SOFTWARE SECURITY ASSURANCE SUMMIT

December 1, 2010 | Westin Tysons Corner | Falls Church, VA

T.E.N. presented by FORTIFY An HP Company

Mastering SSA

A Case Study of the Air Force's Application Software Assurance Center of Excellence

Eric Friese

Software Security Consultant

Shakeel Tufail

Federal Practice Manager

Mastering SSA: ASACoE

Agenda

- History
- The ASACoE Process
- Challenges
- Best Practices
- Q&A

In the beginning…

Mastering SSA: ASACoE

- August 2005 – Human Resource System Breached
- 33,000 Records Stolen
- Attack vector was software related

SecurityFocus™

Run your small business. We'll pr

Complete protection solution designed for small business.

PRINT EMAIL COMMENT

US Air Force scrambles after privacy breach

John Leyden, The Register 2005-08-22

The US Air Force has been forced to notify more than
exposed following the discovery of a computer securit
discovered suspiciously high activity on one account ir
System), dating back to June.

A preliminary investigation suggests a hacker used a legitima

Mastering SSA: ASACoE

- Software Security Pilot Program
  - Lead by Maj. Bruce Jenkins
- Critical vulnerabilities were found in all pilot applications
- Decision was made to organize a group dedicated to software security – Fall 2006

Application

Software

Assurance

Center

of

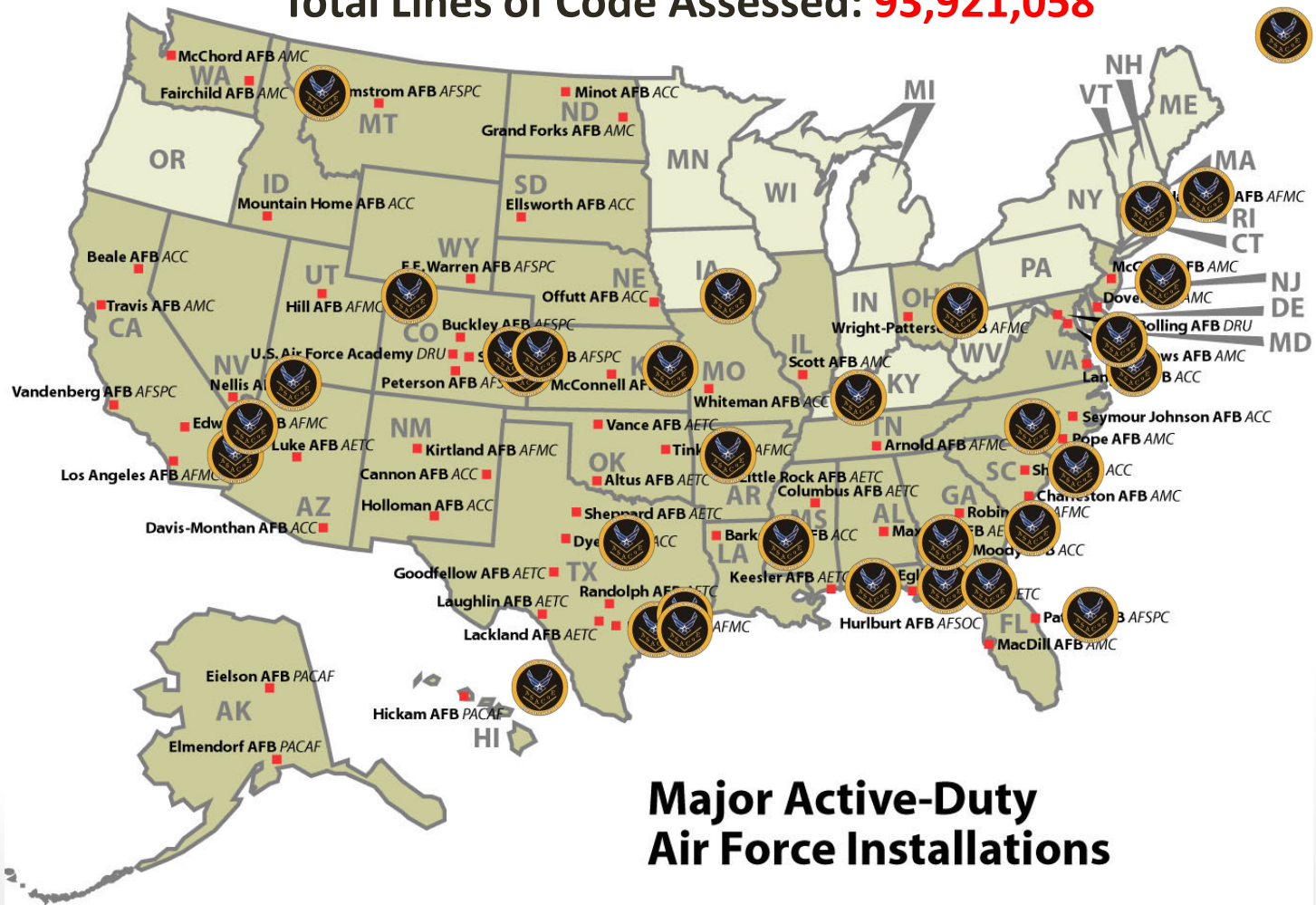
Excellence

Mastering SSA: ASACoE

- **Contract competition to find best automated security software**
- **Focus on 3 areas:**
  - Static Analysis (Source Code Analysis)
  - Dynamic Analysis (Penetration Testing)
  - Data Tier Analysis (Database STIG Checking)
- **The Winners**
  - Fortify Software (SCA and 360 Server)
  - IBM Rational Appscan
  - AppSecInc AppDetective
- **Services**
  - Prime Contractor – Telos
  - Subcontractors – Fortify and Cigital

Mastering SSA: ASACoE

Program Management Offices Visited: 96
Applications Assessed: 600+
Total Lines of Code Assessed: 93,921,058

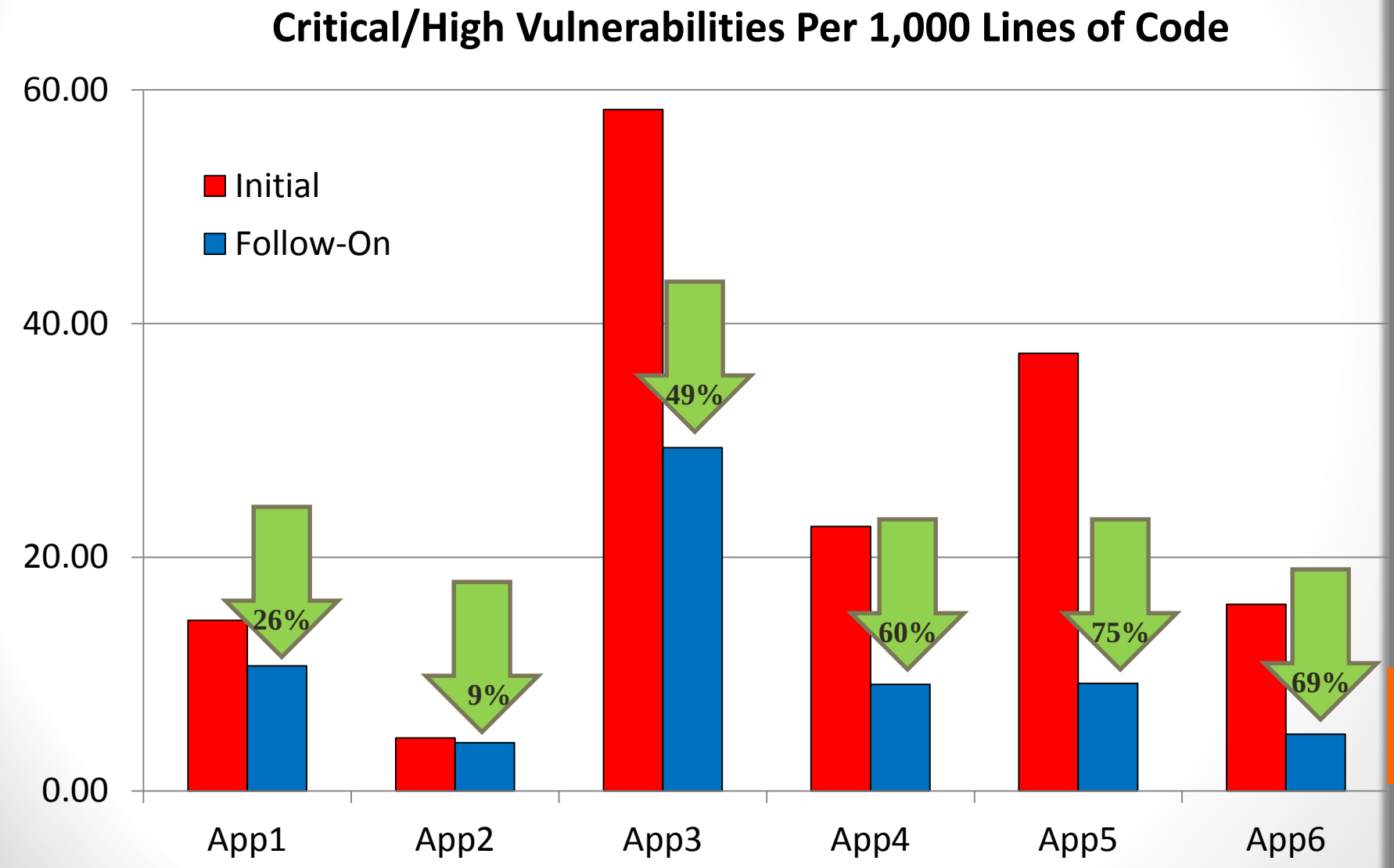


Major Active-Duty Air Force Installations

ASACoE Benefits

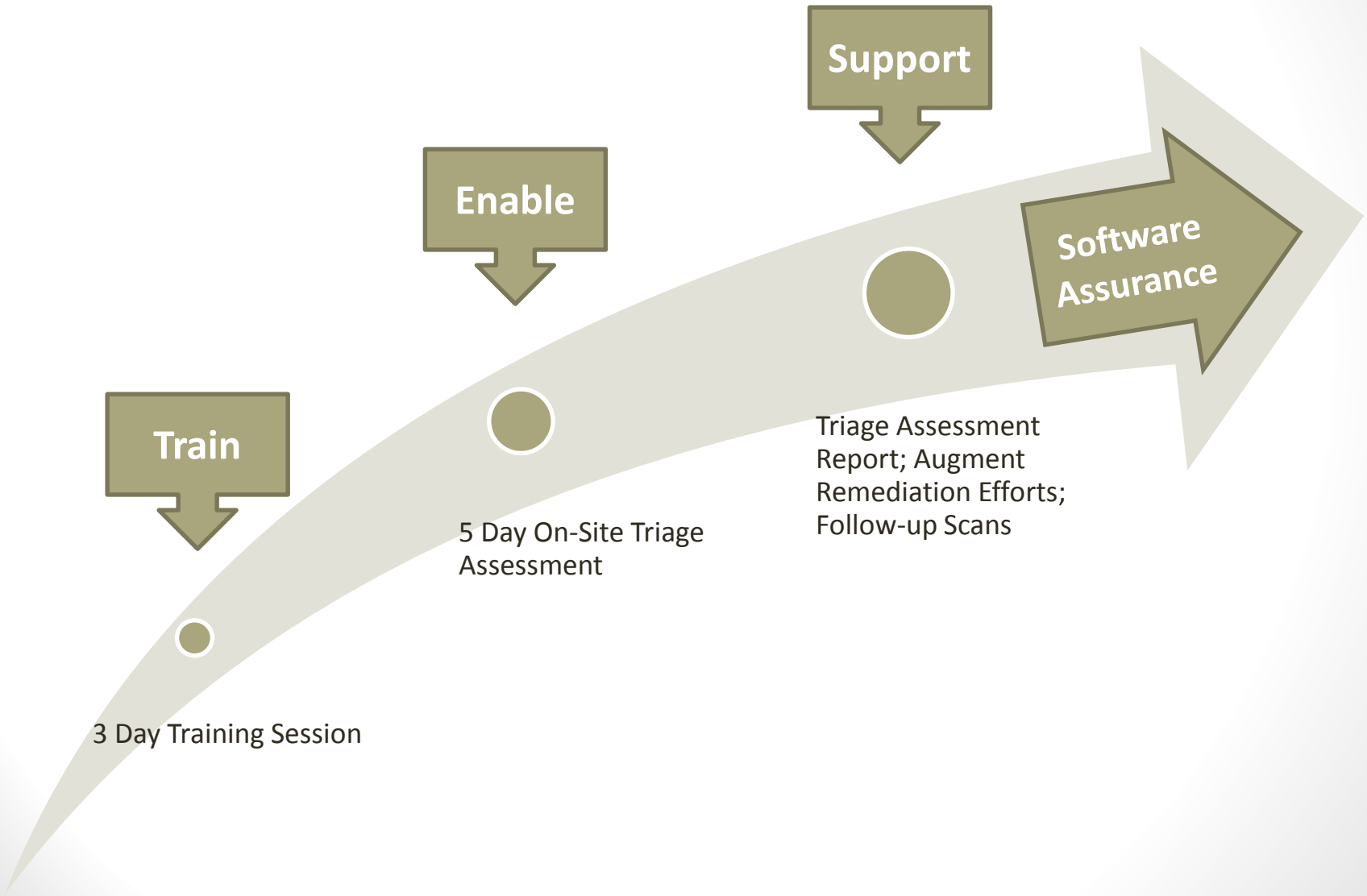
- Significant Risk Mitigation throughout the SDLC
- Cost and Time Savings for PMOs
- Certification & Accreditation Processing Time Reduced
- Real Time Protection for Fielded Operational Systems

Mastering SSA: ASACoE



The ASACoE Process

Mastering SSA: ASACoE



Mastering SSA: ASACoE

3 Day Training Session

- 1 Day Defensive Programming
  - Need for Software Assurance
  - Case Studies
  - Vulnerability Examples
- ½ Day AppDetective Training
- 1 Day Fortify SCA Training
- ½ Day Fortify RTA/PTA/360 Server

- **Mixed audience: Managers, IA, Developers**
- **Hosted at Gunter AFB or other AFBs**

Software Security Assurance Summit
December 1, 2010 | Westin Tysons Corner | Falls Church, VA
TEN presented by Fortify An HP Company

On-Site Assessment Process

Scan codebase with the goal of integrating into the build process

- Help optimize scans to your codebase

Mentor developers on secure coding practices

- Defensive programming techniques

Triage scan results with developers

- Triage your FPR's as well as AppDetective and AppScan results.
- Time is limited so a full triage of the FPR's will be delivered with the final report

The tools will be left behind and a security assessment report will be delivered to the PMO.

- This will enable you to perform regular scans on your own

Mastering SSA: ASACoE

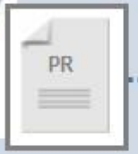
- **ASACoE Assessment Team (4 person team)**
  - 1 Organic and 3 Contractors
  - Contractors serve as Subject Matter Experts
  - Organics serve as Team Chiefs
- **All team members trained to use software suite**
- **Product specialization depending on background**
- **Periodic rotation of duties**

Mastering SSA: ASACoE

Centralized Project Management (Fortify 360 Server)
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

Source Code Analysis (SCA) (Fortify SCA)
Proactive security with targeted, accurate analysis tuned for low false positives



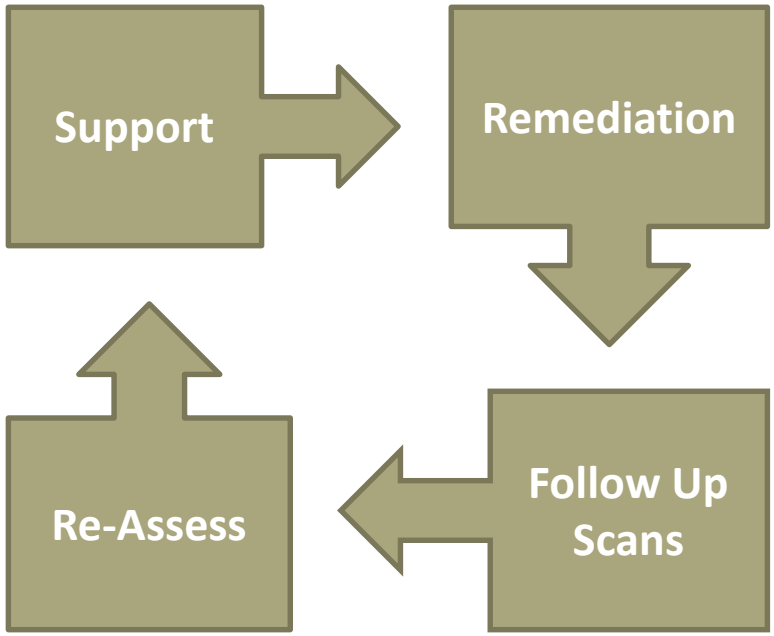
Code Auditing
Pre-build security auditing and analysis of application's entire code base

Penetration Testing (IBM Rational 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

Support

-1st Tier Support
- Link to Vendors



- 3rd Party Resources
- Verification

-New Training
- New Assessment

- Further Analysis
- Custom Rules

Challenges

Challenge #1: NO MANDATE

- No clear vision for software assurance
- Currently working with proactive groups
- Large focus on new business
- Can put a damper on remediation
- Could be making a bigger splash

Challenge #2: Moderate Adoption

- Many re-assessments reveal moderate adoption of software assurance
- Focus on scanning leaves little time for process development and automation
- Need alternate training methods

Challenge #3: Awareness and Education

- Complex problem with complex solution
- All leadership levels need to be made aware of the risks associated with software vulnerabilities
- Getting the word out
  - SAF/A6 and AFSPC – Provide policy recommendations and best practices
  - AF Institute of Technology, Academy, and Cyber Technical Schools
  - Aided US Navy, Army & Canadian Army Stand Up Similar Centers

Lessons Learned

Lesson #1: Clear Communication Regarding Security

- Before assessment, try to define policies and expectations
- Ensure that policies and expectations are communicated to all stake holders
- Consistently enforce policies and expectations

Lesson #2: Software Security is a Unique Skill Set

- Network Security/Information Assurance people are not software security people
- Development background is a necessity
- Even with a development background, extensive training and experience is needed

Lesson #3: Don't Bite Off More Than You Can Chew

- Large amounts of issues are typically found during software assurance assessment – Don't Panic
- Assess risk of vulnerabilities and prioritize what gets fixed first
- Still worried? Try Fortify RTA!

Mastering SSA: ASACoE

- **Closing Remarks**
  - The ASACoE process was designed to assess the largest amount of applications possible – not the best fit for everyone
  - If you like the ASACoE approach, they will help with implementing their model
  - When considering establishing a Center of Excellence, first consult industry standards (OpenSAM, BSIMM)

Questions?