STATIC CODE ANALYSIS IN THE FEDERAL GOVERNMENT

2011 Nominee
International Security Executives (ISE®)
Information Security Project of the Year
North America
Government Sector


A Presentation by
The
Software Angel
of Death

"IF YOU AREN'T DOING STATIC CODE ANALYSIS RIGHT, WHAT ELSE AREN'T YOU DOING RIGHT?

Friedrich Nietzsche

“Sometimes people don't want to hear the truth because they don't want their illusions destroyed.”

How Lewis Black might have said it.

“Sometimes people don't want to hear the truth because they don't want their *delusions* destroyed.”

A WORD OF CAUTION

- I speak differently from the rest of the real world and NIST
- Static Code Analysis in John's World Means Code Quality Checking
- Static Security Analysis in John's World is What Most of You Call Static Code Analysis
- I Apologize In advance For Any Confusion

MY LIMITED OBSERVATIONS

NATIONAL APPROACH

- Software Assurance ***is the level of confidence that software 1.) is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and 2.) that the software functions in the intended manner. (CNSS Instruction No. 4009, 26 April 2010)***

DOD STRATEGY

- ***Software Assurance*** *is the level of confidence that software 2.) functions as intended and 1.) is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.*
  - *Mandated by Federal Law - Section 932, 2011 NDAA*
  - *Defined by Federal Law – Section 933, 2013 NDAA*
  - *New Guidance – Section 937, 2014 NDAA*
- *A Systems Engineering discipline implemented in Newly-Released 5000.02*
  - *Supports Information Assurance: DISA STIG ID APP5080*
  - *Supports Test and Evaluation: DISA STIG IS APP5100*
- ***Laws and Policies Now MANDATE use of Automated Scanning Tools***

RESULTS OF PARTICIPATION IN MULTIPLE EVENTS

- About 10% Are Already Doing Rigorous Static Analysis
  - Primary Emphasis on Security Vulnerabilities
  - But…….
- Another 10% Are In The Planning/Early Implementation Stage
- Another 10% Have Done Their First Scans and Are *Terrified* With The Results
- The Other 70% Are Wondering Who I Am and How Quickly Can They Run And Hide From Me

SHARED "SECRETS"

- **Rigorous Reduction of Security Vulnerabilities Using Automated Tools By Conscientious Developers DIRECTLY Results In Improved Code Quality**
  - **And Vice Versa……..**
- **High Failure Rates During Operational Testing Can Be DIRECTLY Correlated To High Security Defect Density and High Code Quality "Technical Debt."**

The Value Proposition

Aldous Huxley

“Facts do not cease to exist because they are ignored.”

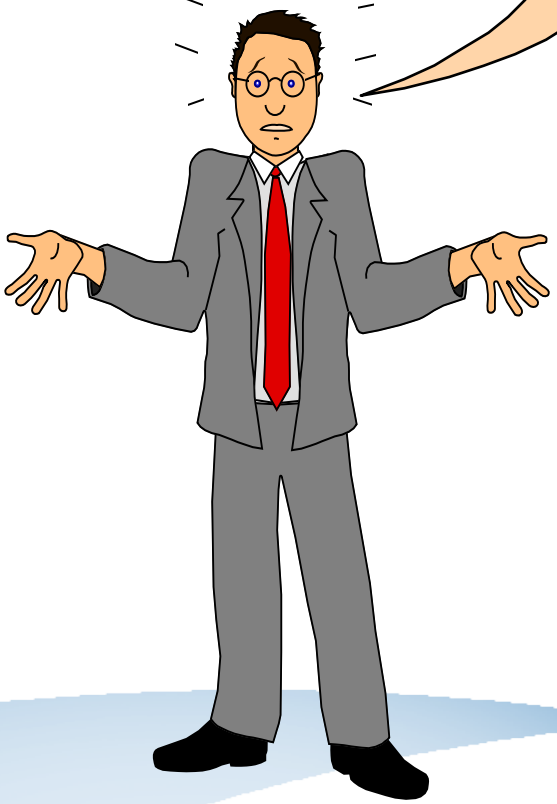
DEFECT DENSITY - BASIC MODEL*

	Requirements Analysis/Design	Code/Unit Testing	Government Testing	Production/ Deployment	Total Cost/ Investment	Return on Investment
Error Distribution	10%	20%	55%	15%		
Hours to Correct		50	120	380		
Cost per Hour		$100	$100	$100		
Cost to Fix 1000 Errors		$1,000,000	$6,600,000	$5,700,000	$13,300,000	

- *Stewart-Priven Group, 2009 Presentation to PMI-MHS "Software Inspection Success"
- DAU Advanced Test and Evaluation (TST 303)

RETURN ON INVESTMENT

Why Focus on ROI?



Clinger-Cohen

SEC. 5122. CAPITAL PLANNING AND INVESTMENT CONTROL.

(a) DESIGN OF PROCESS- In fulfilling the responsibilities assigned under section 3506(h) of title 44, United States Code, the head of each executive agency shall design and implement in the executive agency a process for maximizing the value and assessing and managing the risks of the information technology acquisitions of the executive agency.

(b) CONTENT OF PROCESS- The process of an executive agency shall--

(1) provide for the selection of information technology investments to be made by the executive agency, the management of such investments, and the evaluation of the results of such investments;

(2) be integrated with the processes for making budget, financial, and program management decisions within the executive agency;

(3) include minimum criteria to be applied in considering whether to undertake a particular investment in information systems, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information systems investment projects;

(4) provide for identifying information systems investments that would result in shared benefits or costs for other Federal agencies or State or local governments;

(5) provide for identifying for a proposed investment quantifiable measurements for determining the net benefits and risks of the investment; and

(6) provide the means for senior management personnel of the executive agency to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.

20% DEFECT REMOVAL ROI MODEL

	Requirements Analysis/Design	Code/Unit Testing	Government Testing	Production/ Deployment	Total Cost/ Investment	Return on Investment
Error Distribution	10%	20%	55%	15%		
Hours to Correct		50	120	380		
Cost per Hour		$100	$100	$100		
Cost to Fix 1000 Errors		$1,000,000	$6,600,000	$5,700,000	$13,300,000	
SCQC Applied						
Error Distribution	10%	40%	45%	5%		
Hours to Correct		50	120	380		
Cost per Hour		$100	$100	$100		
Cost to Fix 1000 Errors		$2,013,518	$5,400,000	$1,800,000	$9,213,158	
Cost Avoidance		$1,013,518	$1,200,000	$3,900,000	$4,086,842	
SCQC Investment					$1,868,230	
ROI						**118.75%**

OBSERVED SCQC BENEFITS

- **Testing by itself is time consuming and not very efficient.***
  - Most forms of testing only find about **35%** of the bugs that are present.

- **Static analysis** prior to testing is very quick and about **85%** efficient.
  - As a result, when testing starts there are so few bugs present that testing schedules are cut down by perhaps **50%**.
  - Static analysis will also find some structural defects that are not usually found by testing.

- **Static Security Analysis** prior to DIACAP testing *may* find, and be able to help correct, a large number of the **Applications Source Code** defects identified during Information Assurance testing.
  - When combined with Manual Code Review and Dynamic Analyses, can reduce "False Positives."

***Capers Jones -Distinguished Advisor to the Consortium for IT Software Quality (CISQ). CISQ brings together industry executives from Global 2000 IT organizations, system integrators, outsourcers, and package vendors to jointly address the challenge of standardizing the measurement of IT software quality and to promote a market-based ecosystem to support its deployment.**

85% DEFECT REMOVAL ROI MODEL

	Requirements Analysis/Design	Code/Unit Testing	Government Testing	Production/ Deployment	Total Cost/ Investment	Return on Investment
Error Distribution	**10%**	**20%**	**55%**	**15%**		
Hours to Correct		**50**	**120**	**380**		
Cost per Hour		**$100**	**$100**	**$100**		
Cost to Fix 1000 Errors		**$1,000,000**	**$6,600,000**	**$5,700,000**	**$13,300,000**	
SCQC Applied						
Error Distribution	**10%**	**80%**	**7%**	**3%**		
Hours to Correct		**50**	**120**	**380**		
Cost per Hour		**$100**	**$100**	**$100**		
Cost to Fix 1000 Errors		**$2,960,000**	**$621,600**	**$843,600**	**$4,425,000**	
Cost Avoidance		**$1,960,000**	**$5,978,400**	**$4,856,400**	**$8,874,000**	
SCQC Investment					**$1,868,230**	
ROI						375.04%

WHAT'S THE PROBLEM WITH THE MODEL?

MODEL ISSUES

- The Numbers in Red Are Today's BUDGET Issues
- The Benefits Appear In The Out-Years
- Managers Worry About Budgets
- Leaders Look To The Future
- Are You a Manager or Are You a Leader?

WHAT ABOUT SOME PERSONAL EXPERIENCES?

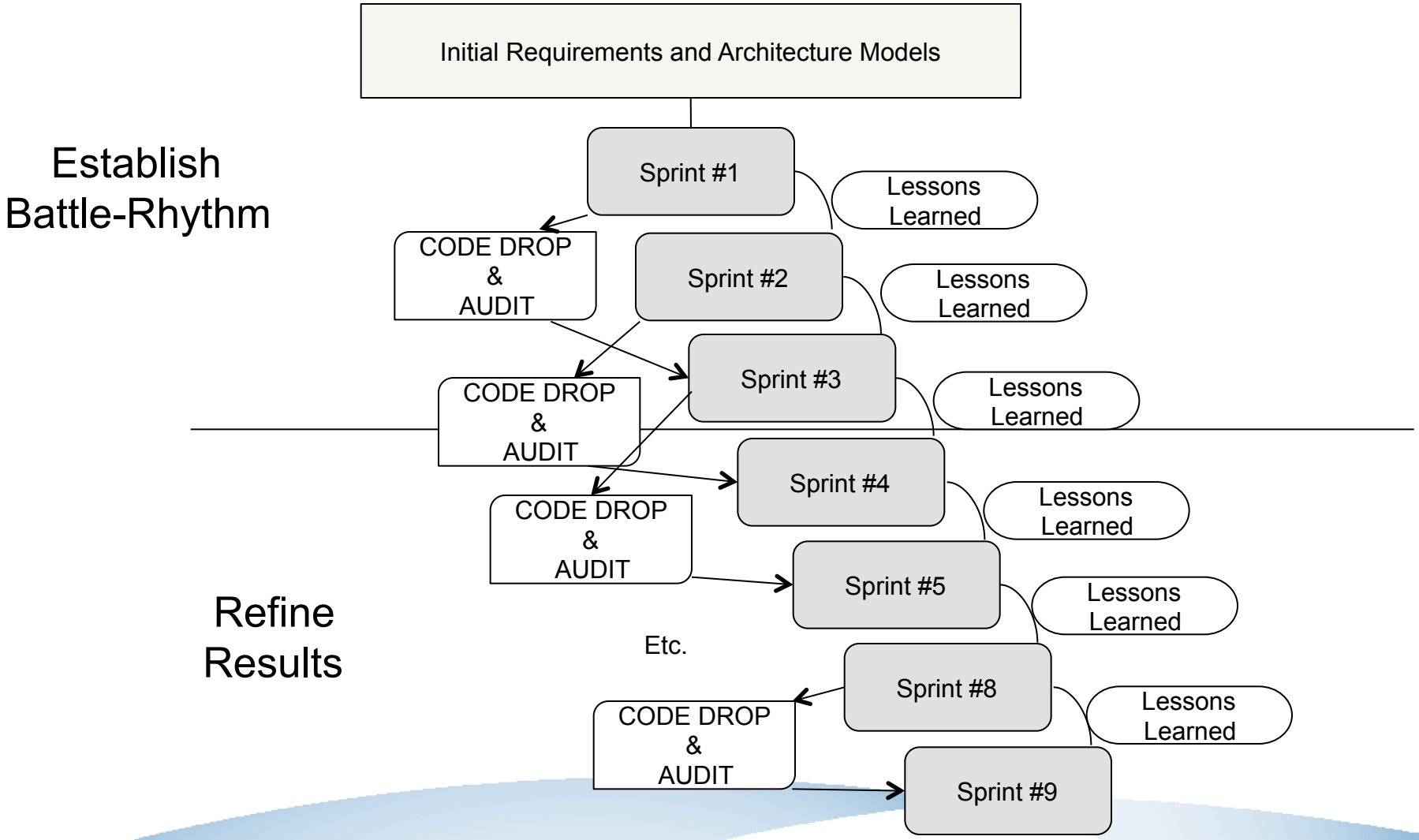
PROJECT X

- *Began Using An Automated Tool – February 2013*
  - *Fully Integrated Into Development Environment*
    - *Works with IDE and Code Quality Tools*
  - *56% Defect Reduction in Three (3) Weeks*
  - *Second Lowest Defect Density (1.07%) in My Recent History*
  - *Achieved 0.21% DEFECT DENSITY AS OF 9 AUGUST 2013*
    - *184 Defects in 86,382 Lines of Code*
  - *Achieved .004244% DEFECT DENSITY AS OF 11 FEBRUARY 2014*
    - *5 Defects in 117,804 Lines of Code*

- *HOWEVER*
  - *526 Defects Mitigated By Compensating Controls*
    - *Log Forging*
    - *System Information Leak*

WHAT ABOUT AGILE DEVELOPMENT?

AGILE DEVELOPMENT MODEL



WHAT WAS THE END RESULT?

0 defects detected
in
per-production environment

WHAT KEEPS ME AWAKE AT NIGHT?

SOME THINKING ABOUT TOOLS

"A Fool With A Tool is Still a Fool"

- *PMT256 - Program Management Tools Course*
- *TST203 - Intermediate Test and Evaluation*
- *Director, Federal Reserve Information Technology*

To achieve success you need a combination of :

- *Skilled People*
- *Disciplined Processes*
- *Enabling Tools and Technologies*

OTHER ISSUES

- Becoming a Commodity
- Failure To Document Lessons-Learned
  - Tie Today's and/or Tomorrow's Successes To Past Performance (or lack thereof)

Questions?