team, to solve one vulnerability management problem, but multiple stakeholders are involved in the vulnerability management process. This creates a situation where the "homegrown" solution solves only one problem, to the detriment of the vulnerability management process across the enterprise.

## **CRITICAL FEATURES** OF A DEDICATED VM TOOL.

For effective vulnerability management in modern data environments, organizations need a dedicated, scalable vulnerability management solution that does all of the following:

- Provides a central repository for vulnerability data, integrating with and aggregating results from all scanning tools, assessments, and penetration tests
- Automates as many steps of the vulnerability management process as possible, including normalizing scan result data, sending notifications to the appropriate remediation teams, handling ticket creation and assignment, and generating reports
- Helps organizations prioritize vulnerabilities and risk using customizable algorithms that can be configured to the vulnerability and asset attributes that are most important to your organization
- Automates and orchestrates response through integration with ticketing systems, issue trackers, SIEMs, and incident response tools

## NUCLEUS **STREAMLINES** ENTERPRISE VM.

Nucleus Security's vulnerability and risk management platform integrates with your existing tools and provides a single pane of glass through which you can monitor your security posture and manage your vulnerability data. Integrating with over 70 scanners and external tools, Nucleus ingests all of your vulnerability data, consolidates it in one place, and automates your vulnerability management processes so that your team works more effectively, and critical findings do not fall through the cracks.

Nucleus delivers value right out of the box, allowing you to manage vulnerabilities at scale through a simple, three-stage process:

1. **Collect and Normalize.** Nucleus ingests and normalizes all of the vulnerability data in your enterprise, including your tools, penetration tests, and audits, allowing security personnel to analyze, track, and search it from a single console.

2. **Prioritize, De-duplicate, and Enrich.** Nucleus enables organizations to produce custom risk scoring algorithms based on risk tolerance and priorities, resulting in risk scoring that is contextual to each organization, a significant reduction in time to determine the true risk of each vulnerability, and more accurate reporting.

3. **Automate Response and Remediation.** Using bi-directional integrations with ticketing systems, issue trackers, incident response tools, SIEMs, and more; flexible automation rules, and real-time views of all active vulnerabilities and remediation statuses, Nucleus enables organizations to respond to vulnerabilities up to 10 times faster.

**Over 70 Integrations and Counting.** Nucleus currently integrates with 70+ tools and is continuously adding more based on customer requests. We also maintain an open GitHub project for customer contributions.

**Support for SSO and Custom Roles.** Nucleus integrates with your single sign-on provider so that you can map your existing roles to Nucleus roles, minimizing administrative overhead.

**Enterprise Speed and Scalability.** Nucleus scales to support any sized organization and remains performant regardless of the number of tools in use, concurrent users, or amount of vulnerability data imported.

**Scheduled Reporting.** Built-in reports for all levels of stakeholders, from executive to technician, can be automatically emailed at any scheduled interval.

**Accurate Vulnerability Status.** It's critical that security personnel track every change to vulnerability status, not just discovery and remediation. Nucleus supports over 10 different vulnerability statuses, ranging from false-positive to risk-accepted, and documents each step along the way to produce a complete and detailed history of each vulnerability, from discovery to remediation.

## TAKE THE **NEXT STEP** WITH NUCLEUS.

How much more secure would your organization be if you could respond to vulnerabilities **10 times faster**? Start your two-week trial Nucleus trial today.

**GET STARTED**