CMU SEI is a DoD R&D Federally Funded Research and Development Center

Our mission: Engineering and securing software

Established in 1984 at Carnegie Mellon University

~700 employees

Offices in Pittsburgh and DC, with locations near customer facilities in MA, MD, TX, and CA

~$145M in annual funding (~$20M USD(R&E) 6.2 and 6.3 Line funding)
Implementing a Secure Development Lifecycle
Implementing a Secure Development Lifecycle

Mission Risk Diagnostic;
Threat Modeling;
SQUARE;
Security Engineering
Risk Analysis

Mission Thread
Threat Analysis
Abuse Cases
Architecture and Design Principles
Coding Rules and Guidelines
Testing, Validation and Verification
Monitoring
Breach Awareness

Requirements and Acquisition
Engineering and Development
Deployment and Operations

Sustainment
Implementing a Secure Development Lifecycle

Requirements and Acquisition

- Mission Risk Diagnostic;
- Threat Modeling;
- SQUARE;
- Security Engineering Risk Analysis

Engineering and Development

- Abuse Cases
- Architecture and Design Principles
- Coding Rules and Guidelines

Deployment and Operations

- Testing, Validation and Verification
- Monitoring
- Breach Awareness

Sustainment

- Mission Risk Diagnostic;
- Security Design Assurance for Cyberphysical Systems;
- Blockchain
Implementing a Secure Development Lifecycle

Mission Risk Diagnostic; Threat Modeling; SQUARE; Security Engineering Risk Analysis

Architecture Analysis & Design Language (AADL); Security Design Assurance for Cyberphysical Systems; Blockchain

Secure Coding; SCALe; Language Design; Code Evaluation; Supply Chain (SPDO); Pen Testing; Fuzz Testing (BFF); Red Team
Implementing a Secure Development Lifecycle

Requirements and Acquisition

Mission Risk Diagnostic; Threat Modeling; SQUARE; Security Engineering Risk Analysis

Architecture Analysis & Design Language (AADL); Security Design Assurance for Cyberphysical Systems; Blockchain

Deployment and Operations

Testing, Validation and Verification

Monitoring

Breach Awareness

Coding Rules and Guidelines

Secure Coding; SCALe; Language Design; Code Evaluation; Supply Chain (SPDO); Pen Testing; Fuzz Testing (BFF); Red Team

Moving Defense; Forensics;

Vulnerability Analysis; Simulation

Disclosure

Sustainment

Mission Thread

Threat Analysis

Abuse Cases

Architecture and Design Principles

Engineering and Development
Implementing a Secure Development Lifecycle

Software Assurance Framework (SAF)

Requirements and Acquisition
- Mission Risk Diagnostic
- Threat Modeling
- SQUARE
- Security Engineering Risk Analysis

Engineering and Development
- Architecture Analysis
- Architecture and Design Language (AADL)
- Security Design Assurance for Cyberphysical Systems
- Blockchain

Deployment and Operations
- Secure Coding
- SCALe
- Language Design
- Code Evaluation
- Supply Chain (SPDO)
- Pen Testing
- Fuzz Testing (BFF)
- Red Team

Sustainment
- Monitoring
- Breach Awareness
- Moving Defense
- Forensics
- Vulnerability Analysis
- Disclosure
- Simulation

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution
Implementing a Secure Development Lifecycle

Sustainment

Engineering and Development

Requirements and Acquisition

Deployment and Operations

Mission Risk Diagnostic; Threat Modeling; SQUARE; Security Engineering Risk Analysis

Architecture Analysis & Design Language (AADL); Security Design Assurance for Cyberphysical Systems; Blockchain

Secure Coding; SCALe; Language Design; Code Evaluation; Supply Chain (SPDO); Pen Testing; Fuzz Testing (BFF); Red Team

Moving Defense; Forensics; Vulnerability Analysis; Disclosure

Software Assurance Framework (SAF); Secure Agile/Team Software Process; SecDevOps

- Mission Thread
- Threat Analysis
- Abuse Cases
- Architecture and Design Principles
- Coding Rules and Guidelines
- Testing, Validation and Verification
- Monitoring
- Breach Awareness
Implementing a Secure Development Lifecycle

Mission Risk Diagnostic; Threat Modeling; SQUARE; Security Engineering Risk Analysis

Architecture Analysis & Design Language (AADL); Security Design Assurance for Cyberphysical Systems; Blockchain

Secure Coding; SCALe; Language Design; Code Evaluation; Supply Chain (SPDO); Pen Testing; Fuzz Testing (BFF); Red Team

Moving Defense; Forensics; Vulnerability Analysis; Disclosure

Software Assurance Framework (SAF); Secure Agile/Team Software Process; SecDevOps; Training
Contact Information

Mark Sherman
(412) 268-9223
mssherman@sei.cmu.edu
info@sei.cmu.edu

Web Resources (CERT/SEI)
http://www.cert.org/
http://www.sei.cmu.edu/