



# **Creating Value from Vulnerability**

**Tony Sager**

**Chief, Vulnerability Analysis & Operations Group**

**Information Assurance Directorate**

**National Security Agency**

**Security Automation Workshop**

**September 2007**



# VAO Vision



## Vulnerability Analysis & Operations Group

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



# VAO in the News



washingtonpost.com

The Washington Post

Today's Paper | [Subscribe](#) | [PostPoints](#)

GOVEXEC.COM

FROM THE MAGAZINE

GCN

Government Computer News



InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

InformationWeek

FCW.COM





# Stakeholders in Assurance



**Authorities**

**Suppliers**

**Buyers**

**Users**

**Practitioners**



# Stakeholders in Assurance



**Authorities**

**Suppliers**

**Buyers**

**Users**

**Practitioners**

**NSA, DISA, NIST, SANS,  
Center for Internet  
Security, etc...**



# Stakeholders in Assurance



**Authorities**

**Suppliers**

**Buyers**

**Users**

**DISA STIGs, NIST  
Checklists, Corporate  
baselines, etc.**

**Practitioners**



# Stakeholders in Assurance



**Authorities**

**Suppliers**

**Buyers**

**AF, DOD,**

**USG Standard desktop**

**Users**

**Practitioners**



# Stakeholders in Assurance



**Authorities**

**OS Vendors, Tool  
Vendors, Compliance  
Checkers**

**Suppliers**

**Buyers**

**Users**

**Practitioners**



# Stakeholders in Assurance



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

**Authorities**

**Suppliers**

**Buyers**

**Users**

**Practitioners**



# Vulnerability “Plumbing”



## “CONTENT”

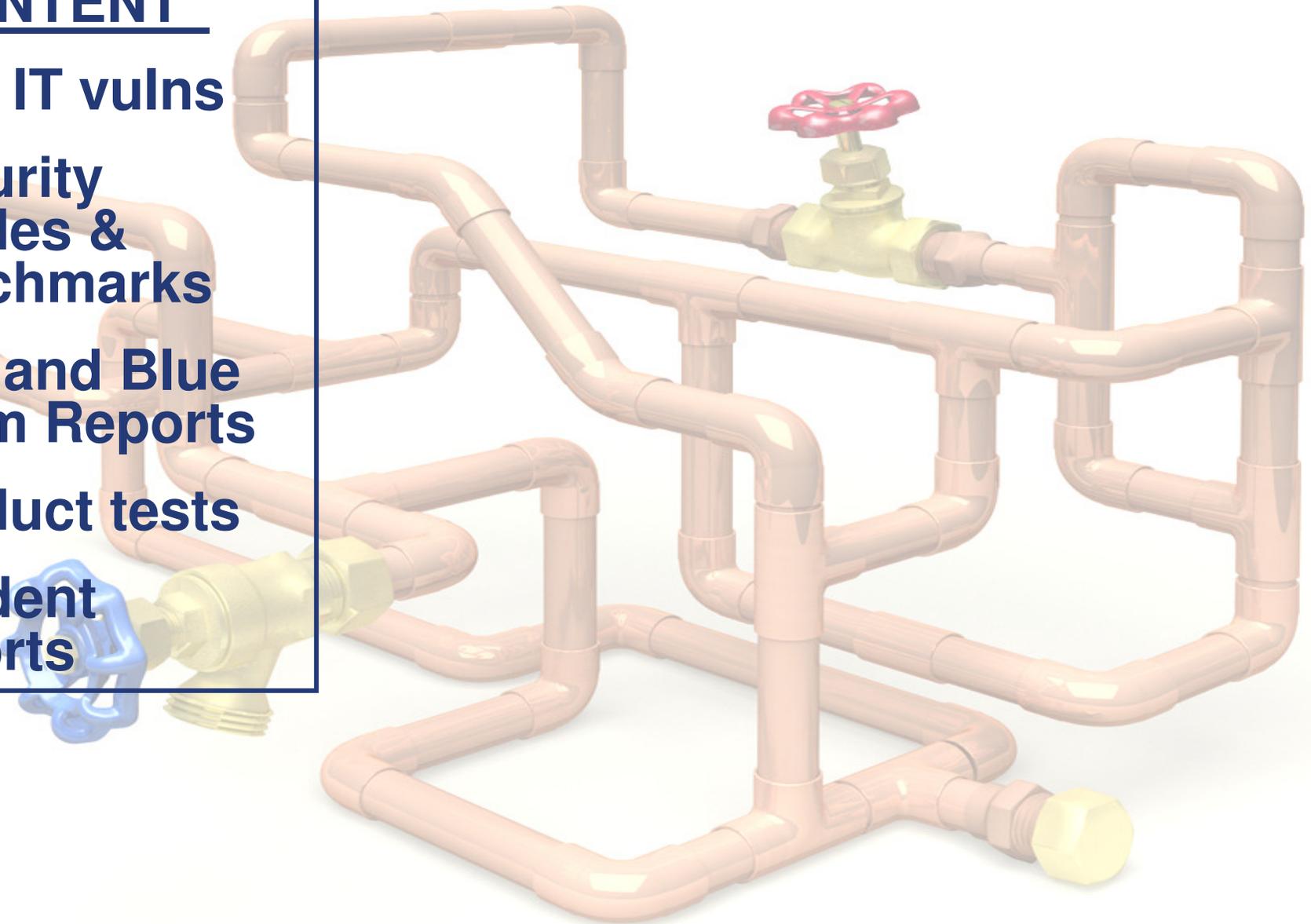
**New IT vulns**

**Security  
Guides &  
benchmarks**

**Red and Blue  
Team Reports**

**Product tests**

**Incident  
reports**





# 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

-----



# Vulnerability “Plumbing”



## “CONTENT”

New IT vulns

Security Guides  
& benchmarks

Red and Blue  
Team Reports

Product tests

Incident reports

Net Mgmt info

## “PLUMBING”

CVE

OVAL

CCE

CPE

CVSS

XCCDF

-----

## “FIXTURES”

Multiple tools to  
measure, fix,  
report

Integrated reports

Integrated tools

Policy  
compliance

Rapid sharing,  
assessment,  
remediation



# Security Content Automation (SCAP)



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

Security Content Automation Program Content - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

## Security Content Automation Program

automating compliance checking, vulnerability management, and security measurement

[Overview](#), [Security Content](#), [Utilities](#), [Compatible Tools](#), [Information](#), [Contact](#) [NVC](#)

**Welcome to SCAP!!** Security Content Automation Program Content

The Security Content Automation Program enables organizations to automate security compliance, manage vulnerabilities, and perform security measurement.

This page contains detailed checklists that specify NSA, DISA, and NIST recommended software configuration requirements. Each vulnerability check is mapped to high level compliance policies such that use of these checklists can automate an organization's technical control compliance activities. Organizations can also use the checklists, apart from compliance activities, to check for vulnerabilities (both misconfigurations and software flaws) and to measure their application security posture.

**Email List**

Enter your e-mail address and press "Add" to receive [Security Content Automation](#) announcements.

**Resource Status**

The Security Content Automation Project contains:  
Definitions and tests to

**NIST recommends use of these files to produce security control testing evidence within Federal Information Security Management Act (FISMA) compliance efforts. More specifically, use of these files can automate production of NIST SP800-53a technical control testing evidence.**

These checklists are written in a machine readable form and are intended to be used in conjunction with [compatible commercial tools](#).

**Operating Systems, Databases, Servers**

OS/Server	Available Content	Configuration Content By	Patch/Vulnerabilities Content By	Comments
Apache HTTP Server	Coming Soon			



## **SCAP is *so cool...***



- *It requires cooperation AND it forces cooperation*
- *We must think about the enterprise*
- *Brings the security community together to voice and document opinions*
- *We can manage our systems cleverly AND comply*
- *The government cooperation with vendors is more “natural”*



## ***SO much left to do...***



- *We have new problems....*
  - *content generation*
  - *Governance*
  - *Systems engineering*
  - *resources*
  
- *What are the new opportunities, new links?*



- ***Develop and bring content***
  - and good people
- ***Equip and organize the stakeholders***
  - esp. the Buyers
- ***Abstract the interfaces***