DevSecOps

A Checklist to Evaluate Your System's Readiness for DevSecOps

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

DevSecOps provides continuous visibility into a system's security posture, delivering strengthened security and streamlined operations.

DevSecOps Goals

- Accelerate the development process with simplified security reviews.
- Maintain consistent security levels, Sprint-to-Sprint, by enabling developers and ISSOs to verify security and compliance early and often during each Sprint.

Are you ready for DevSecOps?

Automation and standardization of security data is essential for DevSecOps. Size-up your readiness with The Security Checklist.

07022020

DevSecOps: The Security Checklist
Pipeline Automation Evaluation

Prerequisite: DevSecOps requires a DevOps environment with a fully automated CI/CD pipeline with no manual user interaction, beyond committing software into the repository.

- [ ] **Security Configuration Settings**

  The pipeline automatically validates each code build's security configuration setting compliance, at each create and configure, including underlying application stack components.

  Evaluates supporting cloud, network, operating system, database, app-server and web-server components' configurations against STIGs, CIS Benchmarks and CCE compliance.

- [ ] **Security Vulnerability Levels**

  The pipeline automatically validates, at each create and configure for each build, the security vulnerability levels of underlying application stack components.

  Assesses software patch levels and CVE compliance.

- [ ] **Least Functionality**

  The pipeline automatically validates, at each create and configure for each build, least functionality of underlying application stack components.

  Limits services, ports and protocols for application stack to function, compliant with NIST SP 800-53 CM-7 Least Functionality requirements.

- [ ] **Static Code Analysis**

  The pipeline automatically performs, at each commit, static code analysis against CMS application source code.

  Analyze at least 95% of the lines of code (95% code coverage) and perform linting checks for security issues against, at a minimum, SANS Top 25 CWE compliance.

- [ ] **Dynamic Code Analysis**

  The pipeline automatically performs, at each create and configure for each build, dynamic code analysis against CMS application compiled/running code

  Assesses code security against, at a minimum, OWASP Top 10 CWE.

- [ ] **Standardized Reporting Format**

  The pipeline automatically generates all of the above security data in the CMS ISPG standard "Heimdall Data Format" for machine-readability, assigning severity levels to each security test result (high, medium, low) and mapping all security test results to NIST SP 800-53 security controls.

  Ensure compliance with JSON output reporter schema including, at a minimum, these labels: title, description, check text, fix text, relevant NIST SP 800-53 tags and impact level for each defect.

DevSecOps: The Security Checklist
Operations Evaluation

- [ ] **Change Tracking**
  The pipeline automatically tracks and compares planned versus executed changes, to prove that planned changes, and *only* the planned changes, were implemented during a Sprint.

- [ ] **Security Resolution Assurance**
  Developers and ISSOs certify that all high security defects and 90% of all medium or low security defects are resolved before allowing affected functionality to be deployed to production.

- [ ] **Manage Security Debt**
  Developers and ISSOs assure that no security defect may carry-over unresolved through more than 2 Sprints.

- [ ] **Minimize Unplanned Changes**
  Unplanned (unauthorized) changes, for any Sprint, are less than 5% of planned (authorized) changes.

Ready to Get Started?

Contact saf@cms.hhs.gov with any questions, or to make a plan.

Glossary and Acronyms

ATO - Authority to Operate
CI - Continuous Integration
CD - Continuous Deployment
CIS - Center for Internet Security
CCE - Common Configuration Enumeration
CWE - Common Weakness Enumeration
CM-7 - Configuration Management (NIST SP 800-53 Control 7 for Least Functionality)
CVE - Common Vulnerabilities and Exposures
ISPG - Information Security and Privacy Group
ISSO - Information System Security Officer
NIST - National Institute of Standards and Technology
OWASP - Open Web Application Security Project
STIG - Security Technical Implementation Guide