CASE STUDY

Closing the Loop: Making Security Everyone's Business with Prioritization & Collaboration

The Challenge

- Maintaining a consolidated view of risk posture & priorities across pipelines & environments
- Reducing the alert fatigue and backlog from fragmented tools
- Determining which team is responsible for implementing a remediation

The Solution

- Prioritize AWS remediation actions based on risk and business context
- Leverage complete view of risk profile to direct software development teams to areas of highest impact
- Scale remediation operationalization through bulk ticketing in remediation for shared resolutions

The Results

- Reduced manual reviews by 80%
- Reduced time spent on prioritization efforts by 70%
- Reduced time spent identifying and assigning fix responsibility by 80%
- Improved number of closed findings by 600% on a monthly basis

Industry Technology

Location Rotterdam, Netherlands

Size 1500 employees | 10M customers

Background

Mendix, a Siemens business, is an industry leading low-code application development platform that helps organizations build multi-experience, enterprise grade applications at scale. More than 4,000 organizations in 46 countries use the Mendix low-code platform. An active community of over 300,000 developers has created over 950,000 applications.

The Challenge

As Mendix modernized its application lifecycle and transitioned to AWS, the security team encountered challenges in:

- Consolidating findings from multiple AWS and 3rd party tools
- Identifying high-impact fixes earlier in the software pipeline
- Communicating priorities effectively with engineering teams in support of the high volume of requests with limited context
- Consistently enabling the "last mile" of remediation by assigning responsibility to the right owner

The outcome was significant inefficiencies in risk prioritization, and time consuming, manual efforts to establish which teams and individuals on the engineering team were responsible for remediation fixes and the issuing of individual tickets for issues with a common fix. As the alert backlog grew, the problem of prioritization and assignment inefficiencies intensified and consumed an increasing amount of time and resources.

"Armis Centrix™ has positively impacted both the productivity and the efficiency of the security team in identifying risks to the business, as well as how the function of security is integrated into our development processes. The security team can collaborate more closely with development teams responsible for implementing the fix for identified priorities, and improve our overall risk profile."

Frank Baalbergen
CISO, Mendix

The Solution

Mendix deployed the Armis Centrix™ through an agentless integration across their pipelines, from CodeCommit to the native AWS environment including EKS, Security Hub, GuardDuty, ControlTower, and many 3rd party security tools. With consolidated findings, visibility, asset profiling, and threat intelligence, the security team gained a clear picture of which findings to prioritize based on actual risk and likely impact. By understanding how findings were related through asset linking, the security focused remediation efforts on the earliest point possible in the pipeline, reducing mean time to resolution (MTR).

The clear understanding of Mendix's risk profile and priorities enabled security teams to interact more constructively with the engineering teams, focusing on clear guidance & counteracting alert fatigue.

In tandem with consolidating and prioritizing output, the security team also implemented Armis' predictive assignment for ownership and ticketing integration, resulting in faster remediation and deeper collaboration between security & software development teams.

Additionally, the security team utilized automated remediation campaigns for bulk ticketing of related findings with a shared solution, dramatically reducing ticket volume and rework.

The Results

The security team experienced significant operational improvements through the remediation lifecycle across multiple native AWS services and code pipeline.

With native & 3rd party detections integrated, the team refined prioritization and assignment rules tailored to their environment to build a complete, reliable picture of risk prioritization for remediation.

The ability to facilitate the "last mile" of the remediation process by identifying which team or person can implement the fix both reduced the pressure on the security team to add additional headcount and helped make security an integral part of the fixer's daily operations.

The combination of operational efficiencies with more accurate and up-to-date reporting has allowed the team to more proactively manage their risk profile across AWS services. In turn, more automated fix assignment for findings with relatively high urgency allowed Mendix to reduce the exposure window while fostering collaboration with software development teams through clear communication of risk.

600% Improved number of closed findings on a monthly basis

80% Reduced time spent identifying and assigning fix responsibility

70% Reduced time spent on prioritization efforts

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