WHITE PAPER | MARZO 2017

Enterprise Data Security: le basi delle analisi comportamentali

Sommario

Executive summary

Oggi, le segnalazioni relative ad attacchi informatici dominano le cronache. E mentre la maggior parte degli attacchi di alto profilo, incluse violazioni significative dei sistemi di aziende come JP Morgan, Anthem e Slack, hanno origine al di fuori dell'azienda, sottrazione e utilizzo improprio dei dati da parte degli utenti privilegiati sono in aumento.

In effetti, il 69% dei professionisti della sicurezza enterprise dichiara di essere stato vittima di furto o alterazione di informazioni aziendali a opera di insider considerati affidabili.[1] Si sono anche verificati casi in cui consulenti terzi, fornitori o partner della società sono stati responsabili di violazioni di rete, attraverso comportamenti dolosi o involontari.

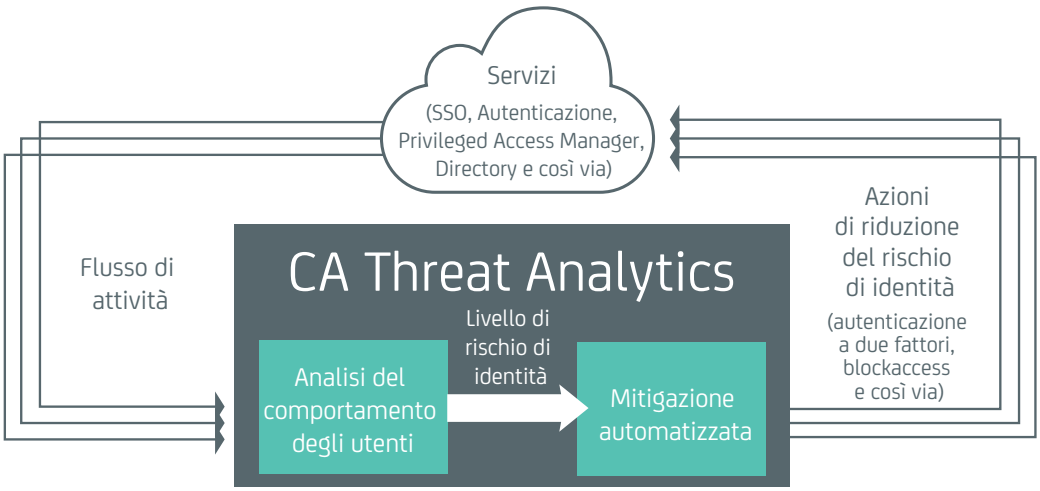
Se eventi come questi insegnano qualcosa, è che la protezione degli accessi privilegiati resta una grande preoccupazione per le aziende di tutte le dimensioni. Nonostante questa consapevolezza, e un surplus di prodotti di sicurezza disponibili, molti sistemi IT restano tuttora vulnerabili agli attacchi.

Il fatto è che i controlli IAM (Identity and Access Management) tradizionali, per quanto estesi, sono statici. E una volta che un utente malintenzionato ottiene l'accesso, è libero di sfruttare il sistema nella misura consentita dai privilegi definiti dell'account.

Tuttavia, tramite il deployment di un approccio alla sicurezza basato sull'identità, che riunisce analisi del comportamento degli utenti e rilevazione delle anomalie in un modello capace di auto-apprendimento, le aziende possono rilevare rapidamente eventuali attività a rischio e far scattare automaticamente controlli correttivi per limitare i danni per l'impresa.

CA Threat Analytics

CA Threat Analytics protegge i dati enterprise con modalità analoghe a quelle con cui le carte di credito proteggono il denaro. Pur rimandando ai concetti corretti, monitoraggio costante e impiego di strumenti di analisi per determinare il rischio e impedire ai "cattivi" di sottrarre risorse, questa similitudine non spiega come tali obiettivi siano raggiunti. Questo white paper descrive in che modo CA Threat Analytics protegge i dati aziendali utilizzando due funzioni correlate: analisi del comportamento degli utenti e mitigazione automatizzata.



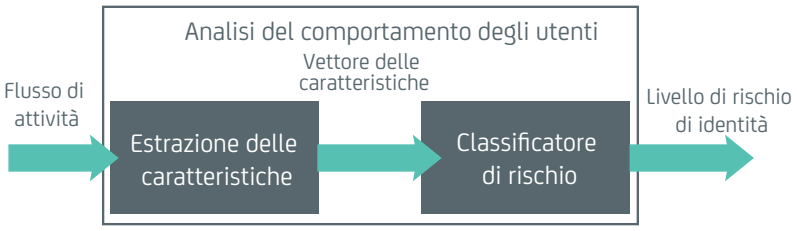
L'analisi del comportamento degli utenti consente all'impresa di valutare costantemente i rischi e di individuare rapidamente le attività dannose. Come input, l'analisi del comportamento degli utenti acquisisce un flusso di dati relativi al modo in cui una determinata identità o gruppo di identità interagisce con servizi o applicazioni, e quindi genera un livello di rischio associato a ogni identità enterprise.

La mitigazione automatizzata consente all'impresa di adottare automaticamente misure che attenuano il rischio e contrastano le attività dannose individuate. L'attenuazione automatica modifica le modalità di controllo degli accessi per le singole identità in base all'output di rischio generato dall'analisi del comportamento degli utenti. Un semplice esempio di mitigazione automatica consiste nel bloccare automaticamente l'accesso ad alto rischio di un'identità, per un'applicazione o un repository di dati particolarmente sensibile.

Anche se analisi del comportamento degli utenti e mitigazione automatizzata sono entrambe essenziali al funzionamento di CA Threat Analytics, questo white paper si concentra volutamente sul primo. Nelle sezioni che seguono, la funzione di analisi del comportamento degli utenti rappresentata in figura sarà suddivisa nei suoi elementi costitutivi. Questi elementi saranno poi discussi singolarmente nel dettaglio. Per semplicità, la discussione si concentra inizialmente sulla protezione di una singola identità su un unico servizio. Dopo aver spiegato le basi delle tecniche utilizzate, vedremo come questi concetti possono essere raffinati quando si opera con una popolazione di identità su più servizi.

Le basi

Concettualmente, la funzione di analisi del comportamento degli utenti è costituita da due componenti: estrazione di caratteristiche e classificatore di rischio.



Il componente di estrazione elabora un flusso di attività e ne estrae un insieme di caratteristiche rilevanti. Le caratteristiche rilevanti sono caratteristiche di una singola identità che sono state osservate nel tempo, come ad esempio:

- L'identità utilizza un device mobile sconosciuto.
- L'identità opera da una posizione remota.
- L'identità proviene da un indirizzo IP sospetto.
- L'identità è un membro di un gruppo privilegiato.
- L'identità ha utilizzato il servizio X al di fuori del suo periodo di funzionamento normale.

L'operazione di estrazione delle caratteristiche è più complicata di quanto sembri, perché non si applica semplicemente a una transazione in corso. Sebbene un flusso di attività venga acquisito come sequenza di eventi separati, l'input effettivo è rappresentato dal flusso completo dell'attività dal suo primo inizio. Questo consente di comprendere utilizzo e comportamento aggregati di ogni identità. Senza esaminare la cronologia completa dell'attività, sarebbe necessario valutare il rischio esclusivamente in base a ogni singolo evento preso individualmente.

Utilizzando un esempio basato sulle caratteristiche citate, cosa significa "periodo di funzionamento normale" nel contesto di un singolo evento? Perché CA Threat Analytics sia in grado di utilizzare caratteristiche determinanti come questa, deve poter calcolare e utilizzare informazioni utili relative anche ai dati storici.

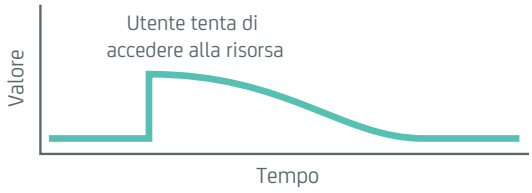
Esaminando il flusso completo dell'attività, CA Threat Analytics fornisce all'impresa una comprensione molto più ampia di quella disponibile in precedenza per valutare il rischio e rilevare attività dannose. L'impresa è ora in grado di valutare il rischio sulla base delle attività passate e di informazioni specifiche sulle singole identità. Questo vantaggio ha un costo, rappresentato dall'esigenza di elaborare un volume elevato di dati, molti dei quali ridondanti. Fortunatamente, eseguendo l'estrazione delle caratteristiche, la dimensionalità dei dati risulta ridotta. La funzione elimina o aggrega i dati ridondanti, evidenziando le informazioni necessarie alla seconda componente della funzionalità di analisi del comportamento degli utenti: il classificatore di rischio.

Determinare il valore nel contesto temporale

Prima di passare oltre, vogliamo evidenziare un dettaglio interessante relativo alle caratteristiche osservate nel tempo. Queste, dato che si modificano all'arrivo delle attività, esistono tecnicamente in un ambito temporale: ovvero, semplicemente, i relativi valori si modificano nel tempo. Quando viene osservata una caratteristica, CA Threat Analytics ne modella l'osservazione come funzione temporale. In altre parole, se un'attività in ingresso causa l'attivazione di una caratteristica, il "valore" di questa può essere al suo massimo al momento di tale attività per poi modificarsi.

La modalità effettiva di tale modifica varierà notevolmente a seconda della caratteristica che è stata estratta. Alcune attività sono totalmente binarie: quindi, quando la caratteristica viene osservata, rimangono al loro valore massimo fino a quando qualcosa procede alla mitigazione, come di seguito.

Un esempio potrebbe essere l'appartenenza a un gruppo sensibile. Il valore per questa caratteristica rimane al massimo per l'intero periodo di tempo in cui l'identità è associata al gruppo. Altre caratteristiche sono modellate come impulsi a riduzione progressiva. Quando viene osservata una caratteristica di questo tipo, il valore è al suo massimo al momento dell'osservazione e si riduce nel tempo, come di seguito.



Un esempio potrebbe essere il caso in cui un utente tenta di accedere a una risorsa per la quale non è dotato di autorizzazione. Anche se questa caratteristica oggi è rilevante per il livello di rischio di un'identità, lo sarà molto meno tra una settimana, e ancora meno tra un mese. Mediante il decadimento del valore delle caratteristiche nel tempo, CA Threat Analytics assicura che esse contribuiscano al rischio nel modo più rilevante possibile.

Il classificatore di rischio

Il classificatore di rischio è una funzione analitica che converte il vettore delle caratteristiche in tre livelli di rischio distinti:

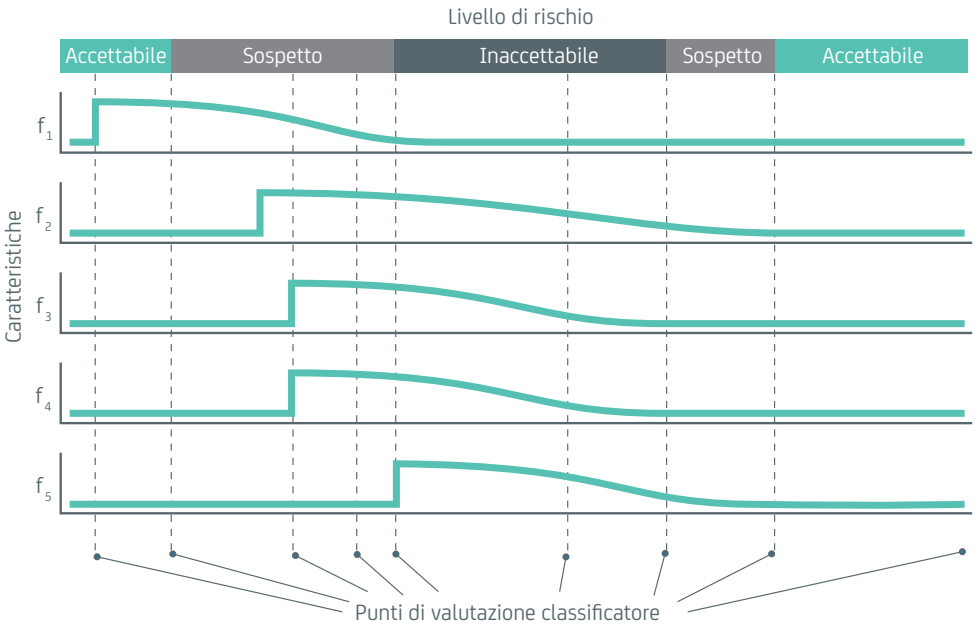
- **Accettabile**: l'identità pone un rischio minimo.
- **Sospetto**: l'identità è stata associata a eventi o attività che comportano un rischio, ma questo non richiede un intervento immediato. Il sistema terrà sotto controllo questa identità più da vicino e potrà avviare una prima serie di misure di mitigazione automatica, in base alla policy aziendale.
- **Inaccettabile**: l'identità è considerata ad alto rischio e richiede attenzione immediata. Il sistema avvierà la mitigazione e genererà avvisi automatici, in base alla policy aziendale.

Le funzioni del classificatore di rischio utilizzano come input un vettore di valori delle caratteristiche, e generano come output una delle classi distinte di cui sopra.

$$\text{Classificatore}(\text{caratteristiche}(t)) \longmapsto \{\text{accettabile, sospetto, inaccettabile}\}$$

Come discusso in precedenza, le stesse caratteristiche sono una funzione temporale, per cui anche la funzione di classificazione del rischio opera nell'ambito temporale. Il classificatore di rischio viene richiamato nei momenti decisionali critici, di solito in risposta a cambiamenti significativi nei valori del vettore delle caratteristiche. Ogni volta che il livello di rischio viene calcolato dal classificatore di rischio per un dato punto nel tempo, tutte le funzioni della caratteristica vengono valutate per tale identità o entità in quel momento. La serie completa di caratteristiche attive per l'entità in quel momento compongono il vettore delle caratteristiche effettivamente impiegato dal classificatore di rischio, e utilizzato per determinare il rischio stesso.

Nella seguente figura sono indicati i singoli punti in cui il classificatore di rischio verrà probabilmente utilizzato. Come indicato, le valutazioni si verificano quando una caratteristica aumenta di valore, e quando il suo valore scende al di sotto di una determinata soglia. I valori passati al classificatore di rischio equivalgono al valore di ogni caratteristica al momento in cui la valutazione viene attivata, corrispondente alle linee verticali sopra. Naturalmente, non ogni esecuzione del classificatore di rischio determina un nuovo livello di rischio. In pratica, i punti di valutazione sono molto più numerosi che nell'immagine, e corrispondono a variazioni di valore della caratteristica, all'attività del sistema, a intelligence sulle minacce. In generale, il classificatore di rischio viene attivato ogni volta che potrebbe essersi verificato un cambiamento nel livello di rischio.



Cos'è allora il classificatore di rischio? Come traduce un vettore delle caratteristiche in uno di un insieme distinto di classi di rischio? Può aiutare partire dalla definizione di cosa non è il classificatore. I classificatori di rischio di CA Threat Analytics non sono semplici regole che eseguono test relativi a caratteristiche specifiche, come "se la caratteristica X è attiva, restituisci non accettabile". Si tratta di un approccio semplicistico, utilizzato da molti prodotti di sicurezza tradizionali. Questo approccio fallisce totalmente perché è fortemente incline ai falsi positivi, è poco robusto e viene superato facilmente. Inoltre, non fa uso di informazioni che sono fondamentali sia per la rilevazione dell'attività dannosa, sia per rendere il sistema utilizzabile dagli utenti legittimi.

Le capacità di CA Threat Analytics sono notevolmente più solide. Il classificatore di rischio di CA Threat Analytics non esamina le caratteristiche nel vuoto, ma nel contesto del loro insieme completo. Grazie a questo approccio, caratteristiche diverse, che in isolamento non hanno alcun impatto sul livello di rischio, possono combinarsi per influenzarlo in modo significativo. Non solo: CA Threat Analytics incorpora il feedback proveniente dai sistemi distribuiti, compresi aspetti collegati ai singoli utenti e modifiche della popolazione di identità, per affinare le proprie decisioni nel corso del tempo. Il risultato è un sistema che fornisce la flessibilità necessaria per adattarsi alle nuove minacce e ai nuovi scenari di deployment.

Popolazioni e servizi

Come accennato in precedenza, molti dettagli pratici sono stati semplificati ai fini della discussione di cui sopra. Partiamo dalle popolazioni di identità. Soprattutto in ambiente enterprise, alcuni aspetti del gruppo di identità sono rilevanti per il livello di rischio per una determinata identità. Alcuni esempi:

- Accesso alle risorse con più device di quanto sia normale per l'azienda
- Operatività in un luogo diverso dalla posizione normale per il gruppo
- Numero di gruppi eccessivamente ampio

Le linee di base delle attività previste, che includono fattori come il numero normale di device associati a un utente, le sedi operative dell'azienda, il numero appropriato di gruppi, sono diverse per ogni azienda. Osservando un gruppo di identità, piuttosto che le identità in isolamento, è possibile ottenere un livello elevato di statistiche demografiche utili, rispetto al quale è possibile confrontare le singole identità. Naturalmente, tutto questo ha un costo. Anziché limitarsi a elaborare l'intero flusso di attività per un'identità, richiede l'esecuzione dell'estrazione delle caratteristiche sulla cronologia completa dell'attività, per l'intera azienda.

In modo analogo, l'estensione dell'analisi da un unico servizio a un gruppo di servizi offre un diverso livello di vantaggi. Esaminando le azioni di un'identità su diversi servizi, è possibile estrarre le caratteristiche per costruire modelli di modelli di accesso tipici e applicarli in modo intelligente, per fornire sicurezza tra servizi diversi. Queste informazioni consentono a CA Threat Analytics di rilevare comportamenti anomali e incoerenti che rappresentano una minaccia per l'identità o l'azienda.

Conclusioni

Questo white paper illustra in sintesi in che modo CA Threat Analytics protegge i dati enterprise mediante l'analisi del comportamento degli utenti. Anche se i concetti di base sono semplici da spiegare, le problematiche pratiche collegate all'estrazione delle caratteristiche e alla classificazione dei rischi vanno ben oltre la portata di questo documento. In effetti, molti dei requisiti reali sui quali si basa il lavoro del nostro team non sono stati nemmeno menzionati, ad esempio rendere possibile il processo decisionale in tempo reale, garantire la precisione del sistema nel tempo e fornire gli amministratori di sistema intelligence reale in relazione alle decisioni di rischio.

Se sei interessato a saperne di più su questi elementi e su come la tua azienda può beneficiarne, consulta: https://www.ca.com/us/products/ca-threat-analytics-for-privileged-access-manager.html

Entra in contatto con CA Technologies all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies lavora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visita il sito **ca.com/it**.

1 Accenture e HfS Research, "The State of Cyber Security and Digital Trust 2016", giugno 2016: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50

CS200-259092