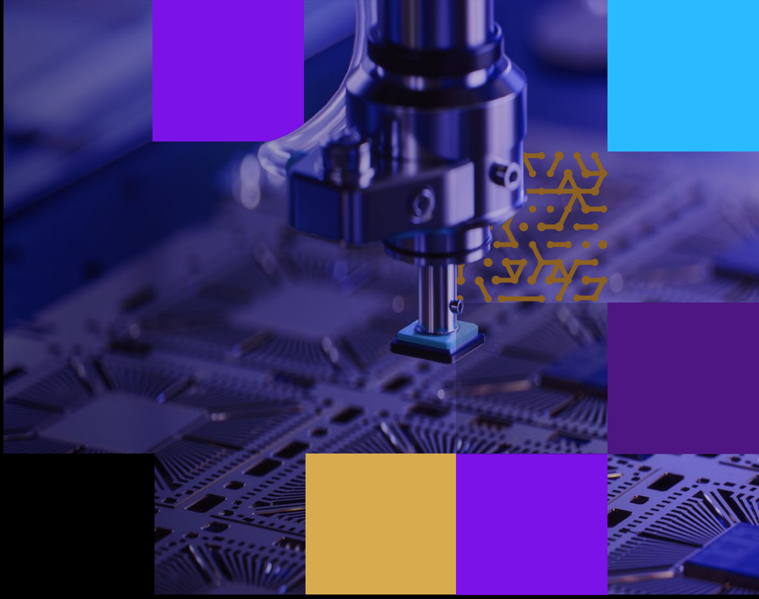

CASE STUDY

Integrating Asset Risk for Remediation Prioritization and IT Collaboration

The Challenge

- No consolidated view from multiple detection tools inherited through M&A, including native tools from AWS, Google, and Azure
- Inefficient and inconsistent processes to identify and communicate high-risk findings
- No effective multicloud platform to model attach chains and dependencies

The Solution

- Native integrations with AWS Security Hub, Google SecOps, Azure Security Center, and many other 3rd party security tools to correlate asset risk & prioritization
- Bidirectional integration with existing IT asset management tools, including ServiceNow, to enrich asset profiles
- Integrated ticketing workflow creating an automated remediation processes

The Results

- 50% increase in the security team's productivity for prioritization
- 200% increase in closed tickets
- Retired tool budget enabled faster consolidation on AWS
- Single CAASM solution on AWS reduced multicloud rework by an estimated 30%

Industry Electronic Manufacturer

Location Taipei, Taiwan

Size 40,000 employees | >$4B revenue

Background

A leading global electronic component manufacturer with over 100 production plants supplying and sales in over 200 countries through 40,000 employees around the globe, resulting in more than $4B in revenue in 2022.

Customer has acquired many disjointed, legacy solutions spanning AWS, Google Cloud, Azure, and private datacenters. Their inability to coordinate, prioritize, and remediate was recognized as a significant risk by their board.

The Challenge

As a global company with a centralized security function, Customer sought a consolidated approach to identifying and managing vulnerability findings across their entire network. Throughout a series of acquisitions, the security operations team inherited multiple detection tools with overlapping, disjointed functionality. The resulting complexity led to inefficient processes consuming resources to sorting through duplicate alerts before findings could be assessed. Alert overload hampered the security team's ability to focus remediation priorities on IT operations based on the highest risk, negatively impacting collaboration.

In addition to the need for a consolidated view of the output from multiple tools, the Customer security team set out to more efficiently and consistently identify and communicate high-risk findings for remediation owners by:

- Improving finding prioritization decisions by incorporating contextualized risk
- Centralizing an asset inventory to support holistic risk analysis and enriched asset profiles
- Ensuring ongoing risk posture assessment through integrated asset and finding assessment
- Operationalizing a consistent process to assign, track, and report remediation task status
- Prepare & assist AWS migration/consolidation of resources

> *"Armis has revolutionized how we identify and prioritize security findings. Regardless of how we discover the issue, we have full visibility across the entire lifecycle and all environments, all in a single interface. That lets us make smarter, faster decisions and centrally track them through to completion"*
>
> Director, Information Security and Compliance

150% effectiveness for prioritized remediation by the security team

200% increase in closed tickets

>$1M freed up budget from tool retirement

The Solution

Customer implemented a phased approach to tackling risk prioritization and resolution challenges the security team faced.

Findings Consolidation

First, the security team deployed Armis Centrix™ to perform consolidation and de-duplication of alerts from each cloud and each tool deployed at various sites to link findings to a centralized asset inventory. Centrix™ helped the team reduce the number of duplicate alerts generated across all tools creating immediate opportunity to reduce tool license spend.

Asset Context Enrichment for Risk based Prioritization

Armis' ability to represent asset context with custom labels and enrich asset profiles in the enterprise CMDB with security information enabled the security team to incorporate risk analysis in their finding assessment process. With this context, the security team was able to provide the IT operations team with a set of clear prioritized findings for remediation.

The more explicit guidance on which remediation tasks to prioritize enabled the security team to more productively interact with IT operations and better determine who was responsible for remediation tasks.

Automated Remediation Fix Integration

The de-duplication of alerts and findings comparison reinforced the value of Armis' unified view of findings and enabled integration with the IT ticketing management system for remediation workflows.

Centrix™ facilitated a centralized approach to assigning fix owners and tracking the status of remediation tasks based on actual risk to their specific environment. With a unified view across the remediation ifecycle in place, the security teams no longer needed to log into multiple dashboards and ticketing systems, further improving collaboration and efficiency.

Results

- 150% effectiveness by the security remediation team due to consolidation and de-duplication of findings combined with automated generation of remediation tickets
- Retired overlapping detection tool with confidence, saving over $1M within 1 year of adopting Centrix™
- Freed up the budget used to accelerate migration and replatforming to native AWS services including EKS, RDS, Lambda and CloudFront
- 200% increase in closed tickets due largely to more effective collaboration between IT and Security teams

ARMIS

1.888.452.4011
www.armis.com

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