# How We Learned to SPL C-o-m-p-l-i-a-n-c-e

**Bob Clasen** (rclasen@mitre.org) | **Splunk Service Manager**

**Eugene Katz** (ekatz@mitre.org) | **Splunk Evangelist**

***The MITRE Corporation***

# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

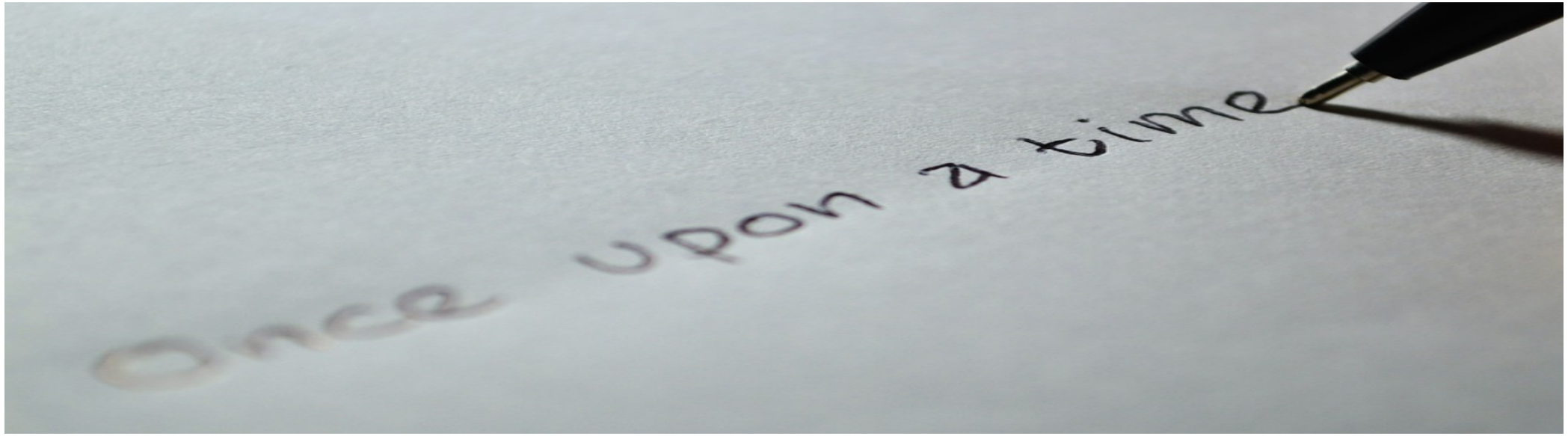
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.



splunk> .conf18

# Overview

- This is a story about how we:
  - Started leveraging Splunk to help us with compliance reporting
  - Are using it today for compliance
  - Are planning to use it in the future



# The MITRE Corporation


part of the ecosystem of federal research centers

established in **1958**
to serve the public interest

not-for-profit

science & tech support to federal government

**~8,000** employees

# Speaker Info

## Bob Clasen

- **Background**
  - Computer/electrical engineer
  - Retired US Air Force
  - At MITRE for 15 years
- **Current roles**
  - Team lead
    - Enterprise systems monitoring
    - Performance & automated testing
  - Splunk service manager
    - Been Splunking for 3+ years
- **Outside of work**
  - Baseball fan
  - Reading
  - Foreign movies

## Eugene Katz

- **Background**
  - Computer science
  - At MITRE for 19 years
    - 17 years software dev
    - Past 1.5 years: All Splunk
- **Current roles**
  - Bob's partner in ~~crime~~ Splunk service management
  - Splunk side of Compliance
  - Splunk Evangelist/User Advocate
- **Outside of work**
  - Tai Chi Chuan
  - Tabletop RPGs & Board Games

splunk> .conf18

# Background - Splunk at MITRE

MITRE

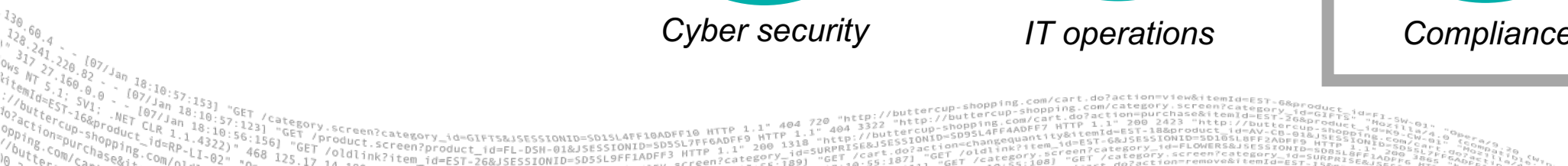
splunk>

- **Primarily used for internal IT**
  - Some isolated labs – classified, etc.
- **Some stats**
  - ~925 GB/day ingestion prod
  - ~300 user accounts (~80 roles)
- **Use cases**

*Cyber security*

*IT operations*

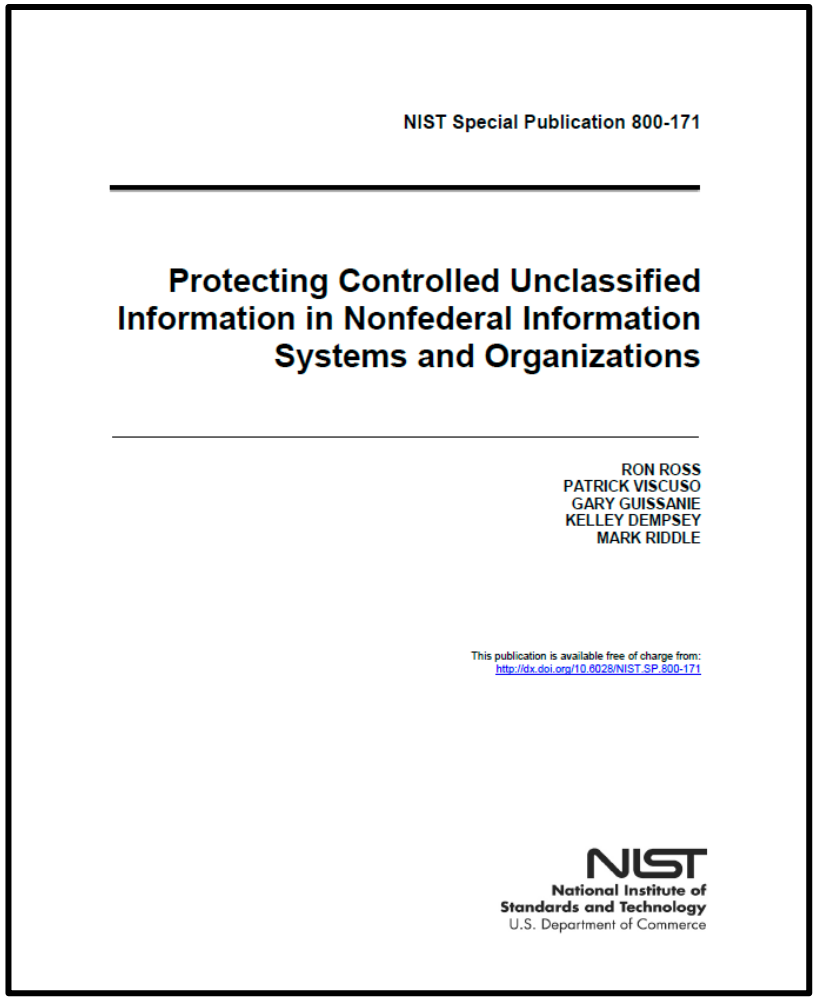
*Compliance*



splunk> .conf18

# The Story Begins…

- In late-2016, our IT staff started hearing about this new thing called **DFARS**
  - Defense Federal Acquisition Regulation Supplement
  - US Dept of Defense security requirements for federal contractors
  - Based on National Institute of Standards and Technology Special Publication (NIST SP) 800-171


NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

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

# Problem

- **New requirement for DFARS compliance**
  - Initial reaction: Yikes, what is DFARS?
  - Some of us didn't even know how to spell compliance
  - But, we did know how to SPL with Splunk
- **How could we leverage Splunk to help?**
  - Could our ninja skills save the day?

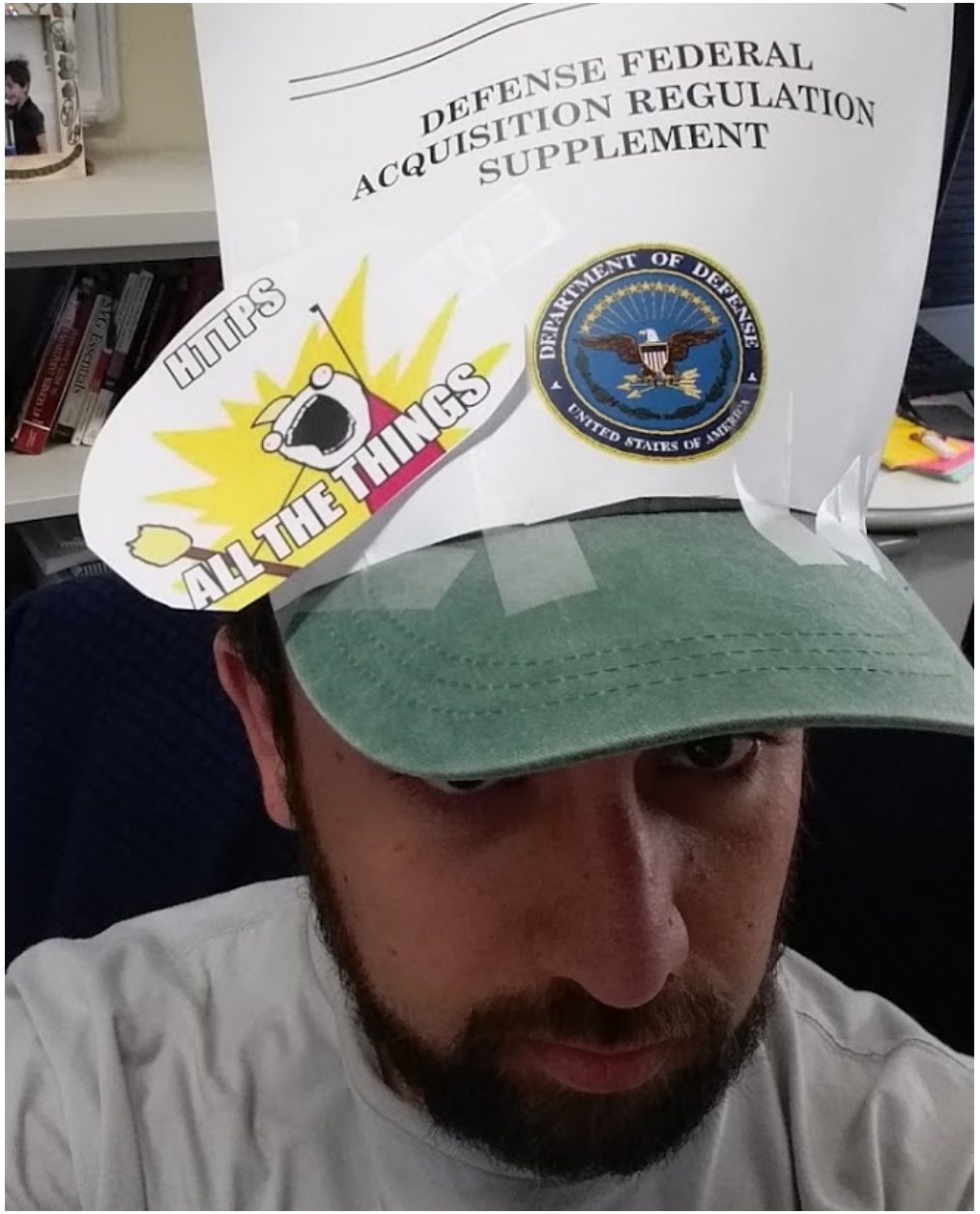
# Approach


- **Learn more**
  - Compliance, in general
  - Data already in Splunk that could be useful
  - Partnered with rest of our compliance team
  - Splunk DFARS data assessment
  - At this point, we knew Splunk could help
- **Assessed options**
  - Build a compliance app ourselves
    - With some help from professional services
  - Buy a commercial tool

# Approach (cont.)

- **Why build instead of buy?**
  - Cost trade-offs
  - We already knew Splunk
    - It was just compliance that was new
- **Getting started**
  - Services engagement to jump start
  - Hired dedicated person for this effort
  - Identified candidate controls for Splunk reporting
    - Use Splunk for ~35% of DFARS controls

# Scariest Halloween Costume



# Implementing Compliance: Expectation vs. Reality

## What we thought we were getting into


By Barry Lewis - Mobile Home, CC BY 2.0,
https://commons.wikimedia.org/w/index.php?curid=27497919

## What we were *actually* getting into

U.S. Air Force photo by Master Sgt. Greg Steele/Released)
http://www.307bw.afrc.af.mil/News/Art/igphoto/2001567611/

# Three-Pronged Approach

**What is this NIST 800-171?**

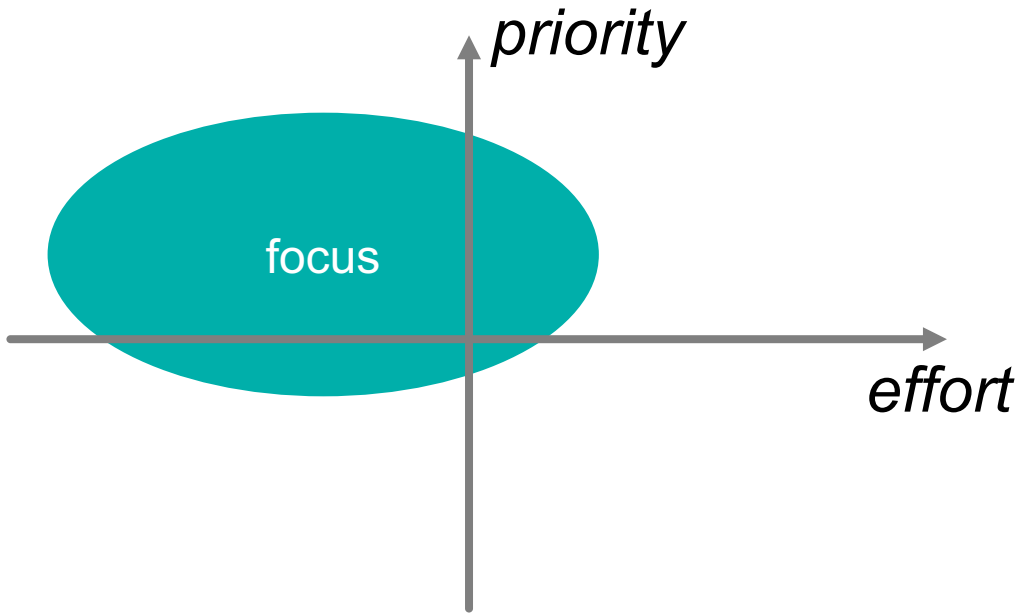
1. Review compliance controls
2. Scope what we have in our environment
3. Test queries/dashboards

By Illustrator unknown [Public domain], via Wikimedia Commons
https://commons.wikimedia.org/wiki/File:Blind_men_and_elephant.jpg

splunk> .conf18

# 1 Review Compliance Controls

**What do we need to actually *do*?**

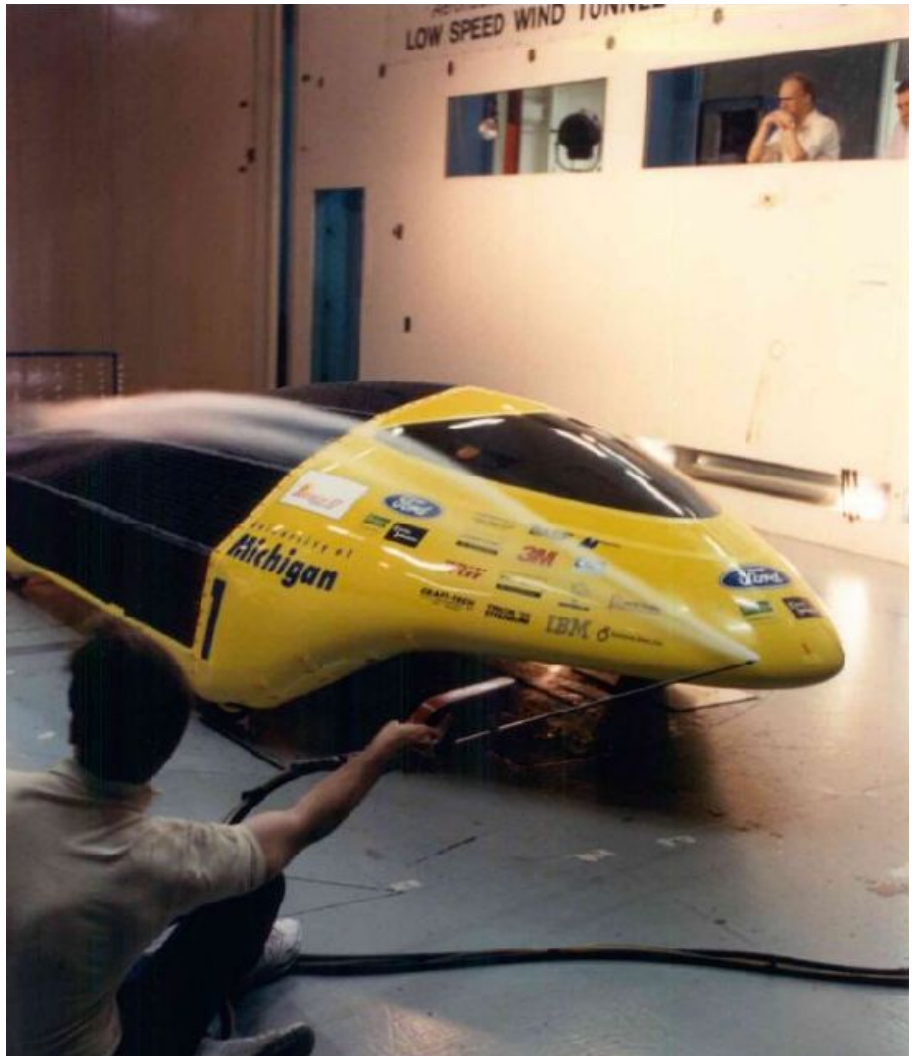



**For vendor engagement, focus on big wins.**

# 2 Scope What We Have in Our Environment


By Snyder, Frank R.Flickr: Miami U. Libraries - Digital Collections [No restrictions or Public domain], via Wikimedia Commons
https://commons.wikimedia.org/wiki/File:Two_women_in_surveying_class_1921_(3190608803).jpg

# 3 Test Queries/Dashboards in DEV and PROD

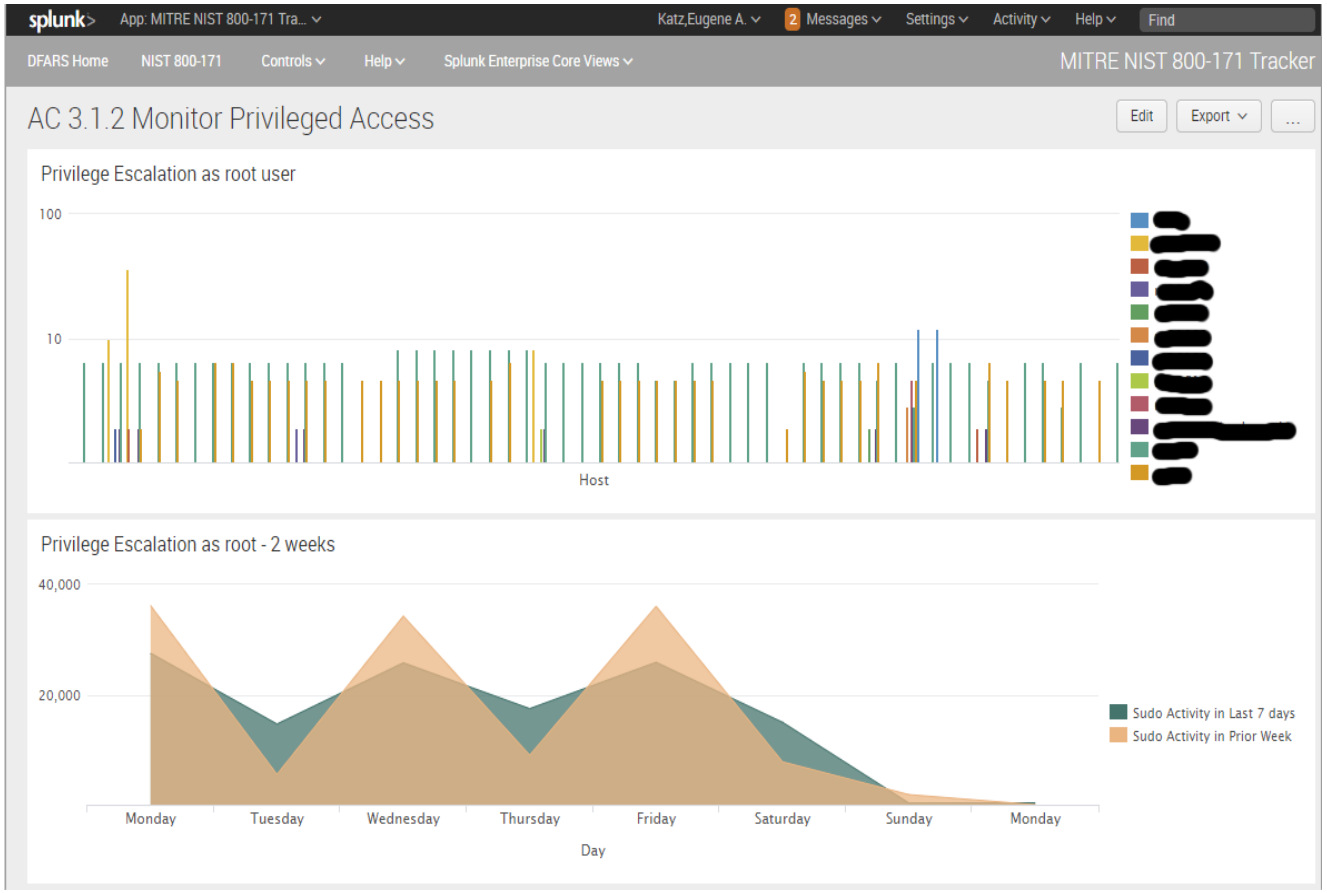


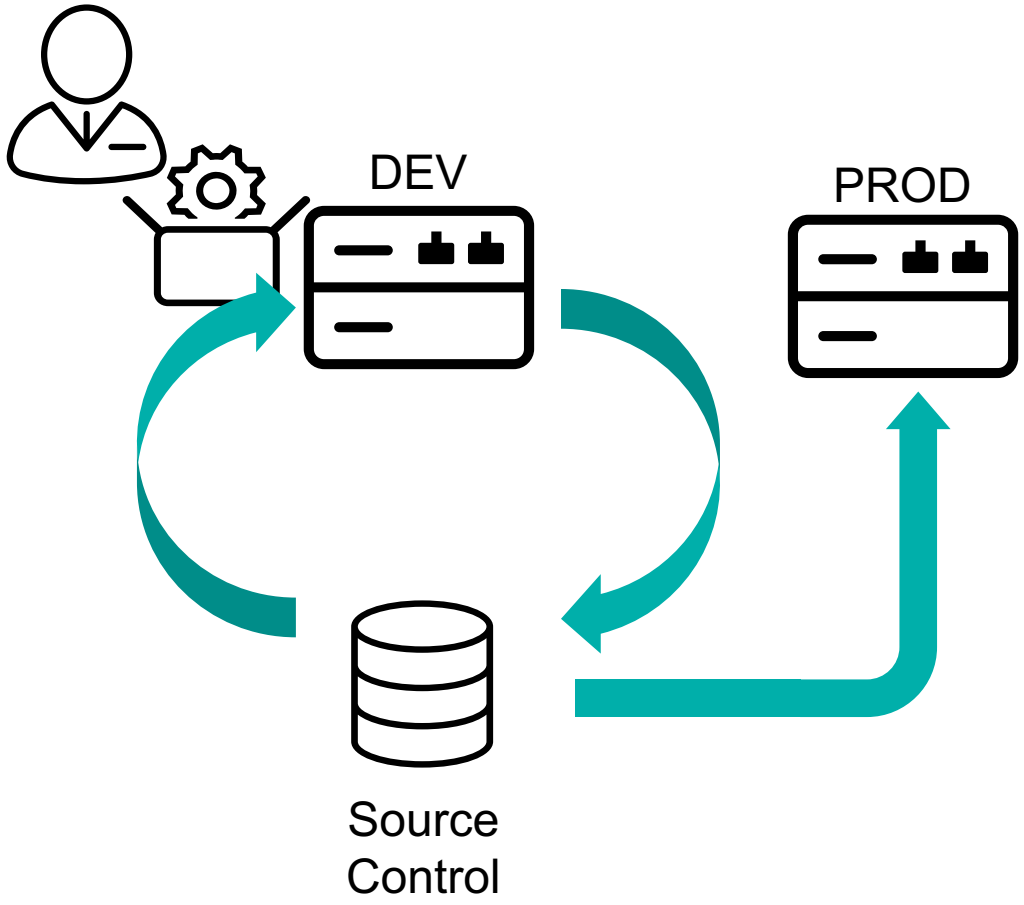

Fnazeeri at English Wikipedia [CC BY-SA 2.5 (https://creativecommons.org/licenses/by-sa/2.5)], via Wikimedia Commons
https://commons.wikimedia.org/wiki/File:Windtunnel_testing.jpg

# Finding and Tracking Issues

| Control # | Family | Derived Security Requirement | Dashboard | Chart Label | Chart Values | DEV status & notes | PROD status & notes | Demo link | Blockers | Next Steps |
|---|---|---|---|---|---|---|---|---|---|---|
| 3.1.2 | Access Control | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | AC 3.1.2 Monitor Privileged Access | in progress | 1 | Windows: NEEDS WORK<br>Linux: READY<br>index=linux-syslog<br>why are there two 3.1.2? | Windows: NEEDS WORK<br>Linux: READY<br>index=linux-syslog | Linux:PROD | Windows Infrastructure App configs | ☐ review for expected functionality @Eugene Katz<br>Linux: review with SME |
| 3.1.4 | Access Control | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | AC 3.1.4 Review Membership of Privileged Groups - Win | in progress | 1 | NEEDS WORK | Windows: REVIEW | PROD | | Waiting to add DEV/ INT<br>[redacted]D/I |
| 3.1.5 | Access Control | Employ the principle of least privilege, including for specific security functions and privileged accounts. | AC 3.1.5 Account Creation and Deletion - Win | in progress | 0.5 | | NEEDS WORK<br>"No matching visualization found for type: horseshoe_meter, in app: horseshoe_meter_app" | | | Replace with a different vis or install horseshoe_meter |
| | | | AC 3.1.5 Account Creation and Deletion - Linux | in progress | 0.5 | | NEEDS WORK<br>index changed to linux-syslog<br>"No matching visualization found for type: horseshoe_meter, in app: horseshoe_meter_app" | | | same as above |
| 3.1.8 | Access Control | Limit unsuccessful logon attempts. | AC 3.1.8 Unsuccessful Logon Attempts - AWS | ready | 0.5 | | READY index=[redacted] | PROD | | |
| | | | AC 3.1.8 Unsuccessful Login Attempts - OS | ready | 0.5 | | Windows: READY<br>Linux: READY | PROD | | change url of dashboard from _linux |
| 3.1.12 | Access Control | Monitor and control remote access sessions. | AC 3.1.12 Login Activity | in progress | 1 | Data not in DEV (was initially, but cycled out) | NEEDS WORK<br>index=vpn sourcetype=cisco_asa on has only blocked events | | | PROD: Look at different ways to see "allow"<br>eventtype<br>Probably need to update to newer Cisco_ASA Ad-on - (Mon 10/23/2017 2:32 PM email) |
| | | | AC 3.1.12 VPN RA: Total Sessions, Total Unique Users, and | ready | 1 | Data not in DEV (was initially, but | READY | PROD | | |

# Finally, an App to Install!




splunk> .conf18

# Other Considerations/Challenges Along the Way

- Which (out of thousands of) our system have CUI?
  - Subnets help, but only so much
- Campus Compliance App came out on Splunkbase
  - Uses Common Information Model (CIM)
- Can we send the reports by email?
  - Are they too sensitive?
  - Do we need to track if they've been reviewed?
- Do users of dashboards need to have access to all the underlying data?
  - Depends

> Your [data] scientists were so preoccupied with whether or not they could, that they didn't stop to think if they should.

*Jurassic Park*

# What Does That Mean for Me?

## Forewarned is forearmed

https://commons.wikimedia.org/wiki/File:Philippines_road_sign_W5-2.svg

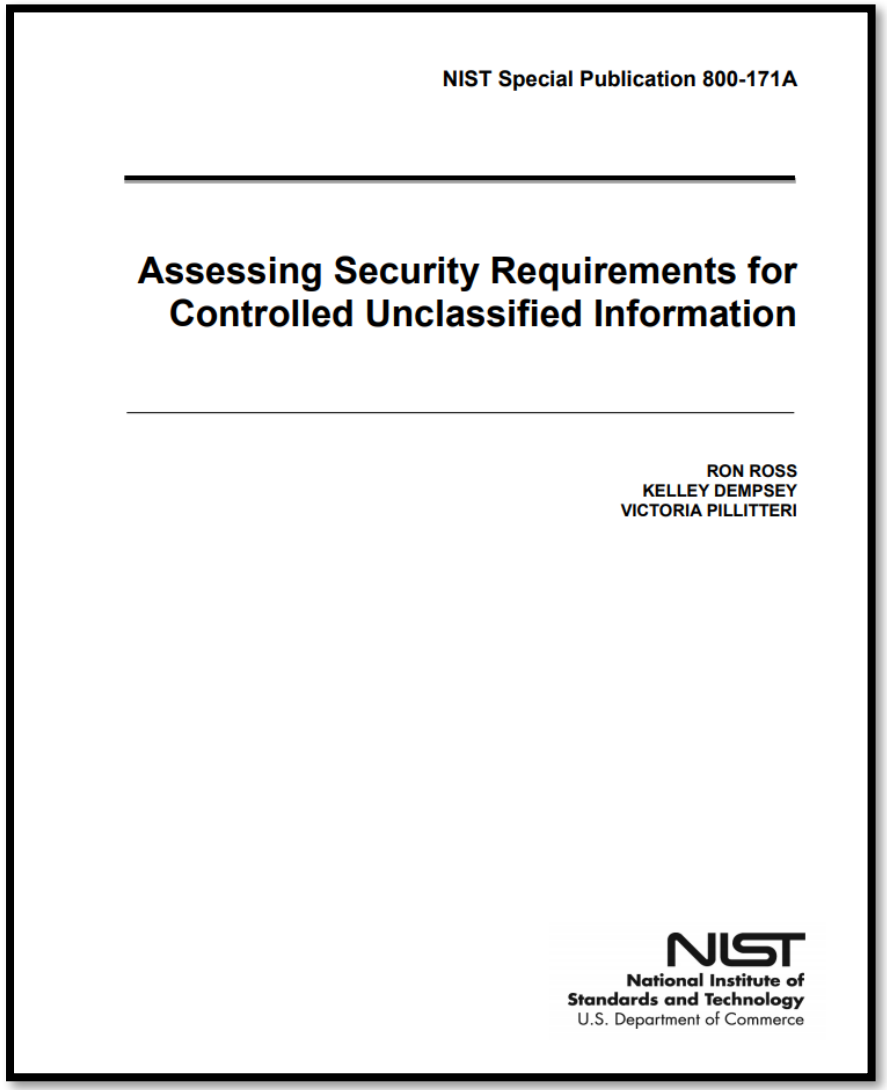
# Don’t Expect a Drop-in Solution

By Barry Lewis - Mobile Home, CC BY 2.0,
https://commons.wikimedia.org/w/index.php?curid=27497919

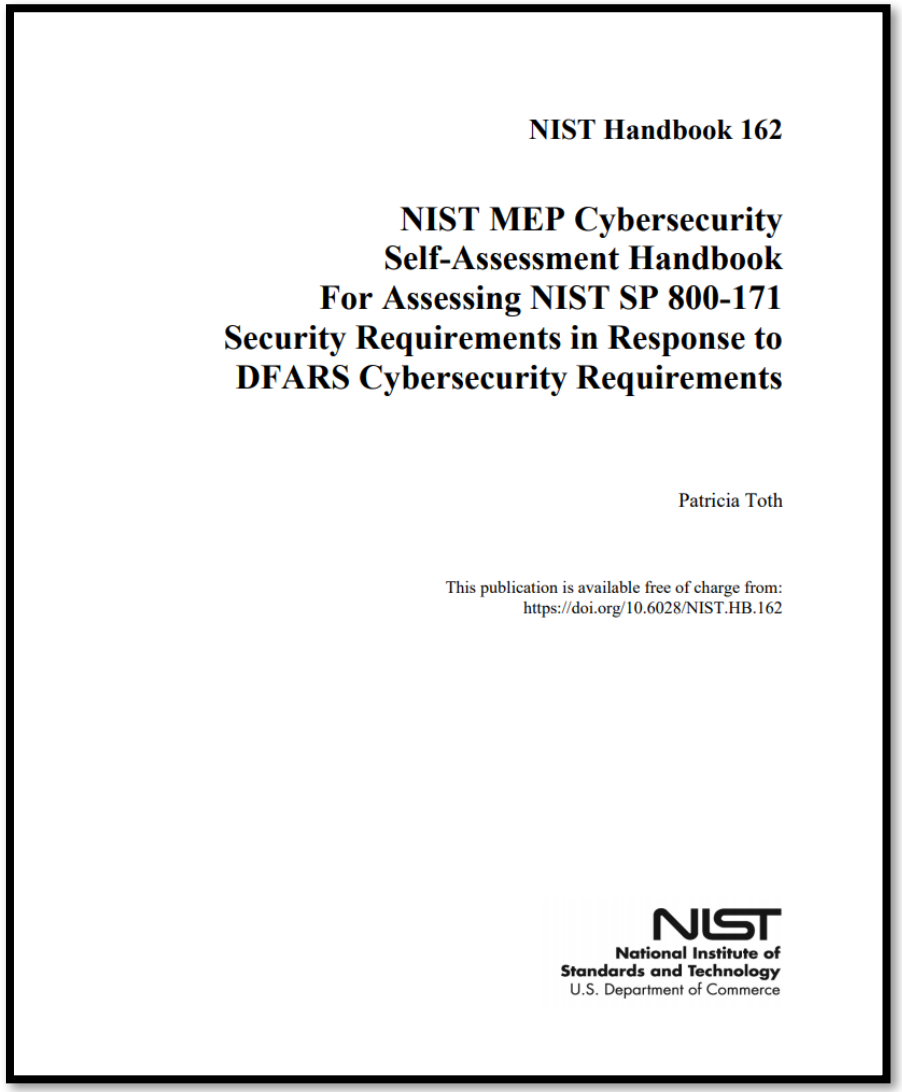
U.S. Air Force photo by Master Sgt. Greg Steele/Released)
http://www.307bw.afrc.af.mil/News/Art/igphoto/2001567611/

- Plan accordingly
- Getting all the right data and add-ons might take some work, even if it looks like you’re ingesting all the right stuff at first glance

# There Is More Guidance out There Now




https://csrc.nist.gov/publications/detail/sp/800-171a/final




https://doi.org/10.6028/NIST.HB.162

splunk> .conf18

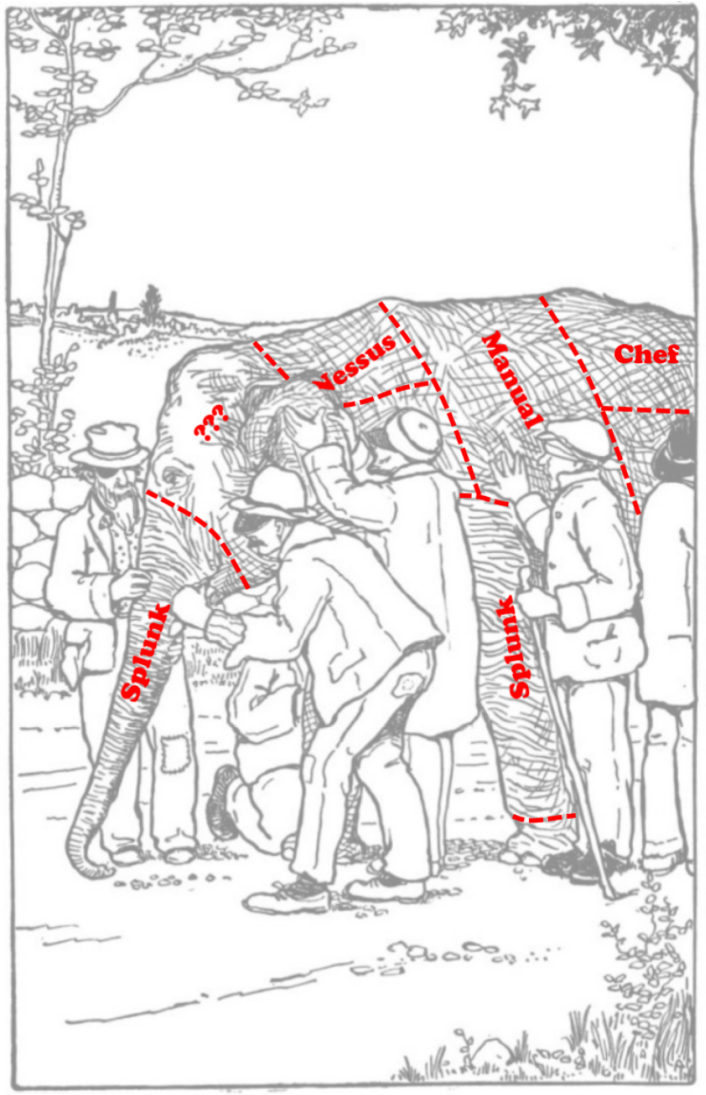
# There Is More Guidance out There Now (cont.)

https://doi.org/10.6028/NIST.HB.162

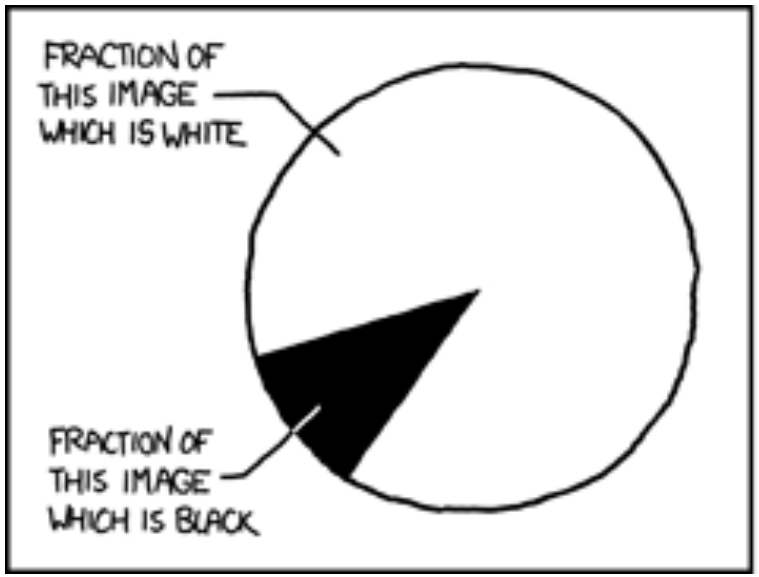
https://csrc.nist.gov/publications/detail/sp/800-171a/final

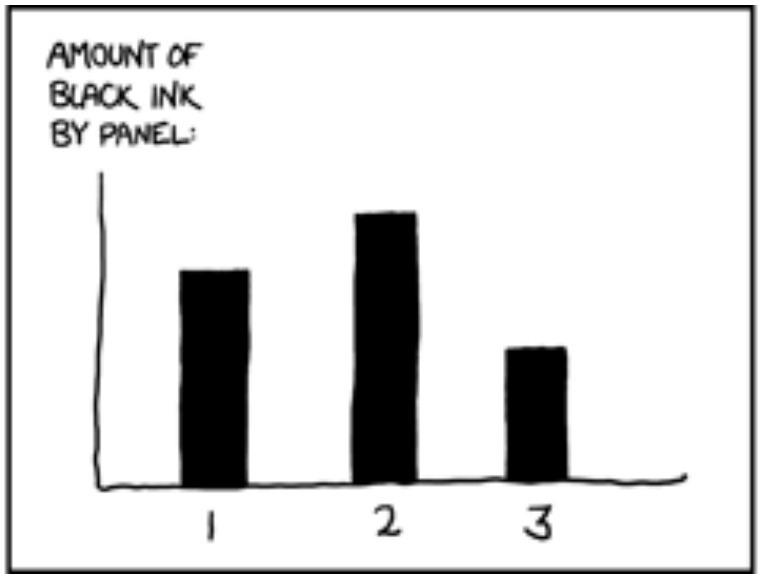
# Think it All the Way Through

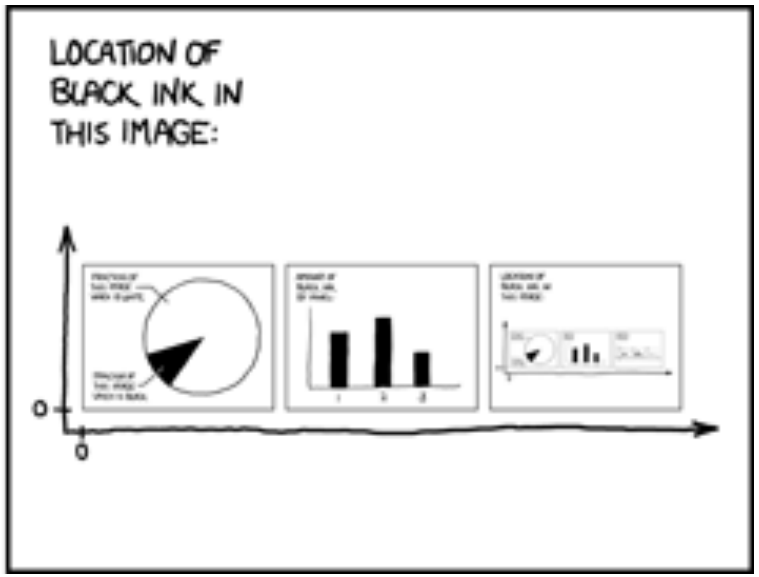
- What do you actually need to produce for the auditors? – Play pretend
- What are the correct tools for each control?
- Seeing everything in Splunk is nice, but doesn't have to be Phase 1



# Don’t Be Fooled by Pretty Dashboards



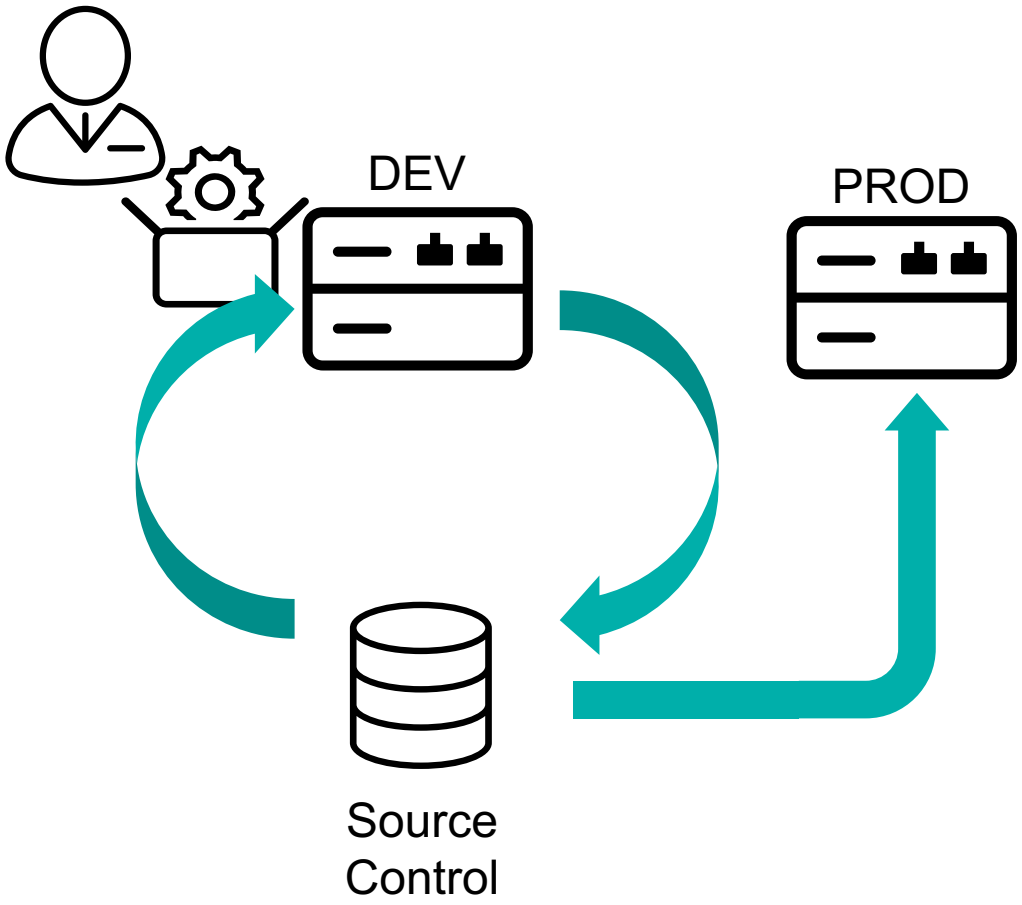






- How will each report/dashboard *really* get used?
  - How does a timechart of failed logins help you meet a control?
- It might be interesting, but is it useful for compliance?

# All the Best Practices Still Apply

## Think: maintenance



# Next Steps for Us

- Continue reexamining controls and using Splunk where appropriate
- Extend compliance services
  - To other teams (not just internal IT)
  - For other types of compliance (Risk Management Framework, classified labs, etc.)

# Thank You

**Don't forget to rate this session in the .conf18 mobile app**