

Addressing Business Challenges for a Crypto Trading Platform with DevSecOps Integration

Customer Overview

A mid-to-large size, highly regulated crypto trading platform operating globally. The company facilitates cryptocurrency exchanges, offering a range of services to users, including secure transactions, trading, and portfolio management. The company is committed to maintaining high operational efficiency while adhering to stringent security and compliance standards. Given the nature of the industry, the platform faces significant challenges in ensuring rapid releases, security, compliance, and operational scalability.

Challenges

Time Spent on Diagnosis and Manual Effort:

Teams are spending excessive amounts of time on diagnosing issues manually, which hinders efficiency. There is a need to reduce dependency on manual scripting to free up resources for more critical tasks.

Security Controls Across SDLC:

The company wants to implement security controls throughout the Software Development Life Cycle (SDLC) to ensure comprehensive protection at every stage of development.

Audit Report Preparation:

Gathering proofs for audit reports is time-consuming and cumbersome. The company wants a more automated process for compliance reporting to minimize manual efforts and improve efficiency.

Shift-Left Approach:

The company aims to reduce the operational costs associated with security by adopting a Shift-Left security approach, enabling earlier detection of vulnerabilities and issues during development.

Improving Efficiency and Reducing Operational Costs:

The company is looking for ways to enhance operational efficiency, streamline workflows, and reduce the cost of operations through automation.

Hyperautomation with DevSecOps:

The company wants to complement its automation strategy by integrating DevSecOps practices to automate security processes and eliminate manual effort where possible.

Unified Dashboard with RBAC:

The company requires a unified platform to provide a comprehensive view of security and operations across multiple teams, with role-based access control (RBAC) for secure and specific visibility.

Multi-Application Support:

The platform must be able to cover multiple types of applications, including Java, Python, and mobile apps, to meet the company's diverse needs.

Bridging Gaps in Existing Security Tools:

The company intends to continue using its existing scanners but needs a solution that integrates seamlessly with these tools and fills gaps in security coverage, such as artifact scans, container scans, and dynamic application security testing (DAST).



Solution: Comprehensive DevSecOps Platform

To address these challenges, the company implemented a DevSecOps platform that integrates security controls, automation, and reporting capabilities, with the following key features:



Unified Security Dashboard with RBAC:

A centralized dashboard that provides end-to-end visibility of security, operations, and compliance activities. RBAC ensures that users have tailored access to relevant data based on their role, enhancing security and operational efficiency.



Security Controls Across SDLC:

Integrated security checks at each stage of the SDLC, from code analysis to build and deployment, ensuring a comprehensive security posture for every application.



Automated Security and Compliance Reports:

The platform automatically generates audit-ready reports and proofs for compliance, reducing manual efforts by 80%. This feature enables quicker responses during audits and enhances the company's audit readiness.



Shift-Left Security Implementation:

Early detection and remediation of vulnerabilities were integrated into the development process, allowing issues to be fixed before they became costly problems in later stages of development.



Automated Artifact Scans and Container Security:

The platform provides automated artifact scanning, container scanning, and DAST to ensure that security controls are applied across all types of applications (Java, Python, mobile apps) and environments.



Hyperautomation for DevSecOps:

By automating security testing, vulnerability management, and compliance activities, the platform enables a seamless DevSecOps workflow that significantly reduces the time spent on manual processes and ensures continuous security coverage.



Integration with Existing Tools:

The platform was designed to integrate with the company's existing security tools, bridging gaps in coverage while maintaining the tools already in use.



Scalable Security and Compliance Controls:

The platform allows for scalable deployments and ensures that compliance and security controls are enforced at every stage of the CI/CD pipeline, regardless of the scale of releases or deployments.



Improved Release Velocity and Efficiency:

By automating security and compliance checks, the platform enabled faster, on-demand deployments, aligning with the business's need for quicker releases without compromising on security or compliance.







Benefits



Reduced Operational Costs:

Automation significantly reduced the need for manual scripting and diagnosis, leading to a 40% reduction in operational costs related to security and compliance activities.




-  **Increased Security Posture:**
Security controls integrated across the SDLC helped detect and remediate vulnerabilities earlier, enhancing the company's security posture and reducing production issues.
-  **Faster and More Reliable Software Releases:**
With automated verification, testing, and security checks, the company improved software release velocity and reduced the number of production issues by 30%.
-  **Streamlined Audit and Compliance Processes:**
Automated audit reporting and compliance checks decreased the time spent gathering proof points for audits by 70%, ensuring that the company remains compliant without the manual effort.
-  **Shift-Left Security Implementation:**
Early vulnerability detection and remediation reduced the operational cost of fixing issues in later stages of development, leading to more cost-effective operations.
-  **Enhanced Scalability:**
The platform's ability to scale with the company's growing needs allowed the team to handle increased release velocity and volume without sacrificing security or compliance.
-  **Unified Visibility for Multiple Teams:**
The RBAC-driven unified dashboard provided real-time insights into security, compliance, and operations, enabling different teams to access relevant information based on their roles.

Net Annual ROI:

 **Savings:** \$1.2M/year.

 **Investment:** \$95,000/year.

 **ROI: 1,100% within the first year**, with consistent improvements in subsequent years as the platform continues to optimize workflows and security practices.

Conclusion

By implementing a comprehensive DevSecOps platform, the crypto trading platform was able to streamline its security, compliance, and operational workflows, resulting in significant cost savings, improved efficiency, and a stronger security posture. The platform not only automated critical tasks but also provided unified visibility across multiple teams, enabling faster software releases and reducing the overall operational burden. This approach empowered the company to maintain high security and compliance standards while keeping pace with the growing demands of the crypto trading industry.

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](http://WWW.OPSMX.COM/SECURE_SOFTWARE_DELIVERY)