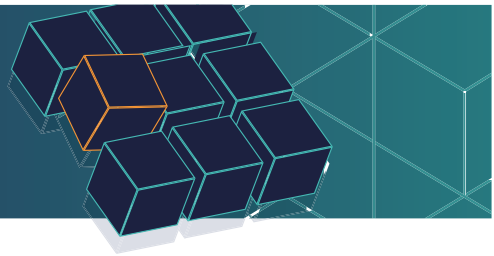
Detecting Malicious Activities in Applications and Platforms

Each application has a unique set of operations and the application logs have no common formats or content. This challenge is augmented by the growing number of SaaS application used by enterprises.

Each user has many activity flows per application, which make the detection of anomalous user journeys (i.e. sequences) very challenging.

TrackerIQ

Application Detection and Response



To address the above challenges RevealSecurity has developed a new and innovative generalized User Journey Model that can be applied across any application. This model is based on the activities performed by the user, the order in which they were performed, and the time gaps between these activities.

The User Journey Model is agnostic to the meaning of the activities and enables a quick on-boarding process for adding new applications. Since each user has many activity flows per each application, TrackerIQ learns for each user (or group of users) his/her Activity Flow profiles. To learn automatically the activity flow profiles per user (or group of users), a patent-pending clustering engine was developed by RevealSecurity for grouping the user's journey and generating profiles. These profiles enable the accurate detection of anomalous user journeys. To prioritize the detected anomalies, TrackerIQ also assigns a risk score to each user journey anomaly based on its activities.

TrackerIQ generates alerts for the detected anomalies with tailored recommendations. For security analysts who want to investigate the anomalies, TrackerIQ also provides analysis tools that enable them to quickly understand the anomaly and make a decision.

Detection based on Activity Flow Analytics

- Provides the context for each operation performed by the user to enable accurate detection
- Anomalies are prioritized based on their activities' risk

Generalized Activity Flow Model

- Agnostic to the activity meaning
- Applicable across all SaaS applications
- No need to develop a unique model
- per application

Application Detection and Response Based on User Journey Analysis

Multiple Activity Flow Profiles

- TrackerIQ detects anomalies that deviate from the user's Activity Flow profiles
- Profiles are generated automatically using innovative ctivity Flow clustering engine

Operationally Efficiency

- Quick and easy on-boarding
- Easy integration with customer's log repositories (Files, Databases, SIEM, SPLUNK/ELK & Syslog)

About RevealSecurity

RevealSecurity introduced the TrackerIQ ADR solution focuses on Application Detection and Response. Our innovative and unique approach delivers unmatched detection accuracy, with low number of false positives based on a patent pending User Journey clustering algorithm. TrackerIQ overcomes the users' activity blindspots inherent in application logs, providing unparalleled detection, visibility and investigation capabilities to minimize exposure and damage to insider threats.

Reveal security | www.reveal.security | info@reveal.security

TAG CYBER 2022 DISTINGUISHED VENDOR