Software Security Assurance Summit

June 9, 2011 | The Broadmoor | Colorado Springs, CO

SSA Insights and Trends

Kelly Collins

President, Fortify Public Sector

T.E.N. TECH EXEC NETWORKS presented by FORTIFY An HP Company

August 2009 “What keeps you up at night?”

"I am not sure that it will be a denial of service attack……

*…….. as much as it will be **sloppy software implementation that has left holes open for hacking”***

Aneesh Chopra
Federal CTO

SOURCE: HTTP://WWW.THESTREET.COM/PRINT/STORY/10579144.HTML

February 16, 2011 Threat Assessment prepared for SSCI

"Last year some of our largest information technology and defense contractor companies discovered that through out much of 2009 they had been the targets of a systematic effort to penetrate their networks and acquire proprietary information.

The intrusions attempted to gain access to and potentially modify the contents of source code repositories, the intellectual crown jewels of most of these companies."

General Clapper DNI

SOURCE: HTTP://WWW.THESTREET.COM/PRINT/STORY/10579144.HTML

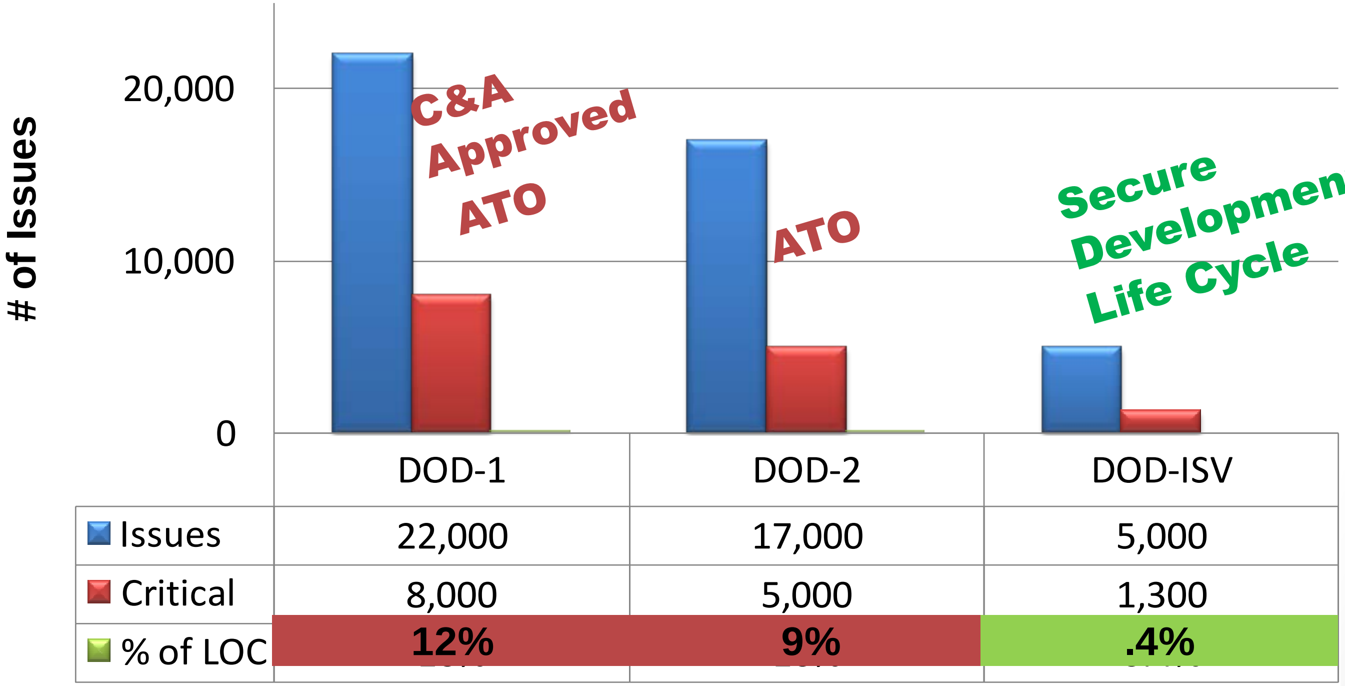
Software Complexity

Application	Lines of Code - Millions
1981 Cadillac	.05
F22 Raptor Avionics	1.7
Space Shuttle	2
Microsoft Word	2
F35 Joint Strike Fighter	5.7
Boeing 787 Dreamliner	6.5
Mercedes w/Nav	20
Premium Car	100

Software Security Assurance

What if 10% of Software had Exploitable Critical Vulnerabilities?

A Tale of Three Scans



C&A Approved ATO

ATO

Secure Development Life Cycle

	DOD-1	DOD-2	DOD-ISV
🟦 Issues	22,000	17,000	5,000
🟥 Critical	8,000	5,000	1,300
🟩 % of LOC	**12%**	**9%**	**.4%**

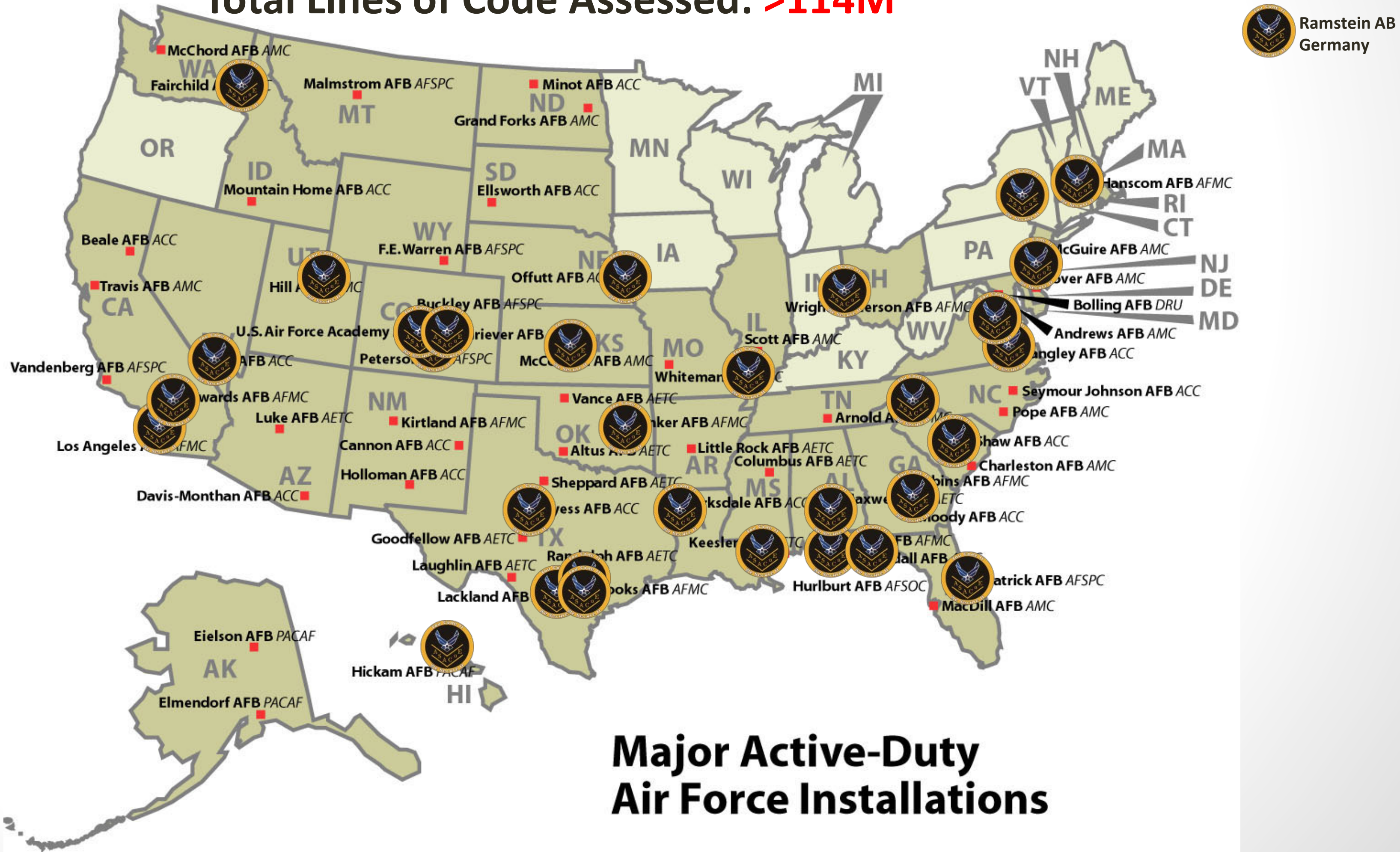
ASACoE
Assessment Status and Coverage

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

Program Management Offices Visited: 184

Applications Assessed: 721

Total Lines of Code Assessed: >114M



Major Active-Duty Air Force Installations

Customer Testimonials

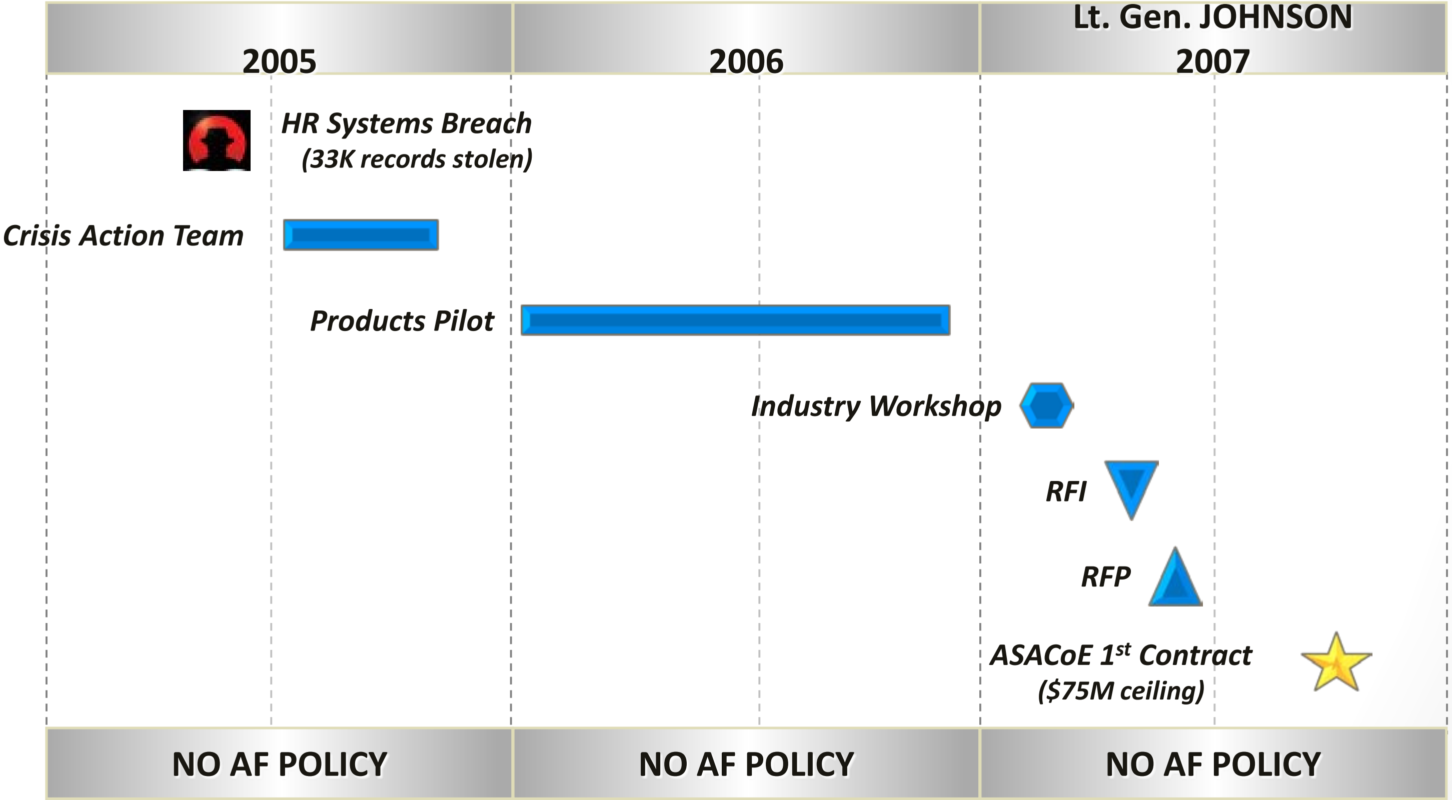
"…What you did for us was to allow us to evaluate more than 5 million lines of code that was proprietary at a cost savings of nearly $500 million…" - Lead Developer at ASC

"…After the assessment was complete, they didn't just pack up and say have a nice day. They kept in touch offering incredible assistance with specific vulnerability fixes, proper procedure for securing code, and even software to help test our code once we fixed it…"

- Lead Developer for a $9.2B contracting system

"…They were instrumental in our team changing our coding practices for the better. Our developers use the ASACoE tools routinely to audit our system and build in security..." - Program Manager for a major logistics system

AF Software Security Timeline



Lt. Gen. JOHNSON

2005

2006

2007

HR Systems Breach
(33K records stolen)

Crisis Action Team

Products Pilot

Industry Workshop

RFI

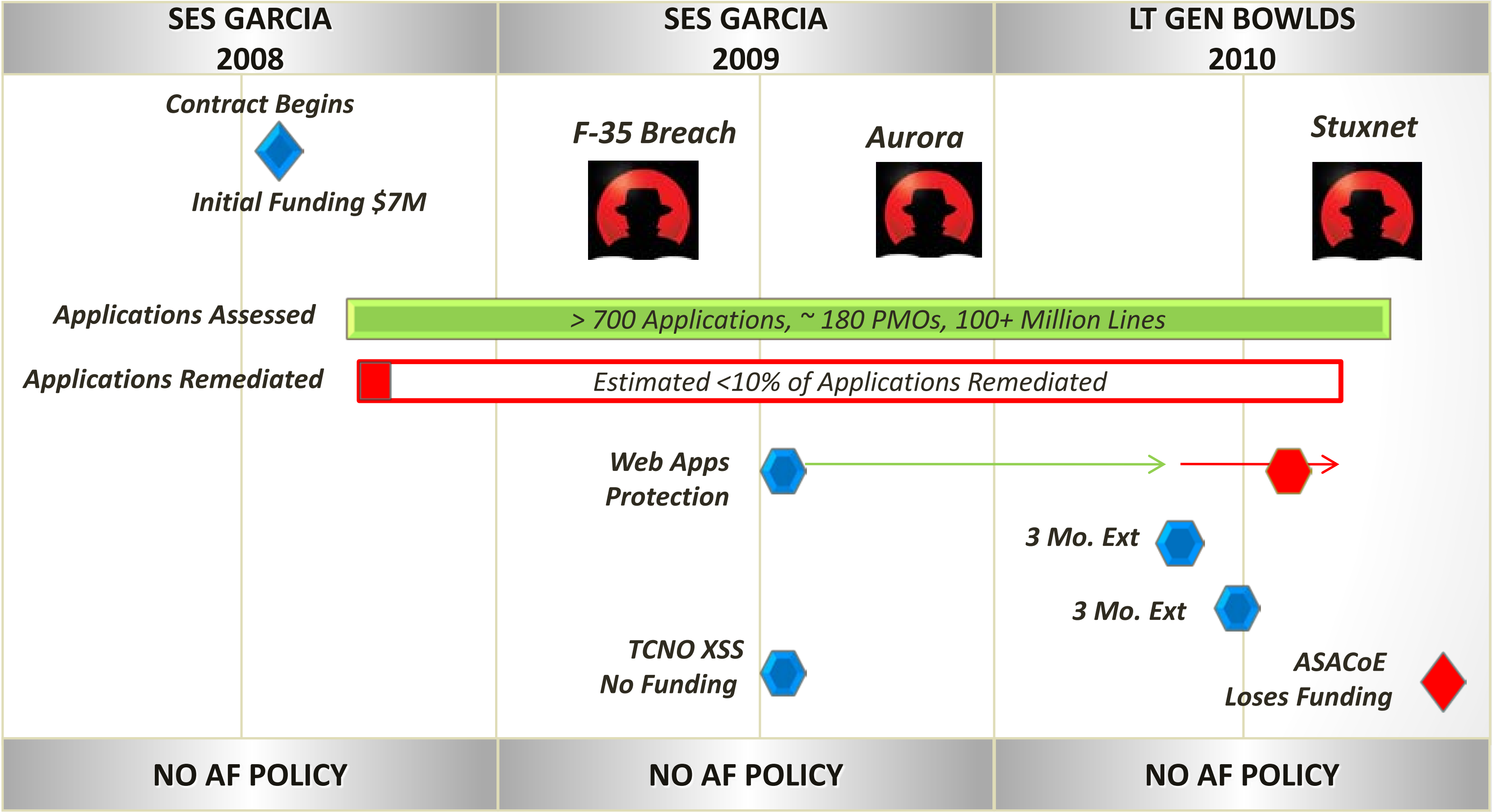
RFP

ASACoE 1st Contract
($75M ceiling)

NO AF POLICY

NO AF POLICY

NO AF POLICY



SES GARCIA 2008

SES GARCIA 2009

LT GEN BOWLDS 2010

Contract Begins

Initial Funding $7M

F-35 Breach

Aurora

Stuxnet

Applications Assessed

> 700 Applications, ~ 180 PMOs, 100+ Million Lines

Applications Remediated

Estimated <10% of Applications Remediated

Web Apps Protection

3 Mo. Ext

3 Mo. Ext

TCNO XSS No Funding

ASACoE Loses Funding

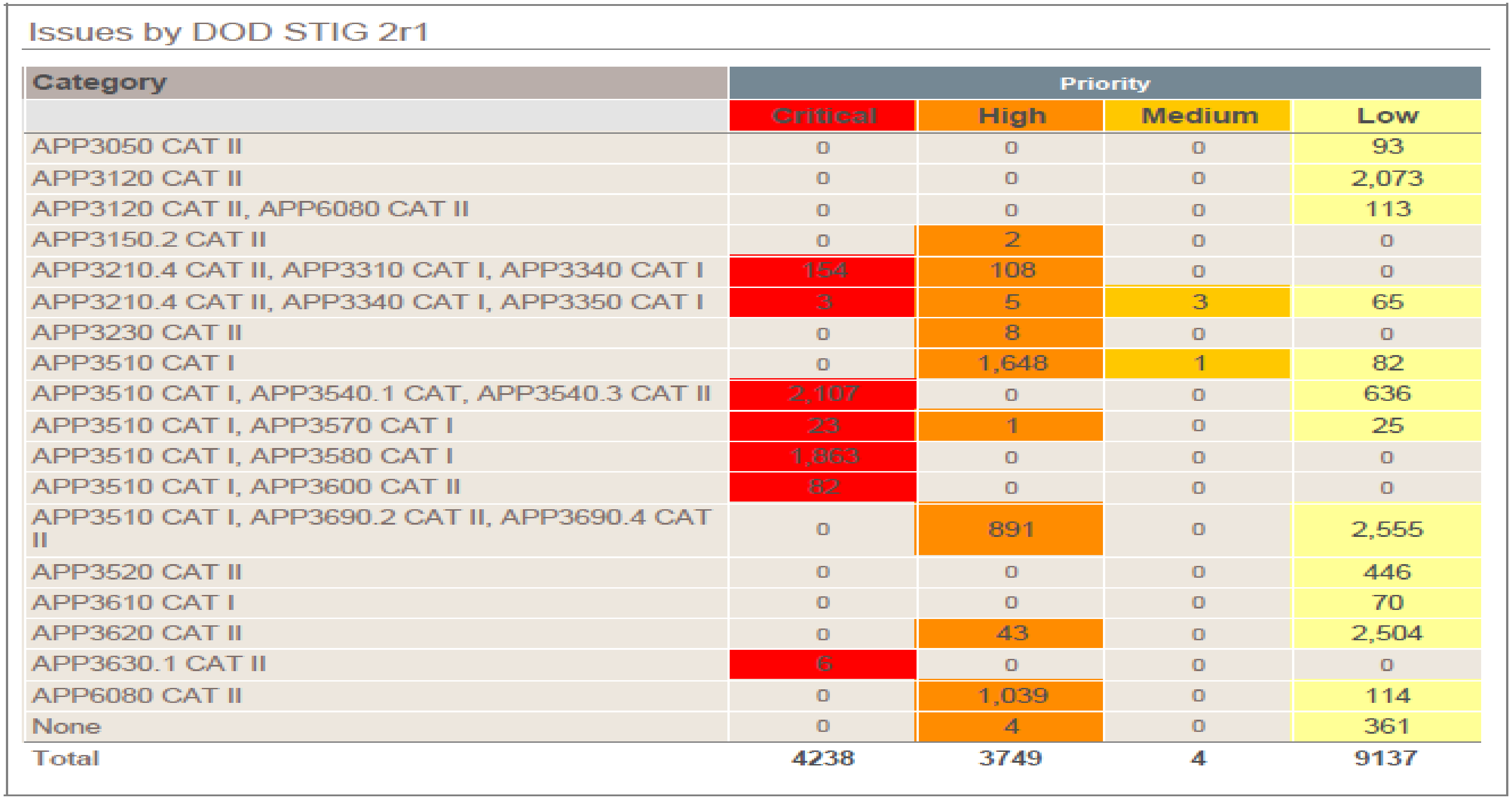
NO AF POLICY

NO AF POLICY

NO AF POLICY

Statistics

Mission	Total Issues	Critical	%Critical	Projects
Application Group 1	934,097	96,847	10%	29
Application Group 2	394,284	157,999	40%	15
Application Group 3	352,943	37,792	11%	17
Application Group 4	327,597	91,680	28%	14
Application Group 5	288,206	12,515	4%	10
Application Group 6	236,061	26,607	11%	34
Application Group 7	230,166	13,591	6%	12
Application Group 8	154,501	6,307	4%	12
Application Group 9	58,973	37,599	64%	4
Application Group 10	52,022	2,052	4%	2
Application Group 11	36,291	2,634	7%	2
Application Group 12	18,444	1,716	9%	4
Application Group 13	12,337	369	3%	13
Application Group 14	5,057	1,172	23%	2
Application Group 15	1,017	111	11%	1



Issues by DOD STIG 2r1

Category	Priority			
	Critical	High	Medium	Low
APP3050 CAT II	0	0	0	93
APP3120 CAT II	0	0	0	2,073
APP3120 CAT II, APP6080 CAT II	0	0	0	113
APP3150.2 CAT II	0	2	0	0
APP3210.4 CAT II, APP3310 CAT I, APP3340 CAT I	154	108	0	0
APP3210.4 CAT II, APP3340 CAT I, APP3350 CAT I	3	5	3	65
APP3230 CAT II	0	8	0	0
APP3510 CAT I	0	1,648	1	82
APP3510 CAT I, APP3540.1 CAT, APP3540.3 CAT II	2,107	0	0	636
APP3510 CAT I, APP3570 CAT I	23	1	0	25
APP3510 CAT I, APP3580 CAT I	1,863	0	0	0
APP3510 CAT I, APP3600 CAT II	82	0	0	0
APP3510 CAT I, APP3690.2 CAT II, APP3690.4 CAT II	0	891	0	2,555
APP3520 CAT II	0	0	0	446
APP3610 CAT I	0	0	0	70
APP3620 CAT II	0	43	0	2,504
APP3630.1 CAT II	6	0	0	0
APP6080 CAT II	0	1,039	0	114
None	0	4	0	361
Total	4238	3749	4	9137

? 2011	? 2012	? 2013

☆ *NDAA Software Assurance Policy*

AF 33-210 ☆

Lost Funding to Continue Performing Applications Assessments

DOD Bill Focus on Remediation of MAC 1 + MAC 2 LEGACY Systems – AF 33-210 SSA Inclusion Fall ‘11

New or Localized COE’s?

⬡	⬡	⬡	⬡
ASC	24th	SPC	ESC

Night Dragon, RSA SecureID, Comodo, Lizamoon, Epsilon, NASDAQ, LMCO… .

?

DoD and AF POLICY	DoD and AF POLICY	DoD AF POLICY

2011 DoD Authorization (H.R. 6523)

Section 932, Software Security Assurance

“The committee emphasizes the importance of developing new technologies for the automated analysis of software code for vulnerabilities and for detecting attempted intrusions. It is not practical to manually examine all the lines of code in all of DOD's critical information systems.”

(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

…

(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber-attack by acquiring and improving automated tools for--

(A) assuring the security of software and software applications during software development;
(B) detecting vulnerabilities during testing of software; and
(C) detecting intrusions during real-time monitoring of software applications.

…

(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems

Software Assurance "COE" Lessons Learned

PHASE ONE = "GATE"

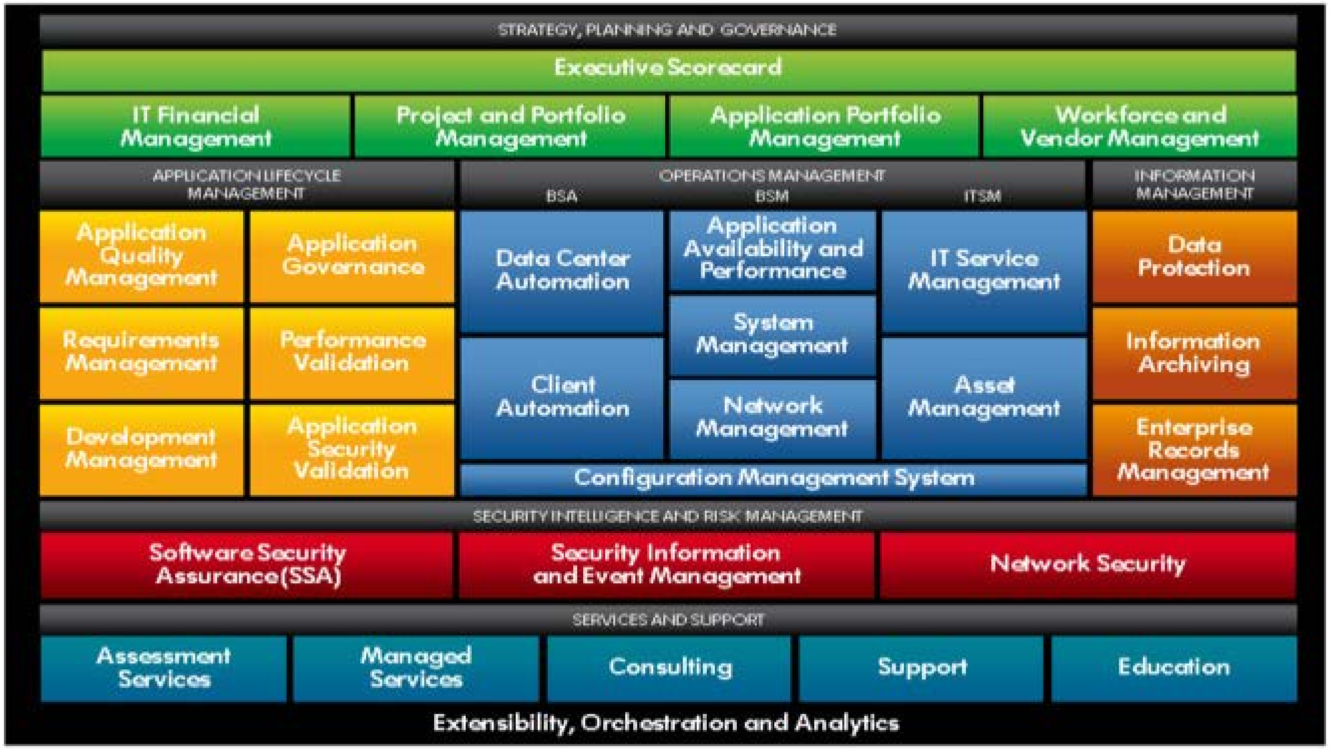
- "FIND"
- TRAIN ONCE
- NO SOFTWARE POLICY
- SCANS Production Systems
- PM GIVEN SCAN RESULTS

PHASE TWO = SSA + Secure SDLC

- "FIND AND FIX"
- TRAIN + Remediation Assistance
- POLICY and GOVERNANCE
- DEVELOPERS Early in Lifecycle
- PM, FSI, GOV ALL EDUCATED

IT Performance Suite

Running the business of IT



STRATEGY, PLANNING AND GOVERNANCE

Executive Scorecard

IT Financial Management | Project and Portfolio Management | Application Portfolio Management | Workforce and Vendor Management

APPLICATION LIFECYCLE MANAGEMENT

Application Quality Management | Application Governance

Requirements Management | Performance Validation

Development Management | Application Security Validation

OPERATIONS MANAGEMENT

BSA: Data Center Automation | Client Automation

BSM: Application Availability and Performance | System Management | Network Management

ITSM: IT Service Management | Asset Management

Configuration Management System

INFORMATION MANAGEMENT

Data Protection | Information Archiving | Enterprise Records Management

SECURITY INTELLIGENCE AND RISK MANAGEMENT

Software Security Assurance (SSA) | Security Information and Event Management | Network Security

SERVICES AND SUPPORT

Assessment Services | Managed Services | Consulting | Support | Education

Extensibility, Orchestration and Analytics

Software Security Assurance

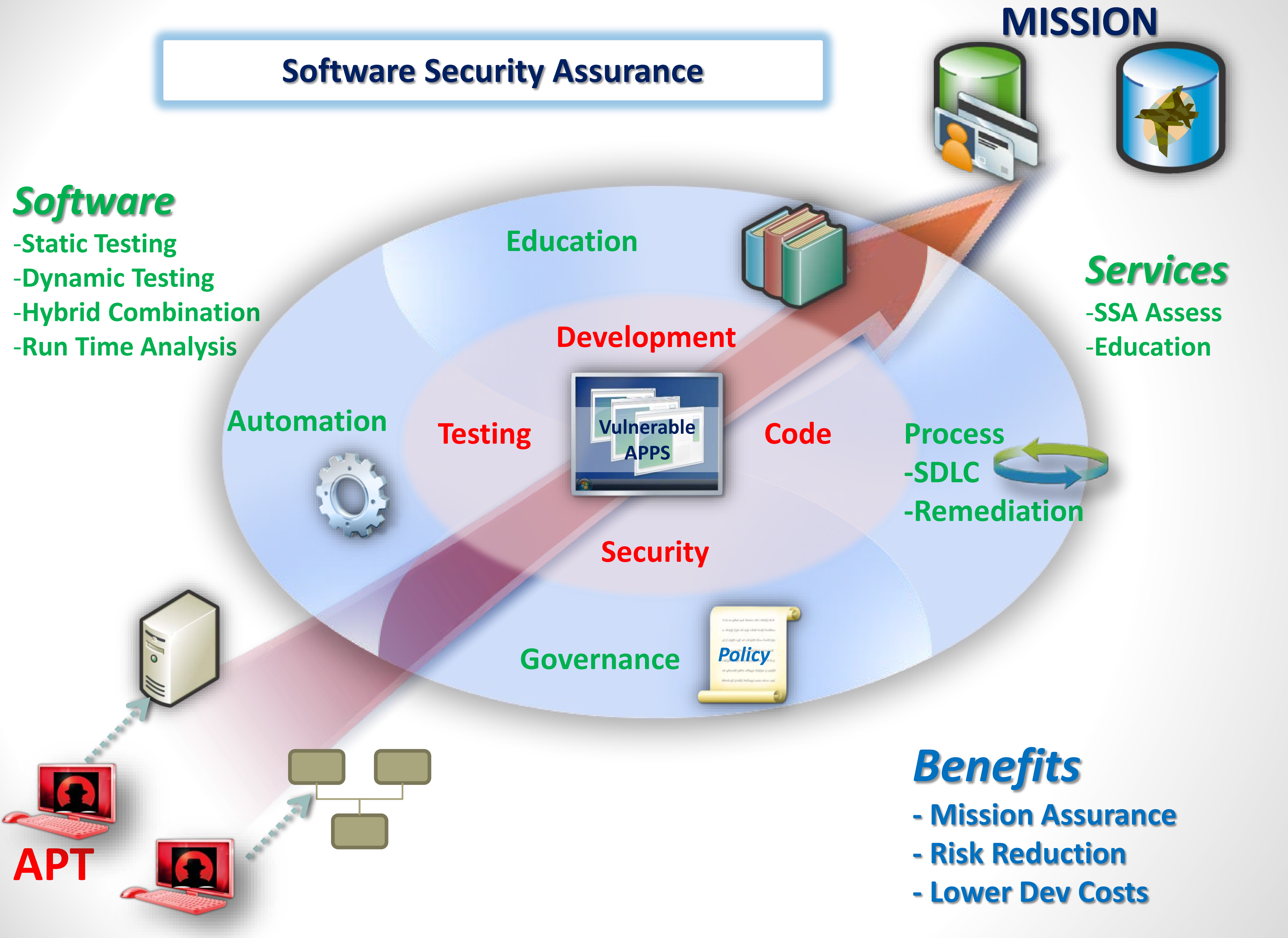
Software

-Static Testing

-Dynamic Testing

-Hybrid Combination

-Run Time Analysis



Services

-SSA Assess

-Education

Benefits

- Mission Assurance
- Risk Reduction
- Lower Dev Costs