SecOps Practices that stop AWS Account Compromise accurately and early.

A Cloud Detection and Response Strategy for AWS

Cyber attackers are exploiting enterprise identities to compromise data on-premises and in the cloud by utilizing AWS accounts as vehicles to execute attacks. Vectra CDR for AWS enables SOC analysts to quickly detect and respond to active AWS account compromises, privilege abuse attempts and unrestrained access by attackers before the target is reached.

Key Challenges

- **SecOps teams struggle** to balance best practices and operational requirements to keep AWS accounts active and secure, due to lack of precise attribution of malicious acts taking place within AWS Accounts.
- **Reliance on a separate AWS cloud team** for insights about compromised AWS accounts to move forward with threat hunting and response. Expanding vulnerabilities and exploits require both signature and behavior-based detection.
- **Lack of complete context of AWS environment** to aid in threat detection and response.

In a hybrid cloud world, the proper identity of compromised accounts — especially AWS accounts (cross-regionally and cross-accounts) continue to be a primary threat vector used on enterprises — causing inevitable data breaches, ransomware and other sophisticated attacks.

How to make sure your AWS accounts aren't compromised

Prioritize AWS account security:

Shift the mindset away from an IT-centric management and prevention approach that executes coordinated efforts of AWS account identity attack detection and response. Incorporate Vectra CDR for AWS for layered controls that precisely pinpoint any trace of an account breach, enabling SecOps to investigate AWS credential misuse so they can respond quickly. Advanced attackers are constantly attempting to exploit trusted AWS Accounts that require privileged access, identity-related workflows, execution and integration into SecOps processes to gain visibility from the inside and move the attack further up the kill chain.

Recognize attacker activity quickly:

Vectra CDR for AWS is powered by Vectra Attack Signal IntelligenceTM to provide AI-driven threat detection, triage and prioritization. This enables SecOps to detect and respond to unknown attacks including AWS account misuse or abuse. Any malicious activity that is detected runs through SAML and is attributed back to the SAML user to make an informed decision on for targeted response.

Identify the root cause:

Vectra CDR for AWS monitors all activity within AWS including any account misuse for any type of unauthorized change. Once detected, SecOps is alerted to initiate the necessary response and communications required to those who can act on the AWS account immediately and streamline efforts to prevent an escalated attack from occurring.

Enables Advanced Investigation:

Security Analysts can take immediate action to contain the compromised AWS account and prevent it from causing harm to an organization. Vectra CDR for AWS quarantines the AWS account in question to contain it, revoke access to additional credentials and block malicious traffic from moving throughout the AWS environment.

Address MITRE ATT&CK® TTPs for AWS:

Sophisticated actors are bypassing perimeter controls of AWS through advanced TTPs to target workloads and identity in order to execute attacks. MITRE outlines that SecOps teams must be able to assess all malicious activity including those on AWS accounts to determine when a compromise occurs. Vectra CDR for AWS assesses AWS accounts from a hacker's perspective to continuously detect all known and unknown AWS account threat activities in your hybrid cloud environment.

Keys to success:

- A CDR for AWS solution purpose-built for SecOps with AI-driven detection and response to cover an entire AWS cloud footprint.
- A CDR for AWS solution that deploys easily with no additional training required from the cloud team or third-party experts.
- A CDR for AWS solution built on the principle of least privilege for AWS accounts instead of an all or nothing approach.

The power to identify an AWS compromise before execution

Vectra CDR for AWS provides the means necessary to detect and respond to attacks on your AWS accounts without any additional training on identity-based attacks. Vectra CDR for AWS puts you in control of your AWS accounts without having to default to an all or nothing account lockdown methodology. Your SecOps teams can trust the power of Vectra CDR for AWS to precisely identify which AWS account is compromised before any exploits on your organization can execute.

Learn more about Vectra CDR for AWS

About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enable security operations teams to prioritize, investigate and respond to cyber attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyberattacks.

For more information please contact us:
Email: info@vectra.ai | vectra.ai