MITRE Security Automation Framework (MITRE SAF)™ Overview

MITRE

The Security Paradox

- Do you see opportunities to automate security work but don't have the time to start?
- Are you stuck doing repetitive manual security tasks or reassessments across multiple systems?
- Has your authority to operate (ATO) ever been delayed by missing security data or late-stage testing surprises?
- Does your software development process collect an overwhelming amount of security data that's hard to aggregate, prioritize, and act on?

MITRE

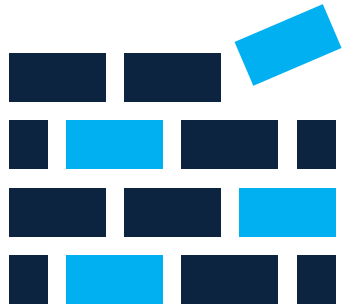
The Security Paradox, cont.

- MITRE's cross-collaborative position between government and industry allowed our engineers to notice these challenges recurring across many organizations.
- "The security paradox" – most teams want to build robust automation, but they cannot devote time to automate because they spend too many cycles dealing with the very inefficiencies that they want to automate away!
- The MITRE Security Automation Framework (MITRE SAF)™ was built to lower the barrier of entry for teams that want to solve the security paradox.

MITRE

What is MITRE SAF™?

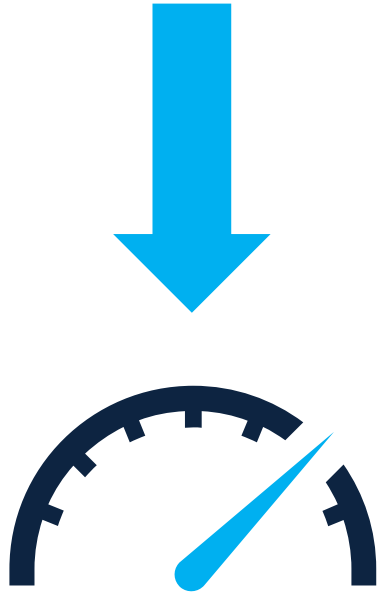
The MITRE Security Automation Framework (MITRE SAF)™ is a constantly growing collection of ready-made solutions to security automation problems across the software development lifecycle.



Build Security Automation Capabilities

Organizations use MITRE SAF™ to:

- Jump-start their own security automation capability in weeks instead of months or years
- Configure systems according to established security baselines to deliver more secure software, faster
- Turn days of manual security compliance and reporting labor into minutes of consistent, accurate automation

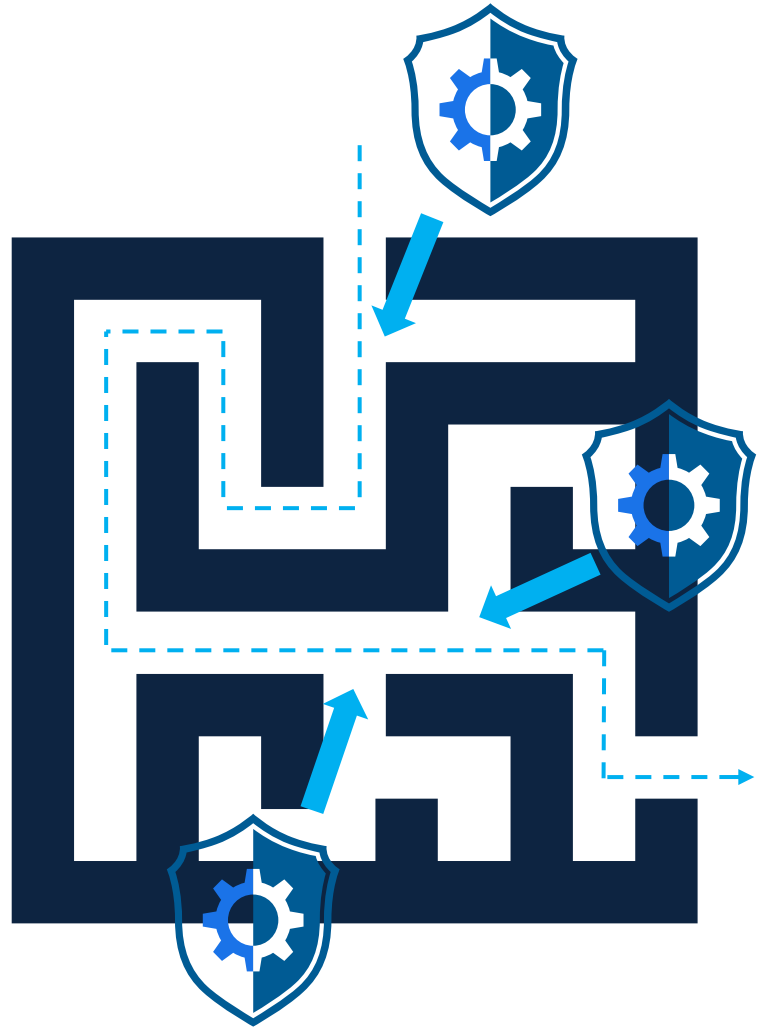


Accelerate Secure Software Development

MITRE

MITRE SAF's™ Guiding Principles

- Many difficult security automation problems facing government and industry teams have already been solved somewhere else—don't reinvent the wheel!
- Provide a common approach to creating security automation solutions
- Supported by an active, open-source security community
- Modular and flexible - use MITRE SAF™ to fill gaps, don't replace working processes
- Free!

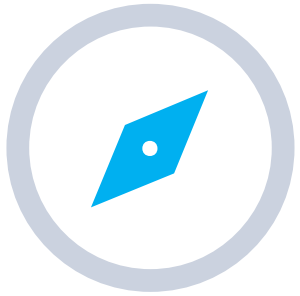


MITRE

MITRE SAF™ Capability Areas

MITRE SAF™ capability areas address security automation challenges across the software development lifecycle.

Use them individually or in concert as needed.



Plan

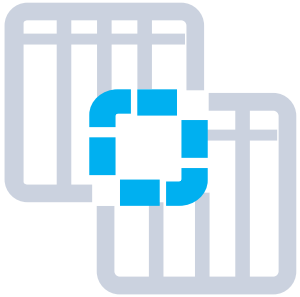
Choose, tailor, and create security guidance appropriate for your mission

Harden

Implement security baselines using our Ansible, Chef, and Terraform content

Validate

Generate detailed security testing results via automated tests and manual attestation



Normalize

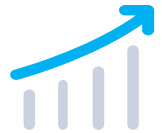
Convert security results from all your security tools into a common data format

Visualize

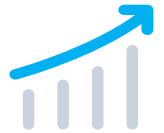
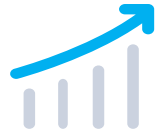
Identify overall security status and deep-dive to solve specific security defects

MITRE

Common User Stories

User Story	MITRE SAF™ Capability Area
"I am an **Information System Security Officer (ISSO)** responsible for **showing how we securely configure a software component** that has no published guidance."	**Plan** 
"I am a **developer** and I need to **rapidly apply a Security Technical Implementation Guide (STIG) to my system**. I don't want to get bogged down doing it manually, and I don't have the time to write quality automation to do it."	**Harden**  **Validate** 
"I am a **DevSecOps pipeline engineer** and my pipeline is running dozens of testing tools. I'm **having trouble managing all the data** and summarizing it for leadership."	**Normalize**  **Visualize** 

Common User Stories, cont.

User Story	MITRE SAF™ Capability Area
"I am a **cloud security engineer** and my environment's gold images are built 'by-hand' for my cloud environment and my on-prem virtual machine environment. I need **standard solutions** for automating gold image builds across platforms."	**Harden**  **Validate** 
"I am an **assessor** and I need to determine how a program's security tooling covers a set of security and privacy controls."	**Normalize**  **Visualize** 
"I am an **ISSO** and I am having trouble **keeping my eMASS instance up to date** with the data coming from my automated pipelines and my monitoring tools."	**Normalize**  **Visualize** 

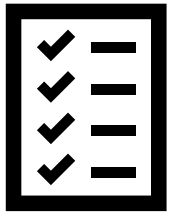
Capabilities - Plan

Security Requirements Guide (SRG)

⇩

MITRE Vulcan™

⇩



Package (STIG, CSV, Hardening & Validation content)

Build your system on a strong foundation of requirements.

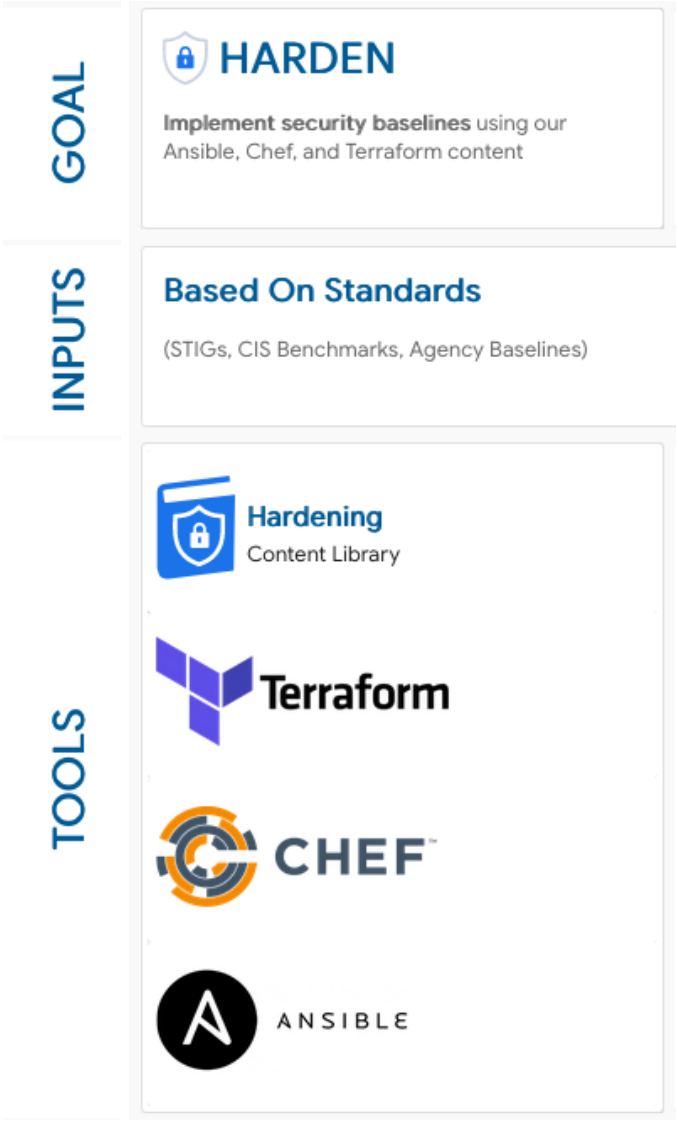
- Use MITRE Vulcan™ to:
  - Develop STIG-ready content aligned to SRGs
  - Speed STIG development via collaboration, reuse, revision across many programs and stakeholder experiences
  - Streamline creation of automated hardening and validation code
  - Define security before you implement it!

MITRE

Capabilities - Harden

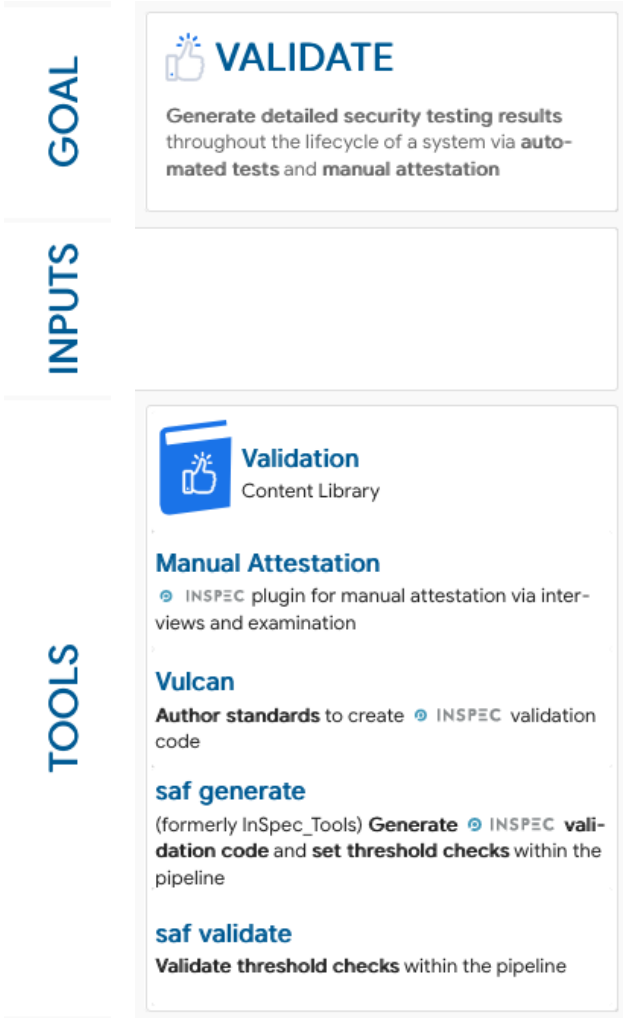
Configure software components for security.

- Use the MITRE SAF™ hardening library to:
  - Provide “off the shelf” automated hardening solutions for common software components—don’t reinvent the wheel!
  - Use standard configuration management tools that developers already know
  - Share across security community—open-source content (Apache v2)
  - Span entire development stack
    - Cloud infrastructure, platform, & operating system
    - Database, webserver, & application



MITRE

Capabilities - Validate



Automate robust, repeatable, and tailorable security validation.

- Use the MITRE SAF™ Validation Library to:
  - Confirm and report on secure configuration of software components
    - Run the tests anytime:
      - Automatically run at every build
      - Manually for point-and-shoot scanning
      - Schedule them for Continuous Monitoring
    - Anywhere:
      - Cloud, container platform, bare metal hardware, virtual machines
    - On anything:
      - Operating systems, cloud infrastructure, platforms, databases, applications, webservers. . .

MITRE

MITRE SAF™ Content Library

- Collection of stewarded security automation code and libraries for hardening and validating a wide variety of systems

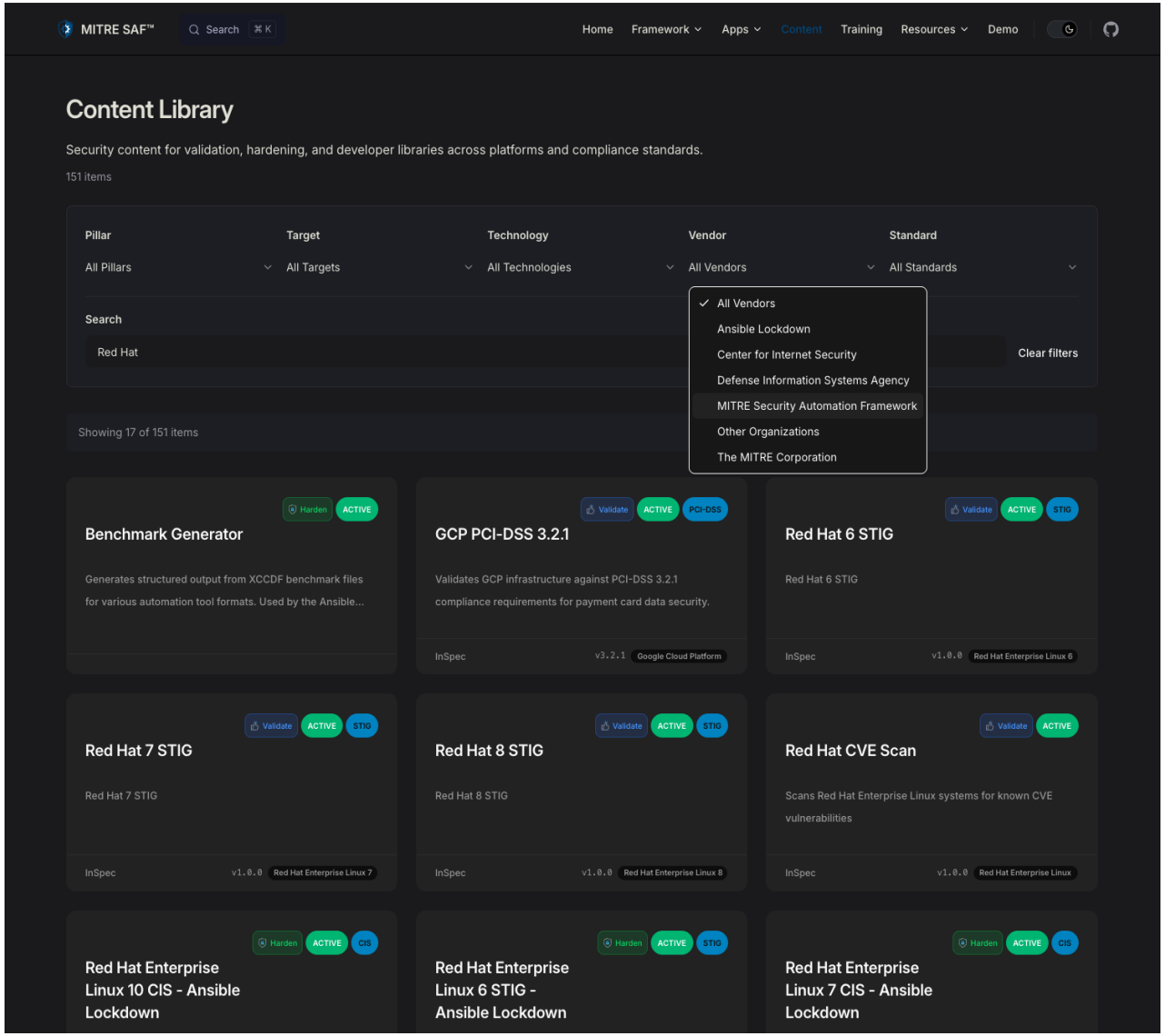
- All are free under an Apache 2 license
  - Use them off-the-shelf, or as the foundation for organization- or project-specific automation

- See https://saf.mitre.org/content and avoid reinventing the wheel!

MITRE SAF™ Content Library

https://saf.mitre.org/content

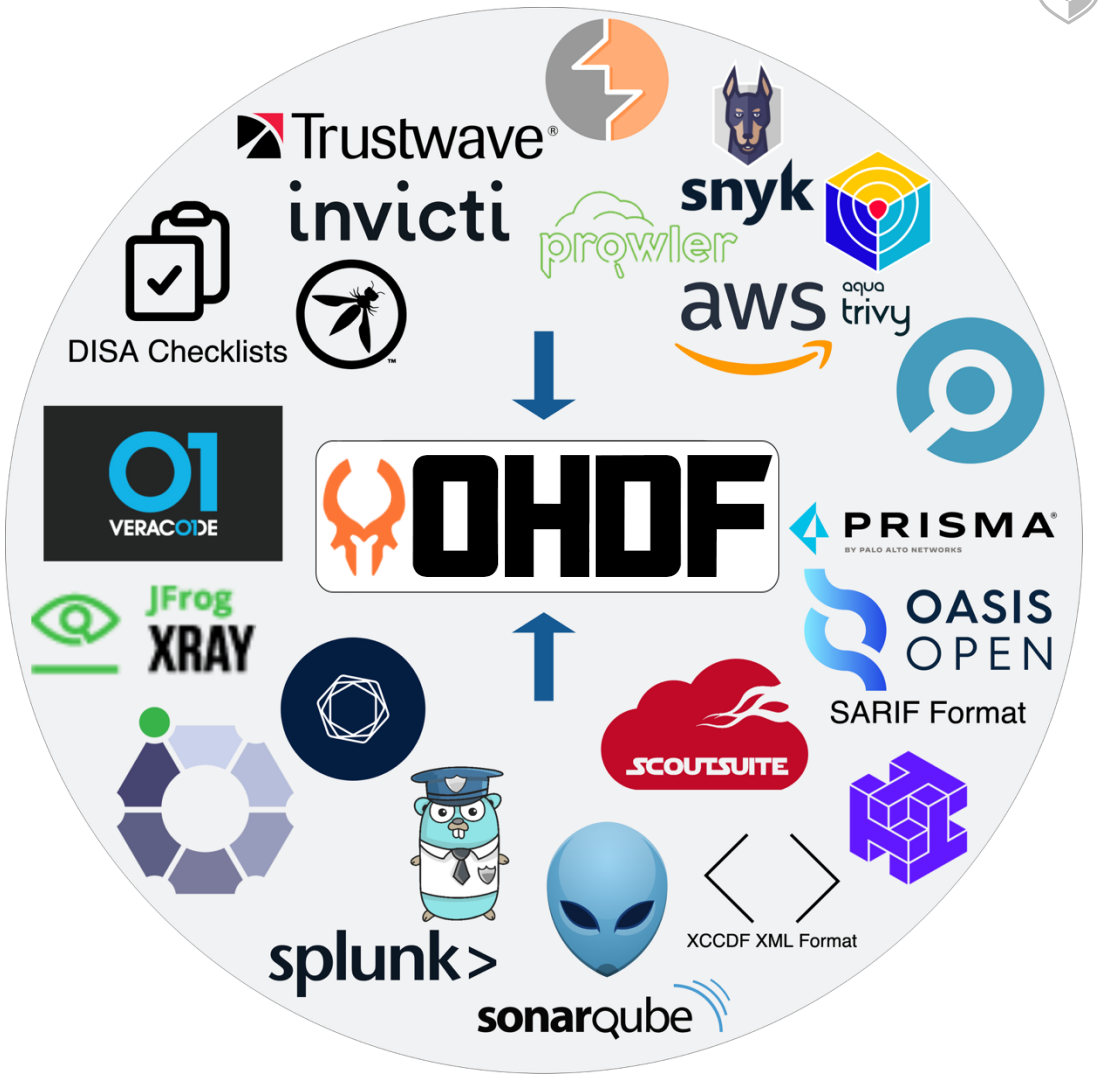
- Collection of stewarded security automation code and libraries for hardening and validating a wide variety of systems
- All are free under an Apache 2 license
  - Use them off-the-shelf, or as the foundation for organization- or project-specific automation
- Avoid reinventing the wheel!



Capabilities - Normalize

Get your security data flows under control.

- Use the OASIS Heimdall Data Format (OHDF) to:
  - Integrate, aggregate, and analyze security data from all available sources
  - Preserve data integrity with original source data
  - Maximize interoperability and data sharing
  - Transform and transport data between security/management processes or technologies
  - Map and enrich security data to relevant compliance standards (GDPR, NIST SP 800-53, PCI-DSS, etc.)



See the full list of supported formats at
https://saf-cli.mitre.org/#convert-to-hdf

MITRE

Capabilities - Visualize

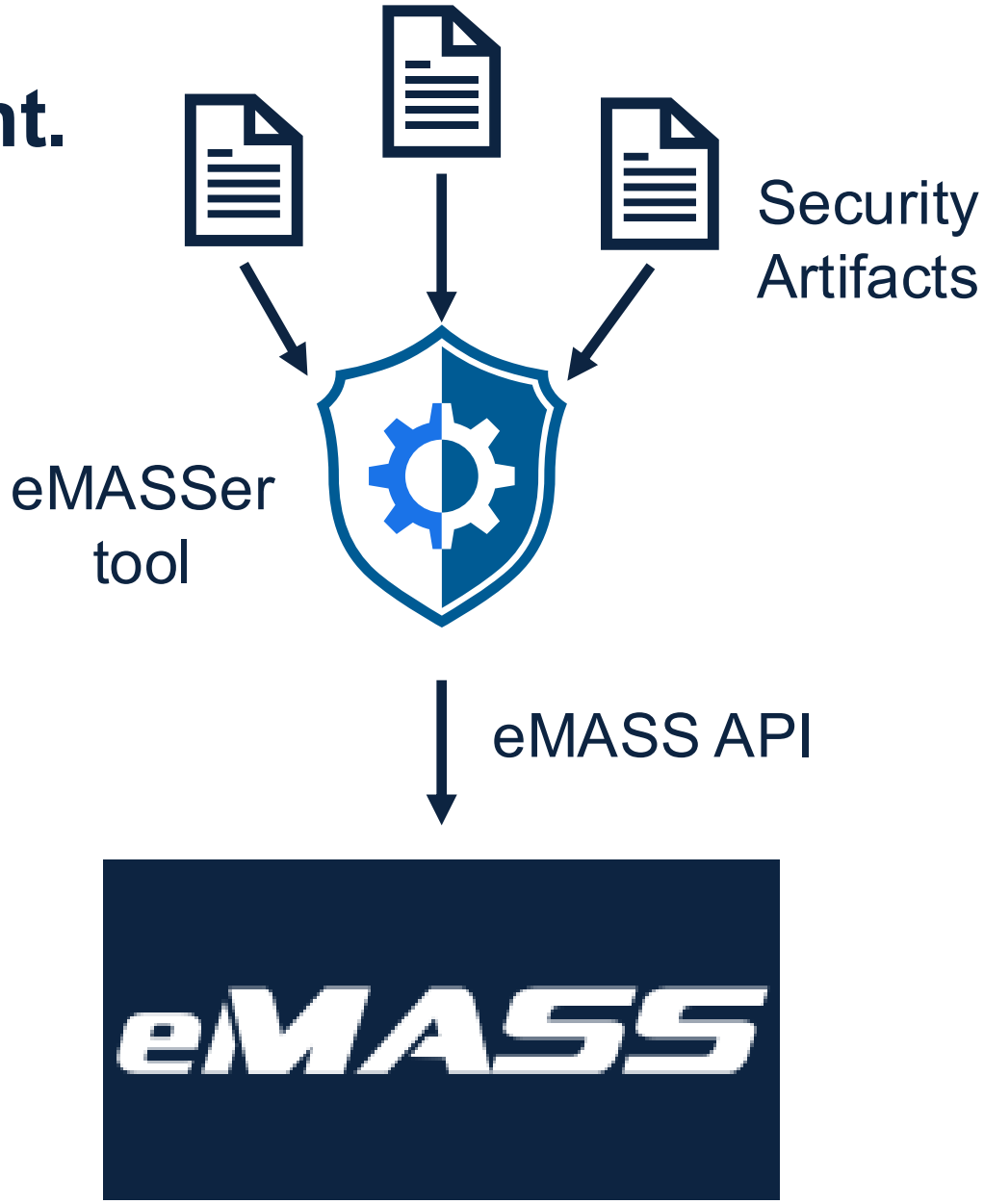
Security data informs risk decisions.

- Use MITRE Heimdall™ to:
  - Aggregate test results into rollups, charts, and timelines
  - Deep dive into data to prioritize actions to reduce risk

Capabilities - Visualize Cont.

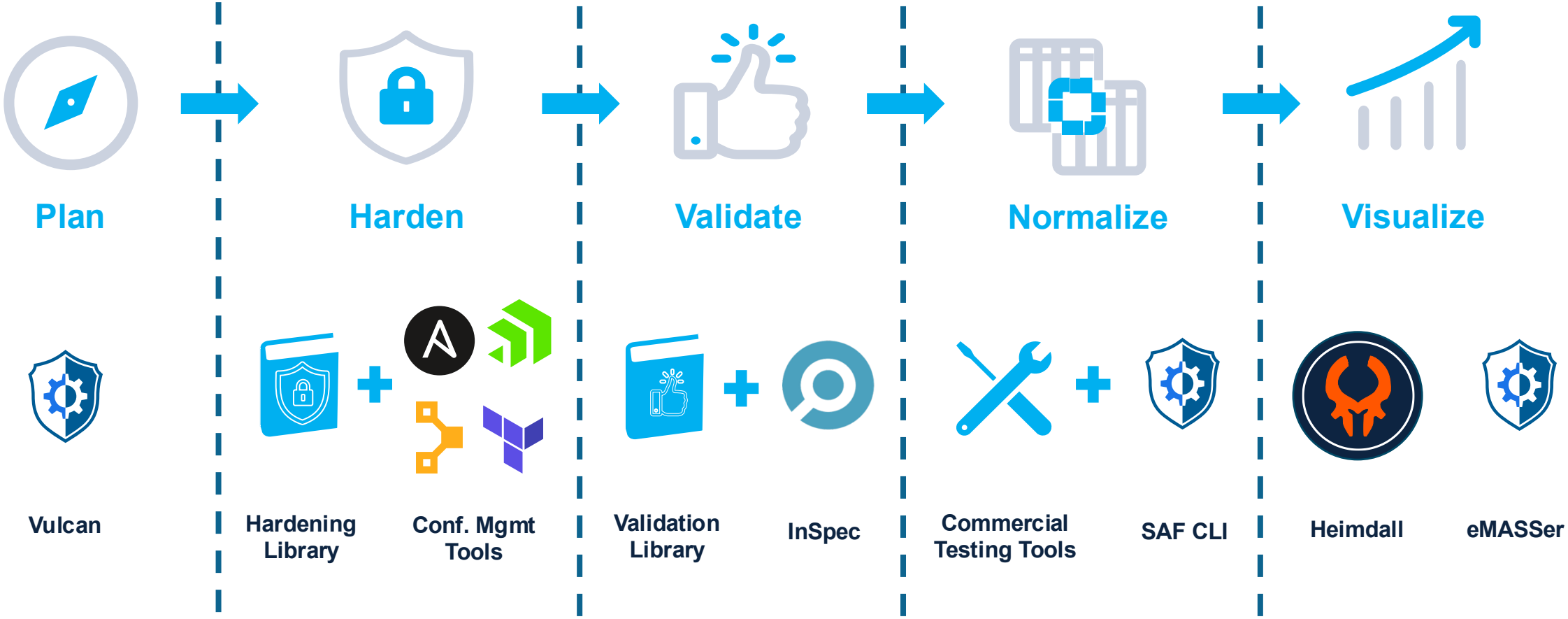
Simplify reporting to governance, risk, and compliance tools.

- Use MITRE SAF™ to push normalized data to systems of record over application programming interfaces (APIs)
  - eMASSer - libraries and convenient command-line interface (CLI) tool for keeping eMASS package up to date
  - Remove friction stemming from manual reporting!



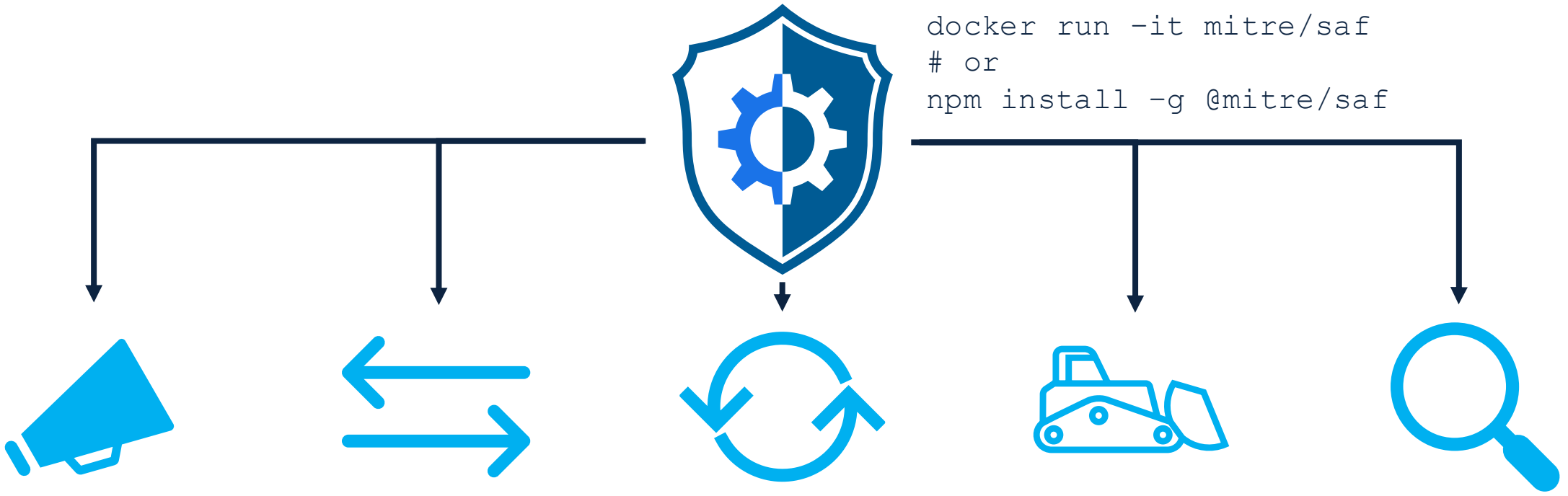
The Big Picture

MITRE SAF™ capabilities flow together to provide a security automation life cycle.



SAF CLI

A Swiss army knife for security automation—one tool, many functions.



```
docker run -it mitre/saf
# or
npm install -g @mitre/saf
```

Attest

Inject manual attestation data into automated workflows

Convert

Translate data into—or out of—OHDF

Delta

Update validation profiles when new benchmarks are released

Generate

Rapidly scaffold new validation code

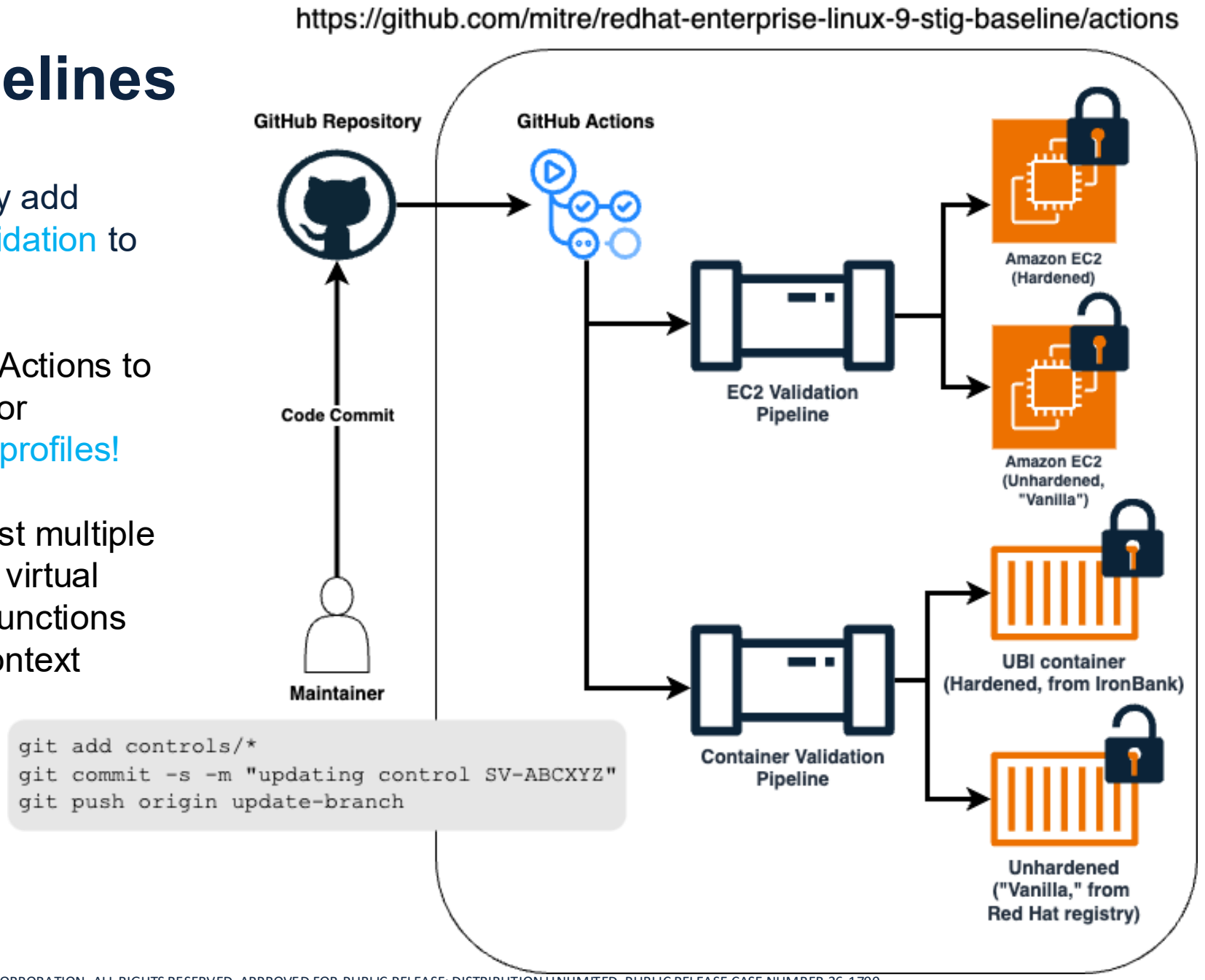
Threshold

Check any OHDF file against a pre-defined definition of security

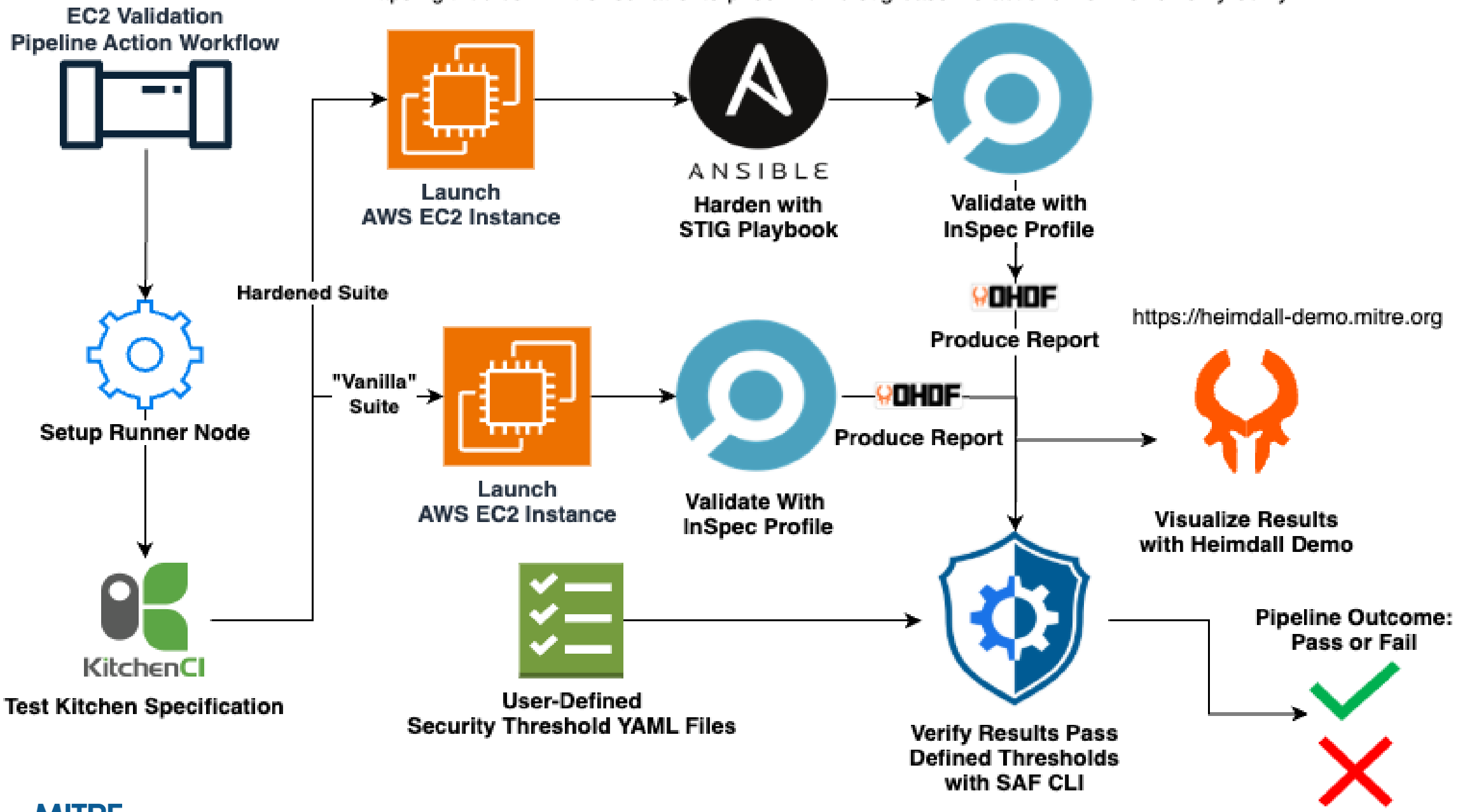
MITRE

Use Cases – Pipelines

- Use MITRE SAF™ to rapidly add tailorable hardening and validation to a gold image pipeline
- MITRE SAF™ uses GitHub Actions to construct sample pipelines for validating its own validation profiles!
- We test major profiles against multiple platforms (container and full virtual machine) to ensure testing functions regardless of deployment context

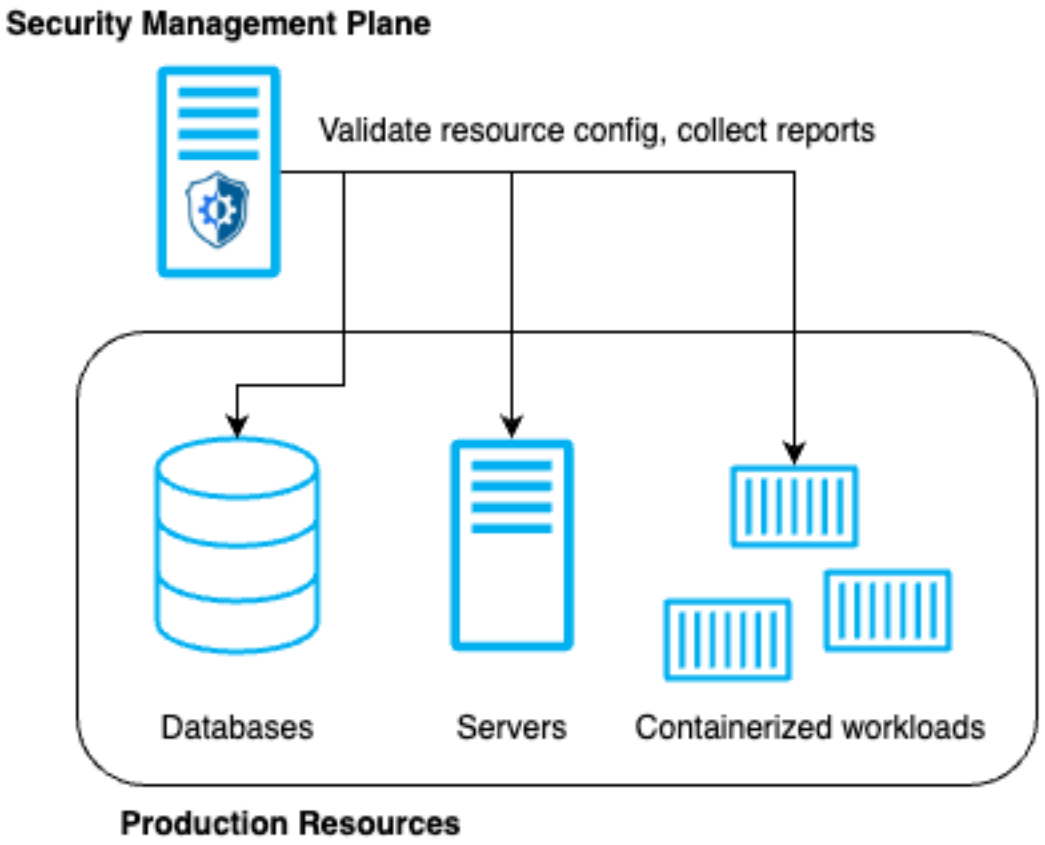


https://github.com/mitre/redhat-enterprise-linux-9-stig-baseline/actions/workflows/verify-ec2.yml



MITRE

Use Cases – Ops Monitoring



- MITRE SAF™ tools and practices can be leveraged to collect and analyze operational data
- Use the same validation in both Dev and Ops – open book testing
- Flexibility of deployment is key to scale
- InSpec validation can run from a security management server, a container, an AWS Lambda function, a Kubernetes cronjob, etc.

Demo – MITRE Heimdall™

https://heimdall-demo.mitre.org

(Feel free to try it yourself!)

MITRE

Questions?

Heimdall Lite	https://heimdall-lite.mitre.org/
Heimdall Server	https://heimdall-demo.mitre.org/
Vulcan	https://vulcan.mitre.org
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
SAF Training	https://mitre.github.io/saf-training/

MITRE Security Automation Framework (MITRE SAF)™

https://saf.mitre.org | saf@mitre.org

MITRE

Backup

From the DODI 8500.01 https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

- "2.b. Develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, **using input from stakeholders**, and **using automation whenever possible**."
- "3.g. Using automation whenever possible in support of cybersecurity objectives including, but not limited to, secure configuration management, continuous monitoring, active cyber defense, and incident reporting and situational awareness."
- "4 d. Standards-Based Approach. The DoD cybersecurity and cyberspace defense data strategy will enable semantic, technical, and policy interoperability through a standards-based approach that has been refined by many in industry, academia, and government. It is an information-oriented approach (see for example the security content automation protocol (SCAP) discussion in NIST SP 800-126 (Reference (ci))."
  - (ci) National Institute of Standards and Technology Special Publication 800-126, "The Technical Specification for Security Content Automation Protocol (SCAP): SCAP Version 1.1," current edition

MITRE

MITRE SAF™ and the DODI 8500.01

- Goals and Intentions based on the policy
  I. Ongoing technology improvements would evolve the state of the art for the capability requirement
  II. That the instruction specifically did not define any specific implementation technology
  III. Technology examples referenced to then current standards and exemplars
- SAF's part of the process
  - Provide automation that is all based on standards (DISA STIGs, SRGs, CIS Benchmarks, etc.) and can be exported in necessary formats for GRC tools (eMASS, Splunk, RSA Archer, DISA Checklist)
  - Integration with eMASS Program of Record for pulling and pushing data
  - Working with DoD CIO to update recommendations and policy to better articulate requirements in the face of ever evolving technologies and capabilities, enabling automated and continuous ATO

MITRE

Example: SCAP vs. InSpec Output Comparison

RedHat 7 Operating System Scans

Score

96.63%

Adjusted Score: 96.63%
Original Score: 96.63%
Compliance Status: GREEN

Pass:	172	Not Applicable:	0
Fail:	6	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	178

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

Note that the SCAP checklist only contains 178/246 checks, making the score much lower

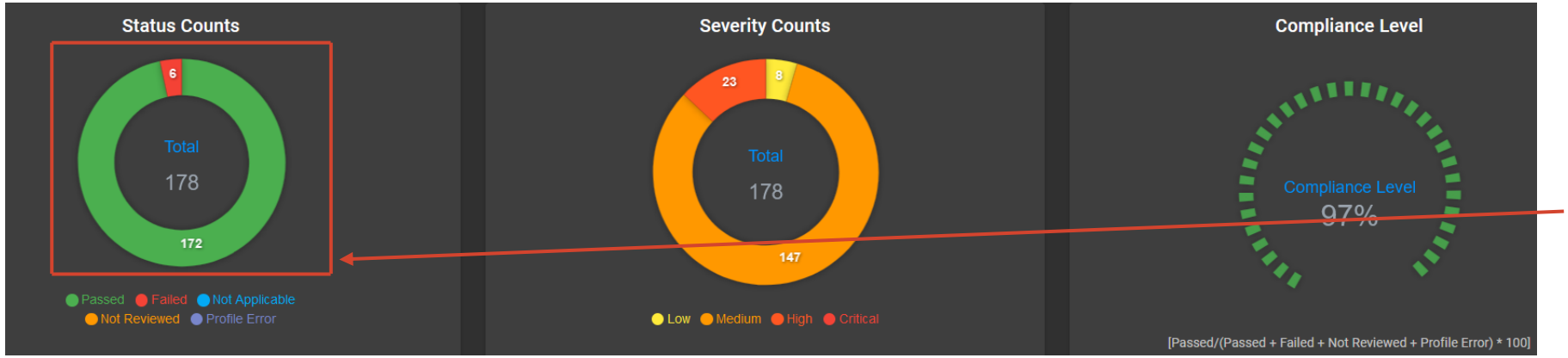
InSpec, visualized by Heimdall, includes all 246 checks even if they are not applicable

Heimdall

Example: SCAP vs. InSpec Output Comparison Heimdall

RedHat 7 Operating System Scans

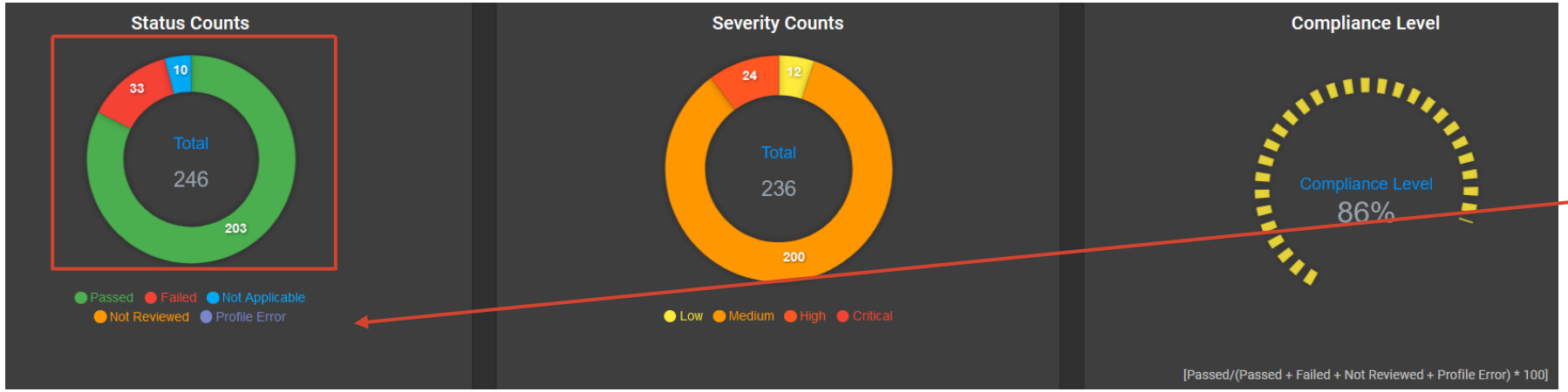
SCAP (SCC)



SCAP output only contains 178 checks out of the 246 STIG items

This does not provide accurate representation of the true compliance posture

Heimdall



InSpec, visualized by Heimdall, includes all 246 checks even if they are not applicable

MITRE

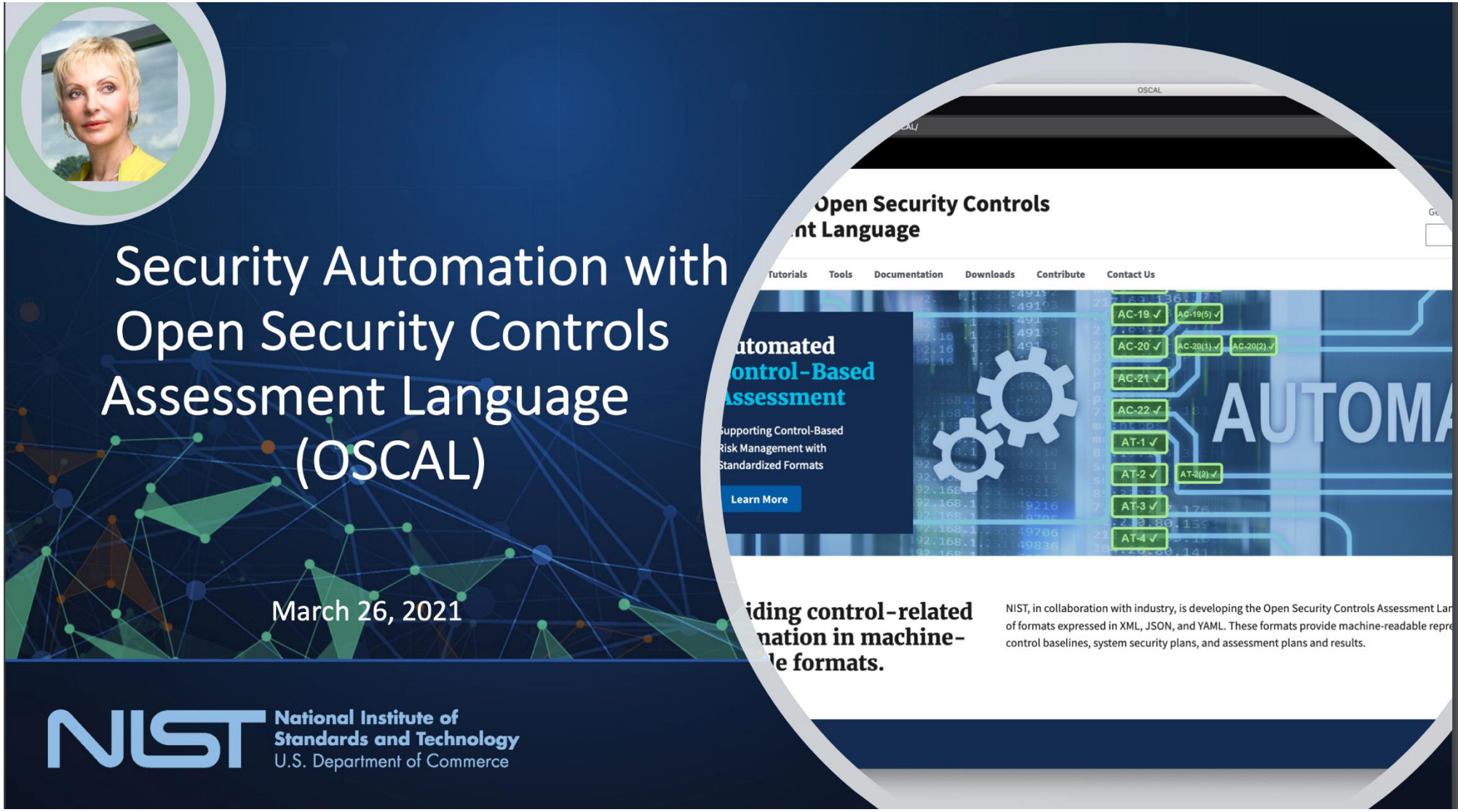
MITRE SAF™ and OSCAL

- OSCAL is a NIST/FedRAMP partnership - Open Security Controls Assessment Language
  - OSCAL can be used to represent SAR, SAP, and SSP in machine-readable format
  - Can also be used to define an organizational subset of NIST security controls
- OSCAL is the language for writing *assessment reports* and MITRE SAF produces the *assessment report's contents*

MITRE

ATARC JK ORION Working Group

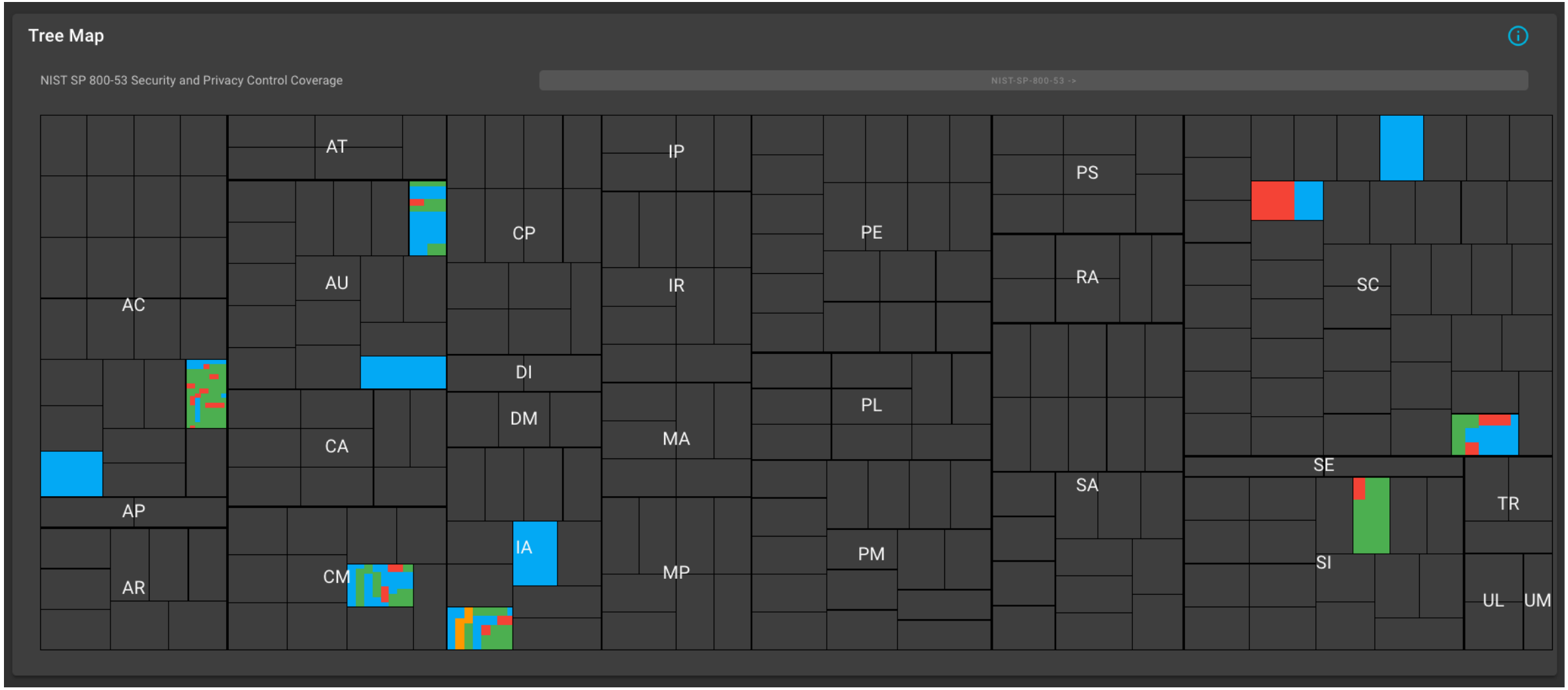
- NIST OSCAL
- GSA GovReady
- FedRAMP
- MITRE SAF™
- Vendors



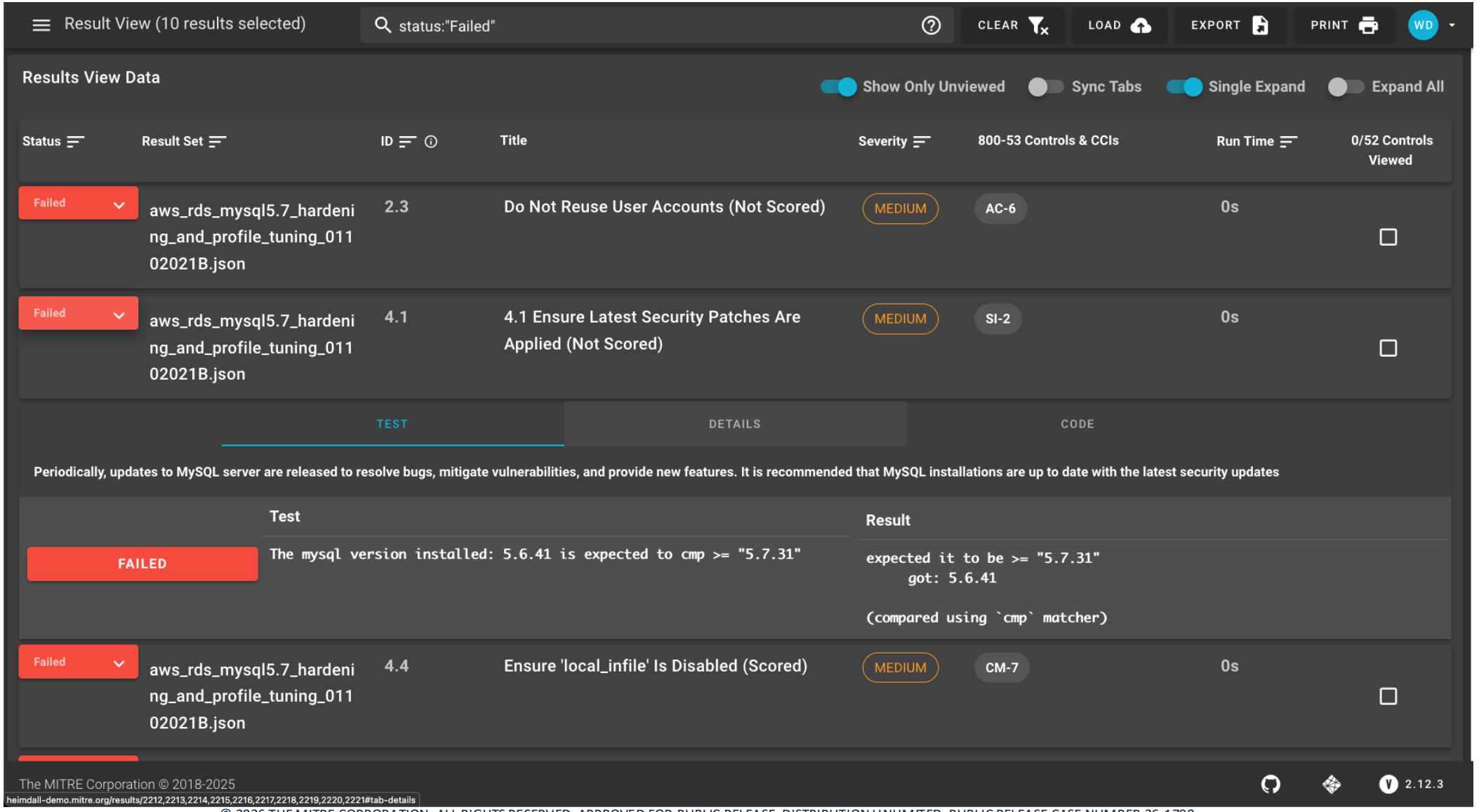
https://gitlab.com/atarc/orion/-/raw/main/presentations/OSCAL.pdf

Heimdall

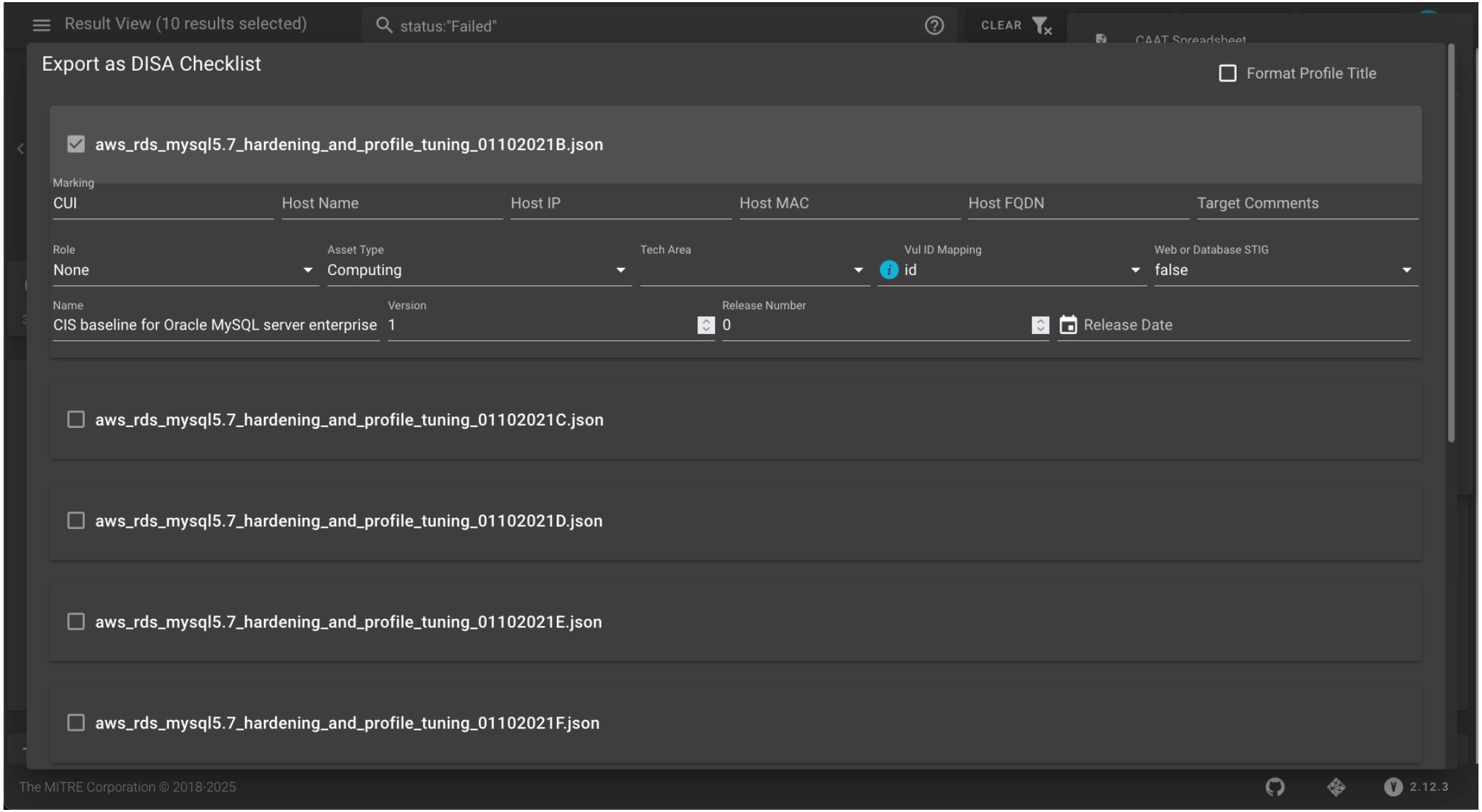
Heimdall – NIST 800-53 coverage tree map



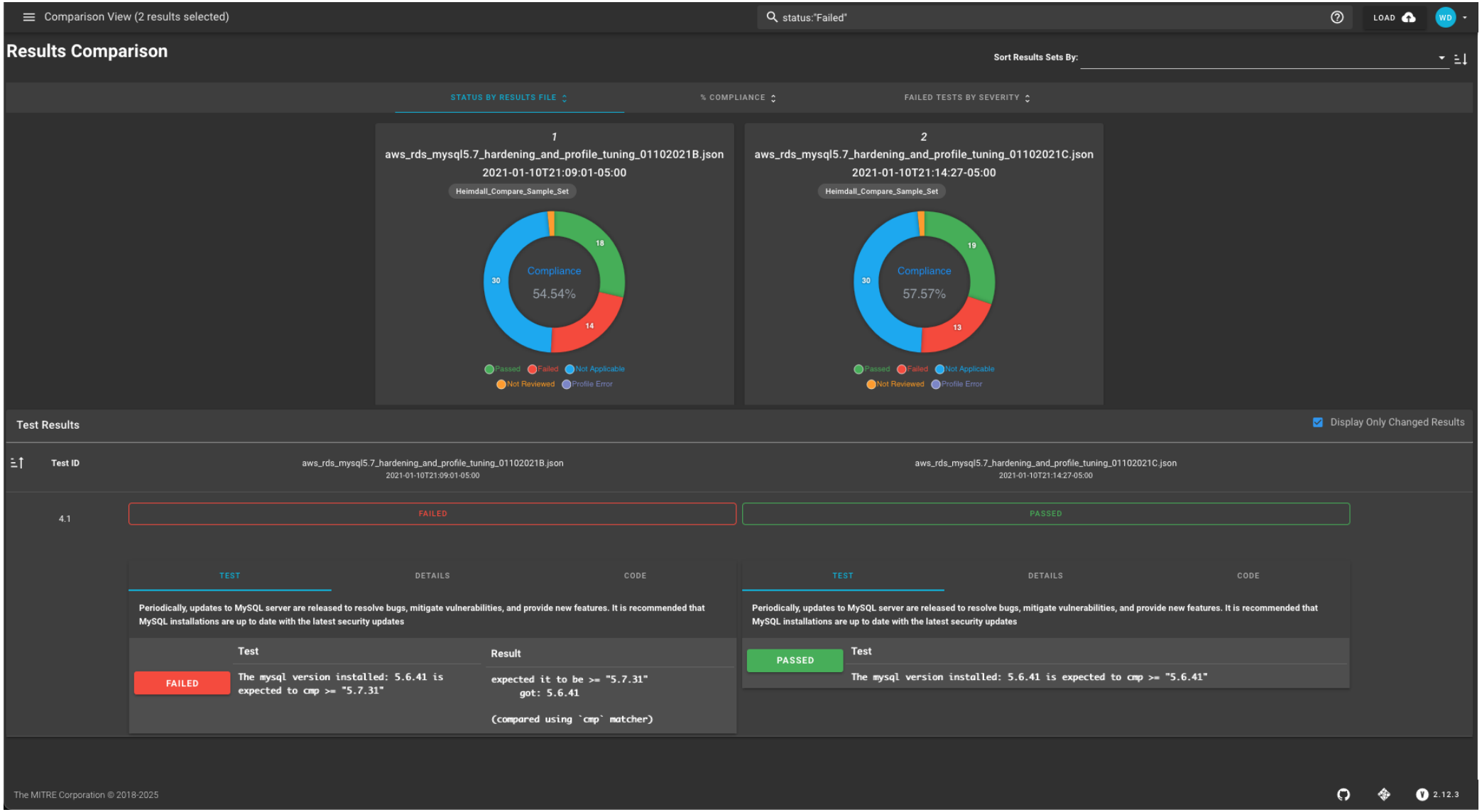
Heimdall – Results View – Deep Dive



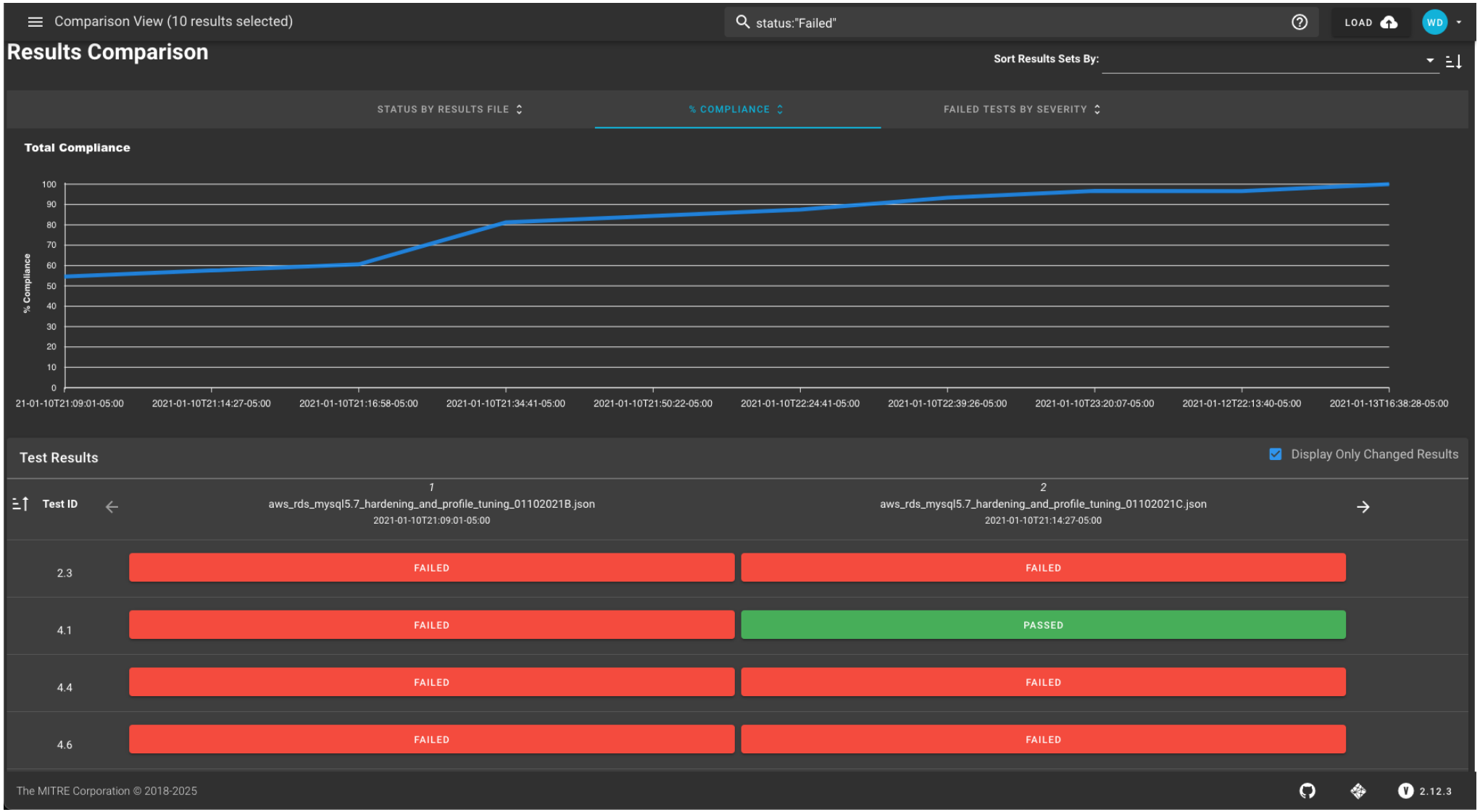
Heimdall – Exports



Heimdall – Comparison View



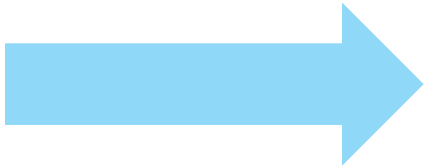
Heimdall – Security Posture Over Time



Develop STIG Ready Content from SRGs with Vulcan

Avoiding repeated manual assessment for programs and capture the value of collaboration

Analysis to determine what guidance is relevant to the system



General Guidance (e.g., SRG)

High-Level Security Requirements, Best Practices, Standards

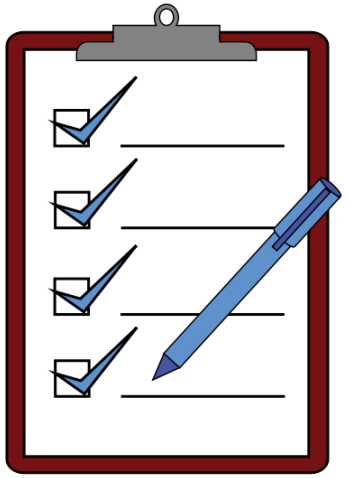
Government and Industry Sources

SRG-aligned STIG Ready Guidance

Specific Instructions for Specific System Components

MITRE

STIG Ready Content

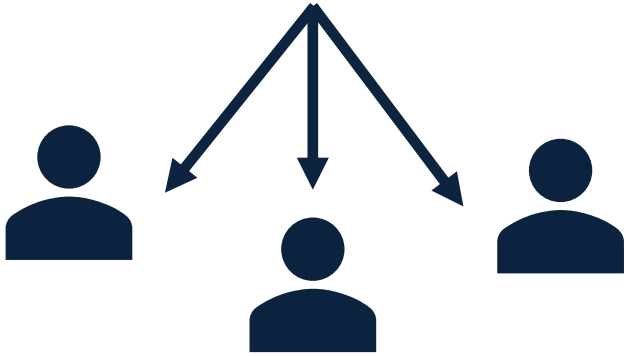


STIG Ready Guidance

DISA Peer Review

Publish!

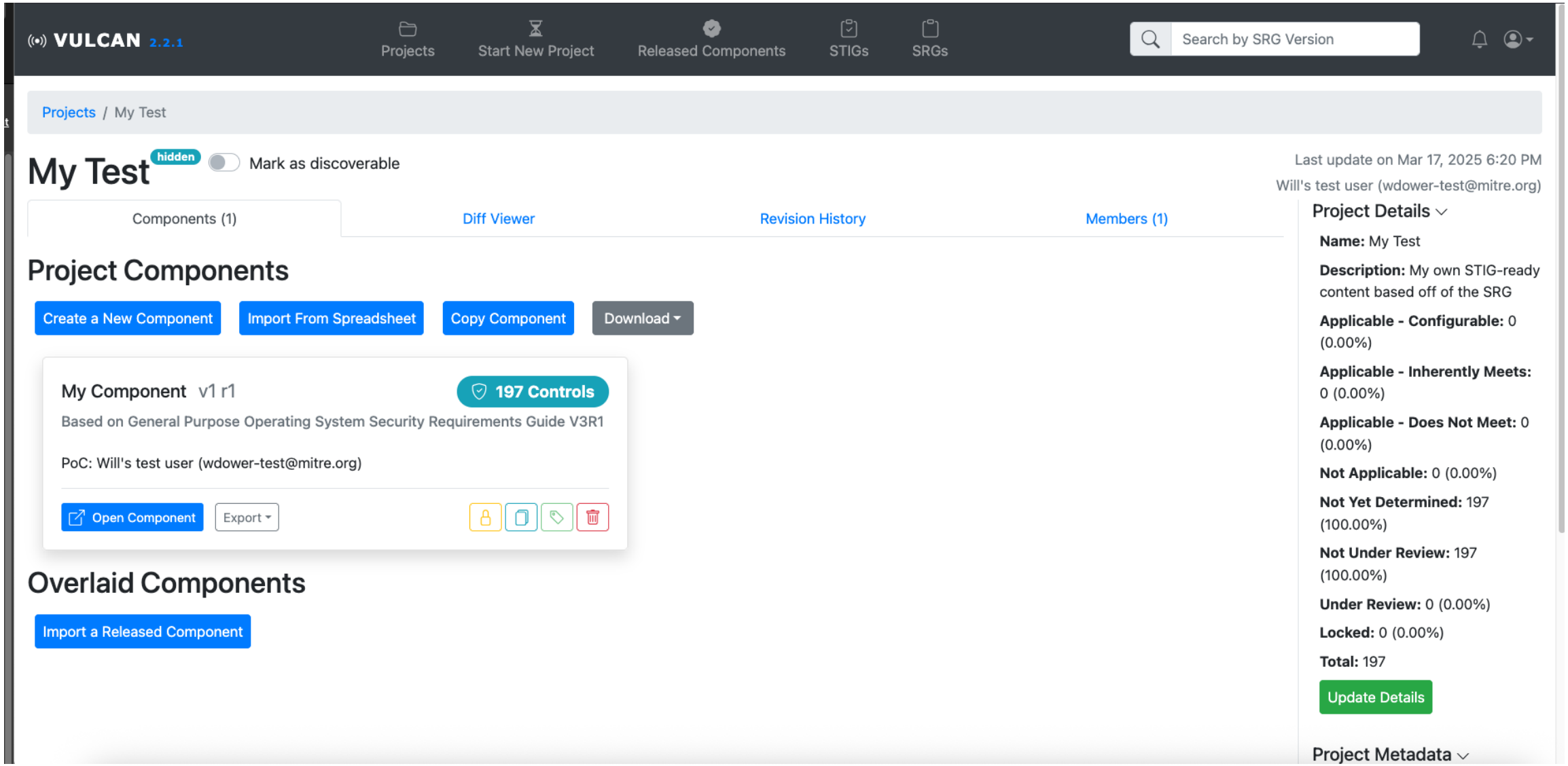
public.cyber.mil/stigs



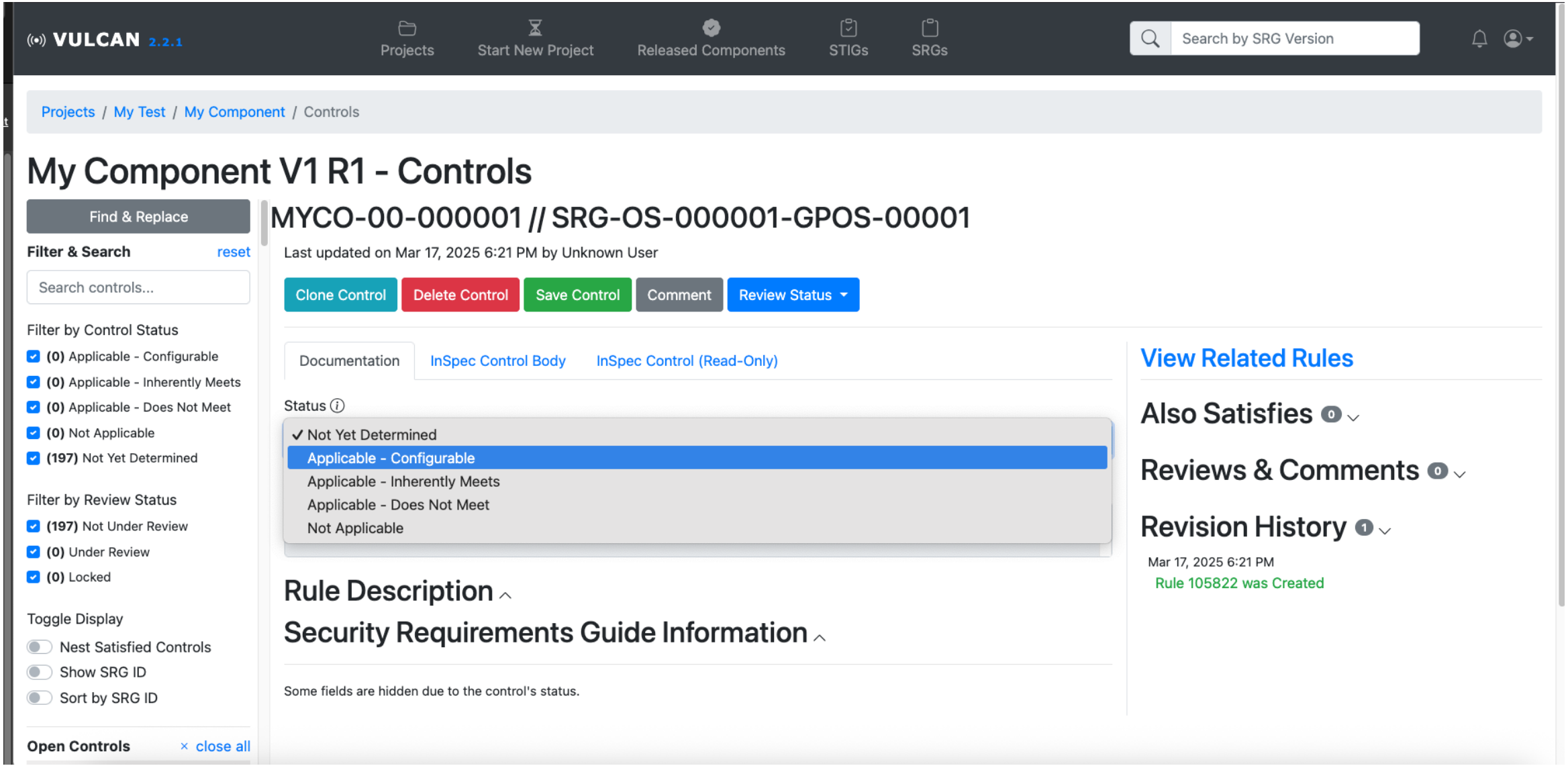
Security Community

MITRE

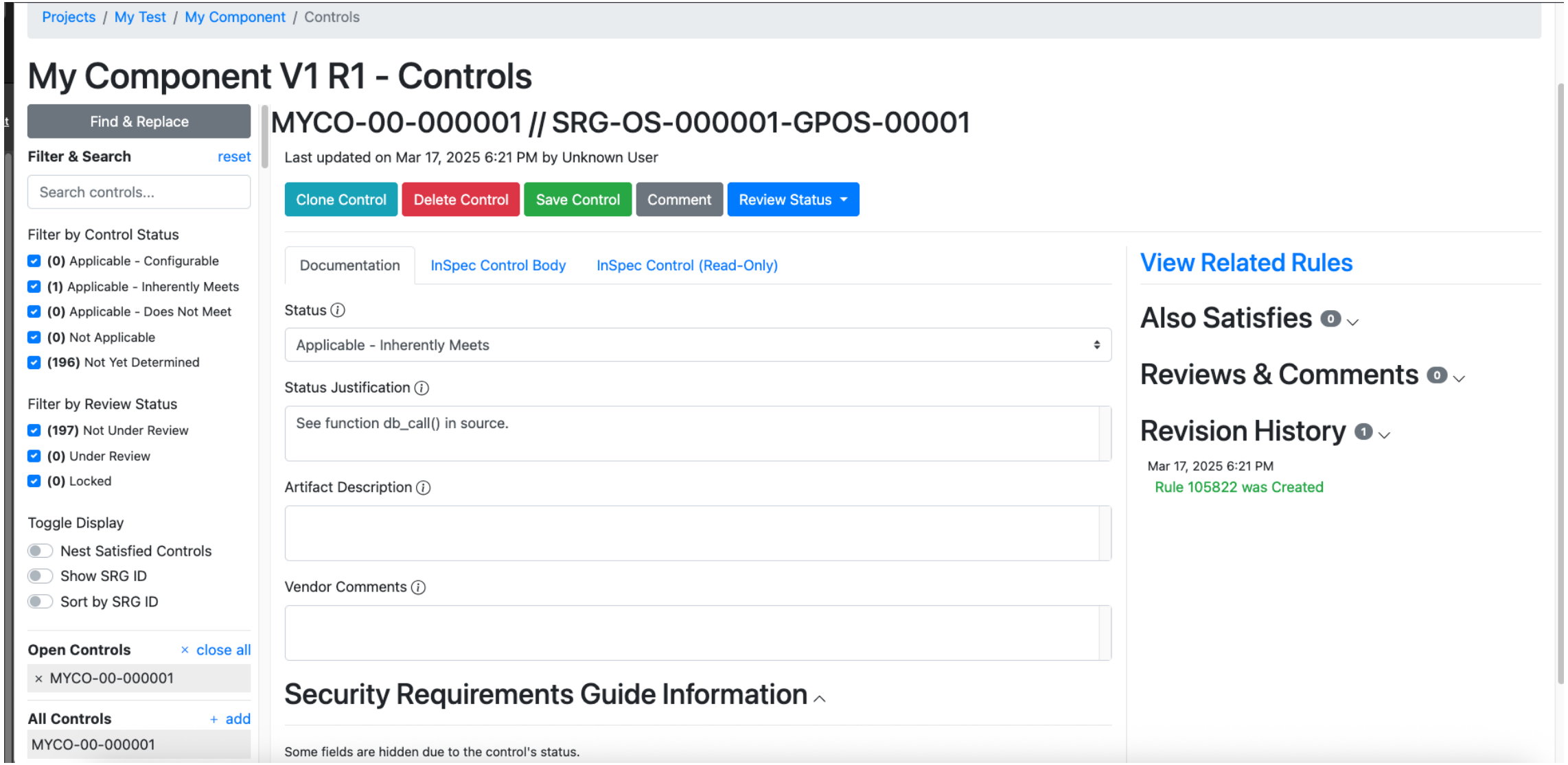
Vulcan



Vulcan - Components



Vulcan - Editing



Vulcan - Automation