Reveal security

Case study

Individuazione precoce dei segnali di una frode commessa da un dipendente

Attività dolose individuate:

Un dipendente aveva effettuato delle modifiche ai beneficiari di una polizza e, alcuni giorni più tardi, aveva iniziato a prelevare denaro dalla polizza. I prelievi si erano ripetuti diverse volte.

User journey analizzati:

La sequenza di attività eseguite dai dipendenti per un periodo di un mese (è stato creato un user journey per ogni utente e per ogni mese).

Processo e presupposti:

TrackerIQ ha imparato i profili di lavoro mensili dell'intera organizzazione e quindi li ha utilizzati per individuare percorsi di lavoro anomali o sospetti. Il presupposto di fondo è che, anche se le attività in sé stesse sono normali, gli effettivi percorsi di attacco sono molto insoliti.

Settore:
Assicurativo, società quotata in borsa

Tipo di applicazione:
Customizzata

Utilizzo dell'applicazione:
L'applicazione è usata dai dipendenti dell'azienda per gestire polizze previdenziali integrative e assicurative

Dati analizzati:
Registri di controllo dell'applicazione, compresi dati storici, attività descrittive dell'utente (ovvero il dipendente) nell'ambito dell'applicazione

Risultati dell'analisi di TrackerIQ (sul monitoraggio di 24 mesi di dati dei registri):

- 30 percorsi sono stati contrassegnati come sospetti
- 6 dei percorsi sospetti riguardavano il dipendente che aveva commesso la frode

Alcuni percorsi anomali sono stati individuati nei dati storici ed erano iniziati sei mesi prima che il dipendente commettesse effettivamente la frode. Il dipendente aveva cominciato a effettuare attività simili alla frode finale, ma di valore economico minimo, pari a pochi centesimi. Se la compagnia di assicurazione avesse individuato questi user journey anomali appena erano iniziati, avrebbe potuto chiedere ragione al dipendente delle anomalie, in modo da poter verosimilmente evitare la frode successiva o, in alternativa, avrebbe potuto iniziare a tenere sotto più stretto controllo il dipendente.

Una considerazione importante:

Il monitoraggio dell'attività dei dipendenti e l'attivazione di allarmi relativi a user journey anomali, anche se tali percorsi non sono effettivamente il risultato di azioni dolose, costituisce un controllo preventivo importante, considerando che il numero di allarmi generati è basso (alcuni al mese).

Vantaggi di TrackerIQ

- Rapido adattamento iniziale del modello di rilevazione utilizzando i dati storici, inclusa l'individuazione di precedenti attività sospette
- Monitoraggio costante dei percorsi dei dipendenti per individuare le attività sospette in corso
- Il monitoraggio costante fornisce sia un controllo preventivo che una compensazione della carenza di efficaci politiche di controllo degli accessi all'interno di un'applicazione aziendale esistente (sviluppata anni prima)
- Un minore numero di allarmi al mese (meno di uno alla settimana) consente di concentrare l'attenzione sulle vere attività sospette
- Uno strumento di indagine di facile utilizzo per i business analyst

Reveal security

Case study

Individuazione di impostori esterni in un'applicazione di e-banking

Attività dolose individuate:

Un gruppo di truffatori era riuscito, sfruttando tecniche di social engineering, a prendere di mira diversi clienti, ottenendo le loro credenziali personali (incluse OTP), bypassando così le procedure MFA. I truffatori quindi si erano connessi all'applicazione come clienti legittimi ed erano riusciti a eseguire (diverse) transazioni di trasferimento di denaro (anche ricevendo le OTP necessarie per confermare i bonifici dai conti delle vittime).
I sistemi basati su regole impiegati dalla banca non erano stati in grado di rilevare molti di questi tentativi di truffa e di fatto avevano generato diversi falsi positivi.

User journey analizzati:

La sequenza di attività eseguite dal cliente in una sessione dell'applicazione (è stato creato un user journey per ogni sessione dell'applicazione).

Processo e presupposti:

TrackerIQ ha imparato i percorsi tipici nell'applicazione di e-banking di ciascun cliente, quindi ogni customer journey è stato confrontato con i percorsi tipici appresi per tale cliente. Il presupposto di fondo è che il percorso di un truffatore all'interno dell'applicazione di e-banking è diverso dai percorsi tipici dei clienti.

Settore:
Bancario, società quotata in borsa

Tipo di applicazione:
Customizzata

Utilizzo dell'applicazione:
Un'applicazione di e-banking (web e mobile) usata dai clienti della banca per la gestione dei propri conti. L'applicazione consente ai clienti e effettuare transazioni in denaro verso conti di terzi.

Dati analizzati:
Registri di controllo dell'applicazione che descrivono le attività dell'utente (ovvero il cliente) nell'interno dell'applicazione di e-banking

Risultati dell'analisi di TrackerIQ (sul monitoraggio di 12 mesi di dati dei registri):

- Circa 750 percorsi sono stati contrassegnati come sospetti
- Il 98% dei trasferimenti di denaro dolosi erano stati individuati da TrackerIQ, mentre molti di essi non erano stati rilevati dal sistema basato su regole della banca

Vantaggi di TrackerIQ

- Rapido adattamento iniziale del modello di rilevazione utilizzando i dati storici, inclusa l'individuazione di precedenti attività sospette
- Monitoraggio costante delle attività dei clienti come controllo compensativo di truffatori che riescono a bypassare i meccanismi MFA e altri controlli dei meccanismi di autenticazione, come le OTP
- Un minore numero di allarmi (in media circa due al mese) consente agli analisti di concentrare l'attenzione sulle vere attività sospette
- Uno strumento di indagine di facile utilizzo per i business analyst

Reveal security

Case study

Individuazione di una fuga di dati di Salesforce operata da un dipendente

Attività dolose individuate:

Un dipendente era stato contattato da un concorrente dell'azienda allo scopo di estrarre dati dei clienti per trarne un vantaggio competitivo. Il dipendente aveva utilizzato le proprie autorizzazioni nell'ambito di Salesforce per eseguire report e lavorare con le dashboard, estraendo così i dati richiesti suddivisi in varie tranche (in modo da non ricadere nella regola DLP che fissa una soglia per il numero di righe estratte per mezzo di report o dashboard).

User journey analizzati:

La sequenza di attività eseguite dal dipendente durante una sessione di lavoro in Salesforce.

Processo e presupposti:

TrackerIQ ha imparato i profili delle sessioni dell'intera organizzazione e quindi li ha utilizzati per individuare sessioni (cioè user journey) anomale o sospette. Il presupposto è che, anche se l'esportazione di singoli report è comune, le sequenze di esportazioni di dati per mezzo di report in modalità dettagliata, associate a corrispondenti attività nella dashboard, sono molto inusuali.

Settore:
Assicurativo, società quotata in borsa

Tipo di applicazione:
SaaS (Salesforce Sales Cloud).

Utilizzo dell'applicazione:
L'applicazione è il principale sistema CRM dell'azienda, usato dai dipendenti per gestire le interazioni con i clienti.

Dati analizzati:
Registri di controllo dell'applicazione generati da Salesforce e disponibili nell'ambito della sua licenza di Monitoraggio evento. Tali file di registro controllano le attività dell'utente (ovvero il dipendente) nell'ambito di Salesforce.

Risultati dell'analisi di TrackerIQ (sul monitoraggio di 5 mesi di dati dei registri di SFDC):

- 4 percorsi sono stati contrassegnati come sospetti (circa 1 al mese)
- 1 dei percorsi sospetti era del dipendente responsabile della fuga di dati

Anche le anomalie di natura non dolosa erano rilevanti, perché consentivano l'individuazione di potenziali fughe di dati e la possibilità di richiedere ai dipendenti di spiegare il motivo dell'esportazione dei dati.

Feedback del cliente:

Il monitoraggio delle attività dei dipendenti e la generazione di allarmi in merito a user journey anomali, anche se non dolosi, è utile come controllo preventivo, considerato il modesto numero di allarmi generati (alcuni al mese). L'alternativa usata aveva consentito il verificarsi di vere fughe di dati non individuate, come nel caso in cui in passato l'organizzazione aveva implementato una regola per rilevare report con grandi numeri di righe e, come risultato, aveva ottenuto decine di allarmi a settimana (falsi positivi).

Vantaggi di TrackerIQ

- Rapido adattamento iniziale del modello di rilevazione utilizzando i dati storici, inclusa l'individuazione di precedenti attività sospette
- Monitoraggio costante dei percorsi dei dipendenti per individuare le attività sospette come controllo preventivo
- Una soluzione pronta per l'uso: nessuna necessità di imparare i registri di Salesforce in profondità e/o sviluppare regole per Salesforce
- Un minore numero di allarmi al mese (circa 1-2) consente di concentrare l'attenzione sulle attività veramente sospette
- Uno strumento di indagine di facile utilizzo per i business analyst

Reveal security

Case study

Individuazione di una fuga di dati di Office 365 da parte di un truffatore

Attività dolose individuate:

Un dipendente ha dato le proprie credenziali a un gruppo di criminali (l'ipotesi è che il dipendente abbia venduto le credenziali o sia stato ricattato affinché le fornisse). Il gruppo di criminali ha usato tali credenziali per accedere a Office 365 dalla stessa geolocalizzazione del dipendente e quindi ha utilizzato le autorizzazioni del dipendente per consultare informazioni riservate (si presume che abbia acquisito determinate schermate che mostravano dati sensibili). I meccanismi CASB e ATO non sono stati efficaci dato che i criminali hanno utilizzato le credenziali del dipendente; anche le regole DLP non hanno funzionato perché i file non sono stati scaricati o condivisi.

User journey analizzati:

La sequenza di attività eseguite dai dipendenti durante una sessione di lavoro nell'ambito della suite di applicazioni di Office 356.

Processo e presupposti:

TrackerIQ ha imparato i profili delle sessioni di lavoro dell'intera organizzazione e di ciascun utente, quindi li ha utilizzati per individuare sessioni (cioè user journey) anomale/sospette. Il presupposto di fondo è che le sequenze di attività di un truffatore non corrispondono ai normali profili di lavoro (né dell'intera organizzazione né di un singolo).

Settore:
Bancario, società quotata in borsa

Tipo di applicazione:
SaaS (Microsoft Office 365)

Utilizzo dell'applicazione:
Il principale strumento di collaborazione per i dipendenti dell'azienda. Il carico di lavoro principale usato in azienda interessa AAD (Azure Active Directory), Exchange, SharePoint, OneDrive, Teams, PowerBI, ecc.

Dati analizzati:
Registri di controllo generati da Office 365 e disponibili nell'ambito della sua licenza E3/E5. I file di registro controllano le attività dell'utente (ovvero il dipendente) nell'ambito della suite di applicazioni di Office 365.

Risultati dell'analisi di TrackerIQ (sul monitoraggio di 6 mesi di dati dei registri di Office 365):

- TrackerIQ genera 1-2 allarmi al giorno per l'intero utilizzo di Office 365
- L'impostore è stato identificato (nel giro di alcune ore dall'evento)
- Sono state individuate alcune altre attività dolose, tra cui una serie di attività rilevate soltanto da TrackerIQ (ovvero ignote all'organizzazione senza TrackerIQ)

Anche l'individuazione di anomalie di natura non dolosa era importante per il cliente. Ai dipendenti è stato richiesto di spiegare i motivi di qualsiasi deviazione dai normali profili di lavoro.

Feedback del cliente:

Il monitoraggio delle attività dei dipendenti e la generazione di allarmi relativi a user journey anomali, anche se non dolosi, è importante come controllo preventivo, considerato il modesto numero di allarmi generati (es. 1-2 al giorno).

Vantaggi di TrackerIQ

- Rapido adattamento iniziale del modello di rilevazione utilizzando i dati storici, inclusa l'individuazione di precedenti attività sospette
- Monitoraggio costante dei percorsi dei dipendenti per individuare le attività sospette in corso e come controllo preventivo
- Una soluzione pronta per l'uso: nessuna necessità di imparare i registri di Office 365 in profondità e/o sviluppare regole per Office 365
- Un minore numero di allarmi mensili (circa 1-2 al giorno consente di concentrare l'attenzione sulle vere attività sospette
- Uno strumento di indagine di facile utilizzo per i business analyst