Alcide and RedHat:

Security baked seamlessly into your entire Kubernetes deployment

CHALLENGES

Tracking & analyzing audit logs can be nearly impossible

Red Hat OpenShift is the industry's most comprehensive enterprise platform for Kubernetes, automating the container application lifecycle and integrating security into the pipeline. To further strengthen your OpenShift deployment, however, you still need real-time analysis. In real time, the audit log remains the most established method to identify incongruent activity or strange user behavior, helping to see whether your systems have been compromised. But - manually reviewing audit logs is tedious and time-consuming and with workloads being added, removed or modified at a mind-boggling pace, it's nearly an impossible mission. DevOps and Security teams need a solution that goes beyond manual K8s log inspections.

THE ALCIDE SECURITY SOLUTION

Alcide helps secure and ensure Kubernetes multi-cluster hygiene

Alcide kAudit addresses this challenge, bridging between the DevOps teams' need to monitor their multi-cluster Kubernetes environment with the Security teams' demand to have visibility and investigation capabilities - without becoming Kubernetes experts. kAudit advances real-time, automated K8s forensics and analysis for your deployment that you can plug in directly to your OpenShift setup, facilitating the swift identification of users and roles with legitimate reasons for accessing sensitive workloads-at any given time. kAudit identifies suspicious activity patterns, observing behaviors with extended context, beyond configured rules, thereby protecting your entire network. The module automatically assembles, catalogs and reports on violations of K8s-related compliance best practices. Red Hat OpenShift users can get Kubernetes audit logs insights and focus on what really matters when it comes to audit logs: reducing the noise usually associated with them, and reducing time to detection.

Benefits

Alcide kAudit is a robust, machine learning-enabled tool, intelligently leveraging Kubernetes audit logs, and summarizing detected anomalies alongside important access, usage and performance trends of the K8s cluster and statistics for user-friendly investigation and auditing.

Focus on impending threats fast

Alcide kAudit offers ongoing analyses of Kubernetes audit logs to detect illegitimate user and service account behavior in real-time. Automated insights on critical threats and security-related abuses enable teams to focus on material incidents while significantly reducing detection time.

Smoothly integrate with your SIEM

Alcide kAudit seamlessly integrates into existing common SIEMs such as Splunk, providing SOC teams visibility on their K8s security events as part of their existing traditional monitoring.

Monitor behavior and react in real-time

With behavioral machine learning, kAudit identifies suspicious activity patterns, in real-time. When anomalous behavior is identified, kAudit traces back to the root causes via fully context-aware, post-mortem investigation and automated forensic analysis.

Stay compliant

Backed by patent-pending artificial intelligence, kAudit learns the patterns of your audit log over time and then enables security and compliance enforcement in response to anomalies accordingly.

Bringing Kubernetes audit log forensics to the Red Hat OpenShift ecosystem

As a certified Red Hat operator, Alcide offers a Kubernetes security solution that you can consume with confidence. The Alcide Security Platform adheres to Red Hat's strict requirements for quality, compatibility, and security features within the Red Hat ecosystem. Alcide kAudit proactively investigates and analyzes Kubernetes deployments for breaches, unusual behavior and misuses in real time. With our robust analysis and forensics capabilities, OpenShift users get k8s audit log insights while still focusing on what really matters: reducing the noise usually associated with audit logs and reducing time to detection. On the landscape of growing networks, multiple cloud setups, and hybrid deployments, Alcide kAudit represents a critical security building block for companies relying on Kubernetes as their application delivery vehicle.

Features

Ongoing protection of against unauthorized access

kAudit helps you protect against:

- Stolen credentials, by actors aiming to gain initial access to K8s-based clusters or pods; or seeking to capture credentials earlier in their reconnaissance process through social engineered access to cluster resources;
- Stolen tokens or misconfigured RBAC, which allow lateral cluster or pod movement; privilege escalation; data access and/or data manipulation.

Real-time automated monitoring of policies and threat detection

Alcide's integration with OpenShift exports Kubernetes findings as well as Kubernetes audit events that violate compliance and security policy controls, enabling you to prevent:

- Exploited vulnerabilities in the Kubernetes API Server, such as authentication, authorization, admission control or validation requests breaches, which seek to gain access to privileged and sensitive resources; and
- Violated security policies in conflict with compliance best practices

Get started with Alcide solutions on RedHat

Visit RedHat OpenShift OperatorHub or Alcide.io to purchase or start a Free Trial today.