TrackerIQ

Detecting Suspicious Behavior in Enterprise Applications

Detecting anomalous behaviors of users in an application is as tough as finding a needle in the haystack. RevealSecurity's solution is ubiquitous and accurate, detecting without the need to develop rules or data models. It can be applied to any application, whether SaaS, custom-built, or to IaaS/PaaS, enabling analysts to focus on the breaches that matter.

The fast-growing migration to SaaS applications significantly increased CISO needs for detecting malice, misuse or abusive activities - aka business operational breaches. Current detection solutions monitor SaaS application access layers and therefore are not effective against internal users or attackers impersonating a legitimate user.

The common practice of detecting anomalies in applications entails countless rules per application for each known attack scenario, thus posing a real barrier towards developing a ubiquitous solution to monitor and protect the organization's applications layer.

Security teams find it impossible to keep up with the need to write countless rules per application. Rule-based detection is notoriously ineffective, costly and inaccurate.

TrackerIQ is a unique solution for detecting business operational breaches in enterprise applications. The system (machine) learns every user and cohort action and operation, as they create multiple behavior profiles per user, per application. TrackerIQ then identifies and alerts the organization of any anomalous behaviors in the application.

TrackerIQ does not need to know the application's log formats and content in advance. Our algorithm analyzes user behavior quickly and accurately. Context leads to better detection accuracy: the better the context, the more accurate the detection (i.e., lower rate of false positives and false negatives).

Challenges in Finding Application-Level Breaches

Application-level detection solutions have evolved significantly in the past decade, from rule-based detection platforms to more advanced solutions which are based on volumetric and frequency-based analysis (UEBA). Rules are static and targeted at known attack scenarios, whereas in the application layer every attack is new and unknown. Rule-based and UEBA solutions generate a high number of false negatives and false positives in the application layer. Furthermore, each user has multiple behavior profiles per application, which grow both in number and frequency of change.

Filling the Gap in Detection of Application Activity Anomalies

There is a large gap between the need to protect enterprise applications and the tools that offer adequate protection at that level. Analysis of business operations manifested by application activity logs requires a deep understanding and comprehensive knowledge of the applications themselves. The sheer number of enterprise applications in use today by any given organization, alongside the variance between their business purpose on the one hand and log structures on the other, poses a real barrier towards developing a ubiquitous solution to monitor and protect an organization's applications layer.

Furthermore, the ever-growing migration to the cloud with the increased use of SaaS applications has intensified this gap. Even though there is no shortage of logs produced by SaaS applications, organizations find themselves unable to analyze these logs, let alone detect anomalies which are hidden in the logs. In our ever-changing reality, the ability to identify anomalous behaviors quickly and accurately in the application layer has become an essential part of our cyber security and risk arsenal. We must be able to track, detect and respond to humans and systems, as they abuse or perform errors, malicious activities and breaches at the organization's application layer.

There is an abundance of application logs which are continuously being collected and stored in organization repositories (e.g., SIEM, data lakes, databases, servers and data warehouses). The challenge is not in collecting the logs, but rather in the ability to analyze them quickly and accurately to find the breaches that they represent, visualizing them as a clear activity flow of business scenarios, and presenting a clear analysis of a business operational breach scenario, one that can be quickly acted upon.

Risk Management has become an integral part of every organization today. In the IT world and more specifically in cyber security, Risk Management has become the baseline of every enterprise, especially in view of the ever-increasing number of hacks and attacks organizations have become exposed to.

Application Detection and Response (ADR) enables organizations to perform risk management at the level of enterprise applications. TrackerIQ's ADR solution brings a new level of application activity analysis, one which is far more accurate and comprehensive than older rule-based and statistical model solutions. The solution is able to quickly analyze vast amounts of data without the need to predefine known threat behaviors.

> "It is what you're not looking for that should keep you awake at night"

TrackerIQ

A New Algorithm for Detecting Anomalous Application Behavior Patterns

TrackerIQ's underlying algorithms are based on unsupervised machine learning of user operation behavior patterns in enterprise applications, which are then clustered into behavior profiles for individuals as well as cohorts. New activity is monitored in real time so that the system can detect any deviation from these learned profiles to identify anomalous behavior patterns as they occur. TrackerIQ then alerts the organization of newly found suspicious activity flows (i.e., sessions) and allows for a quick, clear, and comprehensive investigation of these incidents.

Machine learning of user behavior profiles is based on the analysis of the users' sequences of operations, with an emphasis on (a) which operations were performed; (b) the order in which these operations were performed; and (c) the time intervals between operations in analyzed sequences. This analysis is performed over sequences of operations, thus allowing the identification of any number of unique application activity footprints of a user or cohort. An ongoing comparison of new operations with these existing unique footprints allows for a very low rate of both false positive and false negative alerts.

When TrackerIQ identifies a suspicious session, it generates an alert with a risk score which is based on the sensitivity of operations which comprise the identified anomalous session.

TrackerIQ maintains a minimal storage footprint, keeping only those logs which were identified as part of the anomalous session. It is an agentless solution, and therefore does not require any installation or changes on the application servers.

TrackerIQ's Advantages

- The system identifies business operational breaches at the application level
- No need to pre-define rules or statistical models
- Highly accurate, due to the creation of multiple profiles and analysis of sessions both per user and per application
- A risk score is assigned to every identified suspicious session, based on the individual operations that comprise the anomalous session
- A quick and comprehensive investigation of the incident, with TrackerIQ's visualization tools
- A built-in interface to all existing log repositories, including SIEM, data lakes, databases, log files, and more. Data and logs in these repositories are never duplicated
- Simple and easy to use - no installation required

HOW IT WORKS

Reading

Digestion of any application logs

Learning

Analyzing activity operation sequences for every user and cohort of users

Clustering

Creation of multiple behavior profiles per user

Aggregation

Aggregation of behavior patterns for each user/cohort, per application

Monitoring

Continuously monitoring application activity logs, in search of anomalous behavior sequences

Detection

Identifying anomalous operation sequences as they occur in realtime

Prioritization

Assigning a risk score to identified sequences, based on the risk level of the individual operations in the sequence

Alerting

Sounding the alarm on identified attacks and their associated risks

Investigation

Using a comprehensive visual toolset to highlight identified sessions and assist in analyzing incidents

About RevealSecurity

RevealSecurity monitors privileged users, malicious insiders and imposters to detect anomalies in applications and platforms. Time and again, reputable research has found that the longer it takes to detect a breach, the greater its damage, yet most detection of breaches within applications is still rule-based, thereby costly and ineffective due to a debilitating high rate of false alerts. Meticulous authentication is never enough, as users who have legitimate application access are still involved in misuse, abuse and malice. RevealSecurity champions ubiquity and accuracy in the application detection market.

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

TAG CYBER 2022 DISTINGUISHED VENDOR