SCAP, SAF© and Security Compliance Automation

22 December 2023

* Updated from a 9/15/2021 presentation by Brian Vertullo, Quintin Walters, and Zachary Lowdermilk-Christopher

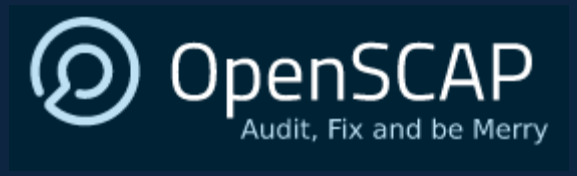
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

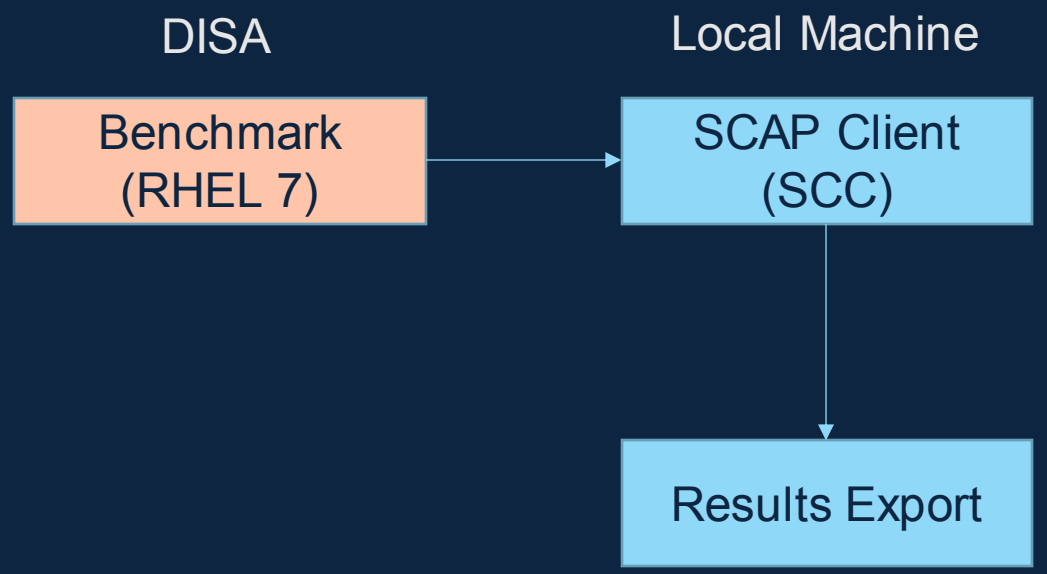
Motivation / Goal

- Provide an overview of the Security Content Automation Protocol (SCAP) and the Security Automation Framework (SAF©)
- Explain how the Sponsor benefits from InSpec and the SAF©
  - Continuous monitoring and automation
  - Reduced Risk Management Framework (RMF) costs
  - A demonstration, or side-by-side comparison, will be used to show the differences
  - This is accomplished by:
    - running an InSpec profile and displaying the results using Heimdall
    - using the SCAP Compliance Checker (SCC) to run the checks and display the results

SCAP Overview

What is Security Content Automation Protocol (SCAP)

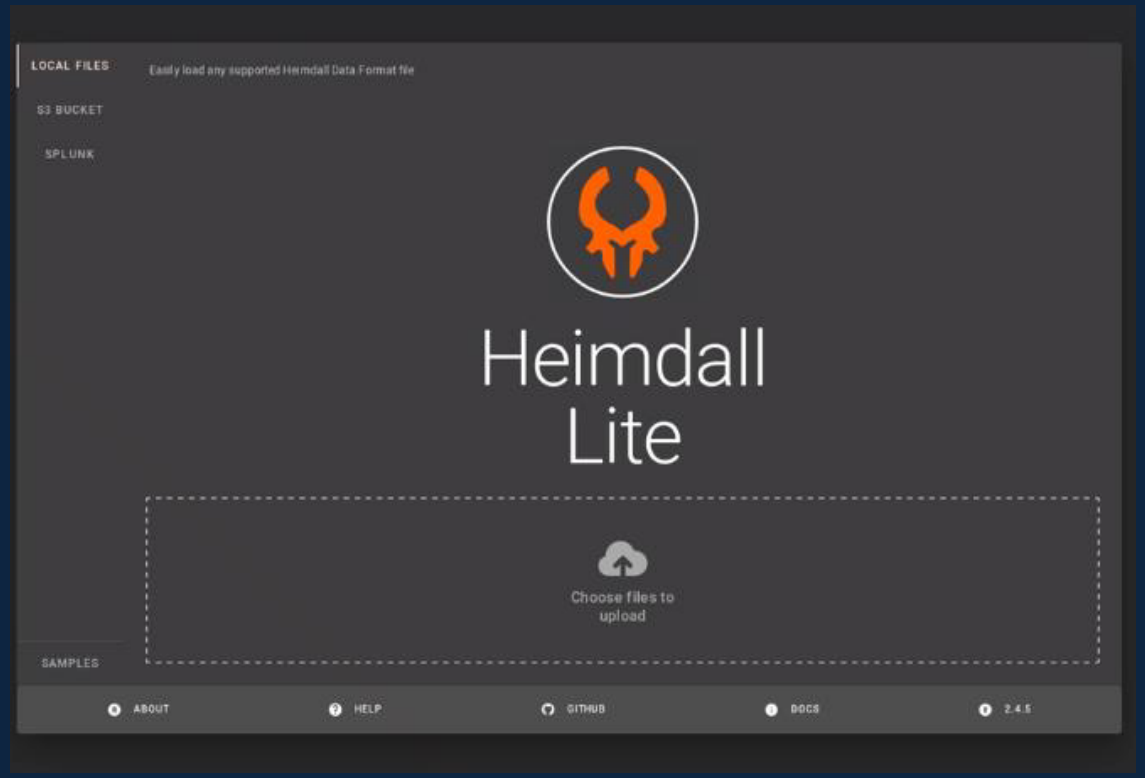




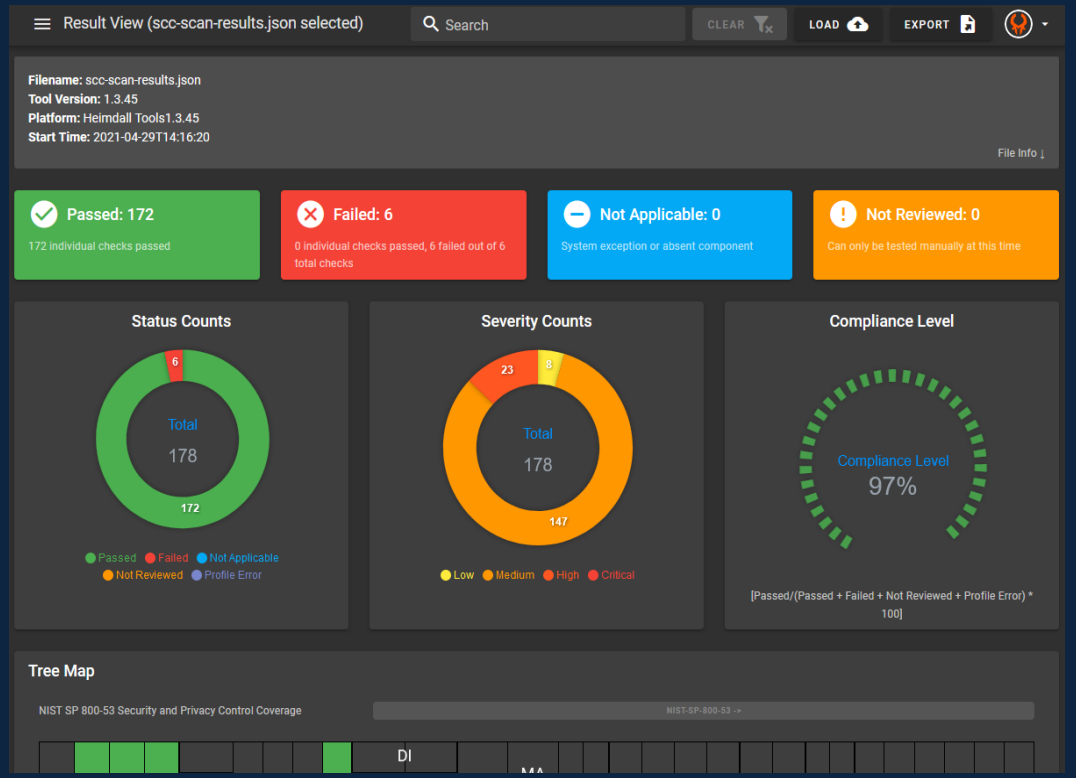
https://www.open-scap.org/
https://www.niwcatlantic.navy.mil/scap/
https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=scap

Heimdall Demo With Converted SCC Results

Heimdall



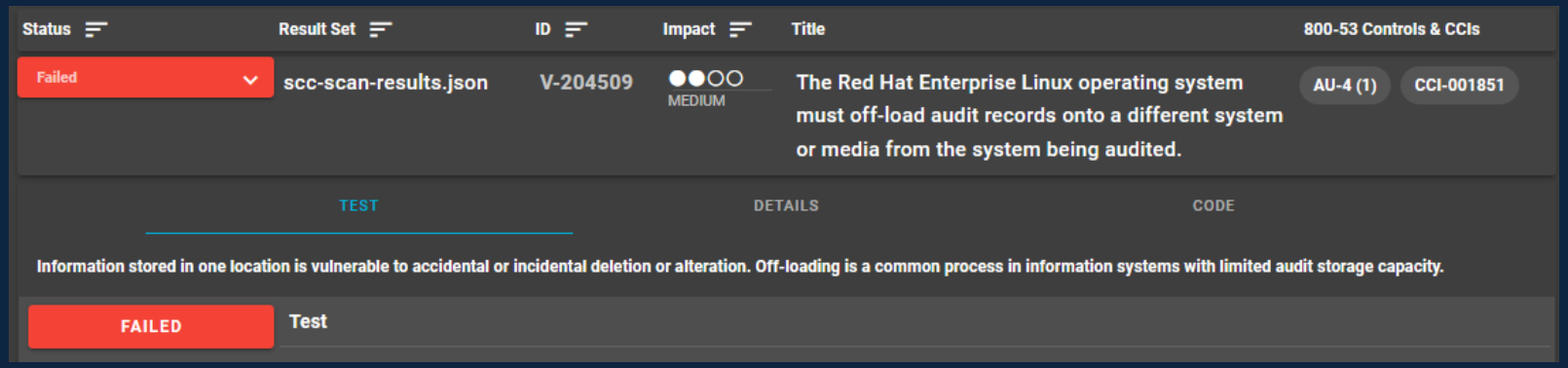
Heimdall Score



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

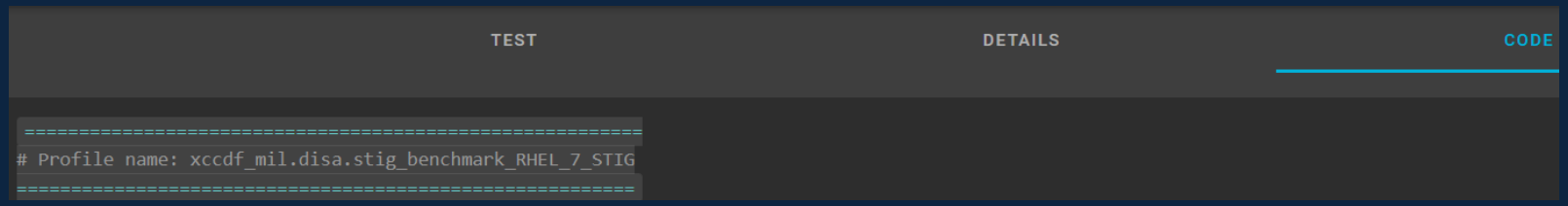
Heimdall Demo With Converted SCC Results

Heimdall Test View



Since the schema is maintained upstream, the control tests or code is not available in the XCCDF output

Heimdall Code View



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Security Automation Framework (SAF©) Overview

SAF© Overview

- **The Security Automation Framework (SAF©) allows users to streamline their security automation by facilitating the:**
  - Hardening – By using Ansible or similar products, hardening procedures and be automated for an environment. RHEL 7 Hardening script exists and is currently used.
  - Validation – Using InSpec to verify that the hardening procedures were successful and IAW the STIG requirements.
  - Normalization – Converting the output data into a standardized format like the Oasis Heimdall Data Format (OHDF) for use.
  - Visualization – Heimdall is used to provide visualizations of the validation output and display the compliance details.
  - Attestation – Allowing you to layer the policy and manual check status as a part of security automation.

InSpec

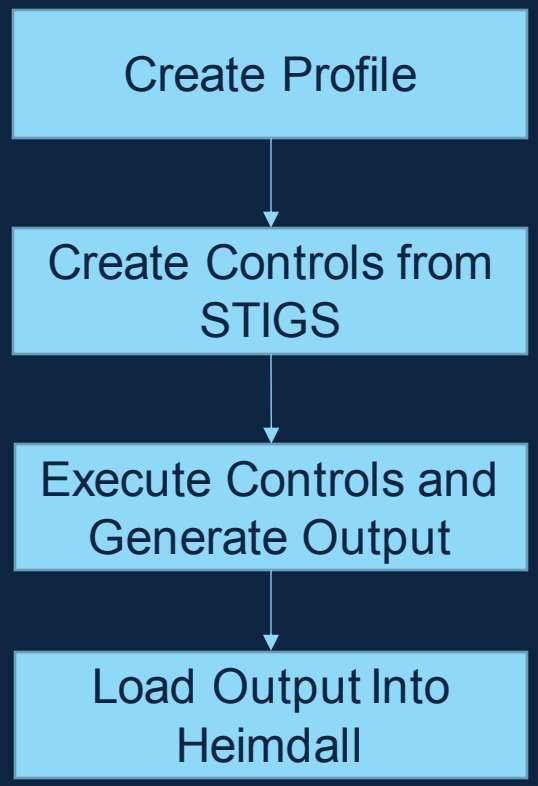
MITRE SAF

INSPEC BY CHEF

Heimdall

Profile – Contains system information such as resource paths

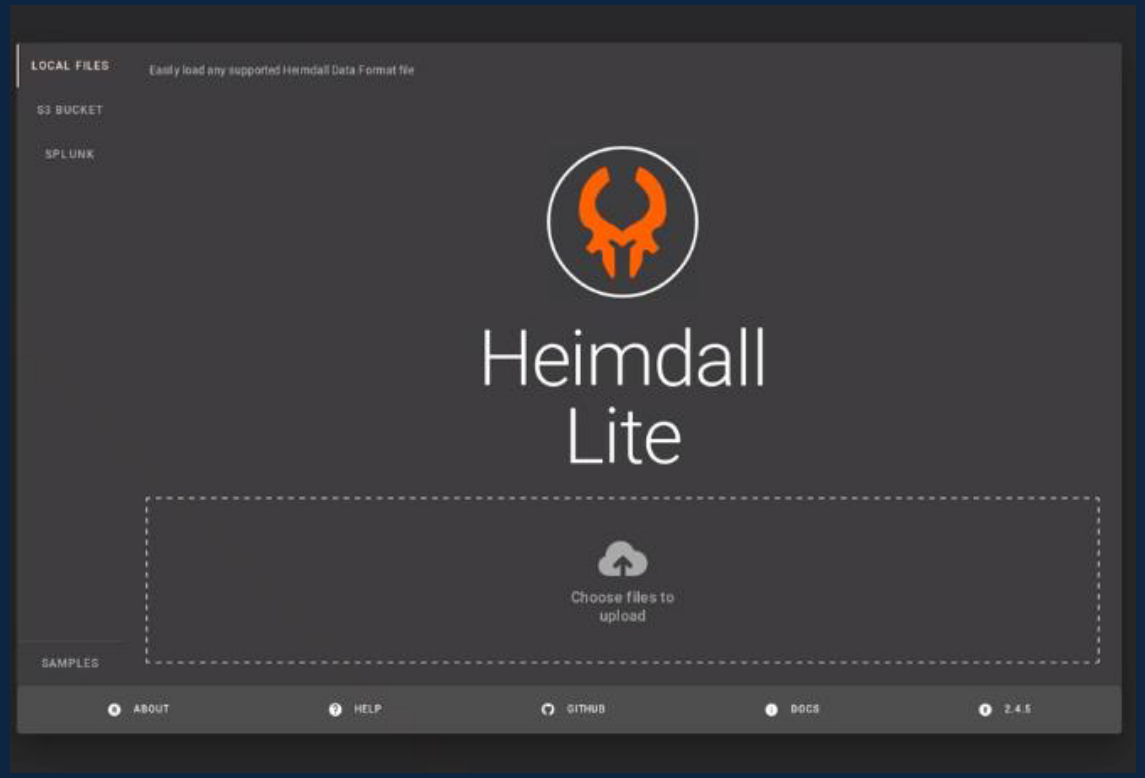
Control – Contains detailed information about the individual check as well as the code for execution



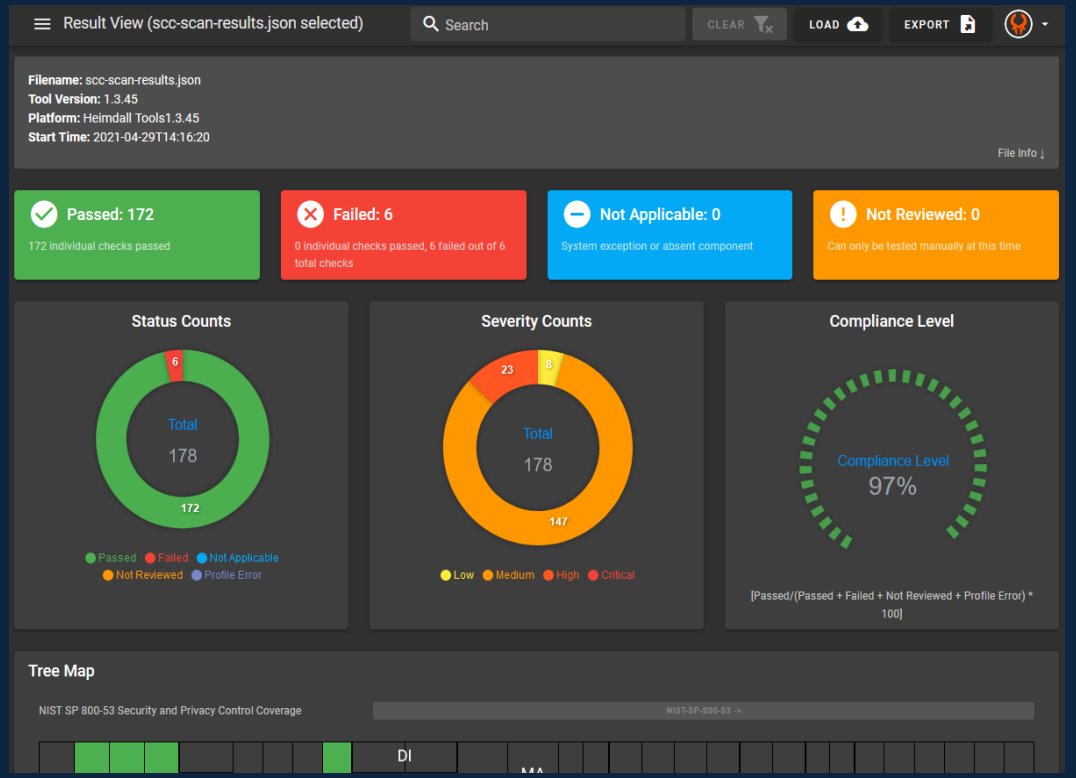
https://docs.chef.io/inspec/install/
https://saf.mitre.org/#/
https://heimdall-lite.mitre.org/

Heimdall Demo With InSpec Results

Heimdall



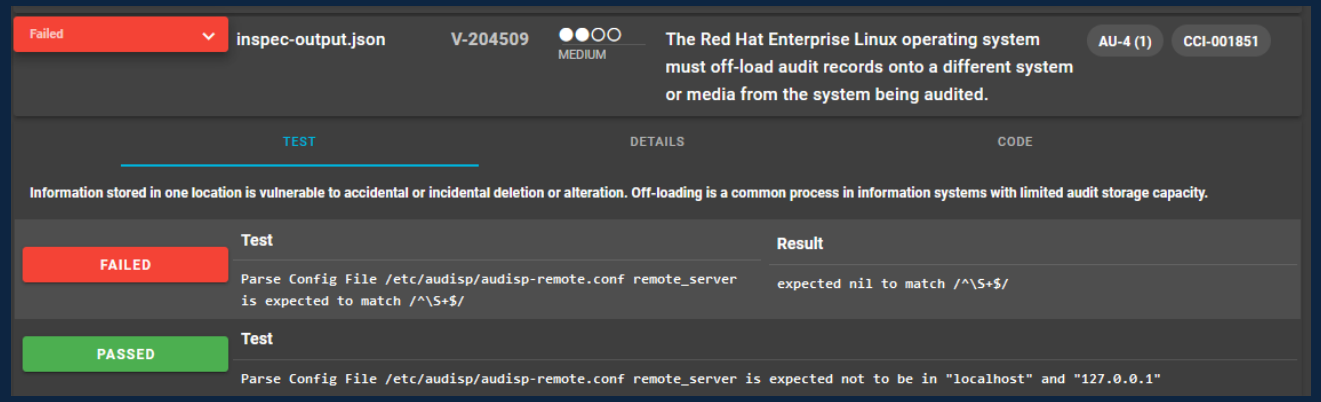
Heimdall Score



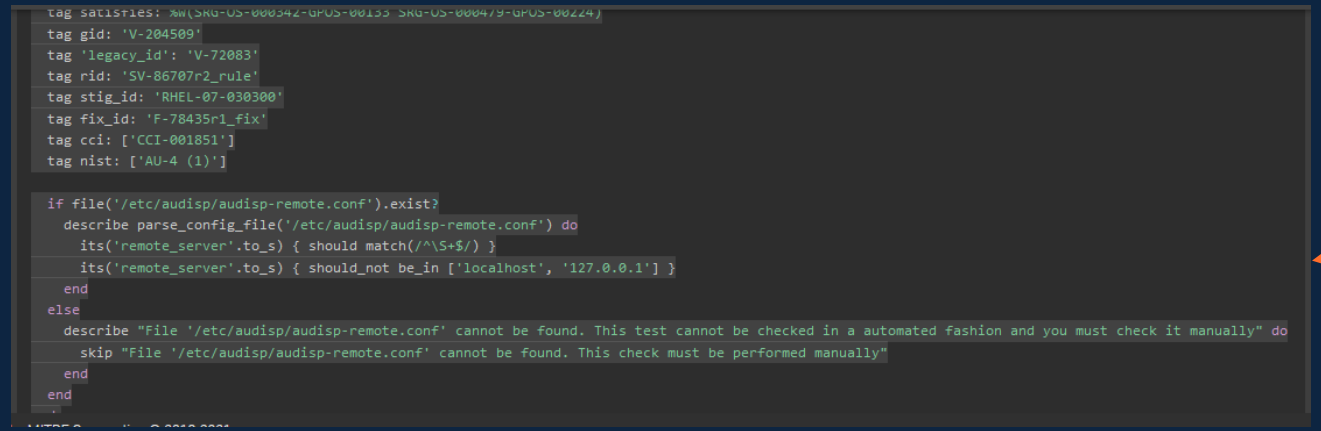
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Heimdall Demo With InSpec Results

Heimdall Test View



Heimdall Code View



Heimdall will display the contents of a .rb file used for the controls

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

SCAP vs SAF©

SCAP Clients

Pros:

- SCC on approved software list for DoD networks
- Most clients have native DISA checklist output support or native HTML output support
- All-in-one interface

Cons:

- Limited to file system checks
- Must be run locally for consistency
- Each client must be updated whenever an update to the schema comes out
- Based on non-funded standard by the government

SCAP Standard

SCAP Pros:

- NIST standard
- Widely used
- Cyber.mil currently provides operating system and other useful content

Cons:

- No longer funded by NIST to extend the schema
- Historically slow to update the schema (18-24 months)
- Updating requires update to the scheme as well as every client to translate
- Requires a client like SCC or OpenSCAP to execute
- Limited to file system checks

SAF©

Pros:

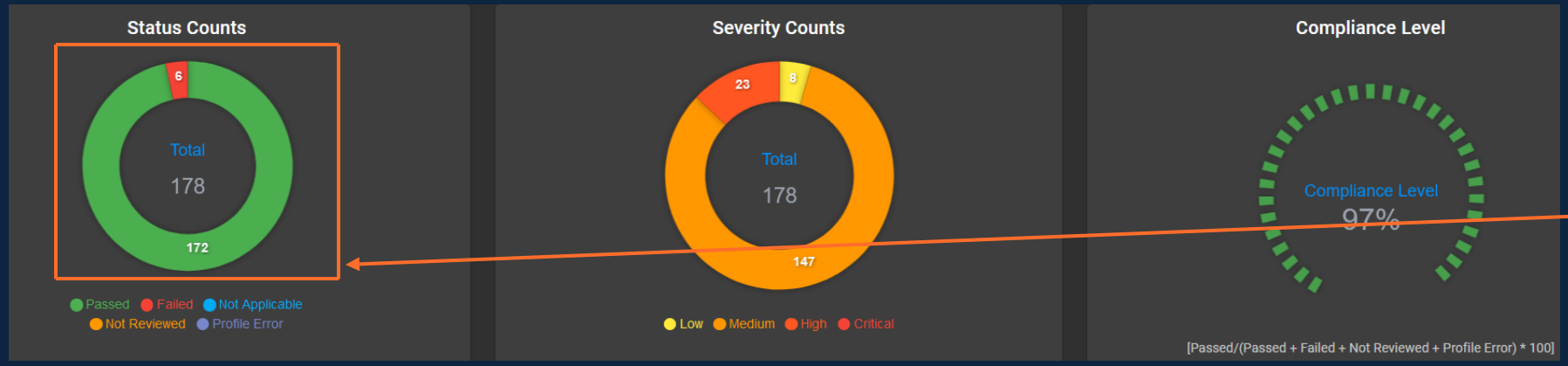
- Being quickly adopted by the defense, intelligence, and vendor communities
- Ever growing library of tools and content
- InSpec profiles:
  - Cover all STIG benchmark checks
  - Quality of the checks are generally better than the SCAP content
  - Content can be easily tailored to meet organizational requirements
  - Both code and output specifically designed to be human readable (both check and output)
- Heimdall storage and visualization
- Ability to scan the application stack, cloud, containers, and applications
- Army ECMA is adopting and integrating SAF (G2 Intel/G6 CIO)

Cons:

- Software approval process
  - DISA has already approved

Output Comparison

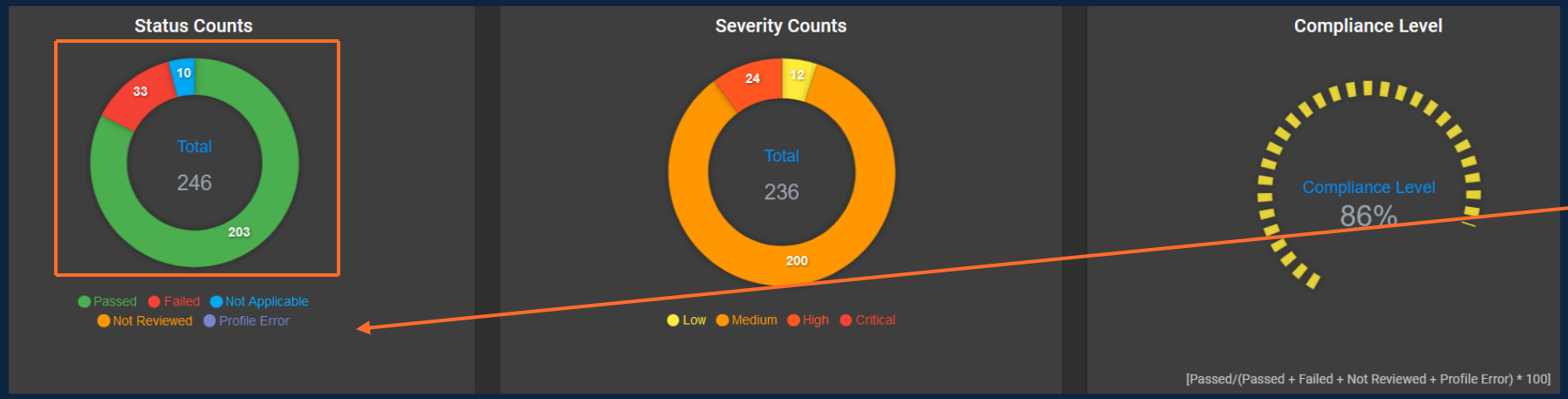
SCAP (SCC)



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

Automation of InSpec and Heimdall

- InSpec can utilize remote access such as ssh and winrm
- InSpec Tools can convert InSpec output to many formats
- Heimdall Server has an API
- InSpec, Heimdall, and InSpec tools can be run in docker containers

- We have developed a script to utilize and automate the above process
- Given an IP, username, ssh key or password and InSpec profile
  - this script runs the profile, uploads it to the Heimdall server, and converts it to xccdf format
- Looking to expand the tool to also compare previous runs and alert on changes

Recommendations and next steps

- We recommend adoption of the SAF to further security compliance and automation goals. To help enrich situational awareness throughout the application stack and allow for your organization to reap the benefits of the next generation of security automation technology.
- Pilot with a key application to show the benefits
- InSpec integration into CI/CD pipeline and automation

Demo

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

SCAP Demo / Steps

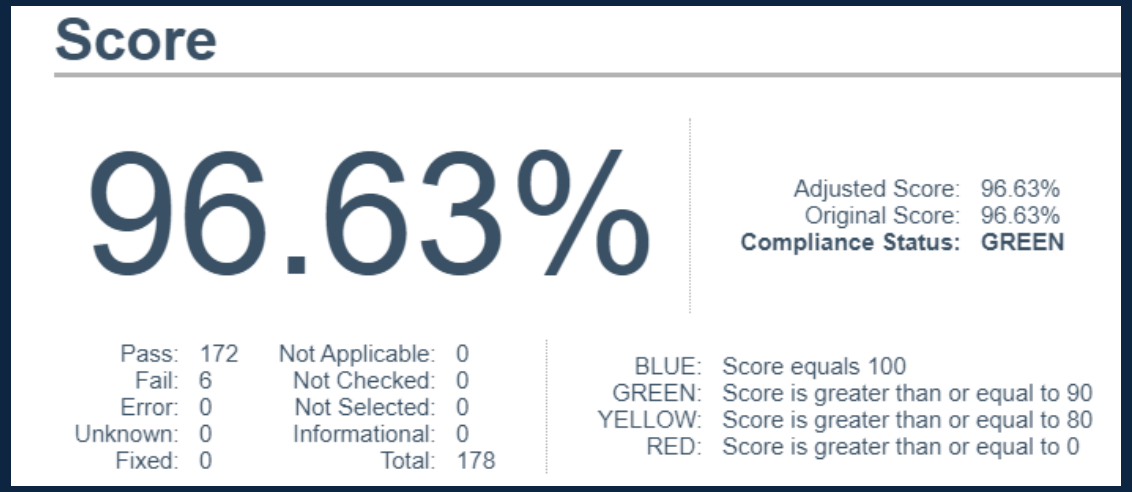
Running SCC

```
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:9571701
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:9571701 [true]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:8658500
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:8658500 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:909
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:909 [false]
15:35:28 - Completed rule  : Red Hat Enterprise Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. [pass]
15:35:28 - Processing rule : (41 of 178) Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.
- (CCE-80354-4)
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:914
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:914 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:915
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:915 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:8658500
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:8658500 [true]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:913
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:913 [true]
15:35:28 - Completed rule  : Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. [pass]
15:35:28 - Processing rule : (42 of 178) Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance
modes. - (CCE-80354-4)
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:9571900
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:9571900 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:9571901
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:9571901 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:8658500
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:8658500 [false]
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:913
15:35:28 - Completed test  : oval:mil.disa.stig.rhel7:tst:913 [true]
15:35:28 - Completed rule  : Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. [pass]
15:35:28 - Processing rule : (43 of 178) The Red Hat Enterprise Linux operating system must not have the rsh-server package installed. - (CCE-27342-5)
15:35:28 - Processing test : oval:mil.disa.stig.rhel7:tst:1272
15:35:29 - Completed test  : oval:mil.disa.stig.rhel7:tst:1272 [true]
15:35:29 - Completed rule  : The Red Hat Enterprise Linux operating system must not have the rsh-server package installed. [pass]
15:35:29 - Processing rule : (44 of 178) The Red Hat Enterprise Linux operating system must not have the ypserv package installed. - (CCE-27399-5)
15:35:29 - Processing test : oval:mil.disa.stig.rhel7:tst:1310
```

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

SCAP Demo / Steps

Score and Results in 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 the decrease in checks. The current DISA STIG has 240 items to be checked but only 178 checks are executed by SCC

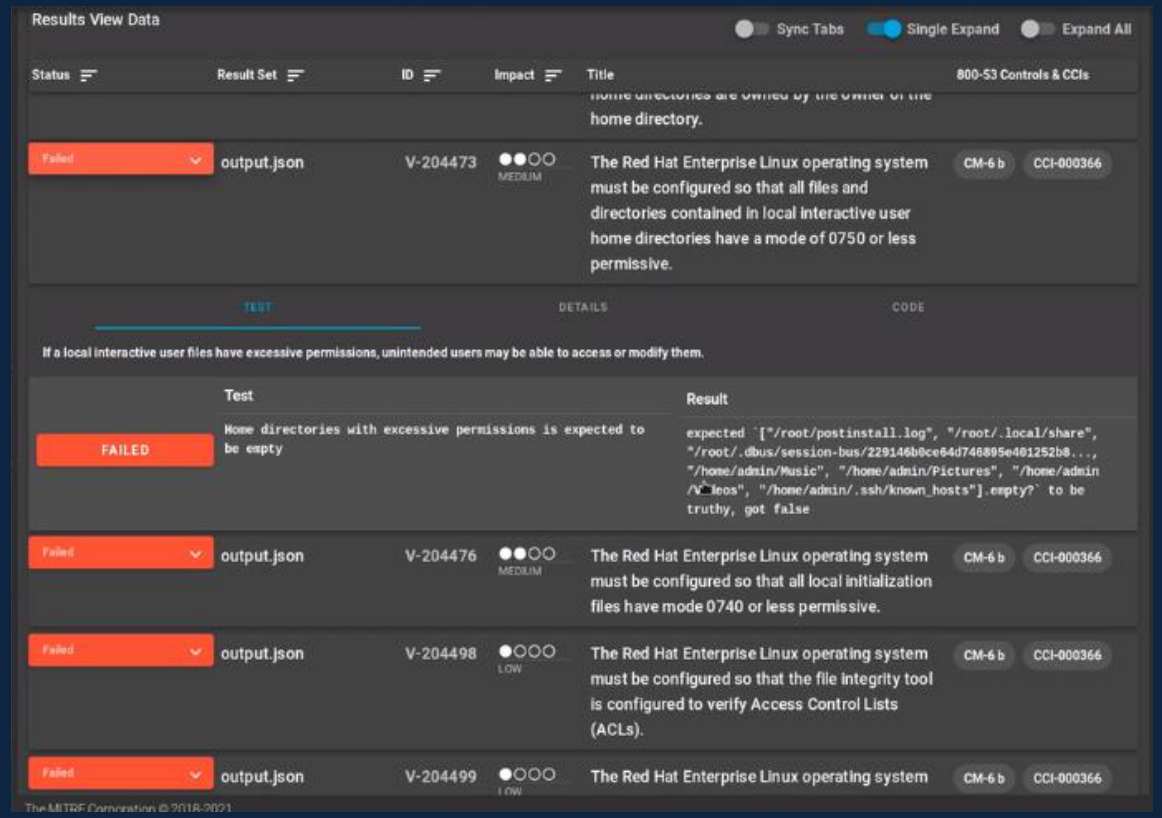
Results

- **SRG-OS-000023-GPOS-00006**
  - The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. - (CCE-26970-4) - Pass
- **SRG-OS-000028-GPOS-00009**
  - The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. - (CCE-80112-6) - Pass
- **SRG-OS-000375-GPOS-00160**

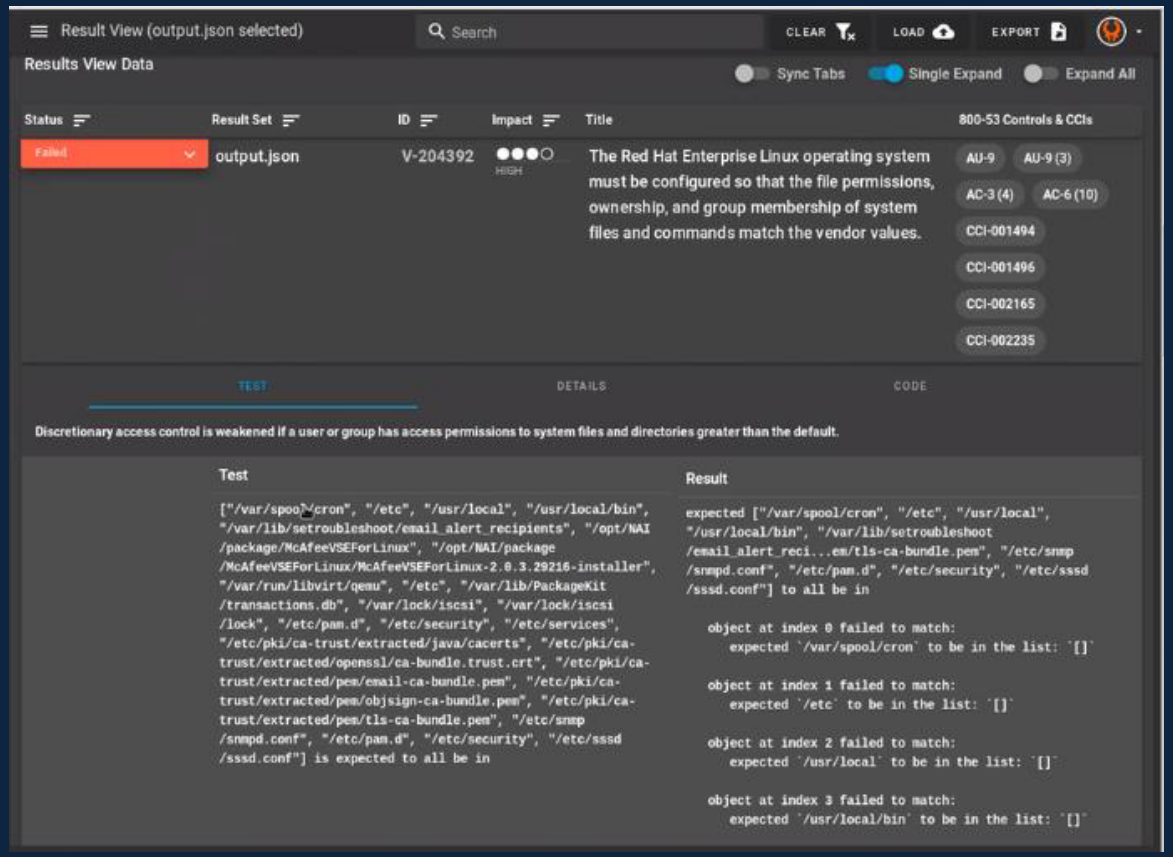
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Heimdall Demo With InSpec Results

Heimdall Results



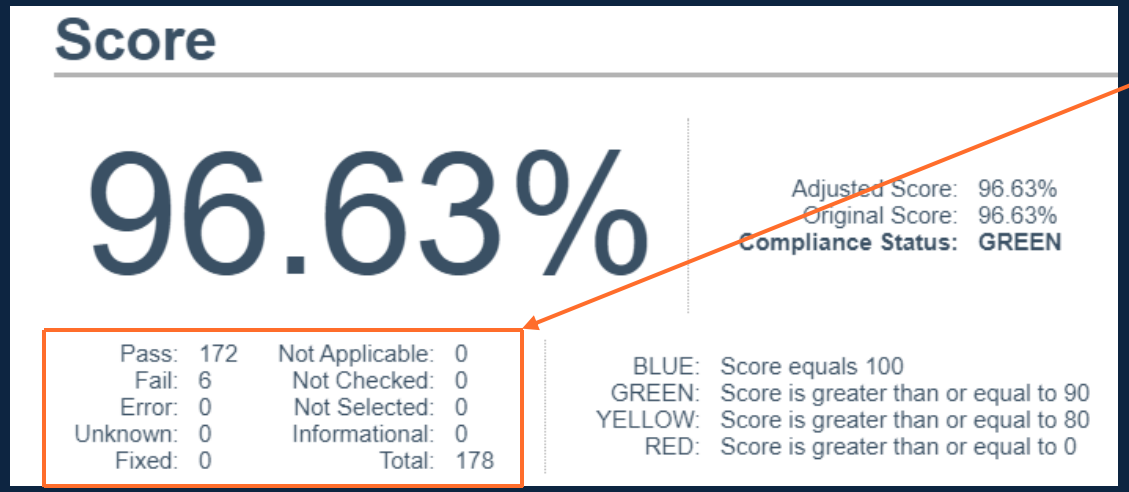
Heimdall Results Expanded



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

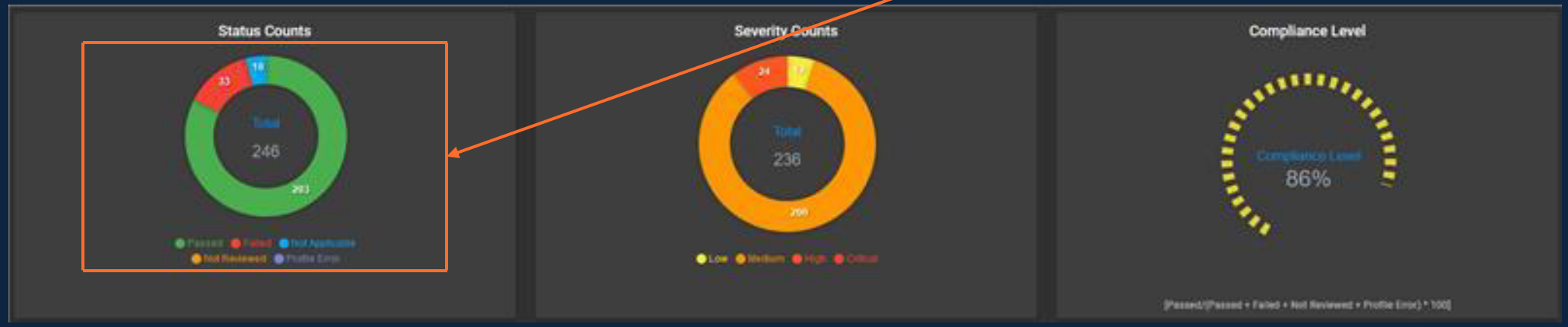
Output Comparison

SCAP (SCC)



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

Heimdall



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

Output Comparison False Negative (V-204578)

SCAP (SCC)

Rule ID:	xccdf_mil.disa.stig_rule_SV-204578r603843_rule
Result:	Fail
Version:	RHEL-07-040110

Tests:

Test ID: oval:mil.disa.stig.rhel7:tst:1400 (textfilecontent54_test)
Result: false
Title: tests the value of Ciphers setting in the /etc/ssh/sshd_config file
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.rhel7:obj:3078 (textfilecontent54_object)
Object Requirements:
- behavior requirements:
  - ignore_case = true
- filepath must be equal to '/etc/ssh/sshd_config'
- pattern must match the pattern '^[\s]*Ciphers[\s]+(.*)'
- instance must be greater than or equal to '1'

State ID: oval:mil.disa.stig.rhel7:ste:3078 (textfilecontent54_state)
State Requirements:
- check_existence = 'at_least_one_exists', subexpression must match the pattern '^"?(aes256-ctr,aes192-ctr,aes128-ctr)"?[\s]*(?:|(?:#.*))?$'

Collected Item Properties:
- filepath equals '/etc/ssh/sshd_config'
- path equals '/etc/ssh'
- filename equals 'sshd_config'
- pattern equals '^[\s]*Ciphers[\s]+(.*)'
- instance equals '1'
- text equals 'Ciphers aes128-ctr,aes192-ctr,aes256-ctr'
- line equals 'Ciphers aes128-ctr,aes192-ctr,aes256-ctr'
- subexpression equals 'aes128-ctr,aes192-ctr,aes256-ctr'

Additional Information: Check requirement not met.

Heimdall

Passed | output.json | V-204578

```
tag fix_id: 'F-78575r3_fix'
tag cci: %w(CCI-000068 CCI-000366 CCI-000803)
tag nist: ['AC-17 (2)', 'CM-6 b', 'IA-7']

@ciphers_array = inspec.sshd_config.params['ciphers']

@ciphers_array = @ciphers_array.first.split(',') unless @ciphers_array.nil?

describe @ciphers_array do
  it { should be_in %w(aes128-ctr aes192-ctr aes256-ctr) }
end
end
```

This is an example of a test from the RHEL 7 benchmark failing in SCC, while the InSpec check passes and is visualized in Heimdall. SCAP is checking for an exact match while InSpec provides the flexibility to execute a more accurate test.

Expected: aes256-ctr,aes192-ctr,aes128-ctr

Subexp: aes128-ctr,aes192-ctr,aes256-ctr