# TrackerIQ

## Détection des comportements suspects dans les applications d'entreprise

Détecter les comportements anormaux des utilisateurs dans une application est aussi difficile que de trouver une aiguille dans une botte de foin. La solution de RevealSecurity est omniprésente et précise, détectant sans qu'il soit nécessaire de développer des règles ou des modèles de données. Elle peut être appliquée à n'importe quelle application, qu'elle soit SaaS, personnalisée ou IaaS/PaaS, permettant aux analystes de se concentrer sur les failles les plus importantes.

La migration en pleine expansion vers les applications SaaS a considérablement accru les besoins des RSSI en matière de détection des activités malveillantes, frauduleuses ou abusives, c'est-à-dire des manquements aux opérations commerciales.

Les solutions de détection actuelles surveillent les couches d'accès aux applications SaaS et ne sont donc pas efficaces contre les utilisateurs internes ou les attaquants se faisant passer pour un utilisateur légitime.

Les équipes de sécurité ne parviennent pas à suivre le rythme quant au besoin d'écrire d'innombrables règles par application. La détection basée sur des règles est notoirement inefficace, coûteuse et imprécise.

TrackerIQ est une solution unique pour détecter les violations opérationnelles des entreprises dans les applications d'entreprise. Le système (machine) apprend chaque action et opération de l'utilisateur et de la cohorte, car ils créent plusieurs profils de comportement par utilisateur, par application.

TrackerIQ identifie et alerte ensuite l'organisation de tout comportement anormal dans l'application. TrackerIQ n'a pas besoin de connaître à l'avance les formats et le contenu des journaux de l'application.

Notre algorithme analyse le comportement des utilisateurs rapidement et avec précision. Le contexte conduit à une meilleure précision de détection : plus le contexte est bon, plus la détection est précise (c'est-à-dire, un taux de faux positifs et de faux négatifs plus faible).journaux de l'application. Notre algorithme analyse le comportement des utilisateurs rapidement et avec précision. Le contexte conduit à une meilleure précision de détection : plus le contexte est bon, plus la détection est précise (c'est-à-dire, un taux de faux positifs et de faux négatifs plus faible).

## Défis liés à la recherche de violations au niveau de l'application

Les solutions de détection au niveau des applications ont considérablement évolué au cours des dix dernières années, passant de plateformes de détection basées sur des règles à des solutions plus avancées basées sur l'analys volumétrique et fréquentielle (UEBA). Les règles sont statiques et ciblées sur des scénarios d'attaque connus, alors que dans la couche application, chaque attaque est nouvelle et inconnue. Les solutions basées sur des règles et l'UEBA génèrent un nombre élevé de faux négatifs et faux positifs dans la couche application. De plus, chaque utilisateur a plusieurs profils de comportement par application, qui augmentent à la fois en nombre et en fréquence de changement.

## Combler les lacunes dans la détection des anomalies d'activité des applications

Il existe un écart important entre la nécessité de protéger les applications d'entreprise et les outils qui offrent une protection adéquate à ce niveau. L'analyse des opérations commerciales manifestées par les journaux d'activité des applications nécessite une compréhension approfondie et une connaissance exhaustive des applications elles-mêmes. Le grand nombre d'applications d'entreprise utilisées aujourd'hui par les organisations, ainsi que l'écart entre leur objectif commercial d'une part et les structures de journalisation d'autre part, constituent un véritable obstacle au développement d'une solution omniprésente pour surveiller et protéger la couche d'applications des organisations.

En outre, la migration croissante vers le cloud avec l'utilisation accrue des applications SaaS a intensifié cet écart. Même si les journaux produits par les applications SaaS ne manquent pas, les organisations se retrouvent dans l'incapacité de les analyser, et encore moins de détecter les anomalies qui y sont cachées. Dans notre réalité en constante évolution, la capacité à identifier rapidement et avec précision les comportements anormaux dans la couche applicative est devenue un élément essentiel de notre arsenal de cybersécurité et de gestion des risques. Nous devons être en mesure de suivre, de détecter et de répondre aux humains et aux systèmes, lorsqu'ils abusent ou commettent des erreurs, des activités malveillantes et des violations au niveau de la couche applicative de l'organisation.

Il existe une abondance de journaux d'application qui sont continuellement collectés et stockés dans les référentiels de l'organisation (par exemple, SIEM, lacs de données, bases de données, serveurs et entrepôts de données). Le défi n'est pas de collecter les journaux, mais plutôt de pouvoir les analyser rapidement et avec précision. Cela a pour but de trouver les violations qu'ils représentent, les visualiser comme un flux d'activité clair de scénarios commerciaux et présenter une analyse claire d'un scénario de violation oprationnelle de l'entreprise, sur lequel on peut agir rapidement.

La gestion des risques fait aujourd'hui partie intégrante de chaque organisation. Dans le monde informatique et plus particulièrement dans la cybersécurité, la gestion des risques est devenue la base de toute entreprise, notamment au vu du nombre toujours croissant de piratages et d'attaques auxquels les organisations sont exposées.

L'ADR (Application Detection and Response, en Français, Détection et réponse des applications) permet aux organisations d'effectuer une gestion des risques au niveau des applications d'entreprise. La solution ADR de TrackerIQ apporte un nouveau niveau d'analyse de l'activité des applications, bien plus précise et complète que les anciennes solutions basées sur des règles et des modèles statistiques.

La solution est capable d'analyser rapidement de grandes quantités de données sans qu'il soit nécessaire de prédéfinir les comportements de menace connus statistiques.

La solution est capable d'analyser rapidement de grandes quantités de données sans qu'il soit nécessaire de prédéfinir les comportements de menace connus.

« C'est ce que vous ne cherchez pas qui devrait vous tenir éveillé la nuit »

# TrackerIQ

## Un nouvel algorithme pour détecter les comportements anormaux des applications

Les algorithmes sous-jacents de TrackerIQ sont basés sur l'apprentissage automatique non supervisé de modèles de comportement des opérations des utilisateurs dans les applications d'entreprise. Ils sont ensuite regroupés dans des profils de comportement pour individus et cohortes. La nouvelle activité est surveillée en temps réel afin que le système puisse détecter tout écart par rapport à ces profils appris pour identifier les comportements anormaux au fur et à mesure qu'ils se produisent. TrackerIQ alerte ensuite l'organisation des nouveaux flux d'activités suspectes (c'est-à-dire des sessions) et permet une enquête rapide, claire et complète sur ces incidents.

L'apprentissage automatique des profils de comportement des utilisateurs est basé sur l'analyse des séquences d'opérations des utilisateurs, en mettant l'accent sur (a) les opérations qui ont été effectuées ; (b) l'ordre dans lequel ces opérations ont été effectuées ; et (c) les intervalles de temps entre les opérations dans les séquences analysées. Cette analyse est effectuée sur des séquences d'opérations, permettant ainsi l'identification de toute empreinte d'activités d'application unique d'un utilisateur ou d'une cohorte. Une comparaison continue des nouvelles opérations avec ces empreintes uniques existantes permet un très faible taux d'alertes faussement positives et négatives.

Lorsque TrackerIQ identifie une session suspecte, il génère une alerte avec un score de risque basé sur la sensibilité des opérations qui comprennent la session anormale identifiée.

TrackerIQ maintient une empreinte de stockage minimale, ne conservant que les journaux qui ont été identifiés comme faisant partie de la session anormale. Il s'agit d'une solution sans agent, et ne nécessite donc aucune installation ou modification sur les serveurs d'applications.

## Les avantages de TrackerIQ

- Le système identifie les violations opérationnelles de l'entreprise au niveau de l'application
- Pas besoin de prédéfinir des règles ou des modèles statistiques
- Très précis, grâce à la création de plusieurs profils et à l'analyse des sessions par utilisateur et par application
- Un score de risque est attribué à chaque session suspecte identifiée, en fonction des opérations individuelles qui composent la session anormale
- Enquête rapide et complète sur l'incident avec les outils de visualisation de TrackerIQ
- Interface intégrée à tous les référentiels de journaux existants, y compris SIEM, lacs de données, bases de données, fichiers journaux, etc. Les données et les journaux de ces référentiels ne sont jamais dupliqués
- Facile à utiliser : aucune installation nécessaire

## COMMENT ÇA FONCTIONNE

### Interprétation
Assimilation de tous les journaux d'application

### Apprentissage
Analyse des séquences d'opérations d'activités pour chaque utilisateur et cohorte d'utilisateurs

### Regroupement
Création de plusieurs profils de comportement par utilisateur

### Agrégation
Agrégation des modèles de comportement pour chaque utilisateur /cohorte, par application

### Surveillance
Surveillance continue des journaux d'activité des applications, à la recherche de séquences de comportement anormal

### Détection
Identification des séquences d'opérations anormales au fur et à mesure qu'elles se produisent en temps réel

### Priorisation
Attribution d'un score de risque aux séquences identifiées, en fonction du niveau de risque des opérations individuelles de la séquence

### Alerte
Signal d'alarme sur les attaques identifiées et leurs risques ssociés

### Enquête
Utilisation d'un ensemble d'outils visuels complets pour mettre en évidence les sessions identifiées et aider à analyser les incidents

## À propos de RevealSecurity

RevealSecurity surveille les utilisateurs privilégiés, les initiés malveillants et les imposteurs pour détecter les anomalies dans les applications et les plateformes. À maintes reprises, des recherches réputées ont montré que plus il faut de temps pour détecter une violation, plus ses dommages sont importants. Qui plus est, la plupart des détections de violations au sein des applications sont toujours basées sur des règles, donc coûteuses et inefficaces en raison d'un taux élevé décourageant de fausses alertes. Une authentification méticuleuse n'est jamais suffisante, car les utilisateurs qui ont un accès légitime aux applications sont toujours impliqués dans des abus et des actes frauduleux ou malveillants. RevealSecurity défend l'omniprésence et la précision sur le marché de la détection d'applications.

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



TAG CYBER 2022 DISTINGUISHED VENDOR