

CIS LEVEL 1 + LEVEL 2 + CUSTOM POLICY

A scan. A clear finding. A verified recheck.

A real lab assessment showing what your IT team receives and how a follow-up scan confirms a fix. This sample uses one dedicated Rocky Linux 9.8 virtual machine, labeled **LAB-01**.

What the scans found

Assessment	Stage	Pass	Fail	N/A	Errors
CIS Level 1 Server	Initial	150	110	35	0
CIS Level 1 Server	Recheck	152	108	35	0
CIS Level 2 Server	Initial	170	195	36	0
CIS Level 2 Server	Recheck	172	193	36	0

Level 1 selected 295 rules; Level 2 selected 401. N/A means not applicable on this machine and is not counted as a pass. Rules outside the selected profile are excluded. No selected checks returned an execution error or an unreviewed result in these runs.

Five checks for a custom policy

Example policy	Initial	Recheck
Passed controls	3	5
Failed controls	2	0

What improved: two CIS banner findings passed on recheck in both profiles. Two custom findings also passed after the agreed notice and file-permission fixes.

What remains: 108 Level 1 findings and 193 Level 2 findings still fail. This was a limited remediation demonstration, not a fully hardened server. Level 2 is a different profile; compare each recheck with its own initial scan.

SELECTED FINDINGS AND FOLLOW-UP

A useful report tells IT what to do next.

These low-disruption fixes were applied only to the dedicated lab VM. Priorities below are analyst workflow priorities, not vulnerability severity scores.

01 Local login banner reveals system details

CIS Level 1 and Level 2: banner_etc_issue_cis

Initial result: fail. /etc/issue contained operating-system information.

IT action: Replace it with the agreed notice, removing OS/version tokens. In the lab: Authorized access only. Activity may be monitored.

Verification: Recheck: pass in both profiles. The custom approved-notice check also changed from fail to pass.

02 Network login banner reveals system details

CIS Level 1 and Level 2: banner_etc_issue_net_cis

Initial result: fail. /etc/issue.net contained operating-system information.

IT action: Replace that file's contents with the agreed notice. Banner content and configuring SSH to display it are separate checks.

Verification: Recheck: banner-content rule passed in both profiles. The separate SSH warning-banner configuration finding remains open.

03 Example policy file is readable by other users

Custom policy: sos-policy-file-01

Initial result: fail. The demonstration file had mode 0644 instead of the agreed 0600.

IT action: Set /etc/sos-demo-policy.conf to mode 0600. Confirm root ownership and check that the intended service can still read it.

Verification: Recheck: pass. The file's root ownership and environment tag checks also passed.

Suggested next work: review the remaining failed rules with the system owner, agree changes and exceptions, test application impact, and rerun the same profile. These selected fixes demonstrate the process; they are not the highest-priority risks on every server.

SCOPE, EVIDENCE AND NEXT STEPS

Clear scope. Traceable results.

What was exercised

- 1. Ran the stock Level 1 Server and Level 2 Server profiles, each with the same five custom controls.
- 2. Bundled results, calculated SHA-256 hashes, and uploaded through SFTP.
- 3. Verified and ingested all four scan sessions into the baselineX collector.
- 4. Applied the three file changes described on page 2 and reran both profiles.
- 5. Checked database results, scan history, the dashboard, and Excel exports.

Component	Verified lab configuration
Operating system	Rocky Linux 9.8, x86_64, dedicated KVM guest
OpenSCAP	1.3.14
Security content	scap-security-guide-0.1.82-2.el9_8.rocky.1.1
Datastream	ssg-rl9-ds.xml
Cinc Auditor	7.2.1
Custom policy	sos-demo-policy 1.0.0

The Rocky datastream identifies the CIS Red Hat Enterprise Linux 9 Benchmark v2.0.0 (June 20, 2024), adapted for Rocky Linux. Content release 0.1.82 is the security-content version, not a claim of CIS certification. Exact OS, content, profile, and benchmark scope are agreed before client work.

What this sample does not establish

This demonstrates one OS version and one lab environment. It is not a test of every supported platform, a vulnerability scan, penetration test, regulatory audit, or certification. Automated configuration checks do not replace evidence review or application testing. The five custom requirements are examples, not a client's policy.

What your engagement includes

Your agreed initial package includes the first assessment, reviewed findings and an Excel summary, plus one follow-up scan within 30 days of the report. Your IT team applies fixes. Optional monthly scanning reruns that agreed configuration; additional remediation is quoted separately.

Talk through your scope: jmarc@smallofficesecurity.com