WHITE PAPER

Stop the Guessing Game:

Operationalizing the Vulnerability Remediation Lifecycle

The uncertainty surrounding the CVE program in April 2025, was a wake up call for many organizations to reassess how they detect and resolve high-priority risks. The event underscored the need for a broader, more adaptive approach to vulnerability detection which embraces multiple threat sources, behavioral signals, early warning technologies, asset context, and clear ownership and accountability for security findings.

In this white paper, we'll be focusing on a few fundamental aspects of the vulnerability remediation lifecycle where, unfortunately, the 'guessing game' is often still present: the asset inventory and the ownership assignments.

Real-time Asset Discovery

A periodically updated list of assets simply won't cut it in today's dynamic threat landscape. With the expansion of cloud services, code repositories, IoT and other non-traditional devices, it became increasingly difficult for organizations to maintain a comprehensive inventory. Not to mention missing assets from mergers, acquisitions and subsidiaries.

A full and up to date asset Inventory is essential for maintaining visibility and control over all connected assets across IT, OT, IoT, cloud, and medical environments. Organizations must discover and classify every asset, managed or unmanaged—providing comprehensive, continuously updated asset inventory. This enables accurate, dynamic configuration tracking and supports better decision-making and risk management.

Once this inventory has been established, security teams need to be able to contextualize asset profiles (asset type, reachability, environmental context and business-specific attributes) - and determine which is the most urgent security finding across different tools. An integral component of this approach is ingestion of asset data from scanning tools, IT service management (ITSMs), configuration management databases (CMDBs), code repositories, and cloud asset inventories - so that the findings are associated with a specific asset, and the asset labeled with technical, environment and business context. Using what other systems of record and tools report about assets, security teams can further contextualize what they know about the assets through custom metadata.

Accurate Ownership Assignment

The larger or more complex the organization, the less likely it is that security teams have clear insight into who, or which team, is responsible for remediation. Using predictive assignment that incorporates environmental and organizational context, security teams that may have spent weeks in the past trying to identify a fix owner, can quickly identify the most likely remediation owner and team.

With a more systematic approach in place, security teams can map and maintain remediation ownership in terms of organizational structure - as well as measure remediation performance by owners and teams. Remediation teams can also re-assign the fix, if they or their teams are not responsible for the asset where a finding has been identified. Using a predictive model, rather than relying on institutional knowledge can help refine assignment accuracy over time as the model learns from ongoing interactions and responsibility reassignments.

There's no point in setting up a 'CVE monitoring' tool without a proper mapping between the asset, the CVE and the remediation ownership assignment.

Cyber exposure management solutions must correlate continuous asset identification, precise hardware and software versions, accurate CVE profile matching, and relevant asset ownership.

Let's take a look at an example where both the asset inventory and the ownership assignment play a critical role:

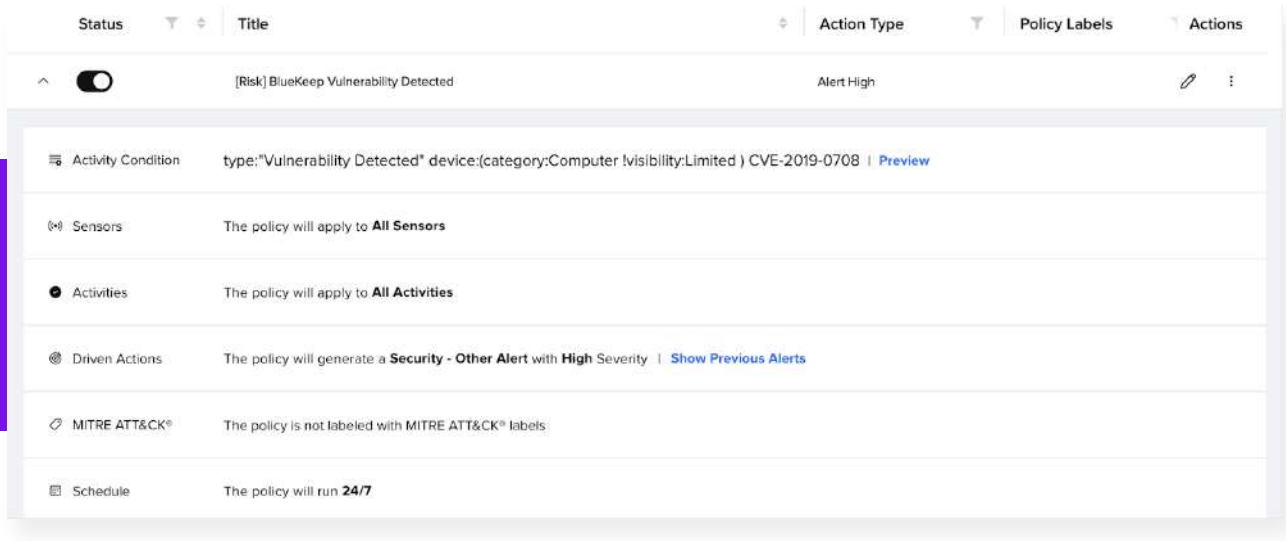
The vulnerability management team receives an RSS feed notification that a specific Access Point and software version is affected by a critical CVE. But when the IT team receives the patch request, the data does not correspond with their asset records in the CMDB. If they knew where the assets were, and who owns them, they could go ahead and patch them, or apply a risk mitigation workaround if patching is not an option (e.g. for OT/CPS systems). But an out-of-date CMDB creates an obstruction in their workflow.

An up-to-date asset inventory and clear ownership assignment would have provided a centralized view, including software versions, patch levels, and hardware configurations, empowering teams to quickly identify and prioritize security findings.

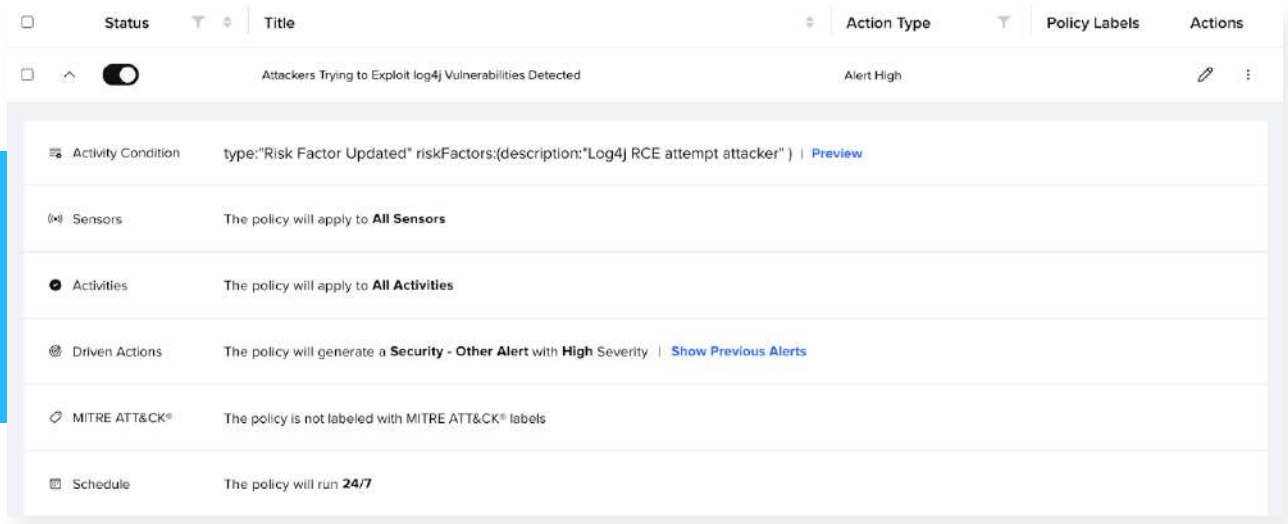
Accurate Ownership Assignment

The Armis Centrix™ Policies Library contains predefined templates recommended by Armis Labs, classified by category and searchable by name or label, including labels such as **New** and **Recommended**. Users can configure and manage policies for specific risk or operational use cases and actions when the conditions match, such as generating alerts or protection countermeasures.

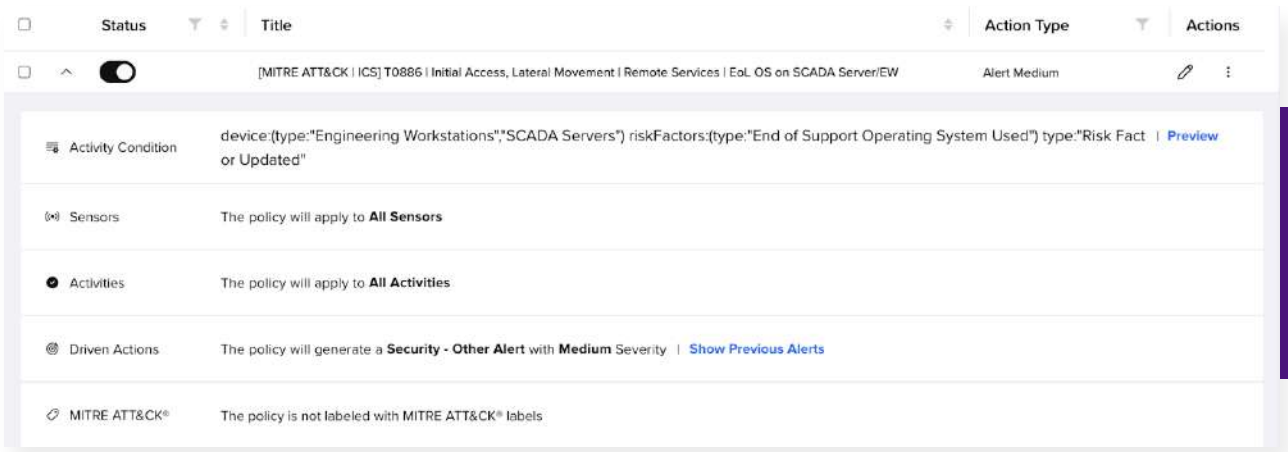
One of the strengths of the Armis approach lies in the combination of real-time asset intelligence, an understanding of what these assets are doing on the network, and a broad coverage of all security findings and vulnerabilities - including Early Warning alerts. Below are a few examples where conditions are used to alert for security findings like CVEs, End Of Support (EOS) hardware and Remote Code Execution (RCE):



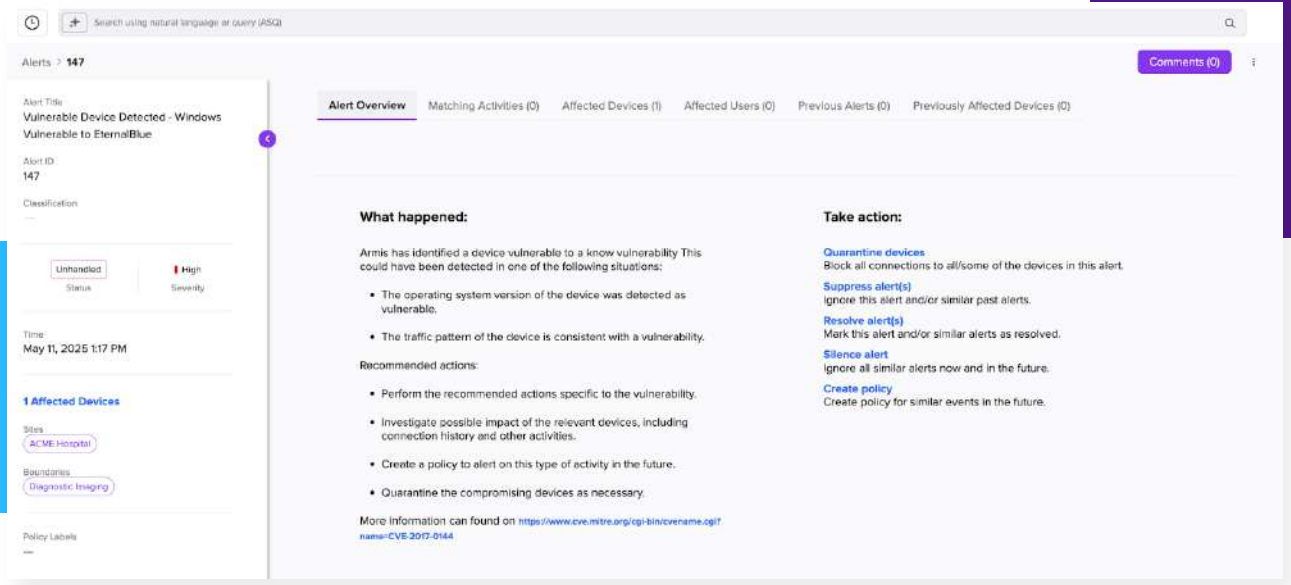
Armis Centrix ™ Security Policy to alert when a device is observed as potentially vulnerable to BlueKeep CVE. and actions when the conditions match, such as generating alerts or protection countermeasures.



Armis Centrix™ Security Policy to alert when an attacker is attempting Log4j Remote Code Execution (RCE).



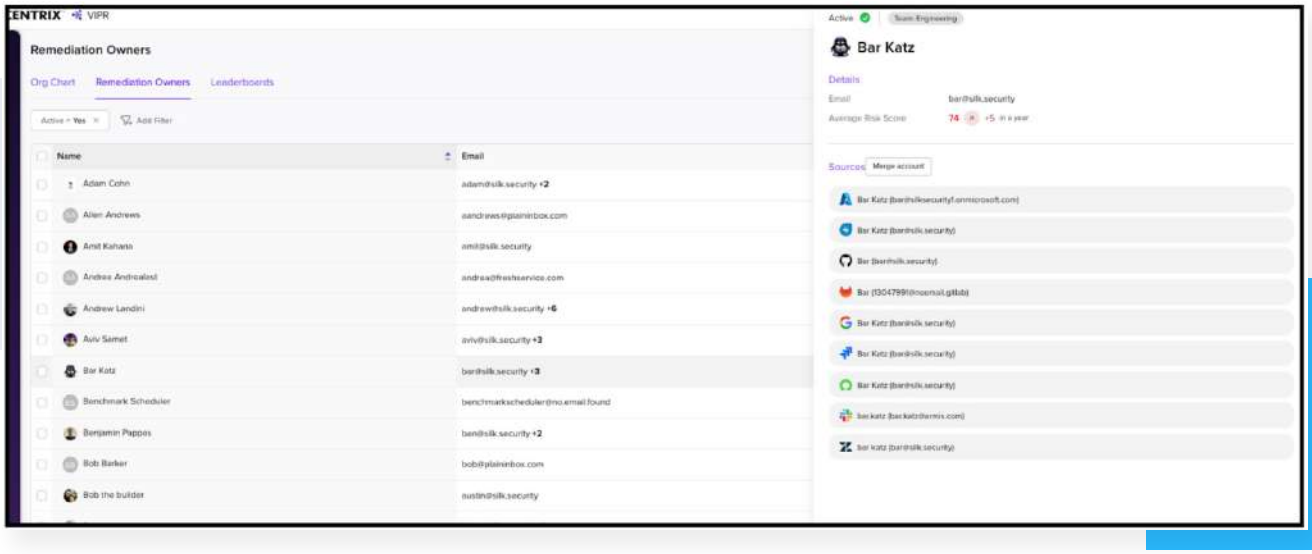
Armis Centrix™ Security Policy to alert when an SCADA Server or an Engineering Workstation is seen with EoS/EoL Component (here: Operating System, matching the MITRE ATT&CK for ICS framework).



Armis Centrix ™ Security Alert of a Windows device seen as vulnerable to EternalBlue (CVE-2017-0144).

In terms of ownership assignments, Armis performs asset ownership association to inform remediation ownership. Security teams can use two methods to assign ownership:

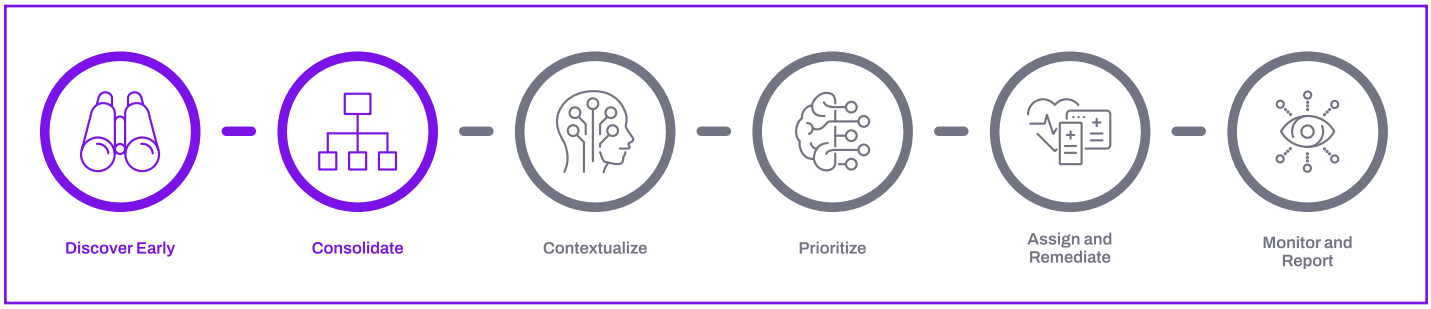
- Predictive ownership assignment, utilizing a predictive AI model based on data ingested from infrastructure logs, code commits and integrations with user directories.
- Ownership rules defined by security teams for assets and findings, using tags and labels from asset data to inform ownership rules.



Remediation owners and asset owners can both re-assign assets and remediation responsibility. For instance, a team that is responsible for the Java code running on an asset, but may reassign responsibility for patching the Linux machine on which the code runs.

The End Goal: Prioritizing and Connecting the Findings to the Fix

The objective of all these efforts should be to identify and reduce risk. Technology should help to group high severity issues identified by multiple tools, as well as applying the common fix to better automate the remediation process. A platform approach like Armis Centrix ™ offers value along the full vulnerability management lifecycle:



Discover Early

Leverage early warning intelligence into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing your organization to understand their impact and take preemptive action.

Consolidate

Aggregate, normalize and de-duplicate data from security scanner and detection tools for endpoints, physical devices, cloud, code and applications. Ingest and inventory asset data from asset management, security tools, ITSMs and infrastructure.

Contextualize

Assign context to findings including threat intelligence, likelihood of exploit, and weighted asset attributes such environmental information and business impact. Understand how findings are related in the context of the software development cycle (SDLC) and application infrastructure.

Prioritize

Automate prioritization based on business impact, adaptable risk assessment, likelihood of the exploit and active exploit activity. Associate and propagate custom metadata with assets to reflect specific attributes, and apply risk weightings.

Assign and Remediate

Leverage AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Ongoing communication for distributed teams through bidirectional integration with their preferred workflow or ticketing system. Bulk ticketing automation and flexible remediation campaigns.

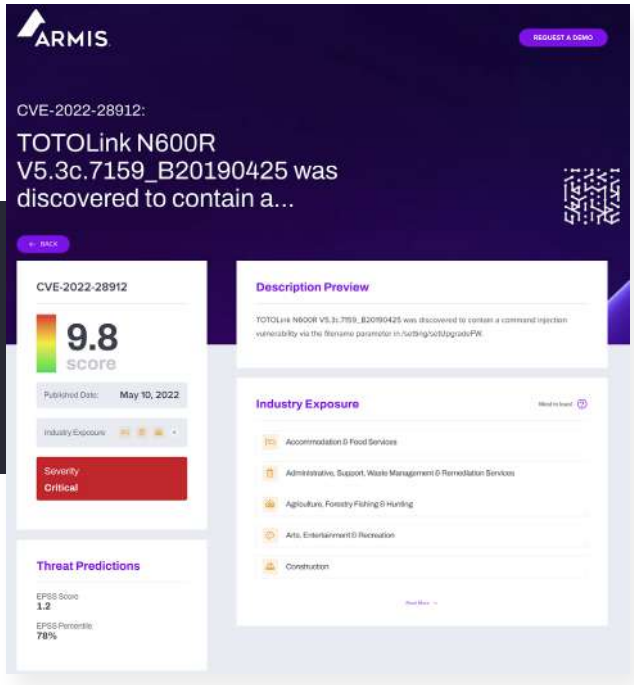
Monitor and Report

Centralized tracking and monitoring of remediation task status, by criticality, finding category and asset class. Measure the effectiveness of the remediation process for executive stakeholder reporting.

The Bigger Picture: Stopping Attacks During The 'Initial Access' Phase

According to the MITRE ATT&CK® framework, Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Stopping an attack at the initial access stage, prevents attackers from moving laterally in the network or reaching their ultimate objective, whether that's data exfiltration, or another form of attack. In reality, 58% of global organizations only respond reactively to threats after damage has already been done. In addition, nearly one-fourth (22%) of IT decision-makers cite a lack of continuous vulnerability assessment as a current gap in their security operations, with many still tracking vulnerabilities and security findings using spreadsheets. There is a clear need to fill these gaps before there's negative impact.



In an effort to provide organizations with the knowledge to better prioritize and mitigate threats in real time, Armis recently announced the free availability of the Armis Vulnerability Intelligence Database.

The community-driven database integrates exploited vulnerabilities, emerging threats and AI-powered insights, providing the cybersecurity industry with the knowledge organizations need to better prioritize and mitigate threats in real time.

Additionally, Armis has been authorized by the Common Vulnerabilities and Exposures (CVE®) Program as a CVE Numbering Authority (CNA). The mission of the international program is to identify, define and catalog publicly disclosed vulnerabilities. As a CNA, Armis can review and assign CVE IDs to newly discovered vulnerabilities.

By delivering critical insights faster than traditional databases, organizations can harden their environments before vulnerabilities or risks are widely exploited.

Conclusion

It's time to question whether traditional methods of identifying and tracking threats are resilient enough for today's evolving risk landscape. Solutions like Armis take a data-centric, AI-driven approach to enable security stakeholders to better identify risks, communicate priorities, assign owners, and collaborate with developers and operations stakeholders to efficiently manage the entire lifecycle of the resolution management process.

This approach extends across any security finding including infrastructure, code, cloud and application security tools, providing security teams with a consolidated view and clear understanding of how to prioritize and remediate along with how these activities impact overall risk posture that can impact the business.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo