iTMethods.

10 MISTAKES WHEN IMPLEMENTING SECURE SOFTWARE SUPPLY CHAIN SOLUTION

1 Not Focusing on Developer Productivity

Developer productivity improves with right security supply chain software. Replace insecure workflow elements to minimize risk to applications post-deployment and changes to vulnerable opensource components.

2 Not Integrating with DevOps Tooling

Ensure that software supply chain security is fully integrated into an organization's development environment, rather than just being used as another standalone application.

3 Not Improving Speed-to-Market for Secure Applications

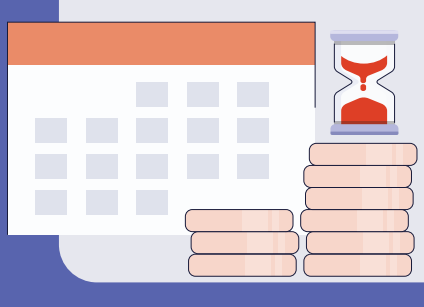
Improvements in secure software supply chains allow teams to produce secure applications faster as they speed up development rework and common security gates prior to production.

4 Not Staying on Top of License Information

Check any version releases, patches, and license issues to protect organization from new vulnerabilities and avoid accidentally misusing an open-source software.

5 Not Blocking Undesirable Components

Use vulnerability scanners to identify undesirable open-source components and block them from entering your development lifecycle.



6 Not Planning Across Silos

Update security, development, and DevOps teams about the new processes and measures required for open-source security and license management.

7 Not Focusing on Customized Policy Enforcements Across the SLDC

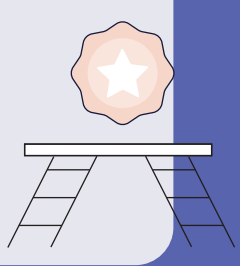
Establish custom standards on components across a variety of application types. Decide whether to enforce stricter standards on components with licenses that are more permissive, or vice versa.

8 Not Having a Strategy & Goals Across DevOps & AppSec Teams

Implement a specific software supply chain strategy and set clear goals which include addressing the security concerns of software development teams, security teams and other stakeholders.

9 Not Starting as Soon as Possible

Components need to be identified and blocked from development environments if they are found to be unsafe, so it's important not to wait too long before beginning the process.



10 Not running your tools on a managed DevOps SaaS Platform

The iTMethods Managed DevOps SaaS Platform addresses all of these challenges for global enterprises, enabling them to integrate, migrate, and modernize their multi-vendor, multi-cloud DevOps environments.

iTMethods.

www.itmethods.com
innovate@itmethods.com

Sources: Sonatype