

# ***Application Software Assurance Center of Excellence (ASACoE)***

---

## ***Building Assurance Into Software Development Life- Cycle (SDLC)***



***James “Woody” Woodworth  
Operations Chief, ASACoE & Sean Barnum,  
Principal Consultant (Cigital)***



- **SDLC Waterfall Process**
- **How to Build Assurance Throughout SDLC**
  - Gain Knowledge of Secure Coding Practices
  - Gain Knowledge of Tools
  - Use Tools Throughout SDLC
  - Why Use Operational Tools
- **Where to Go to Get Started**



# ***SDLC Waterfall Process***

---



- 1. Requirements Specification**
- 2. Architecture**
- 3. Code**
- 4. Integrate**
- 5. Test and Debug**
- 6. Install**
- 7. Maintain**



# Secure Coding Practices



- **Defensive Programming: Attack and Defense: Developing Secure Code**
  - Common attacks against software
  - Maps attacks to a set of common code-level weaknesses
  - Reviews code bases to find the relevant weaknesses
  - Demonstrates how to remediate vulnerabilities



# *Tool Training*



- **Source Code Analysis Tool Training**
- **Database Analysis Tool Training**
- **Web Application Penetration Tool Training**
- **Central Management Tool Training**
- **Operational Tool Training**



# Tool Usage



## Centralized Project Management (Fortify Manager)

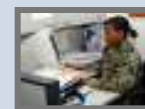
Vulnerability trend analysis and reporting; view multiple projects, all mission areas

### Application Defense (Fortify RTA and AppSec Inc. AppRadar)

Monitor, prevent and report on intrusion attempts against Web-based applications



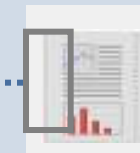
Security Ops Team



Developers

### Source Code Analysis (SCA) (Fortify SCA)

Proactive security with targeted, accurate analysis tuned for low false positives



Security Testers



### Penetration Testing (IBM AppScan and Fortify PTA, AppSec Inc. AppDetective)

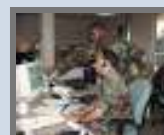
Scripted, controlled external probing of the application's security features

### RunTime Analysis

Black box integration testing and vulnerability analysis



Build Server



Security Leads / Auditors

### Code Auditing (Fortify SCA)

Pre-build security auditing and analysis of application's entire code base



# *Why Use Operational Tools?*

- **Weaknesses Take Time To Fix**
  - Staffing Limitations, Release Cycles, Fundamental Design
- **Protection of Vulnerable Applications and Data**
  - Immediately Provides Significant Risk Mitigation
- **Knowledge of Who Is Attacking Our Applications**
  - Invaluable Forensic Data For Operations and Developers
- **Confidentiality, Integrity, and Availability of Data**
  - Compromised Data Puts the Air Force Mission at Risk

**Secure Data = Warfighter Success!!!**



# *Where to Go to Get Started*



## **Application Software Assurance Center of Excellence (ASACoE)**

**The mission of the Application Software Assurance Center of Excellence (ASACoE) is to foster security into the software development life cycle (SDLC) and software acquisitions through techniques, tools, and education. ASACoE will leverage information technology through the deployment of practices and automated tools to support and improve Air Force software development processes.**



# *Current Training Focus*



- **Class Size – 12 – 20**
- **PMO Courses**
  - **Defensive Programming (1 day)**
  - **Fortify SCA (1 day)**
  - **AppSecInc. AppDetective (1/2 day)**
  - **Fortify 360 and RTA (1/2 day)**
- **Testing Organizations Courses**
  - **Security Testing (1 day)**
  - **IBM Rational AppScan (1 day)**
  - **SCA, AppDetective, 360, & Fortify PTA**
- **Location**
  - **Gunter – 1 week per month**
  - **On-site – Combine multiple program offices if necessary**



# *Multi-perspective Application Risk Assessment*



---

## *Conducted with PMO personnel as mentoring*

- **Scan software using a variety of tools**
  - **Static analysis using Fortify SCA**
  - **Web scanning/pentesting of running software using AppScan**
  - **Data security analysis using AppDetective**
- **Conduct analysis of tool results**
  - **Validate and normalize/align findings**
  - **Characterize findings as risk and prioritize**
- **Identify recommended mitigation approach for findings**



**POCs**



- **Program Manager**
  - Mr. Dan Bartko  
754th ELSG/DOC  
[daniel.bartko@gunter.af.mil](mailto:daniel.bartko@gunter.af.mil)
- **Chief Technology Officer**
  - Major Michael Kleffman  
754th ELSG/DOC  
[michael.kleffman@gunter.af.mil](mailto:michael.kleffman@gunter.af.mil)
- **Operations Chief**
  - James Woodworth  
754th ELSG/DOC  
[james.woodworth@gunter.af.mil](mailto:james.woodworth@gunter.af.mil)



---

# Questions