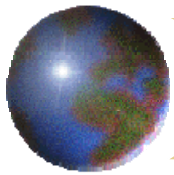
Security Content Automation

Tony Sager
Chief, Vulnerability Analysis & Operations Group
Information Assurance Directorate
National Security Agency
NIST Workshop September 2006

“The reason for collecting, analyzing and disseminating information on a disease is to control that disease. Collection and analysis should not be allowed to consume resources if action does not follow.”

William H. Foege, MD et al,

International Journal of Epidemiology 1976; 5:29-27



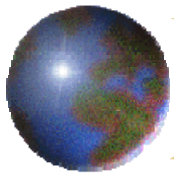
"Every computer in the DoD is configured as securely as possible, all of the time, and the right people know that this is so (or not so)."

Lt. Gen Harry Raduege

DIR DISA and CMDR JTF/GNO

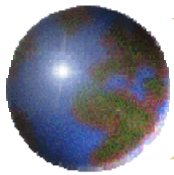
Idealized VM Process

- Unique and consistent identification of vulnerabilities
- Expert agreement on security practice
- Implemented in tools to measure and manage
- Reporting that is well-defined and easily aggregated
- Reporting based on “real sensors”
- Rapid notification of new vulnerabilities and actions



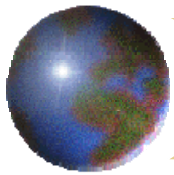
As long as we're dreaming….

- Integrated with NW management tools; but model-neutral.
- Self-help for sys admins, with enterprise reporting
- 90% "out of the box"
- Standards-based, vendor-neutral, open framework ("technical plumbing")
- Clear mapping to policy and compliance



"Plumbing" should connect…

- Security Analysis --> Knowledge & Benchmarks
- Benchmarks --> Operational Configuration
- Operational Configuration --> Implementation
- Implementation --> Measurement, Management
- Management --> Reporting on State, Compliance
- New Information --> Tests, Actions, Situational Awareness



Building the framework ("plumbing")

- ***Standard naming***
  - CVE (Common Vulnerabilities and Exposures)
- ***Standard tests***
  - OVAL (Open Vulnerability Assessment Language)
- ***Best Practice configurations***
  - Consensus Security Benchmarks (e.g., NSA, NIST, DISA, SANS, CIS)
- ***Automation of configurations***
  - XCCDF: eXtensible Configuration Checklist Description Format

Security Content Automation

Tony Sager
Chief, Vulnerability Analysis & Operations Group
Information Assurance Directorate
National Security Agency
NIST Workshop September 2006