SCAP Security Guide

https://github.com/OpenSCAP

SHAWN WELLS, RED HAT
SHAWN@REDHAT.COM
WELLSHAW@NRO.IC.GOV
443-534-0130

30 MINUTES, 3 GOALS

- Detail Security Automation Technology + Initiatives
  - Native Tooling [OpenSCAP]
  - Configuration Compliance [SCAP Security Guide]
  - Remediation & Tailoring [currently scripts, future Ansible]
- Live Demo
  - Configuration Compliance Scanning
  - C&A Paperwork generation

OVERVIEW

- Delivers practical security guidance, baselines, and associated validation mechanisms using the Secure Content Automation Protocol (SCAP)
  - Current content for Red Hat Enterprise Linux ,JBoss, JRE….
  - Prioritizing future content based on community input
- Current upstream source for STIG and SNAC Guides
  - DISA JBoss Enterprise Application Platform STIG
  - DISA Red Hat Enterprise Linux 6 & 7 STIGs
  - National Security Agency SNAC Guide
  - Department of Justice CJIS Baselines

OVERVIEW

- The SSG represents a comprehensive catalog of security controls
- Metadata maps specific rules to formalized policies
  - NIST 800-53
  - DISA OS SRG
  - CCE's
- XSL Transformations generate profiles
  - "Show me all the rules tagged with DISA OS SRG so I can make a STIG"
  - "Show me all the rules I need for a NIST 800-53 H/L/L system"

OPEN SOURCE BENEFITS

- Powerful collaboration tools available
  - Wiki, mailing list, ticketing system, versioning systems
  - Permit and encourage internet-wide collaboration
  - Change is transparent, and accountable
- Enables transparent collaboration
  - Direct vendor, system Integrator, and industry partner involvement
  - Speeds content development and testing
  - Reduces government waste, centralizes baseline development

YES, GOVERNMENT CAN CONTRIBUTE!

- Worked with NSA General Council and Red Hat to update Fedora Contributor Agreement

Fedora.

4. Public Domain United States Government Works.

Sections 1 through 3 of this FPCA do not apply to any Contribution to the extent that it is a work of the United States Government for which copyright is unavailable under 17 U.S.C. 105.

5. Acceptance

SSG COMMUNITY

Author	Commits (%)	+ lines	- lines
Shawn Wells	171 (12.30%)	329366	296736
Jeffrey Blank	372 (26.76%)	242509	141519
Michael Moseley	175 (12.59%)	21116	15961
Kevin Spargur	81 (5.83%)	8012	1775
Kenneth Peeples	6 (0.43%)	5768	5439
Maura Dailey	53 (3.81%)	3316	3968
David Smith	68 (4.89%)	1816	830
Willy Santos	344 (24.75%)	1718	733
kspargur	3 (0.22%)	584	92
Mike Palmiotto	1 (0.07%)	359	1
mmosel	3 (0.22%)	181	195
Michele Newman	71 (5.11%)	168	166
Spencer Shimko	5 (0.36%)	165	117
Michael Palmiotto	8 (0.58%)	149	44
Michael McConachie	15 (1.08%)	145	78
Kenneth Stailey	3 (0.22%)	79	52
Jeff Blank	6 (0.43%)	74	18
Joe Nall	3 (0.22%)	62	64
Simon Lukasik	1 (0.07%)	1	1
root	1 (0.07%)	0	16

Domains	Total (%)
redhat.com	683 (49.14%)
eclipse.ncsc.mil	673 (48.42%)
tresys.com	14 (1.01%)
gmail.com	9 (0.65%)
nall.com	3 (0.22%)
kspargur.csb	3 (0.22%)
kde.example.com	3 (0.22%)
rhel6.(none)	1 (0.07%)
fornax.eclipse.ncsc.mil	1 (0.07%)

SSG COMMUNITY

- In a Nutshell, the community…..
  - .... Has had 3,208 commits from 107 contributors, representing over 1.2M lines of code
  - .... Has participation from all cabnet-level agencies
  - .... Commercially shipping in Enterprise Linux

SSG DEVELOPMENT ROADMAP

DISA STIG, VERSION 1, RELEASE 2, SECTION 1.1:

"The consensus content was developed using an open source project called SCAP Security Guide. The project's website is https://fedorahosted.org/scap-security-guide/.

Except for differences in formatting to accommodate the DISA STIG publishing process, the content of the RHEL6 STIG should mirror the SCAP Security Guide content with only minor divergences as updates from multiple sources work through the consensus process"


I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, IT'S DURING LIVE DEMOS
memegenerator.net