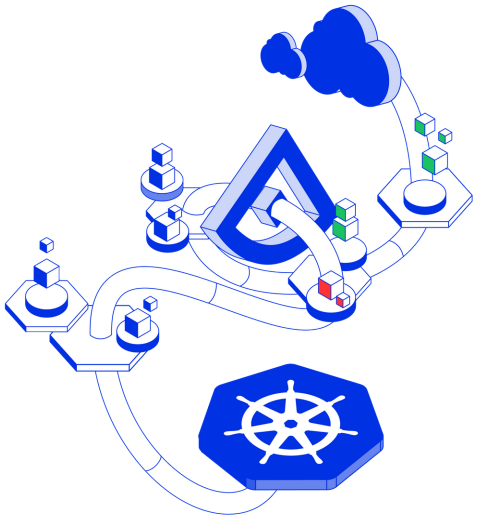
Alcide Integrates with Datadog

Enabling easy Kubernetes audit logs analysis with Alcide kAudit

Challenges of auditing a Kubernetes cluster

The dynamic, distributed and ephemeral nature of Kubernetes deployments results in workloads being added, removed or modified at a fast pace. Security teams' demands for safeguarding and monitoring Kubernetes deployments are many, and keep increasing.
Such demands require a constant and near real-time analysis of Kubernetes audit logs.
However, manually reviewing numerous bundles of raw audit logs is a tedious and time-consuming task, and with an increasing amount of moving parts, it becomes nearly impossible.



Alcide kAudit and Datadog

Access & analyze data with Kubernetes security intelligence

The various challenges with handling Kubernetes' raw audit logs calls for a unified solution that can constantly monitor and analyze relevant audit entries and conform to the organization's policies and compliance requirements.

Alcide's kAudit is an automated analytics and forensics module that is specifically designed for detecting and identifying suspicious activity, based solely on Kubernetes' audit logs and can seamlessly integrate with your Datadog environment and setup.

Comprehensive visibility, all in one place

Alcide's integration with Datadog enables users to gain full access to insights and real-time alerts from Alcide kAudit. This integration allows detection of Kubernetes' compliance violations, security incidents, and administration activity anomalies directly from Datadog's platform.

Users can get full visibility into their Kubernetes clusters for application health status, coupled with security insights for deeper investigation. Additionally, this integration enables DevOps and security teams to focus on compliance violations and active security risks.

Identify Anomalous Kubernetes Behaviour Beyond Configuration Rules

Focus on real incidents. Reduce time to detect

kAudit fits perfectly in the complex multi-cluster Kubernetes environments that companies build today. With an AI-based detection and prevention mechanism, Alcide kAudit provides a high-resolution network detection security layer that gives instant insights and alerts on any suspicious activity.
Armed with machine learning and artificial intelligence for monitoring audit logs, kAudit continuously scans audit logs and flags any unusual or suspicious network behavior.

While there are many potential threats to consider, some of the most crucial and popular ones are the following:

Exploited Vulnerabilities in the Kubernetes API Server

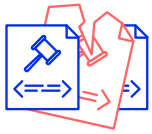
Avoid bypassing of authentication, authorization, admission control or validation request breaches.

Stolen Credentials/Tokens

Prevent hackers from surreptitiously gaining access to k8s-based clusters or pods.

Misconfigured RBAC

Monitor lateral cluster or pod movement, privilege escalation, access to sensitive information and data manipulation.

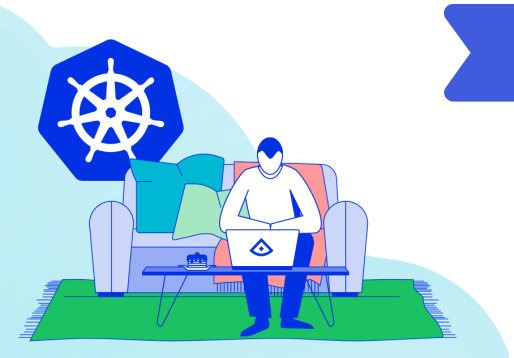


Violated Security Policies

Track and spot any divergence from compliance requirements (GDPR, PCI, HIPAA) and security best practices.

Get started with Alcide and Datadog

Visit Datadog's integrations page or alcide.io for more information



www.alcide.io • info@alcide.io