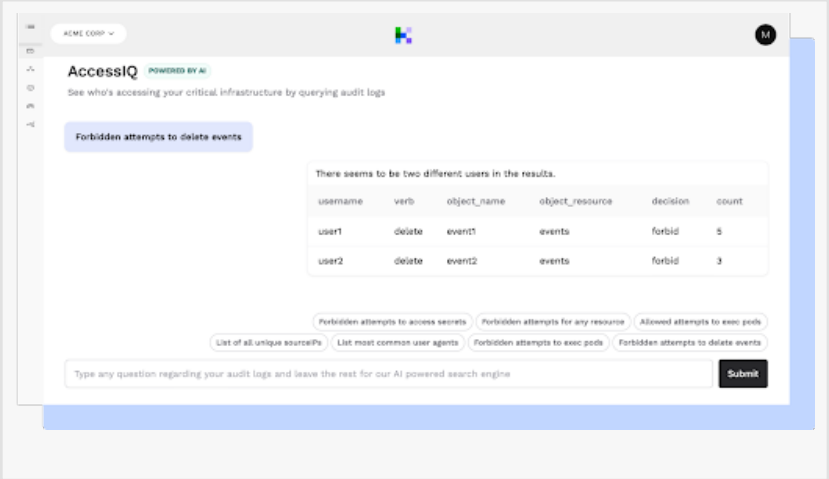
KSOC launches industry's first AI-powered Cloud-Native Identity Threat Detection Platform

Helping overburdened security and engineering teams uncover malicious insiders and attackers trying to access critical cloud infrastructure



SAN FRANCISCO, CA, UNITED STATES, November 7, 2023 /EINPresswire.com/ -- Today, Kubernetes Security Operations Center (KSOC) released the first threat detection capabilities spanning from Kubernetes role-based access control (RBAC) to cloud IAM, using AI to quickly spot anomalous patterns in large amounts of audit logs and cloud metadata. Compromised credentials and malicious insiders represent the most costly and common attack vectors of a breach, and played a key role in three of the four Kubernetes targeted attacks in 2023. With cloud native identity threat detection, security and engineering teams now have insight into the actual usage of over permissions, versus lists of over permissions that don't indicate malicious usage.

> When it comes to identity in Kubernetes and the cloud, the legacy approach is to create noisy lists of misconfigurations and over permissions and call it 'good enough.'"
>
> *Jimmy Mesta, CTO and Co-Founder KSOC*

"When it comes to identity in Kubernetes and the cloud, the legacy approach is to create noisy lists of misconfigurations and over permissions and call it 'good enough.' But security and engineering teams are now too overwhelmed, and identity has proven too critical and challenging to manage at scale, for this approach to remain practical. With this feature, customers are able to take advantage of AI's strength in finding patterns in large datasets to efficiently identify identity-based attacks in their cloud native environments," says Jimmy Mesta, CTO and Co-Founder of KSOC.

The shifting left of security responsibilities, and the shared service model, has challenged CISOs

to incorporate the cloud and Kubernetes into their zero trust and compliance initiatives. Today's containerized, distributed workflows allow for different teams to spin up cloud IAM and Kubernetes RBAC roles independently, which, if left unchecked, can lead to the proliferation of valid credentials with unintended permissions. Recent research suggests that attacks starting with identity have the most grave consequences:

Kubernetes Security Operations Center (KSOC)

- In a breach, malicious insiders are the single most costly initial attack vector

- Stolen or compromised credentials are the second most common initial attack vector malicious use of valid credentials

- Breaches initiated with stolen or compromised creds and malicious insiders took the longest to resolve, compared to alternatives like phishing or exploitation of zero day vulnerabilities

Despite the criticality of cloud native identity, today, CSPM and open source RBAC tools fall short of identifying malicious activity. The most common approach to this problem today applies the tactics used in a classic CSPM or image scanner, by creating lists of over permissions but don't include context to determine the relative importance, or actual usage, of over permissioned identities. This legacy method leads to noise and can even fray the relationship between security and engineering, as security tries to change policies that engineering has set without a full understanding of the policies' impact on the overall security posture.

Cloud native identity is the perfect use-case for the application of AI, the usage of which has been found to cut the time to contain a data breach by 108 days (versus those organizations that don't use security AI and automation). In this case, not only is AI helpful for combing through large amounts of data to find patterns, it also makes it easier to interrogate the logs at scale to detect novel attacks or patterns because of the natural language processing in the query process, speeding further development of the capability.

KSOC's new cloud native identity threat detection platform includes the following capabilities:

- Attack paths between Cloud IAM and Kubernetes RBAC: find risks in the interaction of Cloud IAM and Kubernetes RBAC

- Cloud native identity anomaly detection: AccessIQ shows actual usage based on AI queries of

Kubernetes API audit logs to find malicious insiders and other attacks utilizing valid or overly permissive credentials, plus baselines 'normal' RBAC behavior and detects anomalies using AI to query cloud metadata, RBAC configurations and Kubernetes API audit logs

- Top priority RBAC and IAM misconfigurations: prioritize the most critical configurations based on the connections between RBAC permissions, Kubernetes misconfigurations, network exposure, runtime alerts and image CVEs on the same workload

KSOC has also added the following features to its real-time cloud native security platform, allowing customers to move from CSPM-centric, legacy cloud native security to a more efficient, accurate approach to securing ephemeral cloud native environments:

- Cloud Compliance Frameworks: Adding to our cluster compliance frameworks, these cloud checks encompass more than 20 compliance frameworks
including NIST, SOC and more

- AI-powered auto-remediation: A new, AI-powered remediation capability that provides the actual, suggested changes in your manifest code

- EKS Cluster Discovery: Discover the clusters in your EKS environment, with instant visibility into the clusters that are not currently secured by KSOC

- Resource Tagging: Easily pair a finding to the appropriate team for remediation, show your top risks and threat vectors in your own internal terminology, ignore findings from particular resources, and much more with this new resource tagging capability

The team will be showcasing cloud native identity threat detection and the other new product releases live at Kubecon in Chicago, Nov. 6-9 at booth #O40.

Daniel Delson
Magnitude Growth
daniel@magnitude-growth.com
