ONE PAGE SUMMARY

IT & Software › CI/CD › Pipeline Security

Introduction to Pipeline Security

Secure your CI/CD pipelines to protect software delivery.

DEFINITION

> Pipeline security involves safeguarding the continuous integration and delivery processes from vulnerabilities and threats. It ensures that code is securely built, tested, and deployed.

KEY CONCEPTS

Vulnerability Scanning

Regularly checking code and dependencies for known security issues.

Access Control

Managing who can access the pipeline to prevent unauthorized changes.

Secrets Management

Safeguarding sensitive information like API keys and passwords within the pipeline.

Audit Trails

Maintaining logs of all actions taken in the pipeline for accountability and investigation.

Automated Testing

Implementing tests that check for security flaws during the build process.

EXAMPLES

→ Using tools like Snyk for vulnerability scanning in dependencies.

→ Implementing role-based access control to limit pipeline access.

→ Storing API keys in a secure vault instead of hardcoding them.

MEMORY TIPS

★ Remember 'VASE' for Vulnerability, Access, Secrets, and Audit.

★ Think of 'TAP' for Testing, Access, and Protection.

★ Use the phrase 'Secure the Pipeline' to recall key security practices.

COMMON MISTAKES

✗ Neglecting to update dependencies regularly.

✗ Overlooking the importance of access controls.

✗ Failing to monitor and review audit logs.

QUICK RECAP

Pipeline security is essential for protecting the software delivery process. Key practices include vulnerability scanning, access control, and automated testing to ensure a secure CI/CD environment.