CSP108 - SUPPLY CHAIN SECURITY

Course Learning Objectives

This course has been designed to improve the security of your software supply chain. We'll start by discussing core concepts about supply chains and the attacks that target them. We'll then look at the importance of identifying and documenting every part of your supply chain. Next, we'll explore supply chain vulnerabilities in the open source software you use. Then we'll see how you can protect the processes that take your application from the source code to a release build. And finally, we'll look at the parts of the software supply chain that stretch beyond your business and out to its suppliers.

Description

Supply Chain Security is a course for Software Developers and Managers. It focuses on discussing the vulnerabilities throughout the supply chain, from third-party software to mitigating risk with suppliers. This course provides best practices you can apply to defend against the security vulnerabilities you are likely to encounter as you build out your supply chain.

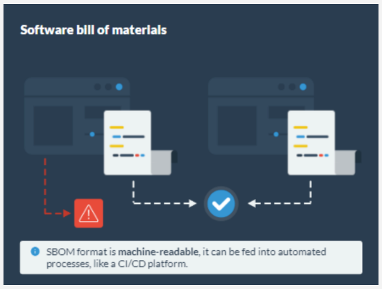
Audience

Developers
Managers

Time Required

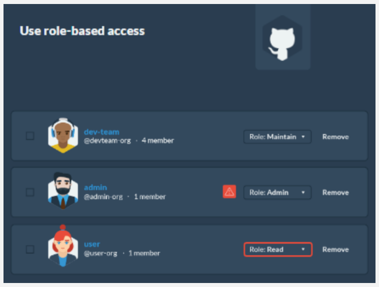
Tailored learning - 75 minutes total (approx.)

What is a software supply chain?



Software bill of materials

SBOM format is **machine-readable**, it can be fed into automated processes, like a CI/CD platform.



Use role-based access

dev-team
@devteam-org · 4 member
Role: Maintain ▾
Remove

admin
@admin-org · 1 member
Role: Admin ▾
Remove

user
@user-org · 1 member
Role: Read ▾
Remove

CSP108 - SUPPLY CHAIN SECURITY

Course Outline

1. Understanding Supply Chain Risks

- What is a software supply chain?
- Supply chain attacks
- Supply chain legislation
- Supply chain risk

2. Supply Chain Mapping

- Supply chain attacks
- Mapping your supply chain
- Best practices
- Third-party code
- Code ingestion
- Best practices
- Software bill of materials
- SBOM example
- Creating an SBOM
- SBOM exercise
- Using SBOMs
- Other tools
- Best practices
- Other SBOMs

3. Securing Open Source Dependencies

- The scope of the problem
- The risks of OSS
- Bottom line
- Dependency vetting
- Dependency count
- Best practices
- Knowledge check
- Dependency confusion
- Typosquatting example
- Best practices
- Open source licensing
- Reminder
- OSS license types
- Other
- Best practices

4. Hardening the Dev and Build Environments

- Hardening the supply chain
- Protecting the development environment
- Use role-based access
- Regularly review repository access
- Use two-person review
- Require 2FA
- Use approved images
- Hardcoded secrets
- Conclusion
- Software provenance
- Using provenance
- Codecov attack example
- Provenance and SBOM
- SLSA
- Active detection
- Intrusion monitoring
- Examples of intrusion monitoring
- Monitoring systems
- Reminder

5. Working with Suppliers

- What is a supplier?
- Know your suppliers
- Security posture
- Regulatory compliance
- Risk exposure
- Security track record
- Financial stability
- Techniques
- Knowledge check
- Supplier contracts
- Contract example
- Service level agreement
- SLA requirements
- The issue
- Code escrow
- Dispute
- Example
- Intellectual property
- Patents, Copyright, Trade secrets, Trademarks

Security Compass