Alone in the Dark

DevOps Primer for INFOSEC

WE’VE HEARD THE STORIES . . . .

amazon.com®

Mean time between deployments: 11.6s (310/hour)

Max number of deployments in an hour: 1,079

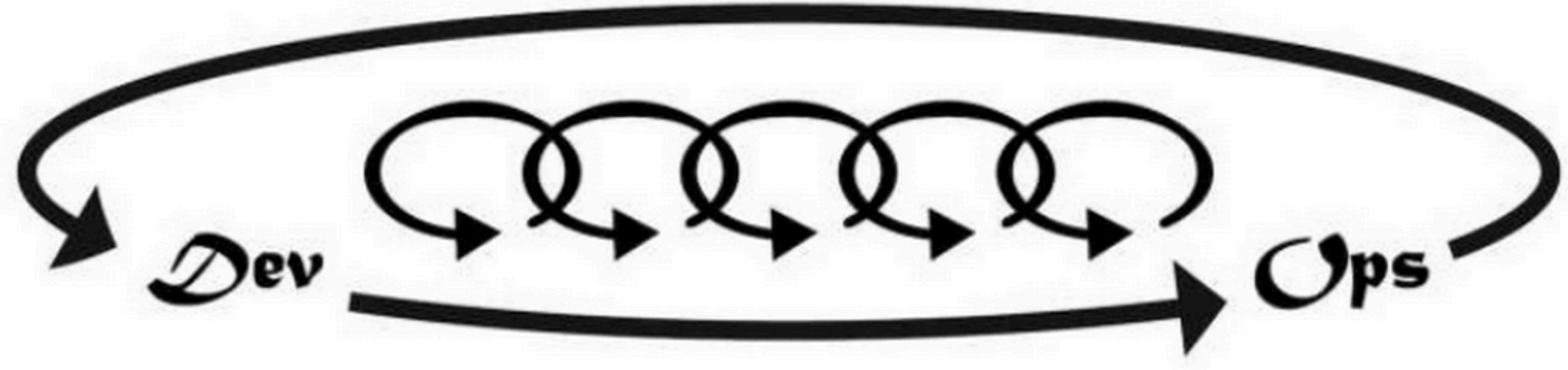
Mean number of hosts receiving a deployment: 10,000

WE’VE HEARD THE STORIES . . . .

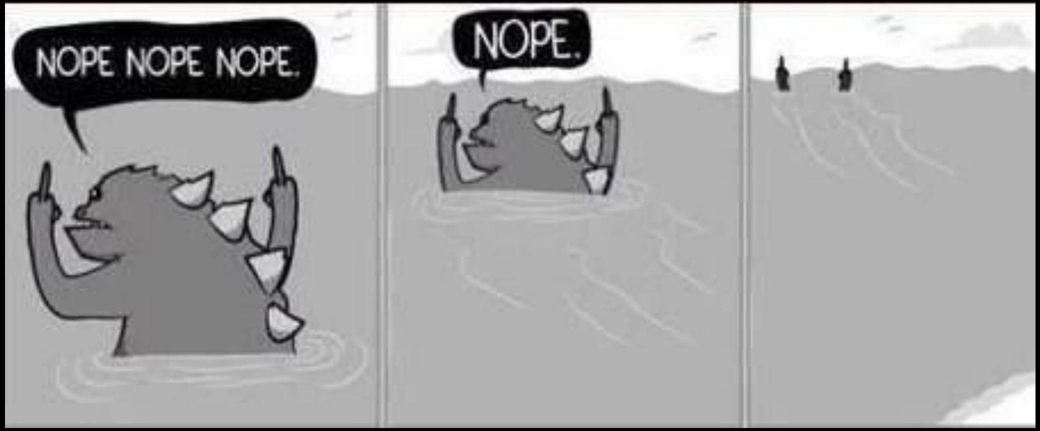
Etsy

2013:	30+ deploys/day
March 2014:	50+ deploys/day
April 2014:	80-90+/day

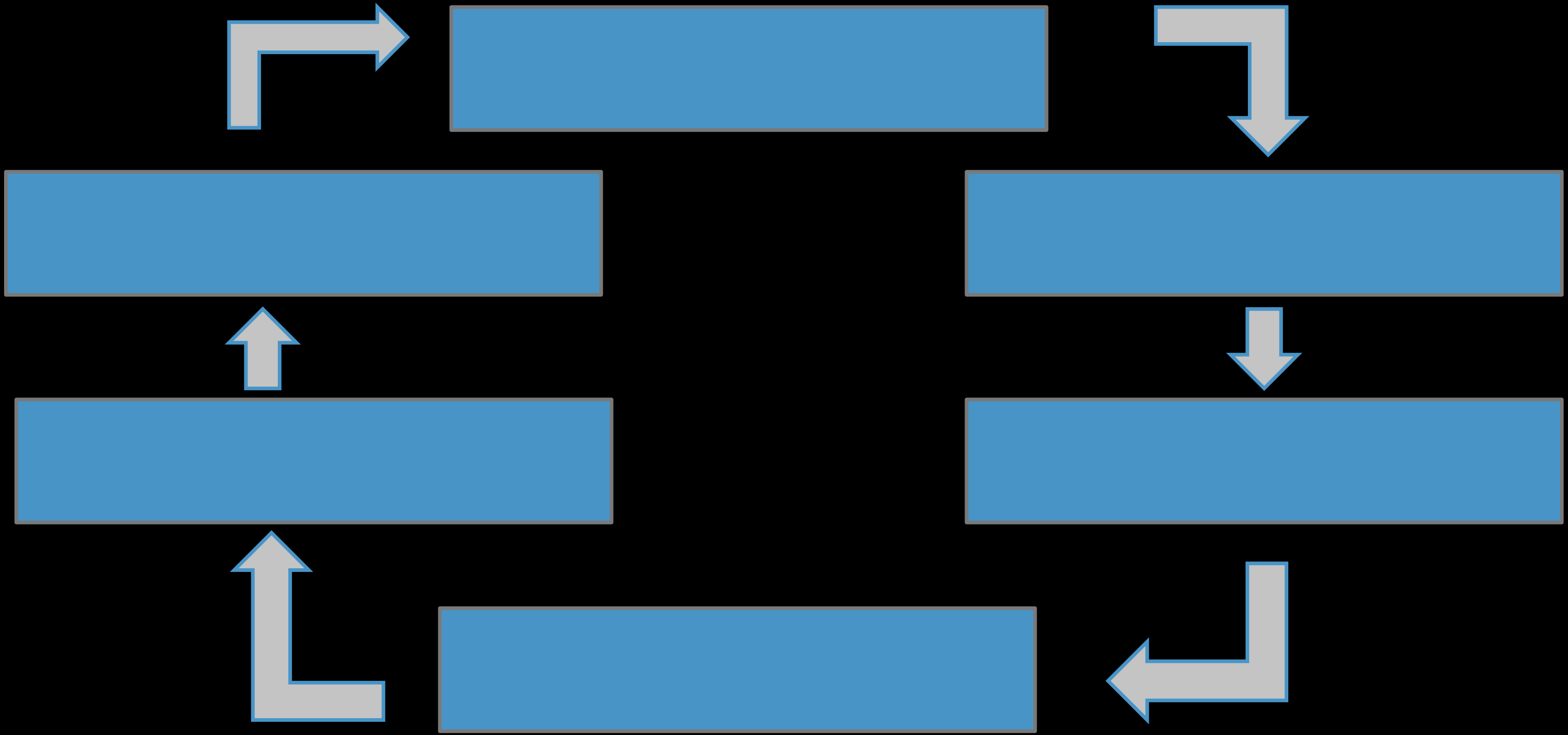
WE'VE HEARD DEV/OPS PROCESS . . .



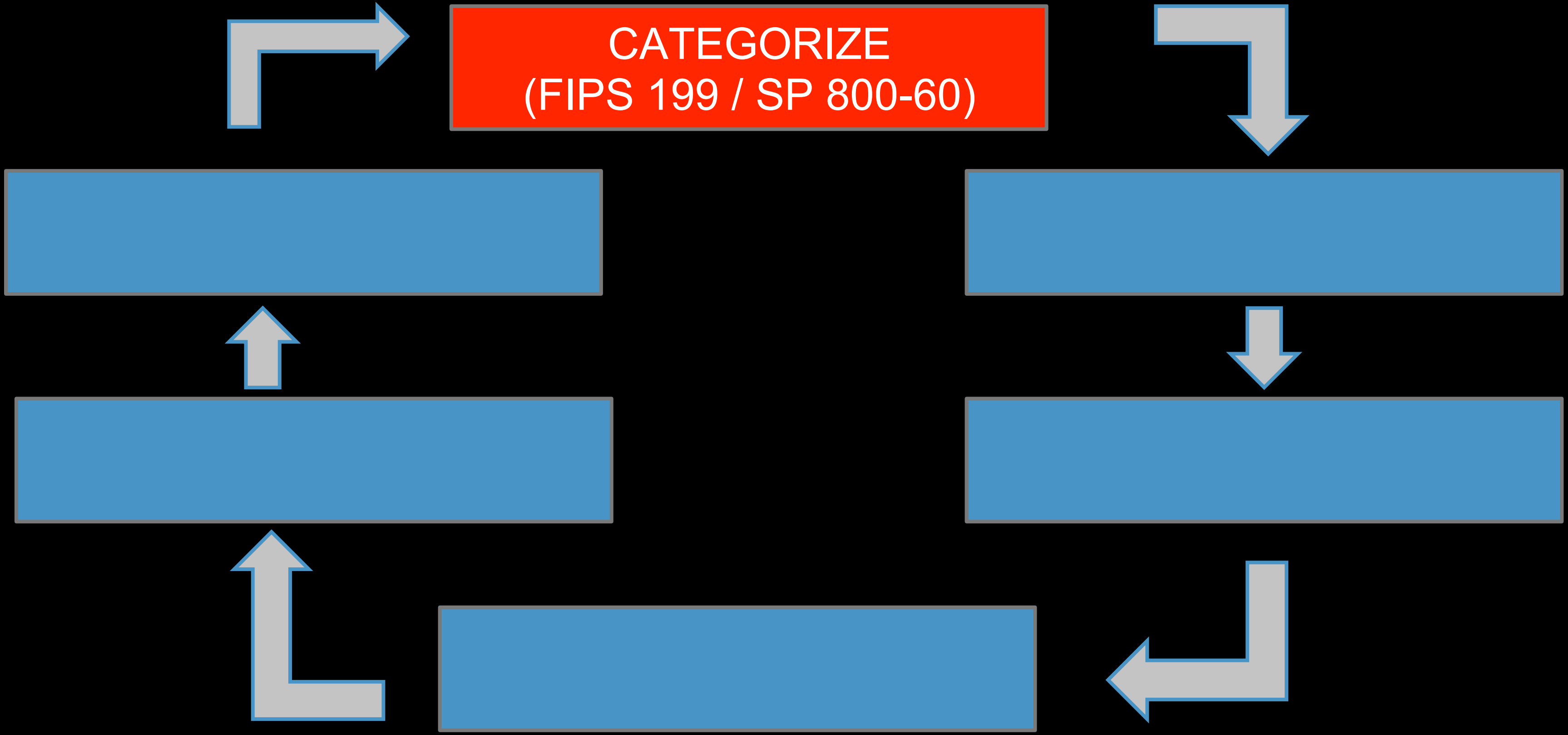
Meanwhile, in Government . . .



MEANWHILE, IN GOVERNMENT . . .

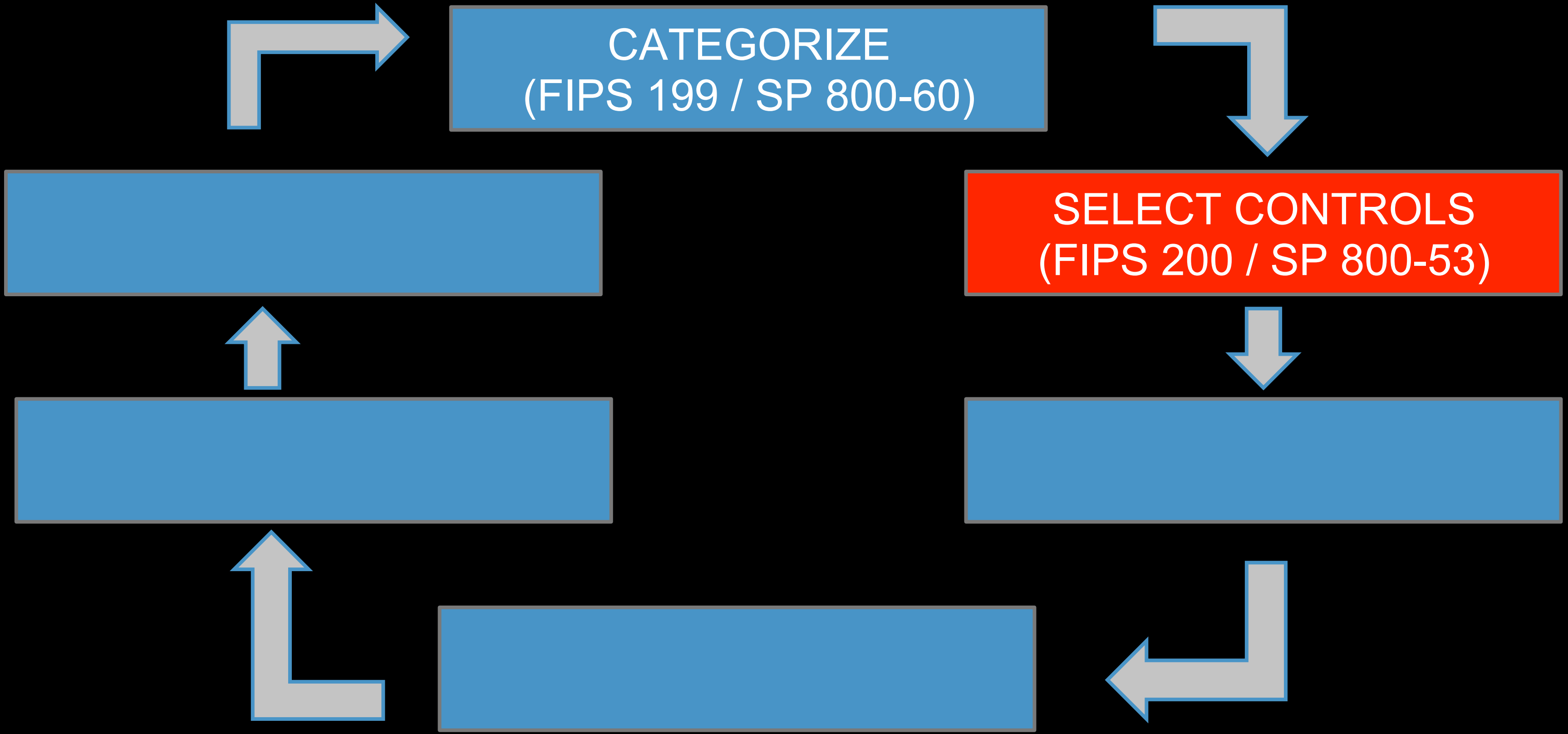


MEANWHILE, IN GOVERNMENT . . .



CATEGORIZE
(FIPS 199 / SP 800-60)

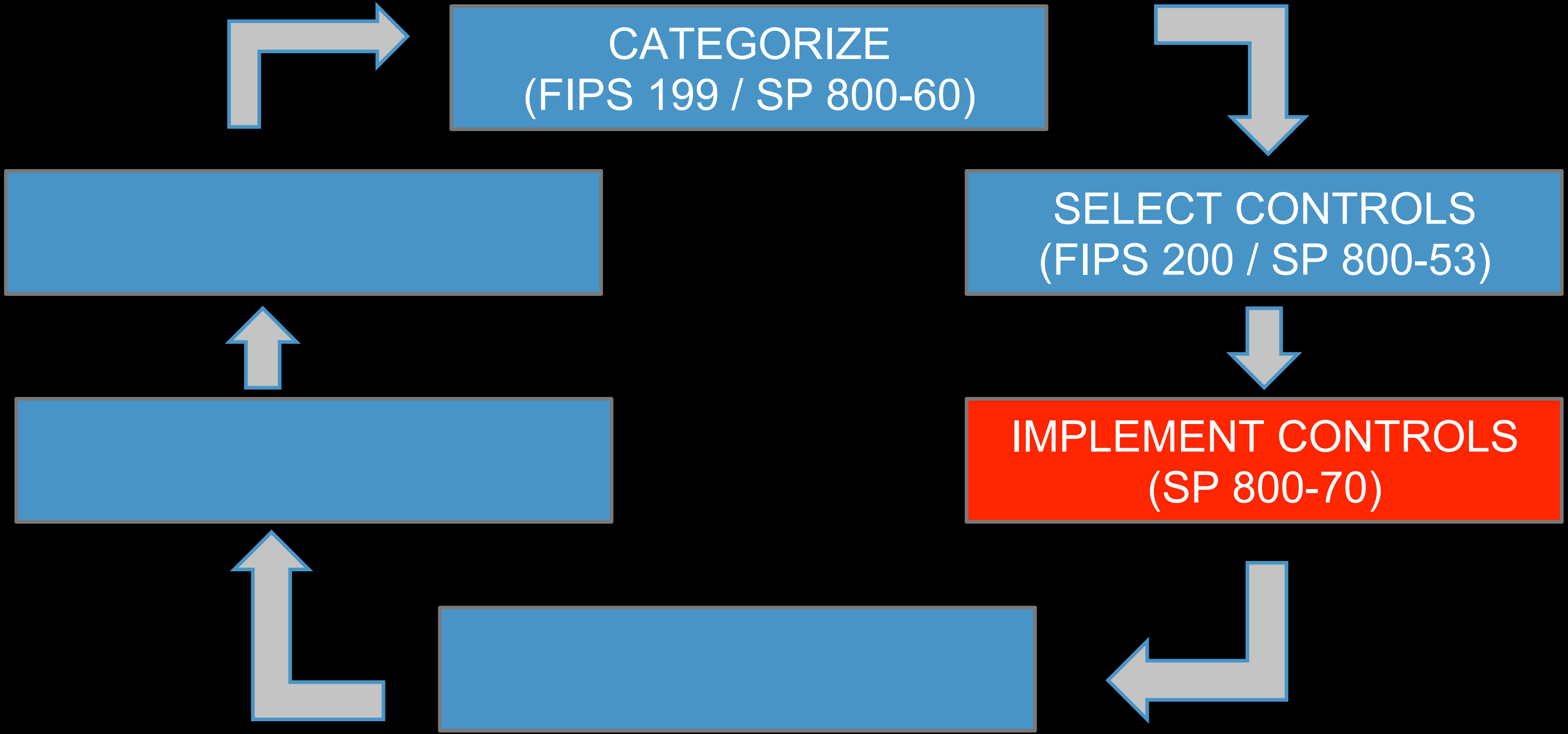
MEANWHILE, IN GOVERNMENT . . .



CATEGORIZE
(FIPS 199 / SP 800-60)

SELECT CONTROLS
(FIPS 200 / SP 800-53)

MEANWHILE, IN GOVERNMENT . . .

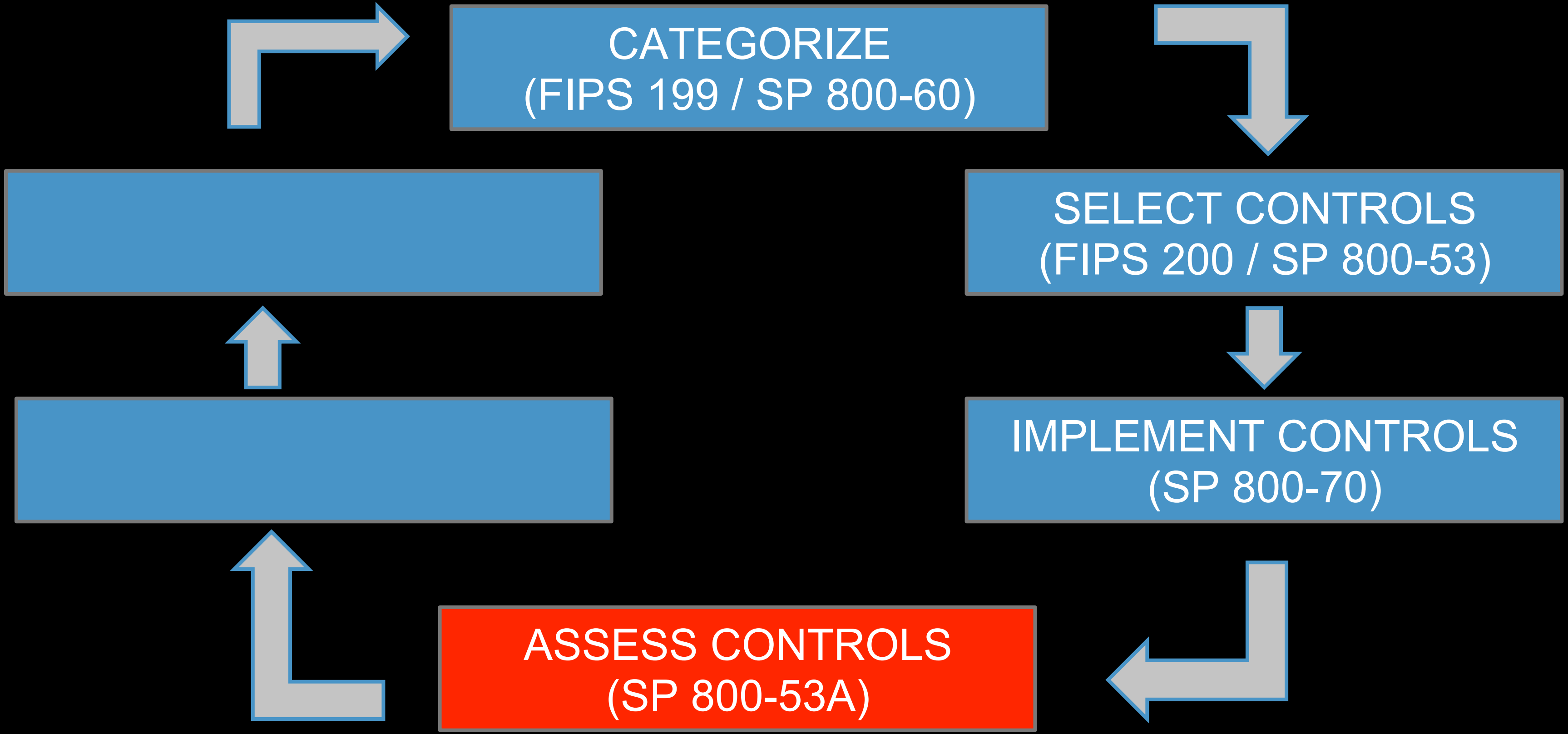


CATEGORIZE
(FIPS 199 / SP 800-60)

SELECT CONTROLS
(FIPS 200 / SP 800-53)

IMPLEMENT CONTROLS
(SP 800-70)

MEANWHILE, IN GOVERNMENT . . .



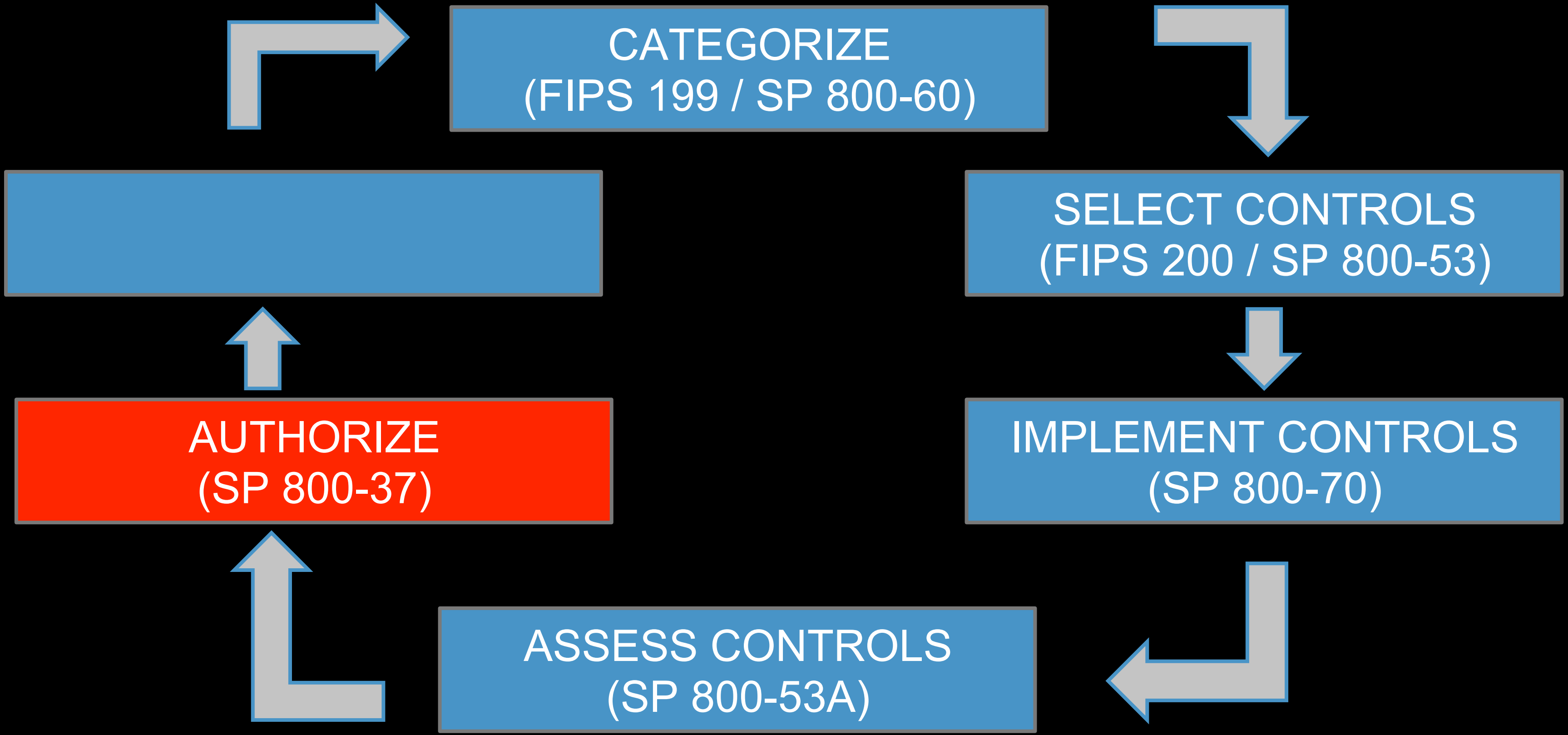
CATEGORIZE
(FIPS 199 / SP 800-60)

SELECT CONTROLS
(FIPS 200 / SP 800-53)

IMPLEMENT CONTROLS
(SP 800-70)

ASSESS CONTROLS
(SP 800-53A)

MEANWHILE, IN GOVERNMENT . . .



CATEGORIZE
(FIPS 199 / SP 800-60)

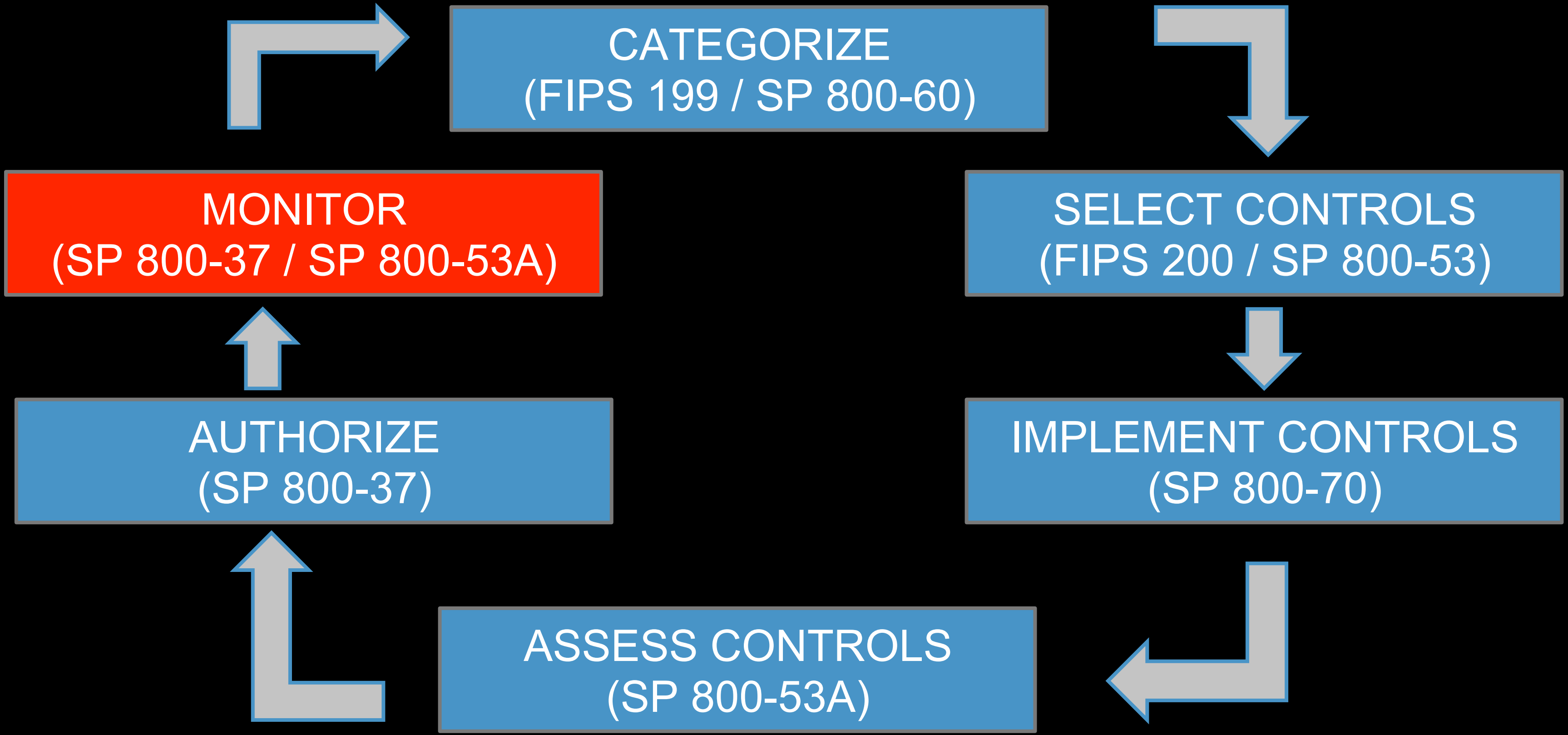
SELECT CONTROLS
(FIPS 200 / SP 800-53)

IMPLEMENT CONTROLS
(SP 800-70)

ASSESS CONTROLS
(SP 800-53A)

AUTHORIZE
(SP 800-37)

MEANWHILE, IN GOVERNMENT . . .



CATEGORIZE
(FIPS 199 / SP 800-60)

SELECT CONTROLS
(FIPS 200 / SP 800-53)

IMPLEMENT CONTROLS
(SP 800-70)

ASSESS CONTROLS
(SP 800-53A)

AUTHORIZE
(SP 800-37)

MONITOR
(SP 800-37 / SP 800-53A)

… and DevOps goes …

INITIATIVE #1: STANDARDIZE CONTROLS + CONFIGURATION BASELINES

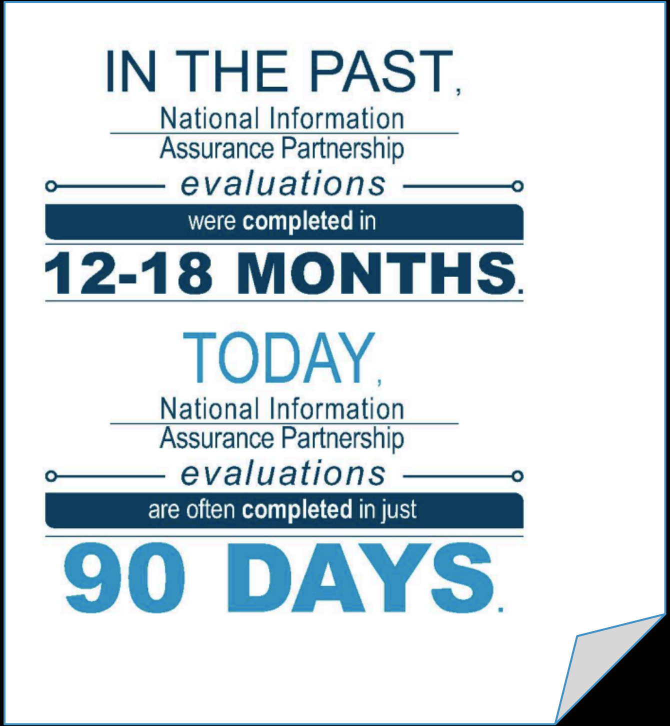
INITIATIVE #2: AUTOMATE ASSESSMENT

INITIATIVE #1: STANDARDIZE CONTROLS + CONFIGURATION BASELINES

- Common Criteria modernization, driven by NSA and NIST

- Consolidate DoD STIG, USGCB into one baseline

- Operating System controls >500 (RHEL6), now ~20 (RHEL7)



IN THE PAST,

National Information Assurance Partnership *evaluations*

were **completed** in

12-18 MONTHS.

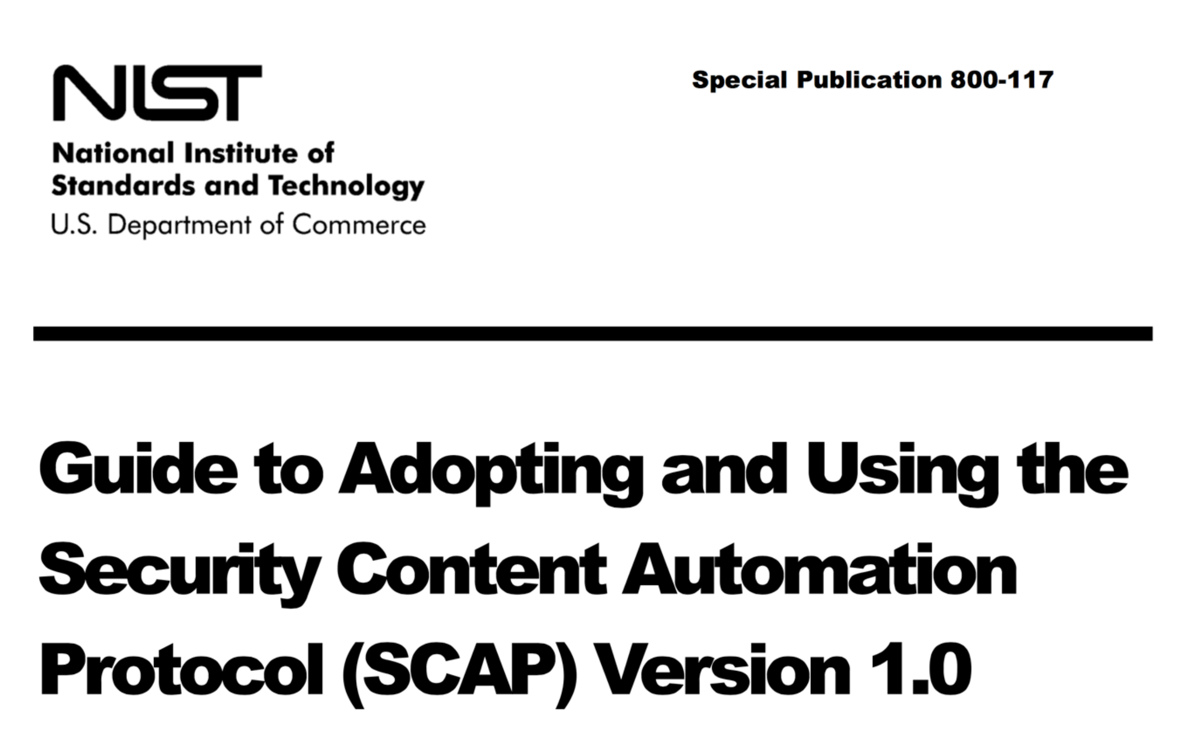
TODAY,

National Information Assurance Partnership *evaluations*

are often **completed** in just

90 DAYS.

INITIATIVE #2: AUTOMATE ASSESSMENT



NIST

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

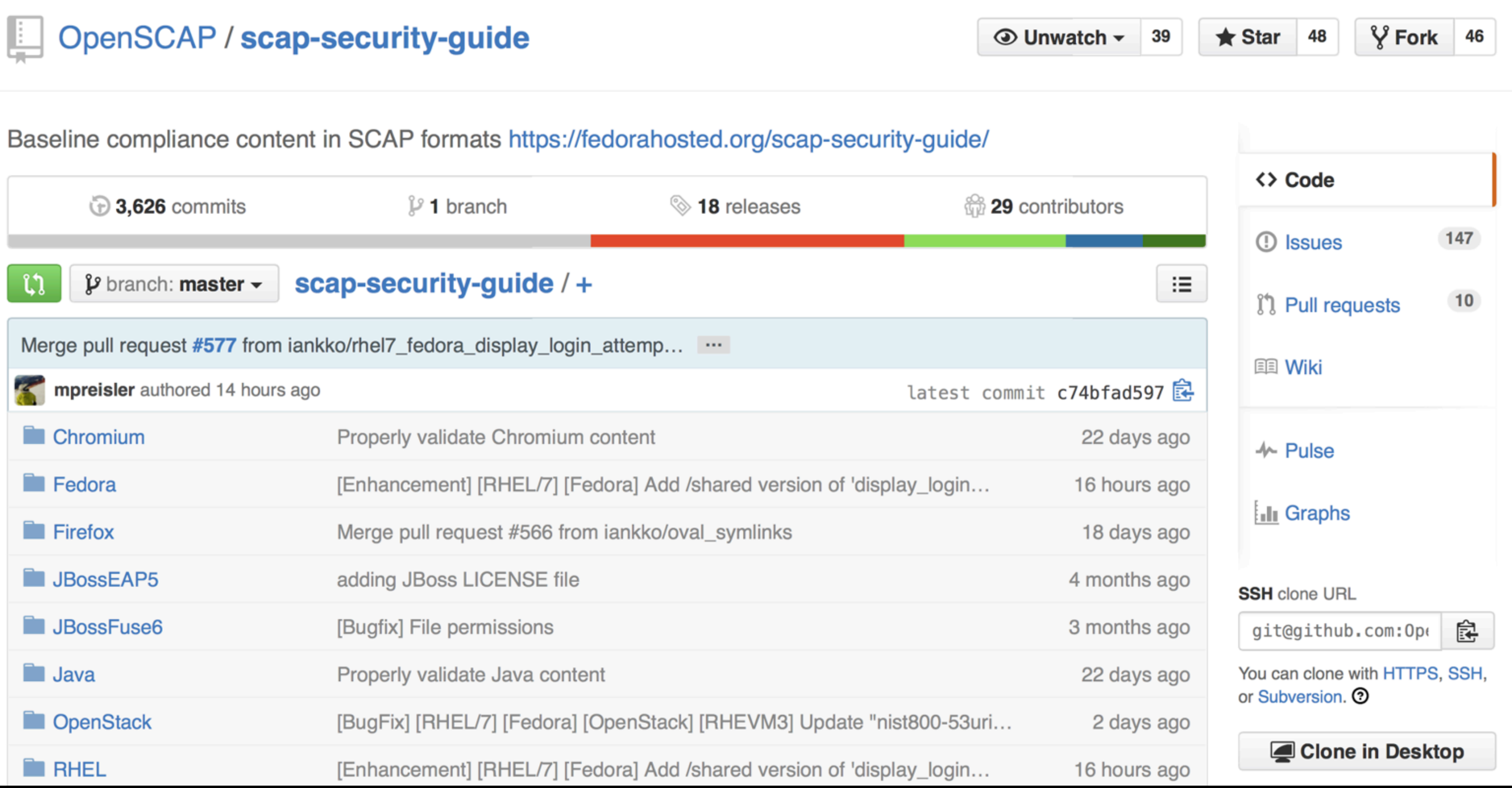
CVSS

OpenSCAP

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

https://github.com/OpenSCAP

DEFENSE INFORMATION SYSTEMS AGENCY
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
ARL
U.S. Army Research Laboratory
OAK RIDGE
National Laboratory
TRESYS
TECHNOLOGY
CivicActions
Empowered
G2
GOV READY
LOCKHEED MARTIN
redhat



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

3,626 commits 1 branch 18 releases 29 contributors

Merge pull request #577 from iankko/rhel7_fedora_display_login_attemp… …

mpreisler authored 14 hours ago latest commit c74bfad597

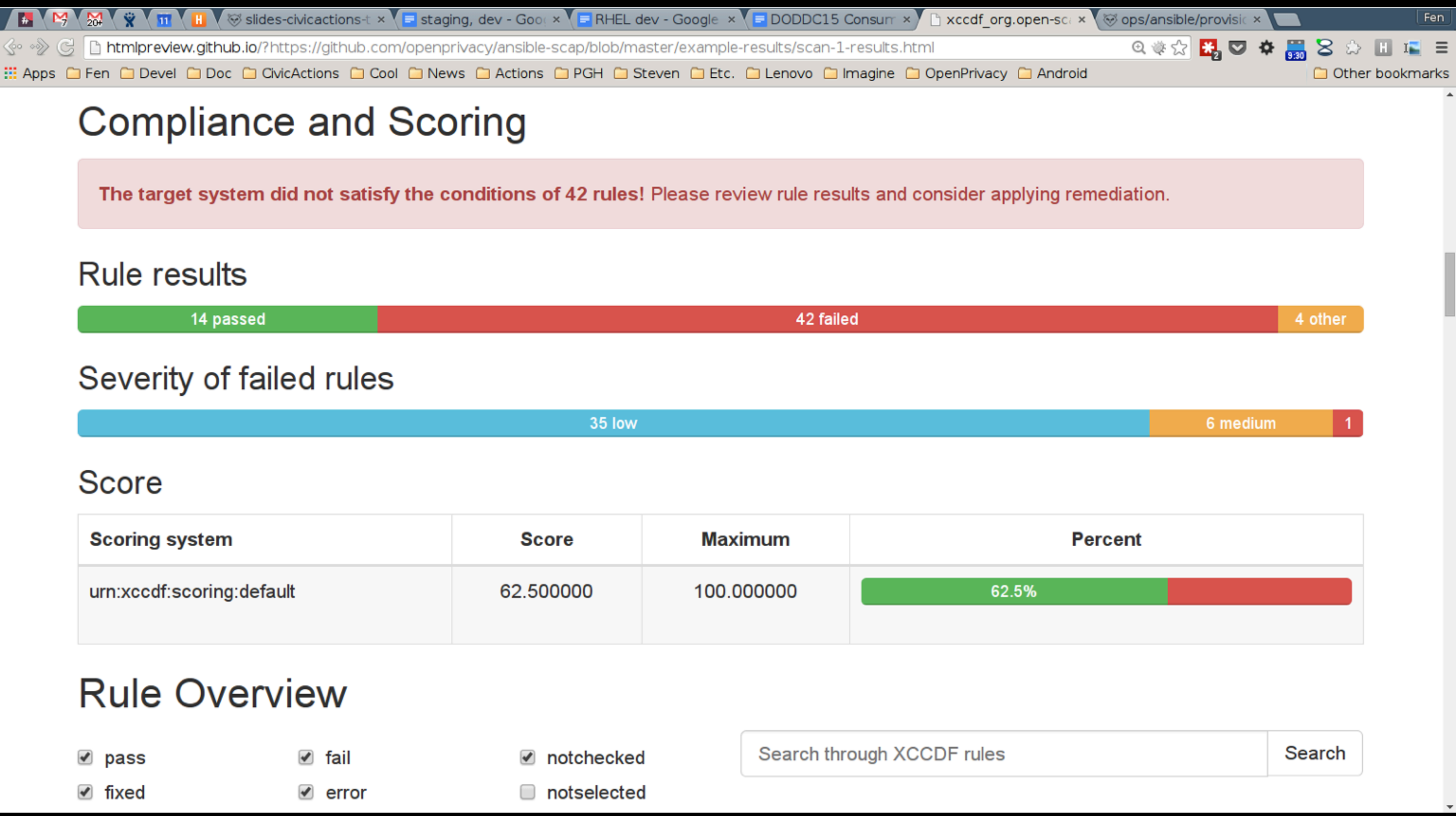
Chromium	Properly validate Chromium content	22 days ago
Fedora	[Enhancement] [RHEL/7] [Fedora] Add /shared version of 'display_login…	16 hours ago
Firefox	Merge pull request #566 from iankko/oval_symlinks	18 days ago
JBossEAP5	adding JBoss LICENSE file	4 months ago
JBossFuse6	[Bugfix] File permissions	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

SSH clone URL

git@github.com:Op

You can clone with HTTPS, SSH, or Subversion.

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

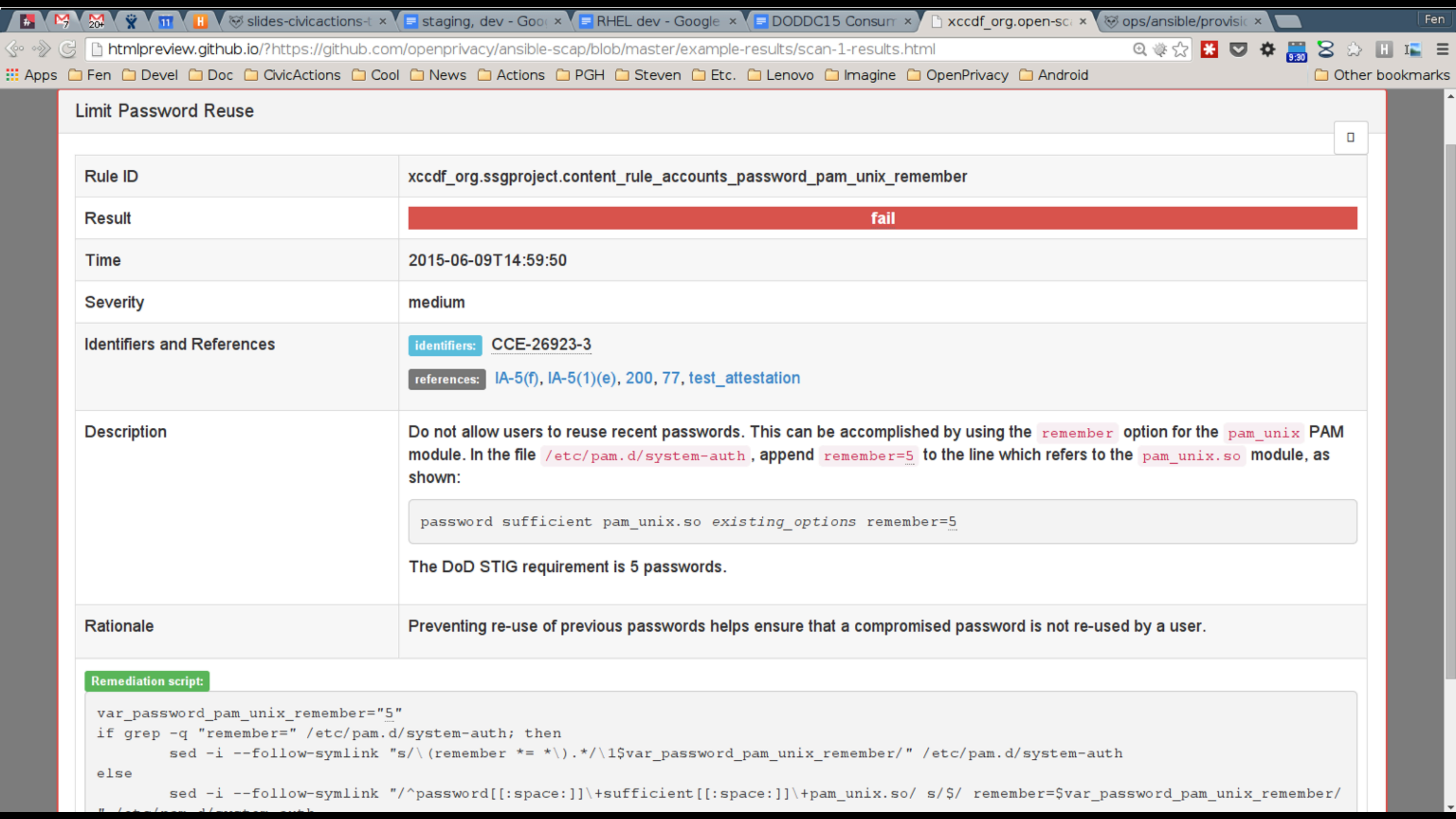
Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	62.500000	100.000000	62.5%

Rule Overview

☑ pass ☑ fail ☑ notchecked

☑ fixed ☑ 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/
" /etc/pam.d/system-auth
```

WE CAN DO MORE WHEN WE WORK TOGETHER

HOW TO ENGAGE

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

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

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

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

CONTACT INFO

Shawn Wells

Director, Innovation Programs
Red Hat Public Sector

shawn@redhat.com
443-534-0130