Security Automation: RHEL7 DoD STIG Update

Shawn Wells (shawn@redhat.com)
Chief Security Strategist &
Upstream Maintainer, OpenSCAP
Red Hat Public Sector

Ted Brunell (tbrunell@redhat.com)
Chief Architect, DoD Programs
Red Hat Public Sector

45 MINUTES, 3 GOALS (+15MIN Q&A)

1. **Detail Security Automation Technology & Initiatives**
    - Security Automation development initiatives (Red Hat + NSA + NIST)
    - RHEL7 STIG and DoD Secure Host Baseline Status

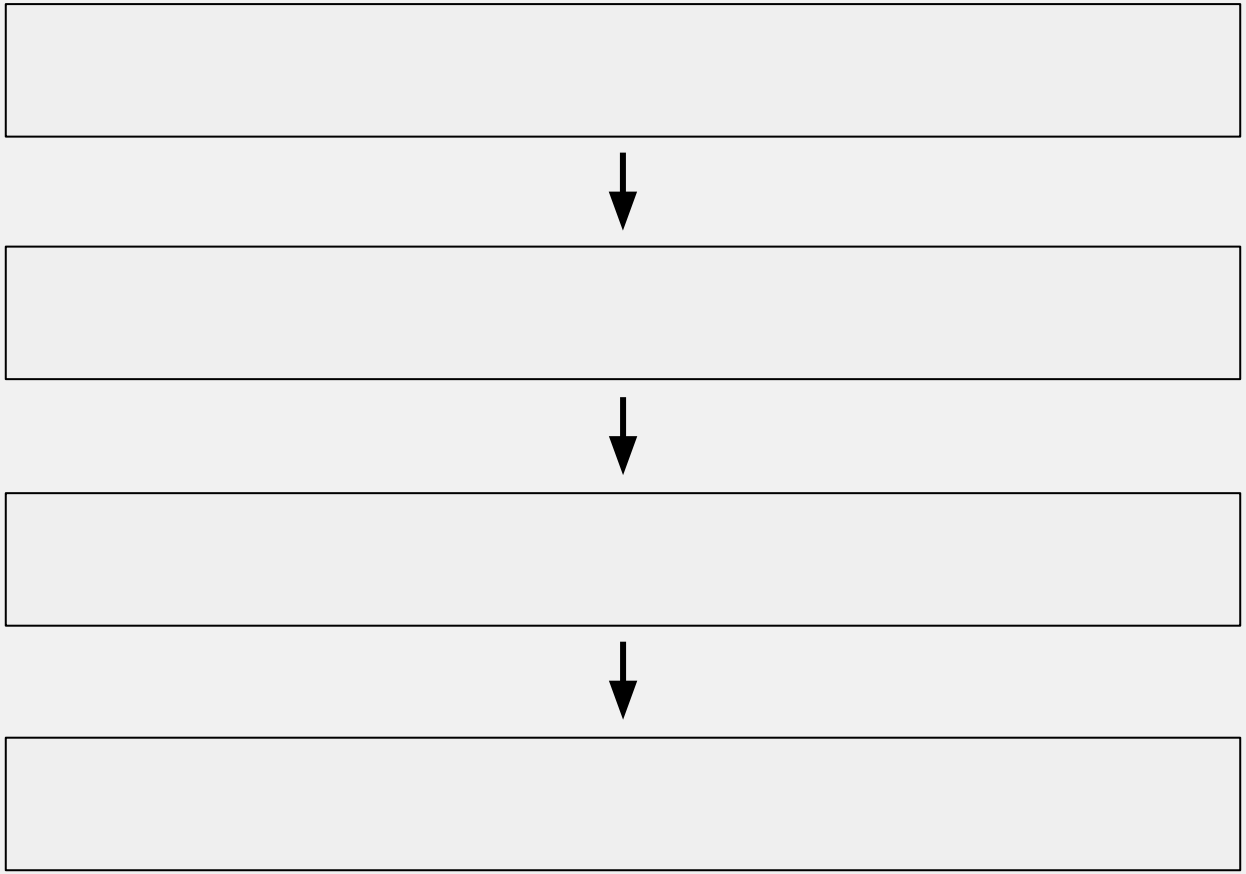
2. **Live Demos**
    - Demo #1
        i. Deploying Directly into STIG Compliance
        ii. Any other profiles available, like C2S?
        iii. What C&A paperwork can be automatically generated?
    - Demo #2
        i. Configuration Compliance Scanning (RHEL7 STIG)
        ii. Customized Compliance baselines with OpenSCAP Workbench
        iii. Certification/Accreditation Paperwork Generation

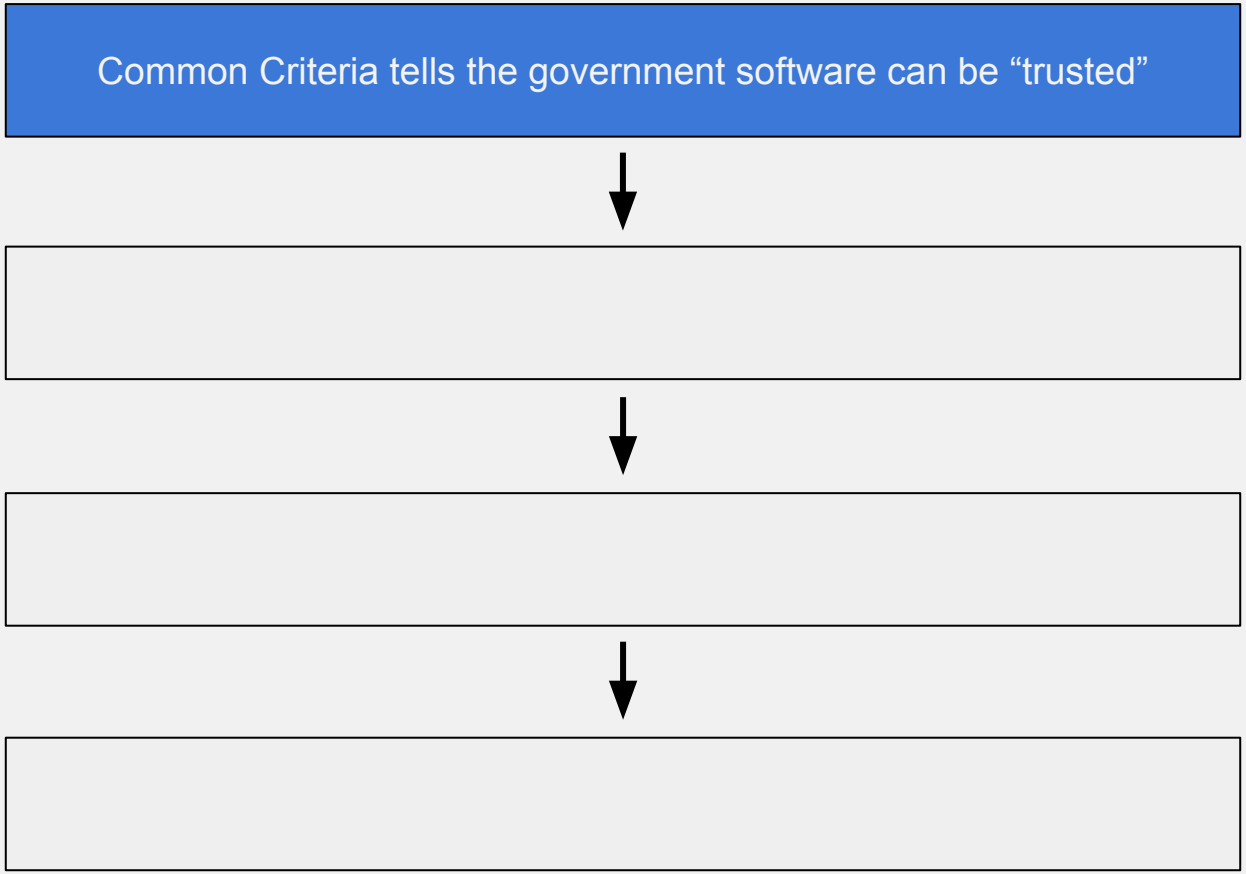
3. **Roadmap Discussion Intermixed (Gov't Plans, Packaging, Future Profiles)**

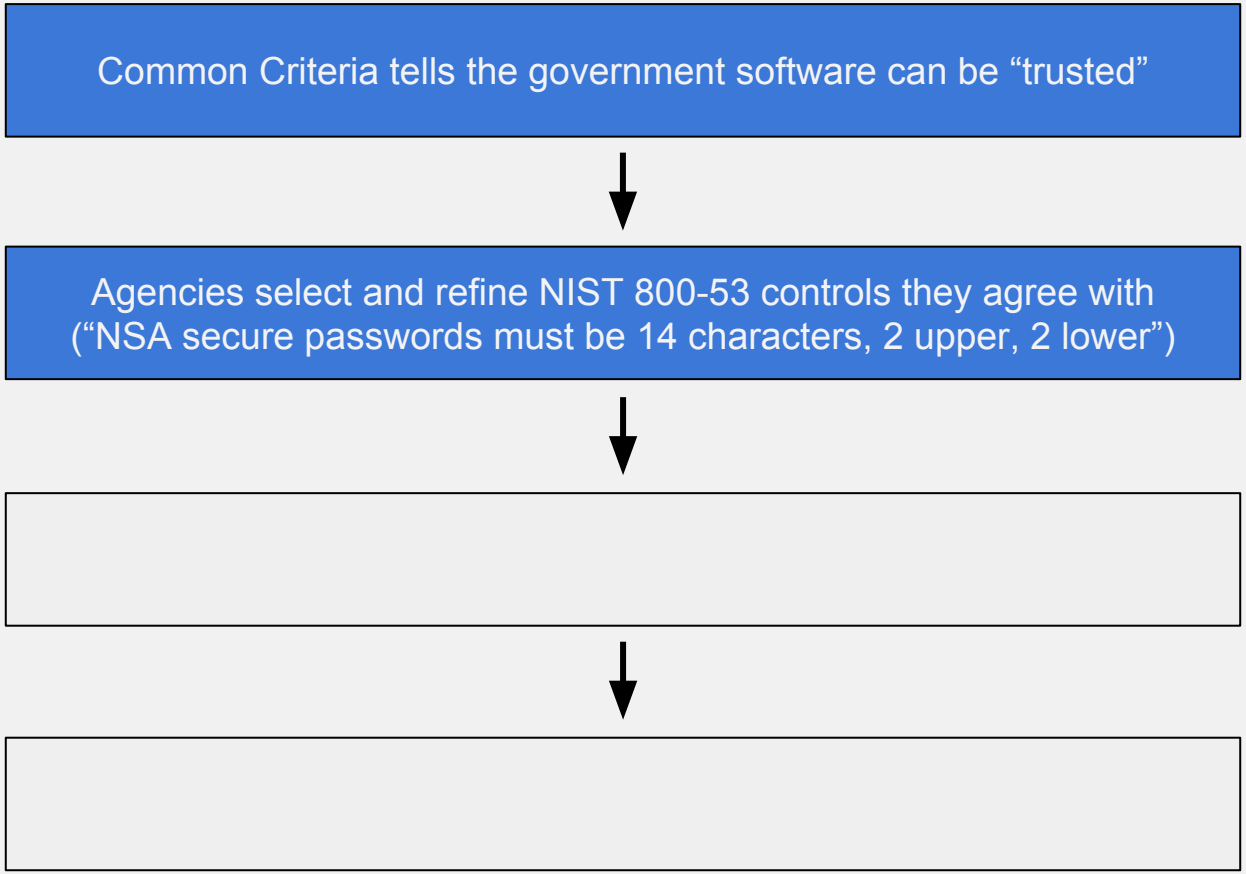
MOTIVATION: Red Hat Enterprise Linux 5 STIG

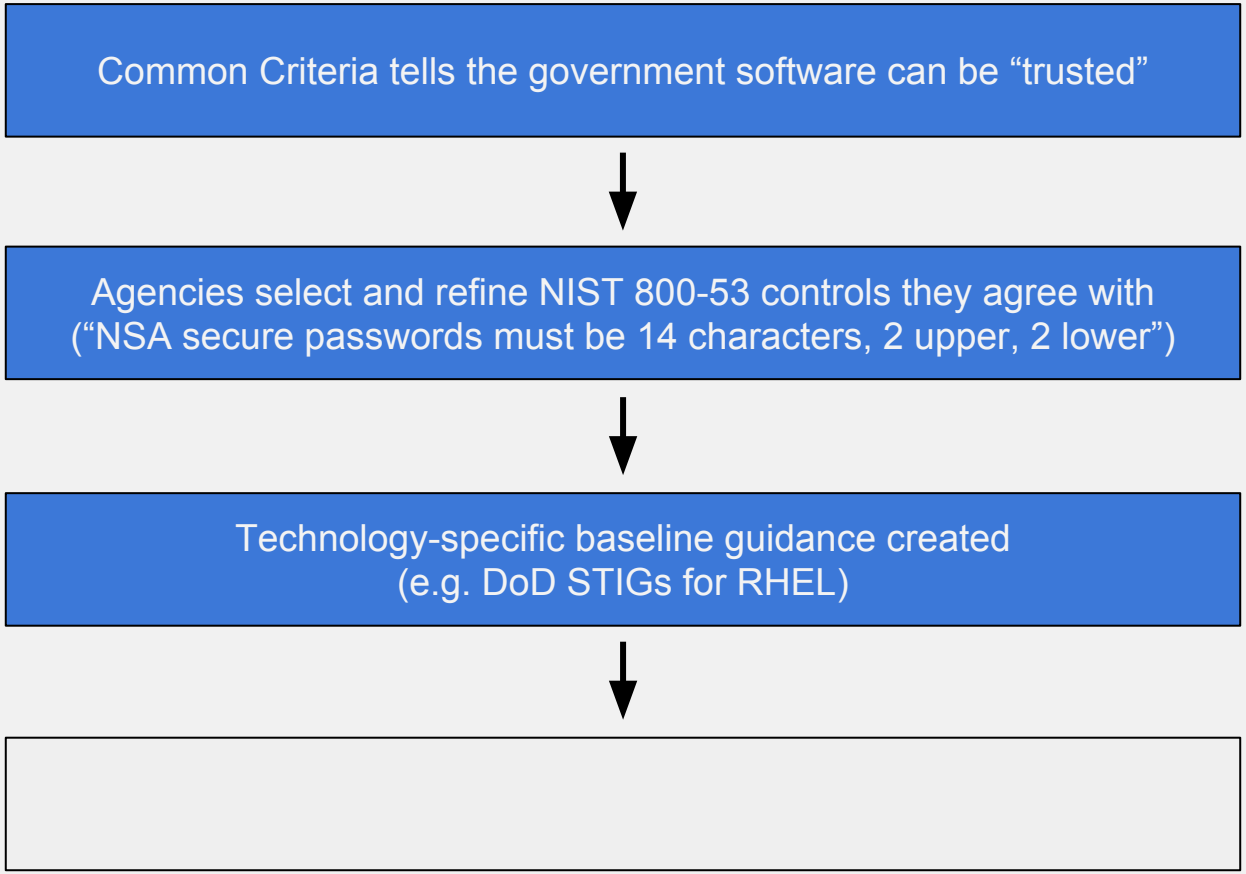
- 587 compliance checks
- No published automation, check everything by hand
- *Released 1,988 days after RHEL 5.0!*

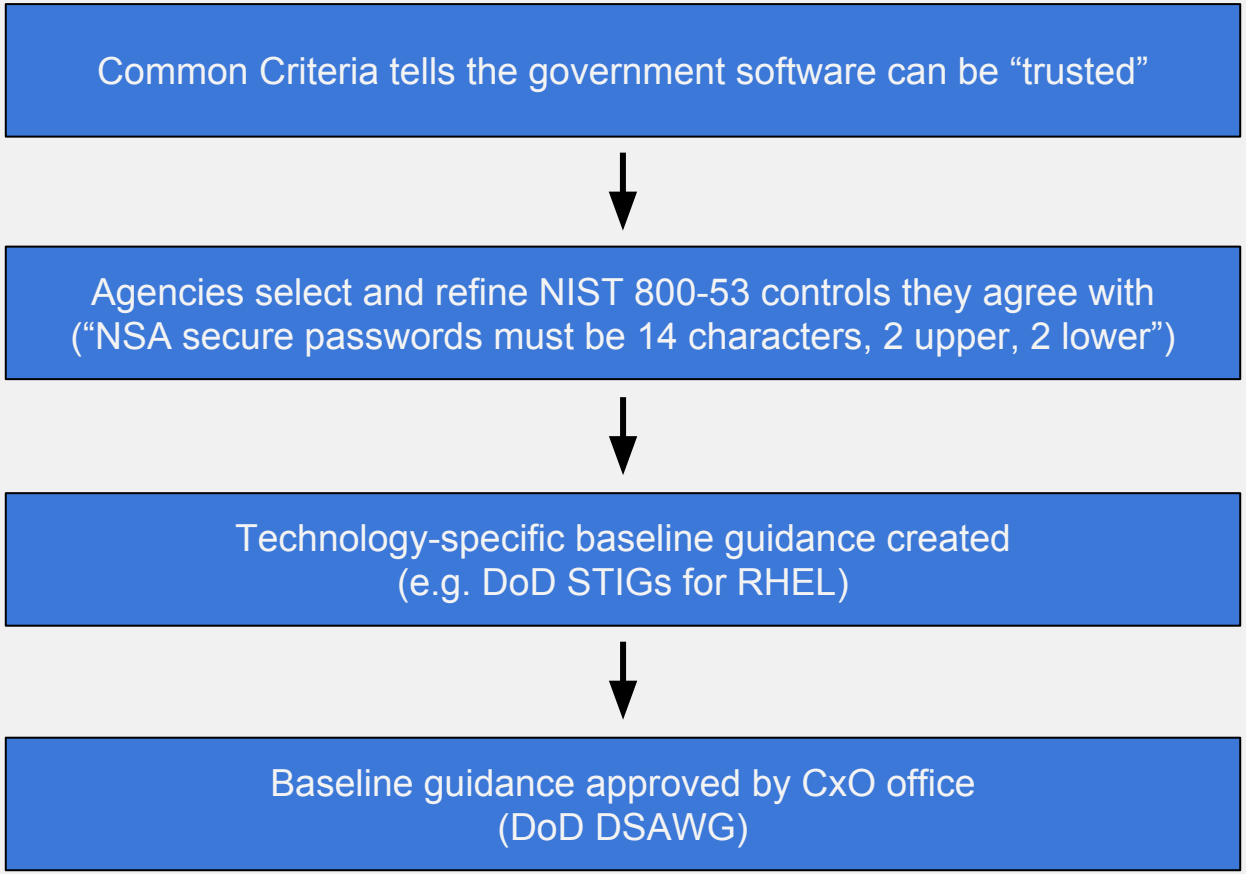
Average time to configure and verify control	# controls	Total time *per RHEL instance*
1 minute	* 587	9.7 hours
3 minutes	* 587	29.4 hours
5 minutes	* 587	48.9 hours



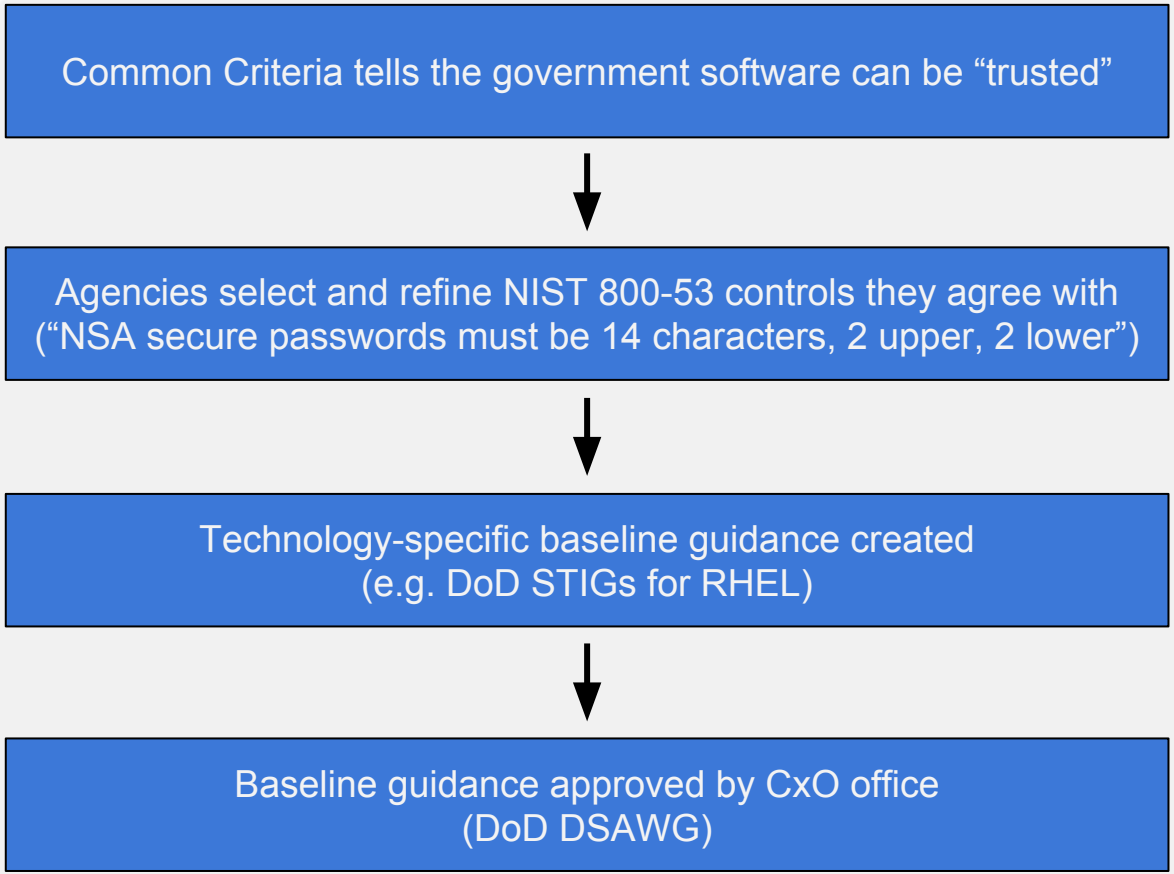

Common Criteria tells the government software can be “trusted”


Common Criteria tells the government software can be “trusted”
Agencies select and refine NIST 800-53 controls they agree with
(“NSA secure passwords must be 14 characters, 2 upper, 2 lower”)


Common Criteria tells the government software can be “trusted”
Agencies select and refine NIST 800-53 controls they agree with
(“NSA secure passwords must be 14 characters, 2 upper, 2 lower”)
Technology-specific baseline guidance created
(e.g. DoD STIGs for RHEL)


Common Criteria tells the government software can be “trusted”
Agencies select and refine NIST 800-53 controls they agree with
(“NSA secure passwords must be 14 characters, 2 upper, 2 lower”)
Technology-specific baseline guidance created
(e.g. DoD STIGs for RHEL)
Baseline guidance approved by CxO office
(DoD DSAWG)

RHEL6 Process



2010-AUG-11 through 2012-OCT-29 (810 days)

DISA Operating System SRG (updated approx. ~3 years)

0 days (done in parallel with common criteria)

122 days

DISA Red Hat Enterprise Linux 5 STIG

- 587 compliance checks
- No published automation, check everything by hand
- *Released 1,988 days after RHEL 5.0!*

DISA Red Hat Enterprise Linux 6 STIG

- 260 compliance checks
- Fully automated checking base off SCAP
- *Released 932 days after RHEL 6.0!*

Red Hat Enterprise Linux 5 STIG

- 587 compliance checks
- No published automation, check everything by hand
- *Released 1,988 days after RHEL 5.0!*

Red Hat Enterprise Linux 6 STIG

- 260 compliance checks
- Fully automated checking base off SCAP
- *Released 932 days after RHEL 6.0!*

5.5 years → 2.5 years (55% faster)

587 checks → 260 checks (56% smaller)

Moving towards fully automated compliance baselines

+

“0 day STIGs”

OpenSCAP & SCAP Security Guide

Project: http://openscap.io

Code: http://github.com/OpenSCAP


NORTHROP GRUMMAN


NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce


LOCKHEED MARTIN


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


redhat


ORACLE


ARL


vmware


DEFENSE INFORMATION SYSTEMS AGENCY


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


HARRIS


OAK RIDGE
National Laboratory


NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA

OpenSCAP BY THE NUMBERS . . .

- 12,109 commits from 155 contributors across all government sectors *(including system integrators!)*
- 1,967,097 lines of code!
- Averages 10.1 commits per day, releases average every 90 days
  - Average 79.9 code contributions per author
  - Up from average of 13 in 2015!
- Red Hat sponsors NIST Configuration & Compliance certifications https://nvd.nist.gov/SCAP-Validated-Tools/

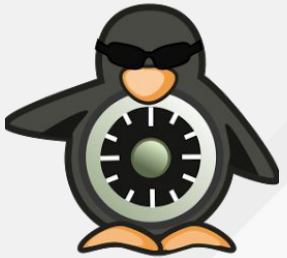
NEW REQUIREMENTS AROUND SELINUX

Making The World a Safer Place

Background:

- “SELinux is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense–style mandatory access controls (MAC).” - wikipedia
- A type is a way of classifying an application or resource. Type enforcement is the enforcement of access control on that type. All files, processes, network resources, etc on an SELinux system have a label, and one of the components of that label is the "type”.
- Much of the kernel work has been done by the NSA and Red Hat

SELinux must be enabled and in enforcing mode - CAT I finding.



WHAT SHOULD I DO WHILE I WAIT FOR DISA TO RELEASE THEIR STIG CONTENT?

STIG

Question:
May I deploy a product if no STIG exists?

Answer:
Yes, based on mission need and with DAA approval.

Question:
What do I use if there is no STIG?

Answer:
DISA FSO developed Security Requirement Guides (SRGs) to address technology areas. In the absence of a STIG, an SRG can be used to determine compliance with DoD policies. If there is no applicable SRG or STIG, industry or vendor recommended practices may be used. Examples include Center for Internet Security Benchmarks, Payment Card Industry requirements or the vendor's own security documentation.

Question:
Does DISA FSO certify products for use in the DoD?

Answer:
No. DISA FSO certifies Information Systems for use in DISA. DISA FSO not does certify products for DoD use. SRGs/STIGs are designed to assist in implementing the secure deployment of products.

http://iase.disa.mil/stigs/Pages/faqs.aspx#STIG

DEMO #1: DEPLOYING INTO STIG COMPLIANCE

- How can we deploy directly into STIG compliance?
  - GUI
  - Kickstart

- Any other profiles available, like C2S?

- What C&A paperwork can be automatically generated?

DEMO #2: CONTINUOUS MONITORING

- How do we tailor the baseline, enabling/disabling certain rules?
- How do we refine values, such as password length?
- Is remediation possible?

THANK YOU


twitter.com/RedHatGov


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos

Backup Slides

WHERE ARE SUPPLEMENTARY MATERIALS:

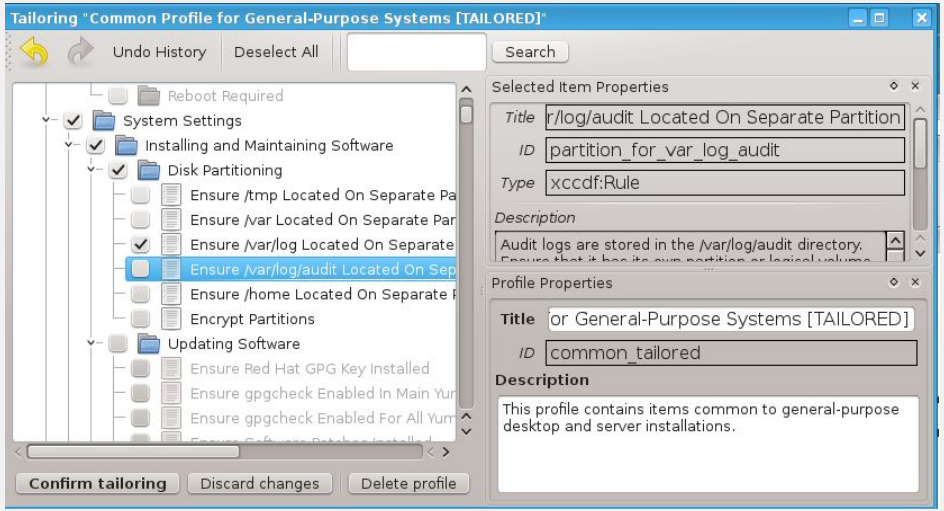
KICKSTARTS, SCRIPTS, NIST MAPPINGS and OTHER ITEMS

Insert paragraph of copy here. Do not exceed 40 words.

- Bullet
- Bullet
- Bullet

TAILORING THE BASELINE

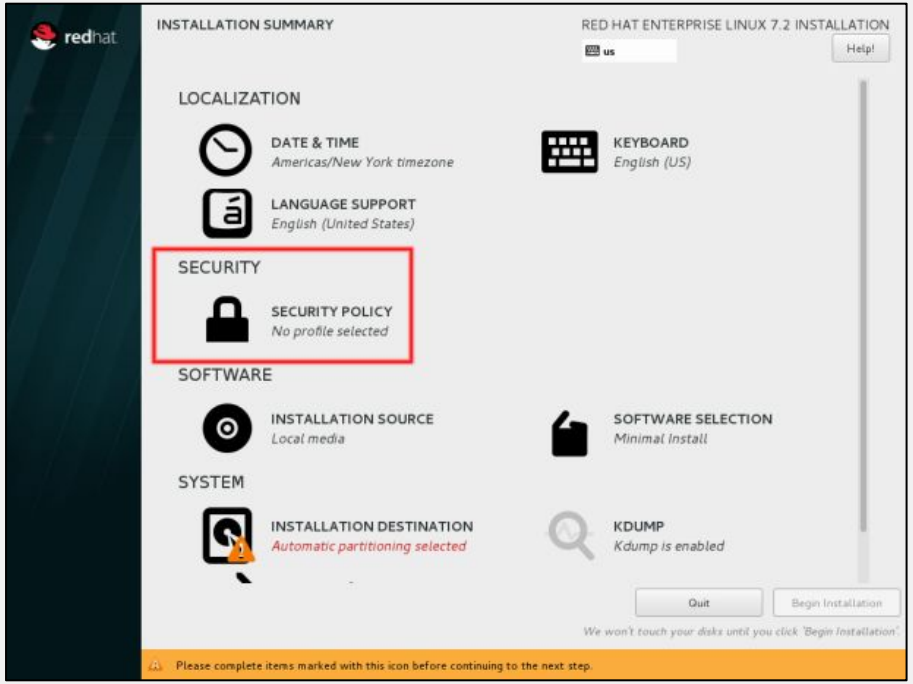
SCAP WORKBENCH



- Bullet
- Bullet
- Bullet

AUTOMATING COMPLIANCE

BOTH AT PROVISIONING and FOR CONTINUOUS COMPLIANCE



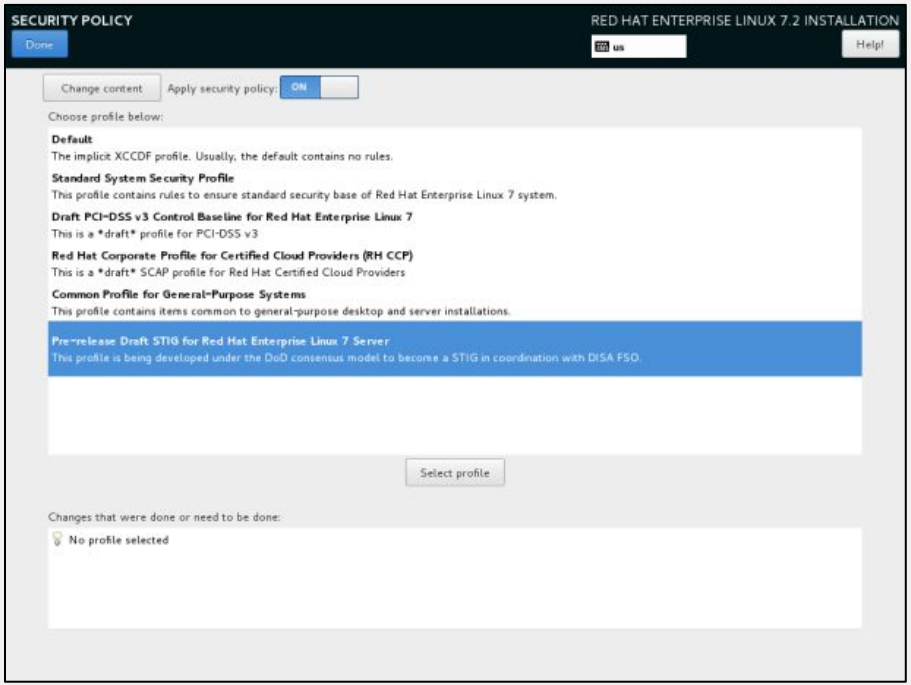
During manual installation

New “security” option in the installer

- Secure RHEL during provisioning
- Specify the profile at installation time
- Supports vendor content and web-based content

AUTOMATING COMPLIANCE

BOTH AT PROVISIONING and FOR CONTINUOUS COMPLIANCE



Supplied Content

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

AUTOMATING COMPLIANCE

BOTH AT PROVISIONING and FOR CONTINUOUS COMPLIANCE

```
%addon org_fedora_oscap
    content-type = datastream
    content-url = http://www.example.com/scap/testing_ds.xml
    datastream-id = scap_example.com_datastream_testing
    xccdf-id = scap_example.com_cref_xccdf.xml
    profile =  xccdf_example.com_profile_my_profile
    fingerprint = 240f2f18222faa98856c3b4fc50c4195
%end
```

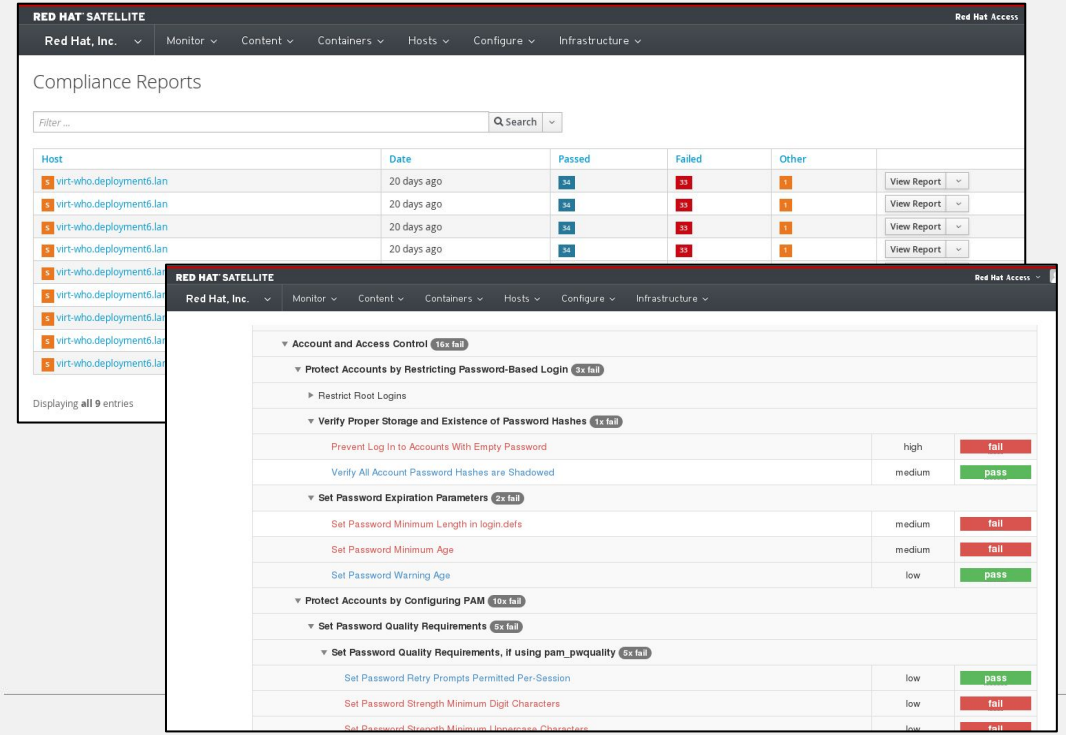
```
%addon org_fedora_oscap
        content-type = scap-security-guide
        profile = pci-dss
%end
```

Automated Kickstart configuration

- New %addon section
  - Content location - included or web based
  - Profile to apply

AUTOMATING COMPLIANCE

BOTH AT PROVISIONING and FOR CONTINUOUS COMPLIANCE



Satellite Server Integration

- Periodic scans from Satellite
- Run remotely
- Provide results for all RHEL systems within the GUI
- Easily deploy and track compliance

NEW CAT I, II, and III FINDINGS

Click to add subtitle

Insert paragraph of copy here. Do not exceed 40 words.

- 39x CAT I
- 242x CAT II
- 14x CAT III

DIFFERENCES:

VENDOR SUPPLIED CONTENT vs DISA CONTENT

Insert paragraph of copy here. Do not exceed 40 words.

- Bullet
- Bullet
- Bullet