BOSTON, MA
JUNE 23-26, 2015

SECURITY COMPLIANCE MADE EASY(ER): ENTERING THE SCAP RENAISSANCE

MOTIVATION

RHEL5 STIG (U.S. Military Baseline)

- 587 compliance items
- Many are manual

Avg Time to Configure & Verify Setting	# controls	Total Time *per RHEL instance*
1 minute	* 587	9.7 hours
3 minutes	* 587	29.4 hours
5 minutes	* 587	48.9 hours

openprivacy / ansible-scap

Watch 1 | Star 2 | F

branch: master ansible-scap / provision.yml

openprivacy 14 days ago comments cleaned up

1 contributor

15 lines (12 sloc) 0.303 kB

Raw Blame History

```
1  ---
2
3  - name: All machines get OpenSCAP scanner installed
4    hosts: all
5    sudo: true
6    roles:
7      - openscap
8  #   - harden  -- Commented out for demo purposes only
9
10 - name: Install SCAP Security Content (SSG) and GovReady on 'dashboard'
11   hosts: dashboard
12   roles:
13     - scap-security-guide
14     - govready
```

… or a single LOC in kickstart

```
$ oscap xccdf eval \
--profile rht-ccp \
--remediate \
--report /root/scan-report.html \
/usr/share/xml/scap/content.xml
```

Compliance and Scoring

The target system did not satisfy conditions of 13 rules! Please review rule results and consider applying remediation.

Rule result breakdown

Failed rules by severity breakdown

Score

Scoring system	Score	Maximum	%
urn:xccdf:scoring:default	93.626541	100.000000	93.63%

OUR (*very ambitious*) AGENDA

1. What's the latest in the Security Automation space?
    a. Government & Commercial Initiatives
    b. Formal and Emerging SCAP Standards

2. What tools and content are available today?
    a. For enumerating (known) software vulnerabilities
    b. For assessing configuration

3. Use Case Story: Lockheed Martin
   and the Centralized Super Computing Facility

LIVE DEMOS

1. Install & Review SCAP profiles in RHEL 7
2. Performing a Compliance Scan
3. System Remediation
4. Creating Custom (derived) Configuration Baselines with SCAP Workbench
5. RHEL 7 “Easy Button” Installations

SPEAKERS

Shawn Wells
Director, Innovation Programs
Developer, OpenSCAP Content
Red Hat

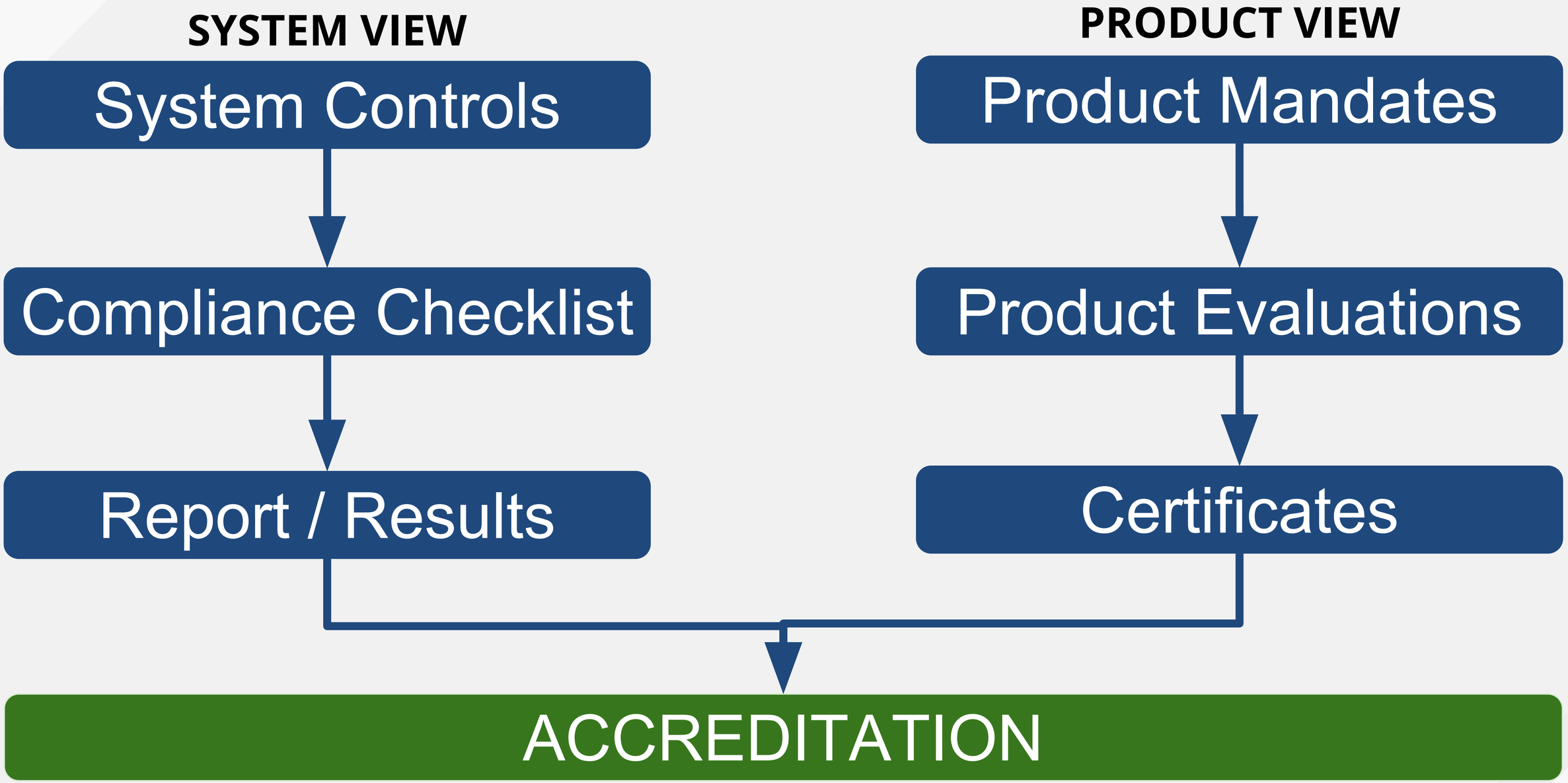
SPEAKERS

Jeff Blank
Technical Director,
OS and Applications Division
Information Assurance Directorate
National Security Agency

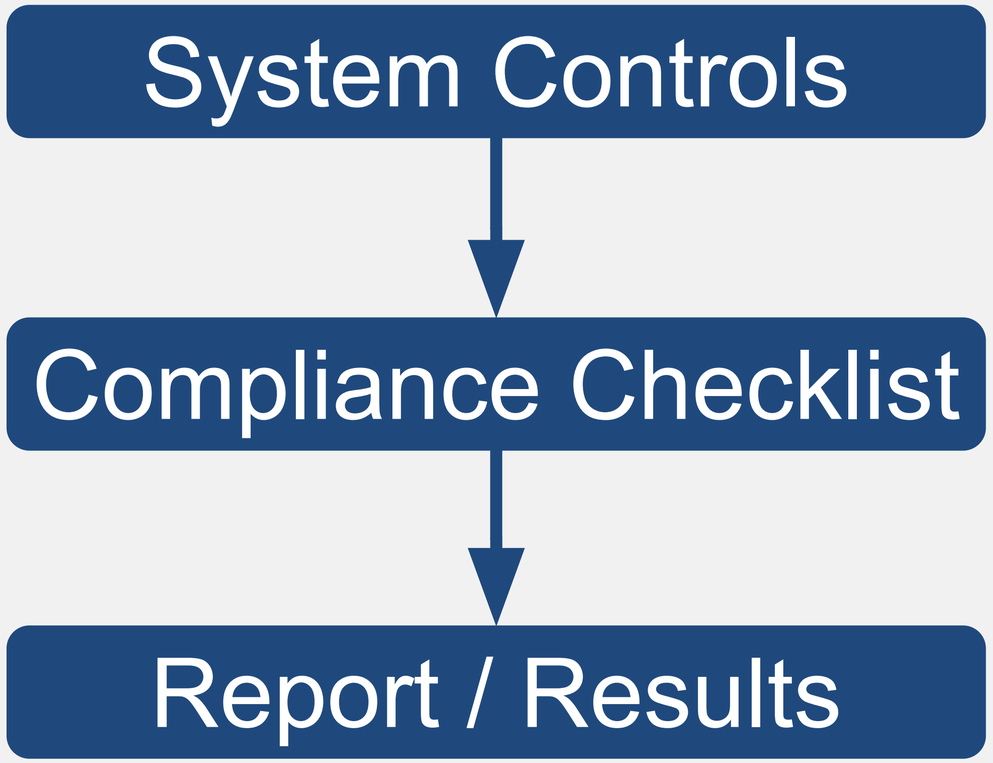
SPEAKERS

Sarah Storms
Josh Koontz
Engineering,
Lockheed Martin

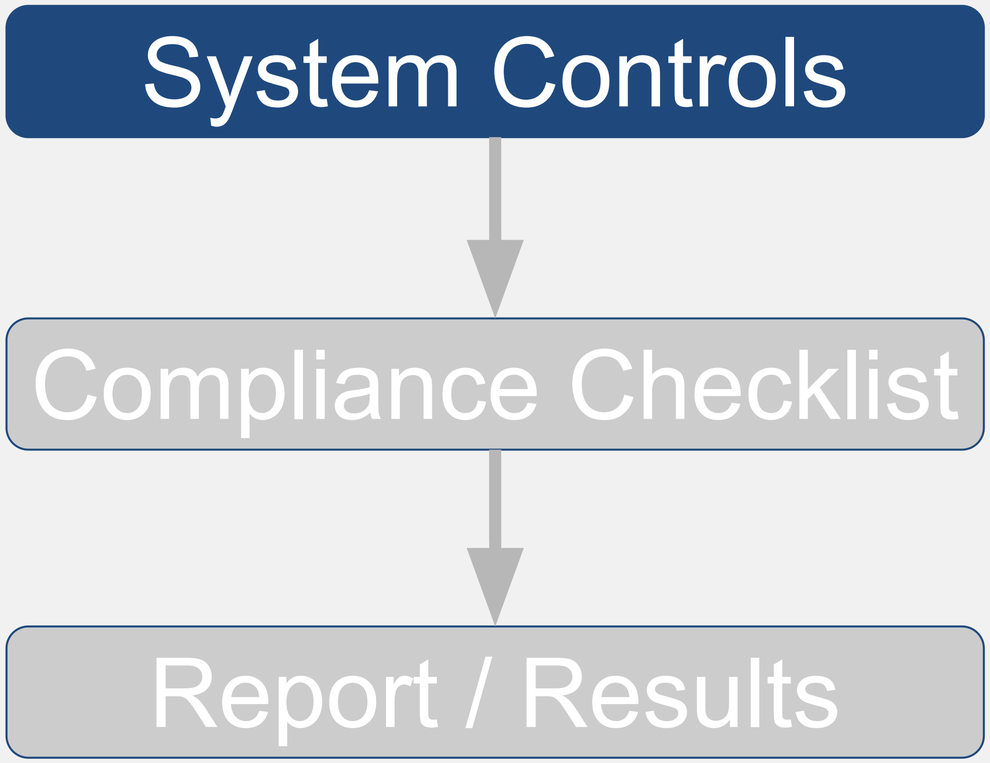
COMPLIANCE BIG PICTURE: PRODUCTS AND SYSTEMS


SYSTEM VIEW
PRODUCT VIEW
System Controls
Product Mandates
Compliance Checklist
Product Evaluations
Report / Results
Certificates
ACCREDITATION

SYSTEM VIEW OF ACCREDITATION



SYSTEM VIEW OF ACCREDITATION



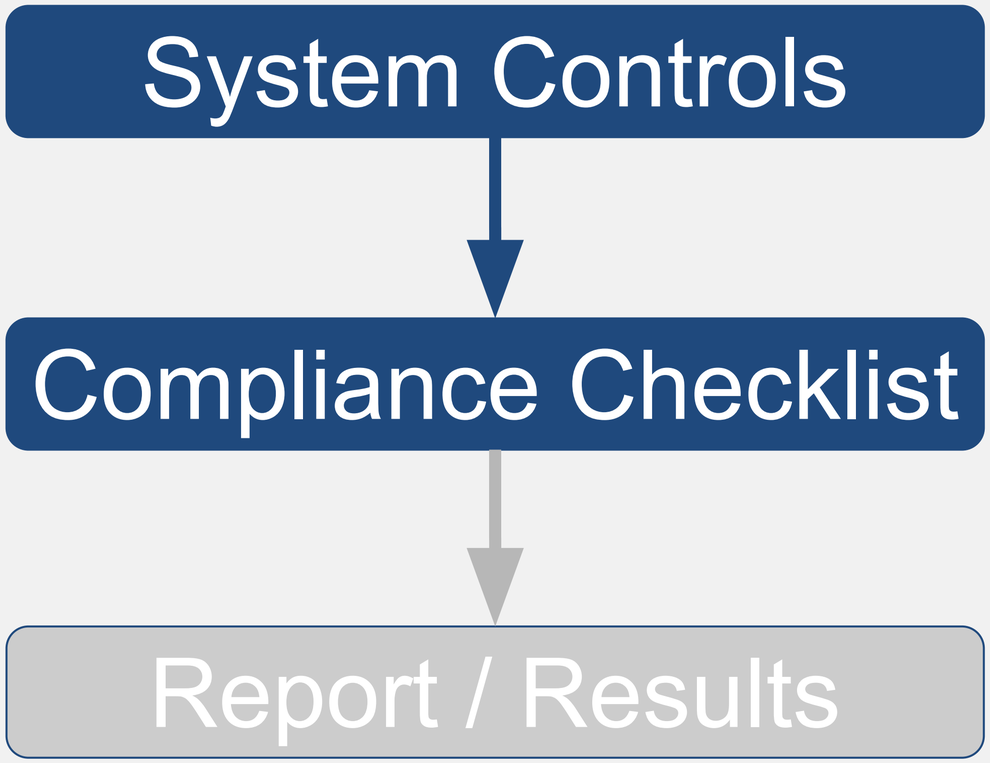
NIST 800-53

FedRAMP

CNSSI 1253

PCI

SYSTEM VIEW OF ACCREDITATION

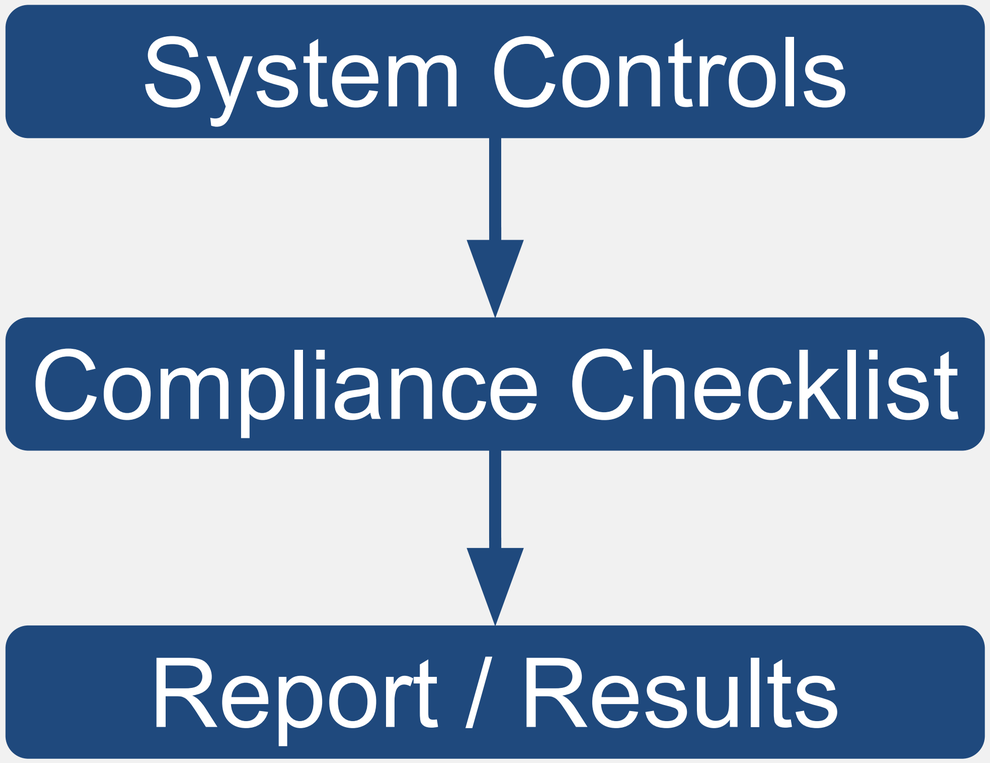


DISA STIG

NSA SNAC

CIS Benchmarks

SYSTEM VIEW OF ACCREDITATION



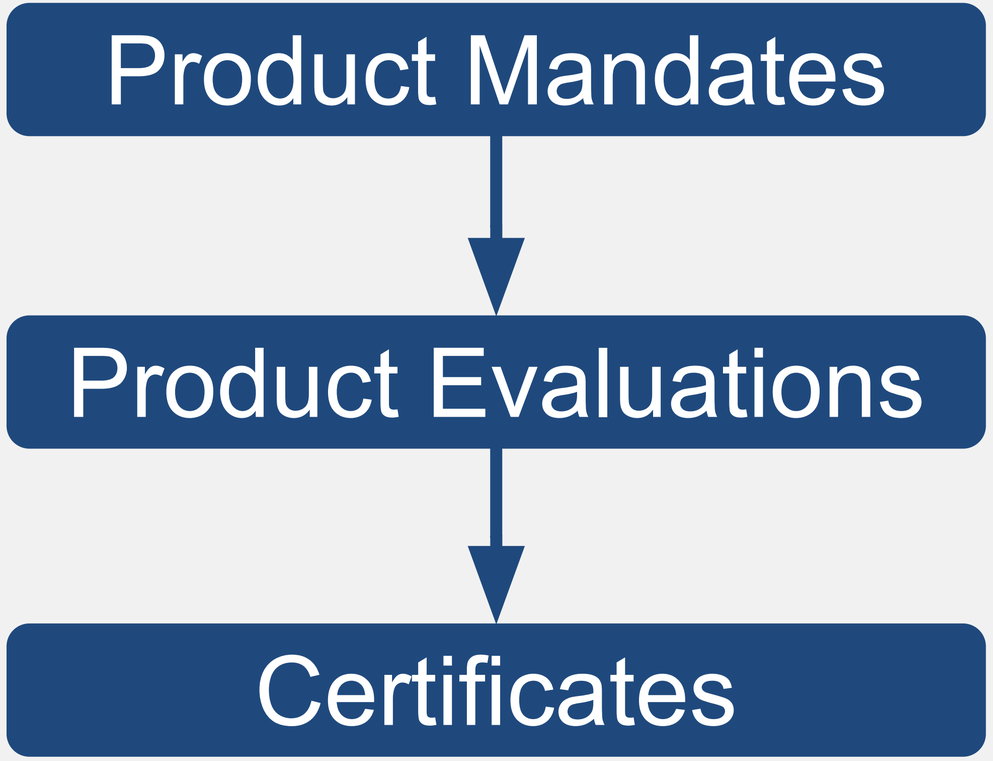
Tenable Nessus

SECSCAN

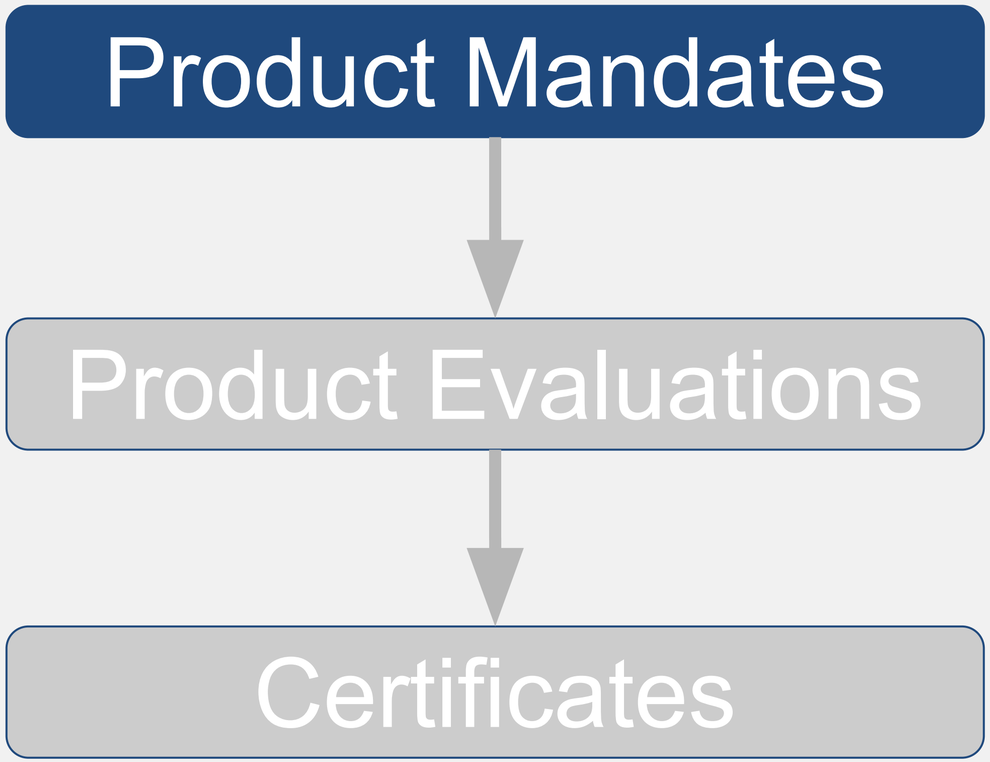
SPAWAR SCC

OpenSCAP

PRODUCT VIEW OF ACCREDITATION



PRODUCT VIEW OF ACCREDITATION



Common Criteria

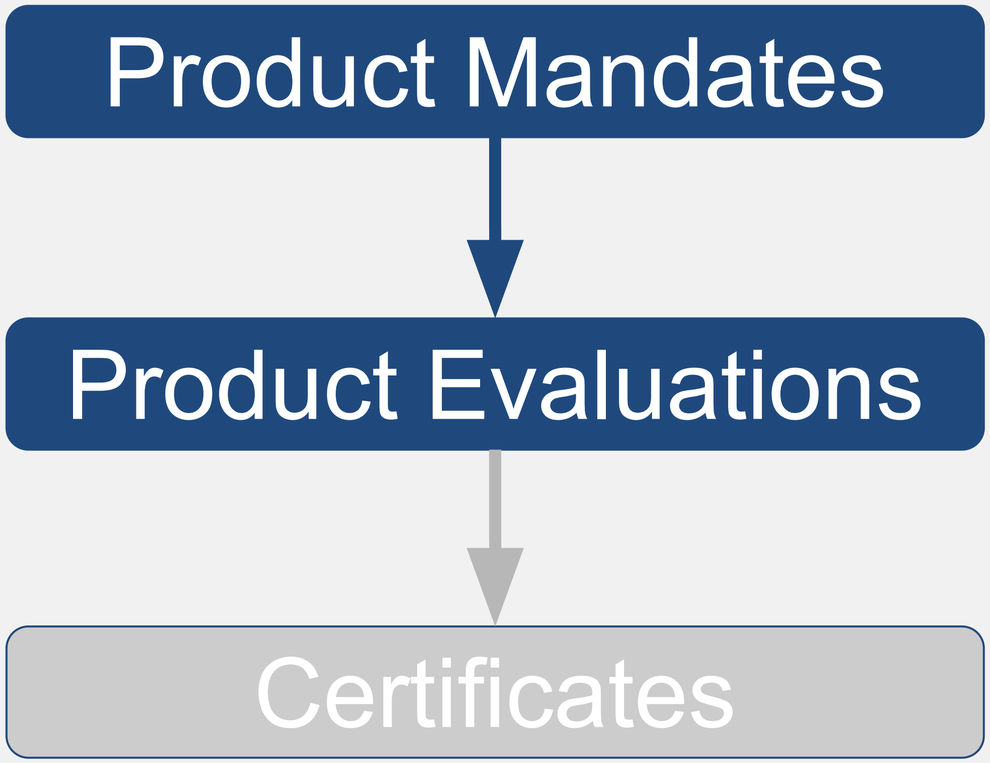
FIPS 140-2

…. wait… what's COMMON CRITERIA?

- international framework for specifying and testing security functional and assurance requirements in IT products
  - through the use of Protection Profiles (PPs)

- vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

PRODUCT VIEW OF ACCREDITATION

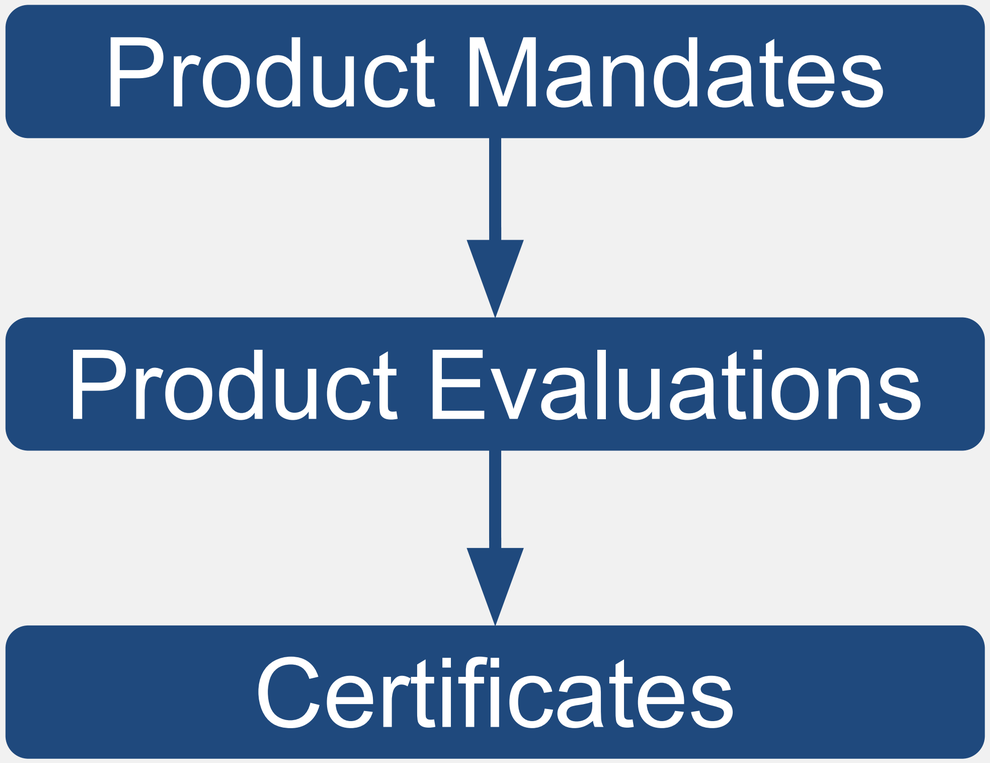


Operating System Protection Profile

Server Virtualization Protection Profile

FIPS Validation

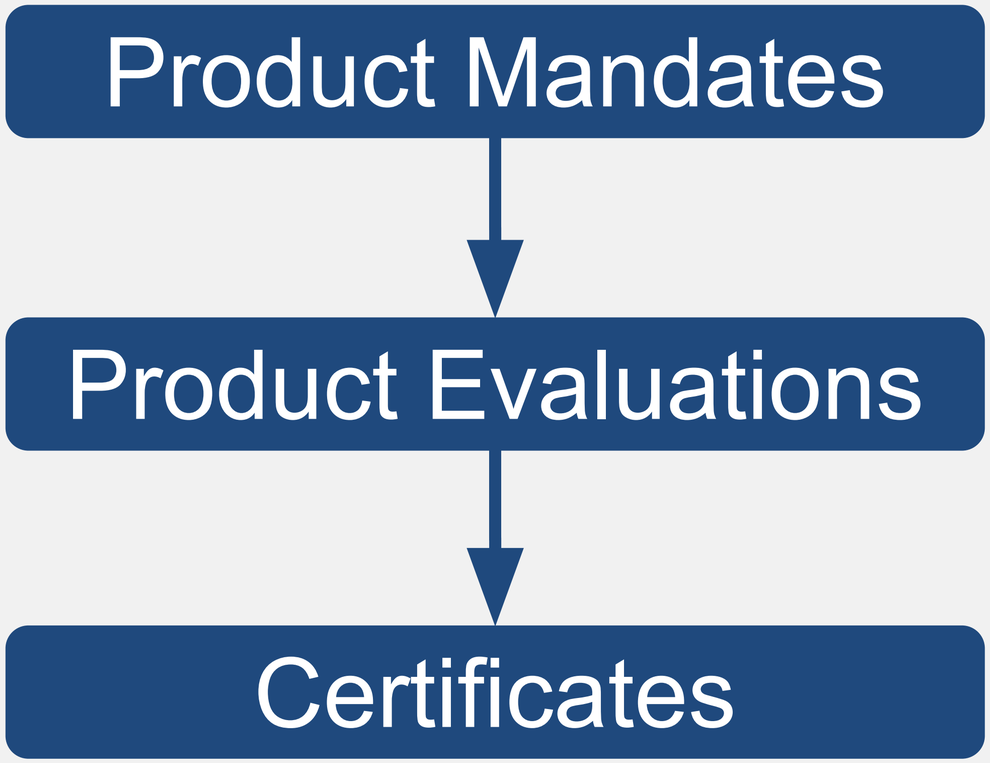
PRODUCT VIEW OF ACCREDITATION



NIAP Product Compliant List

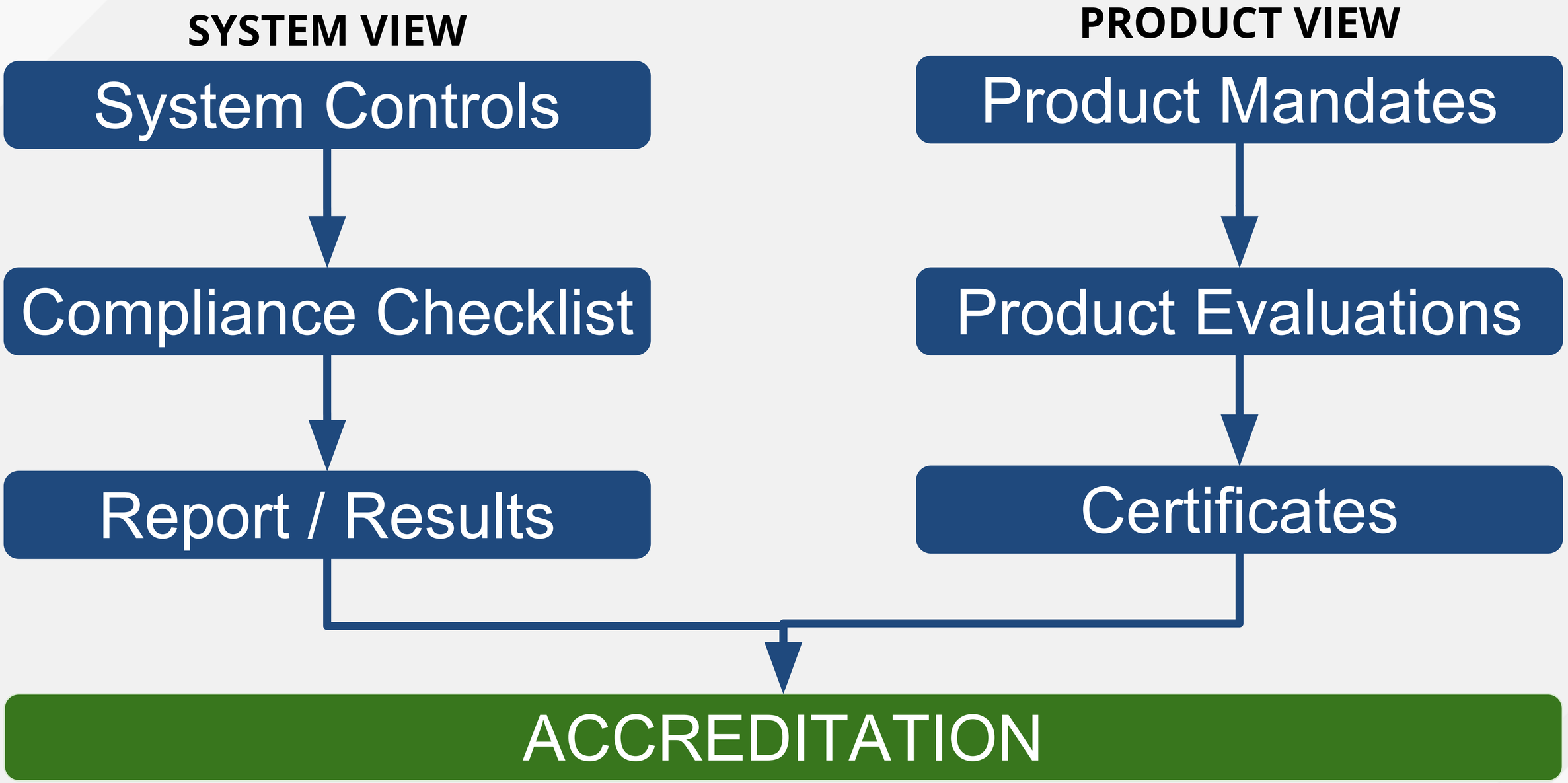
FIPS Crypto Module Validation List

PRODUCT VIEW OF ACCREDITATION



1-2 years+

Costly ($millions)


SYSTEM VIEW
PRODUCT VIEW
System Controls
Product Mandates
Compliance Checklist
Product Evaluations
Report / Results
Certificates
ACCREDITATION

OPEN SOURCE CONFRONTS THE C&A CHALLENGE: PRODUCT CERTIFICATION

COMMON CRITERIA - *REVAMPED*

- Requirements specified in *Protection Profiles*
  - see https://www.niap-ccevs.org
  - development on https://github.com/commoncriteria
  - revamped OS Protection Profile due this July

- Dramatically reduced evaluation time and cost
  - 90 days possible, 180 max
  - compliance checklist produced during evaluation (SCAP)
  - list of system controls provided for evaluated products

COMMON CRITERIA - *REVAMPED*

- DISA STIG creation through ~25 selectable “management functions”
- DoD specific values expressed in *DoD Annexes to Protection Profiles* (succeeding SRGs)
- Remember…
  - RHEL5 STIG: 587 rules
  - RHEL6 STIG: ~255
  - RHEL.future STIG: est. < 100

Management Function
configure minimum password length
configure minimum number of special characters in password
configure minimum number of numeric characters in password
configure minimum number of uppercase characters in password
configure minimum number of lowercase characters in password
enable/disable screen lock
configure screen lock inactivity timeout
configure remote connection inactivity timeout

OPEN SOURCE CONFRONTS THE C&A CHALLENGE: SYSTEM COMPLIANCE

OpenSCAP

Community created *portfolio* of tools and content
to assess systems for known vulnerabilities.

https://github.com/OpenSCAP

2008 First commit to OpenSCAP, execution capability for SCAP on Linux

```
commit 768d2d13c7b95736738ce2a48db7f2e528c161fe
Author: Peter Vrabec <pvrabec@wrabco.englab.brq.redhat.com>
Date:   Mon Nov 3 17:58:30 2008 +0100

    Initial commit
```

2011 First commit to SCAP Security Guide, hardening guidance + policy references Colloquially, “SCAP Content”

```
commit 540a78f26191a69651a167d256b5af47fd3eb983
Author: Jeff Blank <blank@eclipse.ncsc.mil>
Date:   Wed Jun 8 18:45:05 2011 -0400

    added a README
```

Foreman
OpenSCAP

Ruby Gem
OpenSCAP

Puppet
OpenSCAP

SCAPtimony


HARRIS


CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA


TRESYS
TECHNOLOGY


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


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


GOVREADY


DEFENSE INFORMATION SYSTEMS AGENCY


ARL
U.S. Army Research Laboratory


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


OAK
RIDGE
National Laboratory


LOCKHEED MARTIN


WE DON'T ALWAYS
TEST OUR CODE
BUT WHEN WE DO,
IT'S LIVE AT SUMMIT

DEMO #1: INSTALL, REVIEW PROFILES

Install OpenSCAP and SCAP Content

$ sudo yum install openscap-scanner scap-security-guide

What default profiles exist?

$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml

....

Profiles:

pci-dss

rht-ccp

common

stig-rhel7-server-upstream

....

DEMO #2: REVIEW HARDENING GUIDES

Review manpage

$ man scap-security-guide

Review HTML gudes

$ ls -l /usr/share/doc/scap-security-guide/rhel7-guide.html

DEMO #3: LOCAL SCAN, REVIEW RESULTS

Perform 1st Scan

```
$ sudo oscap xccdf eval --profile rht-ccp \
--results /root/summit-results.html \
--report /root/summit-report.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

Review Results

```
$ ${web_browser} /root/summit-results.html
```

DEMO #4: REMEDIATION

Generate remediation scripts from results

```
$ sudo oscap xccdf generate fix \
--result-id xccdf_org.open-scap_testresult_rht-ccp \
/root/summit-results.xml
```

Or, remediate automatically (*be careful - no "undo"!*)

```
$ sudo oscap xccdf eval --profile rht-ccp \
--results /root/summit-results.xml \
--report /root/summit-report.xml \
--remediate \
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

DEMO #5: SCAP WORKBENCH

Download SCAP Workbench

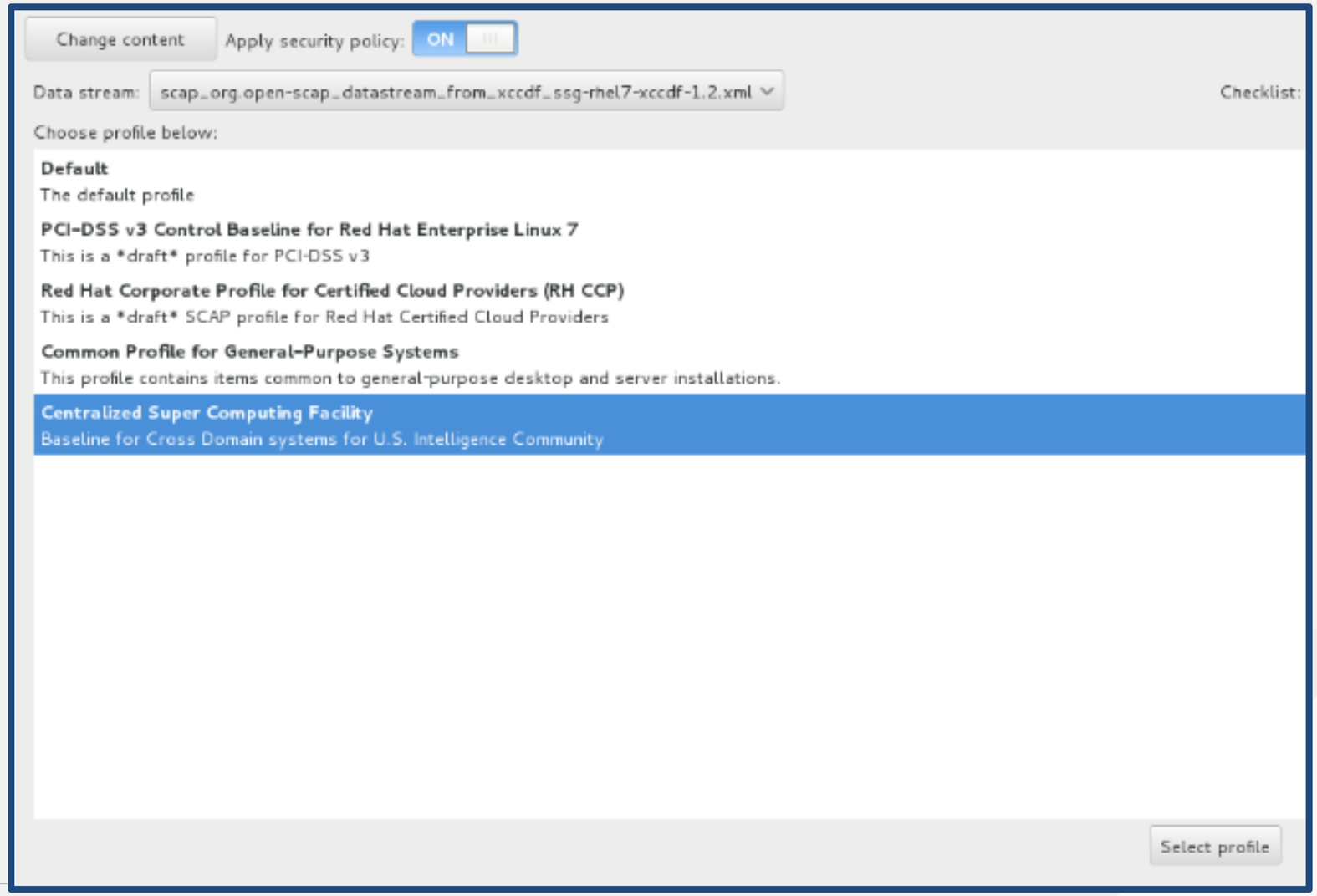
$ sudo yum -y install scap-workbench

Much of this demo is live. For extra details, https://open-scap.org

DEMO #6: “Easy Button Installs”

Live Demo
- RHEL 7.2 Anaconda Plugin
- Sample kickstarts @

  https://github.com/OpenSCAP/scap-security-guide/tree/master/RHEL/6/kickstart/



OpenSCAP IN ACTION
Lockheed's Use Case

Sarah Storms
Project Engineer
Lockheed Martin
sarah.b.storms@lmco.com

Joshua Koontz
Systems Engineer
Lockheed Martin
joshua.koontz@lmco.com

WHAT WE DO

The Centralized Super Computer Facility (CSCF) is an ICD 503 certified, cross-domain computing facility for U.S. Intelligence processing research and development.

ALGORITHM PROESSING

MULTI-TENANT DATA STORAGE

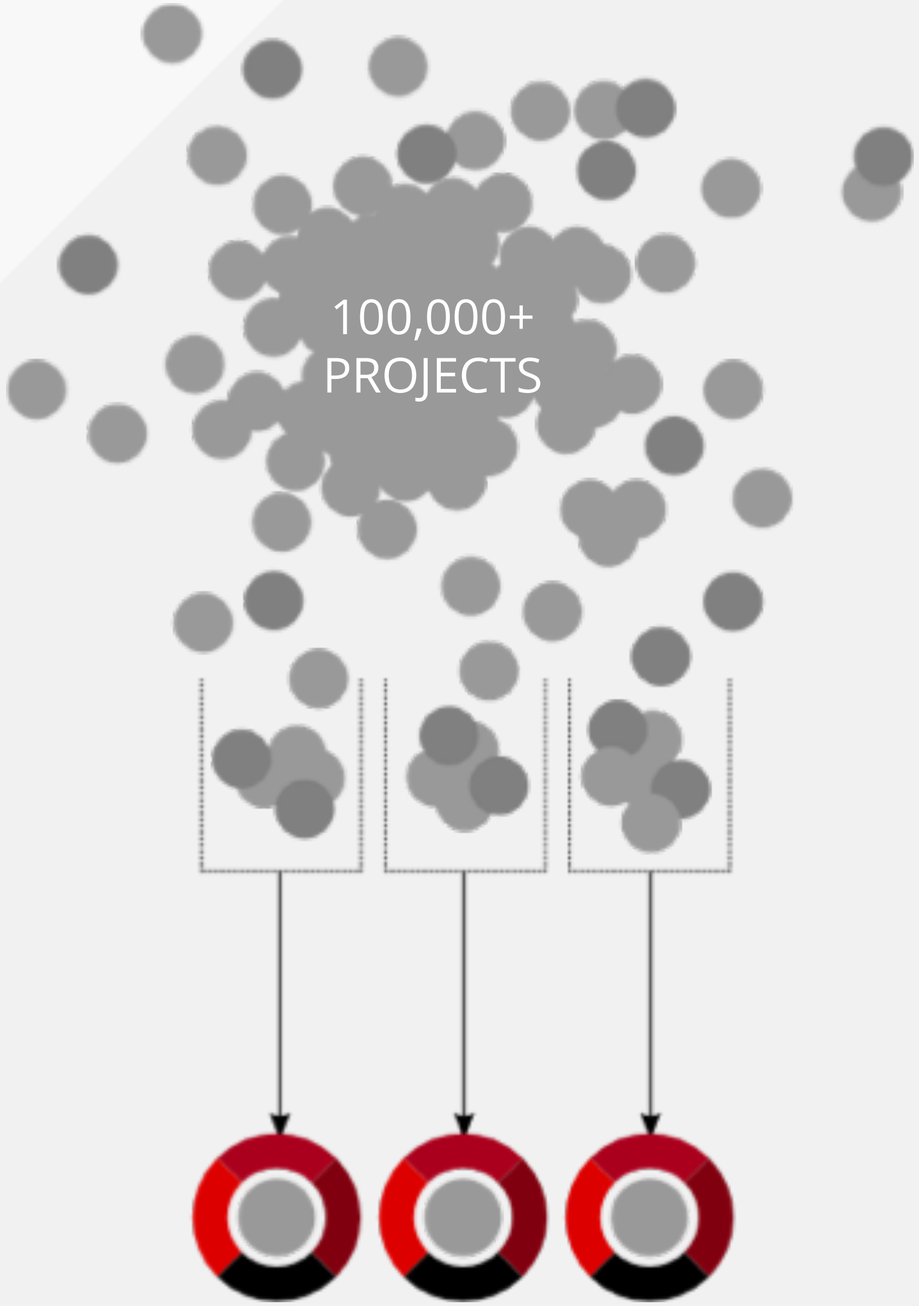
CROSS DOMAIN DATA FUSION

VIRTUALIZATION

CSCF BACKSTORY

- The CSCF program leverages MLS OS configurations for the last 20 years
  - Minimize hardware, licensing, OS configuration, manpower costs
  - Maximize flexibility, data fusion, system utilization

- MLS requires a full ecosystem to be truly useful
  - Certified products
  - OS configuration
  - Resource management
  - Direct and Network attached storage
  - Including long haul data sharing
  - System Monitoring including audit reduction
  - Databases



CONSUMER TO COLLABORATOR

PARTICIPATE
(upstream **projects**)

CSCF participates in community-powered upstream projects, such as OpenSCAP and SELinux.

INTEGRATE
(community **platforms**)

CSCF collaborates with Red Hat to integrate upstream projects into open, enterprise platforms.

https://github.com/CSCF

STABILIZE
(supported **products, platforms, solutions**)

Lockheed commercializes these platforms, together with an ISV ecosystem, and pushes security accreditations.

MLS ECOSYSTEM

ECOSYSTEM PARTNERS

- LMC/CSCF
- Red Hat
- Altair
- Seagate
- Mellanox
- ViON
- Bay Microsystems
- SGI
- Cray
- Splunk
- Crunchy Data
- UNLV/NSCEE

CRAY THE SUPERCOMPUTER COMPANY

redhat

Bay Microsystems™

CRUNCHY DATA SOLUTIONS, INC.

NSCEE
National Supercomputing Center for Energy and the Environment
High-Performance Computing and Communications in Nevada

Seagate

Altair | PBS Works™

ViON
Building your enterprise solutions

splunk>

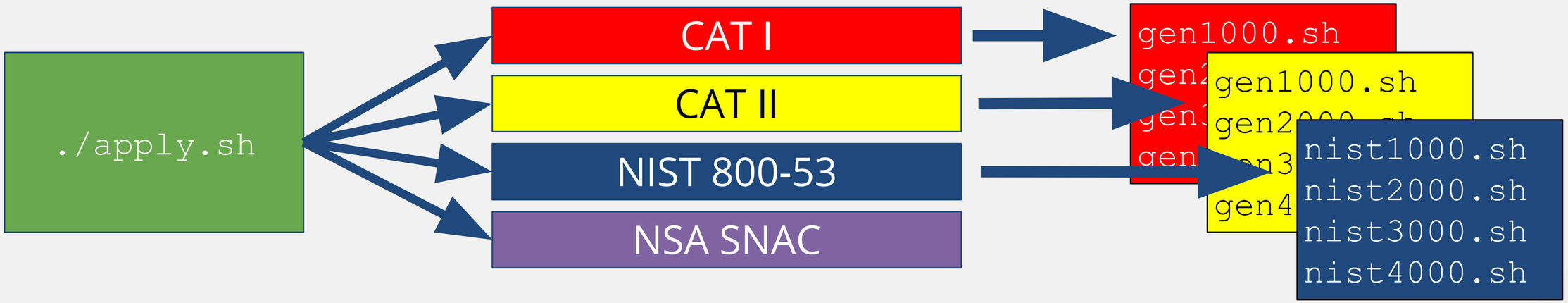
LOCKHEED MARTIN
We never forget who we're working for®

MLS Ecosystem Objective - Provide MLS capable versions of software capabilities integrated with the RHEL MLS configuration to solve complex system configuration and support problems

HARDENING: OLD METHOD

The hardening shell script served several purposes in hardening the system:

- Distributes “baseline” system configurations and policies for authentication, auditing, accounts, services;
- Modular code in folders and separate script allowed for adoption to meet changing system and security needs



C&A TESTING: OLD METHOD

Technical control testing is a subset of overall system controls

- SECSCN - Legacy system security scanner useful for DCID 6/3 testing. Isn't flexible enough to test most of ICD503 technical controls
- Bash script to manually test each control - System testers required a bash script to manually test each system control not checked by SECSCN
- Interactive tests - Tests that couldn't be automatically checked in a bash script or special test cases

Initially took **12+ months** from paperwork submittal until initial approval

HARDENING: NEAR FUTURE METHOD

Use OSCAP Anaconda Addon to specify CSCF-MLS profile during system build. Then apply custom configurations

- CSCF's SCAP profile distributes hardened system configurations and policies for authentication, auditing, accounts, services
- Apply custom configurations separately from security relevant changes

C&A: CURRENT & FUTURE METHOD

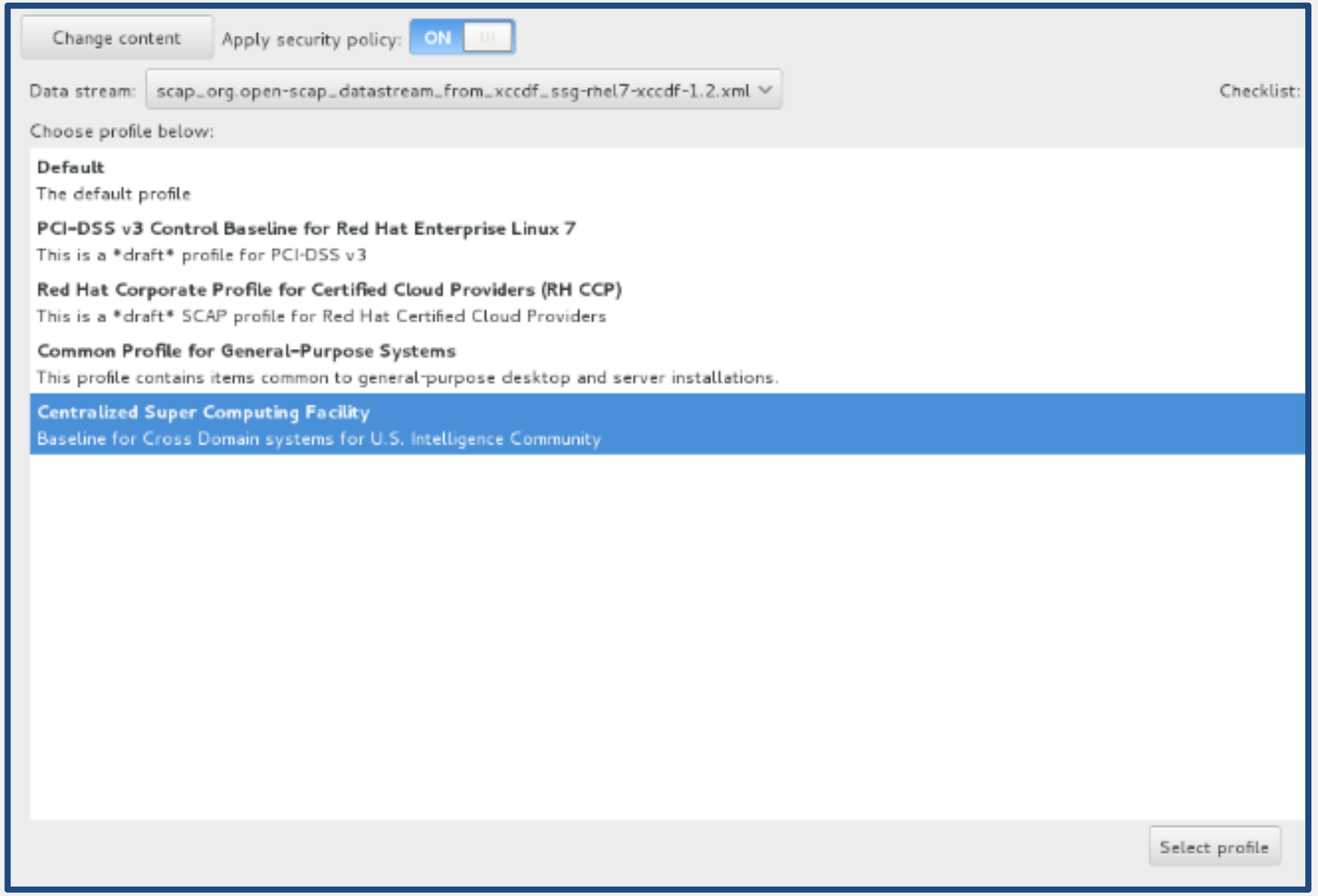
Current (**90 days** from submittal to approval) :

- SECSCN: still in use for familiarity
- NESSUS: vulnerability scan
- OpenSCAP: Configuration Compliance checklist
- Small set of interactive checks

Future (Targeting <30 days from submittal to approval):

- Drop SECSCN and NESSUS
- Fully utilize Anaconda-SCAP to provision directly into secure configuration

….DRAMATICALLY SIMPLIFIED


Change content
Apply security policy:
ON
Data stream:
scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Checklist:
Choose profile below:
Default
The default profile
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.
Centralized Super Computing Facility
Baseline for Cross Domain systems for U.S. Intelligence Community
Select profile

CONTACT INFO

Shawn Wells
Director, Innovation Programs
shawn@redhat.com

Jeff Blank
Tech Director, OS and Applications Division, NSA IAD
blank@eclipse.ncsc.mil

Sarah Storms
Project Engineer, CSCF, Lockheed Martin
sarah.b.storms@lmco.com

Josh Koontz
Systems Engineer, CSCF, Lockheed Martin
joshua.koontz@lmco.com