Red Hat Summit

Connect

Hardening at Scale

Apply CIS-Benchmarks efficiently using OpenSCAP, Satellite & Co.

Steffen Frömer

Principal Technical Account Manager
Red Hat

Agenda

What we will focus on?

- Compliance – Quick and Short
- Overview on Tools
- Q&A

Compliance quick and short

What is understood by Compliance?

Compliance refers to the adherence to statutory, regulatory, and internal company requirements. In the context of IT security, **compliance includes measures** that ensure **systems, processes, and data processing** are **in line with defined standards.**

Compliance quick and short

What is understood by Compliance?

Compliance refers to the adherence to statutory, regulatory, and internal company requirements. In the context of IT security, **compliance includes measures** that ensure **systems, processes, and data processing** are **in line with defined standards.**

How does CIS Compliance differ?

CIS Compliance refers to the adherence to the recommendations of the **Center for Internet Security (CIS)**. This organization publishes best practices for securing IT systems in the form of so-called CIS Benchmarks.

Options for Hardening

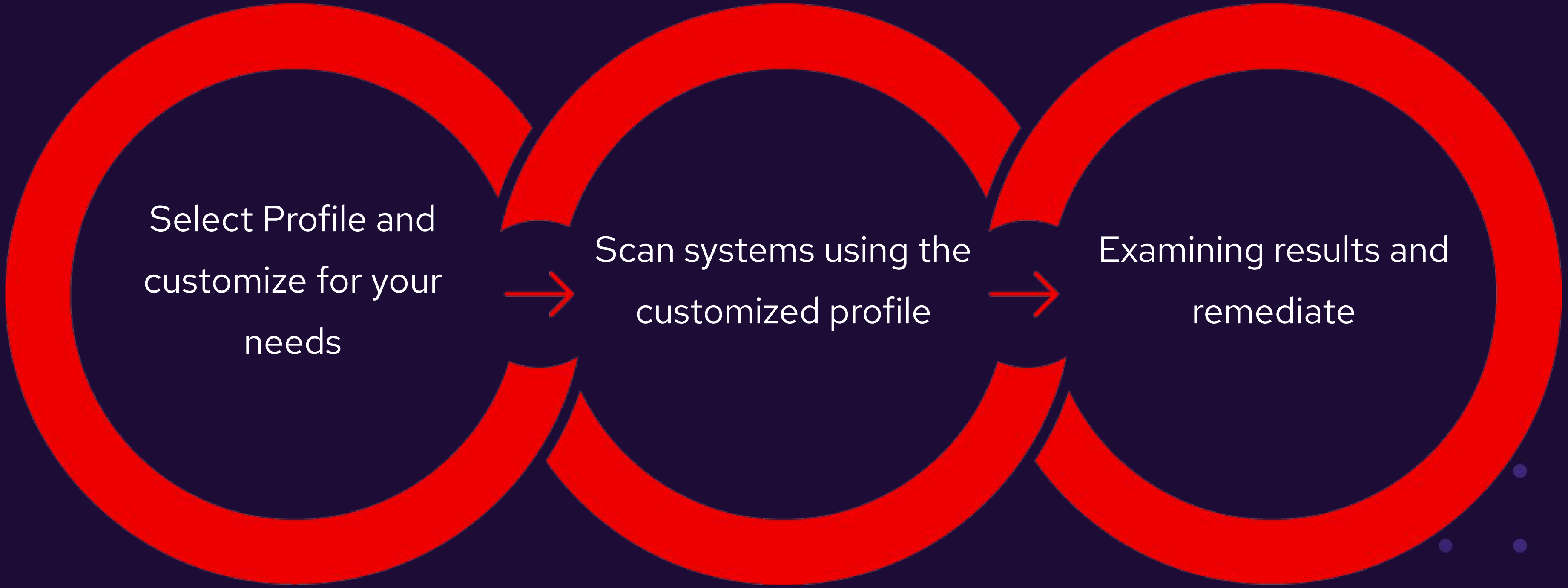
Tool / Method	Description	Used for
SCAP Security Guide (SSG)	Red Hat provides preconfigured security policies in SCAP-Format (z. B. CIS, PCI-DSS, DISA STIG).	Automated checks and hardening
OpenScap	SCAP-Scanner for validation and reporting. CLI-Tool + GUI (optional).	System verification against benchmarks

Options for Hardening

Tool / Method	Description	Used for
SCAP Security Guide (SSG)	Red Hat provides preconfigured security policies in SCAP-Format (z. B. CIS, PCI-DSS, DISA STIG).	Automated checks and hardening
OpenScap	SCAP-Scanner for validation and reporting. CLI-Tool + GUI (optional).	System verification against benchmarks
Ansible + Compliance-as-Code	Automated policy enforcement with preconfigured playbooks.	Enhanced environments with automation
RHEL System Roles: selinux, timesync, firewalld etc.	Ansible system roles for uniform configuration of security-related services.	Automated baseconfiguration
Red Hat ~~Insights~~ Lightspeed (Security Policies)	Cloud-basierte Übersicht über Richtlinienkonformität (CIS, NIST usw.).	Monitoring, Reporting, Alerting
Red Hat Satellite	SCAP profile management, compliance scan scheduling, centralized reporting, and playbook linking for remediation.	Big, centrally managed environment with many hosts
Image Builder with Blueprints	Create preconfigured OS Images with hardening already applied.	Preconfigured, secured deployments

Generic Approach

How compliance is applied to IT systems?



Select Profile and customize for your needs

Scan systems using the customized profile

Examining results and remediate

OpenScap Tailoring

Customizing ruleset according to the needs

What is OpenScap Tailoring?

- enable/disable of specific rules
- Change thresholds (z. B. password length)
- Document your own metadata or reasons for deviations

Source: Customizing SCAP Security Guide

OpenScap Tailoring

Customizing ruleset according to the needs

What is OpenScap Tailoring?

- enable/disable of specific rules
- Change thresholds (z. B. password length)
- Document your own metadata or reasons for deviations

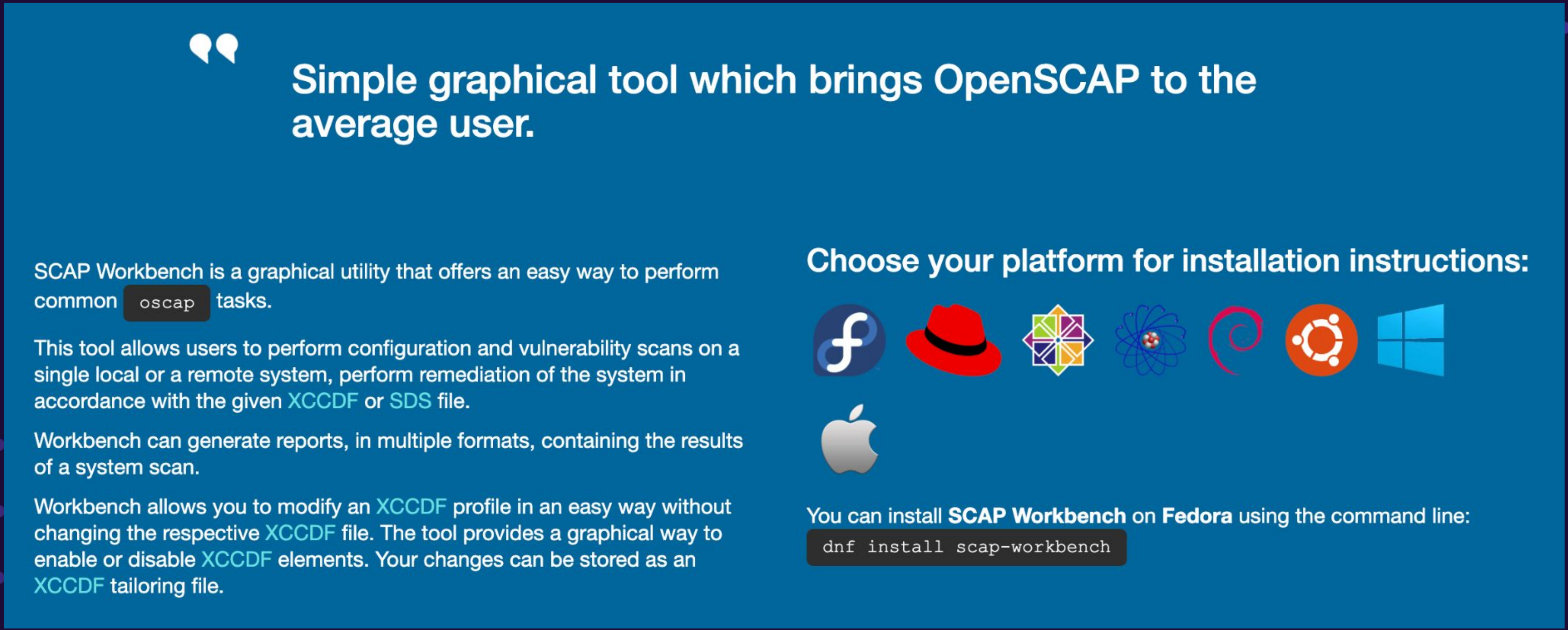
How to proceed?

- get and start SCAP Workbench

Source: Customizing SCAP Security Guide

Scap Workbench

Customizing rules according to the need



> Simple graphical tool which brings OpenSCAP to the average user.

SCAP Workbench is a graphical utility that offers an easy way to perform common `oscap` tasks.

This tool allows users to perform configuration and vulnerability scans on a single local or a remote system, perform remediation of the system in accordance with the given XCCDF or SDS file.

Workbench can generate reports, in multiple formats, containing the results of a system scan.

Workbench allows you to modify an XCCDF profile in an easy way without changing the respective XCCDF file. The tool provides a graphical way to enable or disable XCCDF elements. Your changes can be stored as an XCCDF tailoring file.

Choose your platform for installation instructions:

You can install **SCAP Workbench** on **Fedora** using the command line:

```
dnf install scap-workbench
```

[Scap Workbench Project Page]

OpenScap Tailoring

Customizing ruleset according to the needs

What is OpenScap Tailoring?

- enable/disable of specific rules
- Change thresholds (z. B. password length)
- Document your own metadata or reasons for deviations

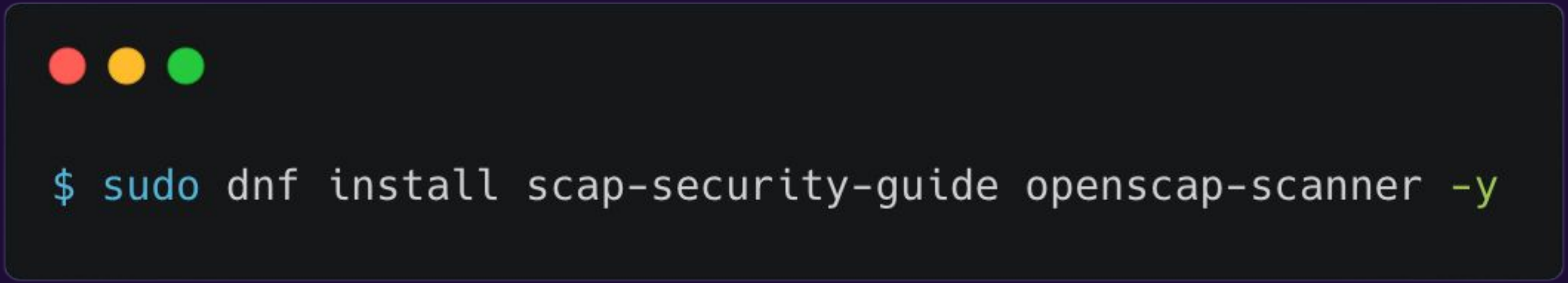
How to proceed?

- get and start SCAP Workbench
- Select target system and profile
- Apply customizations
- export Tailoring file for further usage

Source: Customizing SCAP Security Guide

SCAP Security Guide & OpenScap

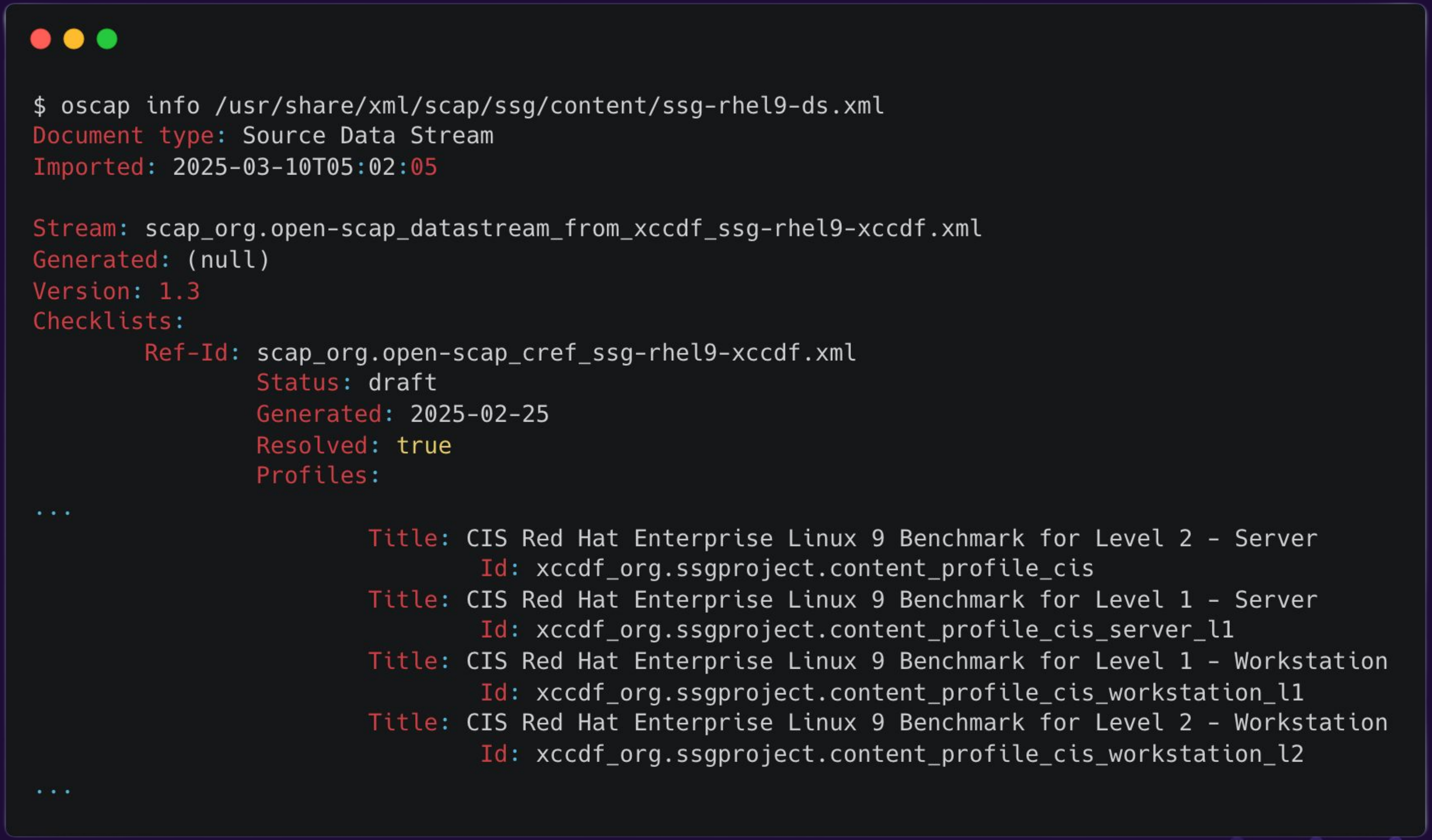
Applying compliance to systems – the basics in practice



```
$ sudo dnf install scap-security-guide openscap-scanner -y
```

SCAP Security Guide & OpenScap

Applying compliance to systems – the basics in practice

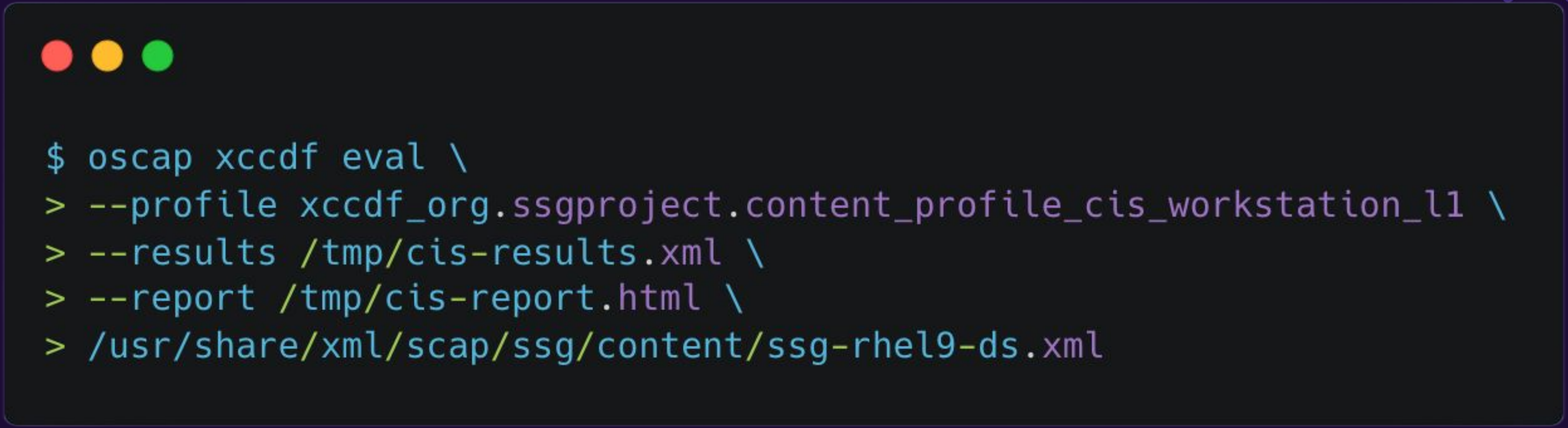


```
$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
Document type: Source Data Stream
Imported: 2025-03-10T05:02:05

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel9-xccdf.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel9-xccdf.xml
                Status: draft
                Generated: 2025-02-25
                Resolved: true
                Profiles:
...
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Server
                                Id: xccdf_org.ssgproject.content_profile_cis_server_l1
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l1
                        Title: CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Workstation
                                Id: xccdf_org.ssgproject.content_profile_cis_workstation_l2
...
```

SCAP Security Guide & OpenScap

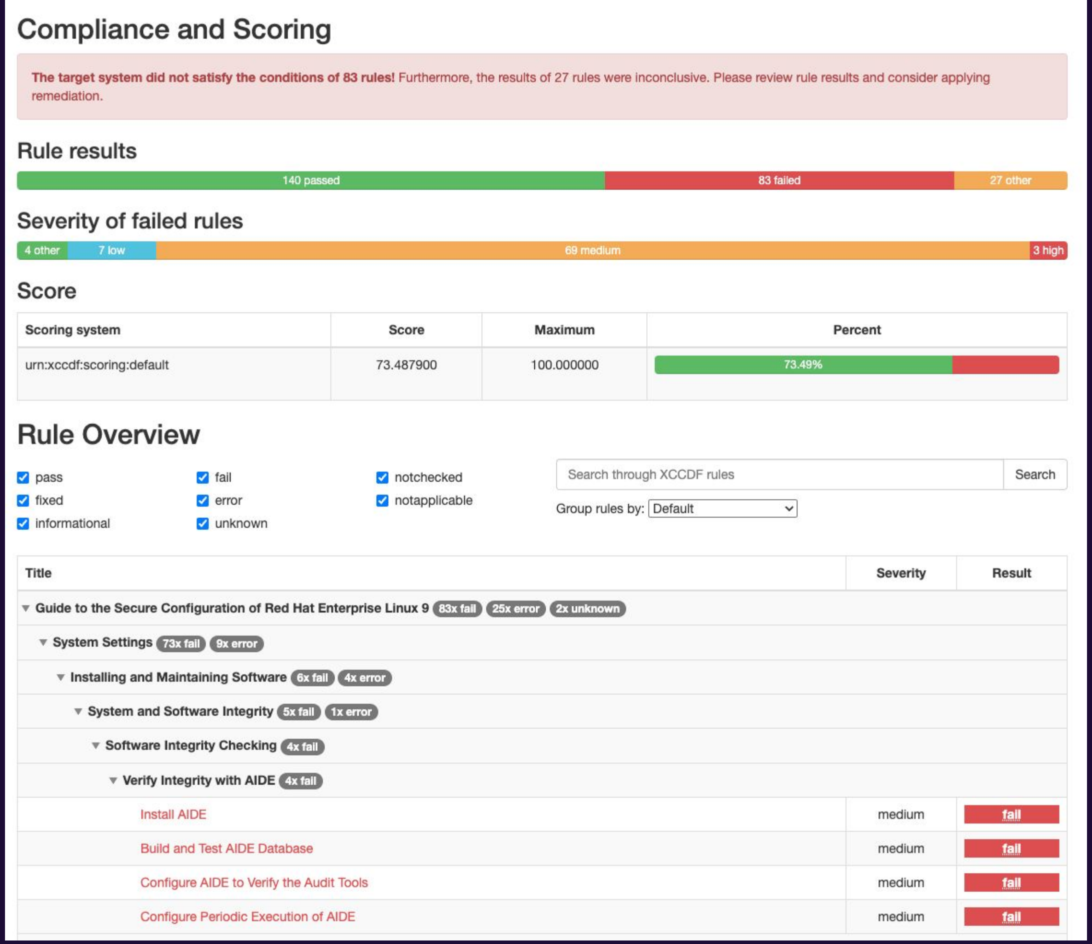
Applying compliance to systems – the basics in practice



```
$ oscap xccdf eval \
> --profile xccdf_org.ssgproject.content_profile_cis_workstation_l1 \
> --results /tmp/cis-results.xml \
> --report /tmp/cis-report.html \
> /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml
```

SCAP Security Guide & OpenScap

Applying compliance to systems – the basics in practice



Compliance and Scoring

The target system did not satisfy the conditions of 83 rules! Furthermore, the results of 27 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	73.487900	100.000000	73.49%

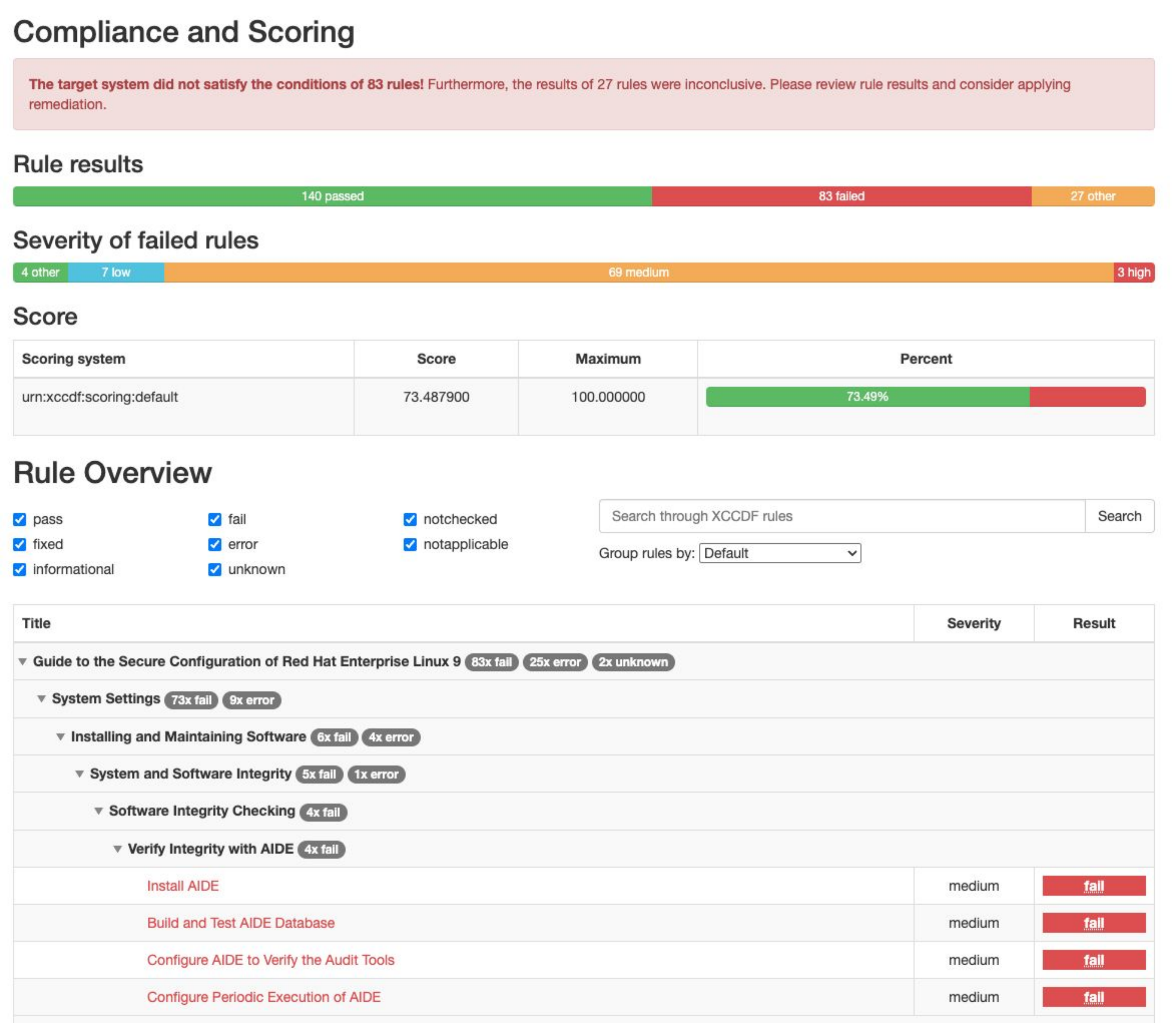
Rule Overview

☑ pass
☑ fixed
☑ informational
☑ fail
☑ error
☑ unknown
☑ notchecked
☑ notapplicable

Search through XCCDF rules | Search

Group rules by: Default

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 9 83x fail 25x error 2x unknown		
▼ System Settings 73x fail 9x error		
▼ Installing and Maintaining Software 6x fail 4x error		
▼ System and Software Integrity 5x fail 1x error		
▼ Software Integrity Checking 4x fail		
▼ Verify Integrity with AIDE 4x fail		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure AIDE to Verify the Audit Tools	medium	fail
Configure Periodic Execution of AIDE	medium	fail



Compliance and Scoring

The target system did not satisfy the conditions of 83 rules! Furthermore, the results of 27 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

140 passed | 83 failed | 27 other

Severity of failed rules

4 other | 7 low | 69 medium | 3 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	73.487900	100.000000	73.49%

Rule Overview

☑ pass
☑ fixed
☑ informational
☑ fail
☑ error
☑ unknown
☑ notchecked
☑ notapplicable

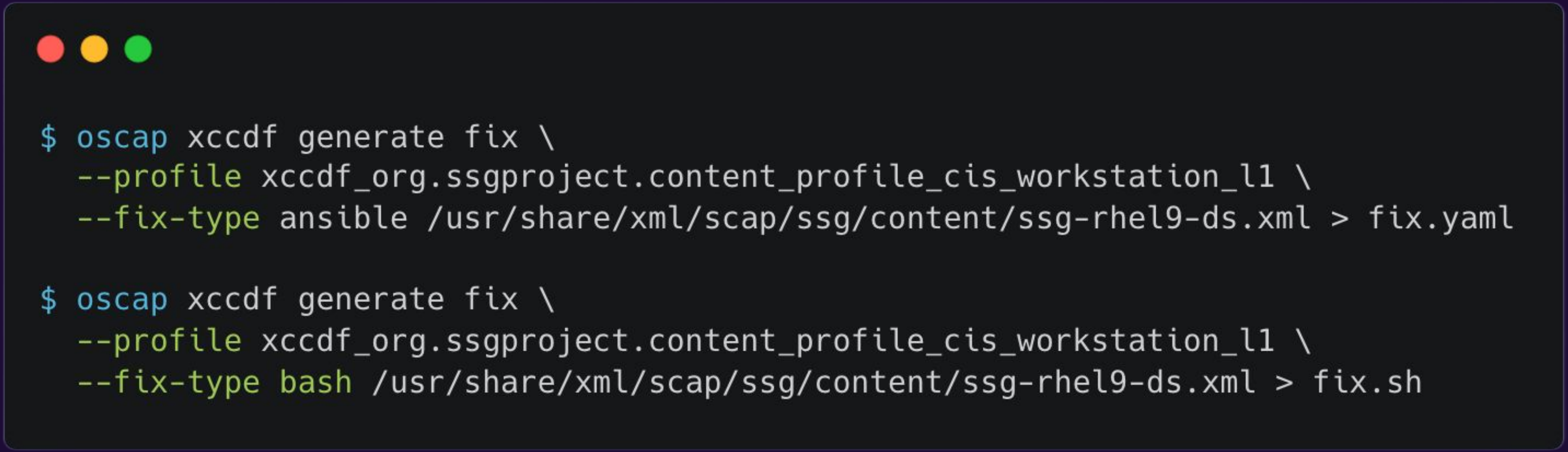
Search through XCCDF rules | Search

Group rules by: Default

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 9 83x fail 25x error 2x unknown		
▼ System Settings 73x fail 9x error		
▼ Installing and Maintaining Software 6x fail 4x error		
▼ System and Software Integrity 5x fail 1x error		
▼ Software Integrity Checking 4x fail		
▼ Verify Integrity with AIDE 4x fail		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure AIDE to Verify the Audit Tools	medium	fail
Configure Periodic Execution of AIDE	medium	fail

SCAP Security Guide & OpenScap

Applying compliance to systems – the basics in practice



```
$ oscap xccdf generate fix \
  --profile xccdf_org.ssgproject.content_profile_cis_workstation_l1 \
  --fix-type ansible /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml > fix.yaml

$ oscap xccdf generate fix \
  --profile xccdf_org.ssgproject.content_profile_cis_workstation_l1 \
  --fix-type bash /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml > fix.sh
```

Red Hat Satellite

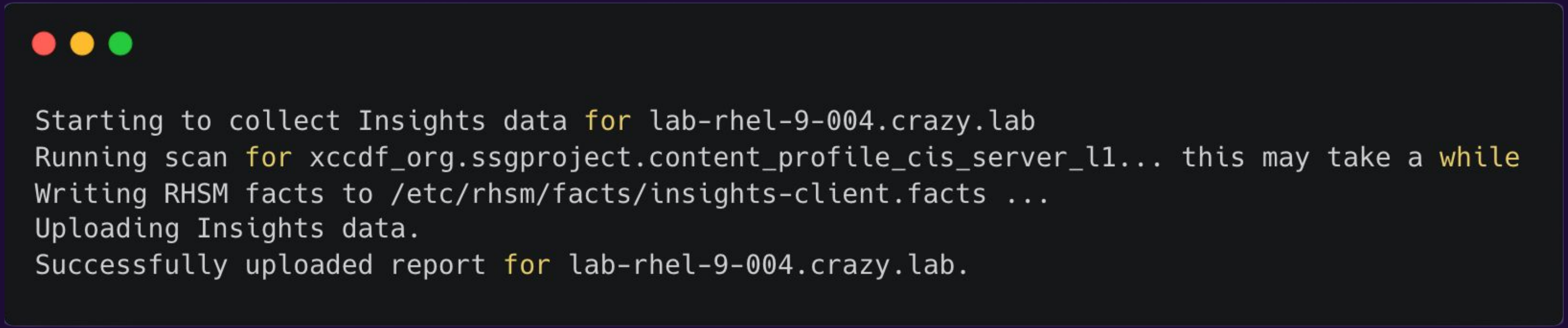
Control center in our own data center

- Distribution and management of SCAP content
- Scheduled audit execution
- Central storage of scan reports
- Automated hardening (via linked Ansible playbooks)

Red Hat ~~Insights~~ Lightspeed

SaaS - mostly everything built-in

~~Insights~~ Lightspeed offers an out-of-the-box solution for creating compliance reports and generating remediation workflows.



```
Starting to collect Insights data for lab-rhel-9-004.crazy.lab
Running scan for xccdf_org.ssgproject.content_profile_cis_server_l1... this may take a while
Writing RHSM facts to /etc/rhsm/facts/insights-client.facts ...
Uploading Insights data.
Successfully uploaded report for lab-rhel-9-004.crazy.lab.
```

Image Builder with Blueprints

Standalone, in Satellite, in Hybrid Cloud console or via API

The Image Builder offers the option of creating pre-built and hardened operating system images that can be used to deploy a system.

- standardized configurations
- Compliant from the very beginning
- Blueprints can be transferred to new operating system versions

Q&A

„Compliance is the evidence that security is happening.“

– Unbekannter IT-Security-Experte

Jetzt Session bewerten!

Einfach QR-Code scannen, Session aus der Liste wählen und bewerten. **Vielen Dank!**

red.ht/rhsc-darmstadt-feedback

Red Hat
Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat