



Creating Value from Vulnerability

Tony Sager
Chief, Vulnerability Analysis & Operations Group
Information Assurance Directorate
National Security Agency

Information Security and Practice Advisory Board
September 6-7 2007



NSA Information Assurance



Coming From	Moving to
Protect classified information	and real-time defense of information & systems
Focus on GOTS crypto	Broad spectrum of COTS IA & IT
More products than services	More services than products, and more influence than "doing"
Avoid risk	Manage risk
Find & mitigate vulnerability	and detect the threat



- Improve the security of Commercial Technology
- Influence all stakeholders:
 - Practitioners, Buyers, Users, Suppliers, Authorities
- Increase partnership
- Build a Knowledge vs Product Business
- Bring a dynamic, operational focus



VAO Vision



The nation's most capable, influential, and trusted source of actionable information on network vulnerabilities and intrusions.



VAO Mission



- Conduct operations to find vulnerabilities in
 - All stages of the life cycle of technology
 - The operational environment
 - Content (networking, signals, space...)
- Analyze vulnerabilities
 - In emerging technologies
 - In core concepts
- Translate vulnerability knowledge
 - Into guidance and countermeasures
 - To understand root causes
- Lead the community
 - In the development of security guidance, training, education and standards development



VAO in the News



washingtonpost.com

The Washington Post

Today's Paper | Subscribe | DostPoints



FROM THE MAGAZINE



Government Computer News











Suppliers

Buyers

Users





Suppliers

Buyers

Users

Practitioners

NSA, DISA, NIST, Center for Internet Security





Suppliers

Buyers

Users

DISA STIGs, NIST Checklists, Corporate baselines





Suppliers

Buyers

AF, DOD, Standard desktop load

Users



OS Vendors, Tool Vendors, Compliance Checkers

Suppliers

Buyers

Users



DoD Policy, OMB, FISMA, Security Content Automation Program (SCAP)

Authorities

Suppliers

Buyers

Users



Vulnerability "Plumbing"



"CONTENT"

New IT vulns

Security
Guides &
benchmarks

Red and Blue Team Reports

Product tests

Incident reports

"PLUMBING"

CVE

OVAL

CCE, CPE

CVSS

XCCDF

"FIXTURES"

Multiple tools to measure, fix, report

Integrated reports

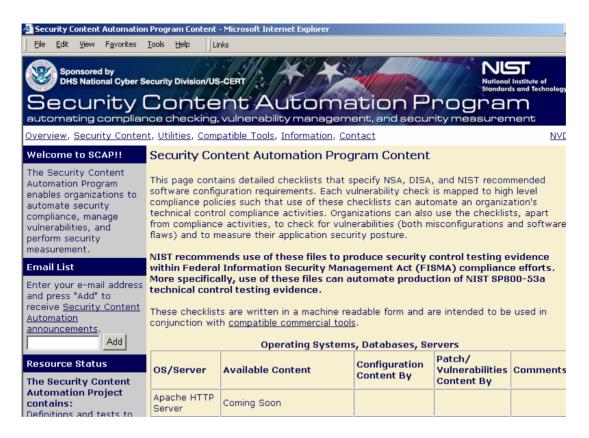
Integrated tools

Policy compliance

Rapid vuln sharing, assessment, remediation

Security Content Automation (SCAP)

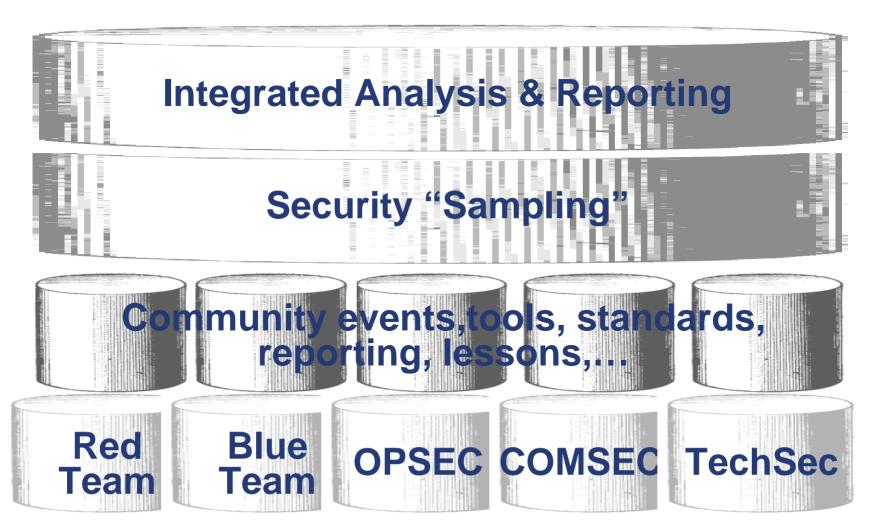
 ... to automate compliance, manage vulnerabilities and perform security measurement





Towards Information Sharing







To gain assurance, we must



- Organize... the data generators
- Standardize... the raw data
- Translate... into something useful upstream
- Link to... other business areas
 - e.g., network management, compliance



- Bring content
 - and good people to the conversation
- Equip and organize the stakeholders
 - -esp. the Buyers
- Abstract the interfaces



To learn more...



- NSA Security Guidance
 - http://www.nsa.gov/snac/
- The Security Content Automation Program
 - http://nvd.nist.gov/scap/scap.cfm
- Common Vulnerability & Exposures
 - http://cve.mitre.org
- The Center for Internet Security
 - http://cisecurity.org