The MITRE Security Automation Framework (MITRE SAF)©

Aaron Lippold
Emily Rodriguez
Will Dower

May 2023

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

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

What is the MITRE Security Automation Framework©?

A suite of open-source security automation tools that facilitate the development, collection, and standardization of content for use by government and industry organizations to:

- **Accelerate ATO**
- **Establish Security Requirements**
- **Build Security In**
- **Assess/ Monitor Vulnerabilities**

MITRE SAF© VISION

Implement evolving security requirements while deploying apps at speed

Did You Know?

- ✓ MITRE SAF© is FREE and OPEN-SOURCE (under Apache 2 license)
- ✓ MITRE SAF© OASIS Heimdall Data Format is in the process of becoming an [OASIS international data standard]
- ✓ MITRE SAF© content is used by sponsors, vendors, and contractors, and often written by non-MITRE contributors
- ✓ Creating new content is quick and easy

MITRE SAF© Capabilities

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 throughout the lifecycle of a system via automated tests and manual attestation

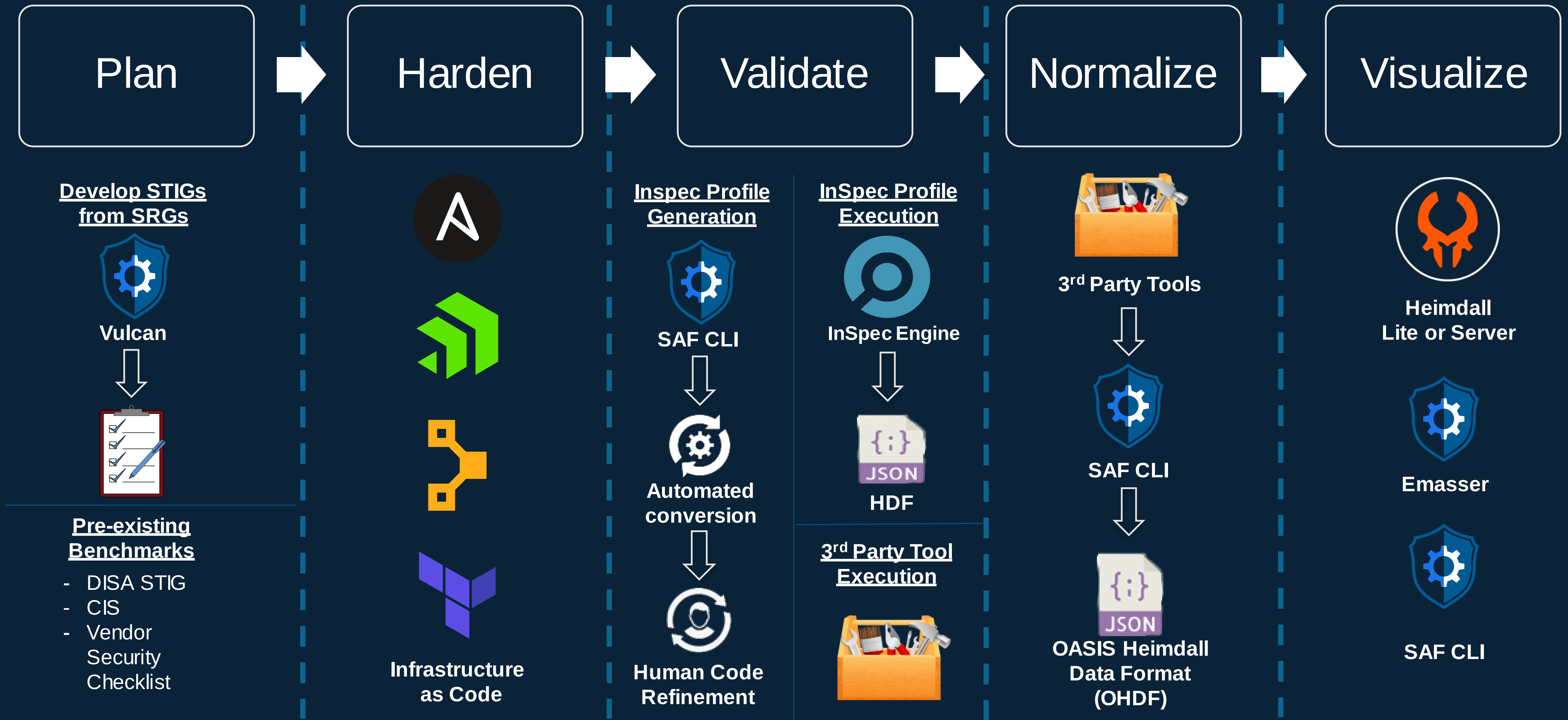
Normalize

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 SAF© Security Validation Lifecycle



Plan → Harden → Validate → Normalize → Visualize

Plan

Develop STIGs from SRGs

Vulcan ⇩

Pre-existing Benchmarks

- DISA STIG
- CIS
- Vendor Security Checklist

Harden

Infrastructure as Code

Validate

Inspec Profile Generation

SAF CLI ⇩ Automated conversion ⇩ Human Code Refinement

InSpec Profile Execution

InSpec Engine ⇩ HDF

3rd Party Tool Execution

Normalize

3rd Party Tools ⇩ SAF CLI ⇩ OASIS Heimdall Data Format (OHDF)

Visualize

Heimdall Lite or Server

Emasser

SAF CLI

MITRE SAF© Capabilities

Plan

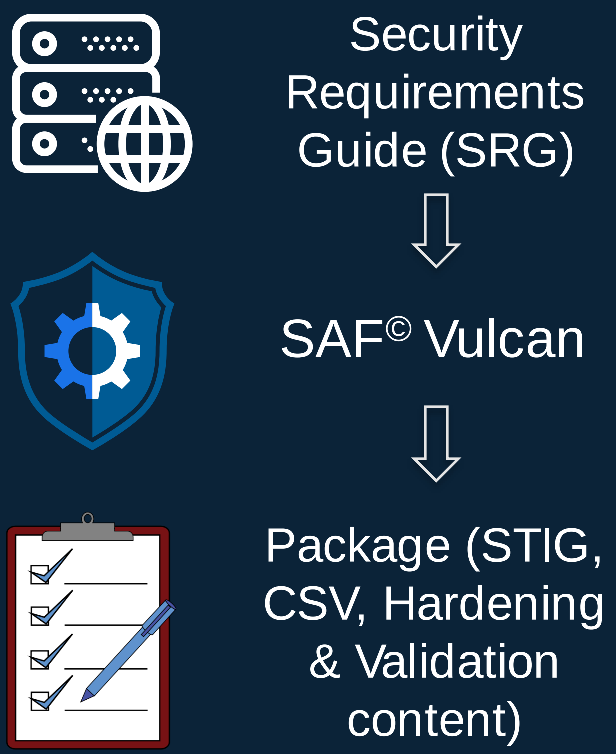
Harden

Validate

Normalize

Visualize

MITRE SAF©: PLAN



Security Requirements Guide (SRG)

⇩

SAF© Vulcan

⇩

Package (STIG, CSV, Hardening & Validation content)

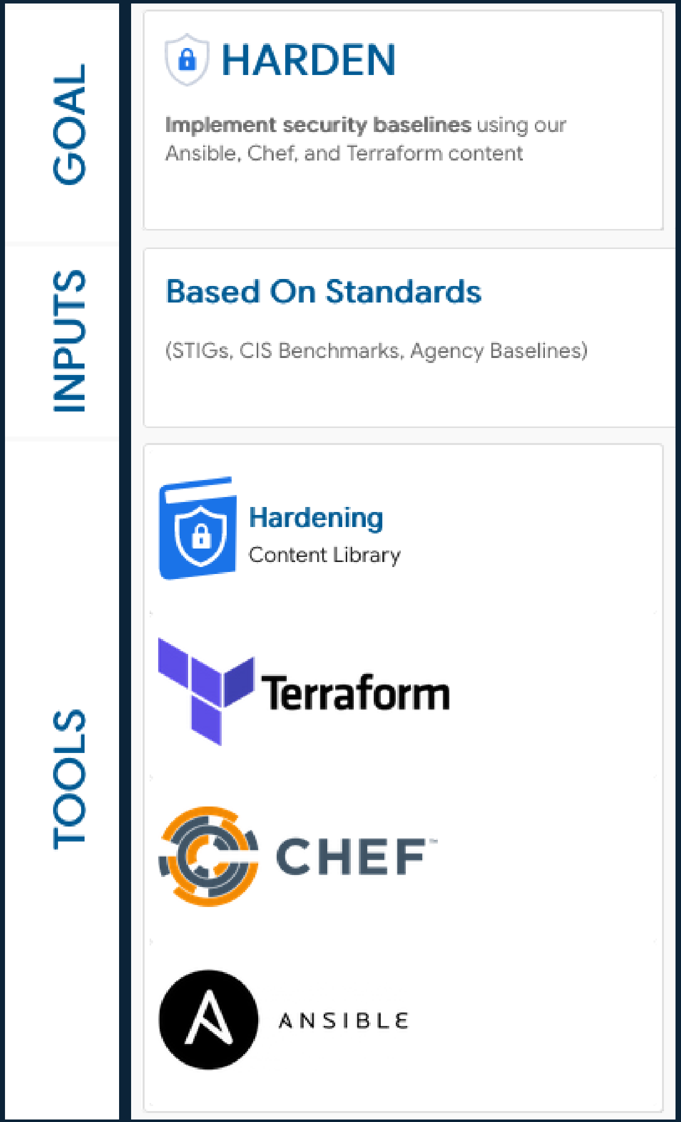
Use MITRE SAF© VULCAN to:

- ✓ Develop STIG-ready content aligned to SRGs
- ✓ Speed STIG development via collaboration, reuse, revision across many programs and stakeholder experiences
- ✓ Speed team creation of automated hardening and validation code

MITRE SAF© Capabilities

- Plan
- Harden
- Validate
- Normalize
- Visualize

MITRE SAF©: HARDEN



GOAL

HARDEN

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

INPUTS

Based On Standards

(STIGs, CIS Benchmarks, Agency Baselines)

TOOLS

Hardening Content Library

Terraform

CHEF

ANSIBLE

Use SAF© Hardening content to:

✓ Automate Configuration Compliance

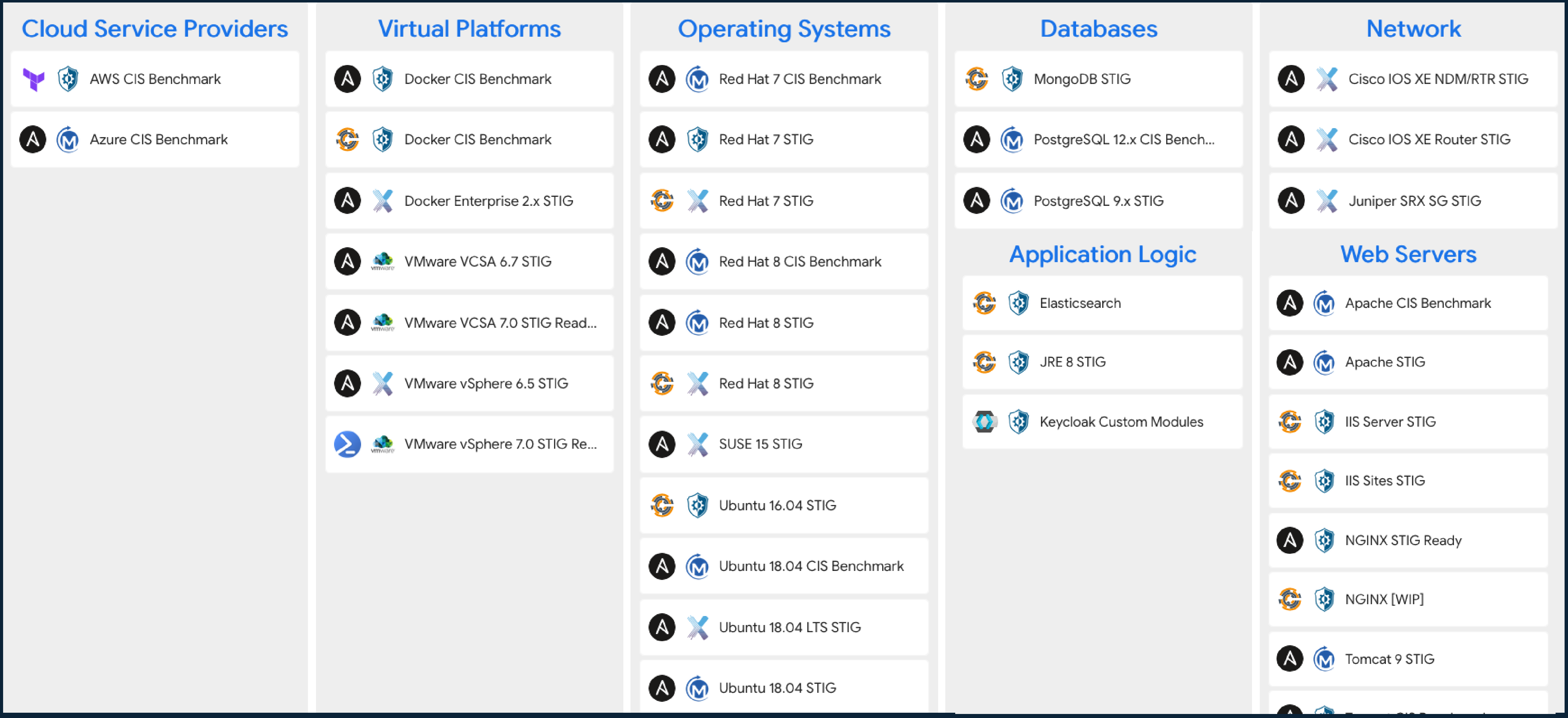
✓ Use standard configuration management tools
  - Terraform, Chef, Ansible, Puppet

✓ Share across security community
  - Open-source content (Apache v2)

✓ Span entire development stack
  - Cloud infrastructure, platform, & OS
  - Database, webserver, & application

Hardening Library

https://saf.mitre.org/#/harden



Cloud Service Providers

- AWS CIS Benchmark
- Azure CIS Benchmark

Virtual Platforms

- Docker CIS Benchmark
- Docker CIS Benchmark
- Docker Enterprise 2.x STIG
- VMware VCSA 6.7 STIG
- VMware VCSA 7.0 STIG Read...
- VMware vSphere 6.5 STIG
- VMware vSphere 7.0 STIG Re...

Operating Systems

- Red Hat 7 CIS Benchmark
- Red Hat 7 STIG
- Red Hat 7 STIG
- Red Hat 8 CIS Benchmark
- Red Hat 8 STIG
- Red Hat 8 STIG
- SUSE 15 STIG
- Ubuntu 16.04 STIG
- Ubuntu 18.04 CIS Benchmark
- Ubuntu 18.04 LTS STIG
- Ubuntu 18.04 STIG

...

Databases

- MongoDB STIG
- PostgreSQL 12.x CIS Bench...
- PostgreSQL 9.x STIG

Application Logic

- Elasticsearch
- JRE 8 STIG
- Keycloak Custom Modules

Network

- Cisco IOS XE NDM/RTR STIG
- Cisco IOS XE Router STIG
- Juniper SRX SG STIG

Web Servers

- Apache CIS Benchmark
- Apache STIG
- IIS Server STIG
- IIS Sites STIG
- NGINX STIG Ready
- NGINX [WIP]
- Tomcat 9 STIG

...

MITRE

MITRE SAF© Capabilities

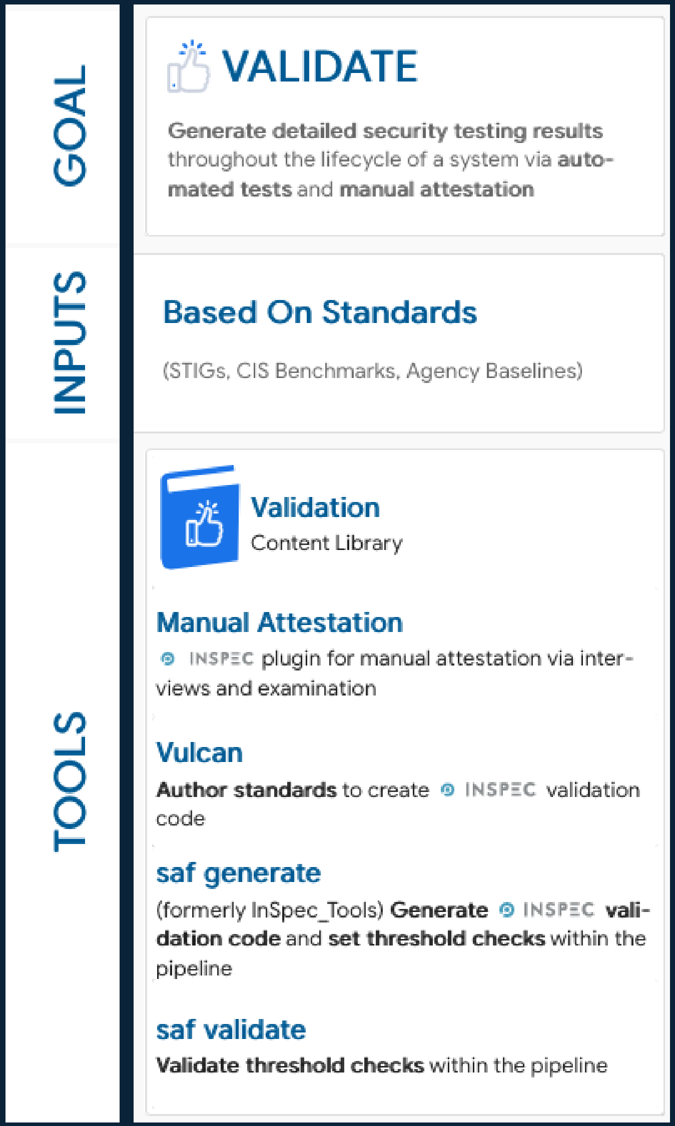
Plan

Harden

Validate

Normalize

Visualize



GOAL

VALIDATE

Generate detailed security testing results throughout the lifecycle of a system via **automated tests** and **manual attestation**

INPUTS

Based On Standards

(STIGs, CIS Benchmarks, Agency Baselines)

TOOLS

Validation
Content Library

Manual Attestation
INSPEC plugin for manual attestation via interviews and examination

Vulcan
Author standards to create INSPEC validation code

saf generate
(formerly InSpec_Tools) **Generate** INSPEC **validation code** and **set threshold checks** within the pipeline

saf validate
Validate threshold checks within the pipeline

MITRE SAF©: VALIDATE

Use SAF© Validation content to:

✓ Confirm configuration compliance
- Automatically run at every build

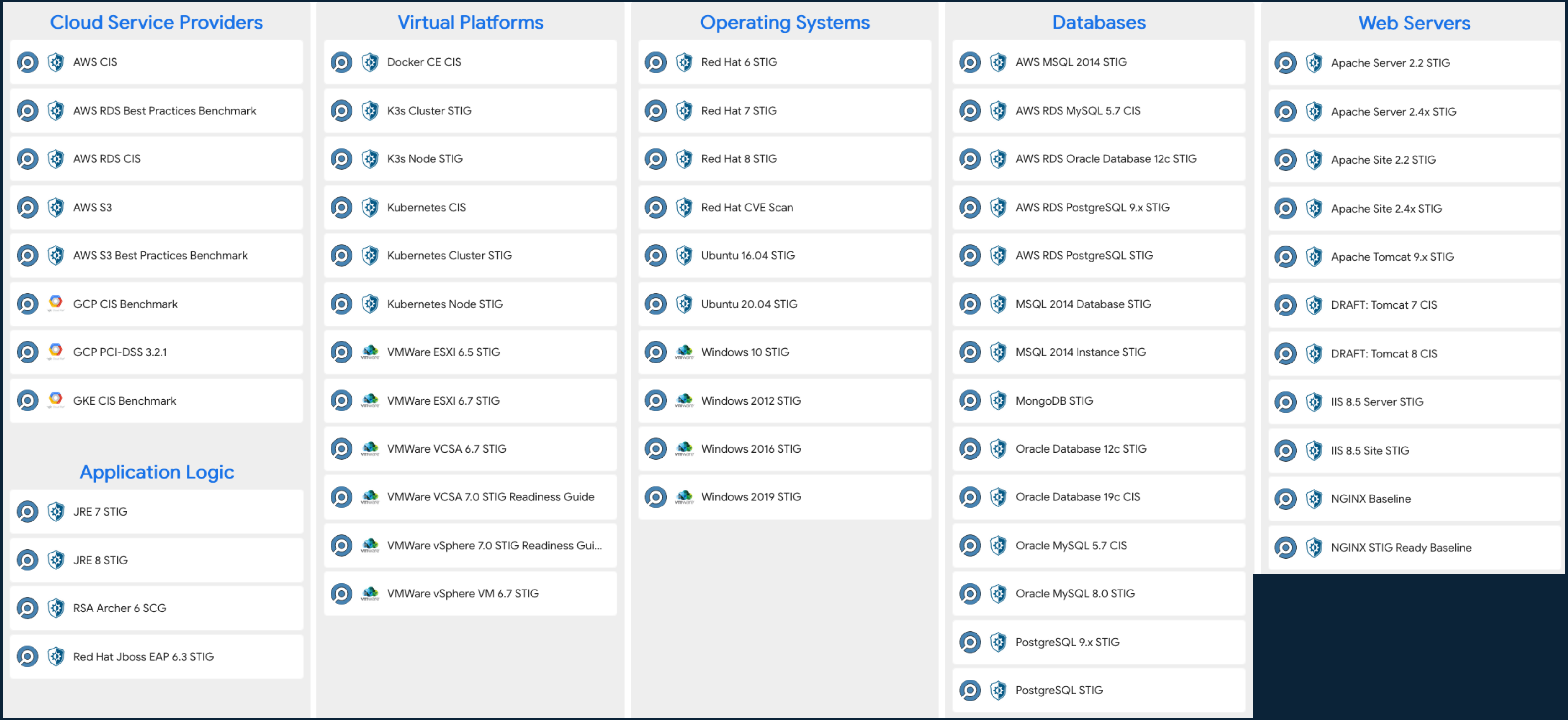
✓ Share across security community
- Open-source, under Apache 2 license

✓ Span entire development stack
- Cloud infrastructure, platform, & OS
- Database, webserver, & application

✓ Incorporate manual attestation
- 100% coverage of interview, examine, or policy requirements

Validation Library

https://saf.mitre.org/#/validate



Cloud Service Providers

- AWS CIS
- AWS RDS Best Practices Benchmark
- AWS RDS CIS
- AWS S3
- AWS S3 Best Practices Benchmark
- GCP CIS Benchmark
- GCP PCI-DSS 3.2.1
- GKE CIS Benchmark

Application Logic

- JRE 7 STIG
- JRE 8 STIG
- RSA Archer 6 SCG
- Red Hat Jboss EAP 6.3 STIG

Virtual Platforms

- Docker CE CIS
- K3s Cluster STIG
- K3s Node STIG
- Kubernetes CIS
- Kubernetes Cluster STIG
- Kubernetes Node STIG
- VMWare ESXI 6.5 STIG
- VMWare ESXI 6.7 STIG
- VMWare VCSA 6.7 STIG
- VMWare VCSA 7.0 STIG Readiness Guide
- VMWare vSphere 7.0 STIG Readiness Gui...
- VMWare vSphere VM 6.7 STIG

Operating Systems

- Red Hat 6 STIG
- Red Hat 7 STIG
- Red Hat 8 STIG
- Red Hat CVE Scan
- Ubuntu 16.04 STIG
- Ubuntu 20.04 STIG
- Windows 10 STIG
- Windows 2012 STIG
- Windows 2016 STIG
- Windows 2019 STIG

Databases

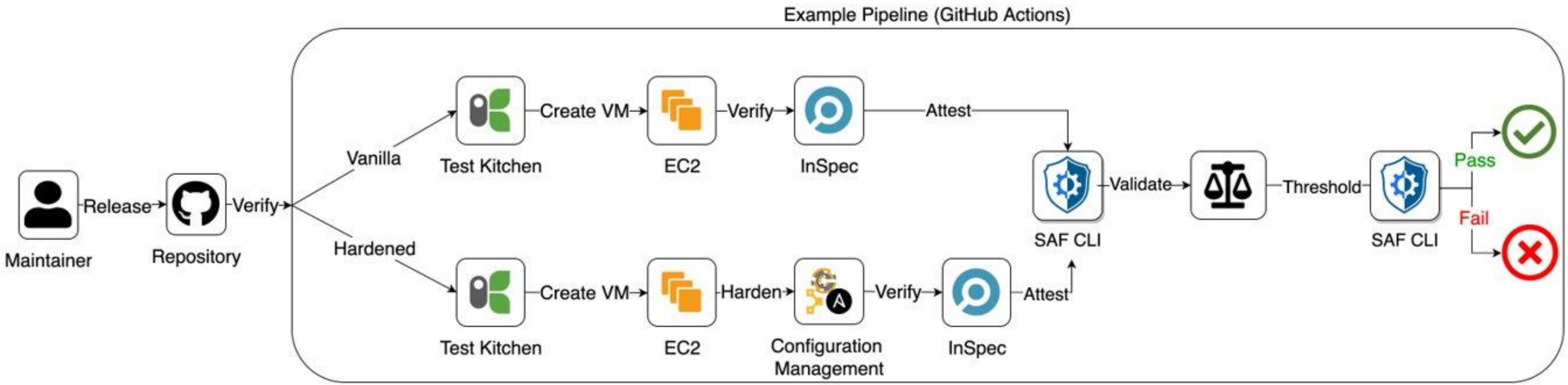
- AWS MSQL 2014 STIG
- AWS RDS MySQL 5.7 CIS
- AWS RDS Oracle Database 12c STIG
- AWS RDS PostgreSQL 9.x STIG
- AWS RDS PostgreSQL STIG
- MSQL 2014 Database STIG
- MSQL 2014 Instance STIG
- MongoDB STIG
- Oracle Database 12c STIG
- Oracle Database 19c CIS
- Oracle MySQL 5.7 CIS
- Oracle MySQL 8.0 STIG
- PostgreSQL 9.x STIG
- PostgreSQL STIG

Web Servers

- Apache Server 2.2 STIG
- Apache Server 2.4x STIG
- Apache Site 2.2 STIG
- Apache Site 2.4x STIG
- Apache Tomcat 9.x STIG
- DRAFT: Tomcat 7 CIS
- DRAFT: Tomcat 8 CIS
- IIS 8.5 Server STIG
- IIS 8.5 Site STIG
- NGINX Baseline
- NGINX STIG Ready Baseline

Automating Hardening and Validation

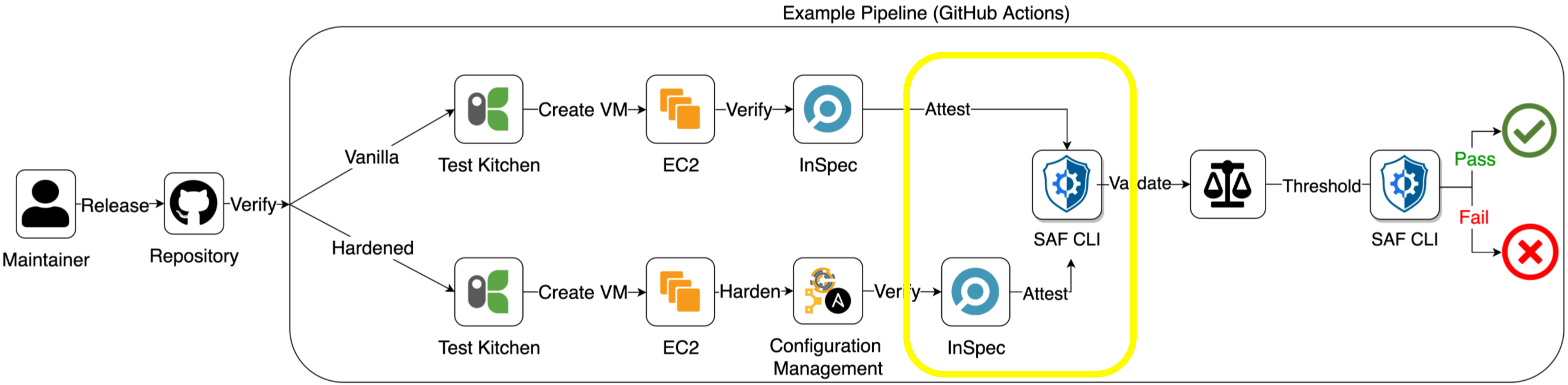
By building security into the software development process, teams prepare in advance to receive approval when seeking an Authorization to Operate



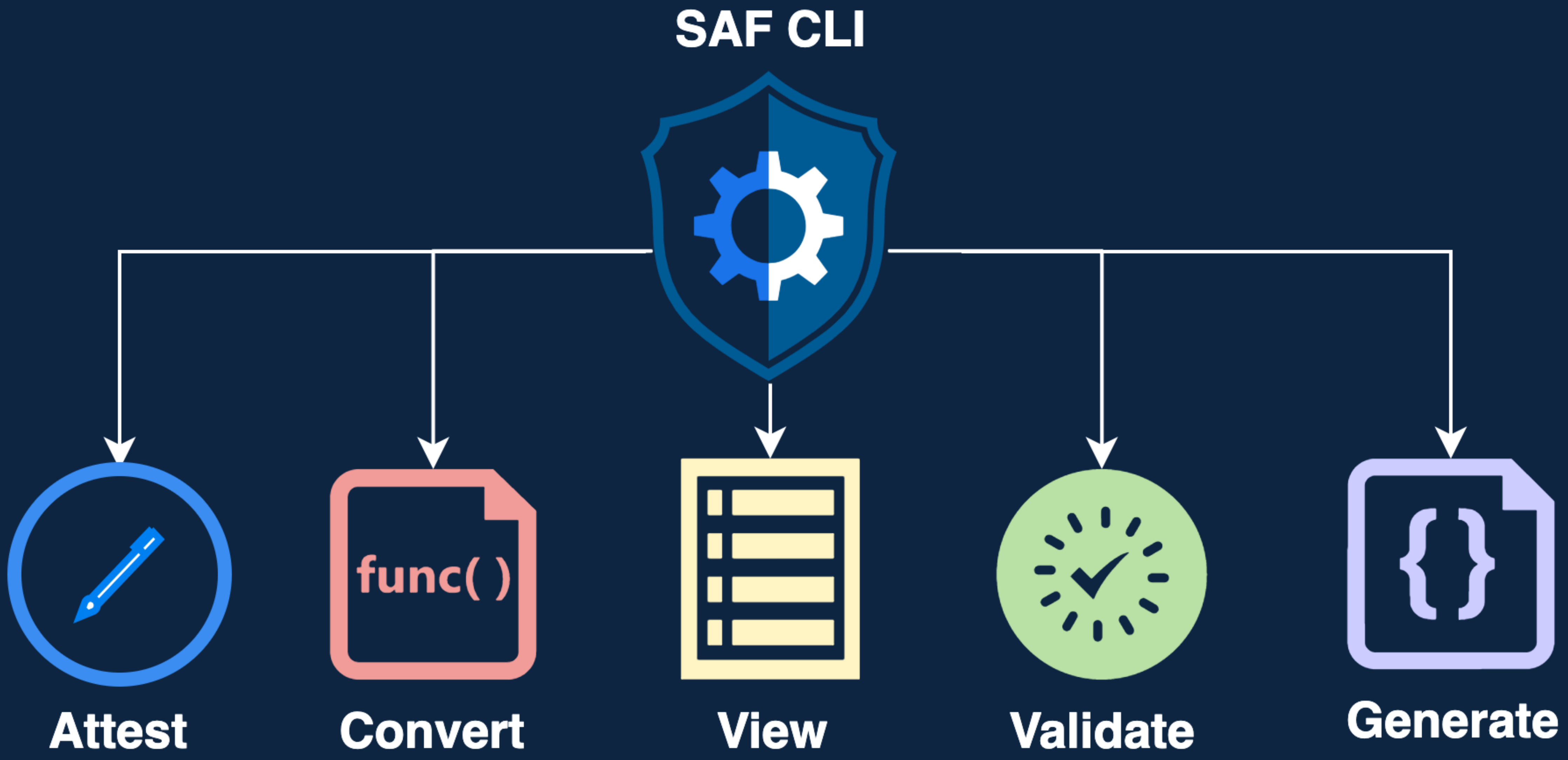
MITRE

Automating Hardening and Validation

By building security into the software development process, teams prepare in advance to receive approval when seeking an Authorization to Operate

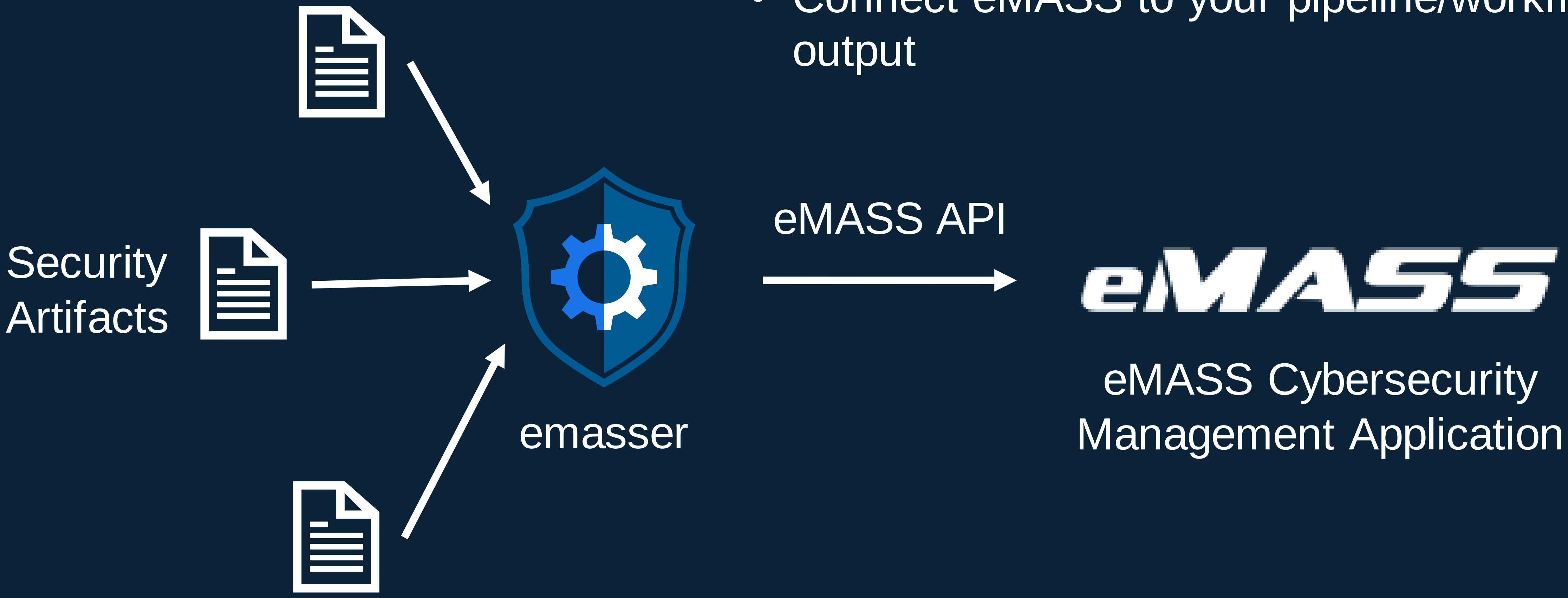


SAF CLI Utility Command Line Tool



SAF CLI – emasser

- One of Army ECMA's first deliverables from the Security Automation team in partnership with DISA eMASS PMO
- Automates interactions with ATO packages
- Connect eMASS to your pipeline/workflow output



Security Artifacts

emasser

eMASS API

eMASS

eMASS Cybersecurity Management Application

MITRE

MITRE SAF© Capabilities

Plan

Harden

Validate

Normalize

Visualize

MITRE SAF©: Normalize

Use SAF © Normalize tools to

- ✓ 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

- OHDF Converters
- SAF© CLI (command line interface)
- SAF© GitHub Actions
- Heimdall Lite
- Heimdall Server

Supported Risk Information Sources

- AWS Security Hub
- Splunk
- AWS Config
- Snyk
- Trivy
- Tenable Nessus
- DBProtect
- CSV / XLSX
- Netsparker
- Burp Suite
- GoSec
- Ion Channel
- Prisma
- SonarQube
- OWASP ZAP
- Prowler
- Fortify
- JFrog Xray
- Nikto
- Sarif
- Scoutsuite
- Twistlock
- DISA Checklist
- DISA XCCDF Results

MITRE SAF© Capabilities

Plan

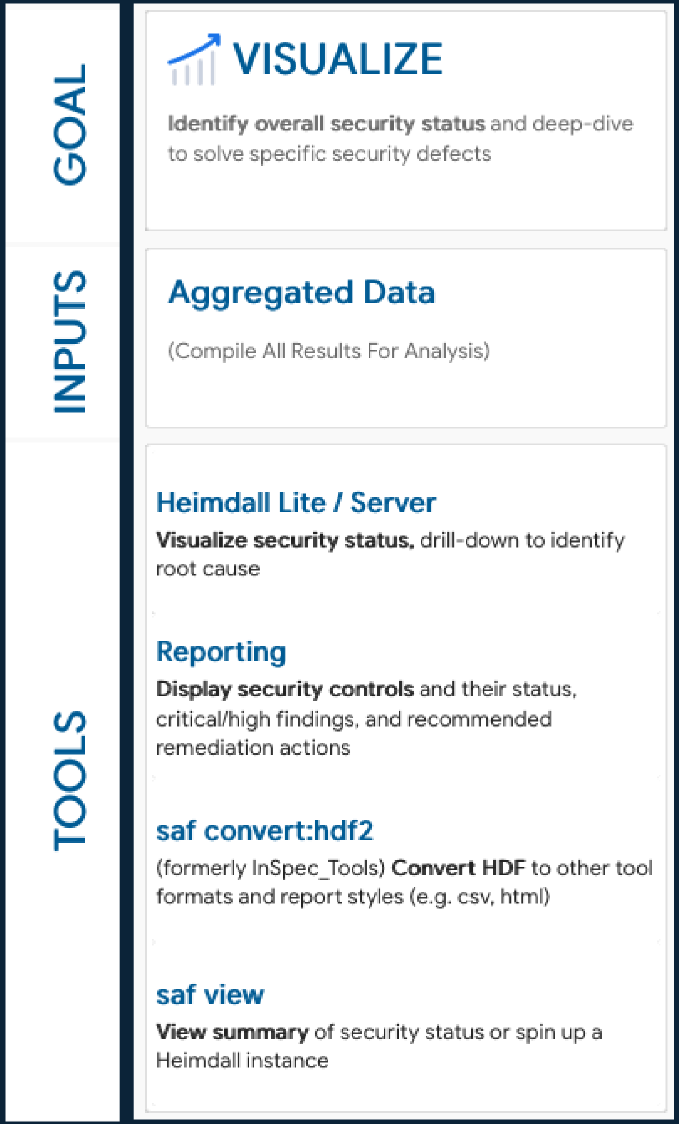
Harden

Validate

Normalize

Visualize

MITRE SAF©: VISUALIZE



GOAL

VISUALIZE

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

INPUTS

Aggregated Data

(Compile All Results For Analysis)

TOOLS

Heimdall Lite / Server

Visualize security status, drill-down to identify root cause

Reporting

Display security controls and their status, critical/high findings, and recommended remediation actions

saf convert:hdf2

(formerly InSpec_Tools) **Convert HDF** to other tool formats and report styles (e.g. csv, html)

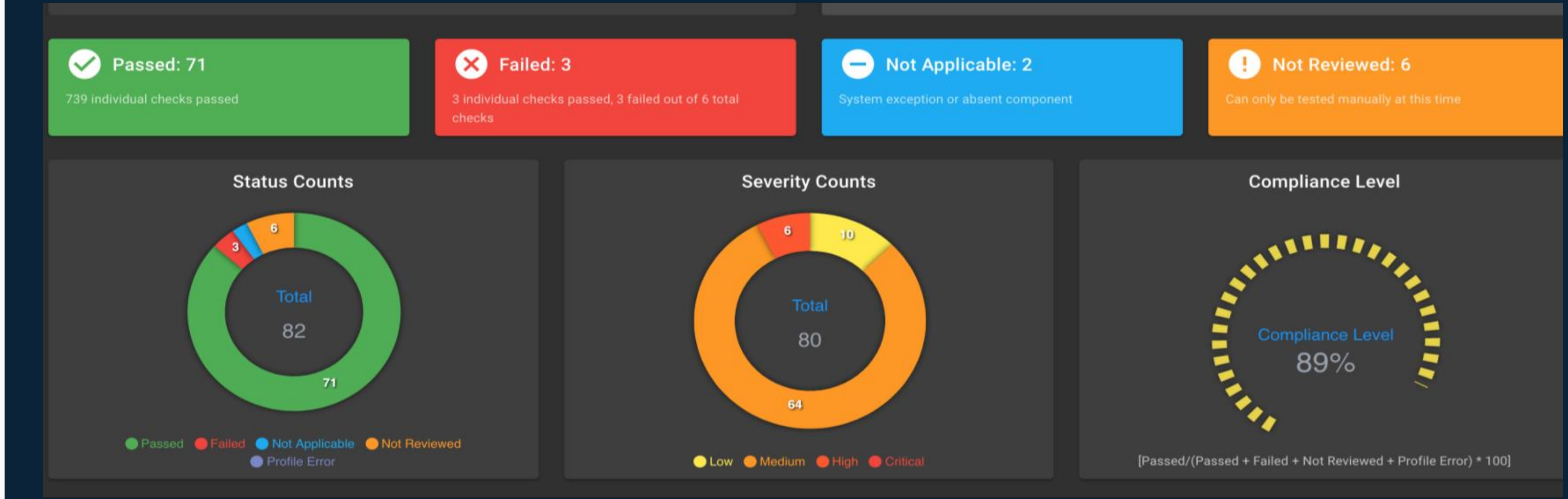
saf view

View summary of security status or spin up a Heimdall instance

Use SAF Heimdall Lite / Heimdall Server to:

✓ Aggregate test results into rollups, charts, and timelines

✓ Deep dive to make decisions on how best to reduce risk



Passed: 71

739 individual checks passed

Failed: 3

3 individual checks passed, 3 failed out of 6 total checks

Not Applicable: 2

System exception or absent component

Not Reviewed: 6

Can only be tested manually at this time

[Passed/(Passed + Failed + Not Reviewed + Profile Error) * 100]

A Look at MITRE Heimdall

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/

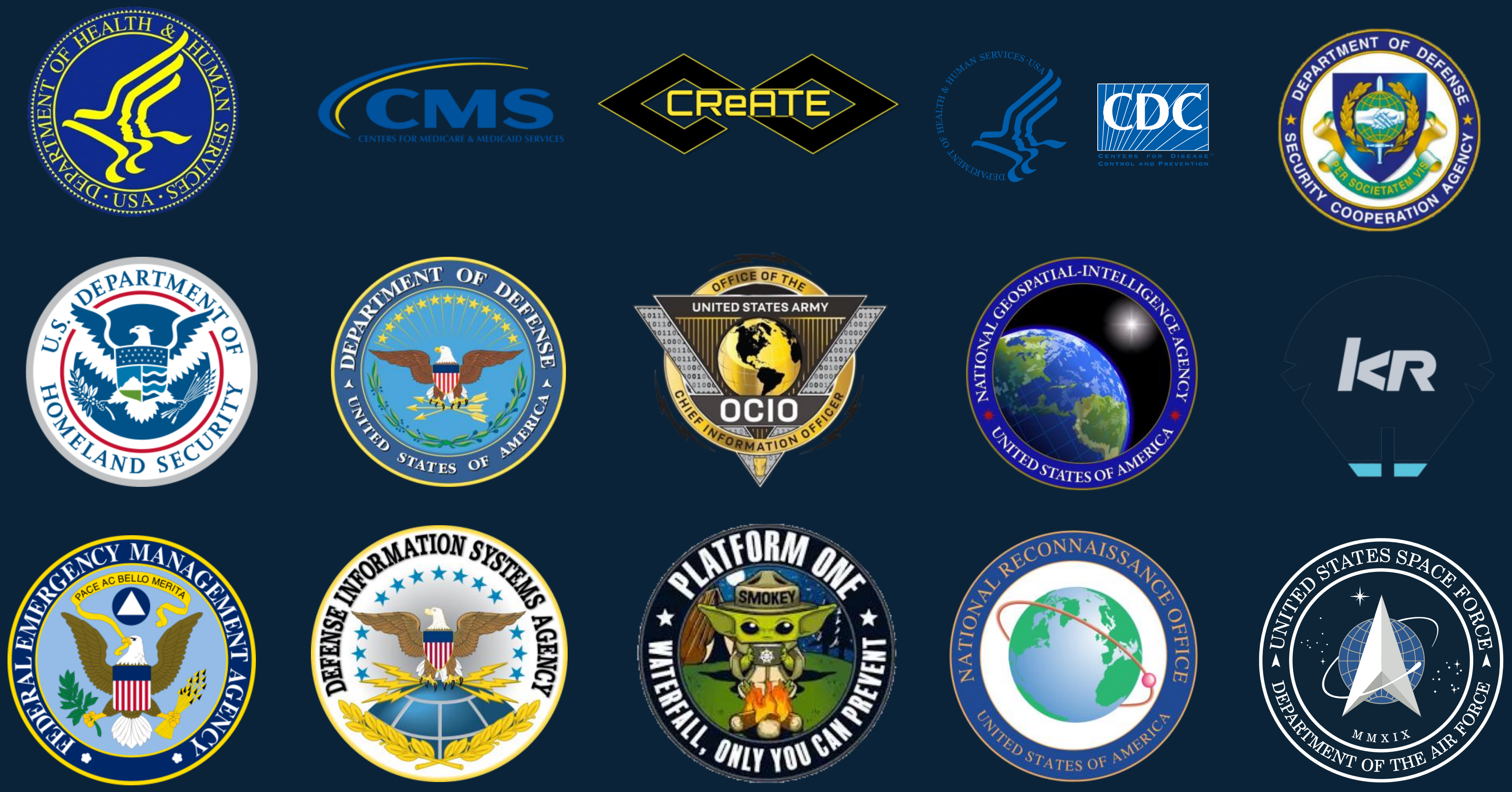
Security Automation Framework©

https://saf.mitre.org

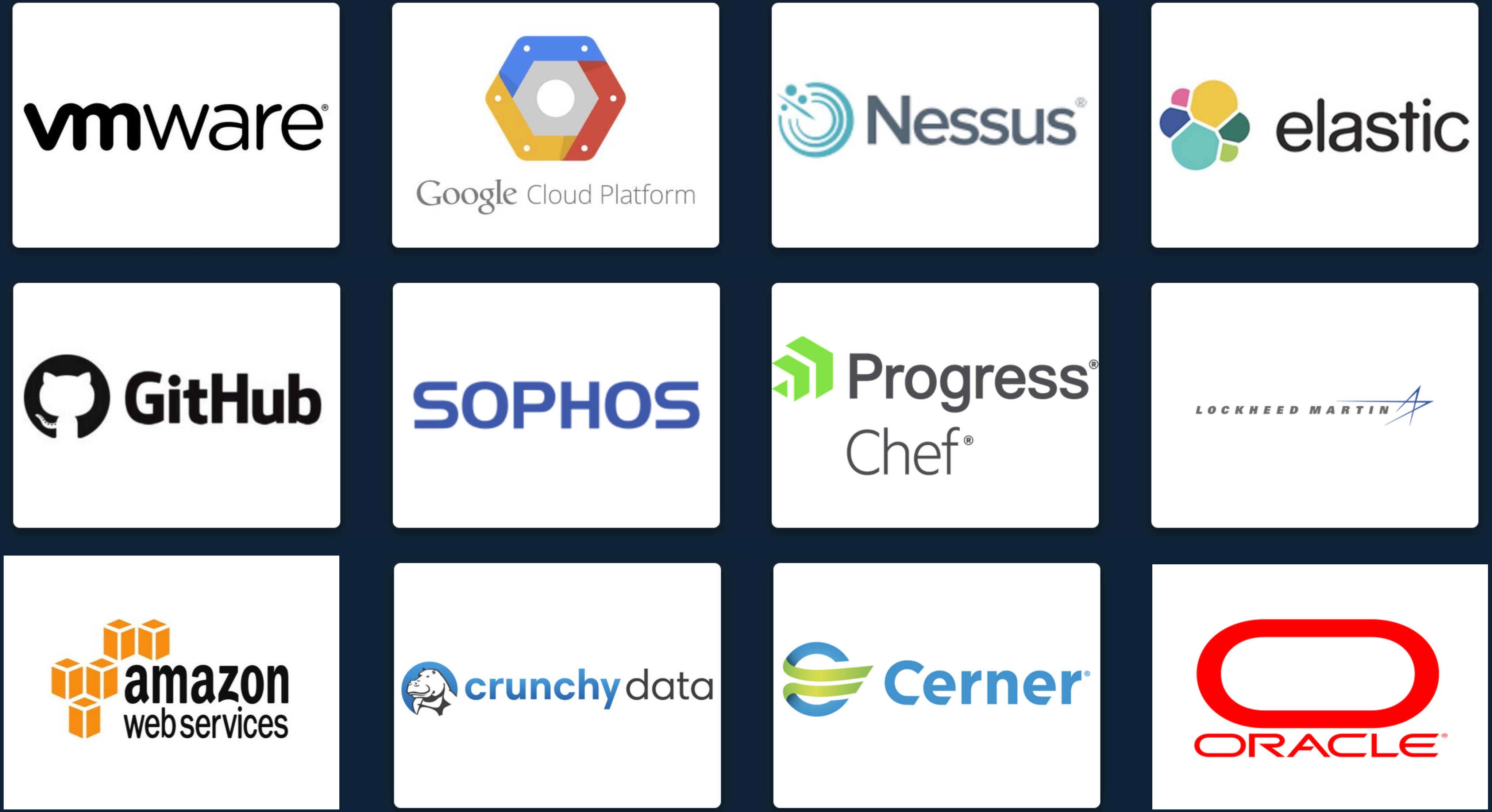
saf@groups.mitre.org

Backup

Select Security Automation Framework Sponsors


DEPARTMENT OF HEALTH & HUMAN SERVICES · USA ·
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CReATE
DEPARTMENT OF HEALTH & HUMAN SERVICES-USA
CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION
DEPARTMENT OF DEFENSE
SECURITY COOPERATION AGENCY
PER SOCIETATEM VIS
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
OFFICE OF THE
UNITED STATES ARMY
OCIO
CHIEF INFORMATION OFFICER
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
UNITED STATES OF AMERICA
KR
FEDERAL EMERGENCY MANAGEMENT AGENCY
PACE AC BELLO MERITA
DEFENSE INFORMATION SYSTEMS AGENCY
PLATFORM ONE
SMOKEY
WATERFALL, ONLY YOU CAN PREVENT
NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA
UNITED STATES SPACE FORCE
MMXIX
DEPARTMENT OF THE AIR FORCE

Additional MITRE SAF© Vendor Partners



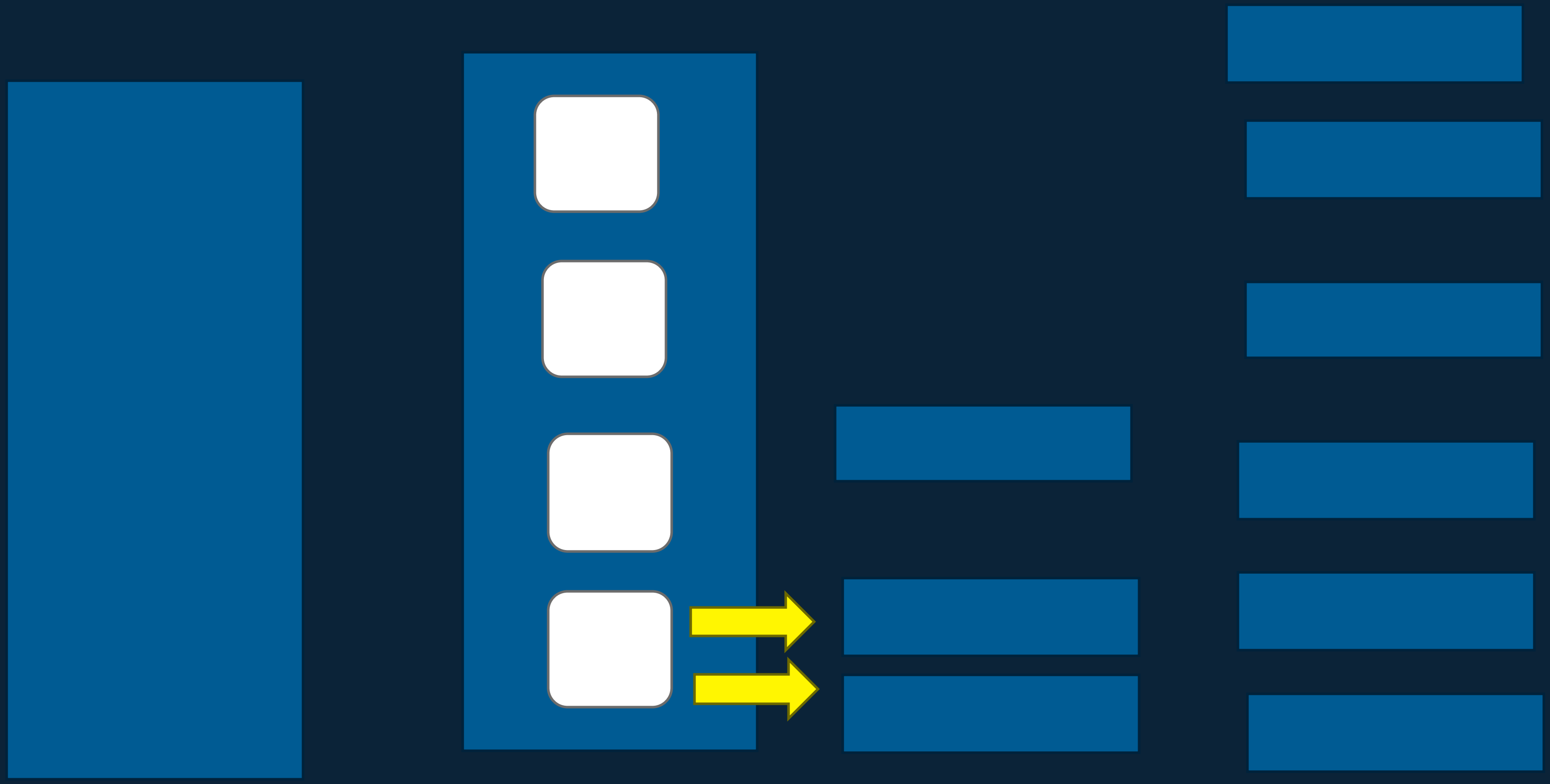
SAF© Sponsor Success Stories – DoD

Organization	SAF Implementation
Army ECMA, cArmy	Integrated the SAF© into their platform services and customer-facing pipelines
Army G2/C2S	Piloted security validation of high-side AWS environments for use by the Department
Space Force	Utilized the SAF© Emasser© client and API to create dashboards of their security packages
Air Force MXS	Integrated the SAF© into IL-2 and IL-5 GovCloud Kubernetes deployment to perform automatic security scans
AF Platform One	Provided hardened and accredited container images of SAF© tooling via IronBank for use by Platform One users
AF Kessel Run	Utilized the SAF© automated scanning and Checklist generation to obtain their initial ATO
DSCA	Piloting a proof-of-concept to determine the extent to which the SAF© will be implemented across the Cyber Security Program
DCSA	Streamlining accreditation processes across DCSA emerging and production services in container and cloud environments
DHA	Utilized the SAF© to pilot and demonstrate a streamlined accreditation process for medical devices receiving an ATO for multiple components over a 6-month period
NGA	Utilized the SAF© toolchain and personnel to achieve their ATO-in-a-day project, a founding sponsor of the SAF
NRO	Automated and streamlined validation of JWICS cloud environments and systems
DISA CTO	Supported the initial development of SAF© Vulcan©: a proof-of-concept for streamlining security guidance development
DISA C2SF	Used InSpec scanning and the SAF© CLI to ensure Software Factory cloud infrastructure images passed STIG-aligned security thresholds
DISA CCM	Researched techniques for containerized components, implemented results as container-aware InSpec profiles
OSD T&E	Provided exemplar DevSecOps SME content for the Department-wide Cybersecurity Test & Evaluation Guidebook

Sponsor Success Stories – Federal Government

Organization	SAF Implementation
CMS/HHS	Full adoption of the SAF (saf.cms.gov), tailored profiles to meet organizational requirements
CDC/HHS	Utilized the SAF to help formulate their approach and execution of DevSecOps and utilized the SAF toolchain as a reference implementation for their team
DHS	Piloted and demonstrated the SAF capabilities for validation of AWS resources in GovCloud
FEMA/DHS	Utilized the SAF to streamline AWS AMI gold discs for RedHat and Windows

It has already been written



SAF CLI – Delta

https://saf-cli.mitre.org/

InSpec Delta

Security Benchmarks are always changing – How do you keep things current?

Delta allows you to easily and efficiently keep your profiles up to date by using the standard publications of common benchmarks to update and merge the latest guidance into your profiles!

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

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

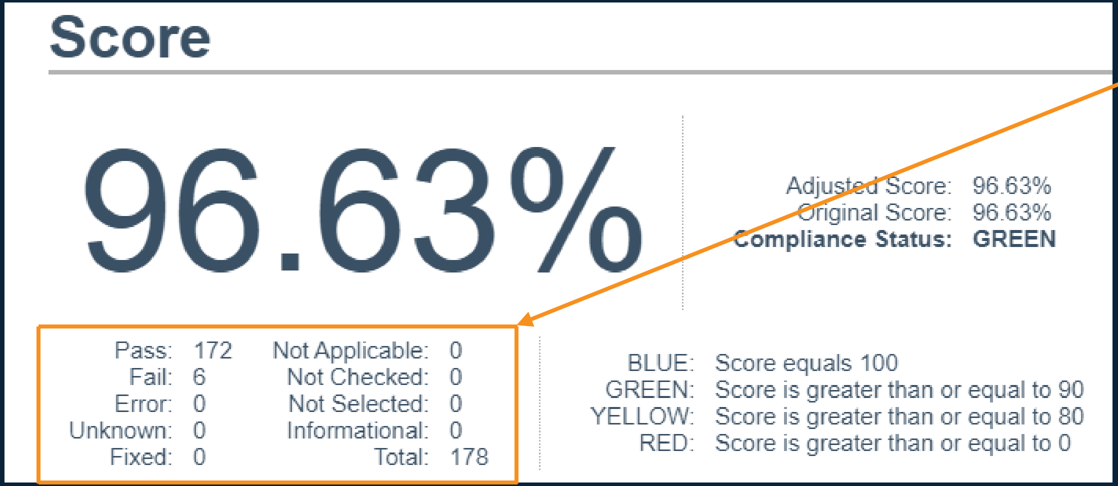
SAF’s part of the process

- 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

Example: SCAP vs. InSpec Output Comparison

RedHat 7 Operating System Scans

SCAP (SCC)



Score

96.63%

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

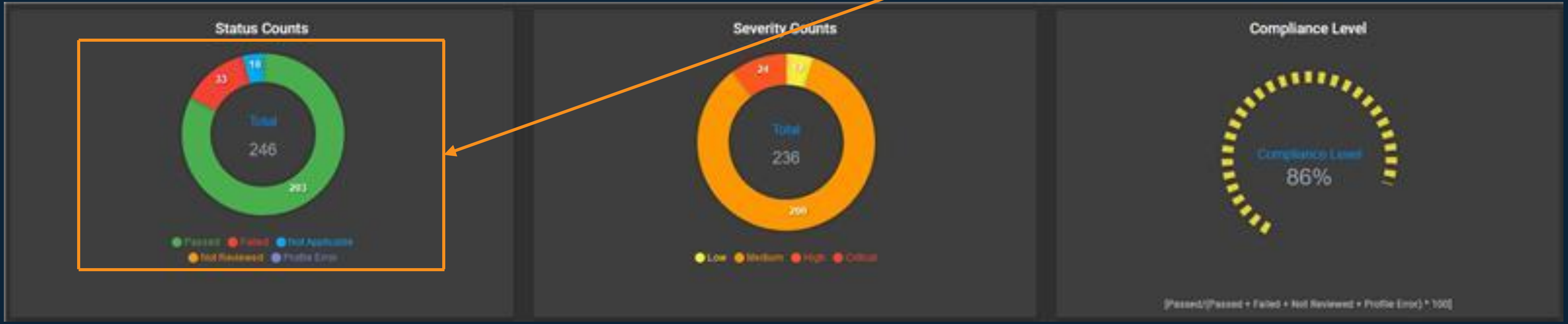
Pass:	172	Not Applicable:	0
Fail:	6	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	178

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

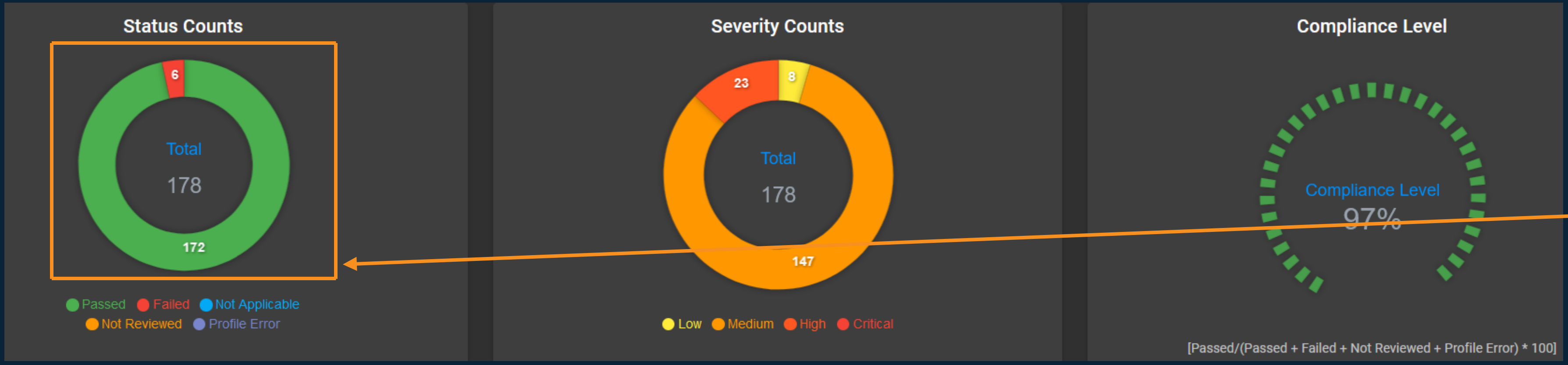


MITRE

Example: SCAP vs. InSpec Output Comparison Heimdall

RedHat 7 Operating System Scans

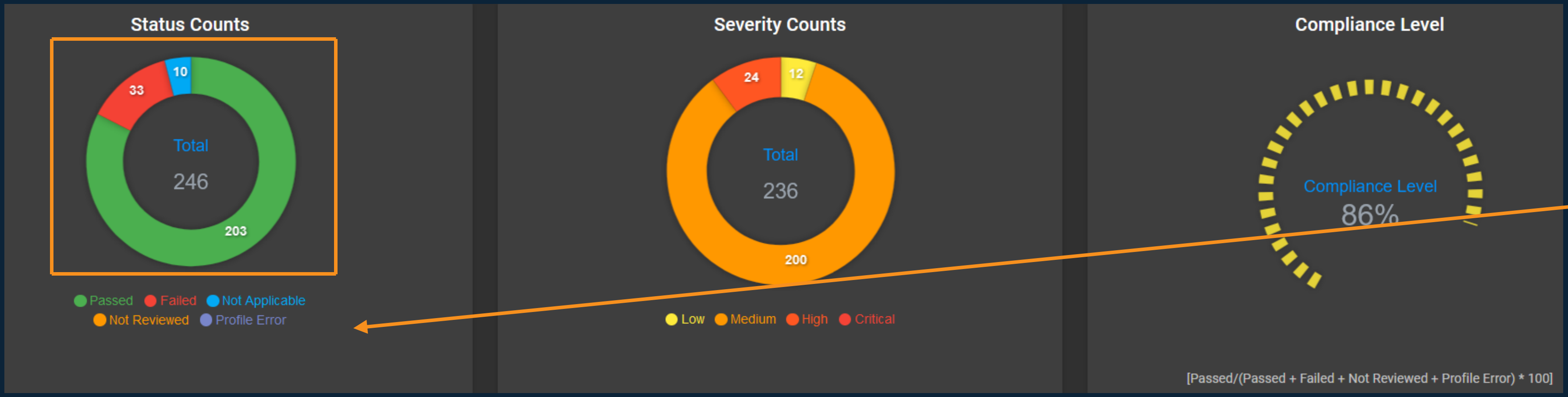
SCAP (SCC)



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

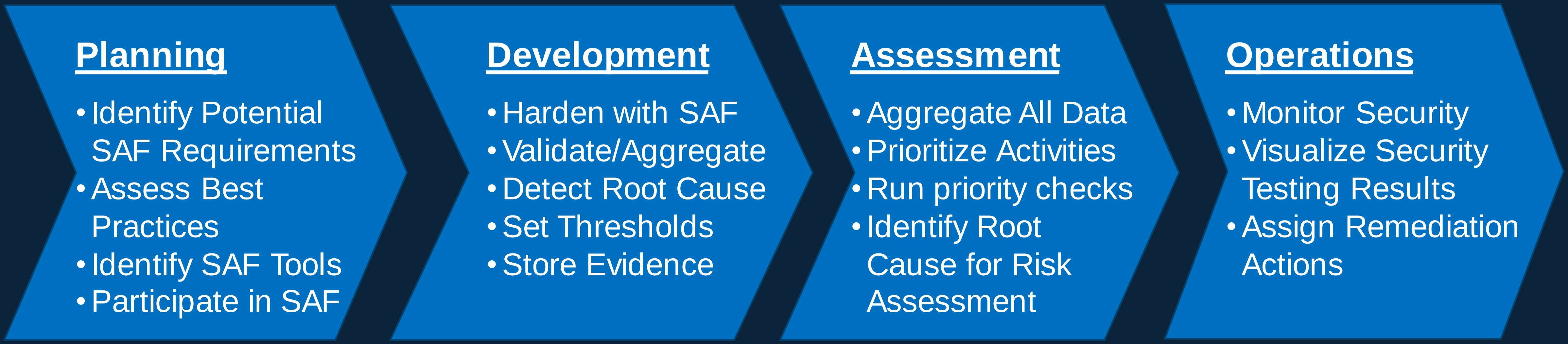
This does not provide accurate representation of the true compliance posture

Heimdall



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

SAF© Use Cases by Role



Planning

- Identify Potential SAF Requirements
- Assess Best Practices
- Identify SAF Tools
- Participate in SAF

Development

- Harden with SAF
- Validate/Aggregate
- Detect Root Cause
- Set Thresholds
- Store Evidence

Assessment

- Aggregate All Data
- Prioritize Activities
- Run priority checks
- Identify Root Cause for Risk Assessment

Operations

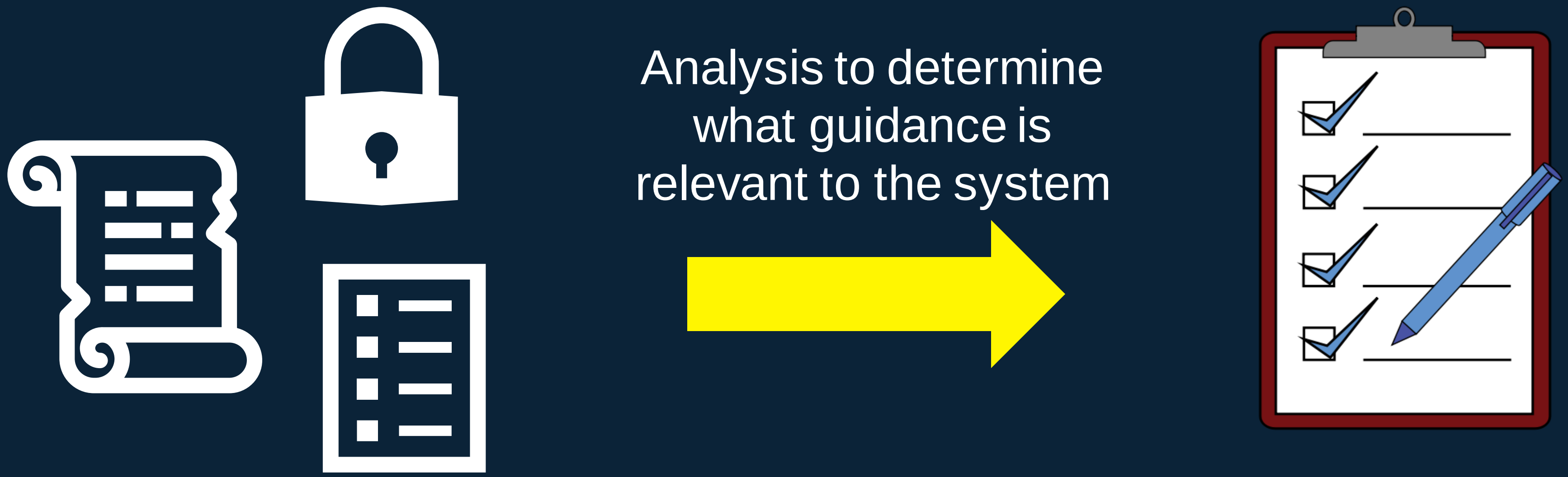
- Monitor Security
- Visualize Security Testing Results
- Assign Remediation Actions

MITRE

A Look at MITRE Vulcan

Develop STIG Ready Content from SRGs with Vulcan

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



Analysis to determine what guidance is relevant to the system

General Guidance (e.g. SRG)

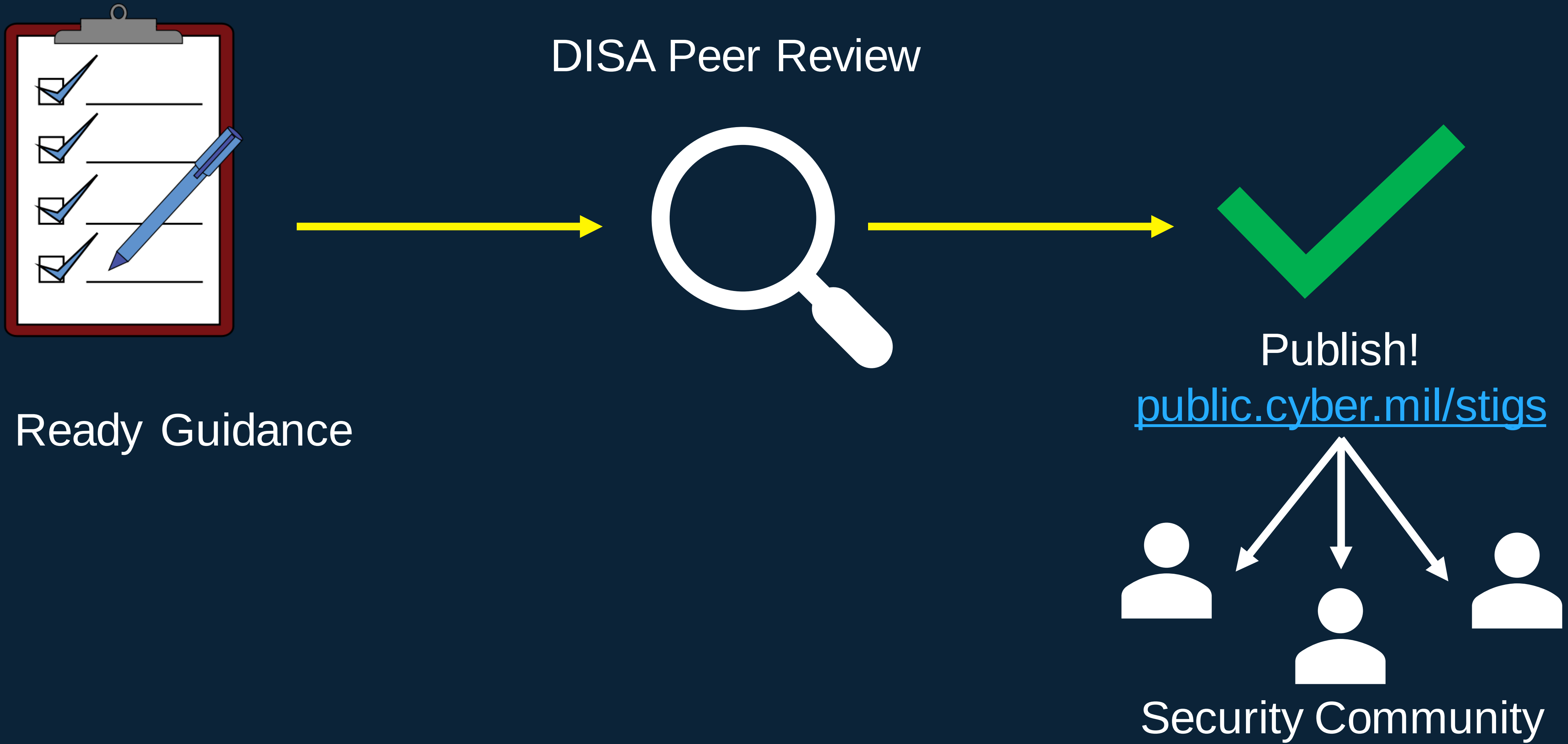
High-Level Security Requirements, Best Practices, Standards

Government and Industry Sources

SRG-aligned STIG Ready Guidance

Specific Instructions for Specific System Components

STIG Ready Content



STIG Ready Guidance

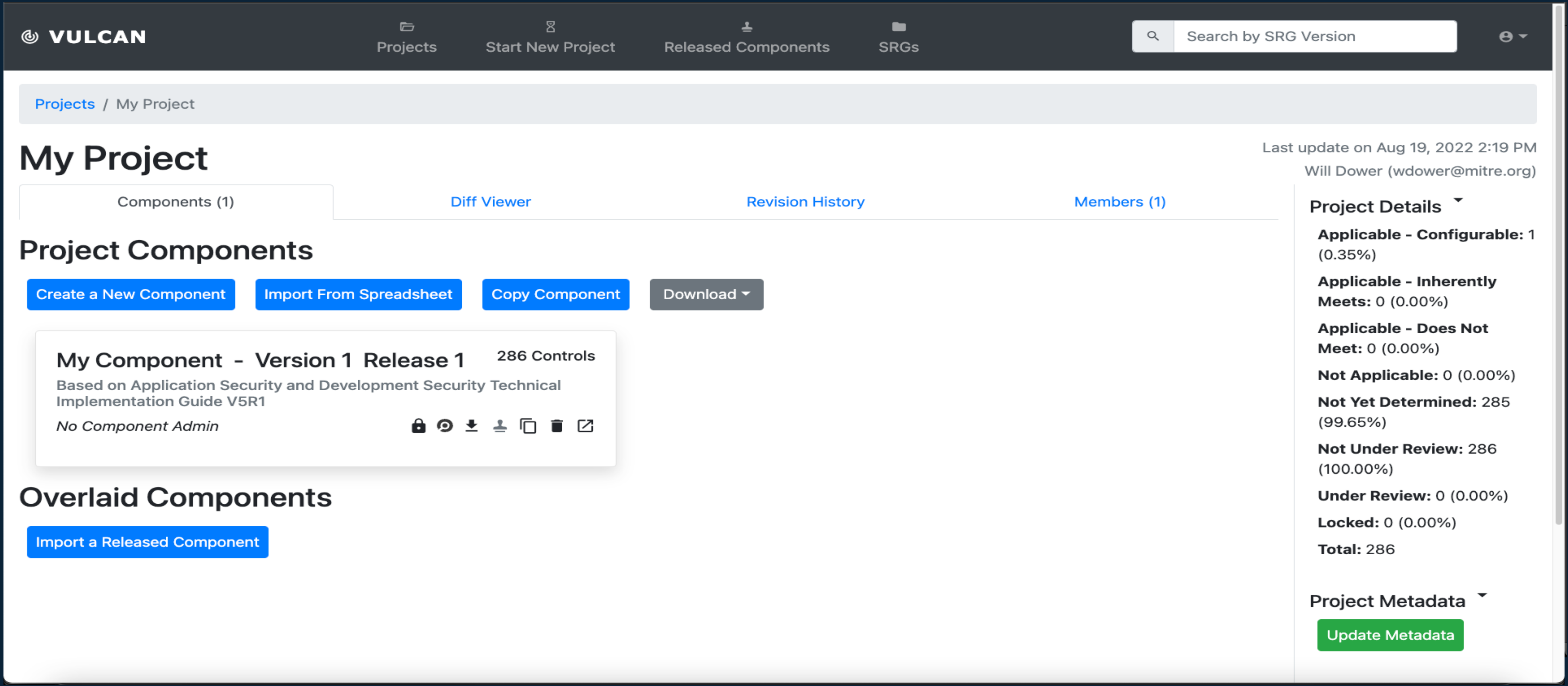
DISA Peer Review

Publish!

public.cyber.mil/stigs

Security Community

MITRE



Projects / My Project

My Project

Last update on Aug 19, 2022 2:19 PM
Will Dower (wdower@mitre.org)

Components (1) | Diff Viewer | Revision History | Members (1)

Project Components

My Component - Version 1 Release 1

286 Controls

Based on Application Security and Development Security Technical Implementation Guide V5R1

No Component Admin

Overlaid Components

Project Details

Applicable - Configurable: 1 (0.35%)

Applicable - Inherently Meets: 0 (0.00%)

Applicable - Does Not Meet: 0 (0.00%)

Not Applicable: 0 (0.00%)

Not Yet Determined: 285 (99.65%)

Not Under Review: 286 (100.00%)

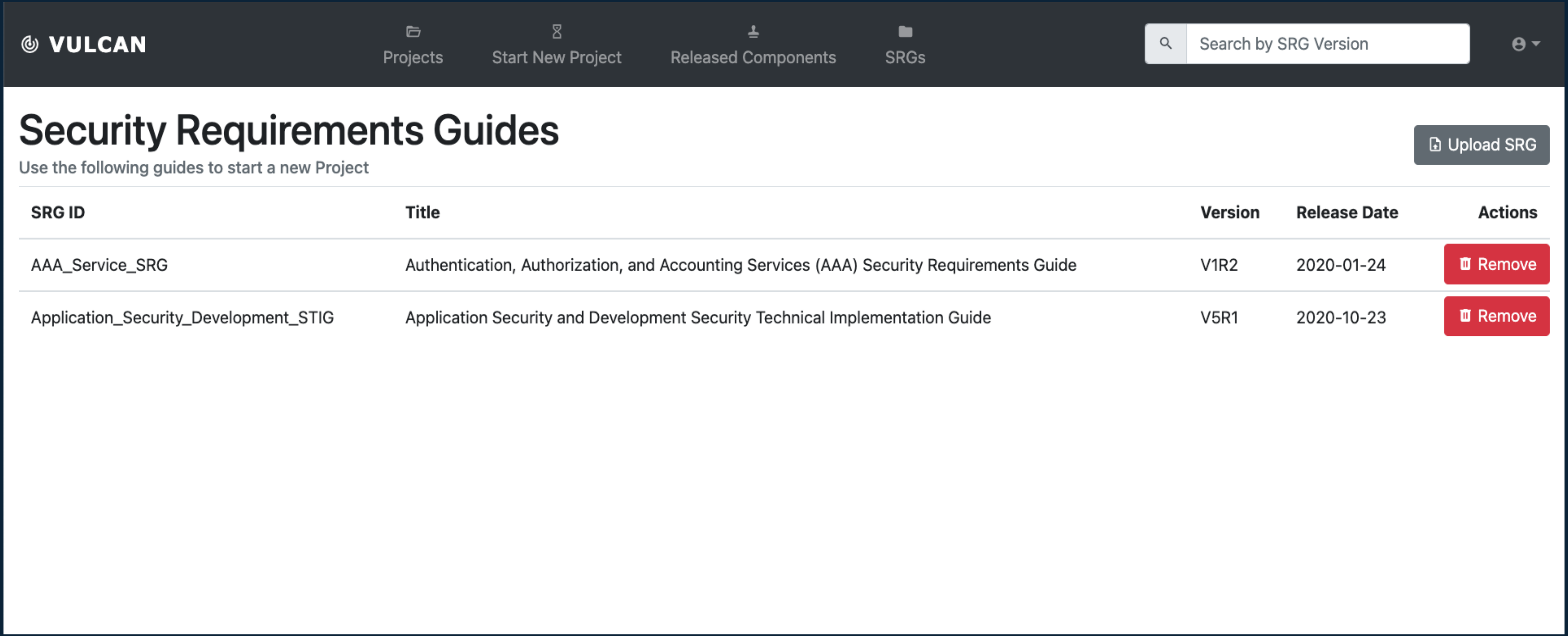
Under Review: 0 (0.00%)

Locked: 0 (0.00%)

Total: 286

Project Metadata

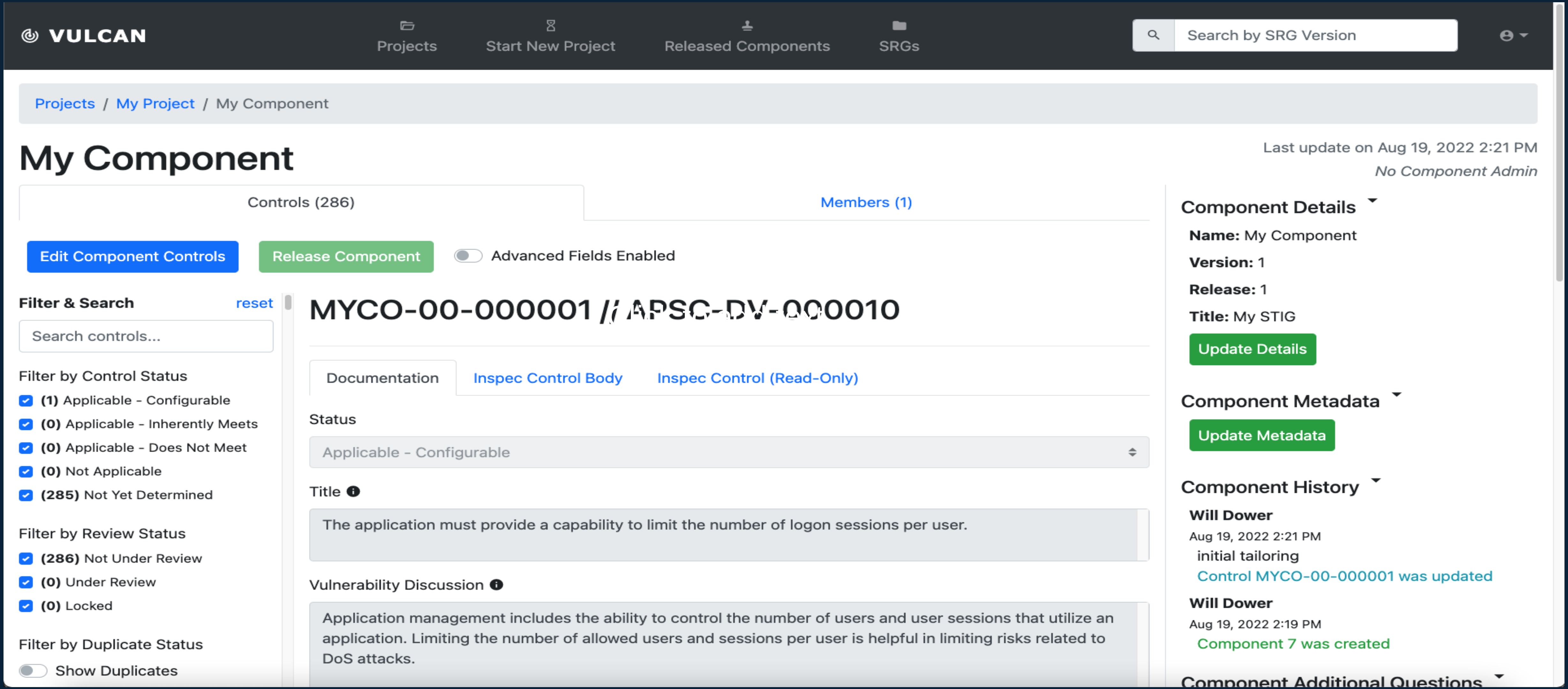
MITRE



Security Requirements Guides

Use the following guides to start a new Project

SRG ID	Title	Version	Release Date	Actions
AAA_Service_SRG	Authentication, Authorization, and Accounting Services (AAA) Security Requirements Guide	V1R2	2020-01-24	Remove
Application_Security_Development_STIG	Application Security and Development Security Technical Implementation Guide	V5R1	2020-10-23	Remove



Projects / My Project / My Component

My Component

Last update on Aug 19, 2022 2:21 PM
No Component Admin

Controls (286) | Members (1)

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

Filter & Search

Filter by Control Status

- ☑ **(1)** Applicable - Configurable
- ☑ **(0)** Applicable - Inherently Meets
- ☑ **(0)** Applicable - Does Not Meet
- ☑ **(0)** Not Applicable
- ☑ **(285)** Not Yet Determined

Filter by Review Status

- ☑ **(286)** Not Under Review
- ☑ **(0)** Under Review
- ☑ **(0)** Locked

Filter by Duplicate Status

- Show Duplicates

Status

Applicable - Configurable

Title

The application must provide a capability to limit the number of logon sessions per user.

Vulnerability Discussion

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

Component Details

Name: My Component

Version: 1

Release: 1

Title: My STIG

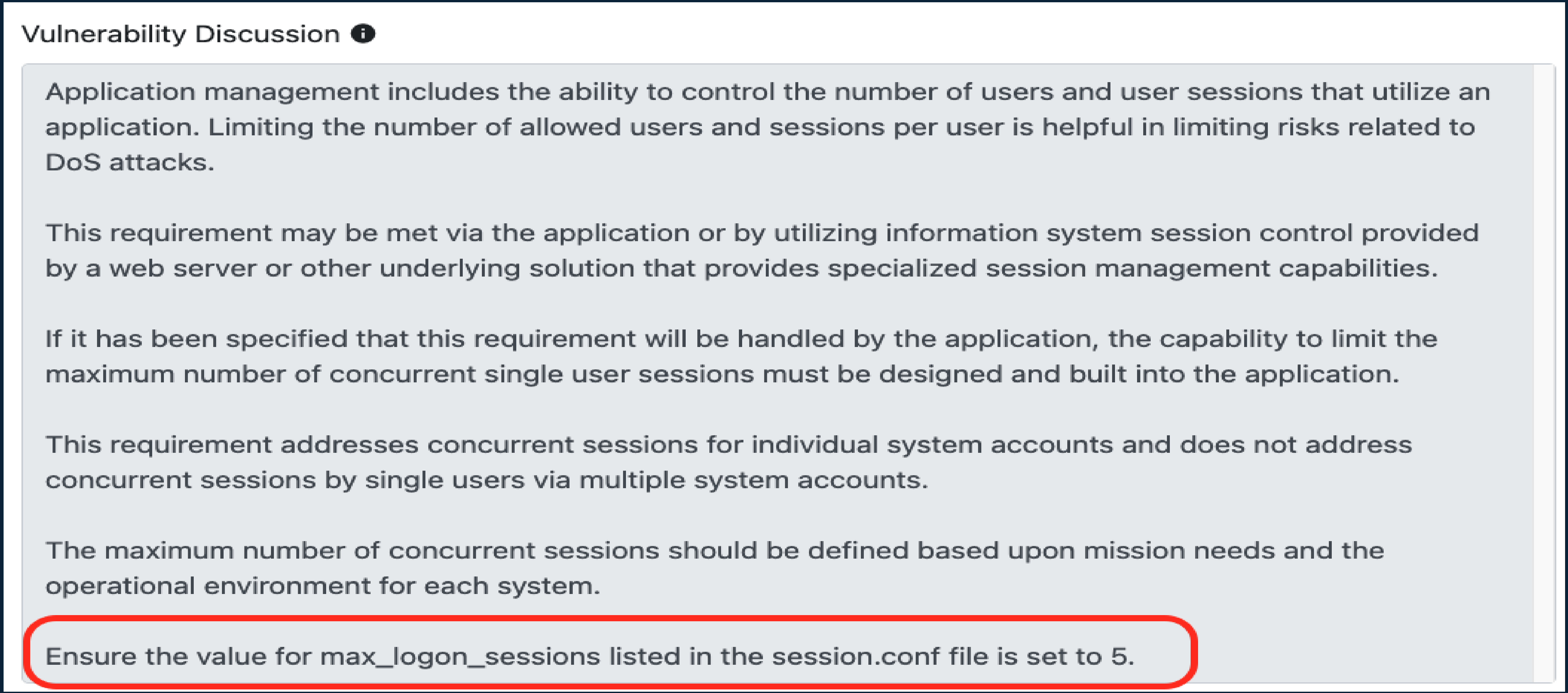
Component Metadata

Component History

Will Dower
Aug 19, 2022 2:21 PM
initial tailoring
Control MYCO-00-000001 was updated

Will Dower
Aug 19, 2022 2:19 PM
Component 7 was created

Component Additional Questions



Vulnerability Discussion

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

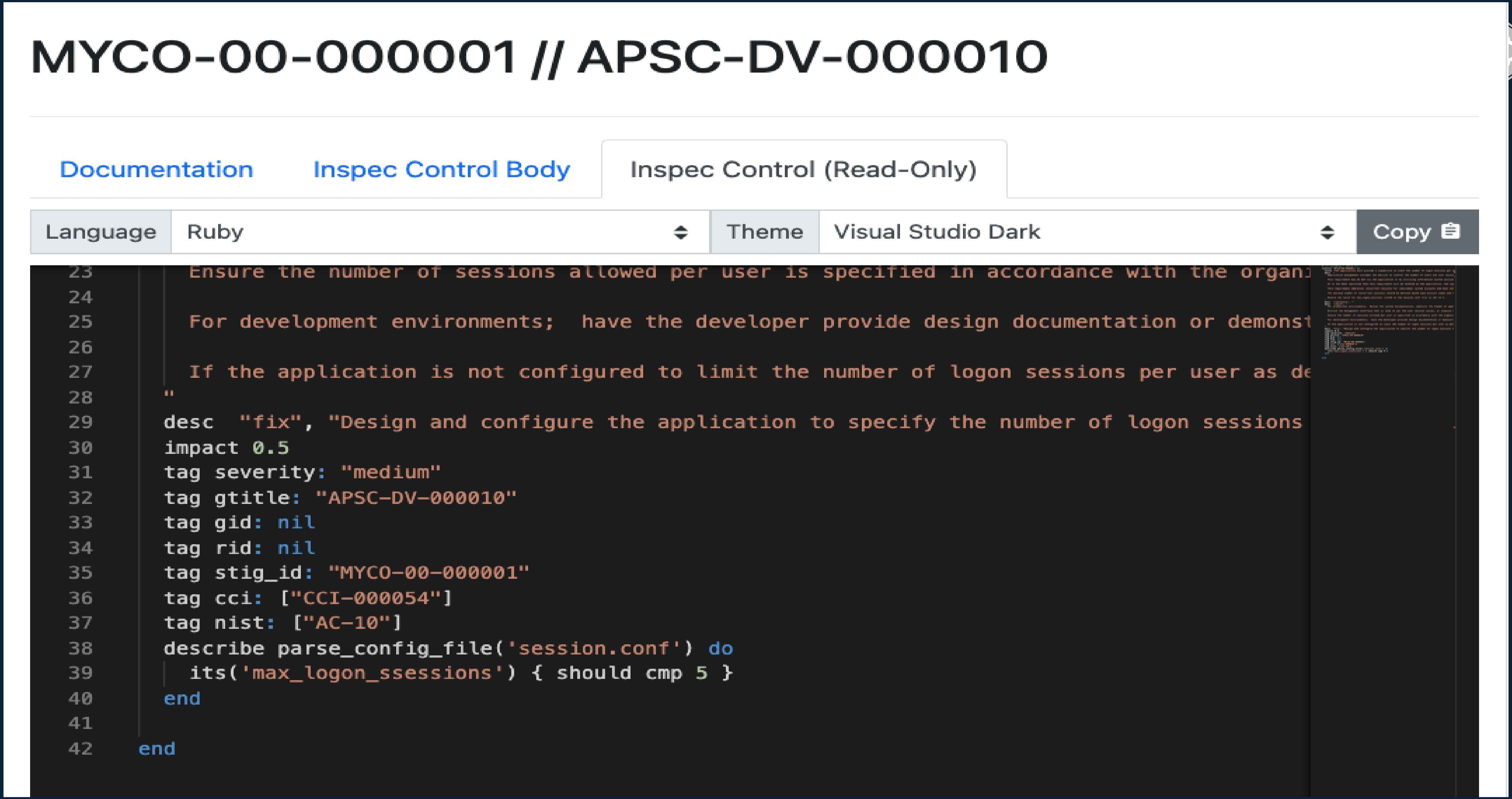
This requirement may be met via the application or by utilizing information system session control provided by a web server or other underlying solution that provides specialized session management capabilities.

If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built into the application.

This requirement addresses concurrent sessions for individual system accounts and does not address concurrent sessions by single users via multiple system accounts.

The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Ensure the value for max_logon_sessions listed in the session.conf file is set to 5.



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

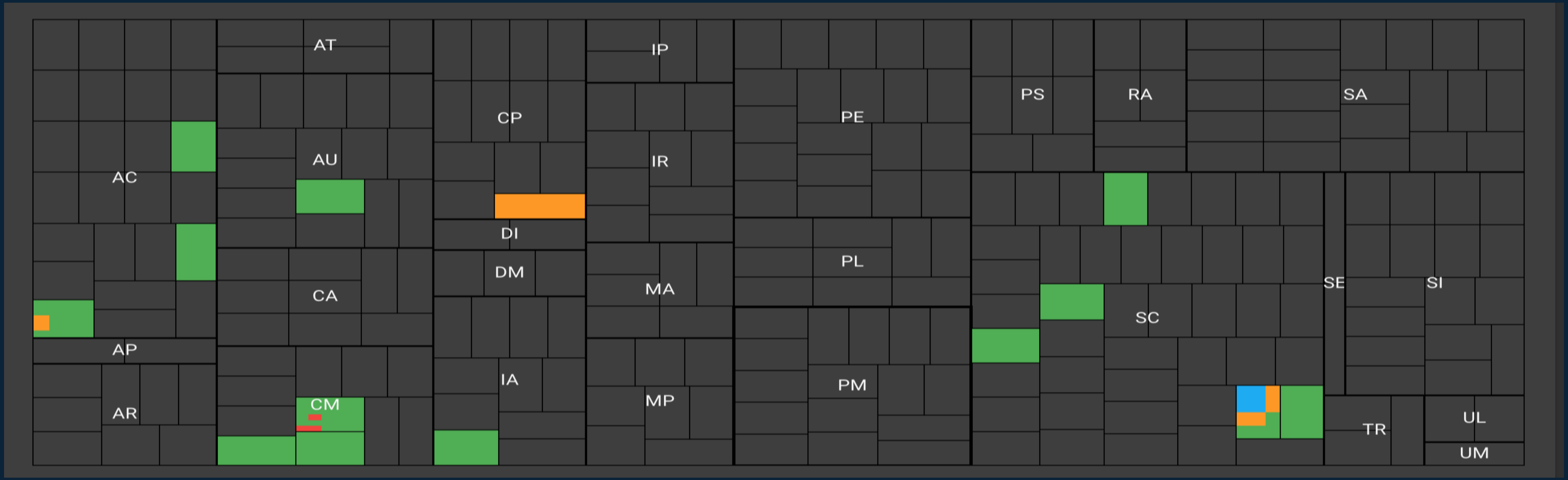
Language Ruby

Theme Visual Studio Dark

```
    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
```

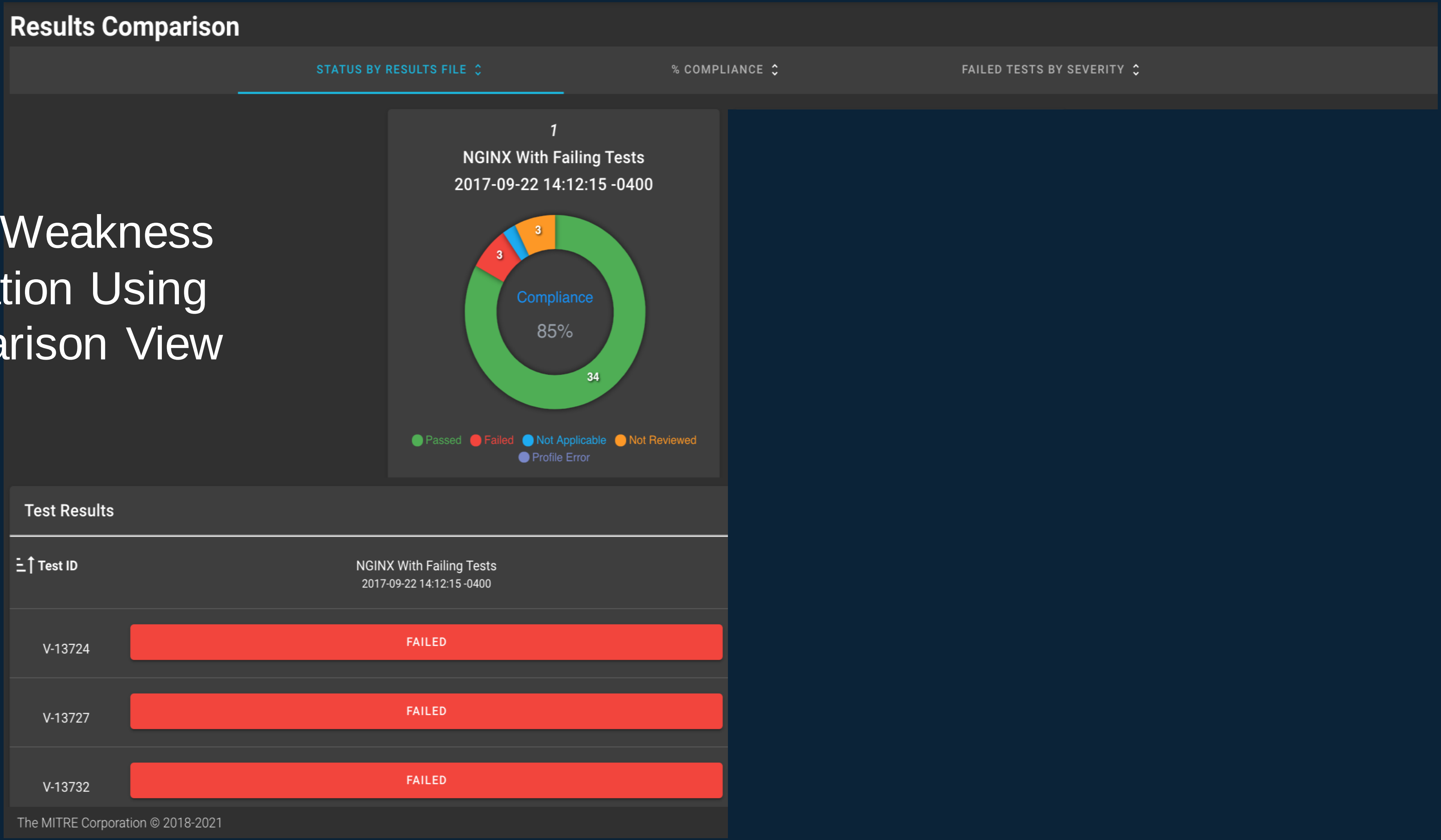
SAF Heimdall Screen Shots

Tree Map:
NIST SP 800-53 Control Coverage



SAF Heimdall Screen Shots

Verify Weakness Mitigation Using Comparison View



Results Comparison

STATUS BY RESULTS FILE ⌃⌄ | % COMPLIANCE ⌃⌄ | FAILED TESTS BY SEVERITY ⌃⌄

1

NGINX With Failing Tests

2017-09-22 14:12:15 -0400

Test Results

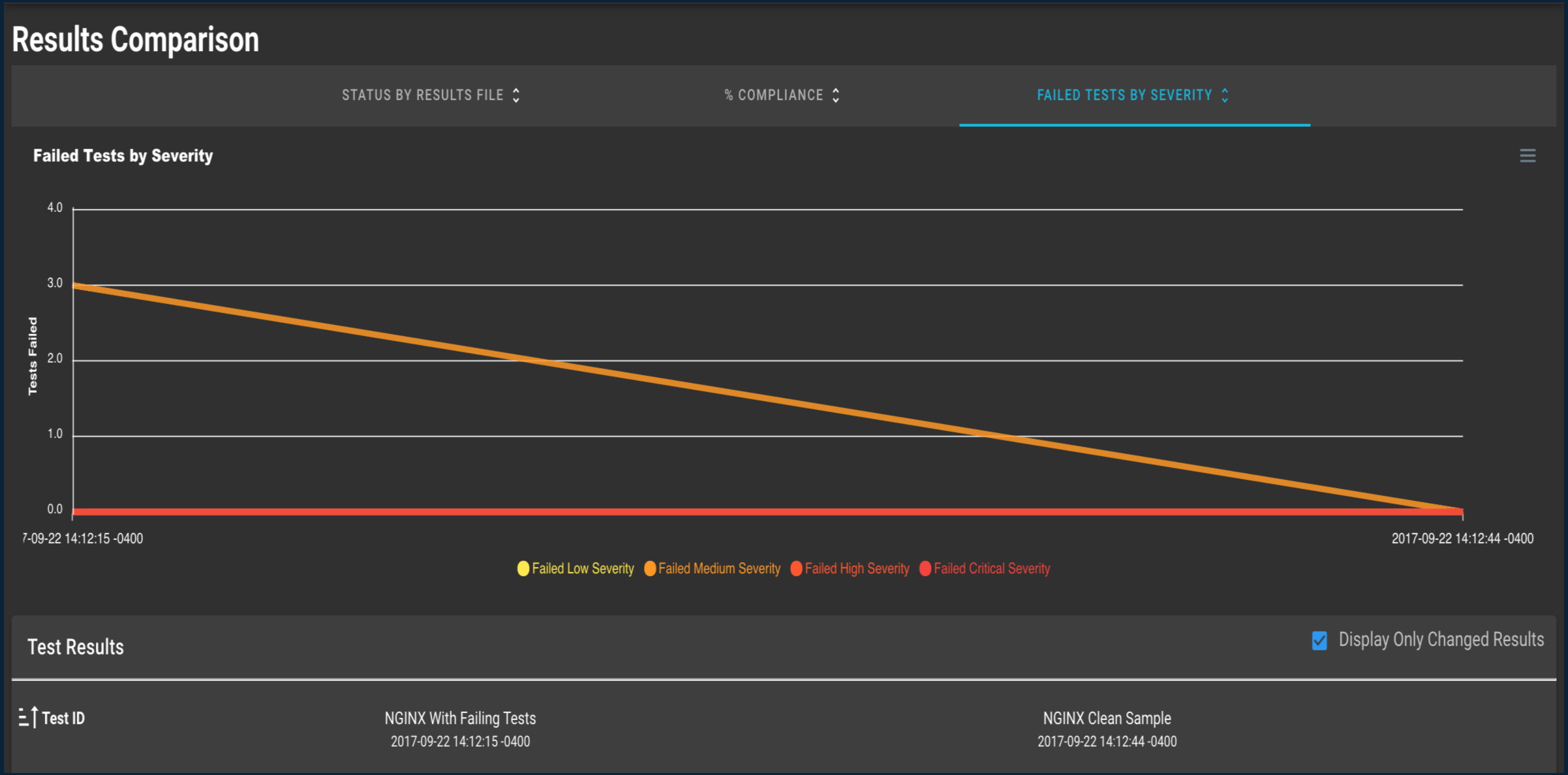
Test ID	NGINX With Failing Tests 2017-09-22 14:12:15 -0400
V-13724	FAILED
V-13727	FAILED
V-13732	FAILED

The MITRE Corporation © 2018-2021

MITRE

SAF Heimdall Screen Shots

Demonstrate Progress with Trending Graphs



Test Results

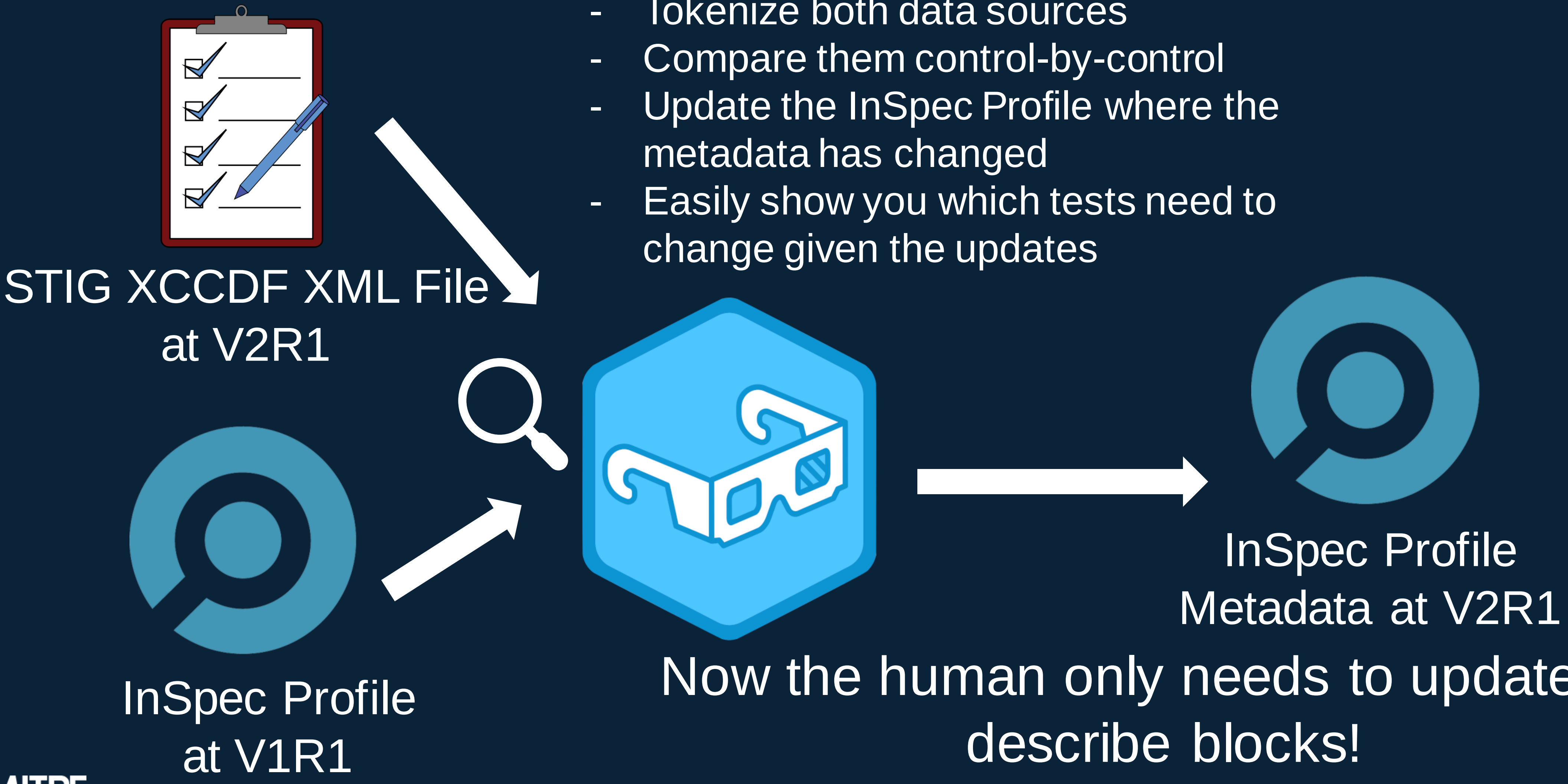
☑ Display Only Changed Results

Test ID	NGINX With Failing Tests 2017-09-22 14:12:15 -0400	NGINX Clean Sample 2017-09-22 14:12:44 -0400

Supporting Tools – Delta – Notional Workflow

Delta will:

- Tokenize both data sources
- Compare them control-by-control
- Update the InSpec Profile where the metadata has changed
- Easily show you which tests need to change given the updates



STIG XCCDF XML File at V2R1

InSpec Profile at V1R1

InSpec Profile Metadata at V2R1

Now the human only needs to update the describe blocks!

What is MITRE SAF©?

MITRE Security Automation Framework (SAF©) is a suite of open-source security automation tools that facilitate the development, collection, and standardization of content for use by the wider security community for use by government and industry organizations to

- Accelerate Authorization
- Establish Security Requirements
- Build Security In
- Assess/Monitor Vulnerabilities