OPENS CAP COMMUNITY REVIEW

Automating Security Compliance

Shawn Wells
Chief Security Strategist
U.S. Public Sector
shawn@redhat.com | 443-534-0130
RHEL 5 STIG:

RHEL 6 STIG:

RHEL 7 STIG:
RHEL 5 STIG: 1,988 days

RHEL 6 STIG:

RHEL 7 STIG:
RHEL 5 STIG: 1,988 days
RHEL 6 STIG: 932 days
RHEL 7 STIG:
RHEL 5 STIG: 1,988 days
RHEL 6 STIG: 932 days
RHEL 7 STIG: 262 days

[vendor release]
OpenSCAP Community

http://www.open-scap.org/
https://github.com/OpenSCAP/
OpenSCAP Community

http://www.open-scap.org/
https://github.com/OpenSCAP/
In a nutshell, the OpenSCAP Community...

- has had **11,068 commits** from **142 contributors**, representing **1,961,708 lines of code**
- Averages **10 commits per day**, releases averaging 90 days
- Averages 60.3 code contributions per author (up from average of 13 in 2015!)
- Shipping in Red Hat Enterprise Linux!
“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”
<table>
<thead>
<tr>
<th>Month</th>
<th>Author</th>
<th>Commits %</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-12</td>
<td>Shawn Wells (Red Hat)</td>
<td>43.96%</td>
</tr>
<tr>
<td>2014-11</td>
<td>Jan Lieskovsky (Red Hat)</td>
<td>47.92%</td>
</tr>
<tr>
<td>2014-10</td>
<td>Gabe A. (Northrup)</td>
<td>40.91%</td>
</tr>
<tr>
<td>2014-9</td>
<td>Shawn Wells (Red Hat)</td>
<td>55.98%</td>
</tr>
<tr>
<td>2014-8</td>
<td>Dave Smith (NSA IAD)</td>
<td>46.53%</td>
</tr>
<tr>
<td>2014-7</td>
<td>Leland Steinke (DISA FSO)</td>
<td>75.00%</td>
</tr>
<tr>
<td>2014-6</td>
<td>David Smith (NSA IAD)</td>
<td>66.67%</td>
</tr>
</tbody>
</table>
Choose profile below:

**Default**
The implicit XCCDF profile. Usually, the default contains no rules.

**Standard System Security Profile**
This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

**Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7**
This is a *draft* profile for PCI-DSS v3

**Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)**
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

**Common Profile for General-Purpose Systems**
This profile contains items common to general-purpose desktop and server installations.

**Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server**
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.
Shipping (Government) Profiles

RHEL 6

- **C2S**: Collaboration with CIA and Amazon, derived from CIS
- **STIG**: Official RHEL6 STIG baseline, derived from OS SRG
- **CSCF**: Cross domain, derived from CNSSI 1253 CDS Overlay

RHEL 7

- **PCI**: Commercial baseline for financial services
- **STIG**: Vendor STIG submission
- **OSPP**: NIAP and NIST 800-53 derived
SCAP Workbench: GUI for tailoring
RHEL7 Discussion
WE CAN DO MORE WHEN WE WORK TOGETHER
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews