TrackerIQ

TrackerIQ détecte les activités malveillantes dans les applications d'entreprise

Le critère le plus important dans une solution de détection est la précision : le nombre de faux positifs et faux négatifs, et le but est évidemment de minimiser ces alertes. Cependant, les solutions actuelles de détection d'applications sont basées sur des règles, qui plus est, très imprécises.

L'approche analytique unique de TrackerIQ atteint une grande précision en utilisant le contexte de l'activité, c'est-à-dire en analysant une séquence d'activités, au lieu de l'activité elle-même. TrackerIQ procède ainsi en analysant le parcours utilisateur dans l'application.

Application de l'apprentissage automatique pour apprendre les profils de parcours utilisateur

L'enjeu est bien sûr de savoir apprendre automatiquement tous les parcours utilisateurs types dans une application (voire entre applications), car chaque utilisateur a de nombreux parcours types (ou profils de parcours). Il est important de souligner qu'un parcours moyen n'a aucun sens, et pour détecter avec précision le parcours anormal, il est nécessaire de connaître tous les parcours types de l'utilisateur.

Pour connaître avec précision les profils de parcours utilisateur, TrackerIQ lit les événements du journal et génère les parcours utilisateur (c'est-à-dire les sessions utilisateur dans l'application). Il regroupe ensuite les parcours d'utilisateurs similaires pour générer les profils de parcours de l'utilisateur. Pour effectuer ce regroupement de parcours avec précision, RevealSecurity a développé un moteur de regroupement en instance de brevet (puisque les moteurs de regroupement existants sur le marché ne fournissent pas la précision requise). Sur la base des groupes générés par le moteur de regroupement, TrackerIQ génère les profils de parcours des utilisateurs et les utilise pour détecter les parcours anormaux. (Remarque : même si des parcours anormaux existent dans les données du journal utilisées pour l'apprentissage, ils sont détectés comme des anomalies par TrackerIQ.) Pour améliorer la précision de la détection, un parcours est comparé à la fois aux profils de parcours de l'utilisateur et aux profils de parcours de la population de l'utilisateur (les deux appris automatiquement par TrackerIQ).

Analyse du parcours utilisateur

Le suivi des parcours des utilisateurs permet un nouveau niveau d'analyse de l'activité des applications, bien plus précis et complet que les anciennes solutions basées sur des règles et des modèles statistiques. Un parcours utilisateur est une séquence d'activités que l'utilisateur a effectuées dans une application. Des recherches ont prouvé que chaque utilisateur a des parcours types lorsqu'il utilise une application. Connaître le parcours type par utilisateur (par application), permet de détecter précisément un parcours anormal, qui ne ressemble pas aux parcours types de l'utilisateur dans l'application.

Par exemple, lorsqu'un initié effectue une activité malveillante, son parcours s'écarte de ses parcours typiques et/ou des parcours typiques de ses groupes de pairs. De plus, un moyen précis de détecter la prise de contrôle de compte (c'est-à-dire l'imposteur) consiste à comparer le parcours de l'imposteur aux parcours réels des utilisateurs typiques.

Solution de détection omniprésente : l'essence des activités ne fait aucune différence pour TrackerIQ

Comme expliqué ci-dessus, la détection de TrackerIQ est basée sur les caractéristiques du parcours utilisateur, c'est-à-dire les activités effectuées au cours d'un parcours utilisateur, l'ordre dans lequel elles ont été effectuées et la différence de temps entre elles. Ces caractéristiques du parcours utilisateur sont complètement indifférentes à l'essence des activités spécifiques de l'utilisateur. Ainsi, le modèle de détection de TrackerIQ peut être appliqué à n'importe quelle application, car il est omniprésent et indépendant de la signification des activités d'une application. Ceci est fondamental pour la détection de RevealSecurity, car chaque application possède un ensemble d'activités différent.

Ce qu'il faut retenir

Application indépendante

Le modèle de détection de TrackerIQ est indépendant de la signification des activités d'une application. Il peut donc être appliqué à n'importe quelle application et même à des applications croisées.

Analyse du parcours utilisateur

TrackerIQ analyse les parcours des utilisateurs (c'est-à-dire les sessions d'application), et non les activités individuelles. Le parcours fournit un contexte qui est important pour une détection précise.

Précision inégalée

Pour atteindre une précision sans précédent, la machine TrackerIQ apprend à l'aide de son moteur de regroupement en instance de brevet tous les profils de parcours utilisateur et les utilise pour détecter les parcours utilisateur anormaux.

Aucune règle requise

La détection basée sur des règles ne détecte que les modèles d'attaque connus, génère un nombre élevé de fausses alertes, nécessite une maintenance constante et coûteuse, et n'évolue pas.

À propos de RevealSecurity

RevealSecurity détecte les initiés malveillants et les imposteurs en surveillant les parcours des utilisateurs dans les applications d'entreprise. La détection de RevealSecurity est omniprésente, appliquée sur n'importe quelle application et sur l'ensemble des applications, y compris les applications SaaS, les applications cloud et les applications personnalisées. La détection protège les organisations d'entreprise contre deux cas : lorsqu'un utilisateur authentifié profite de ses autorisations pour effectuer des activités malveillantes ou lorsqu'un imposteur réussit à contourner les mécanismes d'authentification pour se faire passer pour un utilisateur légitime. Le suivi des parcours utilisateurs par RevealSecurity ne repose pas sur des règles spécifiques à l'application, mais est plutôt alimenté par des analyses innovantes du parcours des utilisateurs, combinées à un moteur de regroupement unique pour détecter avec précision les parcours anormaux qui reflètent des activités malveillantes.