

Operational Compliance

From Requirements to Reality

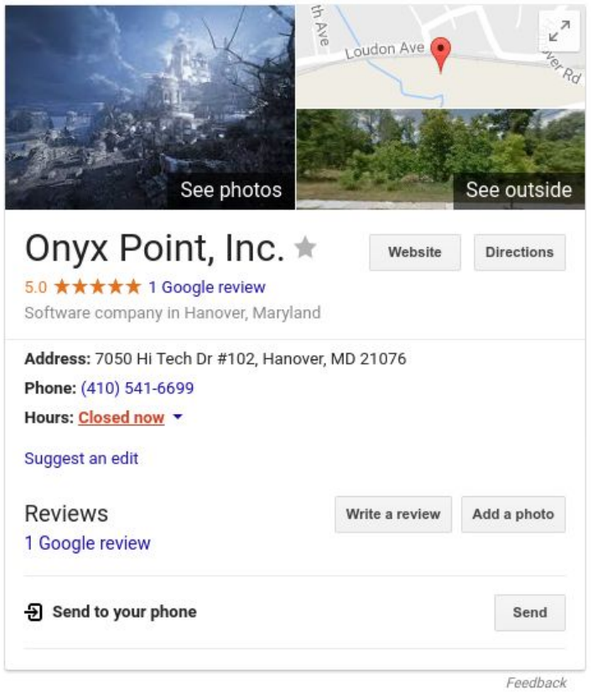
Trevor Vaughan
VP Engineering - Onyx Point, Inc.
SIMP Product Lead
B.S. Computer Engineering,
M. S. Information Assurance
RHCE, PCP, PCD

All trademarks are property of their respective owners. All company, product and service names used in this presentation are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.



- Automation, Security, and Compliance
  - Consulting and Contracting since 2009
    - Government and Commercial
    - Cloud Infrastructure
    - Distributed Data Flow Architectures
    - DevOps Workflow
    - Test Automation
    - Focus on Compliance
- Maintainers of SIMP

OnyxPoint


See photos
Loudon Ave
See outside
Onyx Point, Inc.
Website
Directions
5.0 ★★★★★ 1 Google review
Software company in Hanover, Maryland
Address: 7050 Hi Tech Dr #102, Hanover, MD 21076
Phone: (410) 541-6699
Hours: Closed now
Suggest an edit
Reviews
Write a review
Add a photo
1 Google review
Send to your phone
Send
Feedback



WARNING

This content is **highly opinionated**

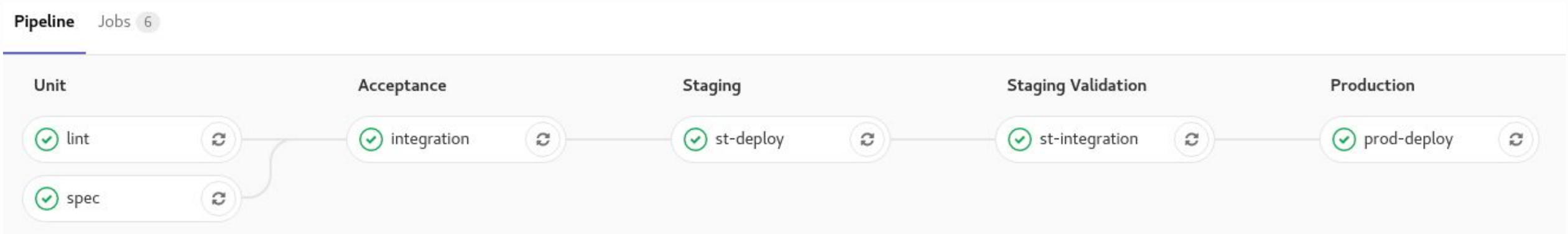



Weekend
Loading... Please Wait

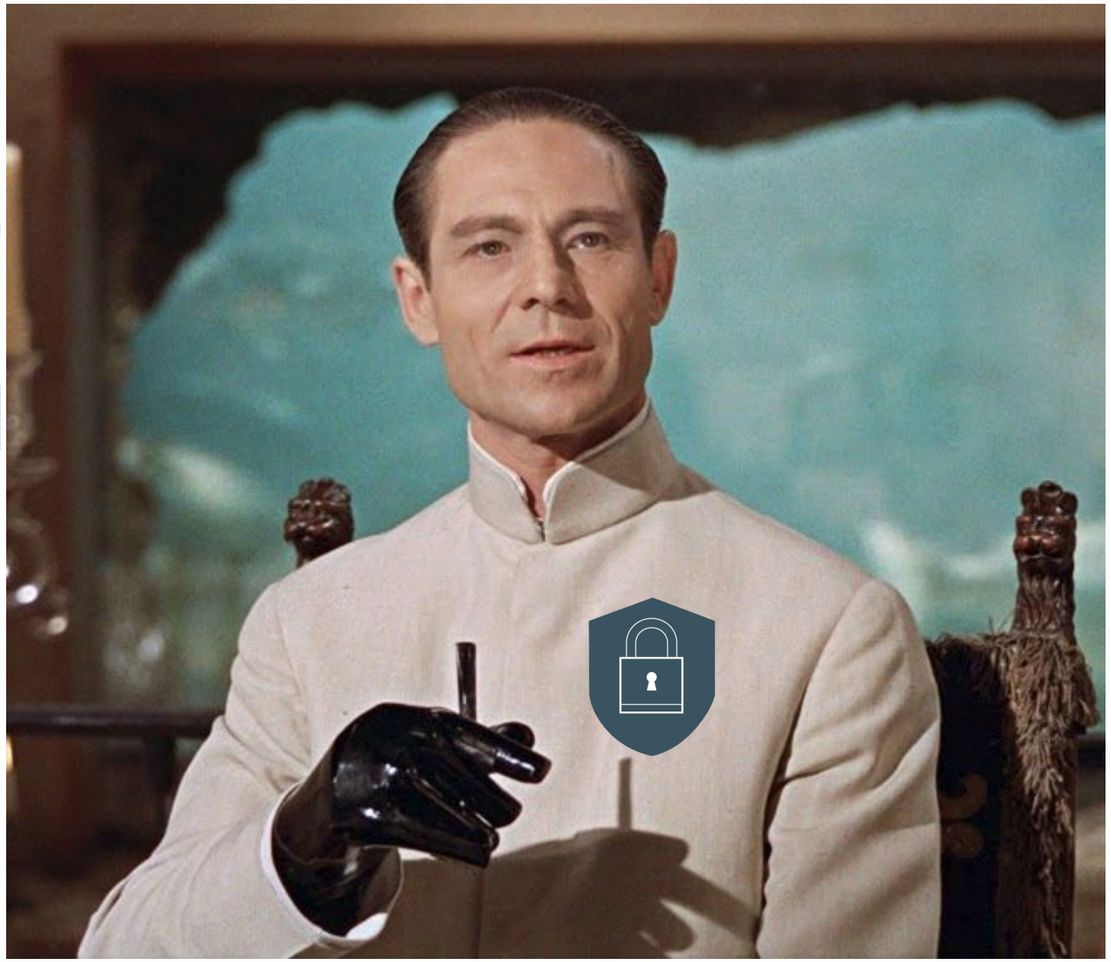

I DON'T ALWAYS
git push -f
BUT WHEN I DO
I DO IT IN PRODUCTION
imgflip.com



GitLab


Pipeline
Jobs 6
Unit
lint
spec
Acceptance
integration
Staging
st-deploy
Staging Validation
st-integration
Production
prod-deploy

BUT WAIT!
DID YOU NOTIFY…



PCI Security Standards Council

COMPLY WITH

Sarbanes-Oxley Compliant

HIPAA Health Insurance Portability & Accountability Act

GLBA Gramm-Leach-Bliley Act

NIST National Institute of Standards and Technology

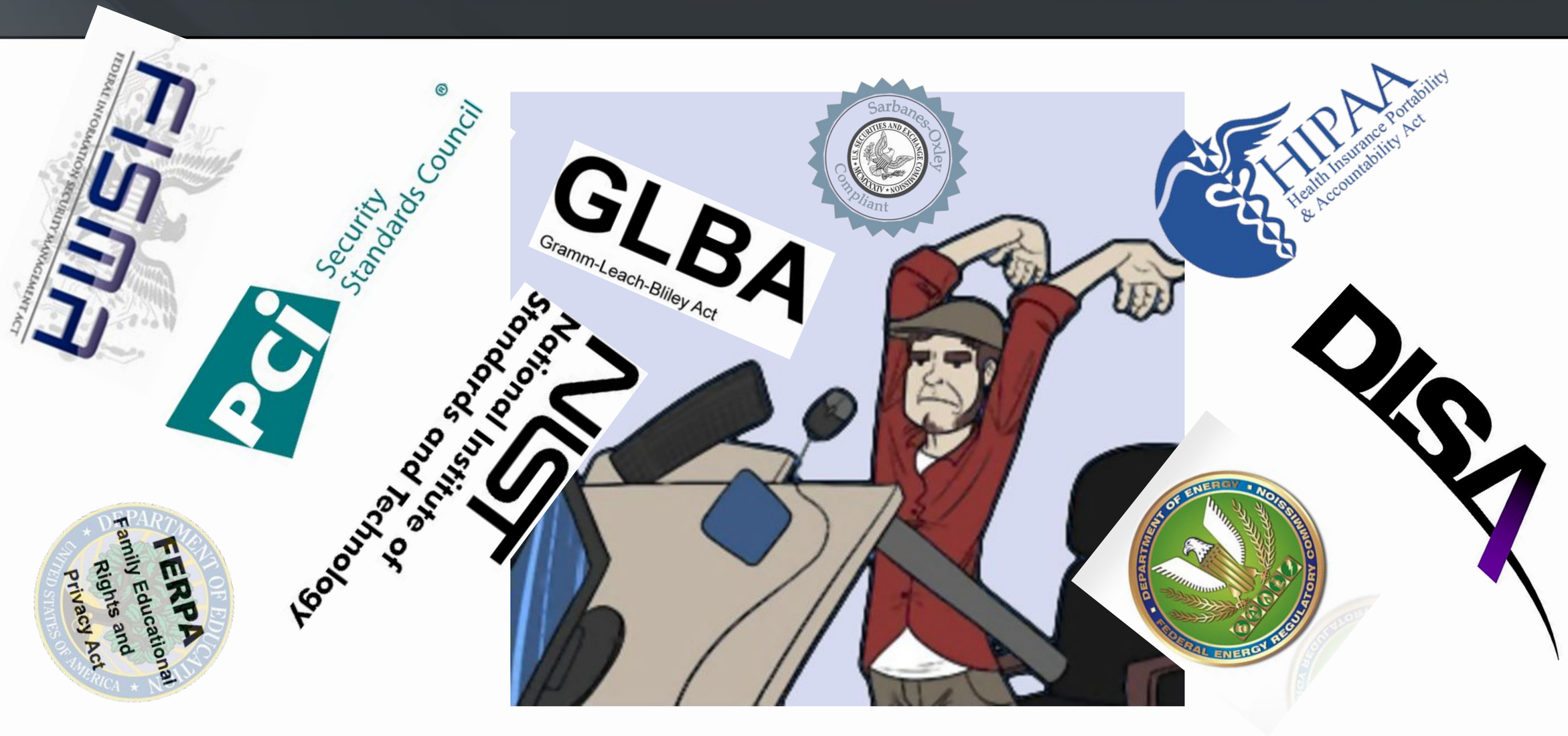
DISA



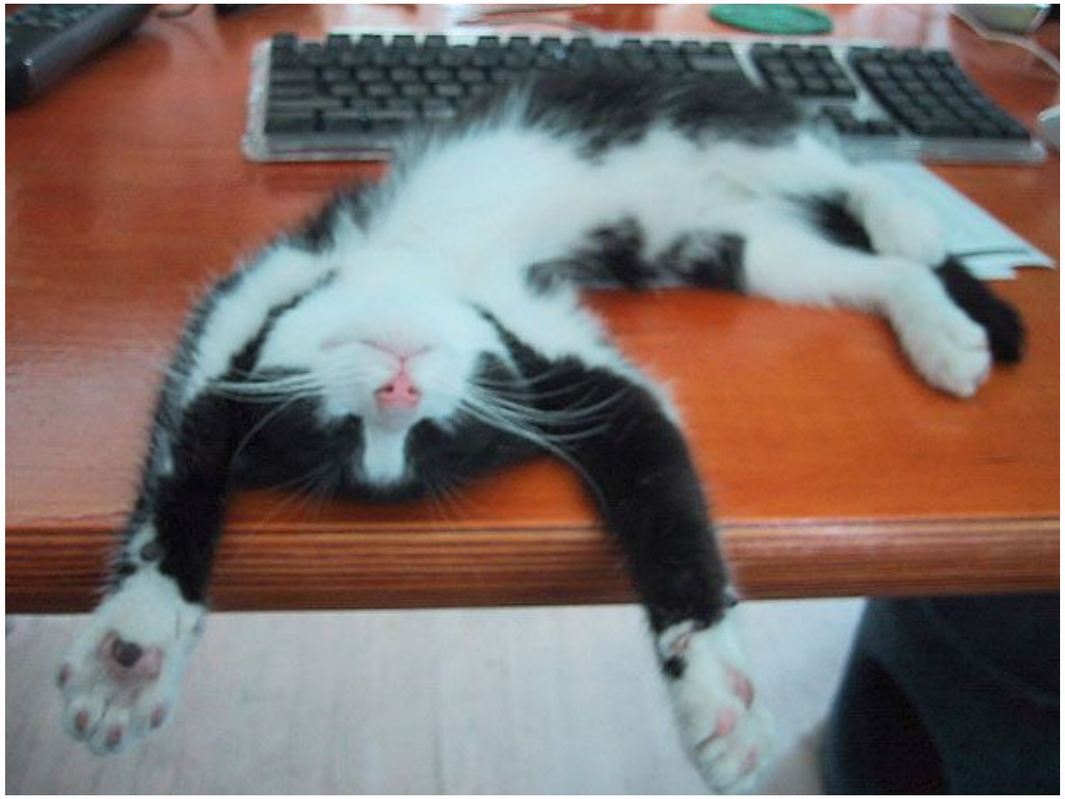
FERPA Family Educational Rights and Privacy Act

FISMA Federal Information Security Management Act

Department of Energy Federal Energy Regulatory Commission

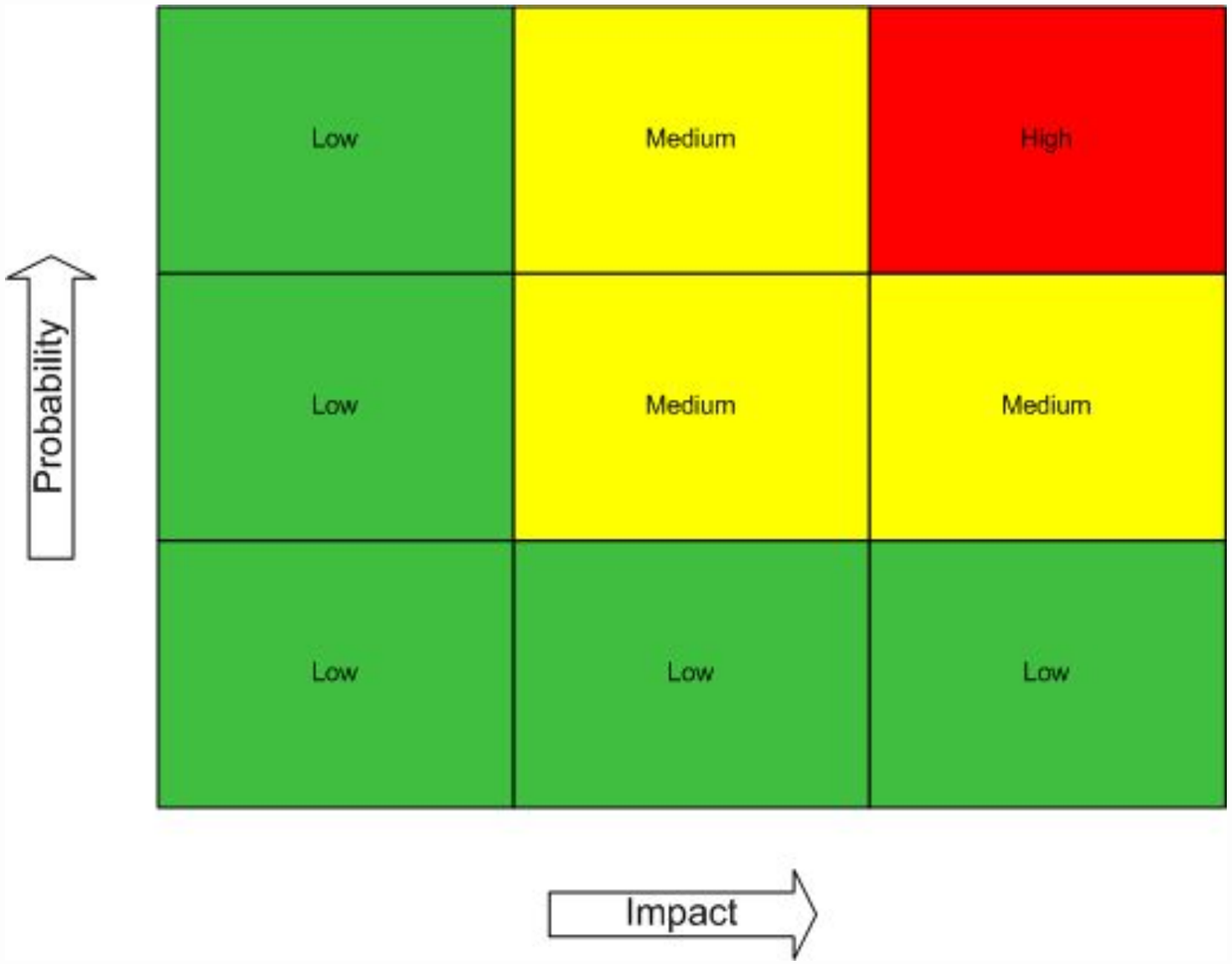

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
PCI Security Standards Council
GLBA
Gramm-Leach-Bliley Act
Sarbanes-Oxley
U.S. SECURITIES AND EXCHANGE COMMISSION
Compliant
HIPAA
Health Insurance Portability & Accountability Act
NIST
National Institute of Standards and Technology
DISA
DEPARTMENT OF EDUCATION
FERPA
Family Educational Rights and Privacy Act
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

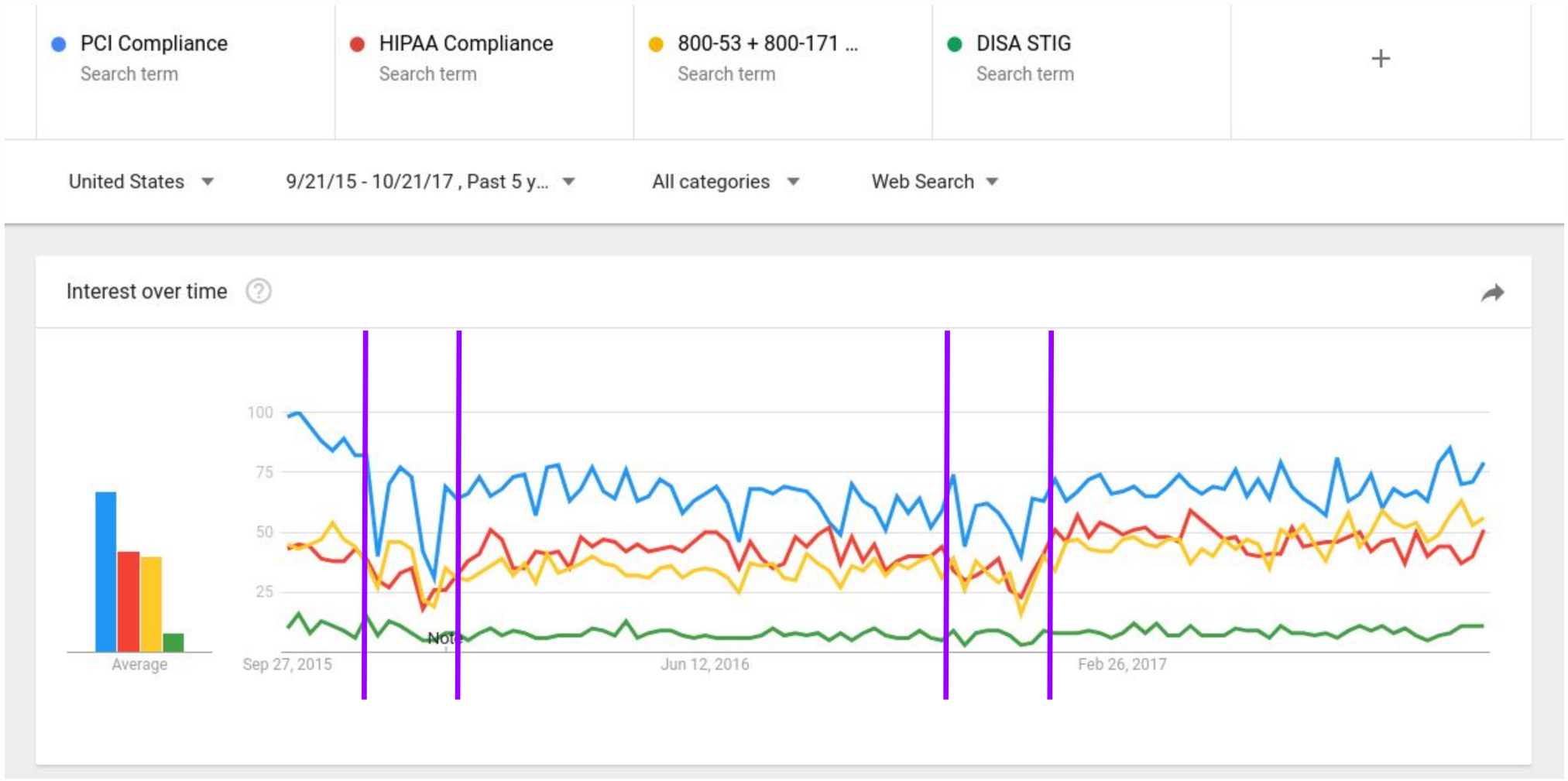
Relax



They're Just Requirements

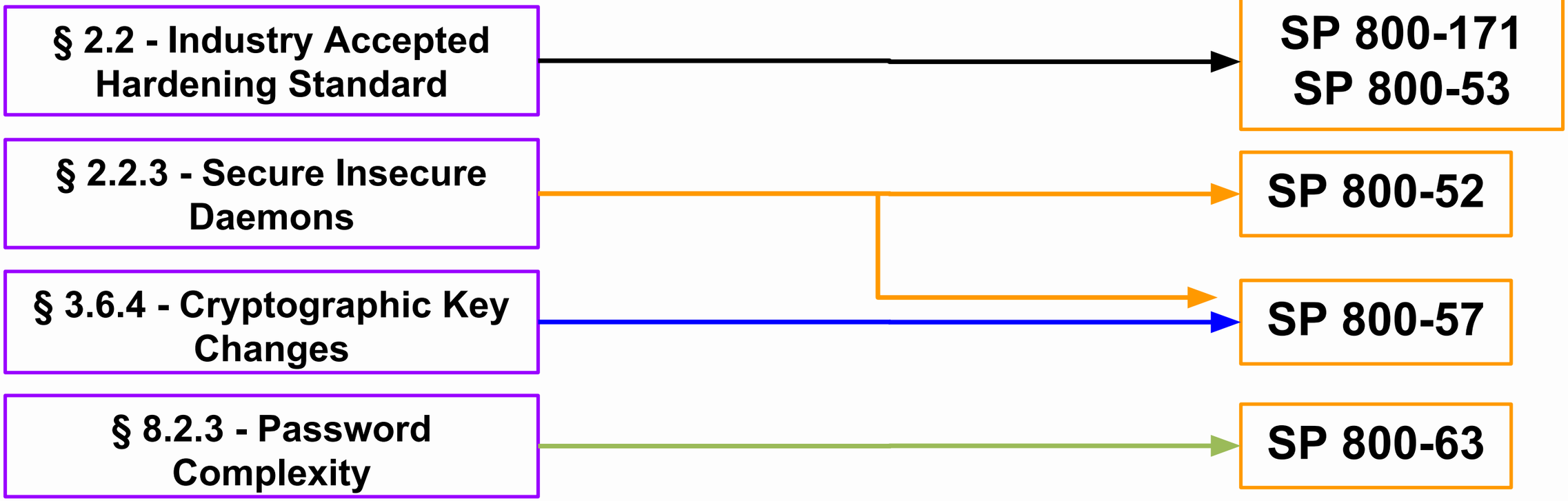
	PROVABLE	DISPROVABLE
SECURITY	X	✔
COMPLIANCE	✔	✔


Low
Medium
High
Low
Medium
Medium
Low
Low
Low
Probability
Impact

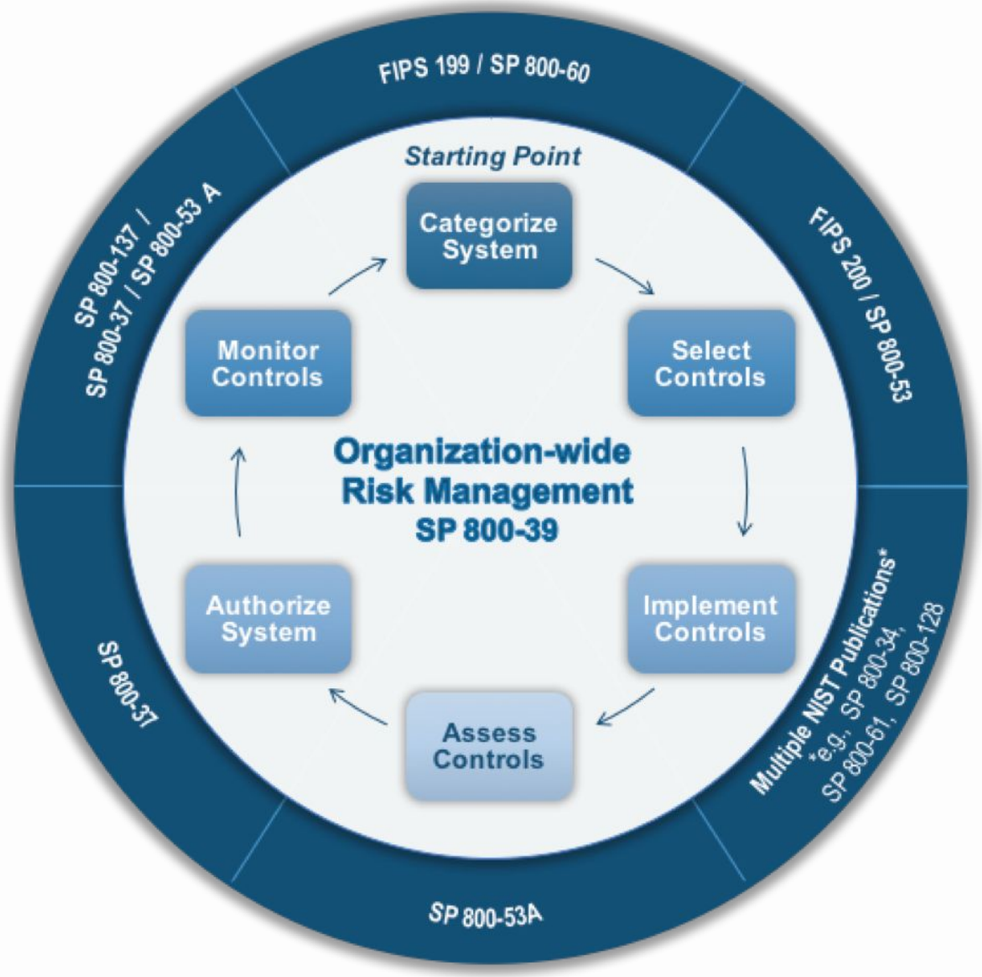

PCI Compliance
Search term
HIPAA Compliance
Search term
800-53 + 800-171 ...
Search term
DISA STIG
Search term
United States
9/21/15 - 10/21/17 , Past 5 y...
All categories
Web Search
Interest over time
100
75
50
25
Note
Average
Sep 27, 2015
Jun 12, 2016
Feb 26, 2017


PCI
Security
Standards Council


NIST
National Institute of
Standards and Technology

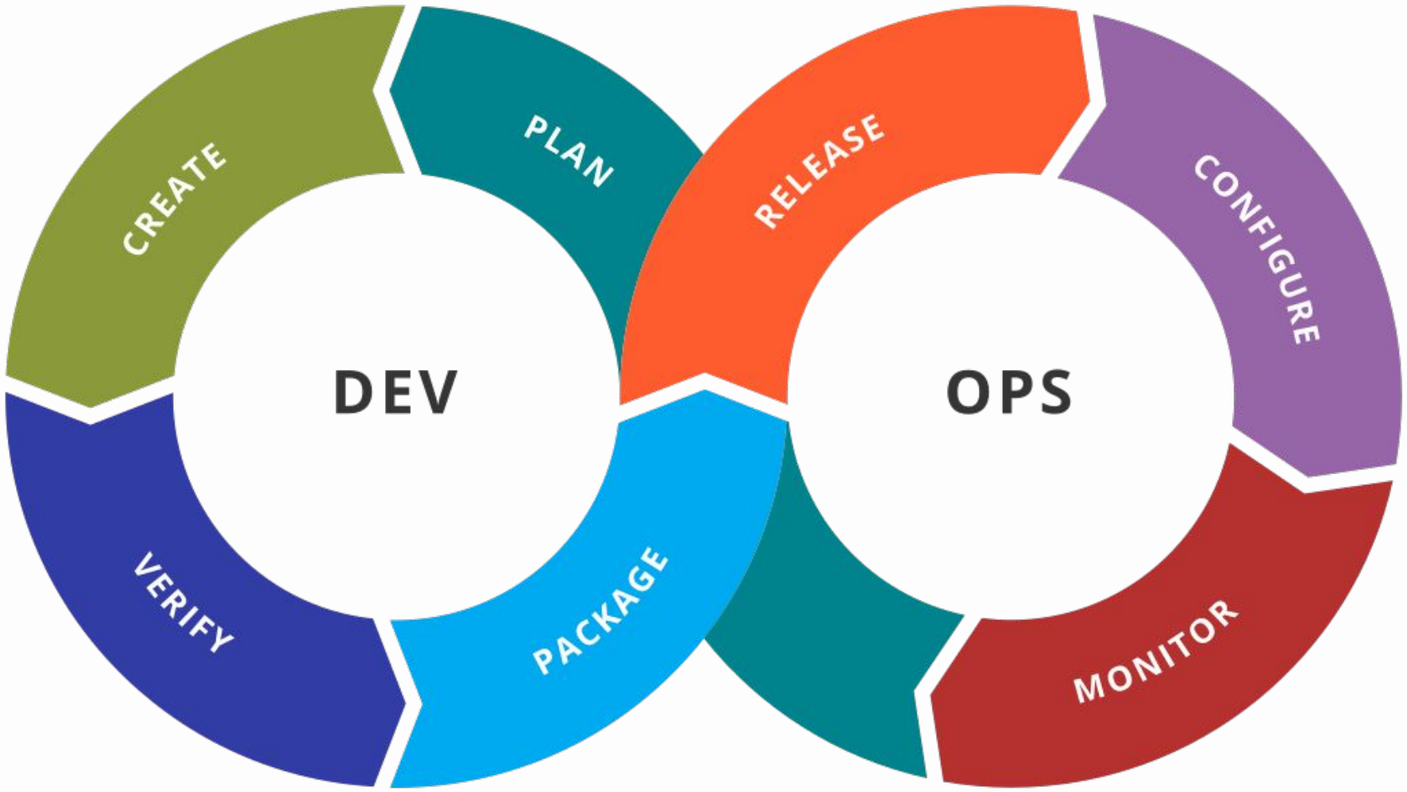

§ 2.2 - Industry Accepted Hardening Standard
§ 2.2.3 - Secure Insecure Daemons
§ 3.6.4 - Cryptographic Key Changes
§ 8.2.3 - Password Complexity
SP 800-171
SP 800-53
SP 800-52
SP 800-57
SP 800-63

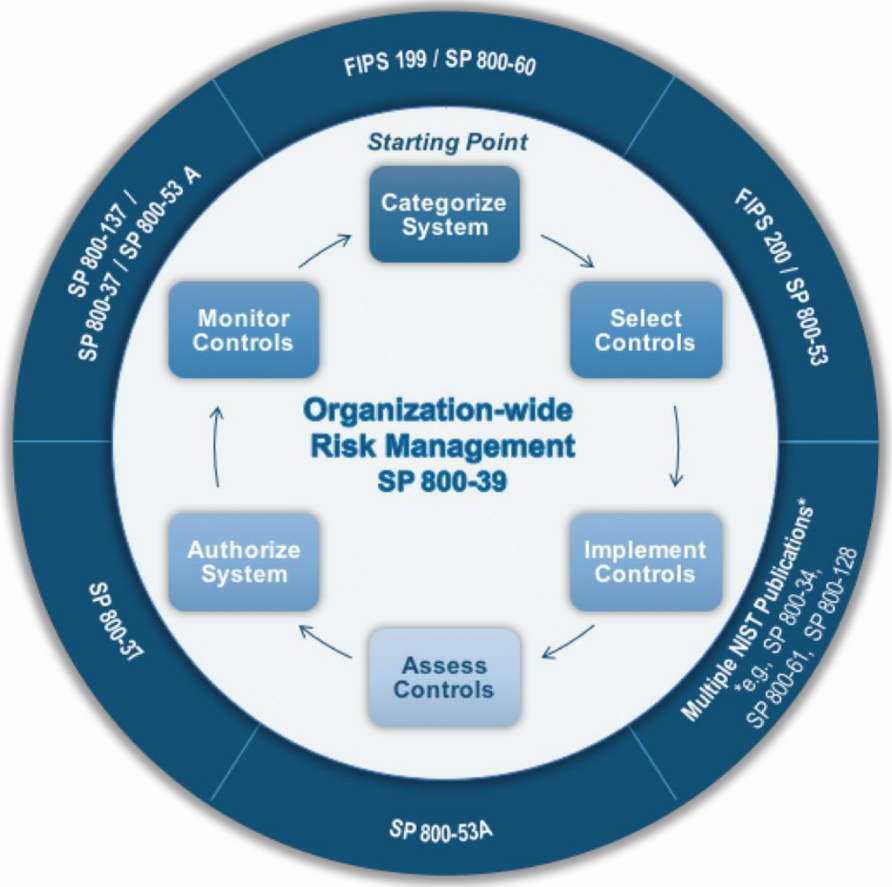
NIST
National Institute of Standards and Technology



Risk Management Framework


DevOps


CREATE
PLAN
RELEASE
CONFIGURE
DEV
OPS
VERIFY
PACKAGE
MONITOR


FIPS 199 / SP 800-60
Starting Point
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organization-wide Risk Management SP 800-39
SP 800-137 / SP 800-37 / SP 800-53 A
FIPS 200 / SP 800-53
Multiple NIST Publications* *e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-37
SP 800-53A

- **Development Team**
  - Must **Ensure Business Functions**



- **Operations Team**
  - First Line of Deployment
  - Last Line of Defense
    - Must **Respond to External Threats**
    - Must **Ensure Business Availability**



- **Security Team**
  - Must **Ensure Compliance**
  - Should **Ensure Security**



We are here to meet policies, not random scanners

- **SCAP Security Guide**
  - NIST 800-126 (SCAP)
  - https://open-scap.org
- **Inspec**
  - Ruby DSL
  - https://www.inspec.io





Title **Ensure gpgcheck Enabled In Main Yum Configuration**
Rule xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Ident

Result **pass**

Title **Record Events that Modify the System's Discretionary Access Controls - lchown**
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_lchown
Ident

Result **fail**



SCAP
SECURITY GUIDE

Trevor Vaughan, Onyx Point

Security Automation for Containers and VMs with OpenSCAP

Friday, Nov 3
2:00 - 3:30pm

Seacliff Room



OpenSCAP

Profile: Auditd demo checks for EL 7 (auditd_demo)
Version: 0.0.1
Target: local://

✔ audit at boot: Auditing should be enabled at system boot time
✔ Command cat /proc/cmdline stdout should match /(\S+\s+)audit=1/

Profile: InSpec Profile (disa_stig-el7)
Version: 0.1.0
Target: local://

× **V-72079:** Enable the audit daemon (expected that `Service auditd` is running)
× **Service auditd should be running**
expected that `Service auditd` is running

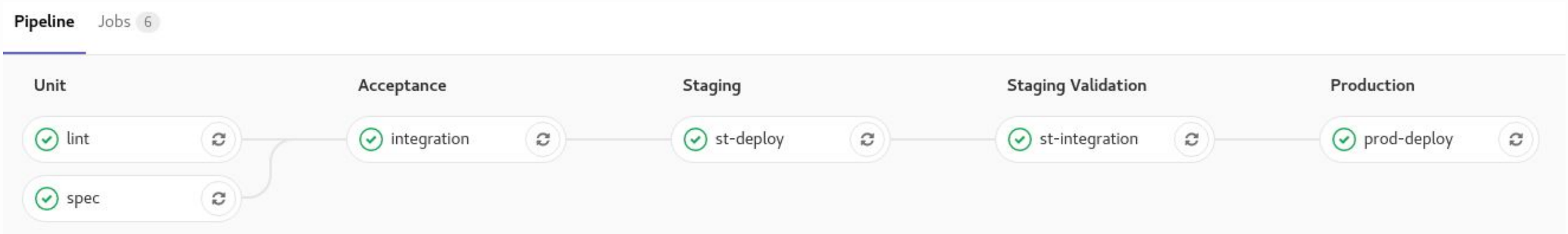
Profile Summary: 1 successful, 1 failures, 0 skipped
Test Summary: 1 successful, 1 failures, 0 skipped



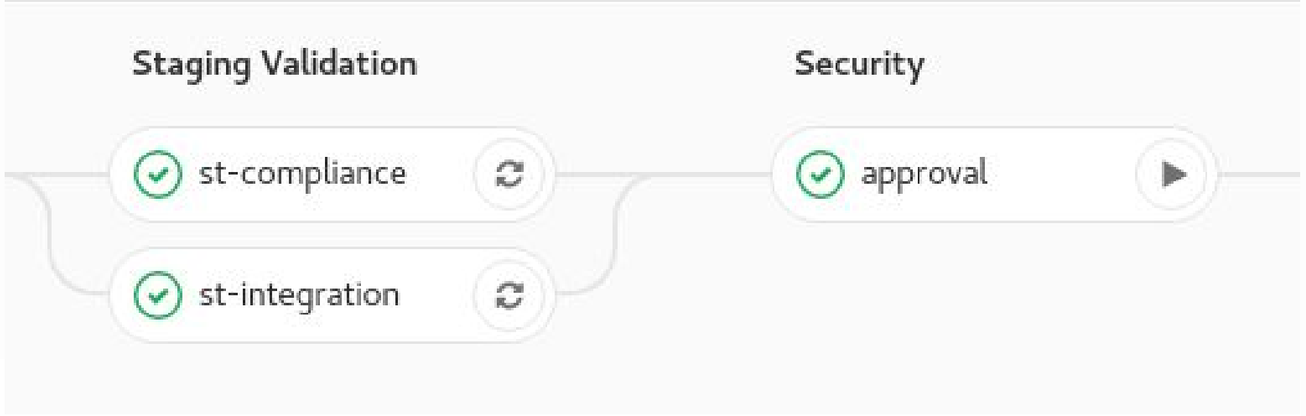
The Security Team must be part of the CI process

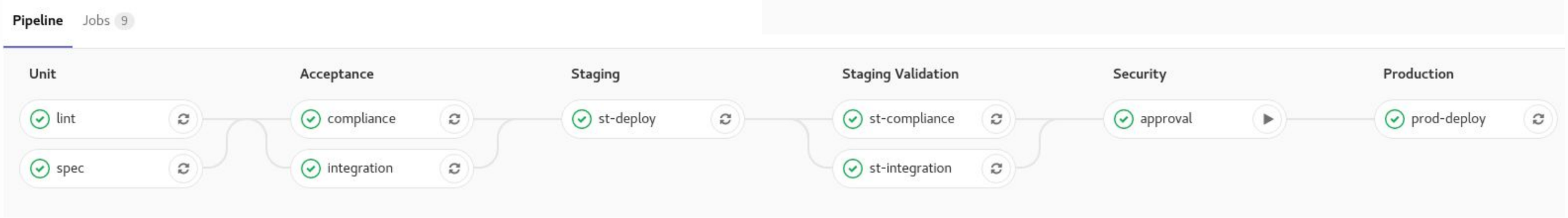


GitLab

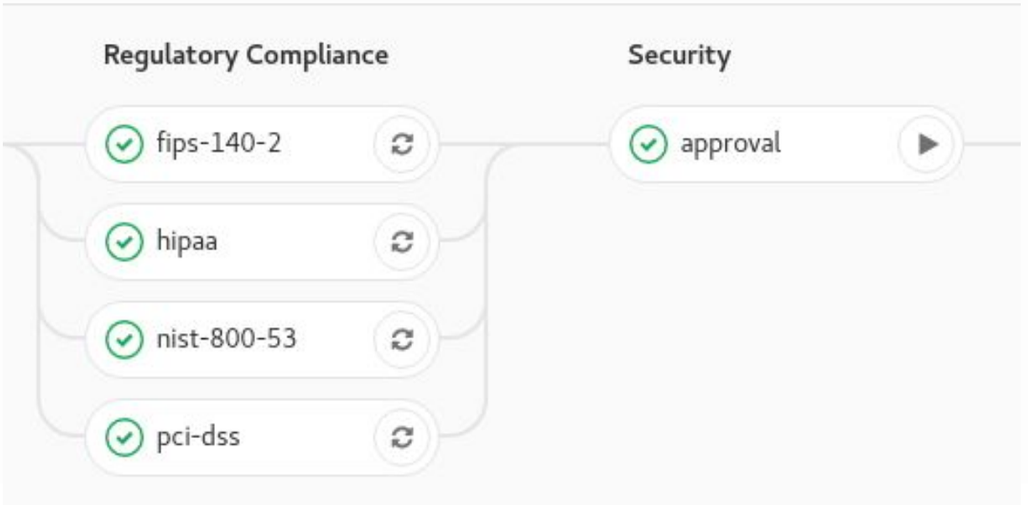

Pipeline
Jobs 6
Unit
lint
spec
Acceptance
integration
Staging
st-deploy
Staging Validation
st-integration
Production
prod-deploy

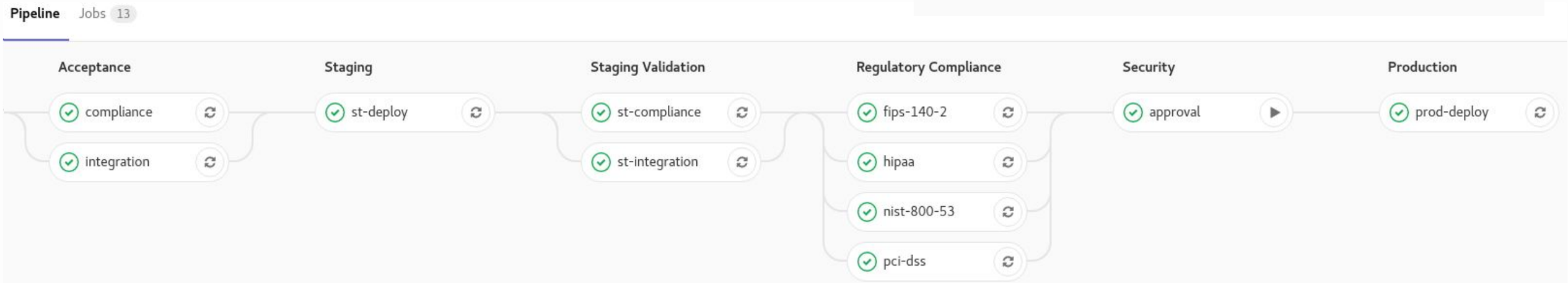
GitLab


Staging Validation
Security
st-compliance
st-integration
approval


Pipeline
Jobs 9
Unit
lint
spec
Acceptance
compliance
integration
Staging
st-deploy
Staging Validation
st-compliance
st-integration
Security
approval
Production
prod-deploy

GitLab


Regulatory Compliance
fips-140-2
hipaa
nist-800-53
pci-dss
Security
approval


Pipeline
Jobs 13
Acceptance
compliance
integration
Staging
st-deploy
Staging Validation
st-compliance
st-integration
Regulatory Compliance
fips-140-2
hipaa
nist-800-53
pci-dss
Security
approval
Production
prod-deploy

Security Teams are NOT outside of the policies and procedures


I AM ABOVE THE LAW!
memecrunch.com

Red Teaming is Good!



© Marvel Comics

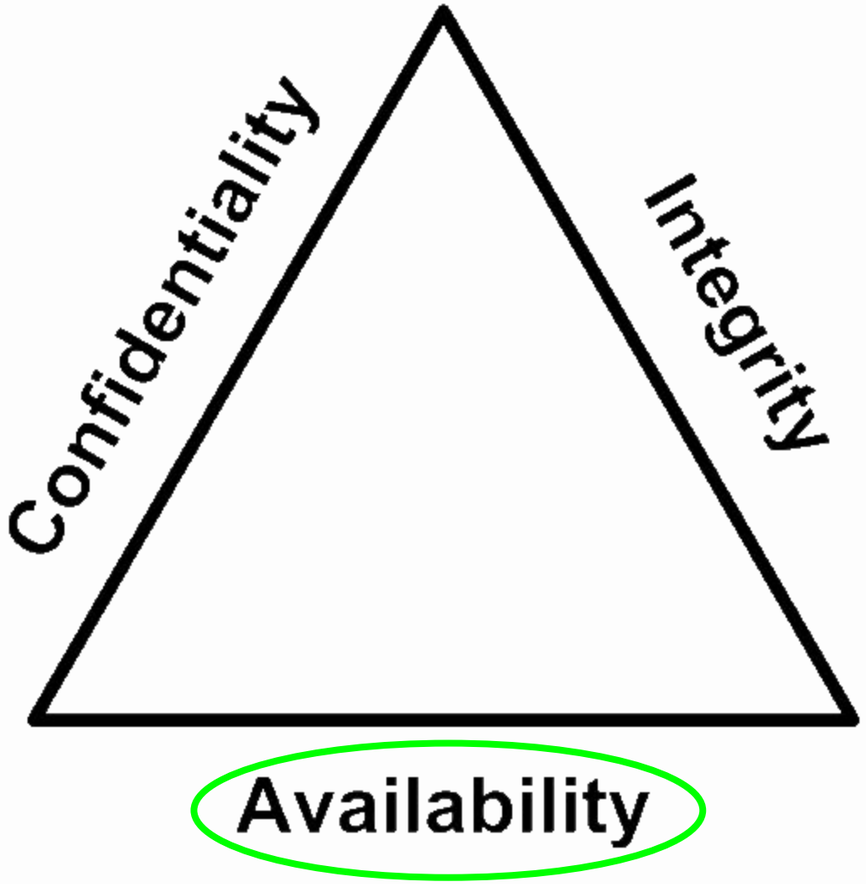
Weakening The System to run Security Tools is Bad



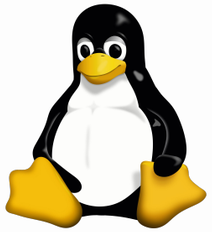
Security Teams must NOT install independent command and control utilities on your systems



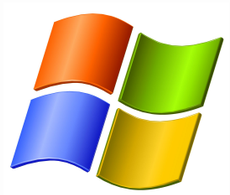
© DC Comics


Confidentiality
Integrity
Availability

Security Teams should NOT dump requirements stacks on other teams



vmware

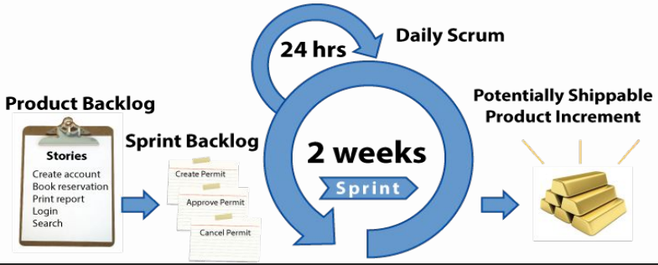


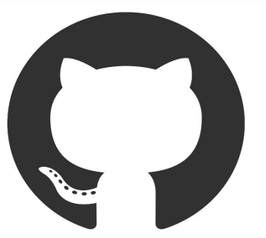


amazon web services™











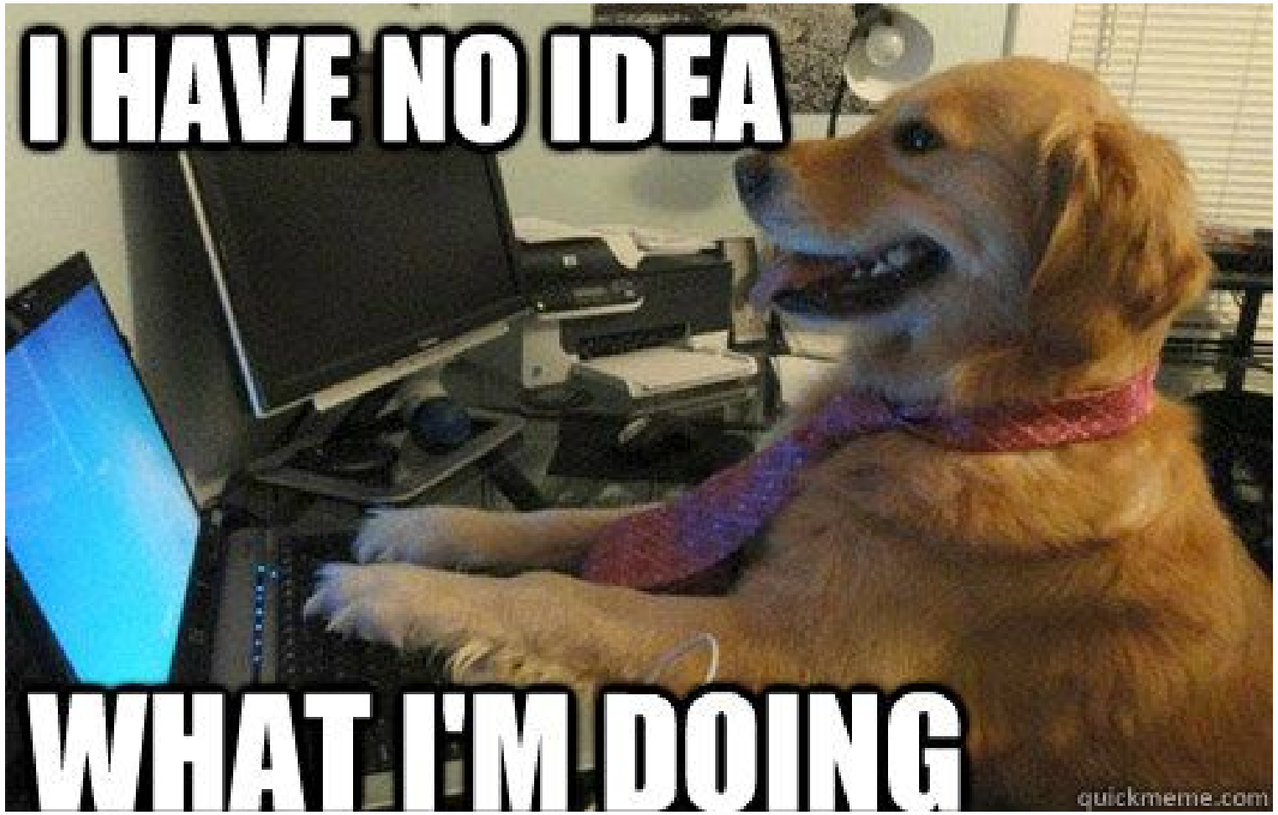
API

SEGA®

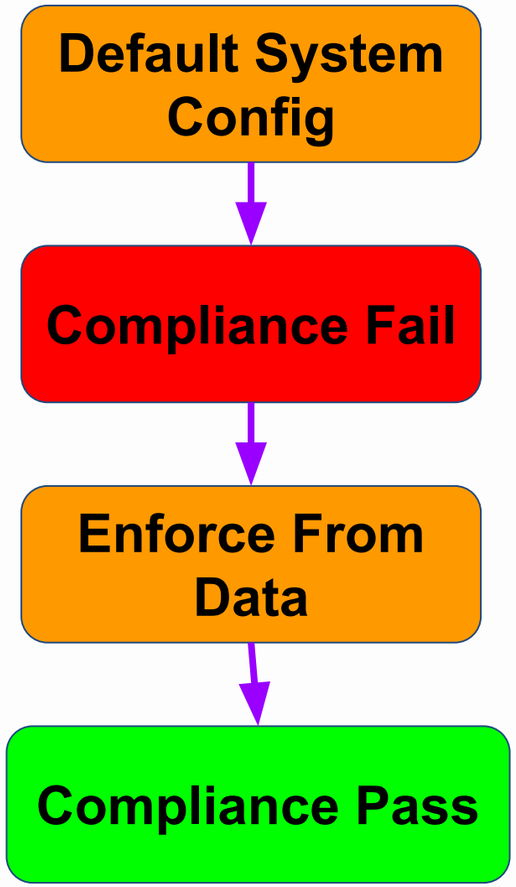


rpm

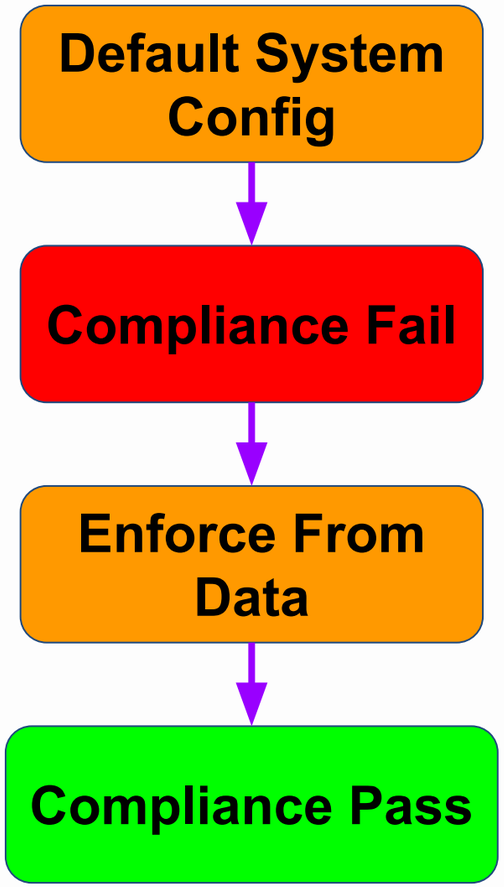
Ops and Dev need to play nice with Security


I HAVE NO IDEA
WHAT I'M DOING
quickmeme.com






```
[thanos@sys0 auditd_demo]$ rake beaker:suites[passing]
```




```
[thanos@sys0 auditd_demo]$ rake beaker:suites[passing]
```

Infrastructure as Code → Compliance as Code



Status	Pipeline	Commit	Stages		
passed	#8500 by latest	regulatory-ov… 2f6b0a46 all the regulations		00:01:45 34 minutes ago	
passed	#8499 by latest	security-manu… 8ebf349d shell runner for approval		00:01:14 37 minutes ago	
passed	#8496 by latest	simple-pipeli… 77a08608 simple pipeline		00:00:55 about an hour ago	
passed	#8492 by	security-manu… 9229aa4a shell runner for approval		00:00:42 41 minutes ago	
passed	#8491 by	security-manu… cce4aa73 shorten strings		00:01:16 about an hour ago	
passed	#8490 by latest	non-manual 95b88323 shorted strings		00:01:06 about an hour ago	

How do we operationalize security?

- Remember that policy == requirements
- Itegrate the security team into the full workflow
- Keep the workflow consistent
- Help, and watch, each other
- Remember availability

SEE ALSO

ABOUT ME

Trevor Vaughan
VP Engineering - Onyx Point, Inc.
tvaughan@onyxpoint.com
@peiriannydd

PROJECT WEBSITE

https://simp-project.com

CONSULTING + TRAINING

http://www.onyxpoint.com
Puppet(8), GitLab(8), Automation(7), DevOps(2), RedHat(8)