4 steps in your Red Hat OpenShift security maturity journey

While Kubernetes has modernized how applications are built and deployed, it has also introduced new layers of security complexity. Follow along with the 4 Red Hat® OpenShift® security maturity levels outlined in this checklist to strengthen your security posture and face the complexity of Kubernetes.

□ Basic level: Establish a strong foundation

Lay the groundwork for a security-focused and compliant Red Hat OpenShift environment by starting with hardened infrastructure and core security practices.

This stage reduces the attack surface and makes sure your production workloads can run with confidence.

- Deploy Red Hat Enterprise Linux® CoreOS, an immutable operating system built for Kubernetes security.
- Apply role-based access control (RBAC) to enforce least-privilege permissions across users, administrators, and service accounts.
- Segment workloads using network policies to reduce lateral movement risks.
- Safeguard sensitive data with encrypted secrets and regular key rotation.
- Enable audit logging to track activity and establish accountability from the beginning.

□ Intermediate level: Automate compliance and enforcement

Move from manual safeguards to proactive, automated security practices.

At this stage, compliance becomes part of daily operations rather than a periodic check, reducing misconfiguration risks and streamlining audits.

- Run the compliance operator to automate assessments against Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) standards.
- Strengthen continuous integration and continuous delivery (CI/CD) pipelines with Trusted Software Supply Chain (TSSC) scanning to detect vulnerabilities and misconfigurations before production.
- Automate policy enforcement so that only signed, verified images progress through pipelines.
- Consolidate audit logs, cluster events, and findings into centralized logging systems for real-time analysis.
- Establish remediation processes to address vulnerabilities quickly and consistently.

□ Advanced level: Establish continuous compliance

Evolve from proactive enforcement to continuous monitoring and automated remediation.

This stage embeds compliance into everyday operations, maintaining alignment with recognized frameworks while strengthening defenses against advanced threats.

- Use Red Hat Advanced Cluster Security to monitor live workloads, detect anomalies, and flag policy violations in real time.
- Generate and manage Software Bills of Materials (SBOMs) to improve visibility into dependencies and vulnerabilities across the stack.
- Enforce image signing and validation to guarantee only trusted container images are deployed.
- Integrate Security Information and Event Management (SIEM) systems with audit logs for unified monitoring and reporting.
- Automate remediation workflows to minimize manual intervention and accelerate response times.

□ Expert level: Achieve peak resilience

Reach the highest maturity through verified supply chains and continuous alignment with strict compliance standards.

This stage is especially critical for organizations in highly regulated industries.

- Deploy confidential containers and confidential computing to protect workloads, even from privileged access.
- Go beyond the most rigorous industry standards such as CIS benchmarks, NIST SP 800-190, and Supply-chain Levels for Software Artifacts (SLSA) requirements.
- Continuously demonstrate audit-ready compliance for regulators, auditors, and customers.
- Extend security maturity with additional Red Hat solutions such as Red Hat Advanced Cluster Management, which assists with governance across hybrid and multicloud environments.

Explore in more detail

Read the Red Hat OpenShift security maturity guide for a more technical look at how each stage builds toward stronger compliance, resilience, and confidence in running production workloads.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhat
x.com/RedHat
linkedin.com/company/red-hat

redhat.com

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1	00800 7334 2835	+65 6490 4200	+54 11 4329 7300
www.redhat.com	europe@redhat.com	apac@redhat.com	info-latam@redhat.com