Reveal security

Product Brief

TAG CYBER 2022 DISTINGUISHED VENDOR

RILEVAMENTO DI COMPORTAMENTI ANOMALI BASATO SULL'ANALISI DEI FLUSSI DI ATTIVITA' ALL'INTERNO DI APPLICAZIONI CORE BUSINESS E SAAS

L'Esigenza dei mercati

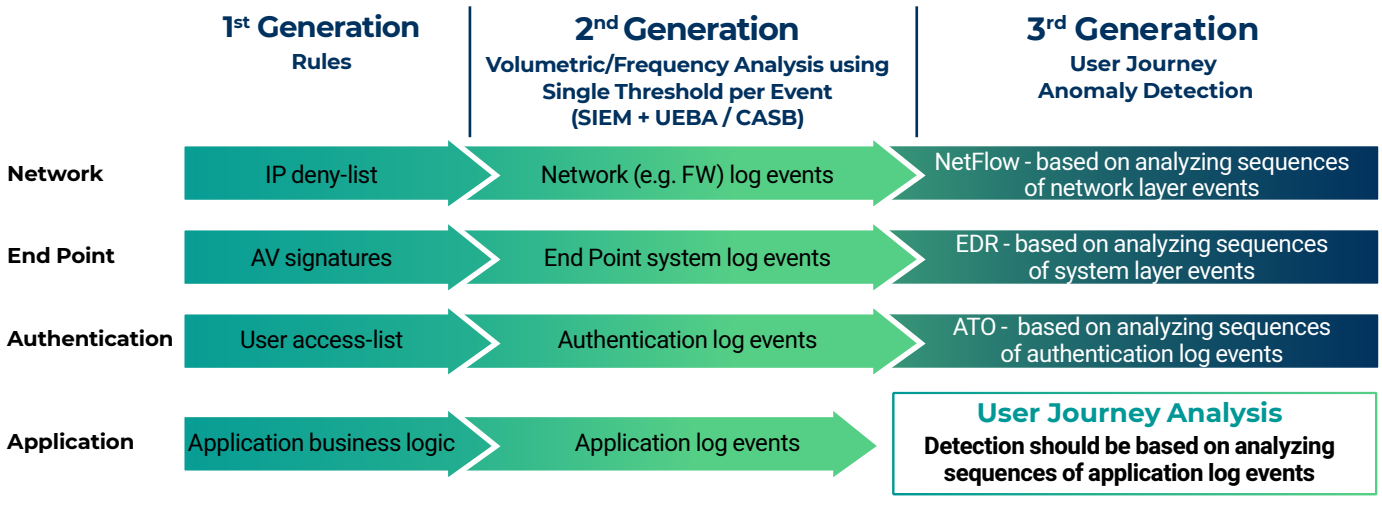
La trasformazione digitale ha cambiato profondamente il business delle aziende in tutti i settori con impatti sul modo in cui comunicano con i loro dipendenti, partner, fornitori e clienti, collegandoli più velocemente come mai prima d'ora, aumentando l'efficienza e offrendo esperienze digitali sempre più sofisticate. Ed è qui che aumentano i rischi per la sicurezza informatica! Infatti, è evidente che nonostante l'attuazione delle misure di sicurezza informatica normalmente adottate, le attività anomali o fraudolente svolte dagli utenti applicativi (addetti ai lavori ma anche clienti esterni) rappresentano una delle principali minacce alla sicurezza dell'organizzazione nell'attuale era digitale. Queste minacce si verificano a livello applicativo del core business e di conseguenza le organizzazioni di tutti i settori verticali sono in parte suscettibili a perdite finanziarie, ma anche ai danni derivanti dalla perdita di dati riservati, fiducia dei clienti, reputazione del marchio e interruzioni operative significative. Inoltre, le applicazioni critiche sono quelle dove anche gli aggressori esterni stanno concentrando i loro sforzi.

Le attuali soluzioni di rilevamento utilizzate dalle organizzazioni sono inadeguate per il rilevamento di minacce al livello applicativo

Le soluzioni attuali di rilevamento di minacce sono progettate per casi d'uso specifici quali la protezione dell'infrastruttura di rete, l'autenticazione degli utenti e l'accesso ai dati, e non analizzano il dettaglio delle attività degli utenti a livello dell'applicazione dopo aver effettuato l'accesso ai sistemi. Tipicamente gli strumenti di rilevamento disponibili si basano su algoritmi basati su regole per rilevare modelli di attacco già noti o impostando soglie di rischio sull'analisi di frequenza e volumetrica delle attività principalmente di autenticazione e accesso ai dati. Queste soluzioni di rilevamento hanno un'efficacia limitata per rilevare gli addetti ai lavori fraudolenti, poiché questi dispongono di credenziali di accesso "legittime" e di solito operano "silenziosamente" al di sotto delle soglie di rilevamento. Pertanto, è necessario un nuovo approccio di rilevamento per affrontare le nuove minacce provenienti da addetti ai lavori in modo tempestivo e accurato in tutte le applicazioni utilizzate dall'azienda (COTS, Custom-build e SaaS).

Un contesto migliore significa un rilevamento più accurato

È noto che per ottenere una migliore precisione di rilevamento, è necessario definire un contesto specifico. Migliore è la definizione di contesto, più accurata sarà la rilevazione, ovvero minore percentuale di falsi positivi e falsi negativi. TrackerDetect ha sviluppato una nuova e innovativa soluzione di rilevamento che si basa sul concetto di **Activity Flow Analytics**, che descrive la sequenza delle attività che gli utenti compiono durante il loro viaggio digitale all'interno delle applicazioni. E' stato dimostrato che l'analisi sulla base della sequenza delle attività produce una maggiore precisione di rilevamento delle anomalie, come viene già ampiamente utilizzato nel caso di protezione di reti e sistemi, come in NetFlow e soluzioni EDR di prossima generazione (vedi lo schema di seguito)



Reveal security

Product Brief

RILEVAMENTO DI COMPORTAMENTI ANOMALI BASATO SULL'ANALISI DEI FLUSSI DI ATTIVITA' ALL'INTERNO DI APPLICAZIONI CORE BUSINESS E SAAS

La sfida di Rilevare Attività Fraudolenti nell'uso delle applicazioni

L'implementazione del rilevamento basato sulla sequenza delle attività al livello applicativo è impegnativo per i seguenti motivi:

Ogni applicazione ha un insieme univoco di operazioni ed azioni ed i log file non hanno formati o contenuti comuni. Questa sfida è aumentata dal numero crescente di applicazioni SaaS utilizzate dalle aziende.

Ogni utente opera su molti flussi di attività per ogni applicazione, il che rende il rilevamento di flussi di attività anomali molto impegnativo.

TrackerIQ™ - Soluzione di Rilevamento e Reazione

Per affrontare le sfide di cui sopra, TrackerDetect ha sviluppato una soluzione di rilevamento e reazione che si basa su un innovativo modello di flusso di attività generalizzato, che può essere applicato su qualsiasi applicazione. Questo modello si basa sulle attività svolte dall'utente, sull'ordine in cui sono state eseguite e sugli intervalli di tempo tra queste attività. Il modello di flusso delle attività è indipendente dal significato delle attività e può consentire un rapido processo di riconfigurazione per l'aggiunta di nuove applicazioni. Poiché ogni utente ha molti flussi di attività per ciascuna applicazione, TrackerIQ apprende per ogni utente (o gruppo di utenti) i suoi profili di flusso di attività. Per apprendere automaticamente i profili del flusso di attività per utente (o gruppo di utenti), TrackerDetect ha sviluppato un motore di clustering (in attesa di brevetto) per raggruppare i flussi di attività dell'utente e generare i profili. Questi profili consentono il rilevamento accurato dei flussi anomali di attività. Per dare la priorità alle anomalie rilevate, TrackerIQ assegna anche un punteggio di rischio a ciascuna anomalia di flusso di attività in base alle sue attività. TrackerIQ genera avvisi per le anomalie rilevate con raccomandazioni personalizzate. Per gli analisti della sicurezza che desiderano indagare sulle anomalie, TrackerIQ fornisce anche strumenti di analisi che consentono loro di comprendere rapidamente l'anomalia e prendere una decisione.

Detection Based on User Journey Analysis

Provides the context for each operation performed by the user to enable accurate detection

Anomalies are prioritized based on their activities' risk

Generalized User Journey 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 Activity Flow clustering engine

Operationally Efficiency

Quick and easy on-boarding

Easy integration with customer's log repositories (Files, Databases, SIEM, SPLUNK/ELK & Syslog)