CLOUDKNOX

Case Study
CRITICALSTART

Tackling the #1 cloud security threat together: CRITICALSTART + CloudKnox

Company Background

CRITICAL**START**, headquartered in Plano, Texas, is one of the fastest-growing providers of cybersecurity Managed Detection and Response (MDR) services in North America. The company's mission is to resolve every alert and to stop breaches, leveraging their award-winning MDR and professional services. This includes penetration testing and incident response through TEAMARES, which serves as both the red and blue teams for CRITICAL**START** clients.

The Challenge

Today, MDR providers and security consultancies face unique challenges combating threats while meeting the business requirements of cybersecurity. Not only must they ensure the security of their service delivery platform, but they need to ensure the customers, with whom they connect, are secure to avoid breach by lateral movement from a compromised network. Moreover, many organizations are enforcing third-party risk management by scrutinizing provider security policy.

As CRITICAL**START** continues to be honored as one of the industry's leading MDR providers, its security team applies the same level of effort devising and executing on its own internal stringent cybersecurity strategies. Specifically, a significant area of focus for CRITICAL**START** is the growing insider threat risk, whether due to negligence or malice.

According to CRITICAL**START** CTO, Randy Watkins, "There is a lot of focus on outsiders breaking in, but an insider threat where the attacker knows how the systems work, how customers maintain and access their data in the cloud, and how to navigate the infrastructure pose a completely different and dangerous type of security challenge for organizations."

The Solution

Recognizing the growing and unpredictable nature of insider threats, the CRITICAL**START** team needed to find a preventive, multi-faceted solution that went beyond the conventional definition of insider threats to include machine identities such as service accounts, bots, and resources like EC2 instances, etc.

Watkins says, "We were looking for a solution (for our customers and us) that would enable us to continuously detect and remediate human and machine identities with excessive high-risk permissions across our AWS environment. We also needed a solution that was quick and simple to deploy, could scale with the growth of our business and easily handle the perpetual addition of new services, users, roles, and permissions in AWS."

The CRITICAL**START** team identified three critical requirements for their ideal solution:

1. Understand the insider threat risk surface

CRITICALSTART wanted to immediately assess their insider threat risk by uncovering all unique groups, roles, and human and machine identities with excessive high-risk permissions. They specifically wanted to know which high-risk permissions were unused over the last 90 days.

2. Continuous enforcement of least privilege policies
The team was finding it cumbersome to manually track, trend, and report on permission drift and wanted to find a quick and straightforward way to understand how every unique identity inherited their permissions and how they were using them within their AWS environment. The team wanted to focus on three key identity groups: a) Active Identities, b) Inactive Identities, and c) Service Accounts (machine identities):

– Active Identities
To keep up with current hiring practices, CRITICAL**START** had instituted rigorous oversight of all new hires and were seeking a more efficient way to scale. They were looking for an automated way to continuously monitor changes or anomalies to prevent privilege creep/ drift as these identities changed job functions over time.

– Inactive Identities
The team was looking for a better way to manage Inactive Identities and groups. These are identities (both human and machine) who have not performed actions in the last 90-days or more.

– Service Accounts
As a best security practice, the team was seeking an automated way to regularly monitor their service accounts to ensure they were only performing a small number of repetitive tasks with a low number of low-risk permissions. If one of those service accounts displayed suspicious behavior, the security team wanted to be alerted immediately.

3. Audit Preparation
Audits pose significant challenges in public cloud environments where the addition and deletion of new identities, resources, services, roles, and permissions happens frequently. To keep up with these changes, the CRITICAL**START** team needed a solution that would enable them to continuously view, monitor, remediate and report on the status of their least privilege policy program without having to manually collect data from multiple disparate sources.

The Results

CRITICAL**START** purchased the CloudKnox Cloud Security Platform for their AWS environment. Within a few weeks of deploying the platform, the team was able to address all of their original requirements, as follows:

1. Implement least privilege policies across their AWS environment for all human and machine identities, groups, roles, and resources:

- Remove all Inactive Identities and groups from their AWS accounts
- Remove Inactive Identities and unused permissions from groups
- Right-size (prune) unused permissions from all identities, groups, roles, and resources
- Create custom roles based only on a common set of permissions required to perform the job of a common group of identities
- Significantly reduce the number of identities and groups with unnecessary access to critical AWS resources (e.g. S3 buckets)
- Limit the scope of identities and roles to only resources in which they have access

2. Continuously measure, evaluate, and compare the company's risk posture against managed service provider benchmarks using CloudKnox's "Privilege Creep Index."

3. Demonstrate to auditors in minutes compliance with key access management controls as well as other regulatory mandates.

"Whether human or machine," states Watkins, "CloudKnox's platform fills a huge gap in the market by delivering an unprecedented level of visibility into who is doing what, when, and where on AWS. It has effectively transformed the way we implement and enforce least privilege policies across our AWS environment."

About CloudKnox Security

CloudKnox Security is the only Cloud Security Platform built from the ground-up to support the monitoring and management of identities, actions, and resources across hybrid and multi-cloud environments using an Activity-based Authorization model. Through a single extensible platform, CloudKnox transforms how organizations implement the principle of least privilege and empowers security teams to proactively address accidental and malicious credential misuse by continuously detecting and mitigating the insider threat risk. CloudKnox is based in Sunnyvale, CA.

May 12, 2021

www.cloudknox.io