Software Assurance (SwA) & Application Software Assurance Center of Excellence (ASACoE)

[uh-SAY-co]

Team ASACoE

7 February 2012

What is Software Assurance?

- **Software assurance (SwA) is defined as “the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.**

- **Software is essential to the operation of the DoD’s critical systems. Vulnerabilities in software can jeopardize intellectual property, Warfighter trust, operations and services.**

- **It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or code of software.**

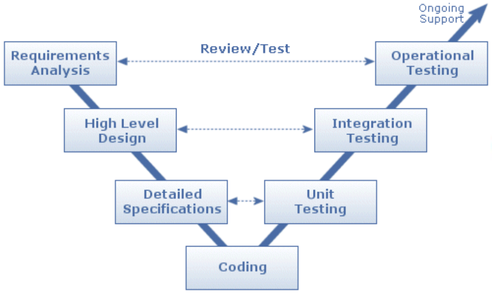
  - **Ensuring the integrity of software is key to protecting the infrastructure from threats and vulnerabilities, and reducing overall risk to cyber attacks.**

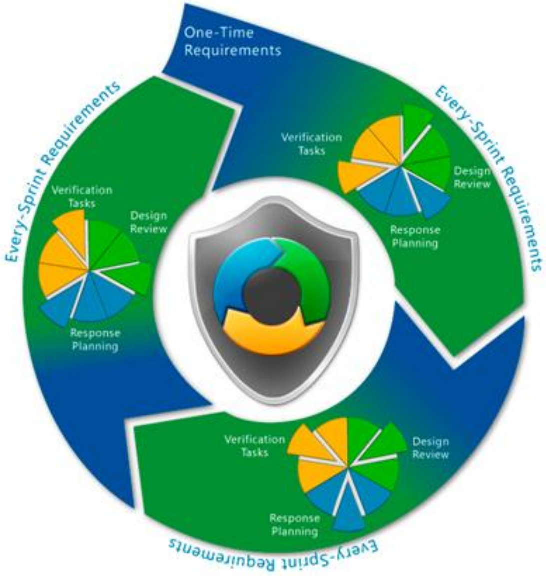
Key Elements for Secure Development

- **Management Support**
- **Developer Training**
- **Professional Career Development**
- **Integration of Software Security Standards into the SDLC**
- **Technical 3rd Party Assessments**

Software Development Life Cycles

- Each SDLC model has its own benefits depending upon your organizational needs.
  - Agile
  - Waterfall
  - Iterative
  - Vee Model
  - Incremental and Iterative Development





- Ultimately, to develop secure software you need to follow a repeatable process.
  - Security needs to be integrated and measured at each SDLC phase.

Why Use Automated Tools?

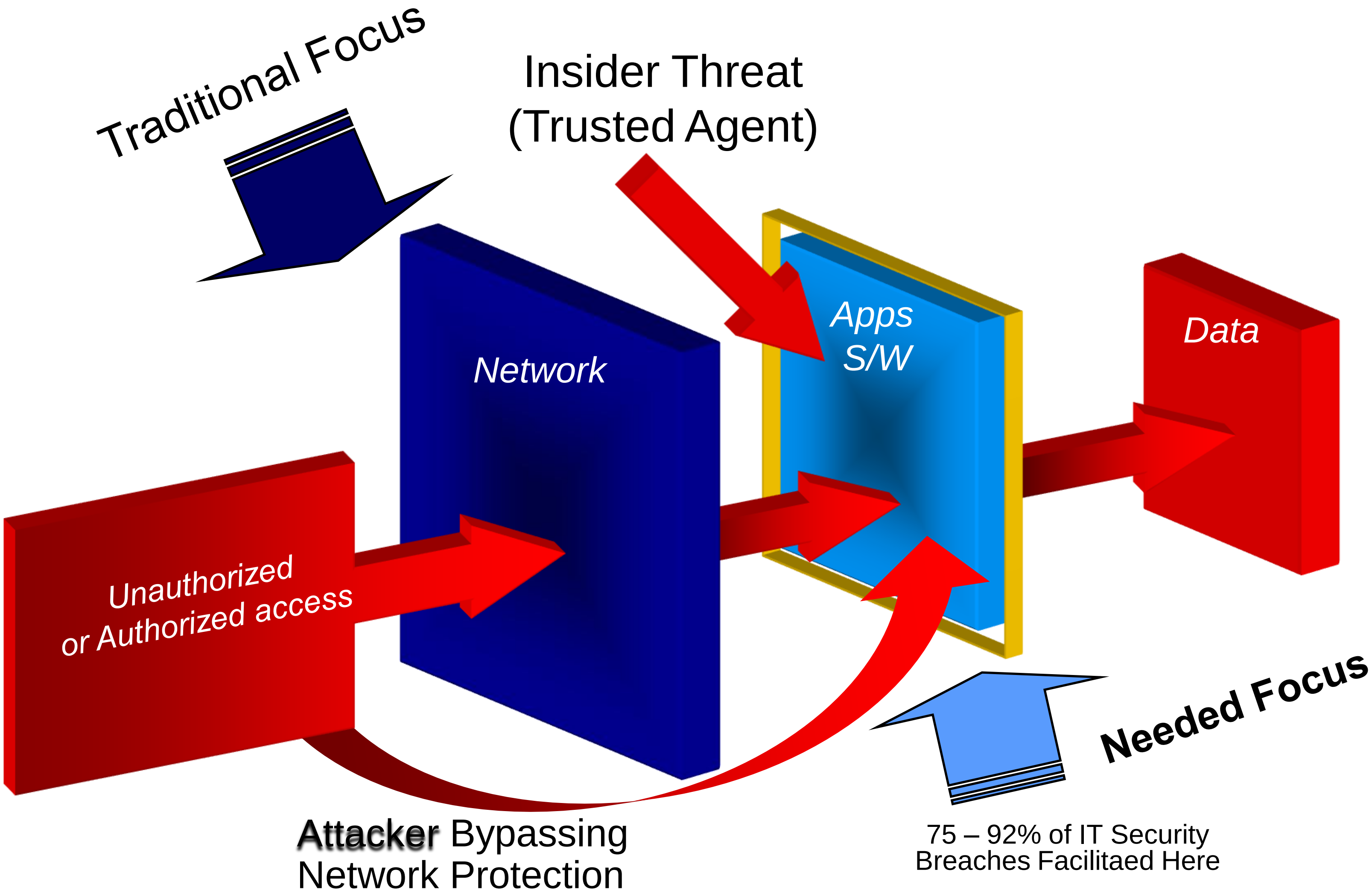
- Weaknesses Take Time To Fix
  - Staffing Limitations, Release Cycles, Fundamental Design
- Protection of Vulnerable Applications and Data
  - Immediately Provides Significant Risk Mitigation
- Knowledge of Who Is Attacking Our Applications
  - Invaluable Forensic Data For Operations and Developers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

Secure Data = Warfighter Success!!!

Public Law

- **Public Law 111-383 (FY11 NDAA, Section 932): Strategy on Computer Software Assurance**
  - **By 1 Oct 11 SecDef required to establish SwA Strategy**
    - **SwA Policy and Directives**
    - **Resources/services to integrate SwA in T&E and C&A**
    - **Acquisition/use of automated SwA tools**
    - **Real-time protection mechanisms**
    - **Define software security assurance**
    - **MAC III systems assessments and plans to prevent MAC I & II systems intrusions**
    - **Funding mechanism to remediate vulnerable legacy systems**

The Problem Area

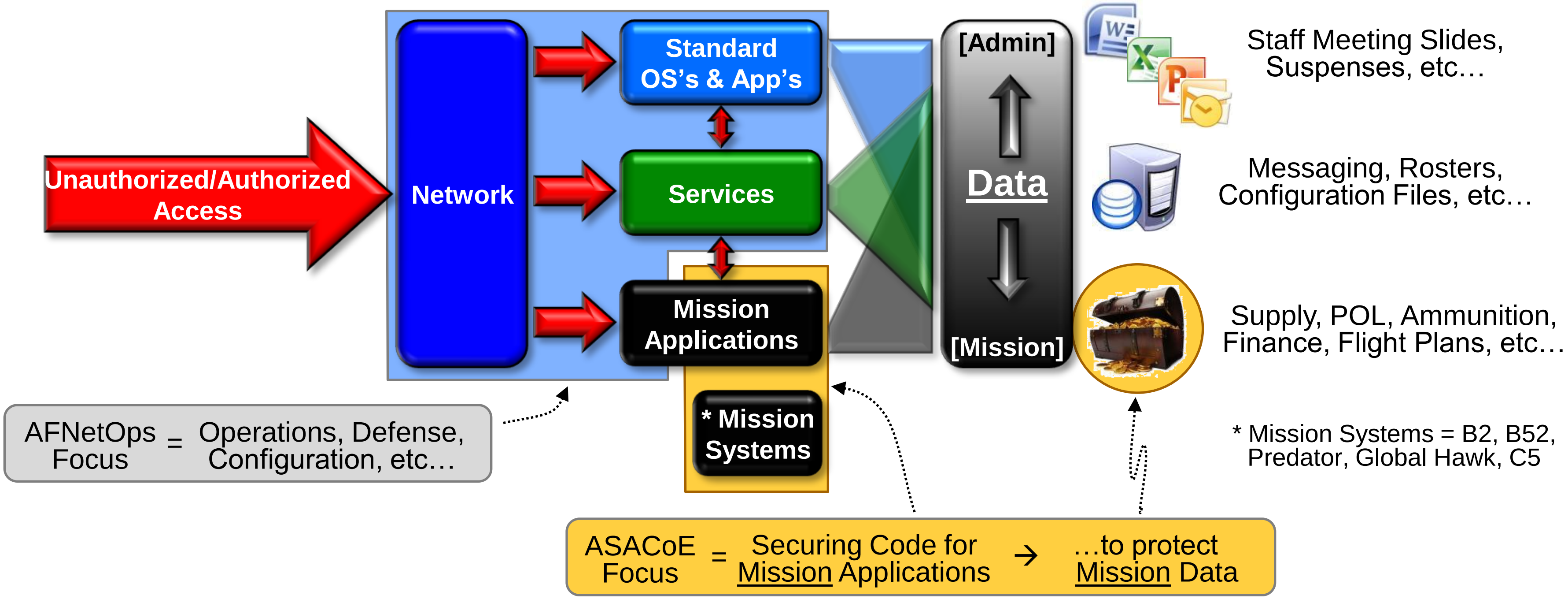


Cross-Site Request Forgery (CSRF)

Live Hacking Demo

Where does the ASACoE fit in?

- **ASACoE assists PMOs in securing software for mission applications in order to protect mission data**



Unauthorized/Authorized Access
Network
Standard OS's & App's
Services
Mission Applications
* Mission Systems
[Admin]
Data
[Mission]
Staff Meeting Slides, Suspenses, etc…
Messaging, Rosters, Configuration Files, etc…
Supply, POL, Ammunition, Finance, Flight Plans, etc…

AFNetOps Focus = Operations, Defense, Configuration, etc…

* Mission Systems = B2, B52, Predator, Global Hawk, C5

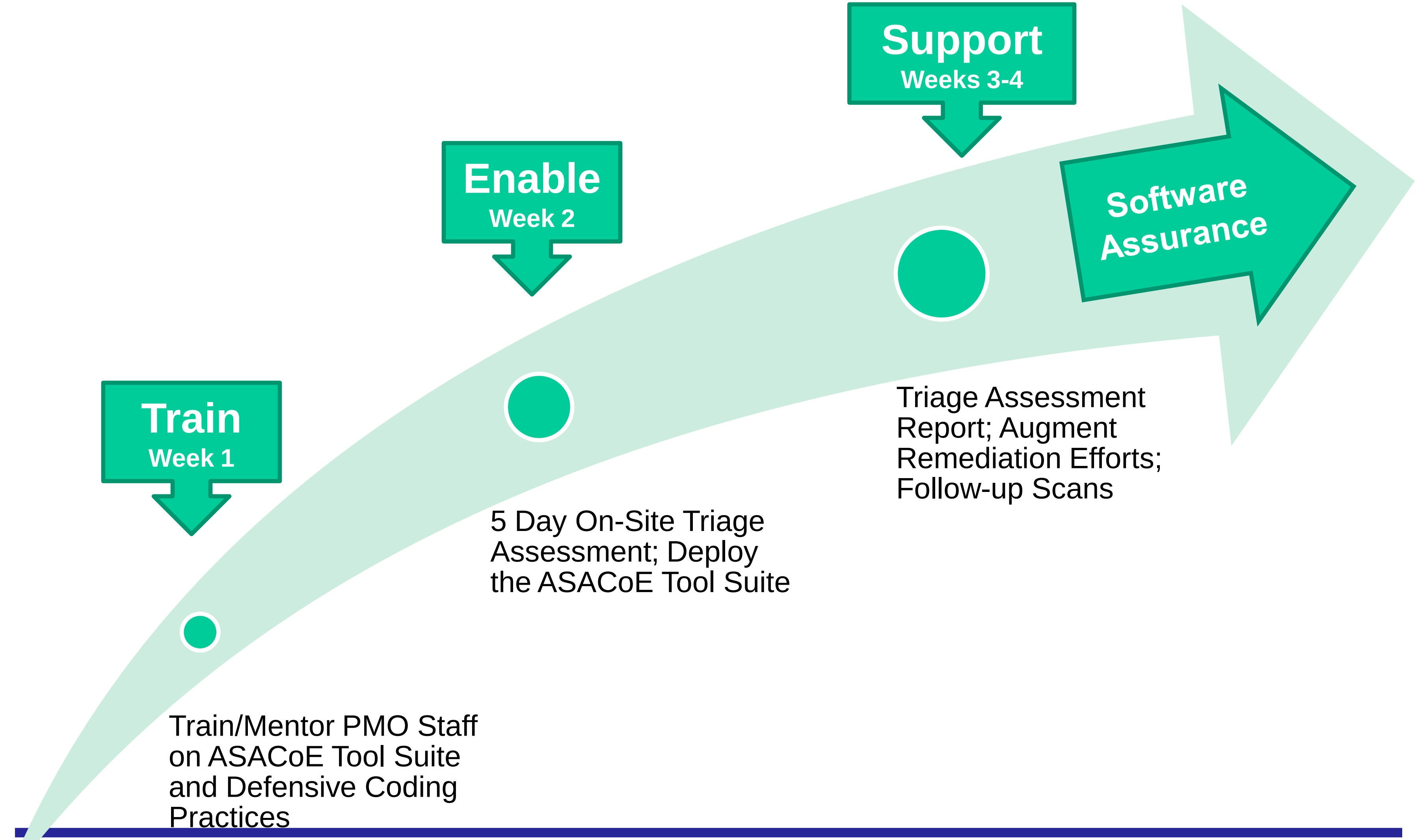
ASACoE Focus = Securing Code for Mission Applications → …to protect Mission Data

- **ASACoE is today where AFNETOPS was 12 years ago (i.e. without a Charter, mandate, enforcement or funding) but we're gaining ground!**

Future Guidance/Governance

- **ASACoE Charter**
  - **Charter to formally establish the ASACoE**
    - **To be signed by SAF/A6-AFSPC/CV-ESC/CC**
    - **ASACoE identified as a Special ACA for Software Assurance**
- **AFI 33-210, Air Force Certification & Accreditation Program (AFCAP)**
- **Air Force Software Assurance Policy**
- **DoD Governance**
  - **On the radar…letting the Air Force take the lead!**

The ASACoE Approach



Train
Week 1

Train/Mentor PMO Staff on ASACoE Tool Suite and Defensive Coding Practices

Enable
Week 2

5 Day On-Site Triage Assessment; Deploy the ASACoE Tool Suite

Support
Weeks 3-4

Triage Assessment Report; Augment Remediation Efforts; Follow-up Scans

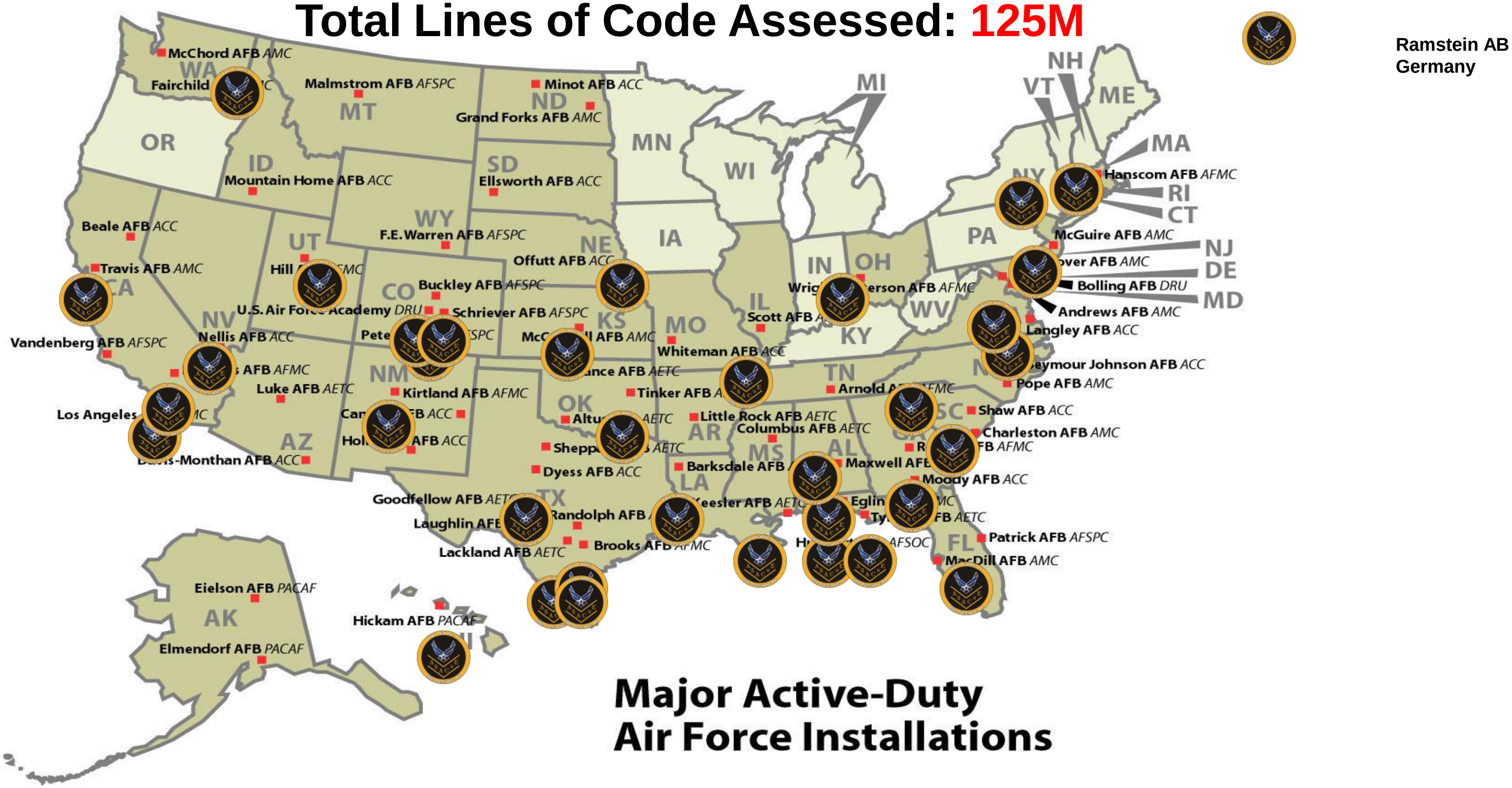
ASACoE
Assessment Status and Coverage

Delivering what we promised when we promised *War-winning Capabilities…On Time, On Cost*

Program Management Offices Visited: 215

Applications Assessed: 851

Total Lines of Code Assessed: 125M



Major Active-Duty
Air Force Installations

Integrity - Service - Excellence

ASACoE Tool Suite

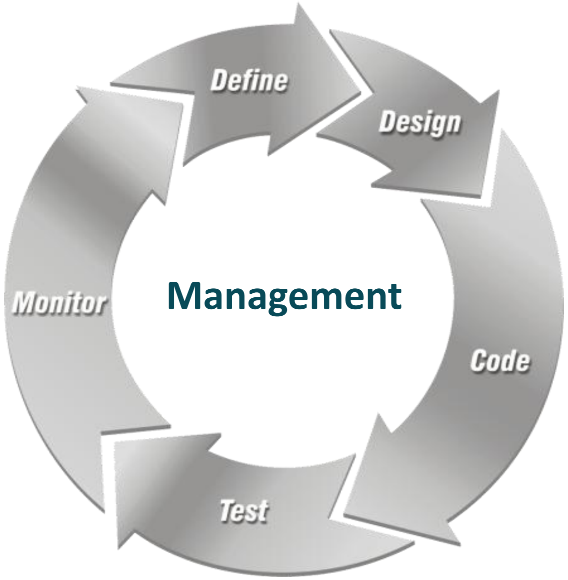
Database Analysis

Compares database setup against current security configuration settings.

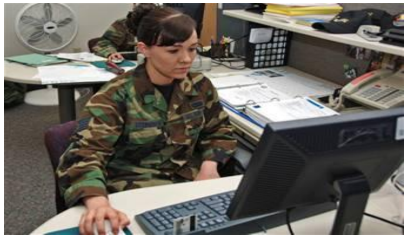
Source Code Analysis (SCA)

Proactive security; analysis tuned for low false positives

Security Ops Team



Developers



Security Testers

Security Leads / Auditors

Penetration Testing & Dynamic Analysis

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

Code Auditing

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

ASACoE Reports and Support

- **Triage Assessment Report**
  - *Executive Summary*
  - *Objectives and Technical Scope*
  - *Assessment Approach*
  - *Report of Findings*
  - *Vulnerability Descriptions*
  - *Recommendations for Mitigation*

UNCLASSIFIED - FOR OFFICIAL USE ONLY

Application Triage Scan

Report

Software Assurance Triage Scan for [System_Name] ([System_Abb])

Version ##

20 January 2009

U.S. AIR FORCE

UNCLASSIFIED - FOR OFFICIAL USE ONLY

DISTRIBUTION STATEMENT D. Distribution authorized to DoD and U.S. DoD Contractors only (Administrative/Operational use), (5/1/2010). Other requests for this document shall be referred to the ASACoE at AFPEO/ES, 501 East Moore Drive, Bldg 884, Maxwell AFB-Gunter Annex AL 36114

- **Augment Remediation Efforts When Requested**

- **Follow-up Reviews by the ASACoE Staff**

- **First Level of Support for Tools and Processes – Customer Service Focus**

Summary

- ASACoE is not a “Silver Bullet”…it is a preventive security measure to aid programs to lower risk factors in their software.
- Whether or not programs engage with ASACoE, Software Assurance must be built into the SDLCs.
- Training developers is essential!
- Educating Senior Management is critical!

ASACoE

Changing the Way the Air Force Thinks about Software

How Secure is Your Code?

POCs

- ASACoE Chief
  - Mr. James “Woody” Woodworth

    james.woodworth@gunter.af.mil
- Operations Chief
  - Ms. Brenda Bryant
    brenda.bryant@gunter.af.mil
- Program Manager
  - 2Lt Michael Parrish
    michael.parrish@gunter.af.mil

Questions

Questions?