VICTORY SMILES UPON THOSE WHO ANTICIPATE THE CHANGE IN THE CHARACTER OF WAR

Guilio Douhet
• Software shared between F-22 & F-35
• Rapid updates
• Continuous innovation
• New software sources

enabled through
DevSecOps
DOD Software Modernization Strategy & Implementation Plan
Joint Warfighting Cloud Capability (JWCC) – DoD’s multi-vendor, enterprise-wide acquisition vehicle

Joint Operational Edge (JOE) Cloud: an integrated mesh of large form factor edge cloud platforms, installed on-premises at DOD locations, to deliver commercial cloud services

Software Defined Compute
Unified Multi-Cloud Ecosystem
Resilient, Localized Data Processing
Strengthen Security Posture
Future-proofed Infrastructure
50+ DoD Software Factories and Growing

- DevSecOps Platforms
- Security First
- Shared Services
- Collaborative Environment
- Scalable Infrastructure
- Continuous Integration & Deployment
- Talent Development
Software Acquisition Pathway 5000.87
Continuous Authorization (cATO)
Workforce Development

Agile Acquisition Approach
Policy Evolution
User-Centered Design
Modernizing Risk Management
Defensive Cyber Operations
Increasing threats to software supply chain

Threat actors incorporating attacks on downstream functions

Scale of impact hard to confine using traditional methods

Securing software development

Accelerating attack detection and remediation

Rapid response to zero-day attacks

Accelerate delivery of system patches and updates

Respond to continuously changing threat environment

Coordination across all stakeholders (cyber defenders, AO, sysadmins, developers, PM, etc)
Increasing threats to software supply chain

- Threat actors incorporating attacks on downstream functions
- Scale of impact hard to confine using traditional methods
- Securing software development

Accelerating attack detection and remediation

- Rapid response to zero-day attacks
- Accelerate delivery of system patches and updates

Respond to continuously changing threat environment

- Coordination across all stakeholders (cyber defenders, AO, sys admins, developers, PM, ...)


Securing the DevSecOps Journey

- Configuration drift detection
- Secrets leak detection
- Patch management & remediation
- Vulnerability management
- Container security
- ICAM & Zero Trust
- API Protection
- Cloud Workload Protection
- Backup & Recovery

Operate & Monitor
- SBOM
- Code signing & pipeline integrity
- Fuzz Testing
- Penetration Testing
- Policy-as-Code
- Artifact repository

Plan & Develop
- Secrets scanning
- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dependency Checking
- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)
- Runtime Application Self-Protection (RASP)
- Threat modeling
- Security Training
- Secure coding standards
- Source code protection
- Infrastructure as Code Scanning
- Memory Safe Programming Languages
- Trusted Component Registry & Typo-squatting protections

Supply Chain
- Code Provenance
- Composition Analysis & Integrity Checks
- Dependency Analysis
- Technical Debt
- Supply Chain Fragility
- Disclosed Vulnerabilities
- Third Party Assessments
- SSDF Attestation

Supply Chain
Securing the DevSecOps Journey

Supply Chain
- Code Provenance
- Composition Analysis & Integrity Checks
- Dependency Analysis
- Technical Debt
- Supply Chain Fragility
- Disclosed Vulnerabilities
- Third Party Assessments
- SSDF Attestation
Securing the DevSecOps Journey

Plan & Develop

- Threat modeling
- Security Training
- Secure coding standards
- Source code protection
- Infrastructure as Code Scanning
- Memory Safe Programming Languages
- Trusted Component Registry & Typo-squatting protections
Securing the DevSecOps Journey

Testing

- Secrets scanning
- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dependency Checking
- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)
- Runtime Application Self-Protection (RASP)
Securing the DevSecOps Journey

Supply Chain
- Code Provenance
- Composition Analysis & Integrity Checks
- Dependency Analysis
- Technical Debt
- Supply Chain Fragility
- Disclosed Vulnerabilities
- Third Party Assessments
- SSDF Attestation

Release
- SBOM
- Code signing & pipeline integrity
- Fuzz Testing
- Penetration Testing
- Policy-as-Code
- Artifact repository
Securing the DevSecOps Journey

Operate & Monitor
- Configuration drift detection
- Secrets leak detection
- Patch management & remediation
- Vulnerability management
- Container security
- ICAM & Zero Trust
- API Protection
- Cloud Workload Protection
- Backup & Recovery
Securing the DevSecOps Journey
The #1 skill I want is the ability to adapt. Adaptability wins - not the one who comes up with the magic thing.

Gen Joe Rainey, Commander US Army Futures Command
Questions