Secure DevOps: Application Security Principles and Practices is a two-day workshop that focuses on concepts, methodologies, and workflows that have been proven to yield more secure code. In this class, we discuss practices adopted at Microsoft (and other companies) that have facilitated improvements in application security. This workshop takes a hands-on approach to implementing secure design, secure verification, and secure implementation techniques to produce more secure software. Target audience are individuals in a technical role who are involved in building, architcting, testing, and designing secure software. People who manage software development teams and software development processes will also find much of the Security Development Lifecycle and Secure DevOps content helpful. This workshop also has an optional 1-day add-on that discuss the OWASP Top 10.

**WorkshopPLUS**

**Duration:** 2 Day  |  **Focus Area:** Security and Compliance  |  **Level:** 300

**OUTCOMES**

**Skills**

Participants will gain essential knowledge that will aid in designing and developing secure software and improve testing for security. They will also understand top security vulnerabilities and how to protect against them.

**Best Practices**

The knowledge gained in this workshop will help participants understand application security and integrate security into the DevOps pipeline.

**Way Forward**

Apply proven code security patterns to your development pipeline to help you build more secure applications.

**PREREQUISITES**

Participants that have existing experience with employing software development processes will receive the most value from this course.

**Recommended Qualifications**

- Web application development experience preferred but not required
- Familiarity with a development process (Agile, Scrum, CMMI, Waterfall)
- Have a general understanding of your build, test, and deployment activities

**Hardware Requirements**

- An Intel Core-i5-based PC
- 4 GB RAM
- 128 GB HDD
- Windows 7 SP1 or later
- Office 2013 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student
AGENDA

Duration: 2 days
Secure DevOps: Application Security Principles and Practices

START

DAY 1

• Module 1: Evolution to Secure DevOps
• Module 1: Lab
• Module 2: Secure DevOps Principles and Practices
• Module 3: Application Security Principles
• Module 3: Lab
• Module 4: Automating a Secure and Compliant Pipeline
• Module 4: Lab

DAY 2

• Module 5: Threat Modeling Concepts
• Module 5: Lab
• Module 6: Policies and Standards
• Module 7: Intro to Red and Blue Teams
• Module 8 Manual Security Verification
• Module 9: Live Site Operations
• Module 9: Lab
• Module 11: Summary and Closing

End
Module 1: Evolution to Secure DevOps
Lesson 1: Threat Landscape
- Credential theft
- Exploiting common and known vulnerabilities
- Compromising workstations and code
Lesson 2: Privacy and Compliance
- Data Classification
- Privacy
- Compliance
- Risk Management
Lesson 3: Microsoft’s History with App Security
- Trust Worthy Computing and SDL
Lesson 4: Software Development Evolution
- Evolution of Waterfall to Agile to DevOps
- Why DevOps?
- Security challenges with DevOps practices and tools
Lesson 5: Secure DevOps Culture and Mindset Shift
- Delivering security at DevOps speeds
- Assume Breach versus Prevent Breach
- Think like a hacker

Module 2: Secure DevOps Principles and Practices
Lesson 1: Secure DevOps Principles
- Software Compliance and Governance
- Shift left and automate
- Secure the pipeline
- No false positives
- Continuous monitoring and learning
Lesson 2: Secure DevOps Practices
Assume Breach
- Red/Blue teaming
- Monitoring and Learning
- Live site penetration testing
- Block lateral movement
Prevent Breach
- Threat Modeling
- SAST
- DAST
- Stay up-to-date
- Code Reviews
- Secret management
- Secure and compliant pipeline
- Software Composition Analysis and Governance

Lesson 3: Practices Alignment
- Waterfall SDL
- ISO 27034
- FedRAMP SAF
- Agile
- Establishing security requirements
Lesson 4: Organizational Considerations
- Executive Sponsorship
- Roles and responsibilities
Lesson 5: Supporting SDL Practices
- Training
- Define Security Requirements
- Define KPIs
- Incident Response Plan

Module 3: Application Security Principles
Lesson 1: Secure Application Basic Concepts
- Authentication and Authorization
- Proper handling of assets
- Input validation and handling
- Logging and auditing
Lesson 2: Understanding Organizational Threats
- Core pillars of information security
- Security effectiveness
- High Value Assets
- Threat Types
Lesson 3: Secure by Design
- Defense in depth
- Secure defaults
- Least privileged
- Attack surface minimization
- Working with services
- Avoiding security by obscurity
Module 4: Automating a Secure and Compliant Pipeline
Lesson 1: Automated Security Verification
• Static Application Security Testing (SAST)
• Dynamic Application Security Testing (DAST)
• Interactive Application Security Testing (IAST)
Lesson 2: Managing Secrets
• Keep Creds Safe
• Automate Credential Scanning
• Do not Expose Secrets in Transit
Lesson 3: Securing automated deployments
• PAWs
• Approvals
• Pipelines
• Pipeline identities
• Container Security

Module 5: Threat Modeling Concepts
Lesson 1: What is Threat Modeling
• Understand the basics of threat modeling
• Introduction to STRIDE
Lesson 2: Threat Modeling Process
• Utilize STRIDE to evaluate threat types
• Overview of elements of a threat model
• Threat model walkthrough
• Mitigation techniques
Lesson 3: Threat Modeling Tool
• Overview of the Threat Modeling Tool
• TMT usage and techniques
• Analyzing the output of the tool

Module 6: Policy and Standards
Lesson 1: Establishing Secure Standards
• OWASP Top 10
• SDL Practices to find Issues
• Internal Security Standards Policies
• Use of End-to-End Practices
• Cryptographic Standards
• Tool and Programming Standards
• Open Source Policy
• Handling Security Issues
Lesson 2: Understanding Compliance
• Compliance Programs
• Azure Compliance
• Standards you should know
  • GDPR
  • HITRUST
  • HIPAA
  • FedRAMP
  • PCI DSS 3.2.1
  • Cloud Security Alliance CCM
  • FIPS 140-2
  • NIST 800-53
  • ISO 27034
  • SOC
Lesson 3: Threat Modeling for Compliance
• Using Threat Models to help drive compliance
• Using threat models to aid compliance
Module 7: Introduction to Red and Blue Teams
Lesson 1: Defining Red/Blue Team Activities
- Microsoft’s journey with Red and Blue teams
- What we learned
- Best practices when establishing teams
Lesson 2: Kill Chain Analysis
- Recon
- Exploit
- Pivoting
- Act
- Persist
- Attack Path
Lesson 3: Attack Decomposition
- Understanding Impact
- Process the output
- Bug Bars
- Track, metric, and measure
- Threat Model Review
- TTP (Tactics, Techniques, and Procedures)
Lesson 4: Monitoring and risk management
- What’s your monitoring story
- Security Incident Lifecycle
- Establishing Incident response plan
- Managing risk

Module 8: Manual Security Verification
Lesson 1: Requirements and Design Verification
- Establishing a checklist
- Secure Design Reviews
- Establishing the first Security Gate
Lesson 2: Development Phase
- Secure DevOps design reviews
- Manual Security Code Reviews
- Pen Testing
- Final Security Review

Module 9: Live Site Operations
Lesson 1: Continuous monitoring, alerting, logging
- Security Information and Event Management
- OWASP Security Logging Project
- Semantic Logging Application Block
- AppInsights
- Azure Monitor
Lesson 2: Threat Detection
- Understand your threat model
- Environment Configuration Analysis
- Behavioral threat detection
- Intrusion Analysis
- Understanding Alert Fatigue
- Agile Security Patching
- Incident Response Planning

OWASP Top 10 Add On
Overview of the OWASP Top 10
Each threat will be explained, and mitigation examples will be provided. The focus will be on .NET Core, and ASP.NET applications.
- A1:2017 – Injection
- A2:2017 - Broken Authentication
- A3:2017 - Sensitive Data Exposure
- A4:2017 - XML External Entities (XXE)
- A5:2017 - Broken Access Control
- A6:2017 - Security Misconfiguration
- A7:2017 - Cross-Site Scripting (XSS)
- A8:2017 - Insecure Deserialization
- A9:2017 - Using Components with Known Vulnerabilities
- A10:2017 - Insufficient Logging & Monitoring

NEXT STEPS: If you are interested in a session for your organization, contact your Microsoft Account Representative.