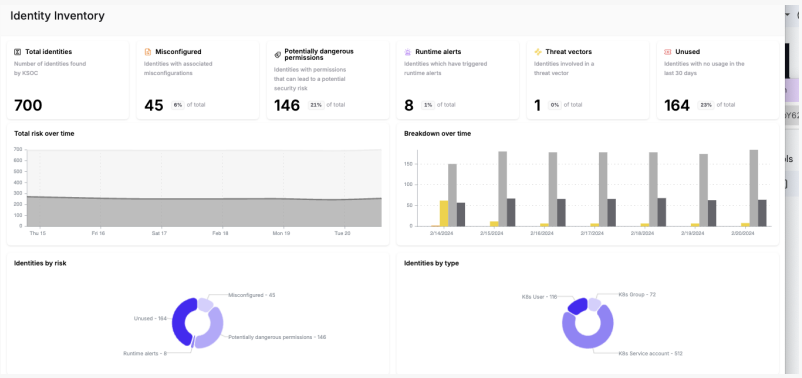
KSOC Releases Industry's First Zero Trust Policy Generator for Kubernetes RBAC

Allowing IT teams to cover the Kubernetes RBAC gap in their zero trust initiatives and streamline implementation of least privilege access



KSOC Kubernetes RBAC Zero Trust Policy Generator

SAN FRANCISCO, CA, UNITED STATES, February 27, 2024 /EINPresswire.com/ -- Kubernetes Security Operations Center (KSOC) has announced the availability of the first zero trust policy generator for Kubernetes role-based access control (RBAC). To-date, security and engineering teams have been unable to incorporate Kubernetes RBAC in their zero trust initiatives, as current Kubernetes or Cloud Identity and Entitlements Management (KIEM/CIEM) tools either ignore RBAC or make right-sizing guidance in absence of the identity's behavior. As part of its Identity Threat Detection and Response (ITDR) platform, KSOC's new RBAC zero trust policy generator automates least privilege recommendations alongside insights into malicious identities.

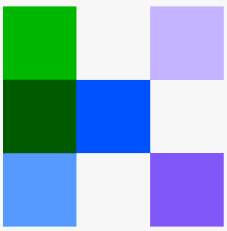
> The broad context from ITDR gives KSOC's customers an idea of how to best cover their gaps with the RBAC zero trust policy generator."
>
> *Jimmy Mesta, CTO and Co-Founder of KSOC*

"Passive lists of over permissions are inadequate for the Kubernetes RBAC gap faced by IT teams in their zero trust initiatives today," says Jimmy Mesta, CTO and Co-Founder at KSOC. "For any least privilege policy recommendation to have practical value, a baseline understanding of the identity's actual behavior is required; to that end, KSOC's customers get broad context with ITDR to understand how best to cover their gaps with the RBAC zero trust policy generator."

All signs point to the prioritization of zero trust initiatives in 2024; recent research places identity and access management and cloud infrastructure as the top two areas of focus for CISOs in 2024. Another recent survey showed that identity has moved up to be the second top priority for CISOs, followed closely by cloud infrastructure security, compared to the 8th top priority last year. And analysts forecast an uptick of 10% in the number of organizations that will have a

measurable zero trust program in place over the next year.

Three of the four major attacks targeting Kubernetes in 2023 relied on overly permissive RBAC identities. In 2024, for the first time, software supply chain attacks targeted kubeconfig files, and a recent survey showed that 58% of teams using Kubernetes had a security issue in the last 12 months with insufficient access controls in their Kubernetes environment.



Kubernetes Security Operations Center (KSOC)

Despite the central role of Kubernetes RBAC in attacks targeting these environments, ITDR, CIEM and KIEM tools either ignore Kubernetes and only list out Cloud IAM issues, or they focus on lists of over permissions without incorporating audit log data or runtime behavior. Unfortunately, this excludes the actual usage required to understand the gaps in a zero trust program, let alone understand malicious activity or prioritize its remediation. And until today, teams have had no practical guidance to help them implement least privilege policies for Kubernetes RBAC.

The primary goal of KSOC's right-sizing engine is to lower the scope of permissions to least privilege. The right-sizing function is available as part of KSOC's cloud native ITDR solution, which allows customers to:

Clearly prioritize identity versus other risks in the environment using:
- Attack paths between Cloud IAM and Kubernetes RBAC
- Threat vectors that map the relationship between runtime events, network, cloud, Kubernetes misconfigurations, image CVEs, and more
- A clear view of the riskiest identities based on identity usage, presence in a broader threat vector, aspects of the identity itself, and more
- An identity inventory showing relative risks, and their relationships to the rest of the environment

Detect anomalies in usage and investigate the riskiest identities with:
- An identity inventory, including audit logs and deep dives into roles, service accounts, rolebindings, and other connections between identities and workloads
- AccessIQ: actual usage based on AI queries of Kubernetes API audit logs to find malicious insiders and other attacks utilizing valid or overly permissive credentials
- A baseline of 'normal' RBAC behavior to detect anomalies in cloud metadata, RBAC configurations and Kubernetes API audit logs

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

- Support for Kubernetes Custom Resources: Now you can include your custom resources in KSOC's real-time KSPM features and threat vectors for complete security coverage. Take advantage of KSOC's admission control capabilities by writing custom policies against these custom resources.
- Github app: Now you can configure and enforce a CI workflow for KSOC across all repos at the organization level, to enforce and measure compliance to standards with less friction, as well as ensure that workloads are scanned for CVEs before entering the deployment pipeline.
- Chainguard integration: Within KSOC's container insights, track the usage of Chainguard's CVE-free images across all your clusters over time, to ensure progress on the road to inbox zero for vulnerabilities and FedRAMP compliance

About KSOC
KSOC is a cloud native security company that empowers engineering and security teams to push boundaries, build technology and drive innovation so they can focus on growth versus security problems. In today's environment, attackers are more versed in cloud native security than security teams. KSOC removes the blind spots of legacy CSPM and container tools, closing the detection and response gap between cloud native infrastructure and runtime.

Daniel Delson
Magnitude Growth
+1 917-328-9337
email us here
Visit us on social media:
Twitter
LinkedIn
YouTube
