ARMIS®

WHITEPAPER

Modernizing Vulnerability Management to Reduce Risk

Introduction

The vulnerability management process is broken

Vulnerability management teams are increasingly overwhelmed by security alert backlogs which can often number in the millions. The growth of alert backlogs is driven both by more alerts, as well as the limitations of existing vulnerability management programs in assessing and triaging the alerts.

In 2024, the cybersecurity community observed a significant surge in reported Common Vulnerabilities and Exposures (CVEs). Over 40,000 CVEs were published, representing a 38% increase from the 28,818 CVEs recorded in 2023. This marks the seventh consecutive year of record-high CVE publications since 2017.

These alert backlogs have compounded existing challenges for vulnerability management teams to identify and fix risk:

- Most employ manual assessment processes that can only scale linearly by adding more analysts
- They struggle to automate prioritization based on actual risk and specific business impact, and justify which a finding is a priority to fix
- Assigning remediation responsibility is a guessing game, especially in complex organizations
- Teams can't standardize processes without a consolidated approach across tools and centralized collaboration across remediation workflows

As a result, teams struggle to systematically, consistently and efficiently determine:

- which findings to fix first based on contextualized risk
- why and how to fix those findings
- who should be responsible for the fix
- and, if a fix was implemented.

Operations teams, in turn, often lack the context needed to assign and operationalize the fix, and struggle to collaborate with security teams through their existing workflows- especially when requesting exceptions or accepting risk.

Why fix the problem?

The current vulnerability management process consumes limited security operations resources, and falls short in efficiently reducing risk.

For security teams, the manual steps involved in vulnerability management have become a significant operational overhead. Based on some statistics that put the average time to assess a single alert at 21 minutes, security teams can spend up to a quarter of their time sifting through alerts and determining priorities.

In turn, risks go unremediated and the window for attacker exploit is elongated because of inefficiencies in assessing, assigning remediation tasks, and providing actionable guidance.

According to the 2024 Verizon Data Breach Incident Report: on average, 85% of identified vulnerabilities included in the CISA Known Exploited Vulnerabilities (KEV) catalog were unremediated after a month; and, even after a year, 8% were still unremediated.

Because CISA KEV covers only CVEs (as opposed to other code, cloud and AppSec exposures or CWEs) and catalogs documented active vulnerability exploits, this protracted average mean time to resolution (MTTR) for high-risk issues underlines the extent to which poor processes expose organizations to threats.

Meanwhile, more automated threat exploit techniques elevate the risks posed to organizations from opportunistic attacks leveraging unremediated exposures and vulnerabilities.

Focus on the fix to unravel the problem

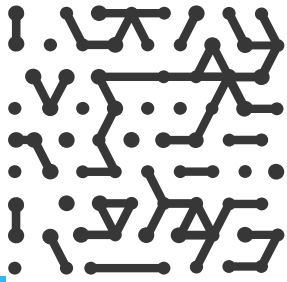
Traditional vulnerability management programs focused on generating a list of identified vulnerabilities categorized by severity, based on scanner output. This approach worked adequately in the past to deal with scans conducted on a quarterly basis for a small number of asset types, with defined processes to coordinate with IT or engineering teams to remediate over a course of months.

Today's reality is more stark: alongside the proliferation of security tools continuously generating alerts without enough context to perform prioritization, the security team with finite resources has to orchestrate remediation across many teams on a more frequent cadence in order to reduce risk.

To adjust to the new reality, vulnerability management teams both need a new orientation on what and why to fix - as opposed to assessing severity alone.

By re-orienting programs to focus on the fix, security teams can begin to reverse the alert backlog in the first instance, and more critically, begin to materially impact technology risk posture.

To facilitate this orientation, a new technology foundation, asset context, automation and bidirectional integrations are needed for operationalization.



To fix the broken process, and achieve the objective of risk reduction, the technology should encompass both prioritization and remediation to enable a comprehensive process:

Identify: Aggregation, normalization and de-duplication of tool output to convert alerts into consolidated, actionable findings

Prioritize: Contextualization of security findings based on asset profiles, business-specific attributes, and exploitability to establish where to focus

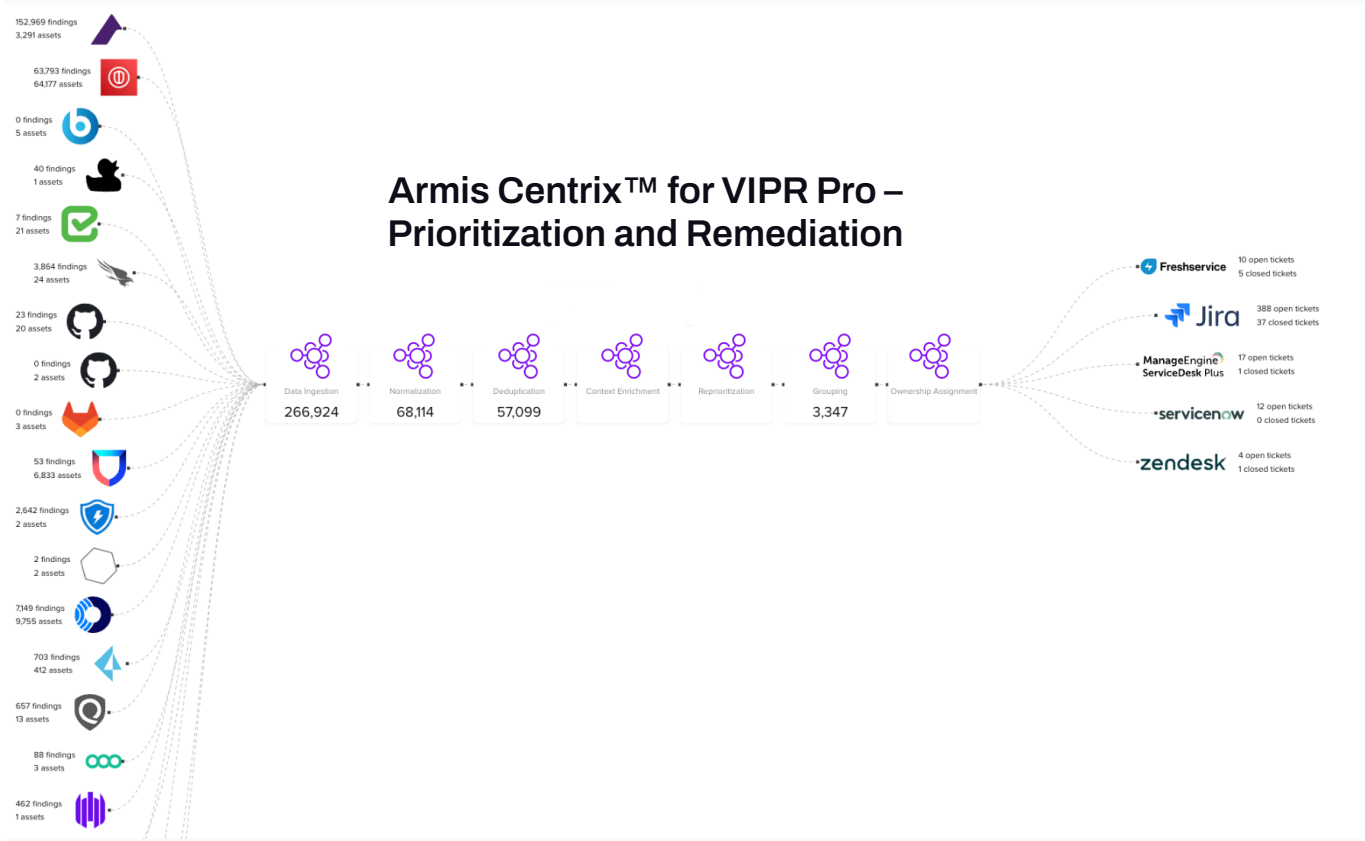
Assess: Re-prioritization of all findings across tools, based on adaptable risk weightings specific to the organization in tandem with asset intelligence and enrichment

Remediate: Grouping of findings based on common fix to automate multiple remediation paths with remediation guidance and justification

Assign: Predictive assignment using AI of remediation task ownership, supplemented with asset ownership rules

Verify: Bidirectional integration with ticketing workflows to provide remediation fix guidance and collaboration on remediation tasks

Report: Centralized reporting of remediation task status across workflows, and monitoring of remediation activity by teams and divisions

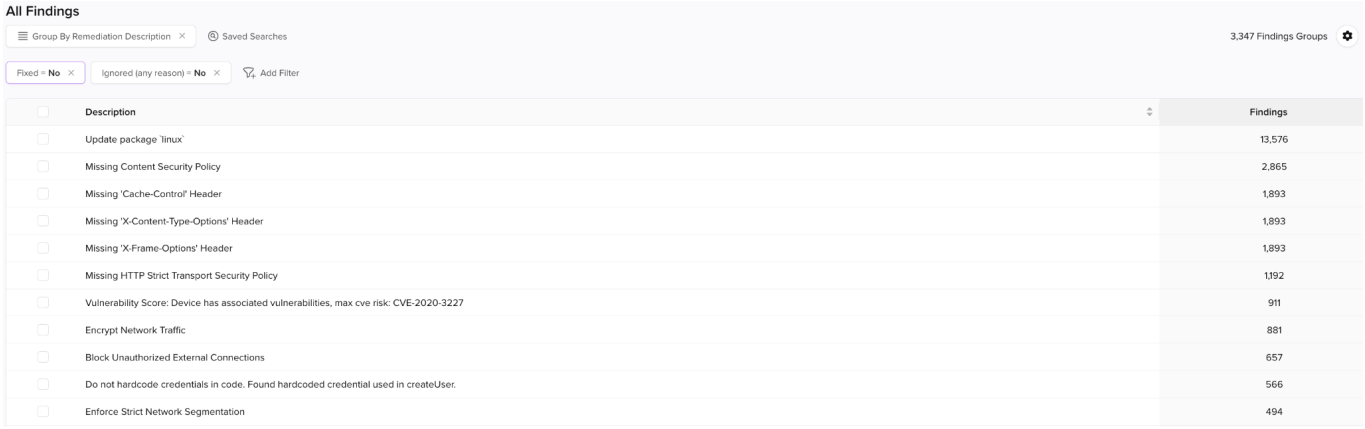


Consolidated process across prioritization and remediation, aligning security and teams responsible for fixes.

Scaling identification with a data-centric approach

The technical foundation needed for a modern vulnerability management process is an extensible and scalable data pipeline that tackles the challenge of volume, diversity and different formats of alerts from multiple tools, and integrates correlation with a range of asset types from code to cloud.

By normalizing both alerts and asset data as part of data pipeline process, security teams can dramatically reduce the overall volume of alerts: firstly, through deduplication (which can reduce the overall volume upwards of 60%); and, secondly, through grouping of findings with a common fix (which can reduce volume by 50 to 1) as an outcome of the data pipeline process.

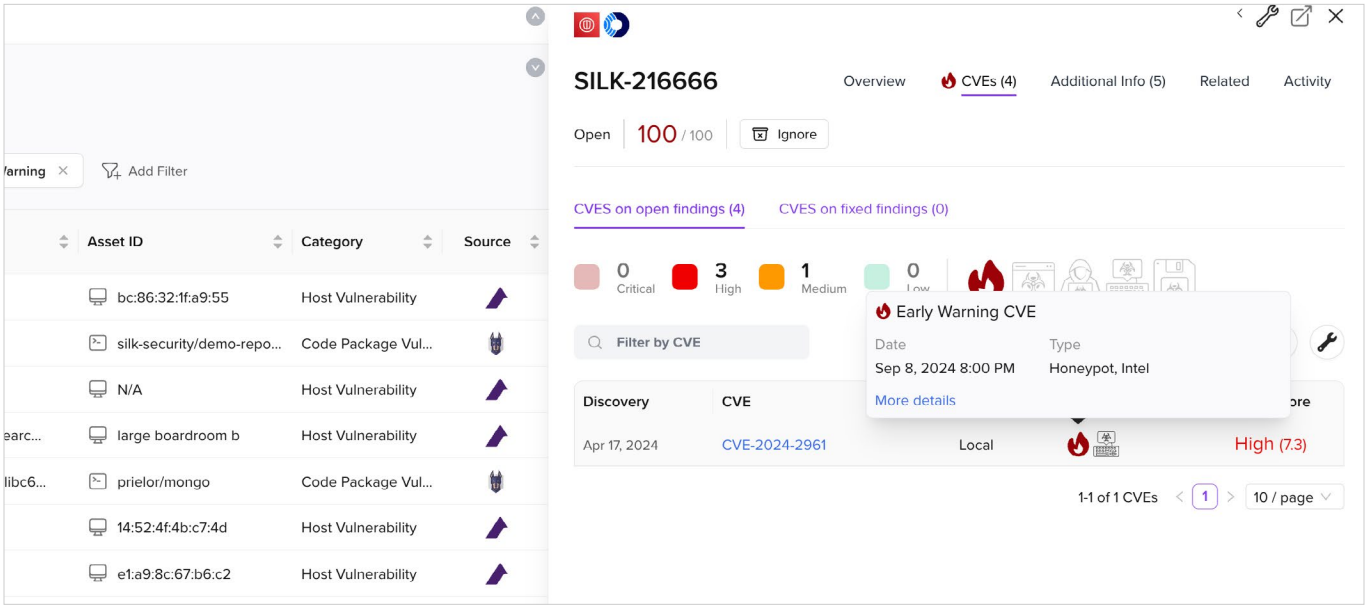


Description	Findings
Update package `linux`	13,576
Missing Content Security Policy	2,865
Missing 'Cache-Control' Header	1,893
Missing 'X-Content-Type-Options' Header	1,893
Missing 'X-Frame-Options' Header	1,893
Missing HTTP Strict Transport Security Policy	1,192
Vulnerability Score: Device has associated vulnerabilities, max cve risk: CVE-2020-3227	911
Encrypt Network Traffic	881
Block Unauthorized External Connections	657
Do not hardcode credentials in code. Found hardcoded credential used in createUser.	566
Enforce Strict Network Segmentation	494

Grouped findings based on a common fix

By automating data consolidation and aggregation, teams can take a more systematic and strategic approach to prioritizing fixes, since they are dealing with a manageable set of fixes that can in turn be remediated using operationalization processes that minimize manual steps, like bulk ticketing, centralized activity monitoring across workflows, and bidirectional communications.

Incorporating a process to de-duplicate data, and then performing an association of assets with findings further minimizes manual assessment, and allows analysts to evaluate the threats to a specific critical asset. This is an important aspect for understanding the risk posed by ‘chaining vulnerabilities’, where one CVE may have a low severity but could be an attack path for a more critical severity exploit.



Evaluate the risk of multiple CVEs on a single asset, augmented with Early Warning threat intelligence

Prioritization: findings plus assets plus risk

While rationalizing the number of findings is important for operational efficiency, the objective should be to identify and reduce risk. The challenge that many organizations face is moving from a generic technical severity to understanding which findings represent the most urgent risk to their organization.

In order to make this determination, teams need to be able to contextualize findings based on which assets were identified, their relative criticality across all findings, as well as exploitability - and active exploit activity. This context includes information asset profiles (asset type, reachability, environmental context and business-specific attributes) - and which is the most urgent across tools.

Also, since new exploits are developed on an ongoing basis, it's imperative to integrate actionable threat intelligence on emerging active - and successful exploits - to hone in which findings present the most critical risk to the organization's specific environment.

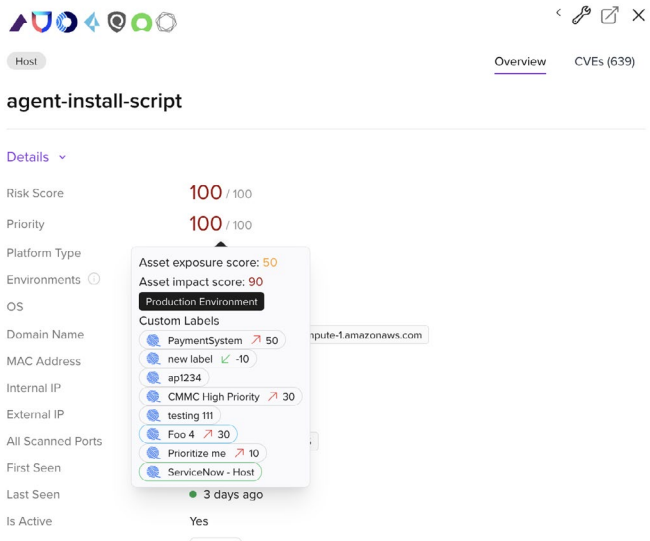
An integral component of the data pipeline is ingestion of asset data from scanning tools, IT service management (ITSMs), configuration management databases (CMDBs), code repositories, and cloud asset inventories - so that the findings are associated with a specific asset, and the asset labeled with 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.

By applying risk weightings to custom metadata - for asset attributes, compliance or properties such as external facing - security teams can both prioritize and suppress findings based on considerations that are specific to their business and environments.

Supplemented with threat intelligence such as Armis Centrix™ for Early Warning, as well as exploit likelihood scores derived from CISA KEV catalog and Exploit Prediction Scoring System (EPSS), security teams can both radically reduce time spent on assessing priorities and maintain a much more efficient process for determining and acting on the highest risk exposure findings.

In turn, they often need more context to prioritize between the high severity issues identified by multiple tools, as well as how to group findings from multiple with a common fix to better automate the remediation process.



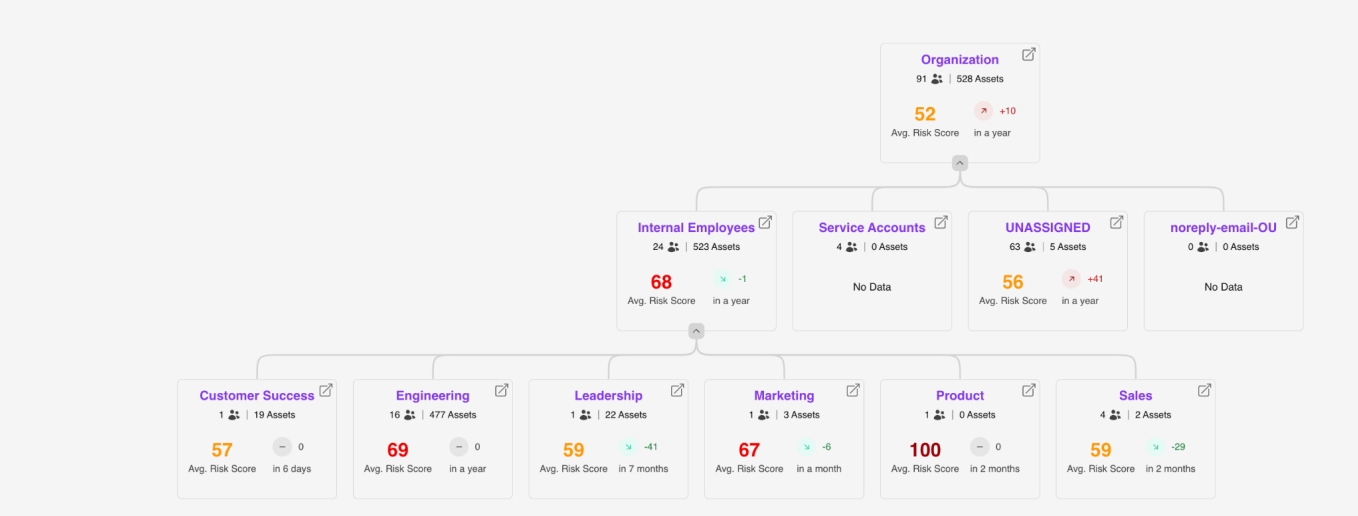
Assign asset exposure and business impact scores using custom metadata and risk weightings

Filling in the missing link between prioritization and remediation: ownership

Just as new technology adoption has put existing vulnerability management approaches under enormous strain, security teams often struggle to identify a fix owner in the absence of consistent organizational knowledge for fix ownership mapping and automated assignment rules. The larger 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 - as opposed to institutional knowledge can help refine assignment accuracy over time as the model learns from ongoing interactions and responsibility reassignments.



Automate organizational mapping of remediation owners, associated assets, and track remediation performance by teams and OU

Closing the loop: Remediation via collaboration

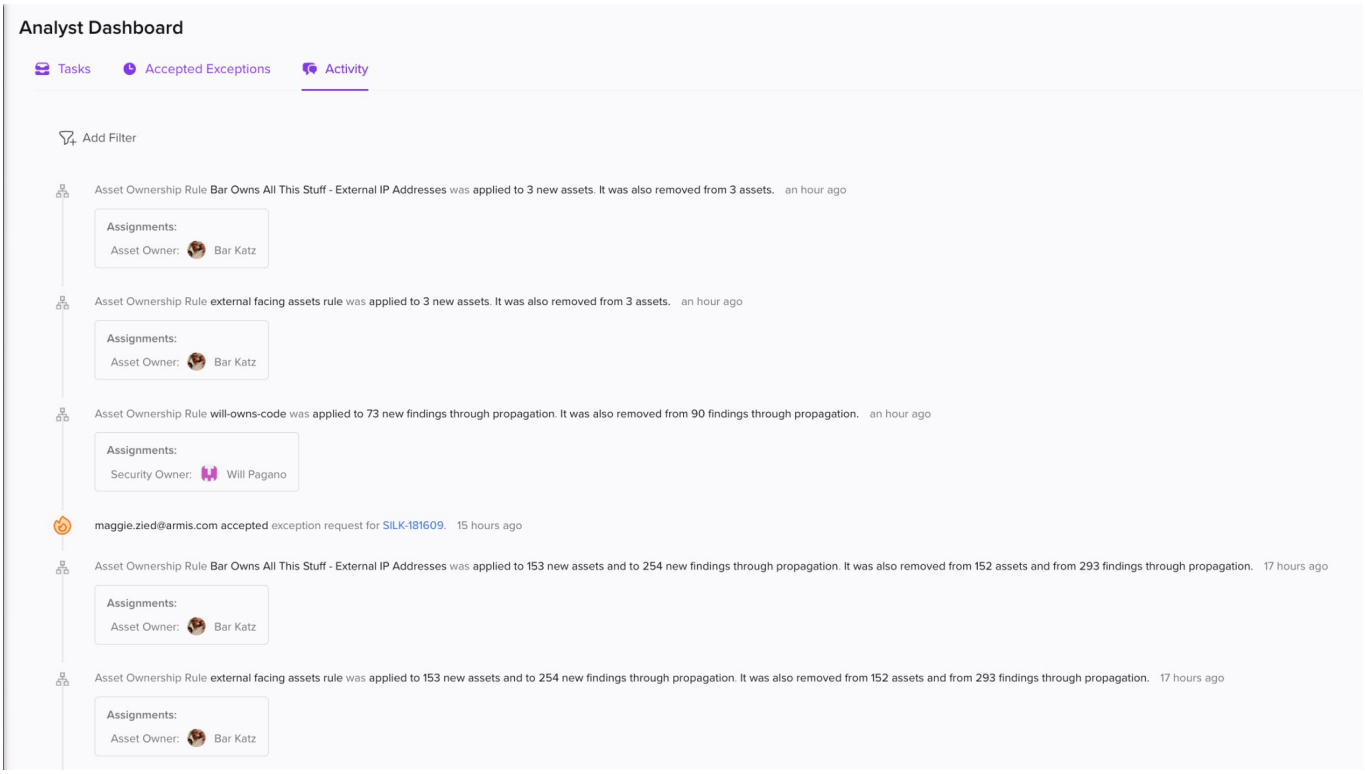
Fixers often face the same scenario: they have no context on how security teams reached a prioritization decision; and, have to decide how to take action based on output designed for security teams, most notably technical severity ranking.

By taking a remediation orientation built on data-driven contextualization, security teams can provide clarity in how they collect data, conduct risk evaluations, and formulate recommendations.

This clarity (as opposed to cut and paste from the detection tool into a ticket) helps build trust, and it also makes it easier for organizations to understand and justify their decisions about managing vulnerabilities, threats and non-CVE exposures, such as cloud security misconfigurations that are not the realm of responsibility for teams that are tasked with host vulnerability remediations.

Once the right fixer has been determined, and security teams have the appropriate information and justification based on adaptable prioritization, the next phase is what analyst firm Gartner refers to as mobilization.

Mobilization entails ensuring that remediation tasks are consistent with the fixer's day-to-day workflow in their ticketing workflow of choice. Also, through bidirectional integration with a centralized dashboard, analysts can interact with fixer feedback on guidance, as well as track exception or risk acceptance requests.



Centralized visibility into remediation activity across tasks and tools through the analyst dashboard

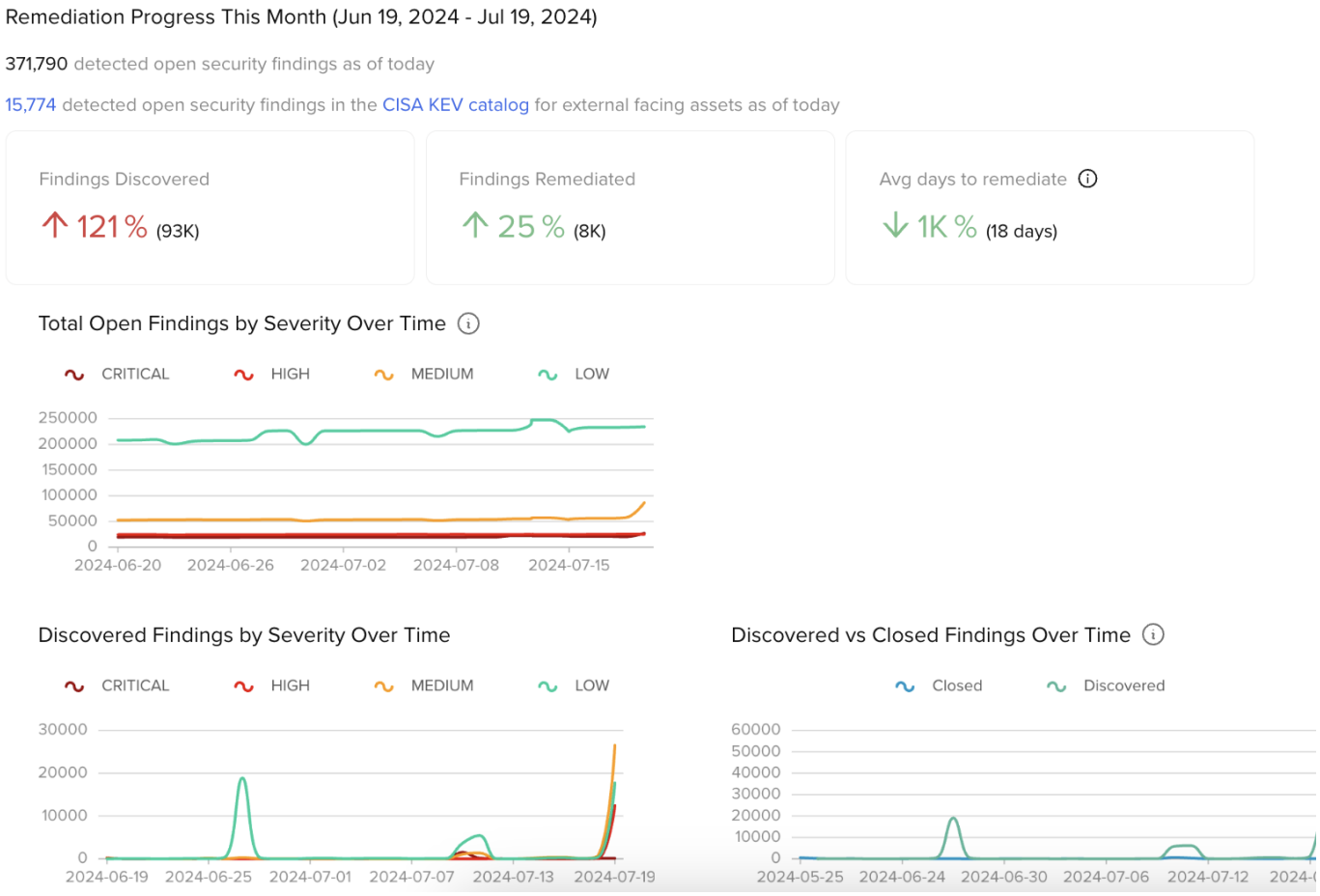
Measure Effectiveness: Centralized Tracking and Reporting

Tracking down individual requests across workflows and instances of the tool can be time-consuming and inevitably involves manual collection of data for reporting.

In turn, this lack of consolidated visibility into remediation tasks stands in the way of not only reporting on remediation trends by criticality - but also by remediation performance and exception requests trends for teams, business units and across the organization - and by extension, overall risk posture.

Centralized visibility across all remediation tasks, team performance and risk posture status fundamentally shifts the conversation across stakeholders and streamlines reporting.

As an integral outcome of centrally tracking and monitoring, Armis can report on remediation and resolution trends - reinforcing the benefits of a holistic approach. Security teams can centrally monitor both remediation task status and exceptions requests - providing a centralized view of open findings across the organization, and which teams or business units are performing well in managing risk posture - and which not.



Centralized monitoring of remediation performance

Revisiting the process

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.

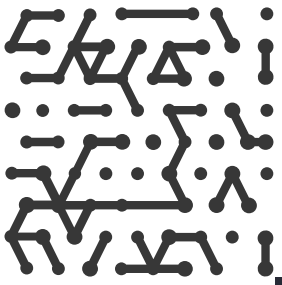
Monitor and Report

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

How Armis Helps

Armis takes 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
Free Trial