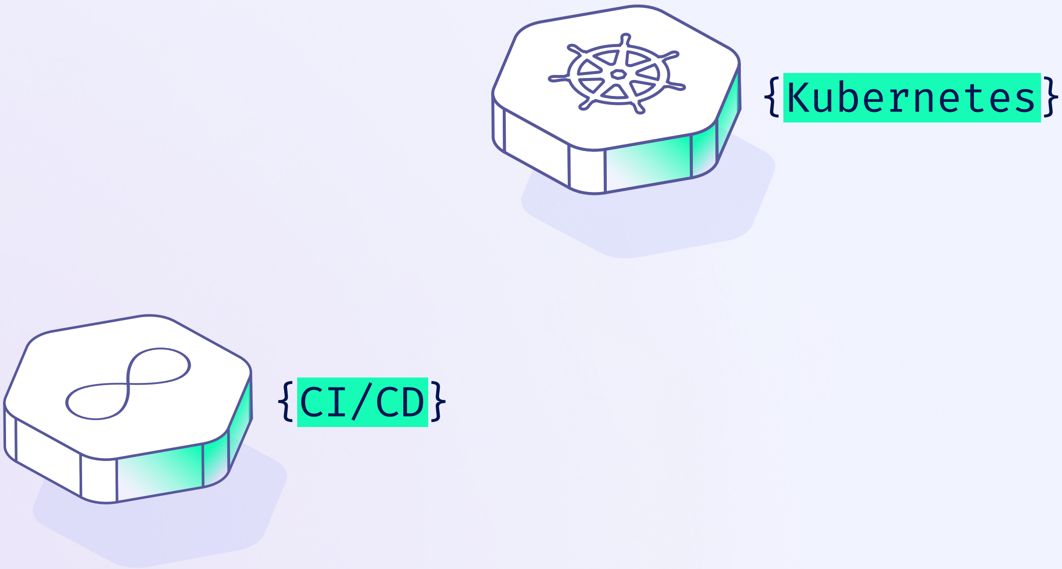
ARMO

Kubernetes Security

{for Security Professionals}



</ The creators of Kubescape

Security Checklist

Security practitioners play a crucial role in ensuring that the appropriate security measures are in place, properly configured, and adhered to throughout the Kubernetes infrastructure lifecycle. They should work closely with the DevOps team to assess, monitor, and continuously improve the security posture of the Kubernetes environment.

Authentication and Authorization

- □ Review and validate the use of strong authentication mechanisms (e.g., client certificates, OAuth2 tokens)
- □ Audit and periodically review role-based access control (RBAC) configurations and permissions
- □ Ensure appropriate access controls and least-privilege principles are followed

Secrets Management

- □ Validate the use of encrypted secrets (e.g., Kubernetes Secrets or a third-party secrets management solution)
- □ Ensure processes are in place for periodic secret rotation and revocation of compromised secrets
- □ Audit and enforce strict access controls for secrets

Container and Image Security

- □ Implement and validate container image scanning processes for vulnerabilities and malware
- □ Maintain and enforce the use of trusted and validated container image repositories
- □ Review and validate the implementation of container runtime security policies (e.g., AppArmor, Seccomp)

Network Security

- □ Validate the implementation and enforcement of network policies to restrict pod-to-pod communication
- □ Ensure the use of network encryption (e.g., TLS) for all Kubernetes components
- □ Review and validate ingress and egress controls for external traffic

Monitoring and Logging

- □ Validate the implementation and configuration of audit logging for Kubernetes API and cluster events
- □ Ensure centralized logging and log aggregation are in place
- □ Implement and configure monitoring for security events, suspicious activities, and compliance violations

Backup and Disaster Recovery

- □ Validate the implementation of regular backups for Kubernetes cluster configurations and data
- □ Test and validate backup restoration procedures
- □ Review and validate the disaster recovery plan for Kubernetes infrastructure

Vulnerability Management

- □ Implement and validate processes for regular scanning and patching of Kubernetes components, nodes, and containerized applications
- □ Ensure subscription to security advisories and mailing lists for timely vulnerability updates
- □ Review and validate vulnerability management processes and remediation procedures

Security Testing

- □ Conduct regular security assessments and penetration testing
- □ Perform code reviews and static analysis for Kubernetes manifests and configurations
- □ Test and validate security controls and incident response procedures

Compliance and Governance

- □ Review and validate the implementation of security policies and standards for Kubernetes infrastructure
- □ Ensure compliance with relevant industry regulations and standards (e.g., PCI-DSS, HIPAA, GDPR)
- □ Audit and validate governance processes for Kubernetes security and operations

How can ARMO help you keep your Kubernetes workloads protected?

Image and configuration scanning

With ARMO Platform you can scan images, manifest, repositories and registries, and easily find vulnerabilities and misconfigurations that can put you at risk for a breach. ARMO Platform results are provided in an easily digestible manner, bubbling up the highest risks based on objective and contextual information.

Continuous compliance

ARMO Platform allows you to easily select one or more industry proven best practice frameworks, or create your own. Scans can be implemented at multiple checkpoints throughout the software development lifecycle and alert if your configuration drifts out of compliance.

RBAC Visualization

Keeping track of RBAC configurations is hard with Kubernetes functionality. Piecing together the access of different roles and users is labor-intensive error-prone work. ARMO Platform’s handy RBAC visualizer provides you with the relationships you need at a glance. You can use pre-defined queries or create your own.

Runtime threat detection

Address the residual threats that may persist during runtime, even after thorough scanning throughout the development and deployment processes. This solution provides actionable results, focusing on reducing false positives. This approach leads to more secure applications while mitigating alert fatigue for security teams.

ARMO’s mission is to equip Security and DevOps teams with a Kubernetes-native solution that delivers noise-free, contextual, and actionable security insights. ARMO is an open-source-driven company and the creator of Kubescape as well as ARMO Platform, the end-to-end Kubernetes security platform.

Learn how ARMO can protect {your applications} from external and internal cyber attacks

Book a demo

Sign up for **ARMO Platform**

Get involved on **Github**

Follow us on **X**

Join the discussion on **Slack**