OpenSCAP Triage Report (Sample)

Target: 10.244.72.95 | Generated: 2026-02-17 18:18:25

Scan Statistics

Total Rules Scanned	247
Rules Passed	195
Rules Failed / Errors	52

Triage Summary

Total Findings Triaged	5
Safe to Remediate	4
Requires Human Review	0
Too Dangerous / Blocked	1

Safe to Remediate (4)

ID	Rule	Title	Severity	Result	Host	OS	Risk	Reason	Impact
openscap_001	package_aide_installed	xccdf_org.ssgproject.content_rule_package_aide_installed	High	FAIL	10.244.72.95	Rocky Linux 10	LOW	Installing aide is a safe, non-disruptive operation with no service impact.	Package installation; no reboot required
openscap_015	accounts_password_minlen_login_defs	xccdf_org.ssgproject.content_rule_accounts_password_minlen_login_defs	High	FAIL	10.244.72.95	Rocky Linux 10	LOW	Password minimum length policy change is safe to apply automatically.	Password policy update; affects new passwords only
openscap_027	sysctl_net_ipv4_conf_all_accept_redirects	xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_accept_redirects	Medium	FAIL	10.244.72.95	Rocky Linux 10	LOW	Sysctl network hardening is low-risk and standard practice.	Network parameter change; no service restart needed

ID	Rule	Title	Severity	Result	Host	OS	Risk	Reason	Impact
openscap_104	service_auditd_enabled	xccdf_org.ssgproject.content_rule_service_auditd_enabled	High	FAIL	10.244.72.95	Rocky Linux 10	LOW	Enabling auditd is a standard hardening step with minimal risk.	Service enablement; no reboot required

Requires Human Review (0)

None.

Too Dangerous to Remediate (1)

ID	Rule	Title	Severity	Result	Host	OS	Risk	Reason	Impact
openscap_048	partition_for_var_log	xccdf_org.ssgproject.content_rule_partition_for_var_log	Medium	FAIL	10.244.72.95	Rocky Linux 10	CRITICAL	Filesystem/partition changes can break boot or services and should not be auto-remediated.	reboot required; filesystems/partitioning; service disruption risk