OpsMx

CASE STUDY

Cybersecurity Enhancement for a Global Enterprise

Customer Overview

This case study highlights a European multinational engineering and technology company with over 200,000 employees and close to 100 billion euros in annual revenue. The organization operates on a global scale and is committed to innovation and operational excellence.

Objective

The objective was to reduce the gap between cybersecurity knowledge and development practices by training developers on tool usage, distributing licenses, and addressing concerns that could not be automated. This approach focused on fixing vulnerabilities early in the Software Development Lifecycle (SDLC) to significantly reduce costs and enhance both security and developer productivity.

Key Metric: Each vulnerability fixed in the development environment rather than in production saved **$5,000.**

Challenges

High Cost of Vulnerabilities in Production

- Vulnerabilities missed during development cycles led to costly fixes in production.
- Estimated cost per vulnerability in production: $5,000.

Manual Efforts in Security Assessment

- Security teams manually classified issues into compliance categories (e.g., PCI, internal, external compliance), leading to significant productivity loss.
- Delays in communication between security teams and developers due to manual processes.

Knowledge Gap Between Security and Development Teams

- Developers lacked the cybersecurity knowledge required to address vulnerabilities effectively.
- Security teams had to bridge this gap, which increased their workload.

Scalability Issues

- The existing process required installing security tools and building infrastructure for every project, which was time-consuming.
- There was a need for a centralized security platform that provided on-demand scanning capabilities.

Compliance Challenges

- Manual compliance checks and audits consumed significant time and resources.
- Lack of readily available compliance scorecards (e.g., PCI) for detailed visibility.

Solution: Centralized Security Platform

On-Demand Security Coverage:

- Included SAST, Git posture, secret scans, license scans, build scans, artifact scans, IAC scans, container scans, and DAST.
- Scanned infrastructure as code and cloud infrastructure for misconfigurations.

AI-Driven Insights:

- Integrated AI/ML (e.g., ChatGPT) for vulnerability insights and real-time analysis.
- Automated aggregation and prioritization of vulnerabilities.

Automated Compliance Management:

- Auto-generated compliance scorecards (e.g., PCI).
- Policy tagging for easy identification of relevant compliance measures.

Developer Training & Knowledge Transfer:

- Conducted training sessions to reduce the knowledge gap between developers and security teams.
- Provided tools to help developers address vulnerabilities during development.

Centralized and Scalable Platform:

- Eliminated the need to install tools repeatedly for new applications.
- Provided detailed visibility with Role-Based Access Controls (RBAC).

Results

Cost Savings Achieved:

- Early detection and resolution of vulnerabilities saved $5,000 per critical vulnerability.
- With a developer base of over 50,000 and 1-2 new applications fortnightly, annual savings exceeded $1.3M.

Productivity Gains:

- Automation reduced manual efforts for security teams, saving approximately 20,000 hours annually.
- Developers resolved vulnerabilities 30% faster on average.

Enhanced Compliance:

- Automated compliance checks and scorecards reduced audit preparation time by 40%.
- Achieved seamless compliance with internal and external requirements.

Improved Scalability:

- On-demand security tools enabled scalability across multiple teams and projects.
- Time saved in provisioning tools accelerated project timelines by 25%.

Strengthened Security Posture:

- Real-time insights and AI-driven prioritization improved vulnerability management.
- The centralized platform ensured comprehensive coverage and reduced risk exposure.

Net Annual ROI:

- **Savings: $1.8M**/year.
- **Investment: $200,000**/year.
- **ROI: 800%** within the first year, with consistent returns in subsequent years.

Conclusion

The implementation of a centralized security platform enabled the organization to significantly reduce vulnerability costs, enhance team productivity, and streamline compliance processes. The solution not only addressed existing pain points but also provided a scalable and future-proof approach to cybersecurity, aligning with the organization's goals of innovation and operational excellence.

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY