DoD-DHS-NIST Software Assurance Forum Measuring Software Supply Chain Risk Panel Briefing

Facilitator: Ian Brown

Mini-Keynote: Bert Miuccio

Homeland Security

Participants

- Ian Brown, Booz Allen Hamilton
- Bert Miuccio, CIS
- Thomas Rhodes, NIST
- Dan Reddy, EMC
- Bruce Weimer, U.S. Army CECOM

Objectives

- Discuss the state of measurement in software assurance, especially in the area of supply chain risk
- Identify some critical success factors for effective assurance measurement

The Role of Measurement in Mitigating Software Supply Chain Risk

Bert Miuccio, CEO
The Center for Internet Security

the CENTER for
INTERNET SECURITY

What Does Knee Replacement Surgery Have To Do With Software Supply Chain Risk?

- hospital = software supplier or integrator
- surgeon or physician = software engineers
- surgery or service = software product
- patient care = software security & integrity
- patient care = coding or software development

- Measuring Outcomes Identifies Process Problems
- Adherence to Best Practices Produces Quality Outcomes
- Monitoring and Reporting Verifies Achievement of Desired Outcomes, Adherence to Best Practices and Gives Integrators and Enterprise Customers the Assurance They Require

Measuring SwA Outcomes

- SAFECode.org: Software Integrity = “software that is free from intentional and unintentional vulnerabilities, and that it functions as intended”
  - Are these outcomes defined without ambiguity, and with enough specificity to be useful?
  - How are suppliers measuring & reporting them?
  - Are these the only two outcomes that are essential?

Are “Free from Vulnerabilities” & “Functions As Intended” the Only Essential Outcome Metrics?

- Application software must run on securely configured operating systems and middleware (database, web server, etc.)
  - Based on DISA, NIST (FDCC) and CIS standards
  - Installation does not require deviations from the standards that expose systems to vulnerabilities

SwA Best Practices

- NIST DRAFT Interagency Report 7622
  - Recommends piloting 32 “key practices” to reduce supply chain risk & that adherence should be monitored
- SAFECode Supply Chain Integrity Framework
  - Defines 11 Principles for Designing Integrity Controls
- IT Sector Baseline Risk Analysis (by the ITSCC)
  - “Produce IT products and services” is one of six IT Sector Critical Functions, with significant identified supply chain risks needing to be mitigated

Enterprise Customers – Participate in the Solution and Use Your Purchasing Power

- Let your suppliers know **what** outcomes you want and **how** you want them measured and reported to you
- Let your suppliers know **how** you want conformity with practice controls across the global supply chain monitored and reported to you

A Call To Action

- Defining outcomes and process controls is a challenging effort – collaboration is essential
- While we're figuring out what's important to measure, let's also figure out:
  - How to measure it
  - What to report and how to report it
  - How to automate data collection and reporting
  - How to provide customers with independent audits

Observations on Software Supply Chain Risk Management (SCRM)

Measuring Software Supply Chain Risk Panel
Software Assurance Forum
4 November 2009

Tom Rhodes

trhodes@nist.gov

National Institute of Standards & Technology

Information Technology Laboratory

Homeland Security

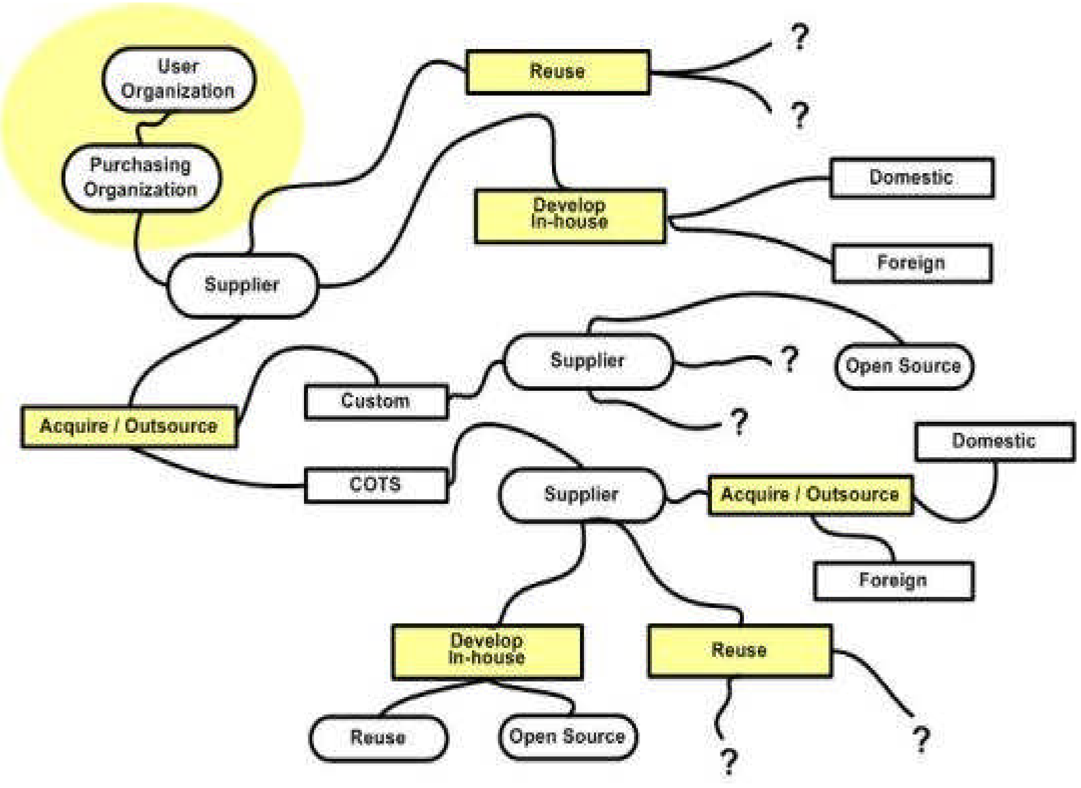
Observations on Software SCRM

- Measuring Software Supply Chain Risk Panel:
  - Broad Questions Posed:
    - Where are we in software assurance?
    - Where are we going?
    - Challenges of achieving software assurance.

Observations on Software SCRM

- What is the software supply chain?
  - Outsourced acquisition of software as off-the-shelf (COTS) or as custom developed software by one or more suppliers.
  - May include open source and reuse libraries.
  - May include compilers and editors that manipulate software.
  - Developers may be domestic, off-shore, or both.
  - Many players and roles.

Observations on Software SCRM



Potential Software Supply Chain Paths

Source: https://buildsecurityin.us-cert.gov/swa/acqwg.html

Observations on Software SCRM

- What are customer objectives?
  - Lower software product costs without loss of quality and security.
  - Reduce & minimize supply chain risks & assure product quality & security.
  - Establish a framework for effective SCRM.
  - Ensure supply chain transparency.
  - Reduce & minimize operational risks & system failures.
  - Establish a base of qualified, dependable, & secure suppliers.

Observations on Software SCRM

- What are some software supply chain risks?
  - All the usual risks when buying software, plus:
    - Global suppliers of unknown qualifications, financial stability, & performance.
    - Suppliers with mal-intent.
    - Software corrupted with weaknesses & vulnerabilities.
    - Counterfeit software & license violations.
    - Mission failure due to poor quality software or exploited vulnerabilities.
    - Untrusted networks & Cybersecurity (espionage, theft...)

Observations on Software SCRM

- Where are we in software assurance?
  - Best practices available & emerging, but may not be practiced by global & domestic suppliers, or required by customer specifications.
  - Absence of threat and risk models, & of security requirements & mitigation strategies in specifications, design, & code.
  - Un-testable specifications & insufficient requirements for assurance cases & automated testing techniques.
  - Software analysis tools available but relatively expensive and can be improved further.
  - SwA & secure development practices not yet widely taught in universities.

Observations on Software SCRM

- Where are we in software assurance? (Cont’d)
  - Catalogs of weaknesses and vulnerabilities available but secure design and coding practices not yet widely adopted.
  - Available guides & standards:
    - SCOR Supply Chain Model
    - University of MD/SAIC White Paper: SC Assurance Reference Model
    - Quality process frameworks (CMM/CMMI/SSECM…)
    - DHS & DoD Publications (BSI & SwA Web sites, SCRM Key Practices)
    - NIST Publications & Catalogs (SP 800 & 500 series, FIPS, NVD)
    - MITRE Catalogs (CWE, CVE, CAPEC…)
    - NDIA System Assurance guidebook.
    - SAFECode Publications (SSC Integrity Framework, Secure SW Dev)
    - Standard Publications (ISO/IEC 12207, 14598, 15026, 15271, 15288, 15408, 15504, 15939, 16085, 19759, 19760, 21827, 24748, 25010, 25040, 25045, 25060, 25062, 26513, 27004, 27005, 9000-3, 9001)

Observations on Software SCRM

- Where are we going?
  - Emerging national focus on the need for SCRM.
  - Ongoing awareness & outreach activities.
  - Increasing industry, government & academic research activities, collaborations, publications & resources.
  - Improved automated test methods and tools.
  - Structured assurance case models beginning to augment traditional testing and C&A activities.
  - Integration of SwA best practices into process framework models (e.g. SEI/CMMI).

Observations on Software SCRM

- Where are we going? (Cont’d)
  - – DoD and NIST Documents (Drafts):
    - Key Practices & Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 - SCRM Pilot Program.
    - Supply Chain Risk Management Practices for Federal Information Systems.
  - – NIST & DHS Projects:
    - Software Assurance Metrics & Tool Evaluation (SAMATE)
    - Metrics, Measurement & Assurance (MMA)
    - SCRM Best Practices Implementation Guidance

Observations on Software SCRM

- Challenges of achieving software assurance.
  - National initiatives and policies supporting SwA.
  - Increased awareness, education & training.
  - Sustained advocacy, sponsorship, and outreach.
  - Increased community partnering & collaborations.
  - Use of threat modeling & secure development practices.
  - Testable specifications & use of automated testing and analysis tools.
  - Formalization & integration of CWE/CVE… into tools.
  - Establishing an extensible, customizable framework for SCRM control & monitoring.

Observations on Software SCRM

- At the end of the day, even if satisfactory software assurance is obtained, we will still need operational run-time protections to monitor, detect, analyze, and mitigate errors, exploits and attacks to ensure that the product and system are protected and can fulfill their intended purposes.

Measuring Product Security at EMC

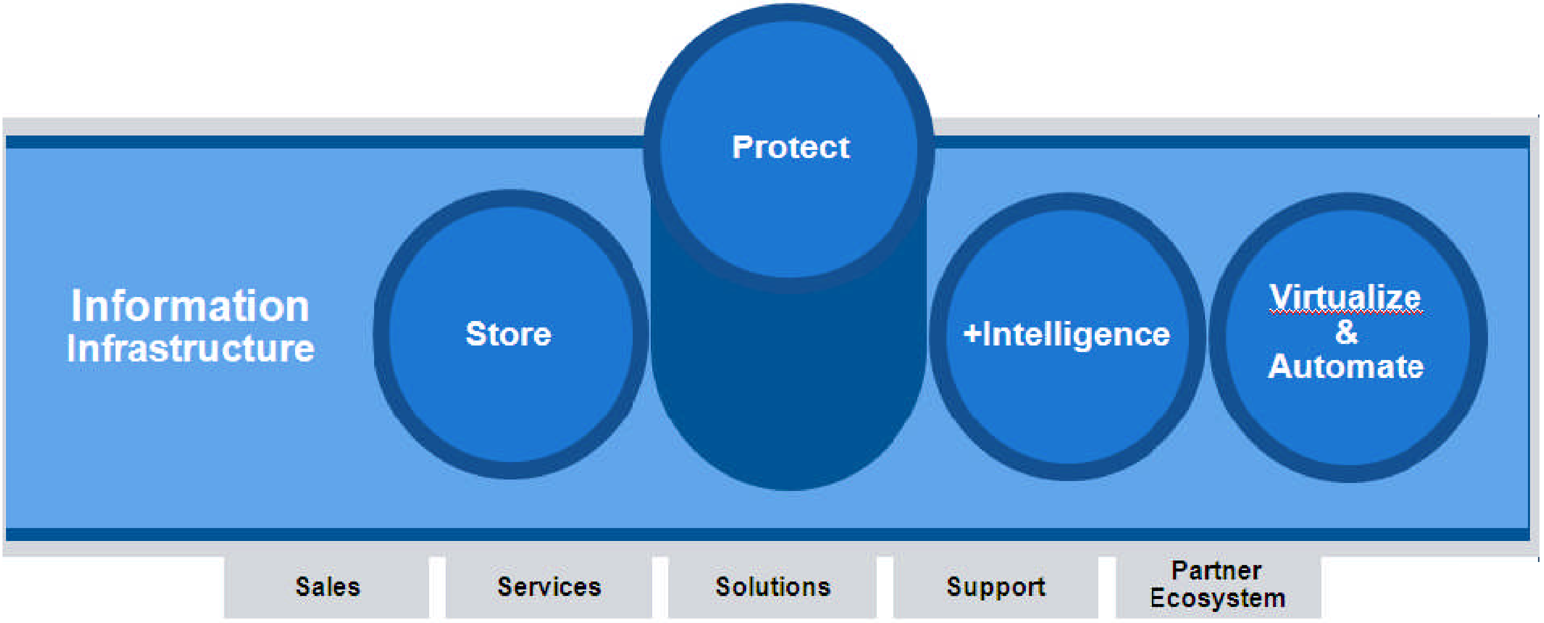
Dan Reddy, (CISSP, CSSLP)
Product Security Office
EMC Corporation

DoD-DHS-NIST
Software Assurance Forum
Measuring Software Supply
Chain Risk
Panel Briefing
November 4, 2009
Arlington, VA

EMC²
where information lives®

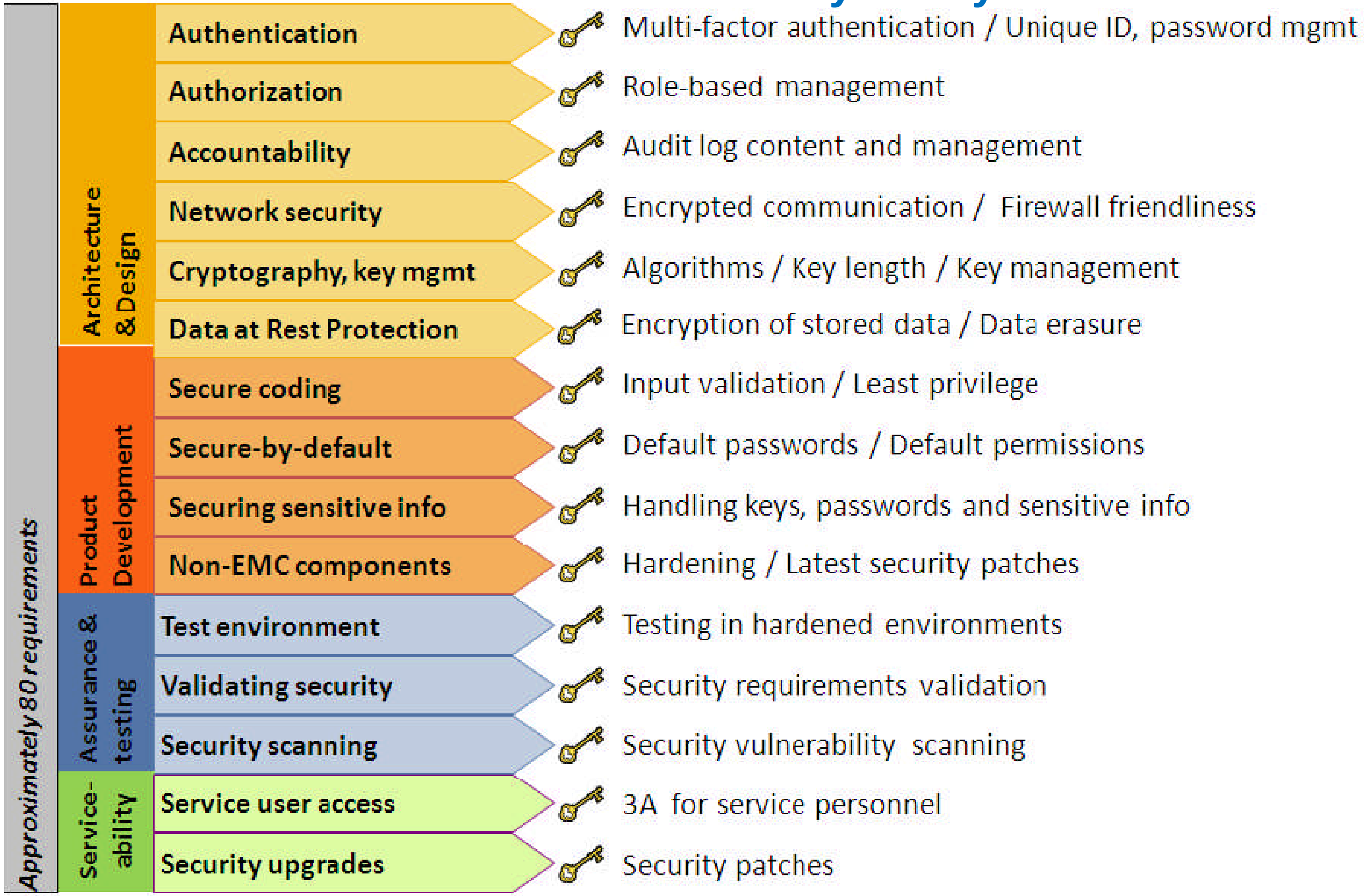
EMC Corporation at a Glance

Revenues *(2008):*	**$14.9 billion**
Net Income *(2008):*	**$1.4 billion**
Employees *(end Q2 2009 worldwide):*	**≈ 41,500**
Countries where EMC does business:	**> 80**
Founded:	**1979**



Assess Security of Current Products

EMC Product Security Policy v2



Approximately 80 requirements

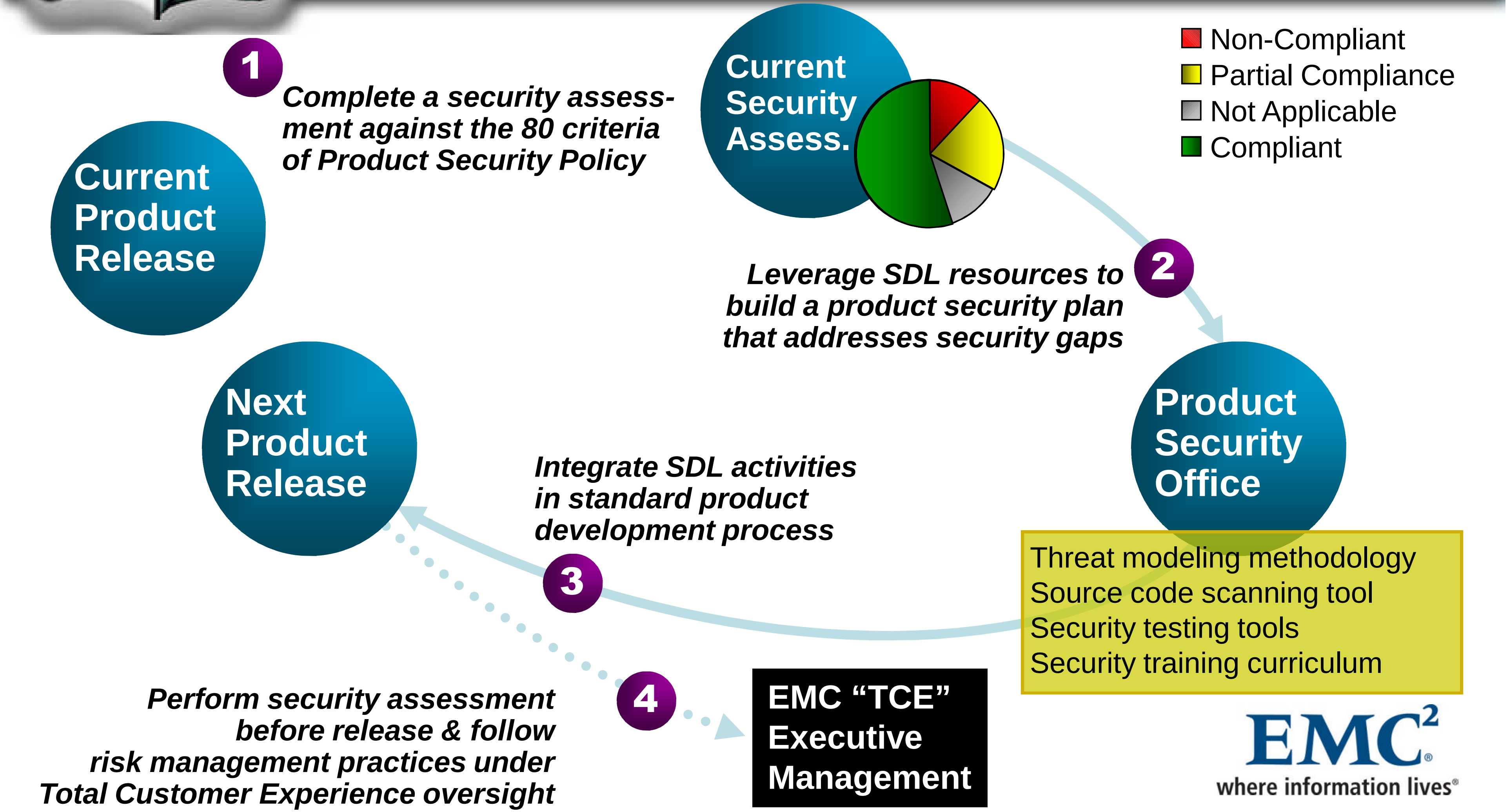
Architecture & Design	Authentication	Multi-factor authentication / Unique ID, password mgmt
	Authorization	Role-based management
	Accountability	Audit log content and management
	Network security	Encrypted communication / Firewall friendliness
	Cryptography, key mgmt	Algorithms / Key length / Key management
	Data at Rest Protection	Encryption of stored data / Data erasure
Product Development	Secure coding	Input validation / Least privilege
	Secure-by-default	Default passwords / Default permissions
	Securing sensitive info	Handling keys, passwords and sensitive info
	Non-EMC components	Hardening / Latest security patches
Assurance & testing	Test environment	Testing in hardened environments
	Validating security	Security requirements validation
	Security scanning	Security vulnerability scanning
Service-ability	Service user access	3A for service personnel
	Security upgrades	Security patches

EMC²
where information lives®

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Product Security Development Lifecycle (SDL)



Current Product Release

1 *Complete a security assessment against the 80 criteria of Product Security Policy*

Current Security Assess.

🟥 Non-Compliant
🟨 Partial Compliance
⬜ Not Applicable
🟩 Compliant

2 *Leverage SDL resources to build a product security plan that addresses security gaps*

Product Security Office

Threat modeling methodology
Source code scanning tool
Security testing tools
Security training curriculum

Next Product Release

3 *Integrate SDL activities in standard product development process*

4 *Perform security assessment before release & follow risk management practices under Total Customer Experience oversight*

EMC “TCE” Executive Management

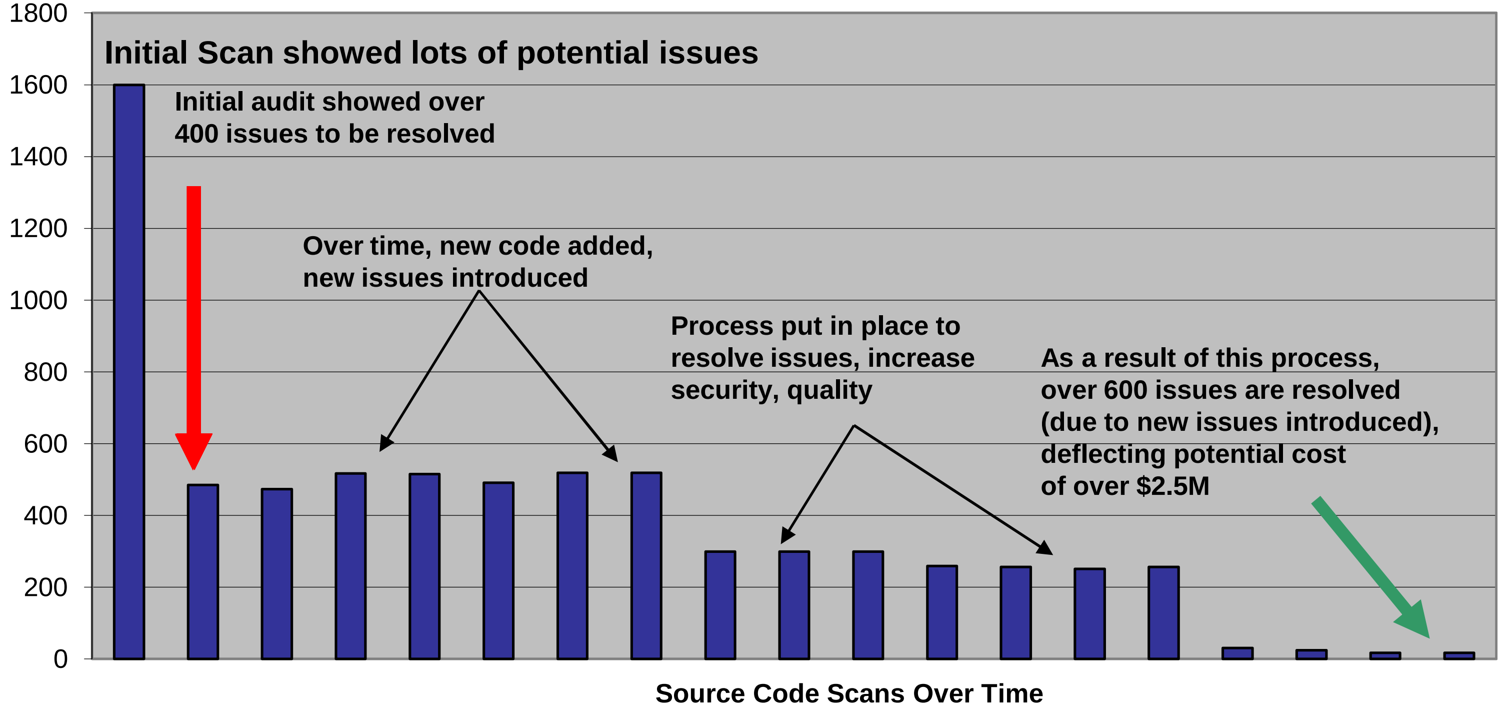
EMC² where information lives®

“Improve Phase”: Outcome Measurement

Phase Overview	Define	Measure	Analyze	Improve	Control	Realize

EMC
Lean Six Sigma

Hot Issues found in Product after Scans



Initial Scan showed lots of potential issues

Initial audit showed over 400 issues to be resolved

Over time, new code added, new issues introduced

Process put in place to resolve issues, increase security, quality

As a result of this process, over 600 issues are resolved (due to new issues introduced), deflecting potential cost of over $2.5M

- Established a formula *(with Finance Approval)* to calculate improvement $ gain for every Security “Gap” point closed.

EMC²
where information lives®

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

4 November 2009

DoD-DHS-NIST
Software Assurance Forum
Measuring Software Supply Chain Risk
Panel Briefing

Presented By: Cheryl Jones

US Army RDECOM

Practical Software and Systems Measurement

www.psmsc.com

Homeland Security

- If we are going to measure software assurance, we need to be assured of the measures….

Measurement Environment

- Multiple suppliers (for profit companies, government organizations), with a variety of trade-off factors
- Multiple technical and management processes
- Multiple perspectives (measurement definitions, methodologies, assumptions)
- Multiple concepts of “assurance”
- They produce and provide the acquirer the measurement data
- How do we know we can use it to make procurement decisions?
  - Assess the risk profile(s) of the supplier’s product
  - Match the risk to our system/user environment/requirements

Key Concepts

- Trust, but verify
  - Product Assurance Standards (attribute charateristics)
  - Independent acquirer analysis of the data
- Understand what the numbers are telling you:
  - Definitions - what is included / what is not
  - Audit trail from measure(s) to assurance attribute (information model)
  - System context - applicability

- Adherence to standards
  - Applicable in development / operations context (process, software, systems characteristics, user environment)
- History of product security anomalies (security “defects” in use)
- Need a measurement process

Measuring Software Assurance

- Proven measurement principles still apply
- You need to know what the product data means in the context of your system requirements
- Product assurance measurement results aligned with prioritized system and software assurance requirements