Ensuring SAP Code Security Excellence: Festo's Success Story

Overview:

Festo, a leading name in the automation industry, is synonymous with innovation and excellence. This German powerhouse delivers high-tech pneumatic and electrical control systems for factory and process automation, with designs often inspired by nature. Since its inception in 1925 in Esslingen, Festo has grown to a global presence with over 20,000 employees in 61 countries, all while staying true to its engineering roots.

As one of the earliest SAP adopters, Festo has built its success on the ability to innovate SAP technology, continually mastering and extending SAP software to create a highly efficient digital infrastructure. Protecting their intellectual property and ensuring operations remain available are vital, making SAP security a strategic priority.

"NO MONKEY ADVISORY delivered outstanding guidance throughout our project, masterfully managing our tight schedule and exceeding our expectations."

Volodymyr Vashchenko
ABAP Lead Developer
at Festo SE & Co. KG

Challenge:

Festo, like many long-standing SAP customers, faces the complex challenge of modernizing thousands of legacy interfaces and applications while transitioning to the cloud. Ensuring security throughout this transformation is critical. The goal is twofold: to guarantee that new developments are free from security flaws and to apply a risk-oriented approach to remediating vulnerabilities in legacy systems. The solution lies in empowering SAP developers to rapidly identify and address security issues without disrupting their agile development practices, in line with the "stay clean & get clean" philosophy.

Approach & Solutions:

To address Festo's security challenges, we implemented a comprehensive approach focused on four key areas:

1) Custom Code Security Assessment:
Conduct a thorough audit of the custom code within Festo's core SAP ERP system to identify any security weaknesses or vulnerabilities. This assessment was a first step to ensure those custom parts were secure before moving forward with other improvements.

2) Revamping Software Release and Quality Assurance (QA) Processes:
Lead a complete overhaul of Festo's software release and quality assurance processes. This involved updating policies, guidelines, and implementing new quality gates, which developers and QA teams now follow to maintain high security and quality standards throughout the software development lifecycle. These changes made Festo's software development and release processes more secure and reliable.

3) Establishing a 'Get-Clean & Stay-Clean' Roadmap:
Develop a clear roadmap that focused on both remediating existing vulnerabilities (getting clean) and maintaining security in ongoing development (staying clean). This included upskilling Festo's software developers and testers in advanced security practices, ensuring they have the knowledge and tools needed to sustain a high level of security in the long term.

4) Stakeholder Management and Risk Awareness:
Engage senior IT leaders at Festo to make them aware of the company's security risks, particularly the potential consequences of unaddressed ABAP vulnerabilities. By clearly outlining these risks and the benefits of remediation, we ensured that Festo's leadership was fully informed and supportive of the necessary security measures. This step was crucial in securing the commitment and resources needed to successfully implement and sustain the security enhancements.

This holistic strategy allowed for early developer feedback, ensuring smooth implementation of new tools and processes. All decisions were data-driven, providing budget owners with clear evidence of project efficiency and benefits.

Results:

Collaborating closely with Volodymyr and his team, NO MONKEY ADVISORY conducted a thorough security review of Festo's software development practices. This included code analysis, assessing the need for additional tooling, and developing ABAP code security guidelines and principles.

In addition to the technical measures, we effectively communicated the security risks to senior IT leaders, emphasizing the importance of addressing ABAP vulnerabilities to avoid potential operational disruptions and data breaches. This proactive stakeholder management ensured alignment at all levels, from developers to executives, fostering a security-first mindset across the organization.

The result was a robust set of process definitions and policies that established security quality gates within the SAP development and software procurement processes. These measures ensured that no new vulnerabilities were introduced—a key component of the "stay-clean" strategy.

Simultaneously, the "get-clean" strategy focused on actively remediating vulnerabilities in legacy code. This strategy was developed in close collaboration with Festo's lead developers, including effort estimation and a process that combined risk-based ad-hoc remediation with mid-term clean-up projects and the retirement of obsolete implementations.

As a result, Festo was able to enhance its SAP development practices, ensuring robust security while maintaining agile development—a critical balance for ongoing innovation in today's digital landscape.