DevSecOps Best Practices and Considerations

Applied Resilience for Mission Systems

Darby Mitchell

Planning	Development	Continuous Integration	Provision	Validation	Deployment	Operations
Customer Involvement	Architecture-First Approach	Automated Build	Base Image Provenance	Interface Validation	Deployment Orchestration	Continuous Monitoring
Issue Tracking	Version Control	Automated Unit Testing	Infrastructure Automation	Integration Testing	Small Releases	Practice Recovery
Threat Modeling	Coding Standards	Static Analysis	Instance Provisioning	Compliance/ Accreditation	Canary Deployments	Upstream Feedback
Release Planning	Dependency Analysis	Code Quality Metrics	Credential Management	Chaos Engineering	Rolling Updates	
Sprint Planning	Observability	Release Packaging		Dynamic Analysis	Instant Rollback	
Sustainable Velocity	Test-Driven Design			Vulnerability Scanning	Promotional Model	
	Peer Review			Deployment Validation		

DevSecOps Methods[1]

This conceptual model serves as a guide for which methods and practices to consider when applying DevSecOps methodology to software-intensive DoD systems. Successfully employing these methods requires a commitment to embrace modern software development culture and philosophy. Attempting to apply these methods in the absence of such a change in culture is unlikely to succeed. It is also important to tailor these practices to the specific program needs, as not all practices are equally appropriate for all programs. However, we believe that all programs could benefit from using this framework to reason about their employment of DevSecOps methodology.

[1] Informed by DoD DevSecOps Initiative: http://dccscr.dsop.io

For more information contact:
ARMS@LL.MIT.EDU

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the United States Air Force under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.

LINCOLN LABORATORY
Massachusetts Institute of Technology