A Whole New Containerized World

Building Security into Containerized Applications

ChefConf | September 27, 2023

MITRE Aaron Lippold
Will Dower
Amndeep Singh Mann
Sophos Mike Fraser

SOPHOS MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Our Team

Aaron Lippold
Principal Cybersecurity Engineer
Chief Engineer of the MITRE SAF
MITRE

Mike Fraser
VP & Field CTO of DevSecOps
Sophos

Will Dower
Lead Cybersecurity Engineer
MITRE SAF
MITRE

Amndeep Singh Mann
Software Engineer
MITRE SAF
MITRE

SOPHOS

Fac

MITRE

MITRE A Company Unlike Any Other

https://www.mitre.org/who-we-are

- MITRE was established to advance national security in new ways and serve the public interest as an independent adviser. We continue to deliver on that promise every day, applying our systems-thinking approach to provide solutions that enhance our national security and way of life.
- Our mission-driven people come to work at MITRE to make a difference. We give them that opportunity by fostering a vibrant and diverse community of thought that drives a culture of innovation. Our not-for-profit status sets us apart. Motivated by impact, our people discover new possibilities, create unexpected opportunities, and lead as pioneers for the public good.
- Fast Company called us "the most important company you've never heard of." But even if you don't know our name, you have experienced our impact. In our 60+ years of catalyzing and sustaining change, we never lose sight of the human factor behind every complex system and innovative solution.

MITRE | SAF

- The **MITRE Security Automation Framework (MITRE SAF)©** brings together applications, techniques, libraries, and tools developed by MITRE and the security community to streamline security automation for systems and DevOps pipelines.
- The MITRE SAF team participated in the development of the InSpec Language with Progress Chef, and many others in the security community.
- We want to be on the **cutting edge** of security automation while avoiding reinventing the wheel**.**

Sophos

https://home.sophos.com/en-us/about-us

- Sophos delivers superior cybersecurity outcomes by providing cybersecurity as a service to protect companies of all sizes from the most advanced cyberthreats. Our cybersecurity products and services include managed detection and response (MDR), firewall, email, endpoint, and cloud protection.

- The Sophos Factory team came in from the Refactr acquisition in 2021 and is helping drive adoption of DevSecOps through the Sophos Factory DevSecOps automation platform.

The Landscape is Changing Quickly

Industry is increasingly deploying software capabilities using fleets of containers.

This means better, more efficient, and scalable applications . . .

But it also changes the threat landscape!

MITRE

How to Change with the Tides & Not Get Swept Away

- What security considerations do I need to take in response to the new containerized world?
  - Conversely, what hasn't changed? What existing processes can we still use?
- What security tools do I use? How can I best use them?
- How can I streamline and manage my security processes?
- What gaps do we still need to fill?

MITRE

MITRE | SAF © Industry Collaborations

- MITRE SAF© works frequently with **Progress Chef**, because we use InSpec and Test Kitchen constantly!
- We leverage **Sophos Factory** for building container management pipelines.
- MITRE and Sophos co-lead the technical committee for the **OASIS Heimdall Data Format (OHDF)**, a standard format for exchanging normalized security data between cybersecurity tools.
- MITRE SAF© also works alongside companies including VMWare and Lockheed Martin to develop new tools and features.

Containers – A Maturing Industry Pillar

- Wide adoption in industry, and increasingly government
- Container orchestrators – e.g., Kubernetes deployments – increasing in scale
- Whole ecosystem of container scanning tools – Trivy, OWASP ZAP, Grype, and of course InSpec!
- Capabilities for generating mountains of data on CCEs & CVEs in containers

New technology, new tools for managing it, hooray!

MITRE

Security Considerations for Containers

- The basics still apply
- Just generating a mountain of data != security
- Containers are ultimately just wrappers for services
- Most of the work of securing a container is in securing its service, host and environment

There's no point in locking your door if your wall has a hole in it!

MITRE

But I’m generating an SBOM now!

Cool. What are you going to do with it?

No amount of security data will get you out of needing to make security decisions!

. . . we would know, we’ve tried

MITRE

What Now?

- What needs to evolve from our legacy security validation processes?
- What are the best security practices for deploying containerized software?

Containerization

Headaches for security engineers and assessors

MITRE

Challenges – Baseline Guidance!

- **How do I know what a secure benchmark is for a container in the first place?**
- Development teams required to align to baseline security guidance from industry or government
- What do I do if the guidance was written before containerization was around?
- What do I do if the guidance does not tell me what to do when I am deploying my system component as a container?

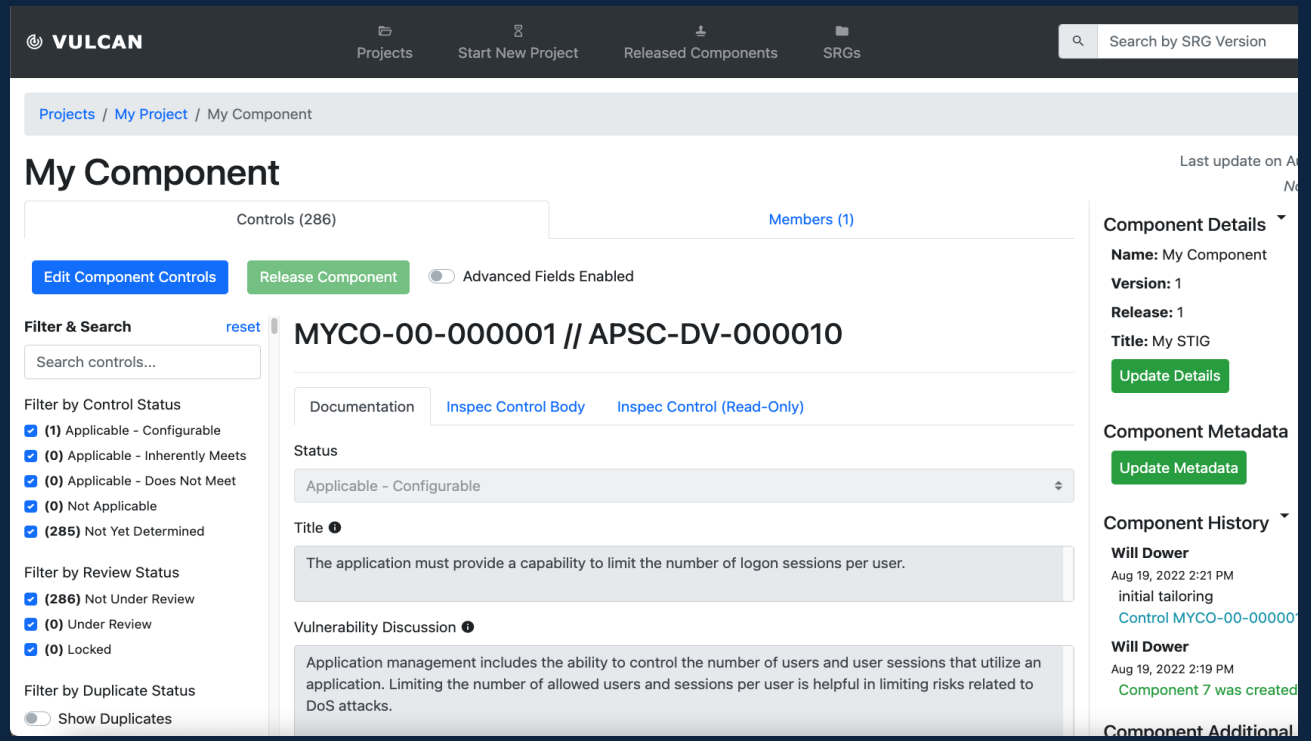
Teams need to be able to write container-aware, cloud-ready security baseline guidance!

MITRE

MITRE | SAF© Vulcan

https://vulcan.mitre.org

- Vulcan is a webapp that enables multiple authors to collaborate on security guidance authorship
  - Role-Based Access Control (RBAC)
  - Change Management
  - Reviewer System
  - Version Control
- Cut your guidance writing time from 18-24 months to 3-6 months!
- Enables the creation of **container-aware** security guidance
- Allows for easy implementation of container-aware InSpec test code



In short, the best way to develop automated security content for containers is to **start from the beginning!**

MITRE

InSpec Your Gadgets – Container Edition

- MITRE | SAF © and then Progress Chef InSpec teams have made it possible to author **container-aware** profiles

```
if virtualization.system.eql?('docker’)
   impact 0.0
   describe "Control not applicable within a container" do
      skip "Control not applicable within a container"
   end
else
   describe ”A control that is only relevant on a full host" do
   subject { the_thing }
      it { should be_secure }
   end
end
```

Challenge – Pipelines & Headaches

- Release process for containerized software means we need quality CI/CD pipelines for new releases
- Many organizations require containers to be sourced from their own, bespoke container registries, which gatekeep entry to their ecosystem behind security pipelines
- In short – releasing containerized software means more **and more complex** pipelines!

Migraine Relief

Apply the SAF CLI Action directly to your GitHub pipelines!

Pipeline Example – Air Force Iron Bank

- Air Force registry for containerized software with stringent security requirements for entry
- US Department of Defense organizations and supporting contractors use it to ensure that the containers they use are compliant
- The MITRE SAF© team wants to make sure our software is available inside this secure registry

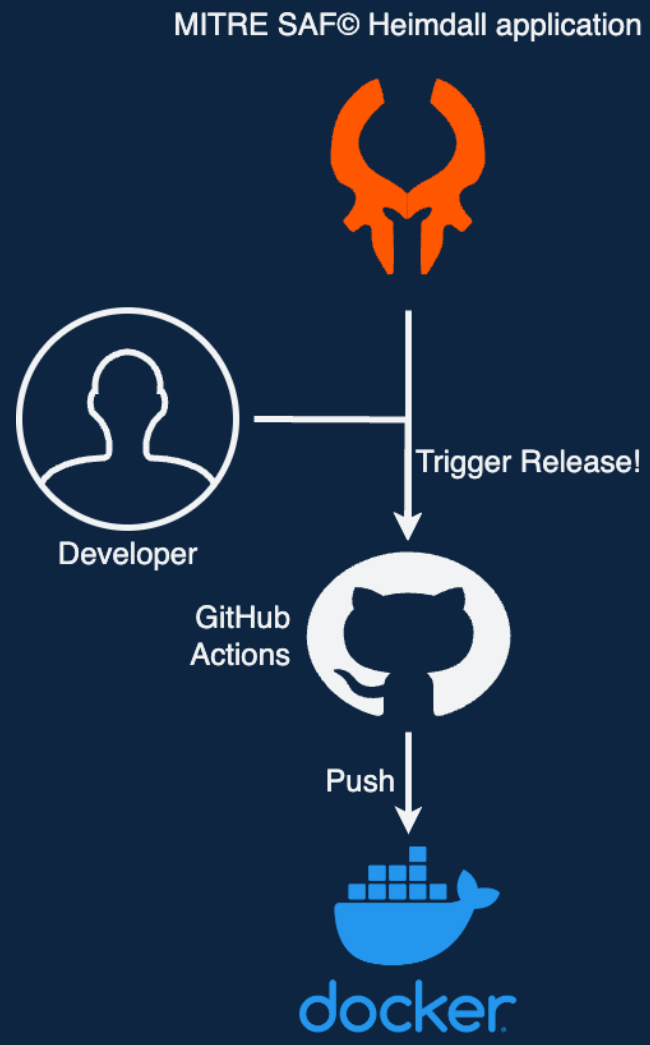
Pipeline Example – Original Release Pipeline

- MITRE SAF © uses GitHub Actions to write CI/CD pipelines for testing and releasing our software

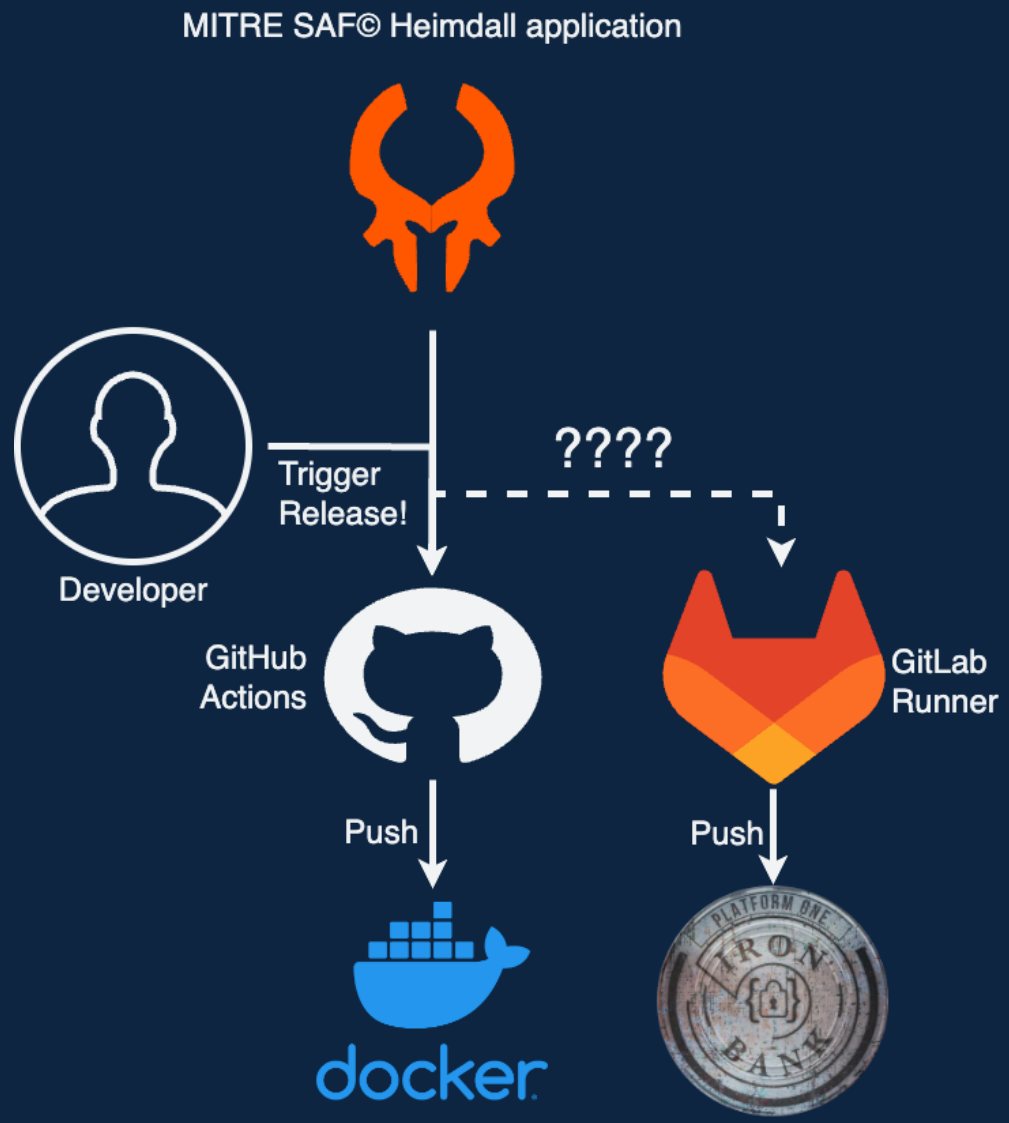
- Automatically push container builds to Docker Hub

```yaml
name: Push Heimdall Server to Docker Hub on every release

on:
  release:
    types: [published]
```



Heimdall Release Process



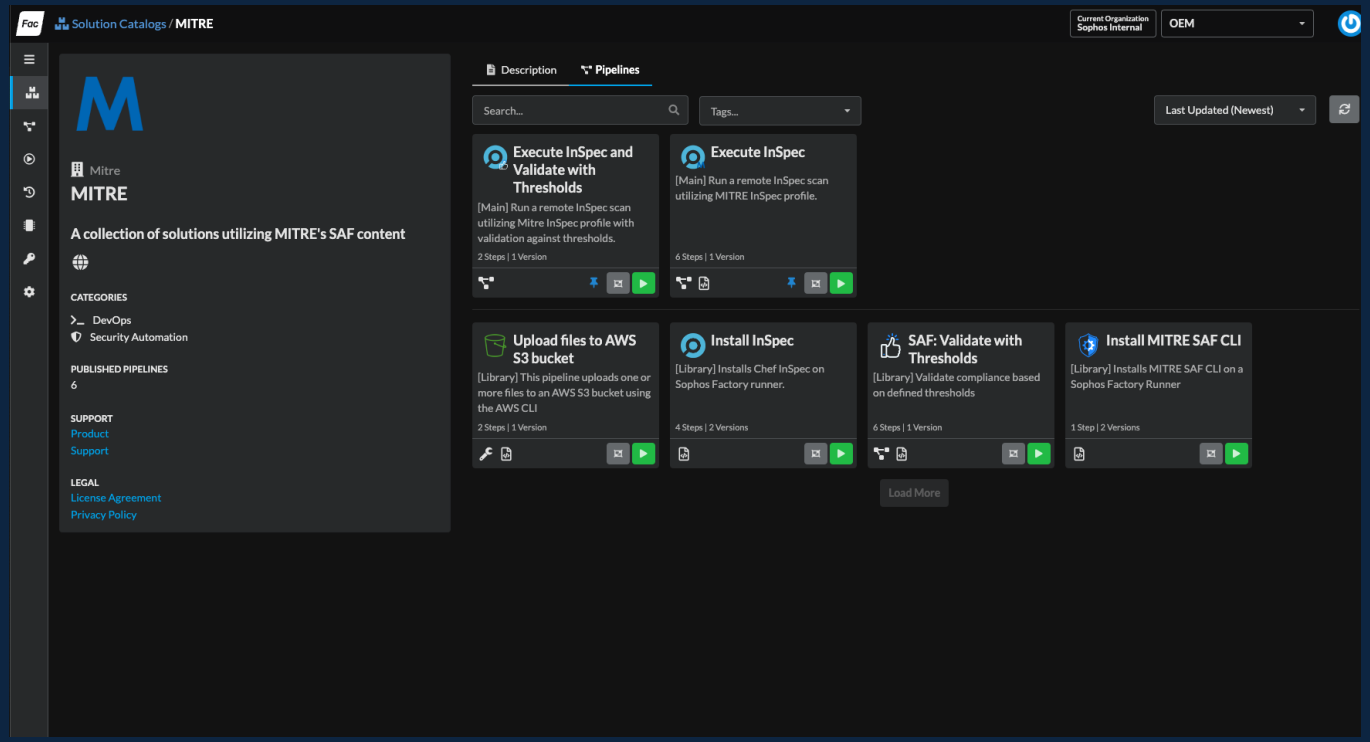
Heimdall Release Process
How to wire up GitHub and GitLab?

Pipeline Example – The Problem

- Iron Bank container Dockerfiles are stored in a GitLab repo
- GitLab Runners handle running security test battery
- Need another pipeline to get the new release into Iron Bank's internal security pipeline

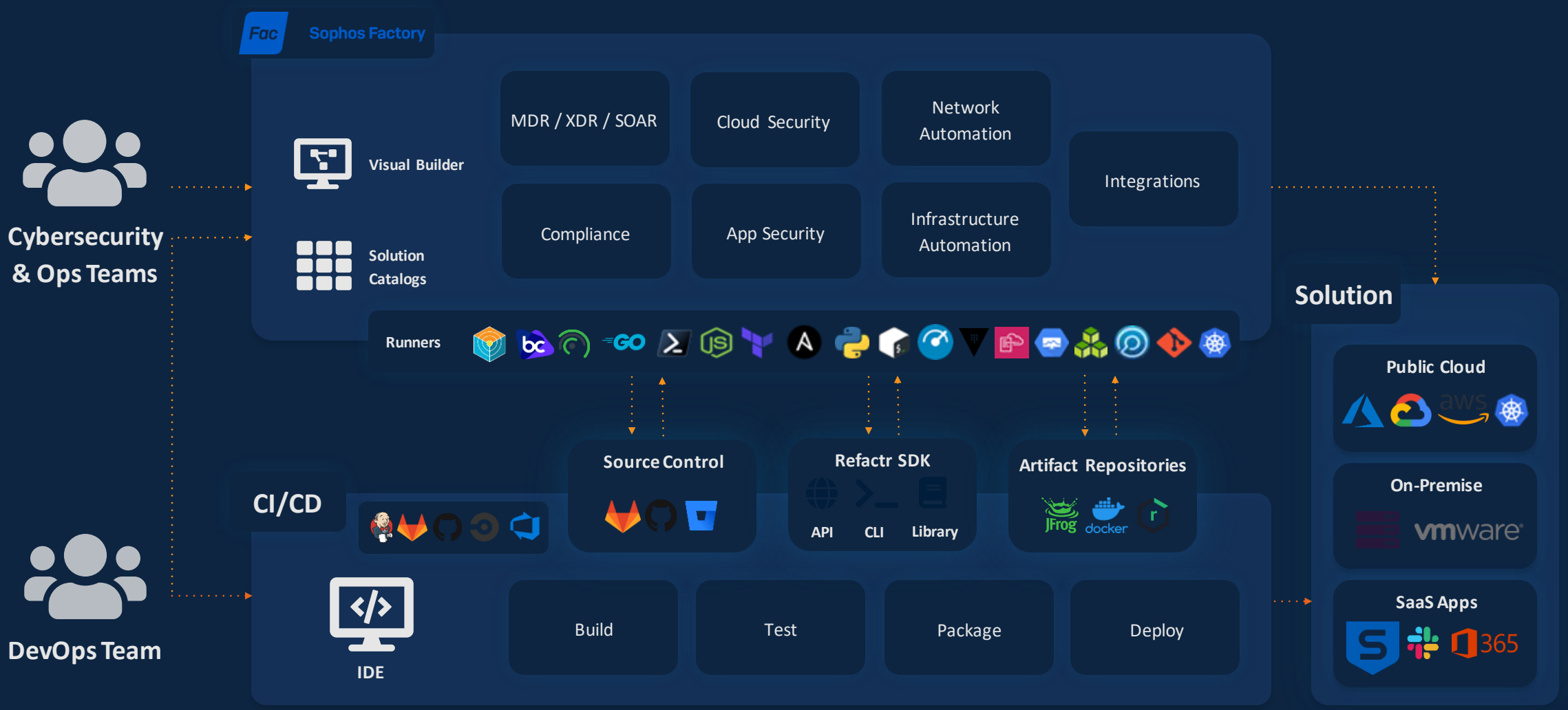
Sophos Factory – DevSecOps Automation Platform

- Collaborative Automation
  - Between Dev, Sec, Ops Teams
- Use Case Driven Automation
  - To Achieve DevSecOps
- Supports DevOps and Security Tools
  - To build modern IT as code solutions
- Ecosystem Enablement
  - Supports vendors through automation



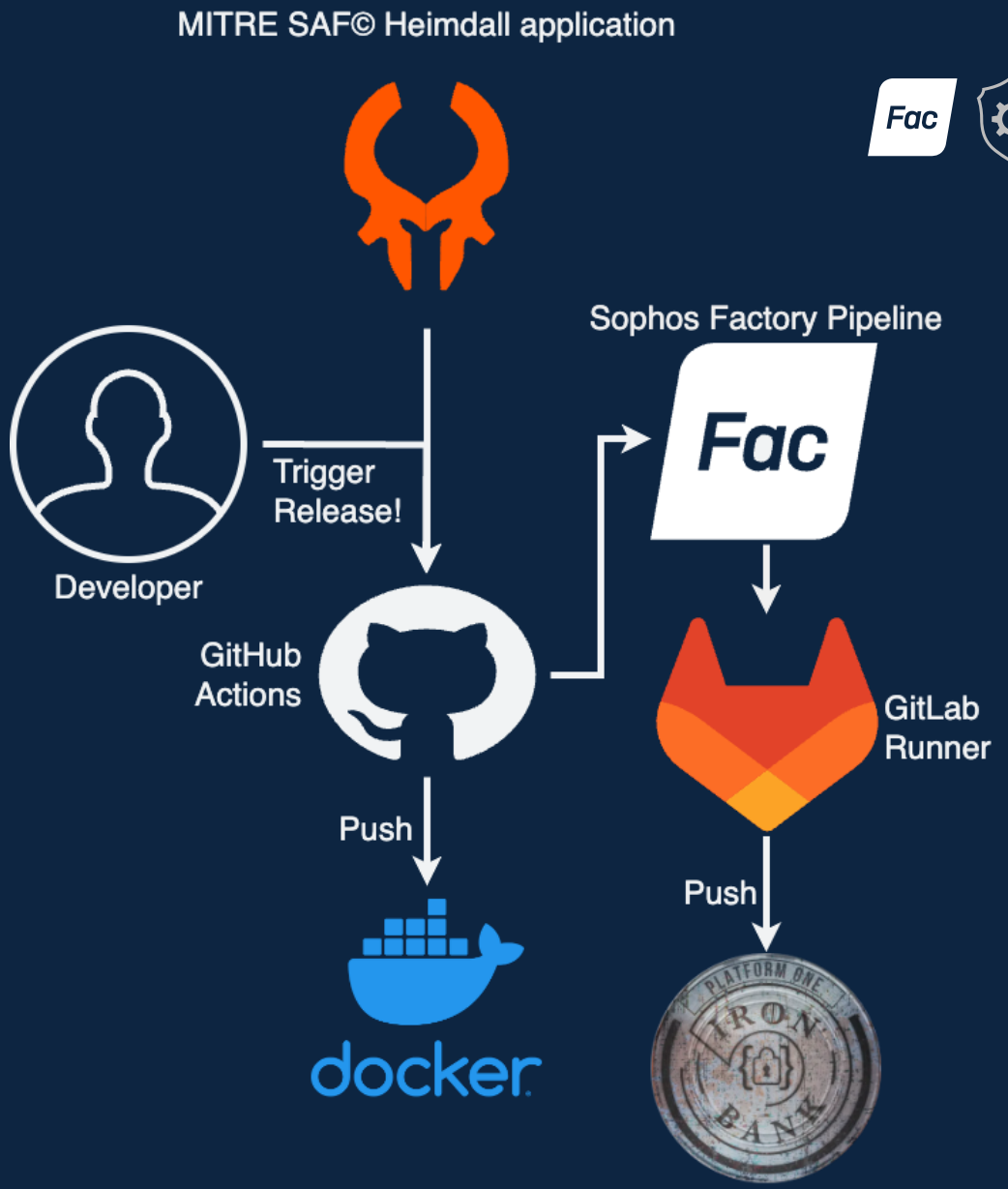
MITRE SOPHOS

Collaboration Between Dev, Sec, and Ops Teams



Pipeline Example – Full Release Process

- Used Sophos Factory to build ”supporting” pipeline
- GUI interface and ability to save functions as pipeline components makes building pipelines vastly more manageable



Heimdall Release Process
Using Sophos to Connect to Platform One/Iron Bank

MITRE

Challenge – So many tools for container scanning

- Helpful and informative tests are done best by **multiple scanning tools in tandem**
  - SAST and DAST, SBOM generation/dependency management, etc.
  - **Plus scanning actively running containers with InSpec!**
- Security tools typically generate data in unique formats that require multiple dashboards and utilities to process
  - Time-consuming process for completing security assessments
  - Data in disparate locations and inconsistent semantics of a data element between formats
  - Many security tools do not provide context to relevant compliance standards for comparison across security tools

MITRE

Security Data Normalization & Standardization

- Convert to **OASIS Heimdall Data Format**
  - Allows for **easier data management and comparisons** if all scan results are in the same normalized format

Already using **multiple tools** for scanning?

Great! Keep doing that!

Security Data Normalization – continued

- ✓ Translate data into a standard format to ensure interoperability
- ✓ Use OHDF Converters as a library in your custom application
- ✓ Add data conversion in your pipeline for automatic normalization in each run

Take a look at https://heimdall-lite.mitre.org for samples!

- SAF© CLI (command line interface)

- OHDF Converters

- SAF© GitHub Actions

- Heimdall Lite
- Heimdall Server

- Sophos Factory
- Tools Support with OHDF
- SAF © Solution Catalog

Supported Risk Information Sources

- AWS Security Hub
- Splunk
- AWS Config
- Snyk
- Aqua Security Trivy
- Tenable Nessus
- DBProtect
- CSV / XLSX
- Netsparker / Invicti
- Burp Suite
- GoSec
- Ion Channel
- Prisma
- SonarQube
- OWASP ZAP
- Prowler
- Fortify
- JFrog Xray
- Nikto
- SARIF
- ScoutSuite
- Twistlock
- DISA Checklist
- DISA XCCDF Results
- And more!

MITRE

Challenge – Host vs Container Responsibilities

- Huge chunks of security controls for containers need to be implemented by the container host
  - Good rule of thumb – any control that involves the kernel should not be implemented by a container
- “Is my container FIPS-enabled?” You'll need to ask the container AND the host!

So how can we make our testing tools reflect this?

MITRE

Total Requirements in the Red Hat 8 STIG:

343!

Total Requirements in the Red Hat 8 STIG
that can be implemented by containerized UBI8:

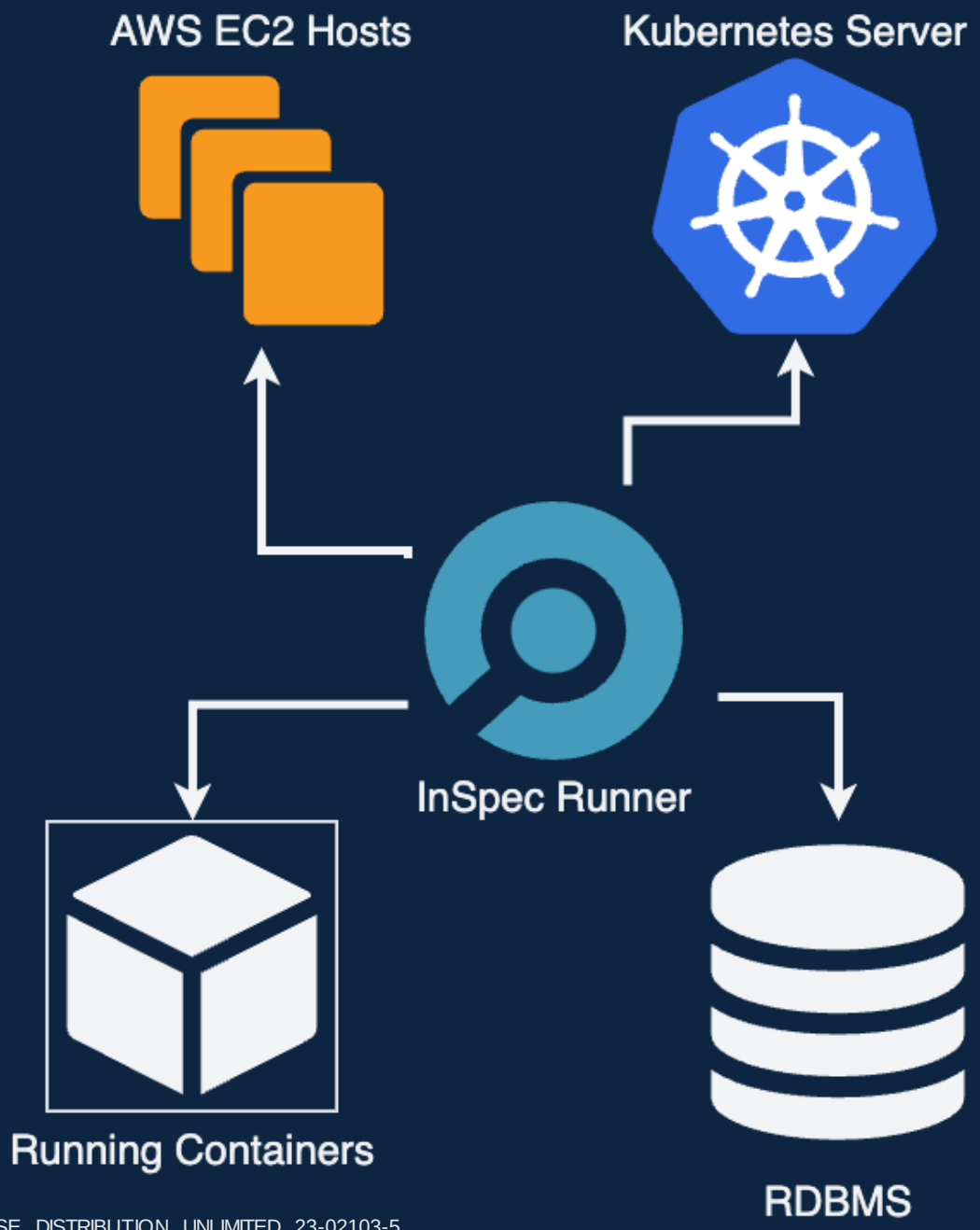
. . .140

If you only scanned the container,
then you're not finished with the validation process!

MITRE

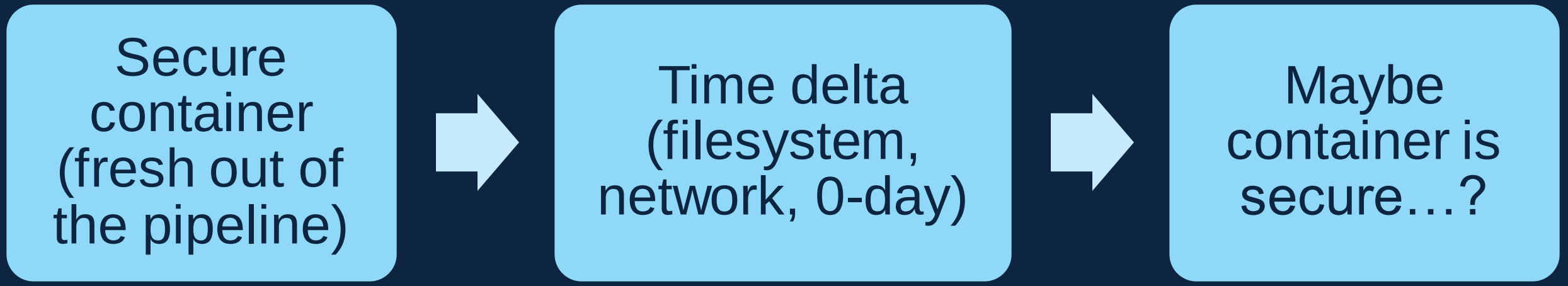
InSpec & the Stack

- InSpec is an effective tool for scanning containers **and the infrastructure that supports them**
- Hosts, orchestrators (e.g., Kubernetes), cloud environments, supporting components like DBs, etc.



Challenge – Maintaining Security Over Time

- Immutable software deployments are a double-edged sword
- You can scan the image, you can pass your pipeline, but how do I confirm that a deployed, running container is **still** secure?



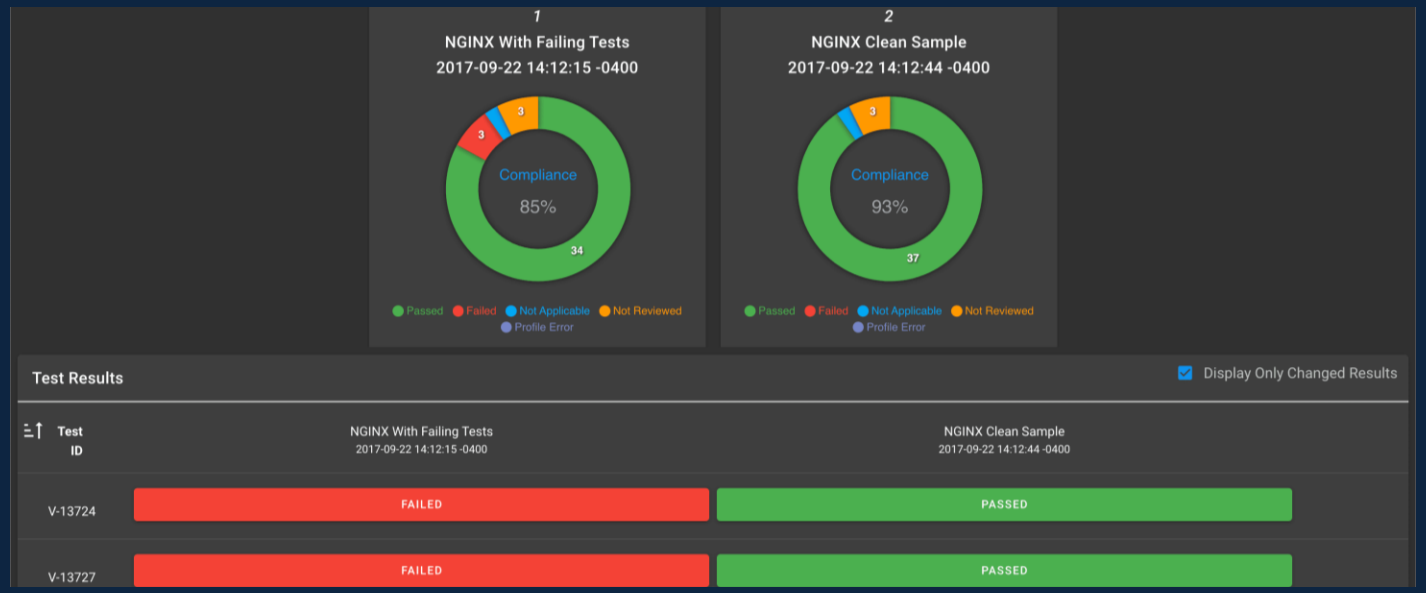
Container scanning

- Can't rely on the single data point from a run of a pipeline
- Need to make sure to regularly scan running containers to validate that there has been no slippage in compliance
- Take appropriate action to address an insecure container

Stonks

Possible compliance if left untouched

Time



Heimdall Compare View

MITRE

Gaps in coverage and future work

- **InSpec**: Direct InSpec transport to Kubernetes-hosted containers
- **Ephemerality**: Containers can be very short lived or inactive
  - Ex. serverless functions
  - A scan might not have finished or even started by the time the container shuts down
  - Scan containers at rest (CCE/CVE)
- **OHDF**: Deeper research & collaboration with the VEX, SBOM and Vuln communities

Running containers

Containers at rest

Questions?

Heimdall Lite	https://heimdall-lite.mitre.org/
Heimdall Server	https://heimdall-demo.mitre.org/
Vulcan	https://mitre-vulcan-staging.herokuapp.com
SAF CLI	https://saf-cli.mitre.org/
SAF GitHub Action	https://github.com/marketplace/actions/saf-cli-action
Emasser	https://mitre.github.io/emasser/
MITRE GitHub	https://github.com/mitre/(*baseline or app)
SAF Training	https://mitre.github.io/saf-training/
OHDF Technical Committee	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ohdf
Sophos Factory	https://www.sophos.com/en-us/products/sophos-factory

MITRE Security Automation Framework© | SOPHOS

https://saf.mitre.org saf@groups.mitre.org *https://sophos.com*

MITRE

BACKUP

Aaron Lippold

Principal Cybersecurity Engineer
Chief Engineer of the MITRE SAF

MITRE Security Automation Framework (SAF) ©

https://saf.mitre.org

alippold@mitre.org

@aaronlippold

https://www.linkedin.com/in/aaronlippold/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Will Dower

Lead Cybersecurity Engineer
MITRE SAF

MITRE Security Automation Framework (SAF) ©

https://saf.mitre.org

wdower@mitre.org

https://www.linkedin.com/in/william-dower-0b036ba7/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Amndeep Singh Mann
Software Engineer
MITRE SAF

MITRE Security Automation Framework (SAF) ©

https://saf.mitre.org

amann@mitre.org

https://www.linkedin.com/in/amndeep-mann-0b219669

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Mike Fraser

VP & Field CTO of DevSecOps

Sophos

https://www.sophos.com

Sophos Factory

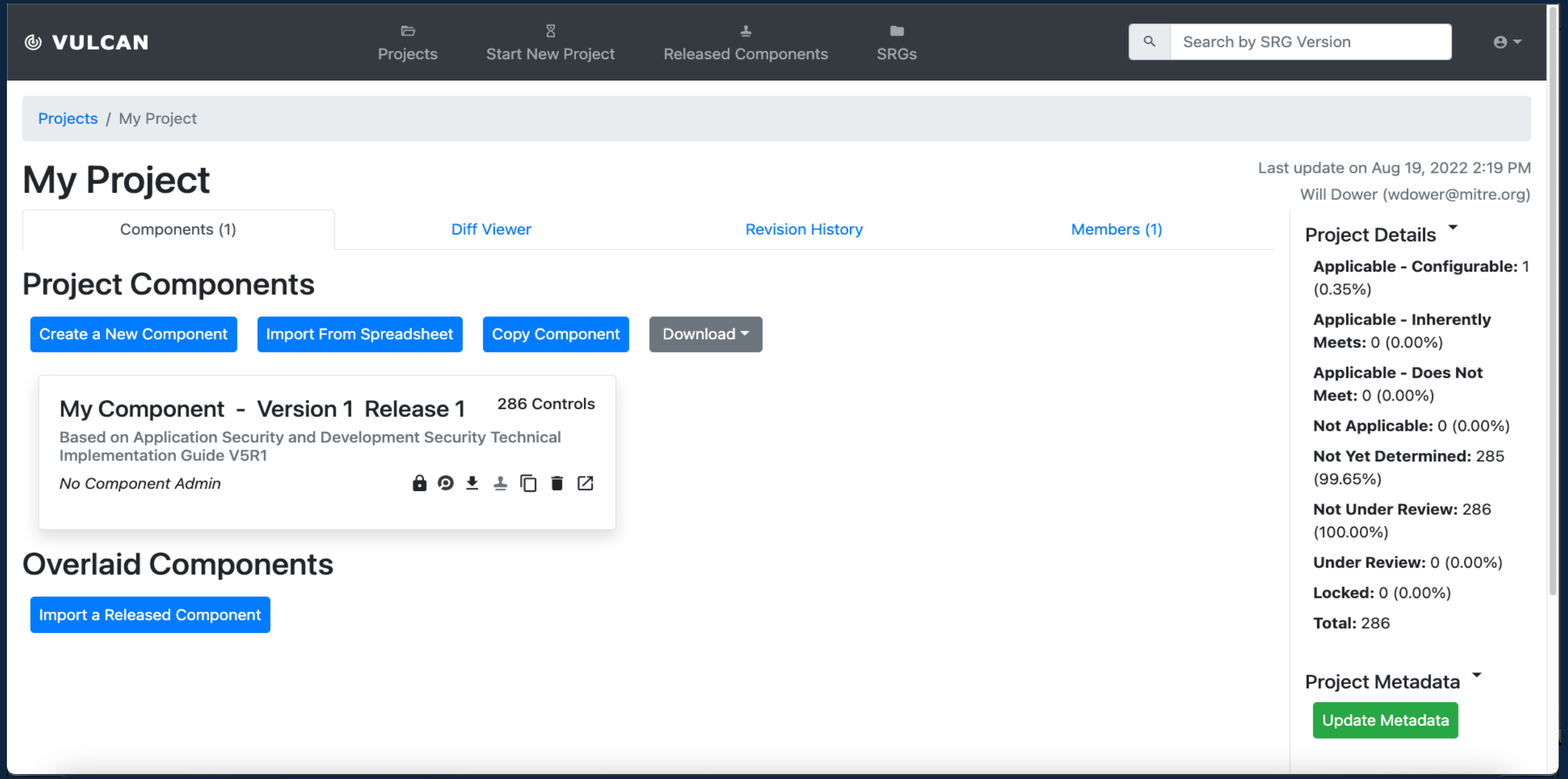
https://www.sophos.com/en-us/products/sophos-factory

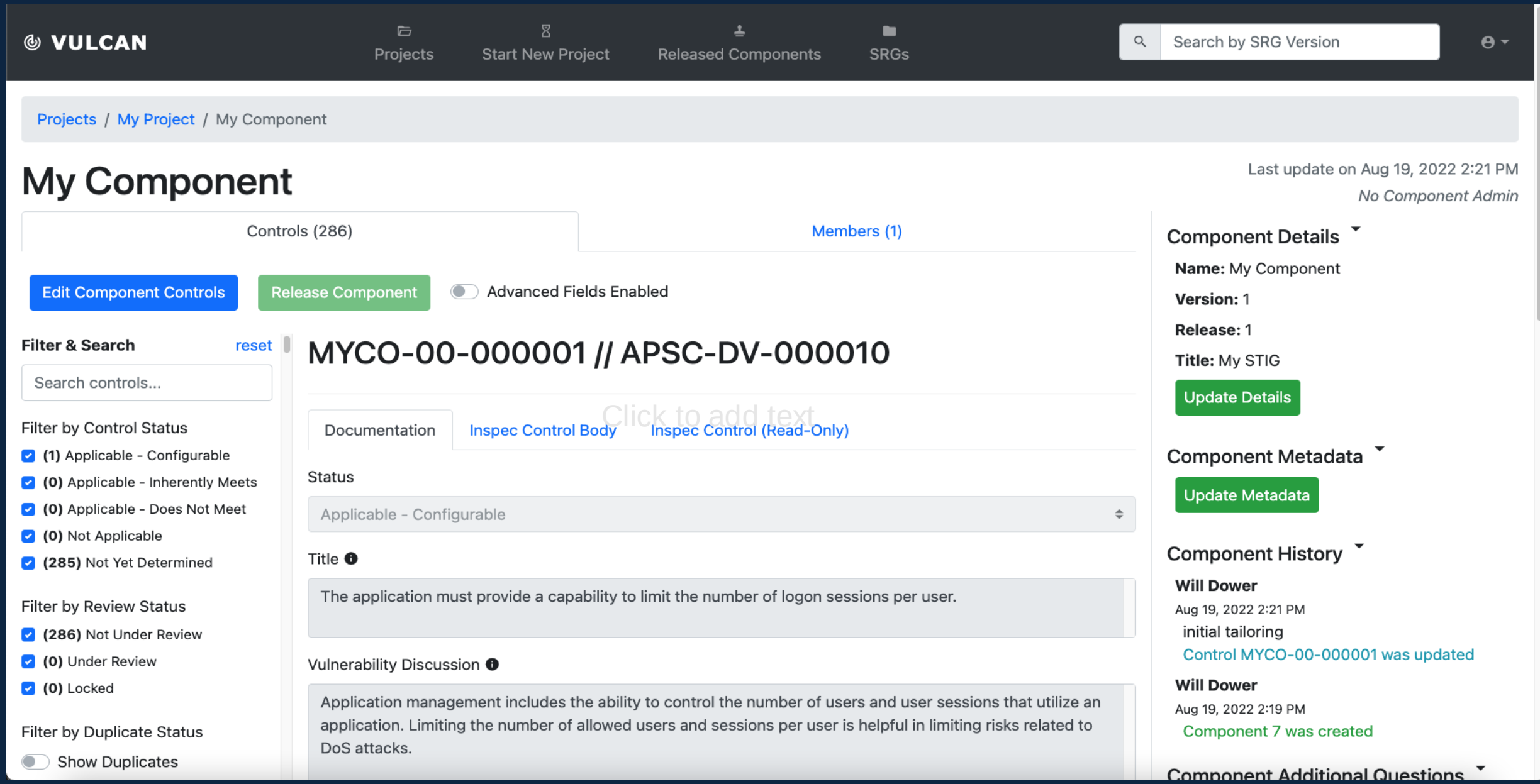
Mike.Fraser@Sophos.com

@itascode

https://www.linkedin.com/in/itascode/

SOPHOS Fac





MYCO-00-000001 // APSC-DV-000010

Documentation | Inspec Control Body | Inspec Control (Read-Only)

Language: Ruby | Theme: Visual Studio Dark | Copy

```ruby
    Ensure the number of sessions allowed per user is specified in accordance with the organi
    For development environments;  have the developer provide design documentation or demonst
    If the application is not configured to limit the number of logon sessions per user as de
  "
  desc  "fix", "Design and configure the application to specify the number of logon sessions
  impact 0.5
  tag severity: "medium"
  tag gtitle: "APSC-DV-000010"
  tag gid: nil
  tag rid: nil
  tag stig_id: "MYCO-00-000001"
  tag cci: ["CCI-000054"]
  tag nist: ["AC-10"]
  describe parse_config_file('session.conf') do
    its('max_logon_ssessions') { should cmp 5 }
  end

end
```