









Kubernetes Security

Building on Kubescape to Secure Kubernetes Clusters











OpsMx Delivery Shield includes Kubernetes security as part of its complete application security solution. OpsMx Kubernetes Security is built on Kubescape, an open-source Kubernetes security platform designed to empower DevSecOps teams, developers, and system administrators with a comprehensive tool to secure their Kubernetes clusters. By integrating security checks directly into the CI/CD pipeline and offering actionable insights, Kubescape ensures that Kubernetes deployments remain resilient against vulnerabilities and misconfigurations.

Kubernetes Security Key Features

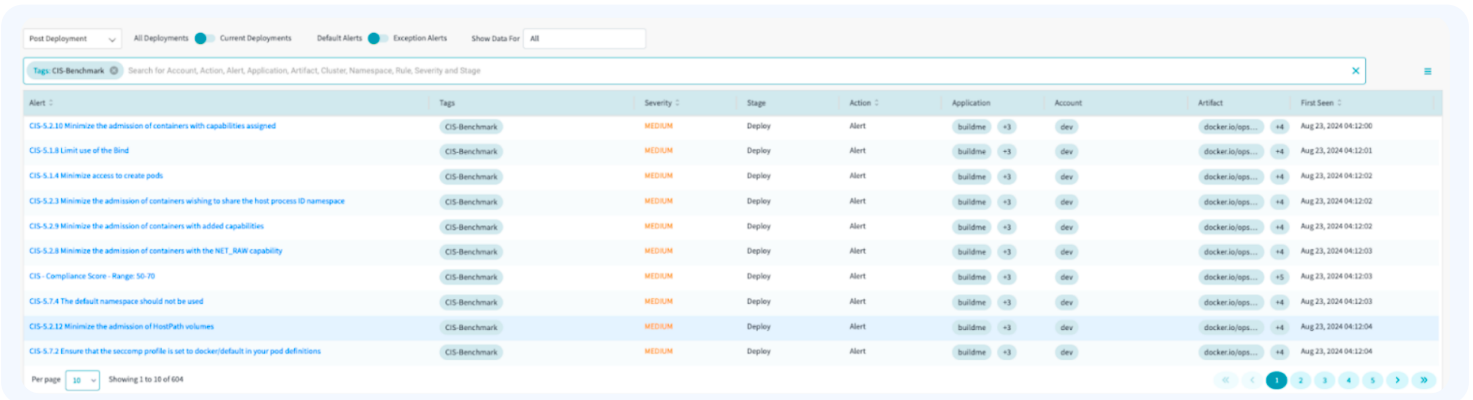
-  **End-to-End Kubernetes Security**
 - Scans Kubernetes manifests, Helm charts, and custom YAML files for vulnerabilities and compliance violations.
 - Identifies misconfigurations in cluster resources and RBAC settings.
-  **CIS Kubernetes Benchmark Compliance**
 - Automates assessments against the Center for Internet Security (CIS) Kubernetes Benchmarks to ensure adherence to industry best practices.
-  **Integrations with CI/CD Pipelines**
 - Seamlessly integrates with popular CI/CD tools like Jenkins, GitHub Actions, GitLab CI, and ArgoCD to detect issues early in the development cycle.
-  **Shift-Left Security**
 - Enables developers to identify and fix security issues during the development phase, reducing downstream risk and remediation costs.
-  **Policy Management and Customization**
 - Includes predefined policies while supporting custom policies tailored to organizational needs.
-  **Integration with Cloud-Native Ecosystems**
 - Compatible with Prometheus, Grafana, and other monitoring tools to enable continuous observability and security monitoring.
-  **Detailed Reporting and Analytics**
 - Provides comprehensive reports with actionable insights, including compliance status, identified vulnerabilities, and remediation steps.
-  **Multicluster Support**
 - Secures multiple Kubernetes clusters from a single dashboard, streamlining the management of large-scale environments.

Key Benefits

-  **Enhanced Security Posture**
 - Automatically detects vulnerabilities and misconfigurations, ensuring Kubernetes environments remain secure against emerging threats.

- 
Reduced Operational Overhead
 - Simplifies the process of maintaining compliance and securing clusters, freeing up resources for other priorities.
- 
Improved Developer Productivity
 - Shift-left capabilities and easy-to-understand reports enable developers to address security concerns without waiting for post-deployment feedback.
- 
Compliance Readiness
 - Out-of-the-box compliance checks for frameworks like CIS, NIST, and PCI DSS ensure readiness for audits.
- 
Centralized Security Management
 - A single platform to manage and secure Kubernetes clusters across cloud environments, increasing operational efficiency.
- 
Faster Incident Response
 - Real-time monitoring and alerts reduce mean time to detect (MTTD) and mean time to remediate (MTTR) vulnerabilities.
- 
Cost Savings
 - Early detection and remediation of security issues save costs associated with breaches and non-compliance penalties.
- 
Scalability and Flexibility
 - Designed to support organizations of all sizes, from startups to enterprises, with flexible deployment options.

OpsMx Delivery Shield's Kubernetes Security offers a comprehensive solution to securing Kubernetes clusters, ensuring compliance, and enabling a proactive approach to DevSecOps. With its robust features, seamless integrations, and open-source foundation, Kubescape is an essential tool for any organization leveraging Kubernetes in their cloud-native journey.



Alert	Tags	Severity	Stage	Action	Application	Account	Artifact	First Seen
CIS-5.2.10 Minimize the admission of containers with capabilities assigned	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:00
CIS-5.1.8 Limit use of the bind	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:01
CIS-5.1.4 Minimize access to create pods	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:02
CIS-5.2.3 Minimize the admission of containers wishing to share the host process ID namespace	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:02
CIS-5.2.9 Minimize the admission of containers with added capabilities	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:02
CIS-5.2.8 Minimize the admission of containers with the NET_RAW capability	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:03
CIS - Compliance Score - Range: 50-70	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:03
CIS-5.7.4 The default namespace should not be used	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:03
CIS-5.2.12 Minimize the admission of HostPath volumes	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:04
CIS-5.7.2 Ensure that the seccomp profile is set to docker/default in your pod definitions	CIS-Benchmark	MEDIUM	Deploy	Alert	buildme +3	dev	docker.io/tps...	Aug 23, 2024 04:12:04

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY