DevSecOps

The Concept of DevSecOps

DevSecOps or DevOps security is about introducing security earlier in the life cycle of application development (a.k.a shift-left), thus minimizing the impact of vulnerabilities and bringing security closer to development team.

Why

By embracing shift-left mentality, DevSecOps encourages organizations to bridge the gap that often exists between development and security teams to the point where many of the security processes are automated and are effectively handled by the development team.

DevSecOps Practices

This section covers different tools, frameworks and resources allowing introduction of DevSecOps best practices to your project at early stages of development. Topics covered:

1. Credential Scanning - automatically inspecting a project to ensure that no secrets are included in the project's source code.
2. Secrets Rotation - automated process by which the secret, used by the application, is refreshed and replaced by a new secret.
3. Static Code Analysis - analyze source code or compiled versions of code to help find security flaws.
4. Penetration Testing - a simulated attack against your application to check for exploitable vulnerabilities.
5. Container Dependencies Scanning - search for vulnerabilities in container operating systems, language packages and application dependencies.
6. Evaluation of Open Source Libraries - make it harder to apply open source supply chain attacks by evaluating the libraries you use.

Last update: August 22, 2024