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

CMP
InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY
Information Week

FCWCOM

SC MAGAZINE AWARDS 2007

Stakeholders in Assurance

Stakeholders in Assurance

Authorities

Suppliers

Buyers

Users

Practitioners

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

Stakeholders in Assurance

Authorities

Suppliers

Buyers

Users

Practitioners

DISA STIGs, NIST Checklists, Corporate baselines, etc.

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

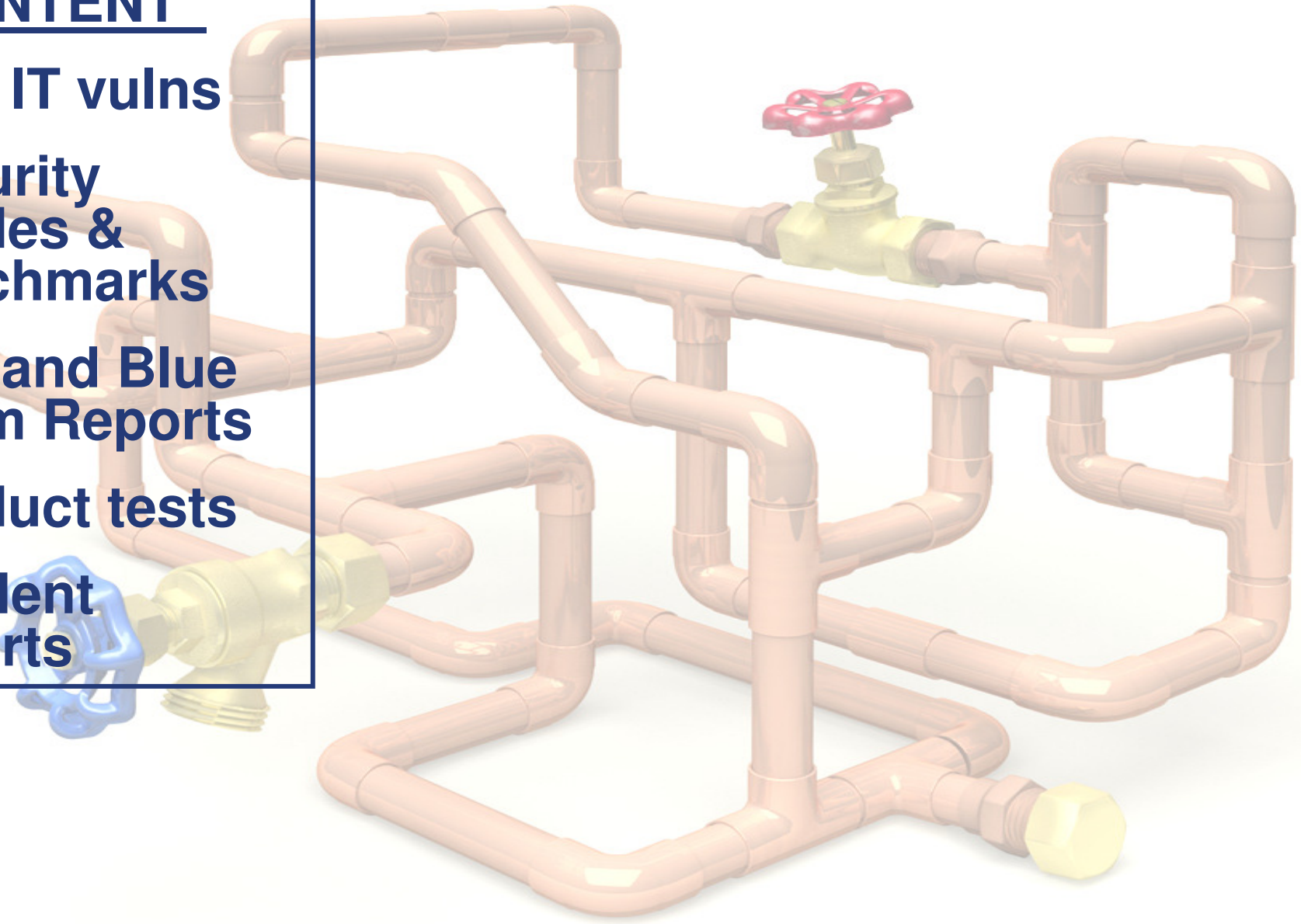
Users

Practitioners

Vulnerability "Plumbing"

"CONTENT"

- New IT vulns
- Security Guides & benchmarks
- Red and Blue Team Reports
- Product tests
- Incident reports



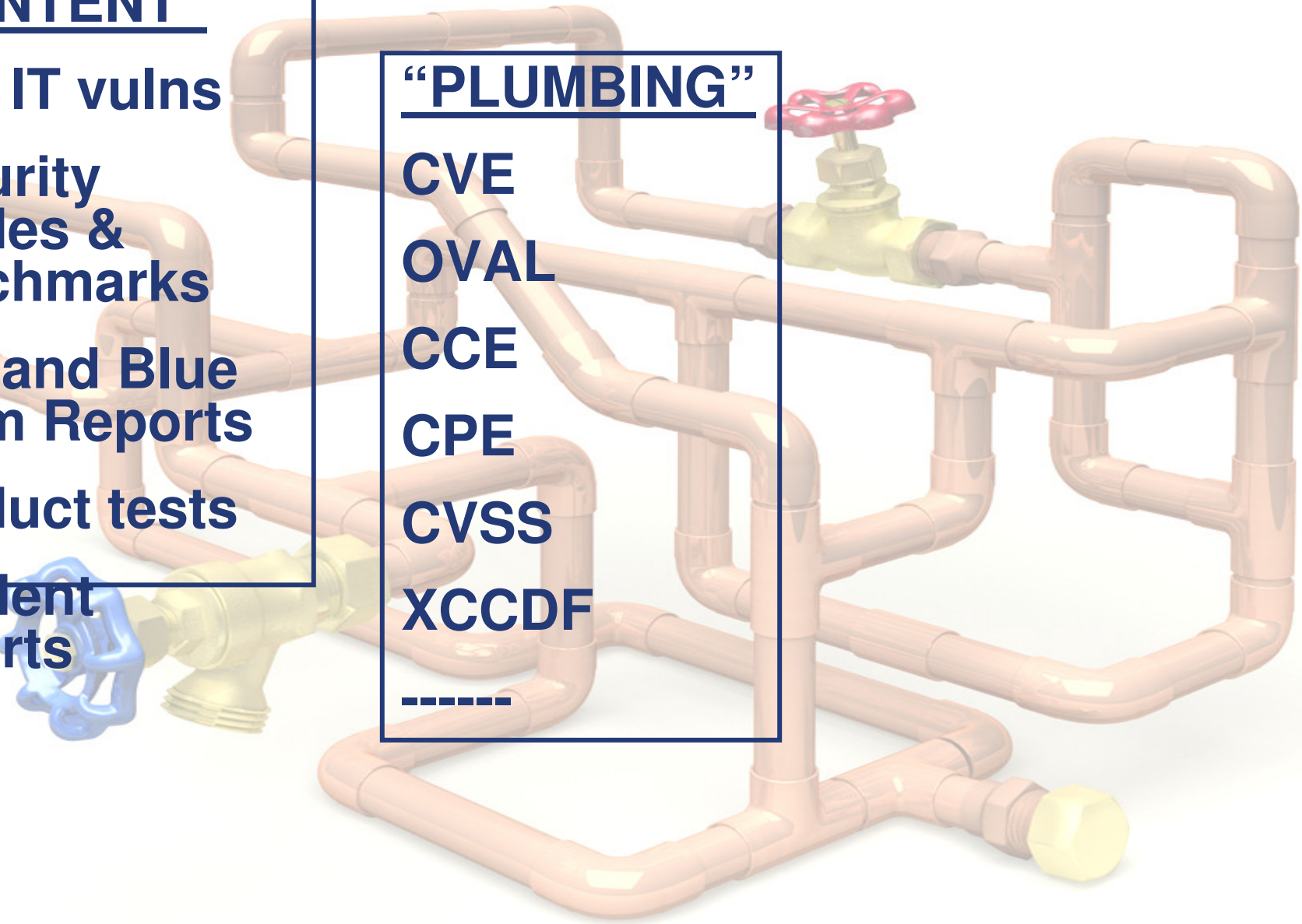
Vulnerability "Plumbing"

"CONTENT"

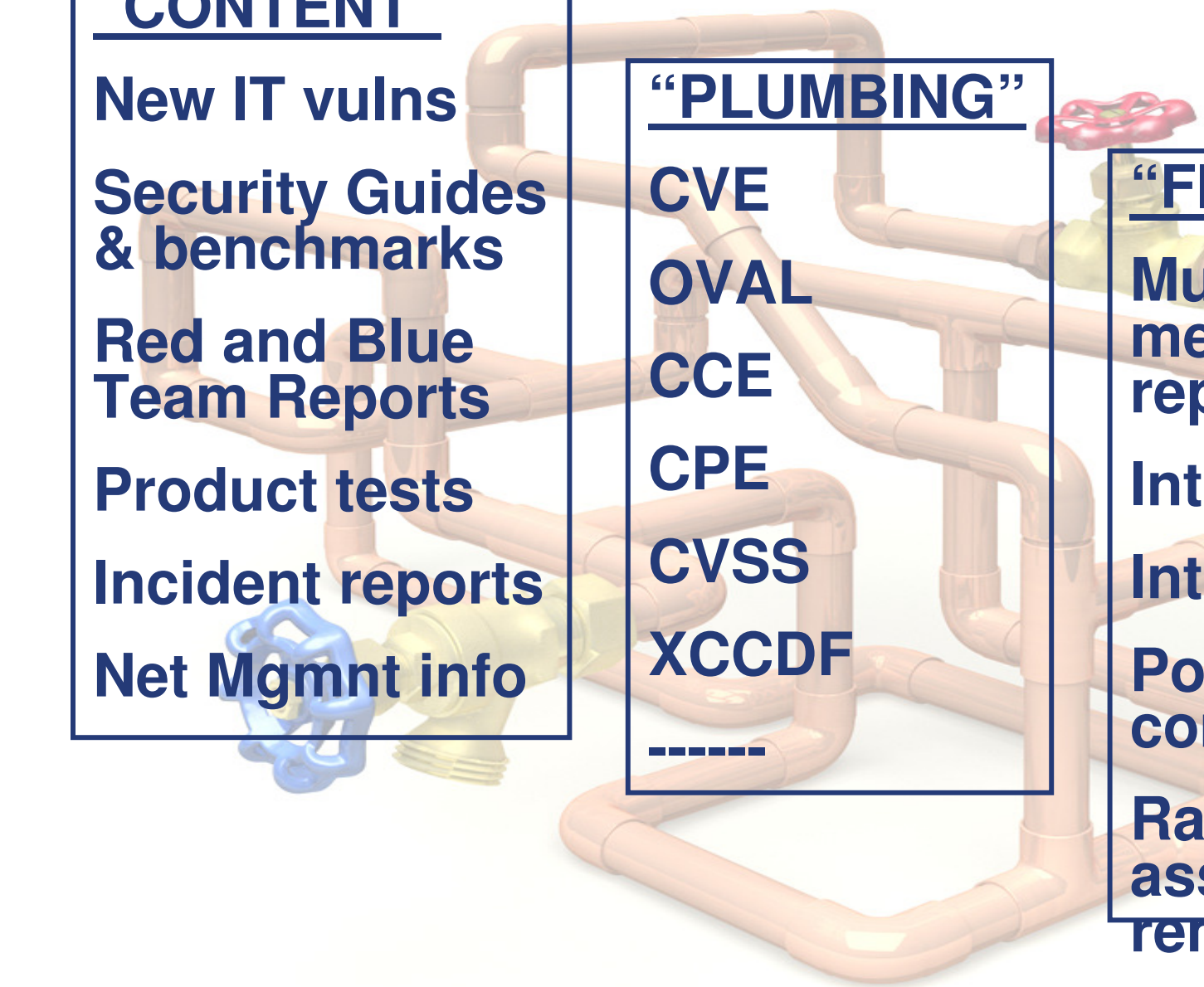
- New IT vulns
- Security Guides & benchmarks
- Red and Blue Team Reports
- Product tests
- Incident reports

"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 Mgmnt 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

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?*

Government–Private Partnership

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