

SCAP, SAF[®] and Security Compliance Automation

22 December 2023

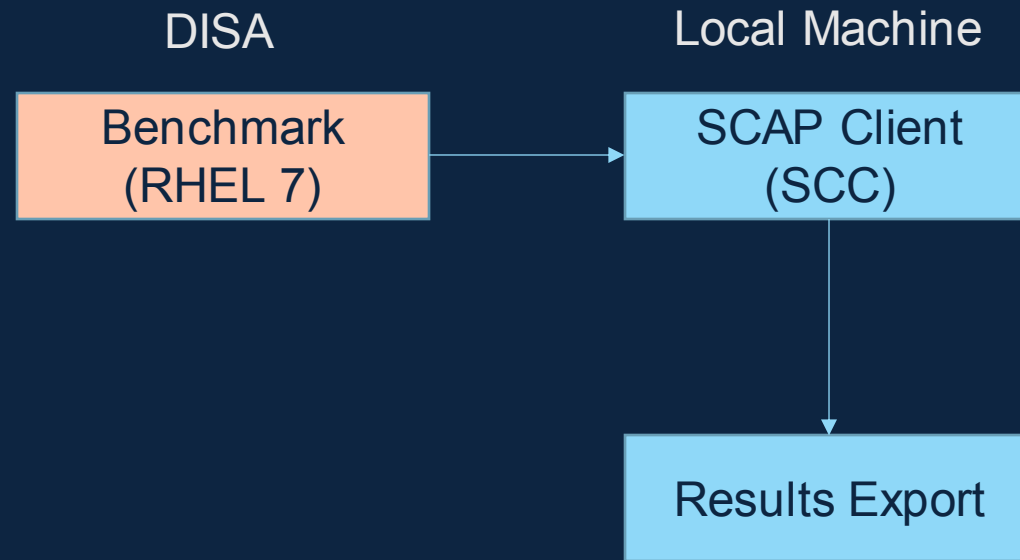
* Updated from a 9/15/2021 presentation by Brian Vertullo, Quintin Walters, and Zachary Lowdermilk-Christopher

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)



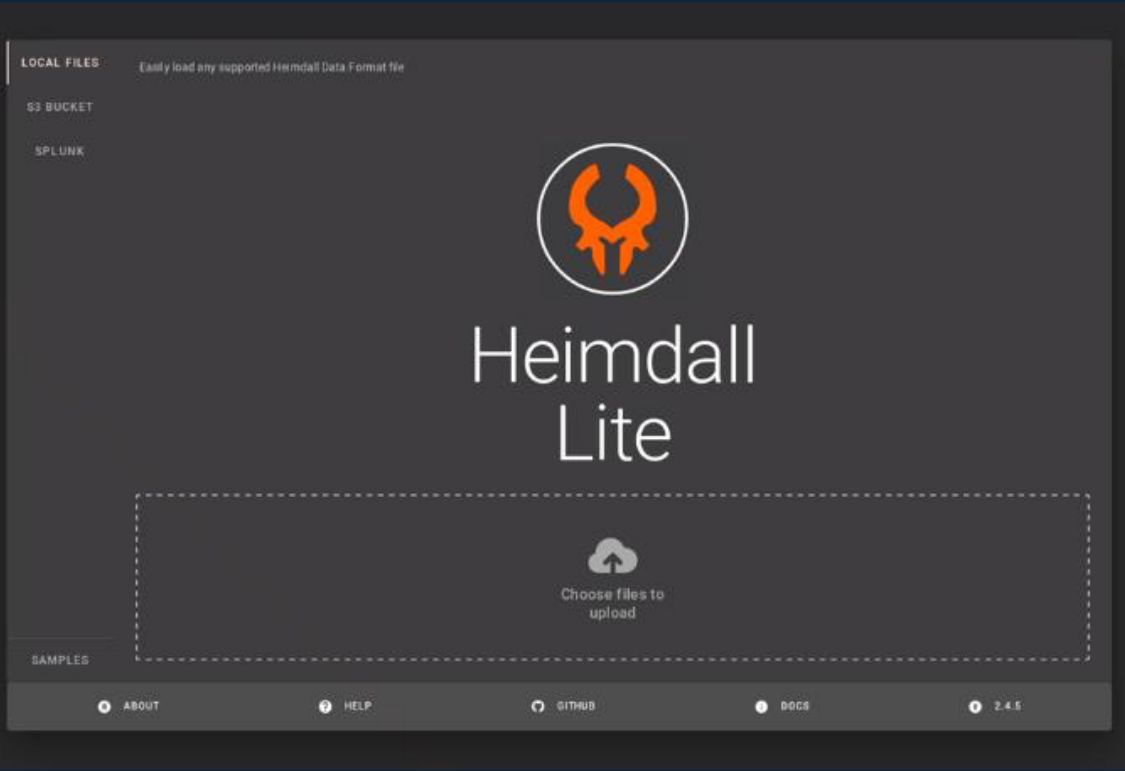
<https://www.open-scap.org/>

<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



Heimdall Demo With Converted SCC Results

Heimdall Test View

Status	Result Set	ID	Impact	Title	800-53 Controls & CCI's
Failed	scc-scan-results.json	V-204509	MEDIUM	The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.	AU-4 (1) CCI-001851
<div> <div>TEST</div> <div>DETAILS</div> <div>CODE</div> </div> <p>Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Off-loading is a common process in information systems with limited audit storage capacity.</p>					
FAILED	Test				

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

Heimdall Code View

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 can 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.



MITRE SAF

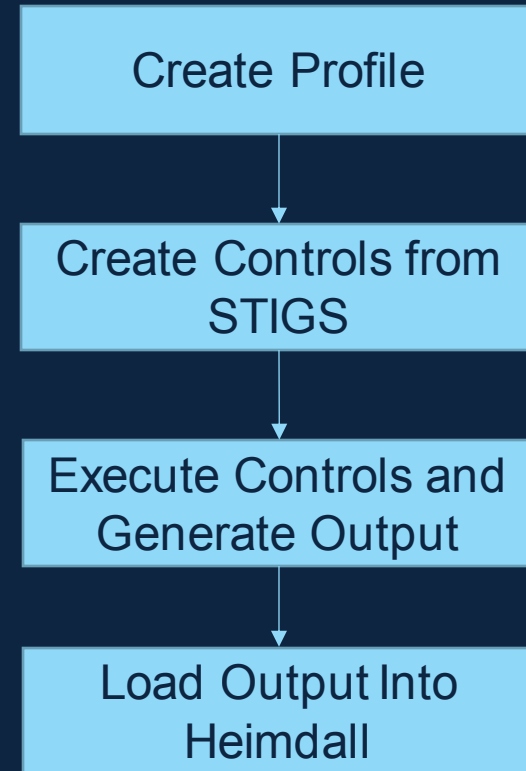


InSpec

Profile – Contains system information such as resource paths

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

Local Machine with InSpec installed



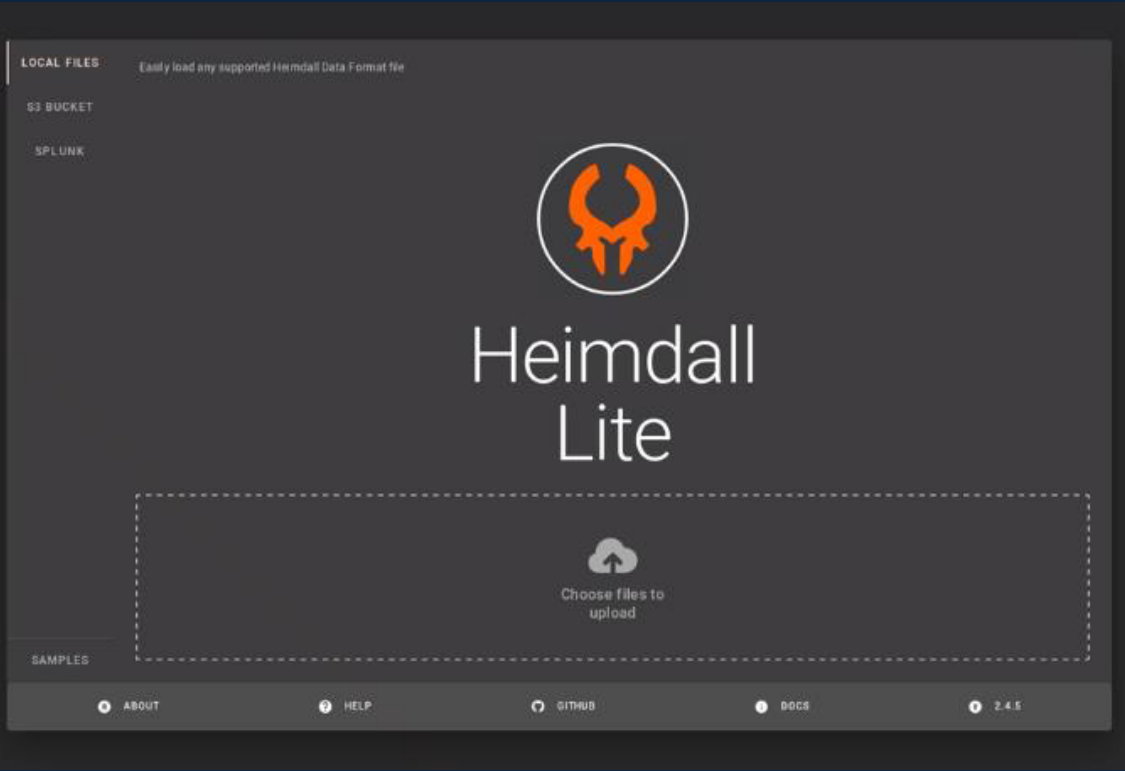
<https://docs.chef.io/inspec/install/>

<https://saf.mitre.org/#/>

<https://heimdall-lite.mitre.org/>

Heimdall Demo With InSpec Results

Heimdall



Heimdall Score



Heimdall Demo With InSpec Results

Heimdall Test View

Failed

inspec-output.json

V-204509

MEDIUM

The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.

AU-4 (1)

CCI-001851

TEST

DETAILS

CODE

Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Off-loading is a common process in information systems with limited audit storage capacity.

Test	Result
<div>FAILED</div> Parse Config File /etc/audit/auditd.conf remote_server is expected to match /^S+\$/	expected nil to match /^S+\$/
<div>PASSED</div> Parse Config File /etc/audit/auditd.conf remote_server is expected not to be in "localhost" and "127.0.0.1"	

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:

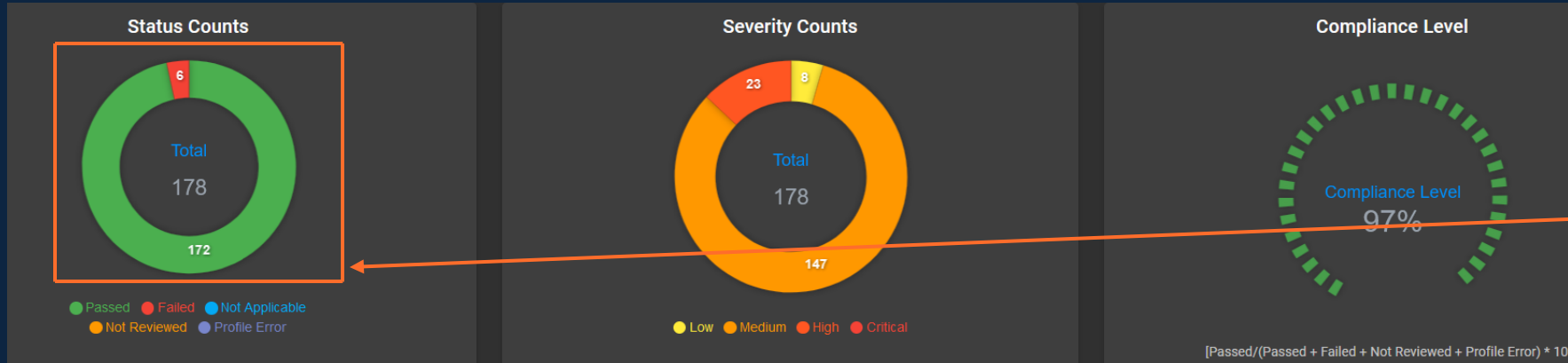
- Being quickly adopted by the defense, intelligence, and vendor communities
- Ever growing library of tools and content
- InSpec profiles:
 - Cover all STIG benchmark checks
 - Quality of the checks are generally better than the SCAP content
 - Content can be easily tailored to meet organizational requirements
 - 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

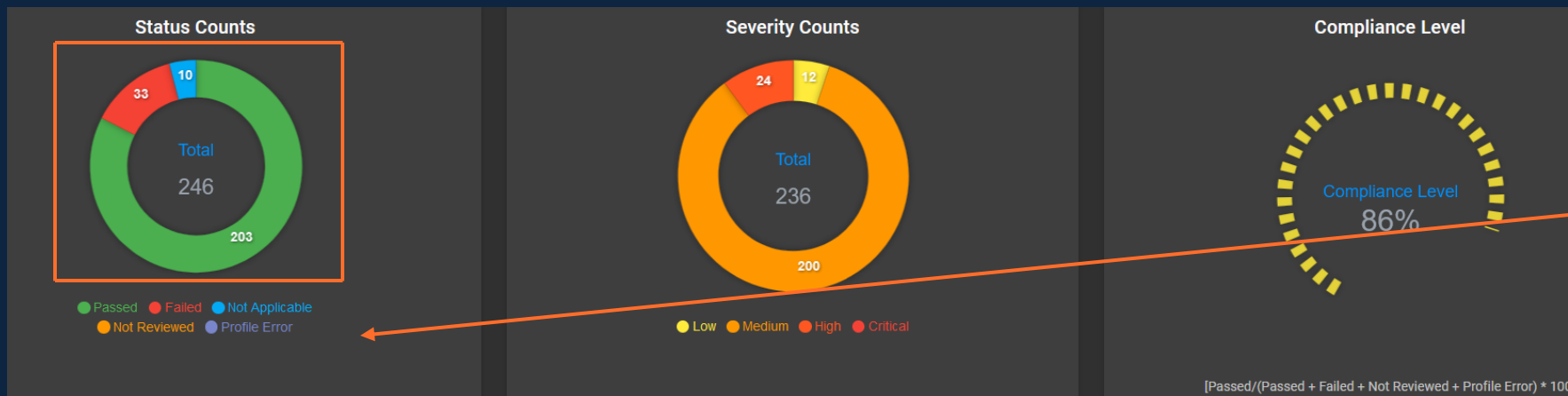
SCAP (SCC)



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

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 ypsserv package installed. - (CCE-27399-5)
15:35:29 - Processing test : oval:mil.disa.stig.rhel7:tst:1310
```

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 login. - (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

Heimdall Demo With InSpec Results

Heimdall Results

Results View Data

Sync TabsSingle ExpandExpand All

Status	Result Set	ID	Impact	Title	800-53 Controls & CCIs	
Home directories are owned by the owner of the home directory.						
Failed	output.json	V-204473	MEDIUM	The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.	CM-6 b	CCI-000366
TESTDETAILSCODE						
If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.						
Test		Result				
FAILED	Home directories with excessive permissions is expected to be empty			expected `["/root/postinstall.log", "/root/.local/share", "/root/.dbus/session-bus/229146b0ce64d746895e401252b0...", "/home/admin/Music", "/home/admin/Pictures", "/home/admin/Videos", "/home/admin/.ssh/known_hosts"].empty?` to be truthy, got false		
Failed	output.json	V-204476	MEDIUM	The Red Hat Enterprise Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.	CM-6 b	CCI-000366
Failed	output.json	V-204498	LOW	The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).	CM-6 b	CCI-000366
Failed	output.json	V-204499	LOW	The Red Hat Enterprise Linux operating system	CM-6 b	CCI-000366

The MITRE Corporation © 2018-2021

Heimdall Results Expanded

Result View (output.json selected)

Search

CLEAR

LOAD

EXPORT

Results View Data

Sync Tabs

Single Expand

Expand All

Status	Result Set	ID	Impact	Title	800-53 Controls & CCIs	
Failed	output.json	V-204392	<div><div></div><div></div><div></div><div></div></div> <div>HIGH</div>	The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.	AU-9	AU-9 (3)
					AC-3 (4)	AC-6 (10)
					CCI-001494	
					CCI-001496	
					CCI-002165	
					CCI-002235	

TEST

DETAILS

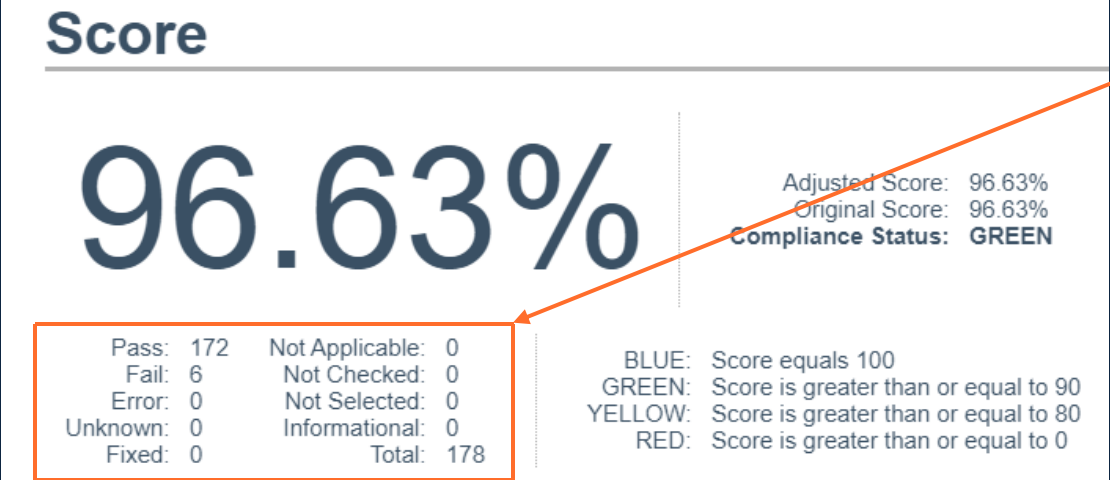
CODE

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Test	Result
["/var/spool/cron", "/etc", "/usr/local", "/usr/local/bin", "/var/lib/etroubleshoot/email_alert_recipients", "/opt/NAI/package/McAfeeVSEForLinux", "/opt/NAI/package/McAfeeVSEForLinux/McAfeeVSEForLinux-2.0.3.29216-installer", "/var/run/libvirt/qemu", "/etc", "/var/lib/PackageKit/transactions.db", "/var/lock/iscsi", "/var/lock/iscsi/lock", "/etc/pam.d", "/etc/security", "/etc/services", "/etc/pki/ca-trust/extracted/java/cacerts", "/etc/pki/ca-trust/extracted/openssl/ca-bundle.trust.crt", "/etc/pki/ca-trust/extracted/pem/email-ca-bundle.pem", "/etc/pki/ca-trust/extracted/pem/objsign-ca-bundle.pem", "/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem", "/etc/snmp/snmpd.conf", "/etc/pam.d", "/etc/security", "/etc/sss/sssd.conf"] is expected to all be in	expected ["/var/spool/cron", "/etc", "/usr/local", "/usr/local/bin", "/var/lib/etroubleshoot/email_alert_recipients", "/etc/snmp/snmpd.conf", "/etc/pam.d", "/etc/security", "/etc/sss/sssd.conf"] to all be in
	object at index 0 failed to match: expected '/var/spool/cron' to be in the list: []
	object at index 1 failed to match: expected '/etc' to be in the list: []
	object at index 2 failed to match: expected '/usr/local' to be in the list: []
	object at index 3 failed to match: expected '/usr/local/bin' to be in the list: []

Output Comparison

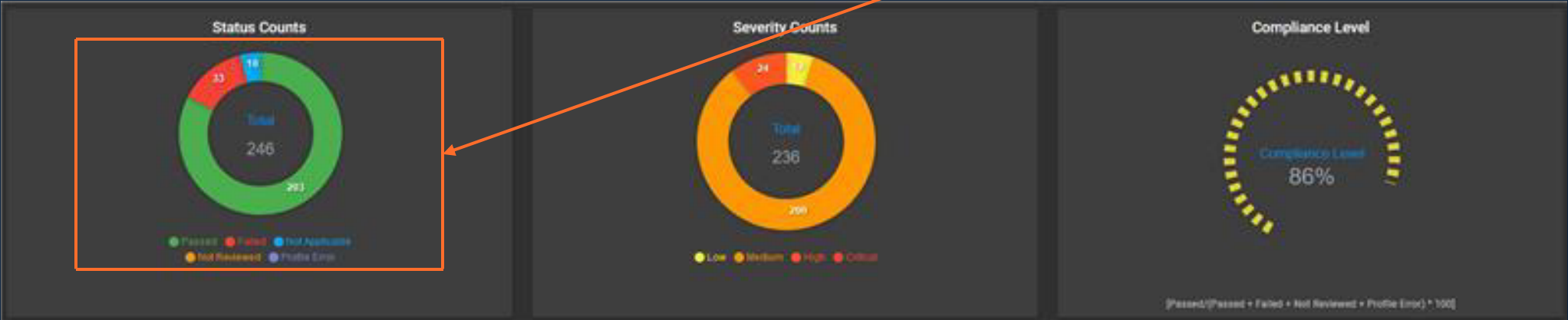
SCAP (SCC)



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



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:	<div>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:<ul style="list-style-type: none">behavior requirements:<ul style="list-style-type: none">ignore_case = truefilepath 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:<ul style="list-style-type: none">check_existence = 'at_least_one_exists', subexpression must match the pattern '^"(aes256-ctr,aes192-ctr,aes128-ctr)"?[\s]*(?:[?#\.])?\$', Collected Item Properties:<ul style="list-style-type: none">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.</div>
--------	--

Heimdall

Passed	output.json	V-204578
<pre>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</pre>		

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