

### **The OpenSCAP Project**

Steve Grubb, Red Hat Kevin Sitto, G2



### What is open scap?

- Open Source Library
- Free to integrate under LGPL
- Cross Platform
- Multiple Languages supported
- Unicode tested



# **A Little History**

IDS Presentation at ISAP/SCAP last year

#### IDMEF

- Designed for NIDS
- HIDS concepts poor fit
- 2.0 needed?
- Sectool



# History (cont.)

- Reviewed other projects
- Started open scap project



### **Project Goals**

- Make the standards easier to implement through open libraries and code samples.
- Work with tool communities to build SCAP standards and models into their offerings.



# Collaborating

- Source Code Repository
  - cvs / svn / git

#### Momentum

Teleconferences / Mail list / IRC

### Coding Standards

#### Source Code Submissions

• zip / tar / file / patch



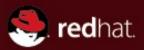
# **Collaborating (cont.)**

### Licence choices

- BSD / GPL / LGPL
- Focus
  - Get involved with standards community
  - Crank out code for ratified standards

### Getting all developers on track

- Wiki pages to organize information
- Keeping the community together on end goal



# The Design



### **SCAP Barriers to Entry**

- Basic FDCC: XYZ LOC
- Full SCAP: XYZ LOC
- Spec:
  - OVAL: ~400 Pages
  - XCCDF: 132 Pages



# **Design Core**

- Separate library for each standard
- Decouple Ingestion from Interpretation
- ANSI C for Cross Platform Support



# **Eating the Elephant**

- Query
- Compare
- Apply



# Integration

- Library Bindings
- Daemon Integration



# **Status**



### **Current State**

### Libraries available in

- Fedora 11 and higher
- Debian
- Will be in RHEL6 GA
- Windows Compilation and Configuration Challenges
- **OVAL Probes needed for other platforms**



### **Future Work**

### Bindings for other languages

- C++
- Java

### Adoption of newer SCAP standards as the are ratified

- ORML
- CEE



# Future Work (cont.)

- Integration with applications
- XCCDF to kickstart
- Policy Editors
- Adhoc query tool
- System Integrity Scanning
  - At boot up
  - At network connect
  - Hypervisor inspect guest OS on startup

### Systems Management Tools

- JBoss Operations Network (JON)
- Satellite
- Puppet



# **Community Participation**

#### Web

www.open-scap.org

#### Mail List

www.redhat.com/mailman/listinfo/open-scap-list

### IRC

#openscap on freenode.net

#### Tutorial

• Thursday, 1:15 - 3:15



### **Questions?**

### Steve Grubb <sgrubb @redhat.com> Kevin Sitto <Kevin.Sitto @g2-inc.com>