Consumer to Collaborator

Re-Imagining the Government’s role
in Open Source

EXPLAIN YOUR FISMA PROCESS

branch: master ▾ ansible-scap / provision.yml

openprivacy a day ago comments cleaned up

1 contributor

15 lines (12 sloc) | 0.303 kB

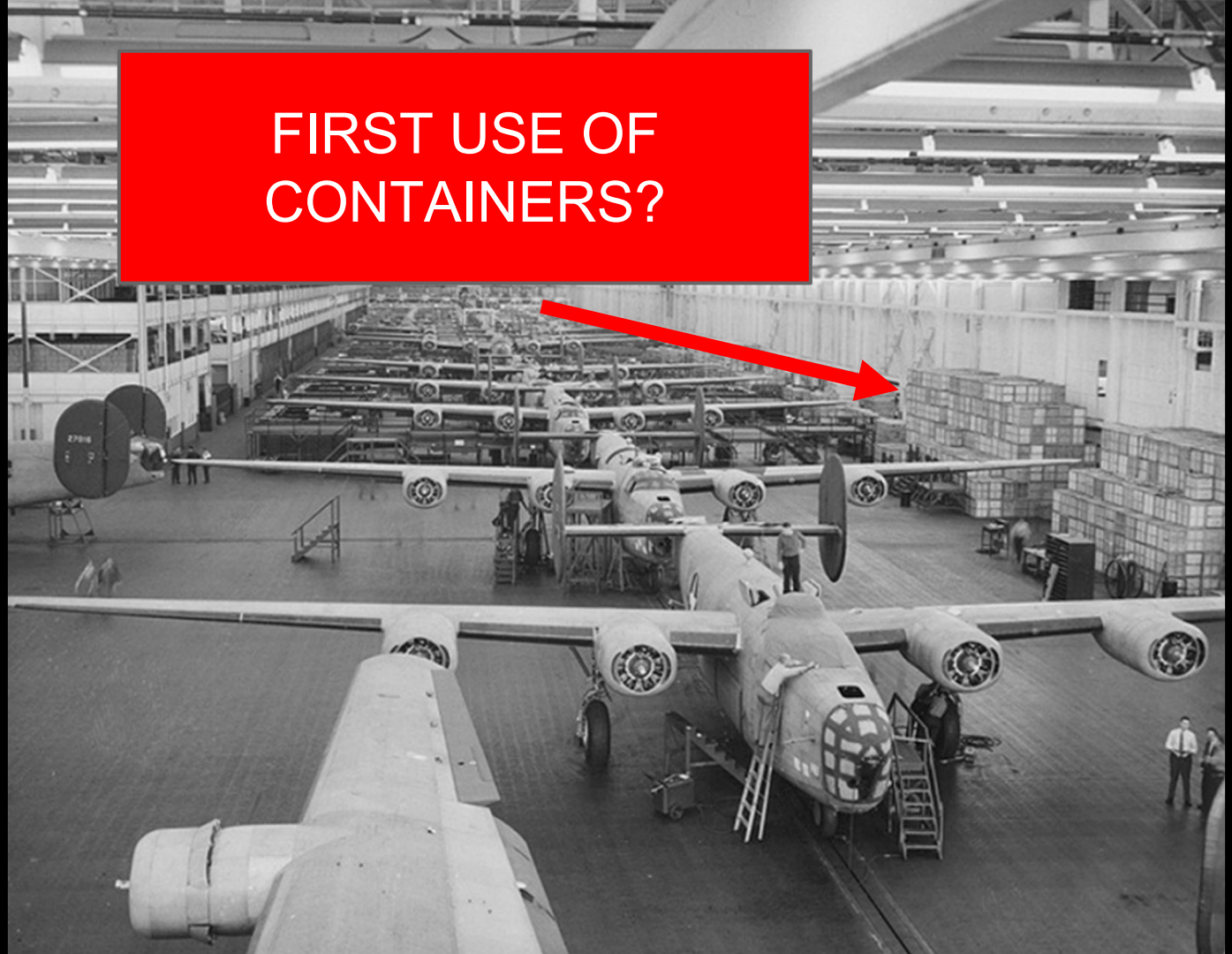
Raw Blame History

```
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, EMBED INTO KICKSTART:

```
$ oscap xccdf eval \
--remediate \
--profile stig-rhel6-server-upstream \
--report /root/scan-report.html \
/usr/share/xml/scap/content.xml
```

Miracle at Willow Run


FIRST USE OF
CONTAINERS?

Mode 1

Mode 2

Mode 1

Mode 2

TRADITIONAL

Mode 1

TRADITIONAL

Mode 2

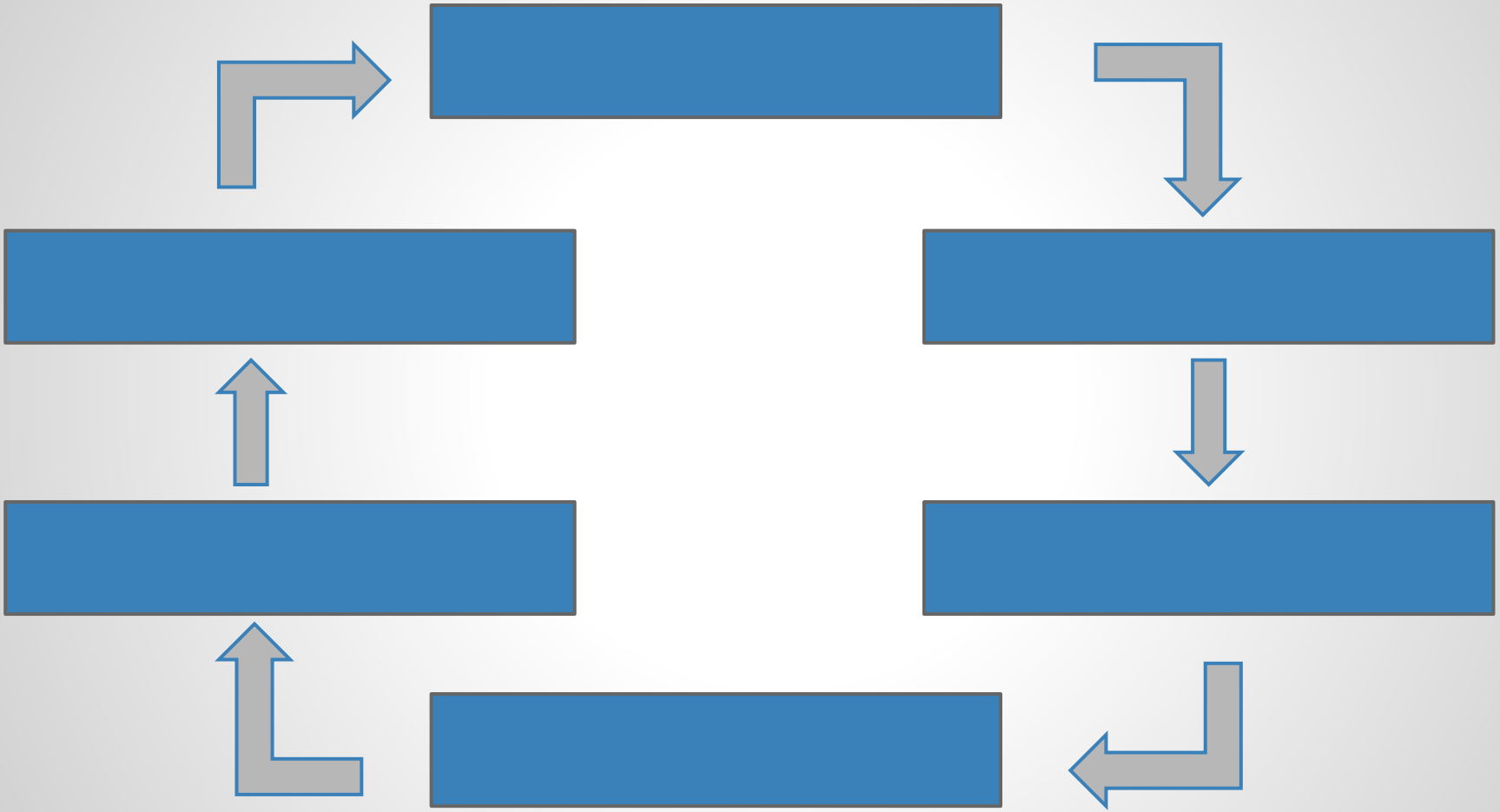
EXPLORATORY

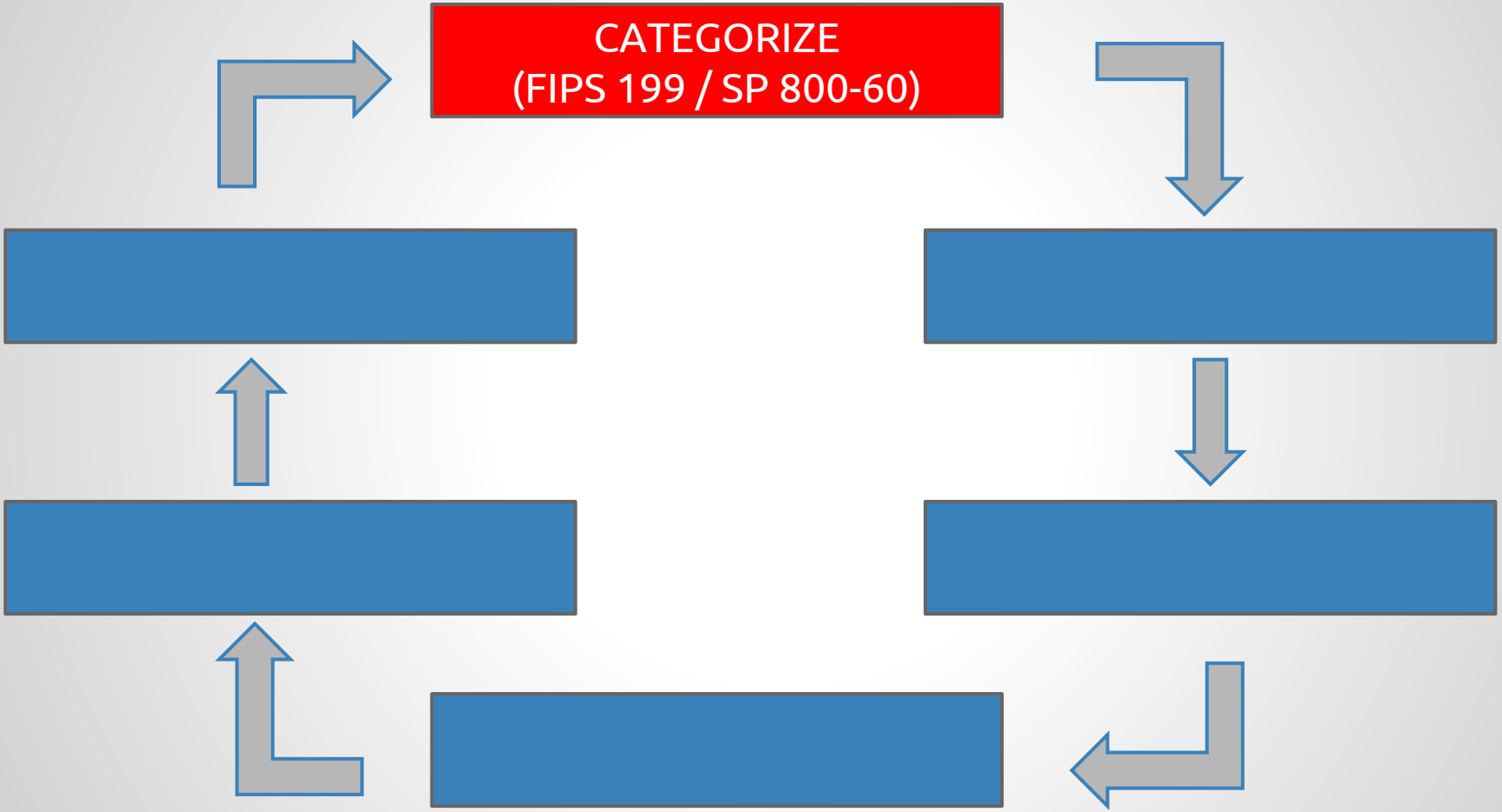
YOU ARE NOT AN

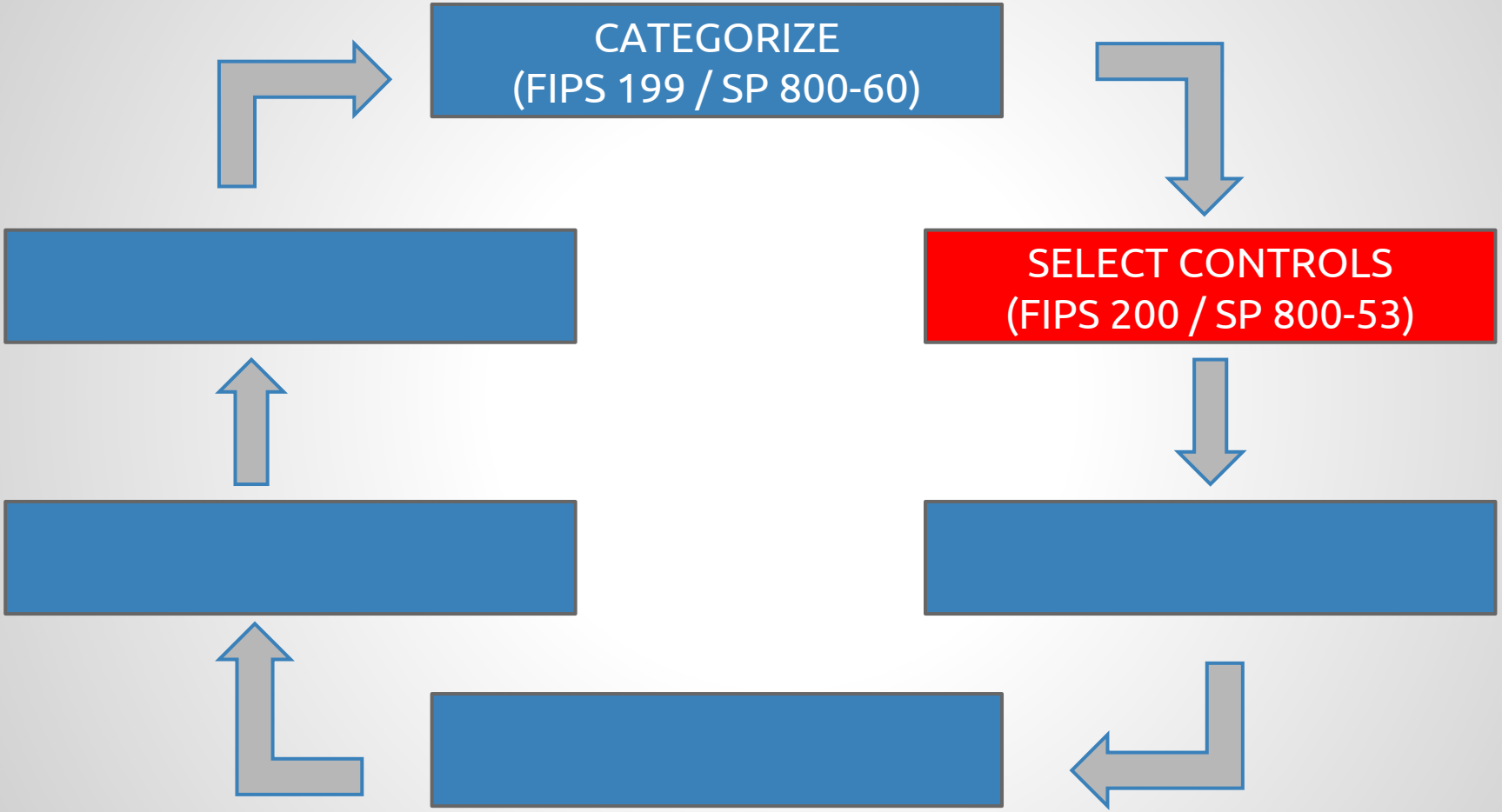
IT CRAFTSMAN

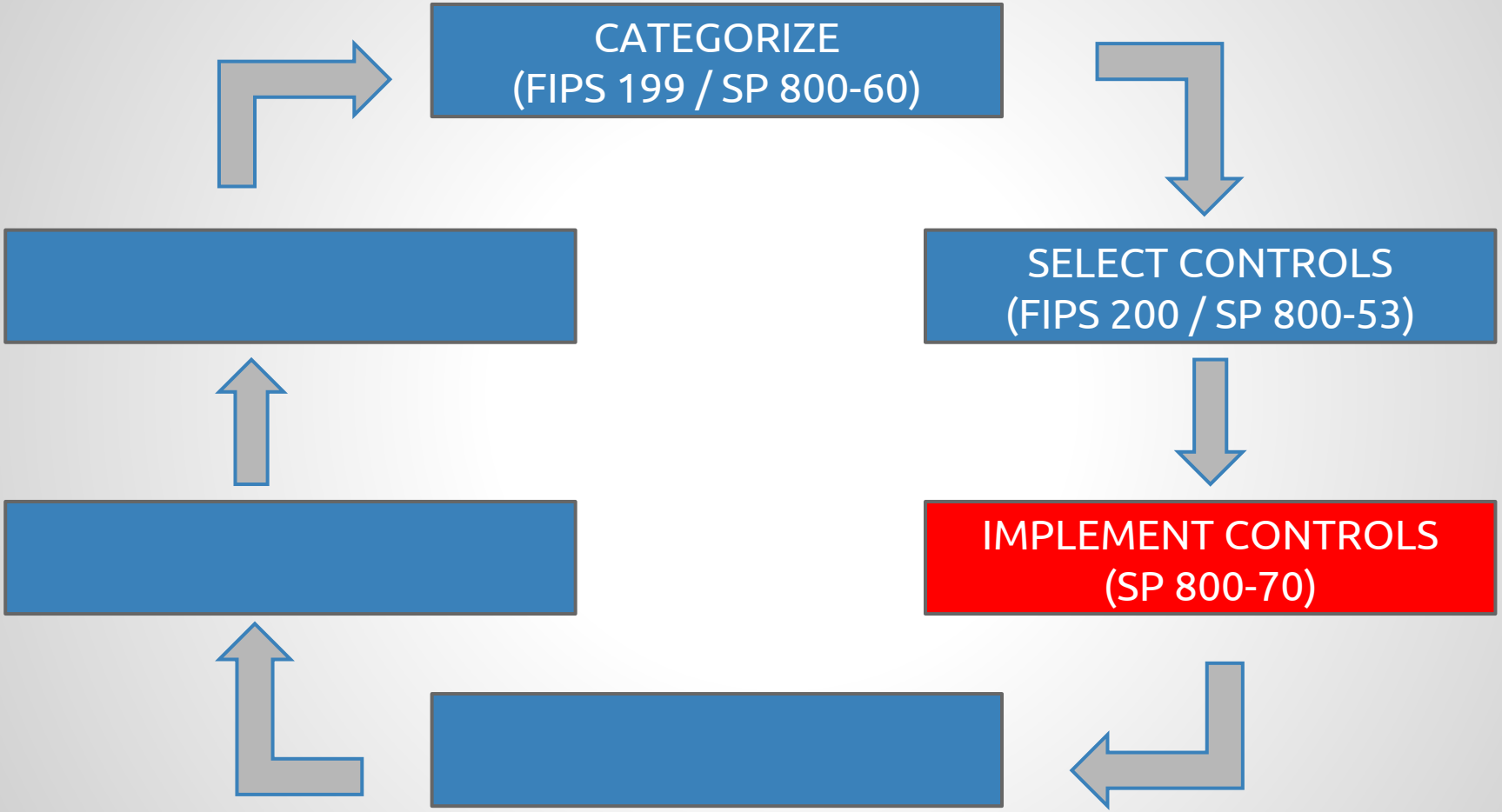
YOU ARE A

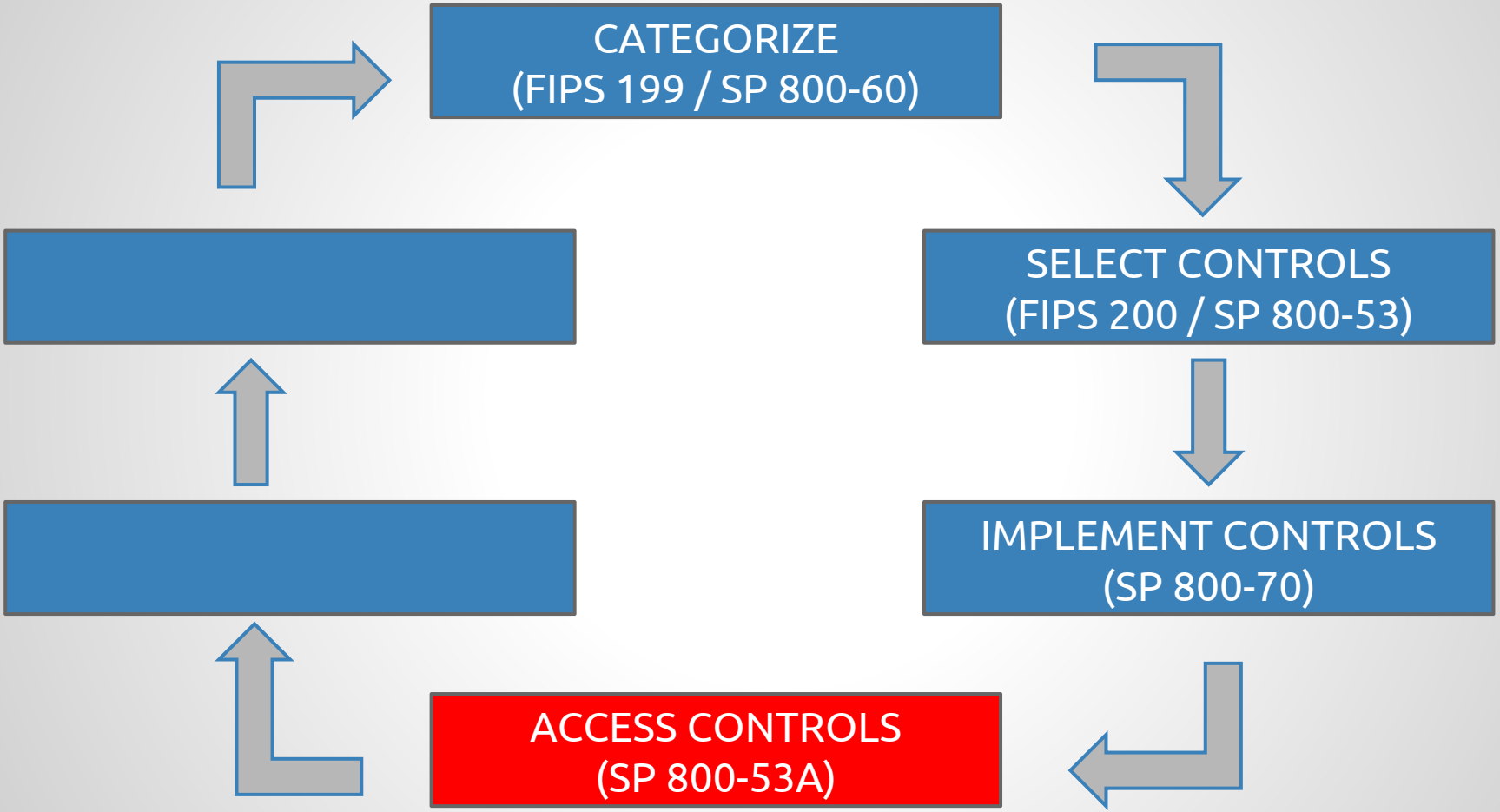
BI-MODAL IT MANUFACTURER

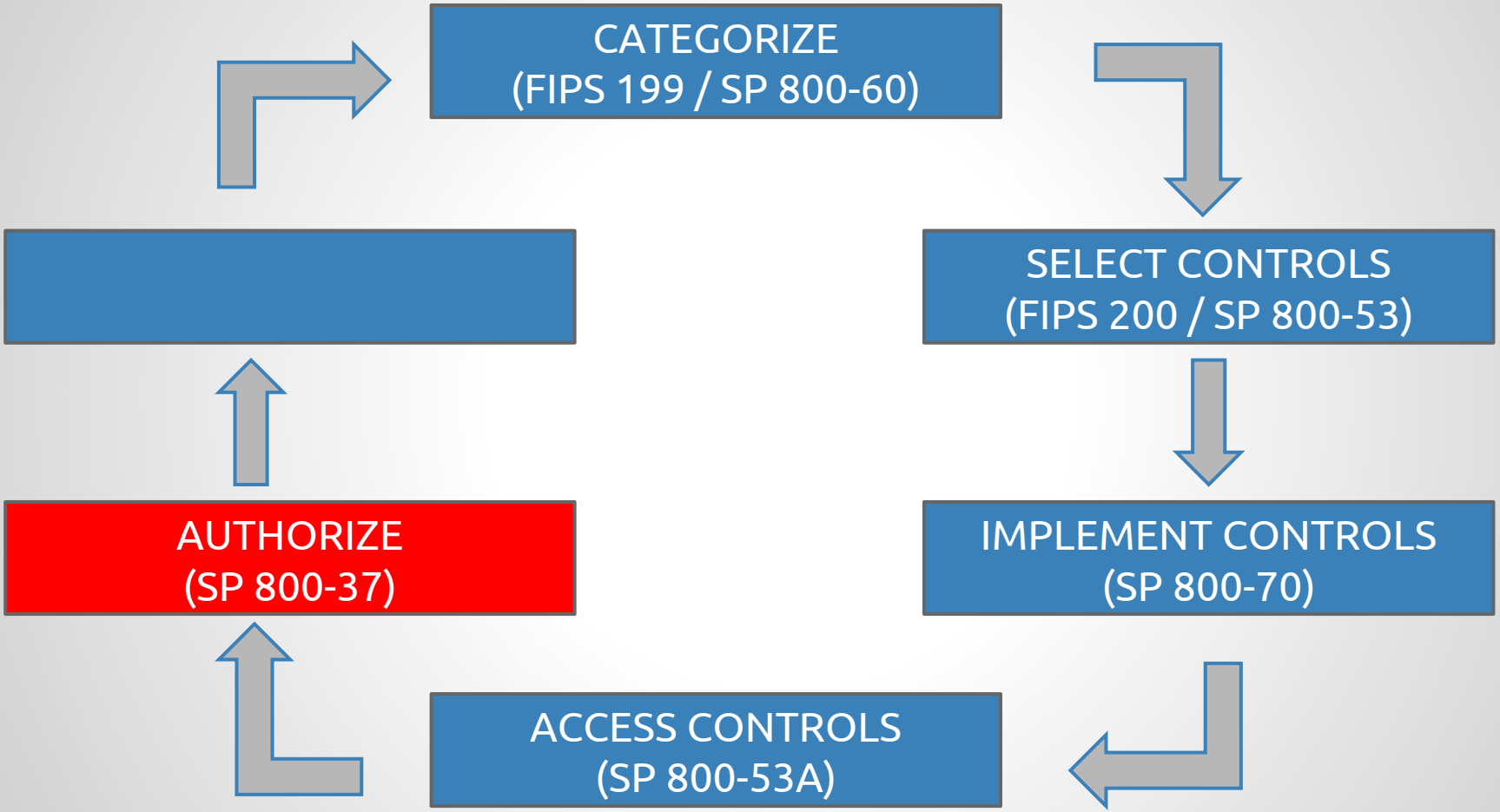


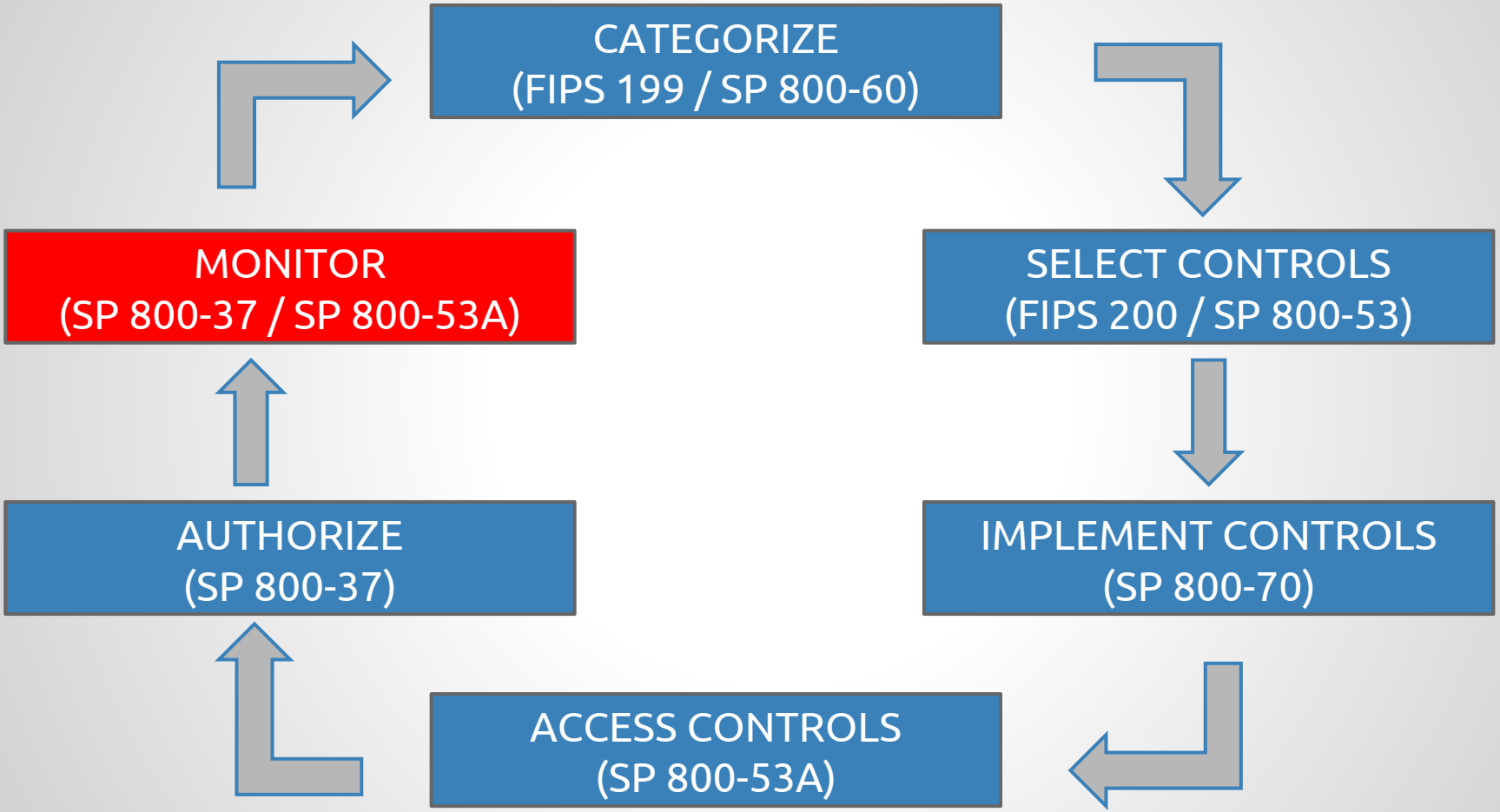

CATEGORIZE
(FIPS 199 / SP 800-60)


CATEGORIZE
(FIPS 199 / SP 800-60)
SELECT CONTROLS
(FIPS 200 / SP 800-53)


CATEGORIZE
(FIPS 199 / SP 800-60)
SELECT CONTROLS
(FIPS 200 / SP 800-53)
IMPLEMENT CONTROLS
(SP 800-70)


CATEGORIZE
(FIPS 199 / SP 800-60)
SELECT CONTROLS
(FIPS 200 / SP 800-53)
IMPLEMENT CONTROLS
(SP 800-70)
ACCESS CONTROLS
(SP 800-53A)


CATEGORIZE
(FIPS 199 / SP 800-60)
SELECT CONTROLS
(FIPS 200 / SP 800-53)
IMPLEMENT CONTROLS
(SP 800-70)
ACCESS CONTROLS
(SP 800-53A)
AUTHORIZE
(SP 800-37)


CATEGORIZE
(FIPS 199 / SP 800-60)
SELECT CONTROLS
(FIPS 200 / SP 800-53)
IMPLEMENT CONTROLS
(SP 800-70)
ACCESS CONTROLS
(SP 800-53A)
AUTHORIZE
(SP 800-37)
MONITOR
(SP 800-37 / SP 800-53A)

… and DevOps goes…

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

Special Publication 800-117

Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0

Everyone knows that SCAP is a suite of XML standards for creating automated checklists for configuration and vulnerability scans!

CVE cve.mitre.org

OVAL Celebrating 10 Years

XCCDF security benchmark automation

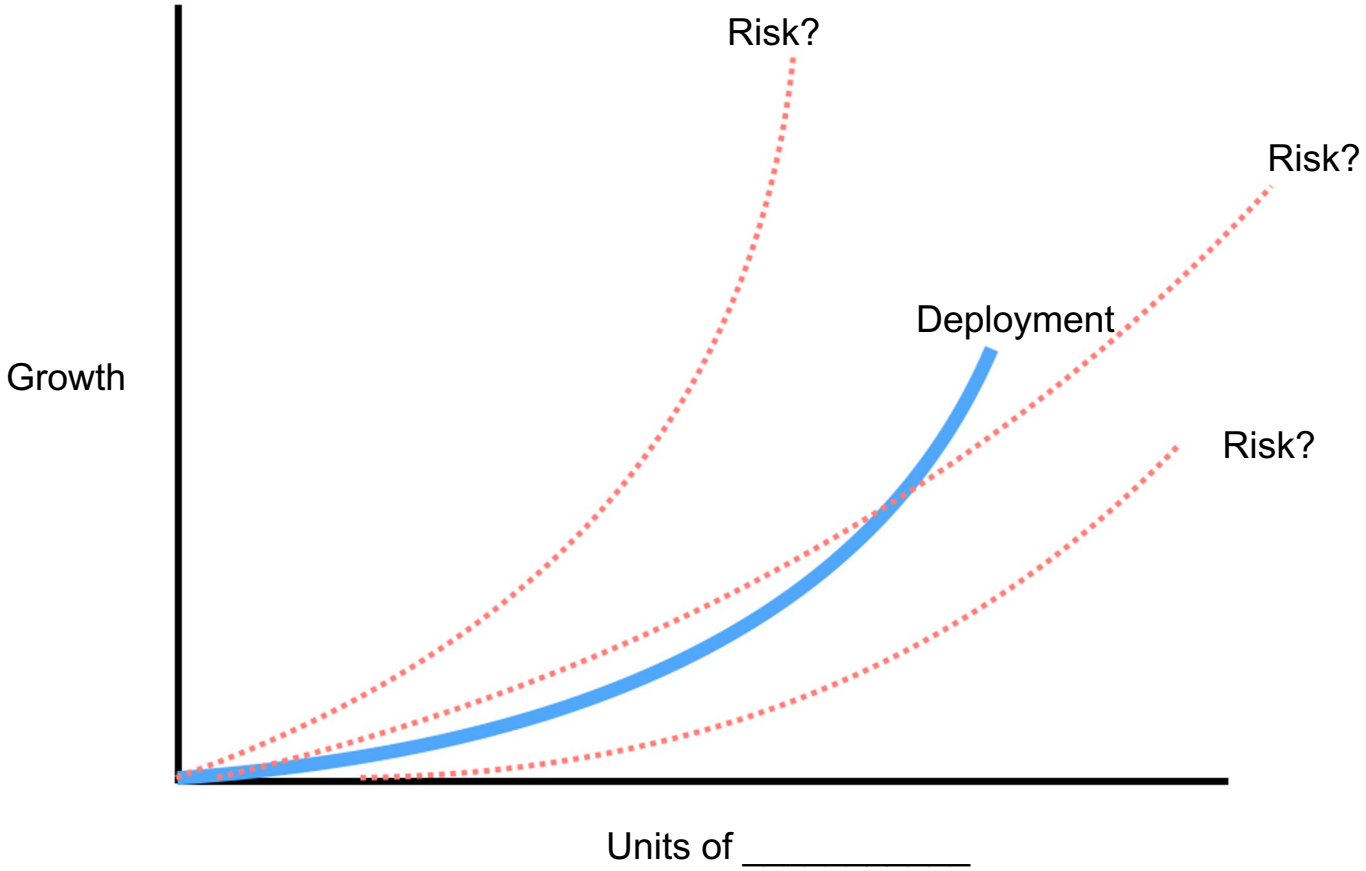
CPE common platform enumeration

CCE Common Configuration Enumeration

CVSS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessments and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Service Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

“Use the families, Luke.”


Risk?
Risk?
Deployment
Growth
Risk?
Units of _____

Community created portfolio of tools and content to make attestations about known vulnerabilities

https://github.com/OpenSCAP

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

ARL
U.S. Army Research Laboratory

OAK RIDGE
National Laboratory

TRESYS TECHNOLOGY

CivicActions
Empowered

GOV READY

LOCKHEED MARTIN

OpenSCAP / scap-security-guide

Unwatch 39 | Star 48 | Fork 46

Baseline compliance content in SCAP formats https://fedorahosted.org/scap-security-guide/

3,626 commits | **1** branch | **18** releases | **29** contributors

branch: **master** | **scap-security-guide** / +

Merge pull request #577 from iankko/rhel7_fedora_display_login_attemp…

mpreisler authored 14 hours ago — latest commit c74bfad597

Chromium	Properly validate Chromium content	22 days ago
Fedora	[Enhancement] [RHEL/7] [Fedora] Add /shared version of 'display_login…	16 hours ago
Firefox	Merge pull request #566 from iankko/oval_symlinks	18 days ago
JBossEAP5	adding JBoss LICENSE file	4 months ago
JBossFuse6	[Bugfix] File permissions	3 months ago
Java	Properly validate Java content	22 days ago
OpenStack	[BugFix] [RHEL/7] [Fedora] [OpenStack] [RHEVM3] Update "nist800-53uri…	2 days ago
RHEL	[Enhancement] [RHEL/7] [Fedora] Add /shared version of 'display_login…	16 hours ago

Code

Issues 147

Pull requests 10

Wiki

Pulse

Graphs

SSH clone URL

git@github.com:Op

You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop

Foreman
OpenSCAP

Ruby Gem
OpenSCAP

Puppet
OpenSCAP

SCAPtimony

Compliance and Scoring

The target system did not satisfy the conditions of 42 rules! Please review rule results and consider applying remediation.

Rule results

14 passed | 42 failed | 4 other

Severity of failed rules

35 low | 6 medium | 1

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	62.500000	100.000000	62.5%

Rule Overview

- [x] pass
- [x] fail
- [x] notchecked
- [x] fixed
- [x] error
- [ ] notselected

Search through XCCDF rules | Search

Limit Password Reuse

Rule ID	xccdf_org.ssgproject.content_rule_accounts_password_pam_unix_remember
Result	fail
Time	2015-06-09T14:59:50
Severity	medium
Identifiers and References	identifiers: CCE-26923-3 references: IA-5(f), IA-5(1)(e), 200, 77, test_attestation
Description	Do not allow users to reuse recent passwords. This can be accomplished by using the `remember` option for the `pam_unix` PAM module. In the file `/etc/pam.d/system-auth`, append `remember=5` to the line which refers to the `pam_unix.so` module, as shown: `password sufficient pam_unix.so existing_options remember=5` The DoD STIG requirement is 5 passwords.
Rationale	Preventing re-use of previous passwords helps ensure that a compromised password is not re-used by a user.

Remediation script:

```
var_password_pam_unix_remember="5"
if grep -q "remember=" /etc/pam.d/system-auth; then
        sed -i --follow-symlink "s/\(remember *= *\).*/\1$var_password_pam_unix_remember/" /etc/pam.d/system-auth
else
        sed -i --follow-symlink "/^password[[:space:]]\+sufficient[[:space:]]\+pam_unix.so/ s/$/ remember=$var_password_pam_unix_remember/
```

$ govready scan

```
>
> This profile identifies 4 high severity selected controls.
>      OpenSCAP says 2 passing, 1 failing, and 1 notchecked.
>
> This profile identifies 12 medium severity selected controls.
>      OpenSCAP says 11 passing, 0 failing, and 1 notchecked.
>
> This profile identifies 44 low severity selected controls.
>      OpenSCAP says 40 passing, 2 failing, and 2 notchecked.
>
```

FOREMAN

Admin User

Any Context | Monitor | Hosts | Configure | Infrastructure | Administer

Compliance policy: fedora20-common-profile

Hosts Breakdown

Compliant with the policy	2
Not compliant with the policy	0
Inconclusive results	0
Never audited	0

Total hosts: 2

Host Breakdown Chart

Latest reports for policy: fedora20-common-profile

Host	Date	Passed	Failed	Other	
fedora20.mydomain	1 day ago	0	0	0	View Report
fedora20.mydomain	3 months ago	0	0	0	View Report
fedora20.mydomain	3 months ago	0	0	0	View Report
fedora20.mydomain	3 months ago	0	0	0	View Report
fedora20.mydomain	3 months ago	0	0	0	View Report


WE CAN DO MORE
WHEN WE WORK
TOGETHER

HOW TO ENGAGE

OpenSCAP GitHub:
https://github.com/OpenSCAP

NIST SCAP Website:
https://scap.nist.gov

OpenSCAP References & Docs:
https://github.com/OpenSCAP/scap-security-guide/wiki/Collateral-and-References

SCAP Content Mailing List:
https://fedorahosted.org/mailman/listinfo/scap-security-guide

GovReady user-friendly front-end:
https://github.com/GovReady/govready

Ansible-SCAP (+ Vagrant) demo. See how it all works - painlessly:
https://github.com/openprivacy/ansible-scap

CONTACT INFO

Shawn Wells
shawn@redhat.com
443-534-0130

Greg Elin
gregelin@gitmachines.com
917-304-3488

Fen Labalme
fen@civicactions.com
412-996-4113