AMISEQ
YOUR TECH PARTNER

Automated Vulnerability Mitigation Accelerates Security Response

Client Overview

A global software company delivers Intelligent Automation solutions for enterprise environments handling mission-critical operations. The security team manages a continuous stream of vulnerabilities from multiple sources, requiring fast and accurate mitigation to maintain system integrity and compliance.

With increasing threat volumes, the organization needed a more scalable approach to vulnerability management that could accelerate response times while reducing manual effort.

Challenges Faced

Vulnerability mitigation relied on manual planning and analysis, slowing response times and increasing security risk.

High Volume of Vulnerabilities

Around 1,400 vulnerabilities from multiple sources created constant pressure on security teams.

Manual Mitigation Planning

Each vulnerability required a step-by-step plan created manually, increasing effort and inconsistency.

Time-Intensive Analysis

Generating a mitigation plan took about 30 minutes per vulnerability type, delaying response.

Delayed Remediation and Risk Exposure

Manual workflows slowed action, increasing exposure to threats and compliance risks.

The Solution

Amiseq implemented a **Vulnerability Mitigation Automation** powered by AI to accelerate response and standardize remediation.
The solution integrates Microsoft Teams Copilot for intake, applies automated filtering based on risk factors, and uses GenAI to generate mitigation plans. These plans are then executed through automated ticket creation and assignment, ensuring faster and more consistent response.

Why the Client Chose

AMISEQ
YOUR TECH PARTNER

- Expertise in AI-driven automation for security operations
- Ability to integrate across collaboration tools and security workflows
- Proven capability in scaling high-volume, complex processes
- Focus on improving response time while maintaining control and accuracy

Strategy and Implementation

Initiate Vulnerability Intake

Users submit vulnerabilities through Microsoft Teams Copilot using structured inputs.

Filter and Prioritize Risks

Automation categorizes vulnerabilities by risk level, type, and affected systems.

Generate Mitigation Plans with AI

GenAI (Odin) creates structured mitigation plans for each identified vulnerability.

Create and Assign Tickets

Automation generates IT tickets and assigns them to the appropriate teams.

Report and Track Resolution

Automation generates reports to track progress and ensure visibility.

What Amiseq Delivered

100%

Effort Reduction

Manual mitigation planning was fully eliminated.

700

Hours Saved Annually

Security teams significantly reduced time spent on repetitive analysis.

$21K

Annual Cost Savings

Operational efficiency improvements led to measurable cost reduction.

Faster Risk Remediation

Accelerated response improved overall security posture and reduced exposure.

Conclusion

Vulnerability mitigation is now executed with speed, consistency, and intelligence. Automated planning and execution reduce delays and ensure that risks are addressed as they arise.

Security teams can focus on higher-priority threats instead of manual planning. The organization benefits from faster response, stronger control, and a scalable approach to managing growing vulnerability volumes.

Modernize Vulnerability Management

See how Amiseq can automate vulnerability mitigation and accelerate security response.

California, AMISEQ HQ

1551 McCarthy Blvd Suite # 207
Milpitas CA 95035.

+1 510 509 9888

AMISEQ
YOUR TECH PARTNER