AlmaLinux

Keeping AlmaLinux Secure

Vulnerabilities, CIS Hardening & the Tools That Help

AlmaLinux Day: Germany · March 26, 2026 · Europa-Park, Rust

Dennis Zimmer
Codenotary

Codenotary
cognitive cybersecurity

AGENDA

What We'll Cover

1. **AlmaLinux as a Secure Base**
   FIPS, SBOM, OVAL & the security ecosystem
2. **Open-Source Tools**
   OpenSCAP, Trivy, Grype, Lynis & friends
3. **CloudLinux Partnership**
   KernelCare, TuxCare ELS & extended lifecycle
4. **Guardian + LLM**
   CIS compliance, fleet protection & AI-powered security
5. **Q & A**
   Questions and discussion

ALMALINUX

A Secure Enterprise Foundation

400+	FIPS	SBOM	10yr
Contributors	140-3 Validated	CycloneDX + SPDX	Lifecycle

Security-First Design

- SELinux enforcing by default
- CIS benchmarks officially published
- First EL9 distro with kernel FIPS 140-3 cert
- One of a few distributions with a DISA STIG
- AlmaLinux SBOMs are notarized using immudb

Community & Governance

- Non-profit AlmaLinux OS Foundation
- Open governance, no vendor lock-in
- Chosen by CERN & Fermilab
- $1M+ annual CloudLinux sponsorship

Ecosystem & Migration

- 1:1 ABI compatible with RHEL
- almalinux-deploy for in-place migration
- ELevate for major version upgrades
- Supports CentOS, Oracle Linux, RHEL

OVAL

Open Vulnerability Assessment Language

What is OVAL?

Standardized XML format (NIST) for defining and evaluating system vulnerability checks. Machine-readable definitions that scanners like OpenSCAP and TuxCare Radar use to audit systems automatically.

AlmaLinux OVAL Streams

```
org.almalinux.alsa-8.xml
org.almalinux.alsa-9.xml
org.almalinux.alsa-10.xml
```

security.almalinux.org/oval/

How It Works

1. AlmaLinux Build System publishes security errata (ALSA)
2. OVAL XML definitions are auto-generated per advisory
3. Scanner (OpenSCAP / Radar) fetches and evaluates stream
4. Compares installed packages against known CVEs
5. Report generated with pass/fail for every check

The Evolution of Vulnerability Reporting

From CVRF to OVAL to CSAF/OSV

PAST

CVRF

Common Vulnerability Reporting Framework

- XML-based advisory format
- Predecessor to current system
- Limited machine-readability
- No per-CVE granularity

PRESENT

OVAL

Open Vulnerability Assessment Language

- Auto-generated from build system
- Integrated with OpenSCAP & Radar
- Covers AlmaLinux 8, 9, 10
- Powers Nessus, Wazuh, Trivy

FUTURE

CSAF + OSV

Common Security Advisory Framework + Open Source Vuln

- VEX documents per CVE
- OSV JSON on osv.dev
- Richer exploitability context
- Broader tooling ecosystem

SECURITY ECOSYSTEM

AlmaLinux Advisory & Errata System

ALSA — Security Advisory

Critical security patches. CVE-mapped with severity ratings.

ALBA — Bug Advisory

Stability fixes and bug corrections for production reliability.

ALEA — Enhancement Advisory

New features and improvements without breaking changes.

MACHINE-READABLE FEEDS

OVAL XML

OpenSCAP & Radar

```
security.almalinux.org/
oval/
```

JSON Feeds

Full & summary formats

```
errata.almalinux.org/9/
errata.json
```

OSV Format

Standards-based JSON

```
osv.dev/list?
ecosystem=AlmaLinux
```

RSS Feed

Real-time notifications

```
errata.almalinux.org/9/
errata.rss
```

Open-Source Security Tools

Free tools for vulnerability scanning & CIS hardening

OPENSCAP

The Gold Standard for SCAP Compliance

What is OpenSCAP?

Open-source SCAP (Security Content Automation Protocol) framework for automated security compliance. Evaluates OVAL vulnerability definitions and XCCDF benchmark profiles to audit and optionally remediate Linux systems.

Key Commands

```
$ oscap oval eval org.almalinux.alsa-9.xml
```

```
$ oscap xccdf eval --profile cis \
    --results results.xml ssg-almalinux9-ds.xml
```

```
$ oscap-ssh user@host 22 oval eval ...
```

Capabilities

- **OVAL Vulnerability Scanning**
  Evaluate AlmaLinux OVAL streams to find unpatched CVEs
- **CIS Benchmark Profiles**
  Run XCCDF profiles (PCI DSS, STIG, CIS) with pass/fail results
- **HTML & XML Reports**
  Generate audit-ready reports for compliance evidence
- **Remote Scanning (oscap-ssh)**
  Scan remote hosts over SSH without installing agents
- **Auto-Remediation**
  Optionally apply fixes via --remediate flag (use with caution)

Trivy & Grype for Application Security

Container images, filesystems, repos & SBOMs

Trivy

Aqua Security · Apache 2.0

- Container image scanning (Docker, OCI, Podman)
- OS package vulnerabilities (AlmaLinux OVAL)
- Language-specific deps (npm, pip, Go, Java)
- Infrastructure as Code (Terraform, K8s YAML)
- SBOM generation (CycloneDX, SPDX)
- Perfect for CI/CD pipelines & GitOps

```
$ trivy image wordpress:6.6-php8.3-apache
$ trivy rootfs --severity HIGH,CRITICAL /
$ trivy fs --scanners vuln,secret .
```

Grype

Anchore · Apache 2.0

- Fast vulnerability scanner for container images
- AlmaLinux & RHEL package database support
- Pairs with Syft for SBOM-first workflows
- JSON, Table & CycloneDX output formats
- Used by Guardian agent for container scanning
- Lightweight — single binary, no daemon

```
$ grype wordpress:6.6-php8.3-apache
$ grype dir:/var/www --only-fixed
$ grype sbom:./app.spdx.json
```

MORE TOOLS

Open-Source Security Essentials

Lynis

System auditing & hardening. 200+ tests, hardening index score.

```
$ lynis audit system
```

SCAP Workbench

GUI for OpenSCAP. Browse XCCDF profiles, run scans, generate reports.

```
$ scap-workbench
```

Wazuh

SIEM/XDR platform. OVAL feed ingestion, centralized logging, compliance.

```
# wazuh-manager
```

Fail2ban

Intrusion prevention. Bans IPs after repeated auth failures (SSH, HTTP, etc.).

```
$ fail2ban-client status sshd
```

AIDE

File integrity monitoring. Detects unauthorized changes to system files.

```
$ aide --check
```

SELinux

Mandatory access control. AlmaLinux ships enforcing by default — keep it on!

```
$ getenforce  # Enforcing
```

All tools support AlmaLinux natively • Combine them for defense in depth

HARDENING

What Does Real-World Hardening Look Like?

System Updates

dnf-automatic, security-only patches, ELS for EOL

SSH Lockdown

Key-only auth, disable root, MaxAuthTries 3

Firewall (firewalld)

Default-deny zone, allow only 22/80/443

SELinux Enforcing

Keep enforcing, audit denials, fix with setsebool

File Integrity

AIDE database, daily cron checks, alert on changes

Network Params

Disable ip_forward, enable SYN cookies, log martians

Password Policies

pwquality: minlen=12, complexity, pam_faillock deny=5

Intrusion Prevention

Fail2ban on SSH + HTTP, 3 retries → 1hr ban

Doing this manually across a fleet? That's where automation and Guardian come in →

CLOUDLINUX

Extended Lifecycle & Live Patching

TuxCare ELS

Critical security patches for AlmaLinux beyond official end-of-life. Extra years of protected operation without forced upgrades.

16yr

At least coverage

KernelCare Live Patching

Apply kernel security patches without rebooting. Zero downtime patching keeps servers secure and SLAs intact.

0

reboots needed

Rapid CVE Response

Dedicated security team provides fast patch turnaround, often ahead of upstream. FIPS-compliant patches available via subscription.

4hr

avg turnaround

Guardian

CIS compliance, vulnerability management & AI-powered security

FREE for up to 10 systems

https://apps.codenotary.com/

CIS Benchmarks & Vulnerability Scanning

AlmaLinux 8
CIS v4.0.0 • 322 checks

AlmaLinux 9
CIS v2.0.0 • 354 checks

AlmaLinux 10
CIS v1.0.0 • 390 checks

WHAT GUARDIAN CHECKS

- **SSH Hardening** — Root login, ciphers, timeouts
- **SELinux** — Enforcing, policy validation
- **Kernel Hardening** — ASLR, ptrace, core dumps
- **TLS/SSL Config** — HSTS, ciphers, protocols
- **Password Policies** — Complexity, expiry, lockout
- **Network Security** — IP forwarding, SYN cookies
- **Firewall (firewalld)** — Zones, default deny
- **Web App Hardening** — WordPress, LiteSpeed, Nginx

Example: SSH Check

```
grep PermitRootLogin /etc/ssh/sshd_config
→ Expected: no
```

Example: Network Check

```
sysctl net.ipv4.conf.all.accept_redirects
→ Expected: 0
```

FLEET PROTECTION

Ansible, Patching & Remediation at Scale

Ansible Integration

Guardian exports findings as Ansible-ready playbooks. Apply CIS hardening and patch management across your entire fleet from a single control plane.

Workflow

1. Guardian scans fleet → identifies findings
2. Export as Ansible playbook or remediation job
3. Review, approve & execute across fleet
4. Ansible applies patches & config changes
5. Guardian re-scans to verify compliance

Fleet Capabilities

Rolling Patch Deployment

Stage patches across groups with automatic rollback on failure

Auto Backup & Rollback

Every config change backed up before modification. One-click revert.

Fleet Security Posture

Real-time dashboard shows compliance status of every server

Drift Detection

Continuous monitoring detects configuration drift between scans

Audit Trail

Complete log of who remediated what, when, and the result

LLM-Powered Security

AI for audit, forensics, hardening & documentation

Audit & Forensics

LLM analyzes scan results and system state to provide actionable intelligence

- Explain findings in plain language with business impact
- Correlate CVEs across fleet to identify attack patterns
- Root cause analysis: why a config drifted
- Priority triage: what to fix first based on exploitability
- Generate executive compliance summaries
- Timeline reconstruction for incident forensics

Hardening & Documentation

LLM generates remediation steps and compliance documentation automatically

- Context-aware remediation commands per finding
- Generate Ansible playbooks from scan results
- Write CIS compliance reports for auditors
- Document every change with before/after diffs
- Suggest hardening steps tailored to workload
- Auto-generate runbooks for common scenarios

LLM SKILLS

Extensible AI Skills for Security Automation

What are LLM Skills?

Reusable, composable AI task definitions that encode security expertise. Skills combine prompts, tool access, and domain knowledge into repeatable automation units. Create once, apply across your entire fleet.

Skill Examples

- “CIS Hardening Advisor” — explain findings, suggest fixes
- “Vulnerability Triage” — rank CVEs by real-world risk
- “Incident Reporter” — generate forensic timelines
- “Compliance Auditor” — produce audit-ready docs

HOW SKILLS WORK

1 Define

Write a skill definition with instructions, tool access, and constraints

2 Connect

Link to Guardian API, scan results, errata feeds, and fleet data

3 Execute

LLM runs skill against live data, generates output with citations

4 Share

Publish skills to your team. Version, test, and iterate like code

Thank You!

Questions & Discussion

- AlmaLinux provides a FIPS-validated, SBOM-tracked, enterprise-grade base
- OVAL + CSAF/OSV feeds give you machine-readable vulnerability transparency
- Trivy, Grype, OpenSCAP & Lynis form a strong free security toolkit
- Guardian adds CIS compliance, fleet protection & LLM-powered security
- Free for up to 10 AlmaLinux systems — start securing your fleet today

Dennis Zimmer | Codenotary | dennis@codenotary.com

CloudFest 2026 · AlmaLinux Day