Development, Security, and Operations (DevSecOps)

Go up to Terms and Definitions

Discussion

Development, Security, and Operations (DevSecOps) integrates security practices, responsibilities, and evidence-producing activities throughout Development and Operations (DevOps) workflows.

DevSecOps treats security as a continuous lifecycle responsibility rather than as a separate review performed only after development or immediately before deployment.

DevSecOps commonly integrates security activities into:

- Requirements definition
- Architecture and design
- Source-code management
- Dependency management
- Build operations
- Artifact creation
- Automated testing
- Configuration evaluation
- Vulnerability analysis
- Compliance evaluation
- Deployment
- Runtime monitoring
- Incident response
- Maintenance
- Retirement

DevSecOps workflows can generate and preserve:

- Test results
- Compliance Findings
- Vulnerability findings
- Software Bills of Materials
- Digital Signatures
- Attestations
- Provenance
- Traceability
- Compliance Evidence
- Deployment records
- Validation results

Within Crucible documentation, DevSecOps provides the lifecycle context for automated build, security evaluation, compliance assessment, controlled deployment, validation, Evidence generation,

and transfer into Connected or Disconnected Environments.

Definition

approach that integrates security practices, responsibilities, controls, and evidence-producing activities throughout development and operational workflows

Source

Adapted from:

- National Institute of Standards and Technology Special Publication 800-204C
- National Institute of Standards and Technology Special Publication 800-204D
- National Institute of Standards and Technology Special Publication 800-215
- National Institute of Standards and Technology Cybersecurity Practice Guide 1800-44

Note

The term **DevSecOps** combines **Development**, **Security**, and **Operations**.

DevSecOps extends DevOps by integrating security throughout the lifecycle rather than treating security as an isolated final-stage activity.

DevSecOps does not mean that every security decision is fully automated. Responsible actors retain responsibility for activities such as risk acceptance, Security Control assessment, and Authorization to Operate (ATO) decisions.

A CI/CD Pipeline can implement DevSecOps activities, but the existence of a pipeline alone does not establish DevSecOps. The workflow must integrate security activities, results, responsibilities, and feedback into development and operations.

Example

A repository change initiates a CI/CD Pipeline that builds an Artifact, evaluates dependencies, performs security and compliance checks, records Compliance Findings, generates Provenance and Evidence, signs the resulting Artifact, deploys it to an authorized environment, and validates the deployment.
