Red Hat Summit

Connect

Beyond Installation

Automating continuous compliance and security hardening in Red Hat Enterprise Linux

Stockholm

2026-11-11

Red Hat

Speakers





Alessandro Rossi

RHEL Advocate

alerossi@redhat.com

Sam “the TAM” Wachira

Principal Technical Account Manager, RHEL

samthetam@redhat.com

Red Hat

What we'll discuss today

- ⇒ Why continuous security and compliance are essential
- ⇒ About OpenSCAP and the security content it provides
- ⇒ Integrating OpenSCAP with Ansible Automation Platform (AAP)
- ⇒ Compliance workflows: image scanning, remediation, and reporting
- ⇒ Key takeaways and known limitations



The need for a Framework and Automation



The Core Problem

01

Different individuals and teams build systems differently

02

Baselines changes with every version update

03

Custom rule sets become unmanageable

04

Reactive fixes slow everything down



Why You Should Care



Compliance Drift

Compliance drifts fast and is prone to human errors.

Scalability Limits

Manual checks don’t scale well in large environments.

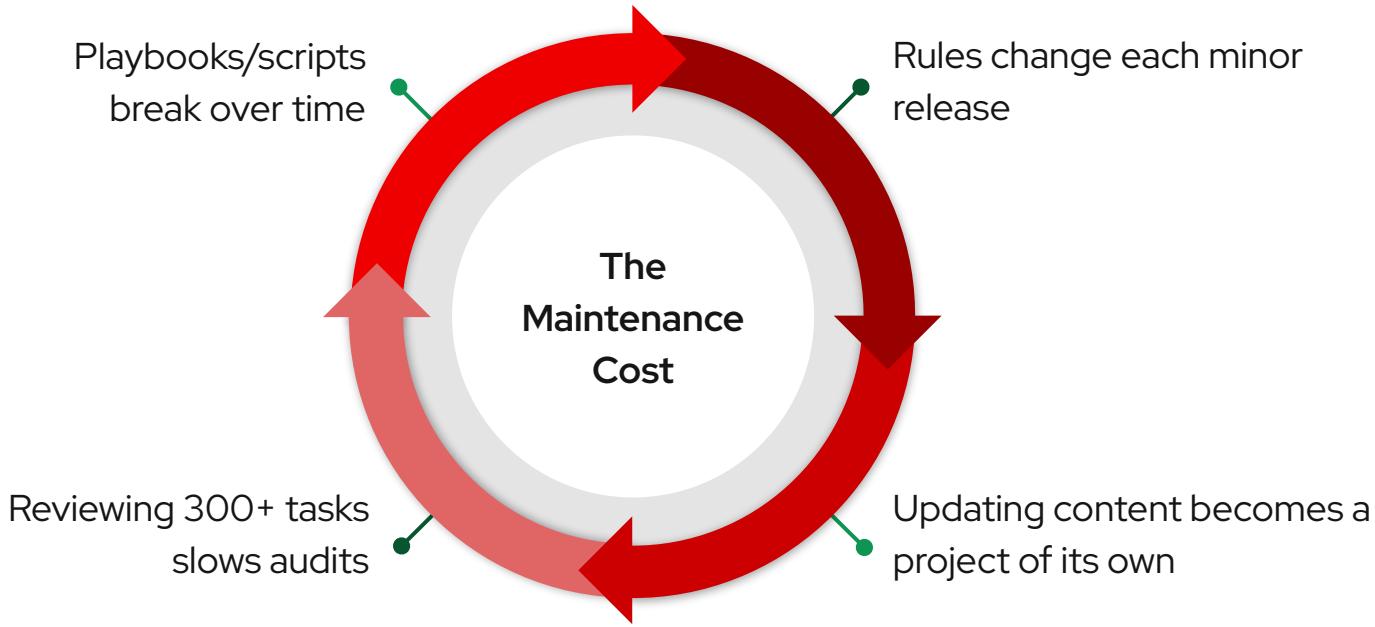
Audit Expectations

Auditors expect proof, not intent.

Continuous Enforcement

Requirement of continuous, consistent enforcement.

Manual rule writing is painful



Day-2 pain points with large infrastructure

Security and compliance are non-negotiable for enterprise-scale financial operations



Customers have

- 10,000+ managed hosts
- Executing server provisioning workflows daily
- Performing weekly and monthly refreshes of provisioning images
- Validating and updating compliance baselines across emerging OS versions on a regular basis

This results to

- Cumbersome Day 2 maintenance
- Security remediations are performed host-by-host, increasing the risk of human error

Achieving Continuous Compliance with OpenSCAP



SCAP (Security Content Automation Protocol)



WHAT IT IS & PURPOSE

A standardized framework of specifications that enables automated assessment of system security, vulnerability management, and policy compliance.

Implements the SCAP standard used globally for consistent enterprise security baselines and audits.

WHAT IT DELIVERS

Machine-Readable Content

STIG, PCI-DSS, CIS-style rules, and RHEL hardening profiles.

Automated Auditing

Generates consistent, scalable scan results and automated reports across the fleet.

COMPONENTS & TOOLS

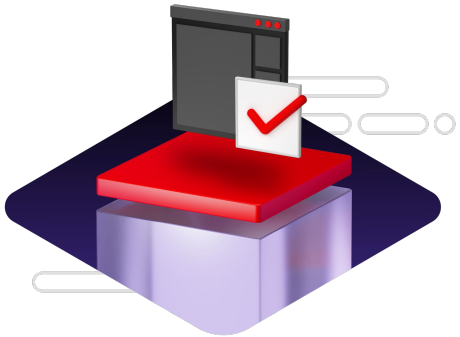
Key Standards

XCCDF for checklists & **OVAL** for automated XML-based vulnerability checks.

Supported Ecosystem

OpenSCAP, Red Hat Lightspeed & Satellite, Tenable, Qualys, and CIS-CAT.

OpenSCAP: Scanning remote systems, VMs, containers



ADVANCED SCANNING & PURPOSE

OpenSCAP provides utilities built on top of oscap for advanced scanning use cases.

Content maintained and updated by Red Hat and community.

These tools simplify scanning with single commands, without changing core OpenSCAP behavior.

UTILITIES & PACKAGES

Easy Installation
Available via the **openscap-utils** package.

Supported Utilities
oscap-ssh, oscap-vm, oscap-podman, oscap-docker

Standard Structure
Removes guesswork - no need to write ~350 CIS tasks manually

Reporting
Auditor-friendly reporting built-in.

SCAP Security Guide (SSG) is developed and maintained under the **ComplianceAsCode** project.

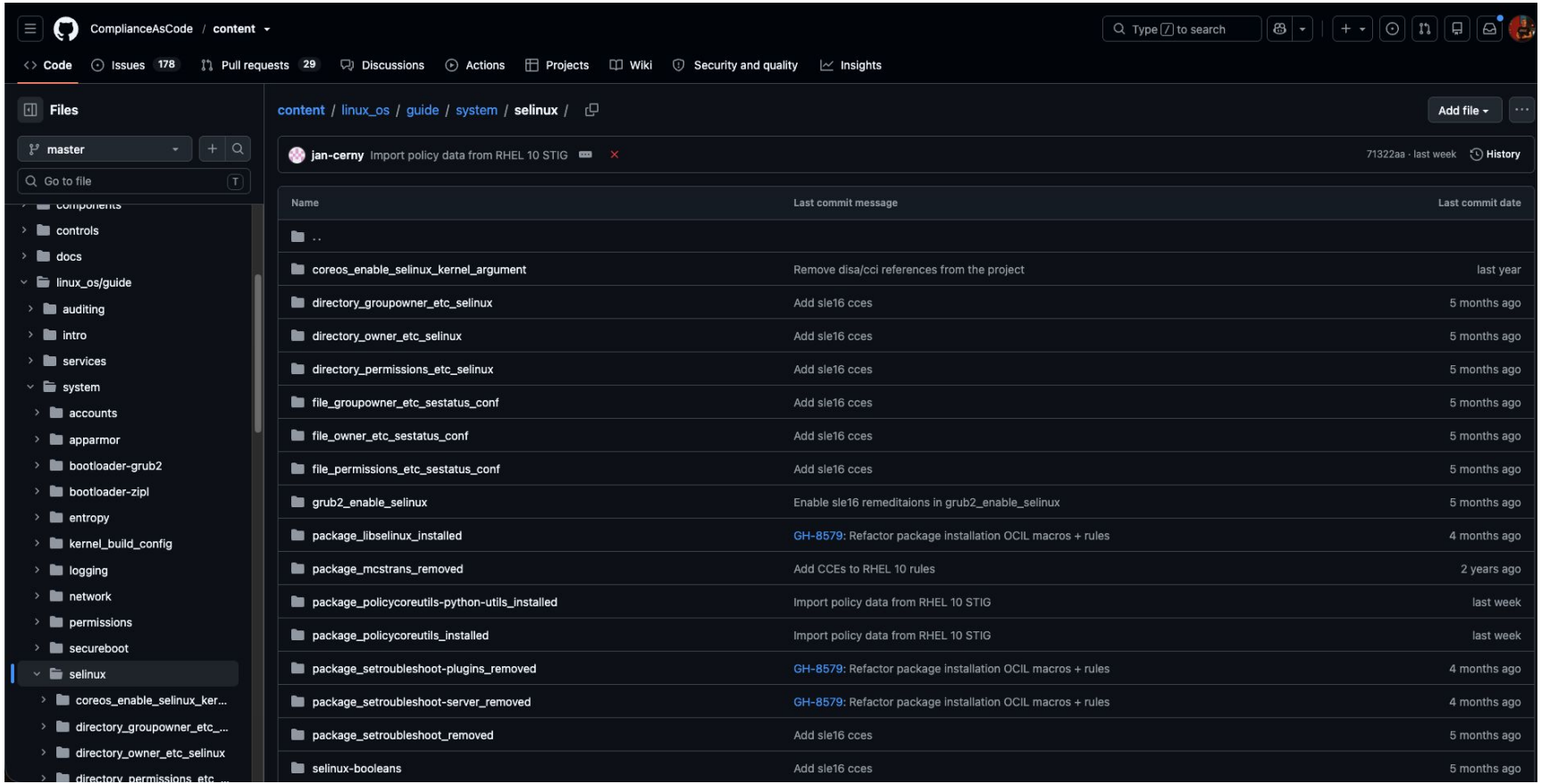
Explore the Repository

Access the source code, open issues, and submit your pull requests on GitHub:

github.com/ComplianceAsCode/content

Contributions welcome

Help improve the project by contributing bug fixes, updates, and new compliance rules.



github.com/ComplianceAsCode/content

Modular Directory Structure

Structured Path

Rules are logically organized by OS, guide section, and specific subsystems (e.g., **`system/selinux`**).

Modular Rules

Individual folders isolate policy checks for package installation, service states, and file permissions into manageable pieces.

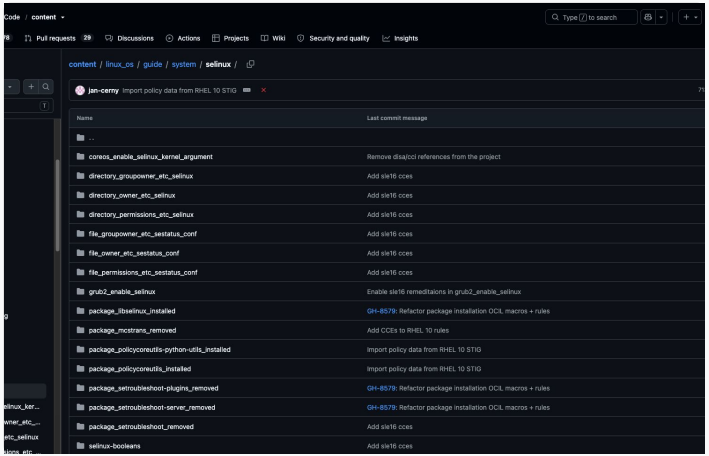
Open Repository

The codebase is open for public collaboration on GitHub, making security policy maintenance transparent.

`github.com/ComplianceAsCode/content`

GitHub Repository Path

`linux_os/guide/system/selinux`



XCCDF and profiles

The XCCDF Standard

eXtensible Configuration Checklist Description Format. A language to express, organize, and manage security policies. It serves as the core building block of SCAP compliance.

ComplianceAsCode Repo

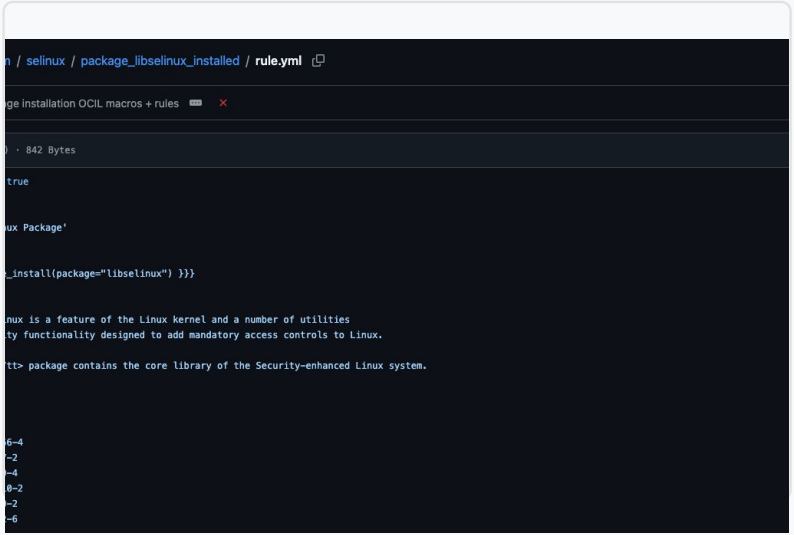
Rules are not stored in one massive, unmanageable XML file. Instead, they are completely modularized on GitHub.

YAML to XML Compilation

Rules exist as small, structured YAML files, which compiled tools build into the final XCCDF XML (**`ssg-*-ds.xml`**) files.

Source File Structure

`rule.yml`



OpenSCAP integrations



OpenSCAP in General

```
# Installing OpenSCAP and SCAP content
$ dnf install openscap-scanner scap-security-guide

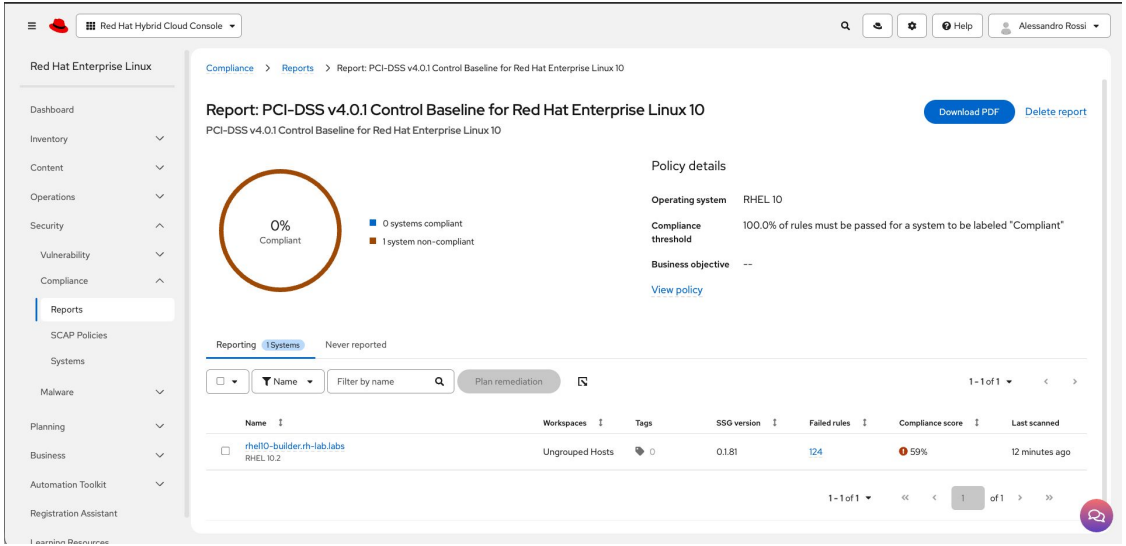
                        # Displaying information about SCAP source data streams
                        $ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel10-ds.xml

        # Audit
        $ oscap xccdf eval \
            --profile xccdf_org.ssgproject.content_profile_rht-ccp \
            --results ssg-rhel10-xccdf-result.xml \
            --report ssg-rhel10-report.html \
            /usr/share/xml/scap/ssg/rhel10/ssg-rhel10-ds.xml
```




Compliance scanning and remediation

Red Hat Lightspeed



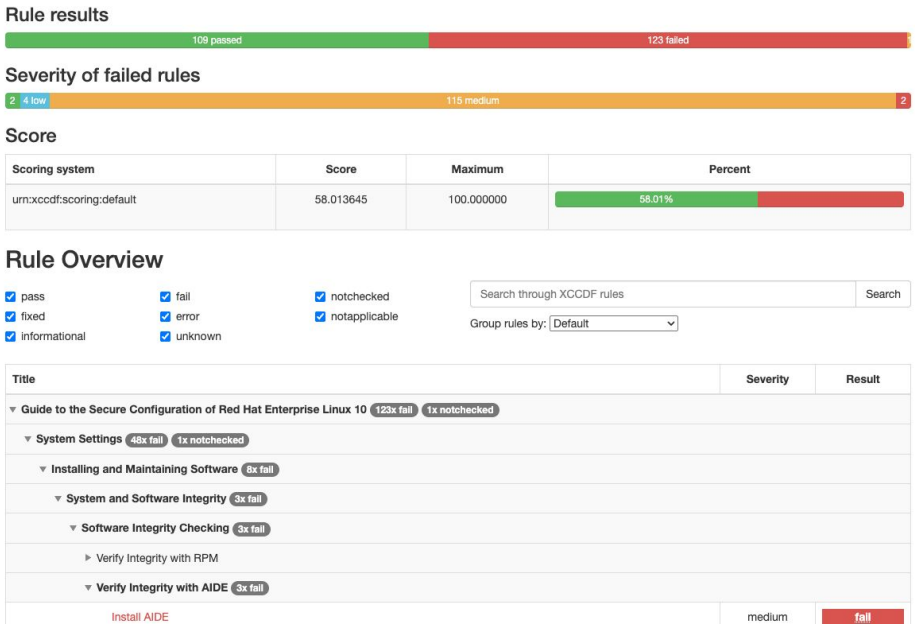
- Create policies
- Perform configuration scans on RHEL systems to validate compliance
- Automatically remediate systems that have been found in a non-compliant state
- Deploy already-compliant systems with Image Builder's pre-hardened images.
- Disconnected offering via Red Hat Satellite planned*

Live demo

Red Hat

Compliance scanning and remediation

Red Hat Satellite



- OpenSCAP plugin enabled by default in Satellite server.
- Use XCCDF profiles from SCAP content and tailoring files (customisations) to define compliance policies.
- Scanner evaluates hosts against the rules and generates report - Asset Reporting Format (ARF) displayed in Satellite UI.
- Automatically remediate systems that have been found in a non-compliant state

Red Hat

OpenSCAP and Ansible

```
# Remediation playbook
$ oscap xccdf generate fix \
   --profile ospp \
   --fix-type ansible
   /usr/share/xml/scap/ssg/content/ssg-rhel10-ds.xml > playbook.yml

        $ ansible-playbook -i inventory remediation.yml

                # Post-Remediation Evaluation:
                $ oscap xccdf eval \
                     --profile xccdf_org.ssgproject.content_profile_cis_level1_server \
                     --results post-remediation.xml \
                     /usr/share/xml/scap/ssg/content/ssg-rhel10-ds.xml
```




Generic fix content or per system

Generate content centrally and use for several systems

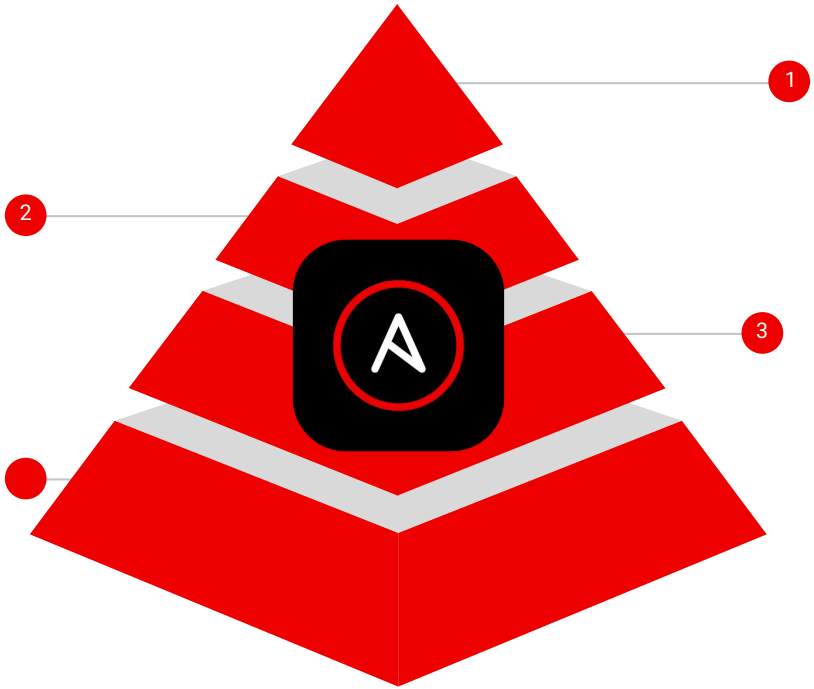
OpenSCAP is used only for centralized remediation playbook generation; managed nodes require no OpenSCAP installation.

Audit and generate content per system

OpenSCAP should be available on target hosts



OpenSCAP + Ansible Automation Platform



Fits into CI/CD, pipelines, and image builds for repeatable and automated workflows

Fleet-wide scans or targeted checks. Integration with SIEM, ticketing, dashboards

AAP drives scheduling, orchestration, scale, drift detection and auto-remediation

OpenSCAP provides rules and remediation

Automating compliance workflows



Compliance Workflow

01
Build & Scan

Build system → image scan → remediate

Scan the base image during build to catch issues early.

Apply automated remediations so only compliant images move forward.

02
Deploy & Monitor

Deploy → scheduled scan → drift fix

Run recurring scans on deployed systems to detect drift.

Trigger targeted fixes to bring systems back to the expected baseline.

03
Report & Audit

Push reports → dashboard or SIEM

Send structured results to Lightspeed, Splunk, or any SIEM.

Make compliance visible and auditable across teams.

04
Alert & Resolve

Create tickets automatically on failures

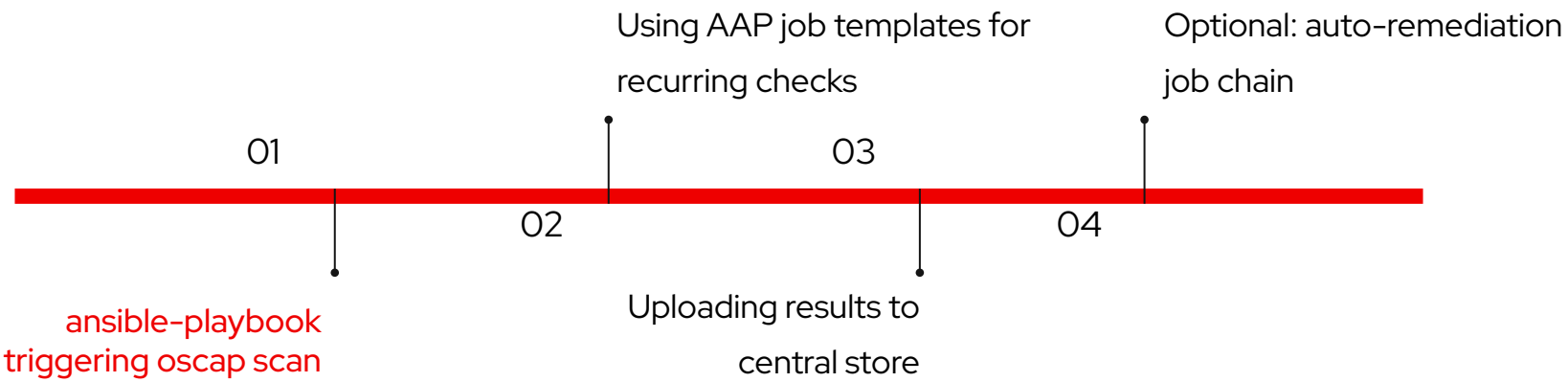
Open tasks in JIRA, ServiceNow when rules fail.

Give Ops teams a clear workflow to resolve and track issues.



Basic implementation

High Level



Real Use Cases

Baseline enforcement for RHEL fleets

Apply a consistent security baseline across thousands of systems.

Catch deviations early before they grow into exposure.

Hardened golden images for cloud or on-prem

Bake compliant images during build time with repeatable checks.

Ensure every new instance starts from a trusted, approved state.

Continuous compliance for regulated environments

Meet guidelines like **PCI**, **DISA STIG**, and **CIS** without manual effort.

Provide auditors with clear, automated evidence.

Drift control for large distributed teams

Monitor and correct configuration drift across mixed environments.

Keep systems aligned even when many hands manage them.



Typical Customer Scenario

The Challenge

Audits were manual, taking 80+ hours per month to prepare and execute.

Compliance drift resulted in a 40% failure rate on random quarterly checks.

The Solution: Compliance-as-Code

Implement OpenSCAP to define standardized, machine-readable security policies.

Deploy Red Hat Ansible Automation Platform (AAP) for automated, scheduled fleet-wide scans and zero-touch auto-remediation.

Integrate AAP with their existing SIEM for real-time compliance visibility.

Quantifiable Results

Reduce Time to Compliance: Audit preparation time drop from 80 hours to under 4 hours (a 95% reduction).

Improve Consistency: Achieve a 99.5% compliance rate across all RHEL environments.

Accelerate Remediation: Detect and fixed compliance drift in less than 30 minutes instead of days.



Known Limitations of OpenSCAP

Content Type	Examples	Source of Truth
Enterprise Linux	RHEL, CentOS Stream	Red Hat (Official)
Community Linux	Ubuntu, Debian, SLES	Community (ComplianceAsCode)
Cloud-Specific	Amazon Linux, Google Cloud OS	Cloud Vendor / Community
Applications	Firefox, JRE, Chromium	Community
Windows	Windows 10/11, Server 2022	**NIST / DISA / CIS (Not SSG)**

- Windows support removed
- Some CIS rules don’t map 1:1 to SCAP
- Remediation strongest on RHEL
- Reports may need normalization



Key Takeaways

01

Continuous Compliance

Ensure hardening and compliance configurations are monitored in real-time.

02

Simplified Rules and Reporting

OpenSCAP streamlines complex policy definitions into repeatable rules and generates actionable reports.

03

Automation at scale

Leverage Ansible to automate remediation and enforce policies across your entire RHEL fleet.

04

Unified Posture

Combine these tools to achieve a highly resilient and enforceable compliance state.



Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 x.com/RedHat

Red Hat