Reveal security

Solution Brief

TrackerIQ for AWS

Monitor Privileged User Behavior and Detect Suspicious Activity with ML-Based Detection

aws

Benefits

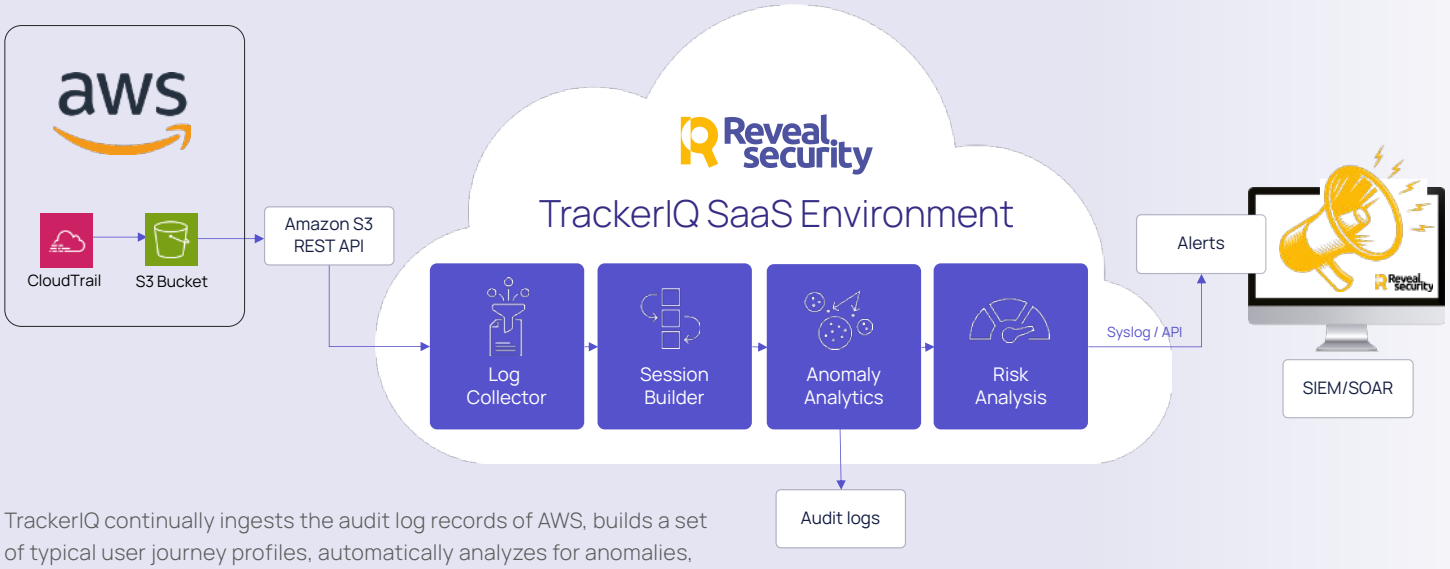
- Detect malicious or accidental configuration changes by insiders or adversaries
- Detect unauthorized management activities by insiders or adversaries
- Detect unauthorized security setting modifications (e.g. Access control policies) by insiders or adversaries
- Enable faster mean-time-to-detection (MTTD) of insider and external threats
- High-fidelity alerts enable focus on real threats and improves response times
- Context-rich alerts with activity sequencing helps speed incident response and investigations

Overview

Monitoring Amazon Web Services (AWS) environments is a complex task due to the sheer volume of user activity audit logs generated daily. Privileged users may perform thousands of actions (events) per day, making manual security monitoring impractical. Traditional methods of security monitoring using rules or User and Entity Behavior Analytics (UEBA) usually result in a flood of false alerts, overwhelming security teams and making it difficult to identify actual threats. The challenge lies in distinguishing between normal and anomalous behavior, especially in the context of the vast and dynamic AWS environment.

TrackerIQ, by RevealSecurity, addresses the challenges of AWS security monitoring by leveraging its advanced Machine Learning (ML) engine to detect both unauthorized and accidental changes as well as anomalous activity that could be indicative of compromised credentials or a malicious insider. The ML engine continuously tracks operations performed using AWS web UI and API activity by users across AWS services such as EC2, IAM, S3, RDS, KMS, ECR, Secrets Manager and more. Unlike static rules or UEBA solutions, TrackerIQ's approach significantly reduces the number of false alerts, allowing security teams to focus on investigating only a handful of anomalies raised weekly.

TrackerIQ Analysis Flow



TrackerIQ continually ingests the audit log records of AWS, builds a set of typical user journey profiles, automatically analyzes for anomalies, and generates high-fidelity alerts prioritized by risk posture.

Detection Use Cases

TrackerIQ supports a broad spectrum of detection use cases in AWS, enabled by monitoring privileged user behavior for anomalies. The following table highlights suspicious administrator behavior that can be detected automatically, leveraging the TrackerIQ ML engine, and without rules.

Unauthorized creation of new Amazon Identity and Access Management (IAM) users, roles, or access keys
(e.g. Create an AWS user, deactivate MFA for user access, add an AWS user to a group, attach an Administrator Policy)

Unauthorized modification of the security configuration of Amazon instance
(e.g. unusual sequence of network configuration operations like delete bucket encryption, CloudTrail logging disabled, Create HTTP target group without SSL, add inline policy in a group to allow access to all resources)

Unauthorized modification of Amazon VPC instance network configuration
(e.g. unusual sequence of network configuration operations like allocate a new elastic IP address to AWS account, associate an elastic IP Address to an AWS network interface, create an internet-facing AWS public-facing load balancer)

UI and API calls used to modify access permissions that was invoked in an anomalous way

UI and API calls used to evade defensive measures that was invoked in an anomalous way

Unusual Amazon RDS snapshot generation that can be part of data exfiltration attempts

Comprehensive Threat Detection

TrackerIQ helps detect a range of suspicious management and configuration activities, including unauthorized creation or modification of IAM users, roles, or access keys, UI/API calls to modify access permissions, attempts to evade defensive measures, and unauthorized modifications to AWS configurations such as instance security and VPC network settings.

Advanced Anomaly Detection Delivers the Highest Fidelity Alerts…with Context

TrackerIQ uses sequence-based analysis to provide context to anomalies. Instead of alerts on isolated activities, it analyzes sequences of events, making it easier for security teams to understand the context and identify potential threats. For example, it can reveal that an IAM user not only invoked the S3 ListBuckets API anomalously but also performed other related operations like GetBucketACL and PutBucketPublicAccessBlock. Each operation by itself may not be an anomaly but the sequence of operations is anomalous, making the detection much more accurate.

By employing sequence-based analysis, TrackerIQ delivers a very low volume of high fidelity alerts – no more than a few per week – with deep contextual information, unlike the deluge of false positive alerts generated by static rules or UEBA techniques. Security teams can prioritize investigations based on the severity and context of anomalies, leading to more efficient use of resources.

Improved Incident Response and Investigations

TrackerIQ translates AWS audit logs into human-readable language and provides security analysts with a summary of sequence activity. Analysts can quickly assess suspicious activities and access detailed lists of all activities within a sequence, including success and failure details. This contextual information is crucial for both anomaly detection and efficient triaging of alerts.

Security teams can also swiftly investigate and triage new threat detections, improving incident response. The solution provides valuable context on each activity within a sequence, aiding in identifying compromised credentials and understanding the attacker's objectives.

About TrackerIQ

TrackerIQ's advanced detection capabilities offer a comprehensive and context-rich approach to AWS security monitoring, empowering security teams to efficiently identify and respond to real threats while minimizing the impact of false alerts.

TrackerIQ uses patented User Journey Analytics to model how users interact with AWS and delivers detailed alerts when suspicious behavior is detected. TrackerIQ operates out-of-band using log data integrations, so it's completely non-disruptive to your critical business applications.

TrackerIQ's application-independent approach translates the often cryptic logging terminology of individual applications into a normalized format for analysis. From there, User Journey Analytics, based on unsupervised machine learning, develops micro-personas representing your trusted users and establishes baselines of their normal behavior. This includes user journeys that span multiple applications for maximum context and accuracy. Ongoing application usage of trusted identities is compared to past journeys by the same individual and comparable peers, and information-risk alerts are generated when high-risk anomalies are detected.

About RevealSecurity

Reveal Security is an identity threat detection company that delivers accurate behavior-based user analytics without rules. This allows organizations to cost effectively detect, alert and quickly respond to the abuse and misuse of trusted identities operating inside and across the mission-critical applications that drive their business.

For more information, visit www.reveal.security