Guida all'acquisto delle soluzioni di gestione delle minacce interne

Questa guida all'acquisto mette in evidenza le funzionalità più importanti di una soluzione di gestione delle minacce interne (ITM, Insider Threat Management). Riassume ciò che Proofpoint ha appreso dalla creazione di programmi ITM efficaci per aziende di tutte le dimensioni in tutto il mondo e in tutti i settori. Vuole essere una guida di riferimento sia che tu stia iniziando a gestire questa problematica o che desideri modernizzare la tua soluzione ITM esistente.

Sicurezza incentrata sulle persone

Per proteggere i dati dalle minacce interne, hai bisogno di una soluzione che supporti un modello di sicurezza incentrata sulle persone, Questo tipo di modello fornisce visibilità completa sui comportamenti a rischio degli utenti e sulle loro interazioni con i dati sensibili. In questo modo ottieni informazioni contestuali importanti sulle loro intenzioni quando le loro azioni sembrano pericolose per l'azienda, in modo intenzionale o meno.

Grazie a una soluzione incentrata sulle persone, puoi valutare rapidamente i tuoi rischi interni basati su indicatori comportamentali. Quando questi indicatori vengono considerati in modo globale, nel corso del tempo e nel contesto di altre attività, possono rivelare che un utente potrebbe nuocere a un'azienda e giustificare ulteriori indagini per determinare la risposta più appropriata.

Elementi chiave di una soluzione ITM

Se desideri bloccare le minacce interne, devi essere in grado di identificare, proteggere, prevenire e neutralizzare gli incidenti legati a queste minacce particolari. Solo compiendo tutte queste azioni in modo coordinato con un approccio proattivo puoi limitare il rischio di minacce interne.

Identificare

Hai bisogno di una soluzione che fornisce visibilità sui comportamenti a rischio prima che si verifichi una minaccia interna. Devi poter identificare i comportamenti anormali secondo in base a valori di riferimento. La soluzione deve permettere il monitoraggio degli utenti a rischio, come gli utenti con accesso con privilegi, i collaboratori in uscita dall'azienda o che stanno per farlo, liberi professionisti, dirigenti e utenti oggetto di indagini. L'identificazione degli utenti a rischio può tenere conto di specifici fattori di innesco come un cambiamento dello stato del collaboratore (licenziamento o dimissioni), cambiamenti nella struttura aziendale (fusione, acquisizione o riorganizzazione) e comportamenti preoccupanti (espressioni di malcontento, conflitti finanziari, ecc.).

Ogni azienda deve decidere quali controlli di prevenzione implementare sulla base dei loro obiettivi aziendali, cultura e velocità di innovazione.

Proteggere

La soluzione ITM adottata deve contribuire a proteggere dati sensibili e sistemi con controlli di sicurezza incentrati sulle persone. Policy e regole devono integrare indicatori comportamentali per rafforzare la protezione contro i comportamenti a rischio.

È importante impedire a un utente di violare intenzionalmente o meno le policy di sicurezza attraverso formazione adeguata, promemoria in tempo reale e funzionalità di blocco. Naturalmente, non tutte le attività possono o devono essere bloccate: la prevenzione non deve ostacolare la produttività degli utenti. Ogni azienda deve decidere quali controlli di prevenzione implementare sulla base dei loro obiettivi aziendali, cultura e velocità di innovazione.

È inoltre importante che una soluzione ITM fornisca un modo semplice e flessibile per gestire l'accesso ai dati dell'utente. La soluzione implementata deve disporre di controlli d'accesso per garantire che gli analisti di sicurezza abbiano visibilità sui dati solo se davvero necessario.

Rilevare

Una soluzione ITM deve fornire attività e avvisi in tempo reale sui comportamenti degli utenti. Le attività a rischio che possono attivare degli avvisi includono le seguenti:

- Mascheramento delle informazioni
- Incremento dei privilegi
- Aggiramento dei controlli di sicurezza
- Sottrazione di dati
- Download di software non approvati
- Sabotaggio informatico
- Creazione di una backdoor
- Accesso non autorizzato
- Utilizzo inaccettabile

Quando una regola viene violata, la soluzione deve essere in grado di acquisire tutti i dettagli (chi, cosa, quando e dove) dell'attività dell'utente per fornire un contesto preciso e informazioni pertinenti sui comportamenti e le intenzioni associate. La soluzione deve anche acquisire schermate per poter fornire prove irrefutabili nell'ambito delle indagini. Deve anche offrire la flessibilità necessaria per rispondere dinamicamente a comportamenti a rischio e acquisire schermate solo dopo la generazione di un avviso, contribuendo a proteggere la privacy dell'utente e permettendo agli analisti della sicurezza di lavorare in modo più efficiente.

Gli utenti negligenti sono la causa principale della perdita di dati e delle minacce interne. Sebbene animati da buone intenzioni, questi utenti commettono degli errori, che possono avere gravi conseguenze.

Rispondere

È importante indagare e rispondere in modo rapido ed efficiente in caso di incidente. Più tempo è necessario per neutralizzare una minaccia interna, più danni può causare in termini di risultati finanziari e reputazione. I flussi di lavoro delle indagini sono fondamentali per tracciare lo stato di un incidente, in particolare quando è necessario rivolgersi a gruppi esterni alla sicurezza, come le risorse umane, l'ufficio legale, la conformità e la privacy, che potrebbero dover essere coinvolti in un'indagine su un incidente. Una solida soluzione ITM deve anche essere integrata con un sistema di gestione degli eventi centralizzato, come una soluzione SIEM, che il team di analisti della sicurezza utilizza già.

Tre principali scenari di perdita di dati

Esistono tre tipi principali di minacce interne. Tutti sono causati da un intervento umano. Una soluzione ITM incentrata sulle persone deve poter identificare questi tre tipi, ovvero:

- **Utenti negligenti.** Persone disattente che commettono errori.
- **Utenti malintenzionati.** Persone che cercano di danneggiare l'azienda.
- **Utenti compromessi.** Persone le cui credenziali di accesso sono state rubate da un criminale informatico esterno.

1. Utenti negligenti e errori comuni

Secondo il report Data Loss Landscape 2024 di Proofpoint, gli utenti negligenti sono la principale causa di perdita di dati e minacce interne. Si tratta di utenti animati da buone intenzioni ma che commettono degli errori. Spesso, desiderano solo svolgere il loro lavoro nel modo più efficiente possibile, tuttavia, i loro errori possono avere gravi conseguenze: interruzione delle attività, danni alla reputazione, indebolimento della posizione concorrenziale, violazioni normative e sanzioni, cause legali, ecc.

Ecco alcuni esempi di azioni a rischio di questi utenti:

- Invio di email al destinatario errato, con o senza allegati
- Condivisione di dati sensibili sui siti di IA generativa
- Consultazione di siti phishing
- Installazione di software non autorizzati
- Condivisione pubblica di file e dati sensibili
- Invio tramite email di informazioni personali a un account email personale
- Archiviazione di dati aziendali sensibili su dispositivi personali

Gli utenti malintenzionati sono pericolosi perché si trovano nella posizione ideale per appropriarsi di dati sensibili e danneggiare l'azienda. Sono motivati dal loro interesse personale.

Protezione contro i comportamenti negligenti

Una soluzione ITM efficace permette di rilevare e prevenire le attività a rischio. Deve inoltre formare gli utenti negligenti per aiutarli a comprendere cosa c'è di sbagliato nel loro comportamento affinché possano cambiarlo.

Elementi indispensabili:

- **Classificazione.** Verifica che email, dati e contenuti vengano monitorati costantemente sia manualmente che con l'intelligenza artificiale (IA) per identificare e classificare gli utenti a rischio. Se l'utente è considerato a rischio elevato, il sistema assegnerà un punteggio di rischio per proteggere i dati di conseguenza.
- **Monitoraggio.** La soluzione deve monitorare comportamenti e attività a rischio come l'uso non autorizzato di web e applicazioni, la modifica di nomi e tipi di file di documenti sensibili, l'accesso a dati al di fuori dell'ambito del loro ruolo o la sottrazione di un elevato numero di documenti riservati. Il monitoraggio di gruppi ad alto rischio può permettere di identificare gli utenti che hanno bisogno di un monitoraggio più approfondito.
- **Prevenzione.** Agli utenti deve essere impedito di esfiltrare dati sensibili dall'endpoint: email inviate al destinatario errato con o senza allegati, chiavette USB, caricamento su web, sincronizzazione cloud, condivisione di rete, stampa, ecc. Se commettono un errore, questi utenti devono ricevere immediatamente un messaggio di avvertimento contestuale, permettendo loro di correggerlo e prevenire l'incidente in tempo reale senza intervento dell'amministratore. Se necessario, gli utenti possono spiegare perché hanno bisogno di accedere ai dati. Di conseguenza, il team della sicurezza può autorizzare o rifiutare tale richiesta.
- **Formazione costante.** Gli utenti negligenti spesso non si rendono conto che il loro comportamento è pericoloso. Una soluzione ITM deve fornire formazione e sensibilizzazione agli utenti attraverso notifiche di comportamenti pericolosi e link alle policy aziendali.

2. Utenti malintenzionati

Gli utenti malintenzionati sono pericolosi perché si trovano nella posizione ideale per appropriarsi di dati sensibili e danneggiare l'azienda. Inoltre, sono motivati dall'interesse personale. I collaboratori in uscita dall'azienda sono uno dei tipi più pericolosi di utenti interni ma ne esistono molti altri tipi.

I principali tipi di minacce interne dannose sono i seguenti:

- **Frode.** Atto ingannevole che provoca un'interruzione dell'attività aziendale.
- **Sabotaggio.** Azione che causa danni a un sistema o la distruzione di dati.
- **Furto.** Furto di informazioni proprietarie di valore per l'azienda.
- **Spionaggio.** Appropriazione e vendita di dati preziosi, segreti commerciali e altro a un concorrente o avversario

Un sistema incentrato sulle persone monitora più da vicino alcuni utenti rispetto ad altri e applica controlli di sicurezza più rigorosi agli utenti più a rischio

Ciò che rende gli utenti interni malintenzionati una tale minaccia è che si trovano in una posizione di fiducia. Possono restare in attesa e utilizzare il loro accesso con privilegi per trovare dati preziosi e sfruttare falle nella sicurezza. Inoltre, le aziende spesso creano vulnerabilità consentendo ai collaboratori di consultare e archiviare i dati sui loro dispositivi personali. Ciò rende più facile rubare dati sensibili e causare danni.

Protezione contro gli utenti malintenzionati

Un sistema incentrato sulle persone può monitorare più da vicino alcuni utenti rispetto ad altri, applica controlli di sicurezza più rigorosi agli utenti più a rischio e blocca proattivamente le azioni dannose in base ai fattori di rischio, come in caso di dimissioni o licenziamento.

Elementi indispensabili:

- **Visibilità.** La visibilità sugli spostamenti dei dati e i comportamenti fornisce una visione olistica e informazioni contestualizzate sulle attività di un utente e le sue intenzioni. Dovrebbero essere raccolti dati di telemetria sulle interazioni degli utenti con i dati e i sistemi, come quando rinominano un file sensibile o lo caricano su un sito web non autorizzato o in una cartella sincronizzata nel cloud. Se un utente scarica applicazioni non autorizzate, altera i controlli di sicurezza o installa un browser TOR, è necessario monitorare queste attività a rischio. Una cronologia degli eventi contestualizzata aiuta a comprendere tutti i dettagli (chi, cosa, quando, dove) delle attività degli utenti e fornirà informazioni su cosa un utente stava facendo prima e dopo un avviso.
- **Libreria delle minacce.** Una libreria di avvisi per i casi di minacce interne più comuni (come frode sull'orario di lavoro, esfiltrazione di dati, elusione dei controlli di sicurezza, ecc.) è fondamentale. In questo modo potrai essere subito operativo, con regole che permettono di identificare gli indicatori comportamentali più frequenti.
- **Indagini.** Scegli una soluzione che fornisce metadati dettagliati e schermate delle attività degli utenti, che possono servire come prove nell'ambito di indagini forensi. I flussi di lavoro collaborativi sono importanti per gestire gli incidenti legati alle minacce interne. Poiché le indagini sulle minacce interne coinvolgono parti interessate esterne al team della sicurezza (team che si occupano di risorse umane, questioni legali, privacy e conformità, per esempio), è necessario condividere i report sui rischi legati agli utenti in formati facili da consultare e interpretare, come documenti in formato PDF.
- **Controlli della privacy.** Una solida soluzione ITM include funzioni come i controlli d'accesso basati su attributi, mascheramento e anonimizzazione dei dati e supporto dei data center multiregionali. Permetterà anche di soddisfare i requisiti di privacy e residenza dei dati ed eliminare i pregiudizi nelle indagini. Deve permettere di modificare in modo dinamico e flessibile una policy di monitoraggio degli utenti in tempo reale se un utente attiva un avviso, assicurando così la privacy degli utenti acquisendo le schermate solo quando necessario.

3. Utenti compromessi

Gli account degli utenti compromessi possono essere controllati e utilizzati in modo inappropriato da un criminale informatico esterno. Una volta violati gli account, i criminali informatici hanno un accesso con privilegi ai tuoi dati e sistemi. La situazione è ancor più problematica dato che spesso i sistemi interni vengono compromessi per diversi mesi prima che l'attacco venga rilevato.

I criminali informatici esterni sfruttano e vulnerabilità del fattore umano. Il social engineering, e in particolare, il phishing, è una delle tecniche più comuni con cui i criminali informatici manipolano gli utenti. Non c'è da stupirsi, visto il tasso di successo elevato di questo tipo di attacchi: il 71% delle aziende ha subito un attacco di phishing andato a buon fine.

Le tecniche di phishing comuni includono:

- Invio di link dannosi, allegati pericolosi e richieste di dati
- SMiShing (phishing tramite SMS)
- Phishing tramite social media
- Attacchi tramite telefonate (TOAD, Telephone Oriented Attack Delivery)
- Violazione dell'email aziendale (BEC, Business Email Compromise)
- Autenticazione a più fattori (MFA)

L'obiettivo dei criminali informatici è sempre lo stesso: ottenere l'accesso a dati e sistemi di valore, da sfruttare a loro vantaggio e a scopo di lucro.

Protezione contro gli utenti compromessi

Una soluzione IT efficace deve fornire visibilità e contesto per aiutare a comprendere se il comportamento di un utente è insolito. Se un utente è incline a fare clic su un link di phishing, per esempio, puoi monitorare quell'utente a rischio per individuare tutti i comportamenti insoliti. Puoi anche proteggere i dati assicurando che possano essere consultati solo da persone specifiche, se assolutamente necessario.

Elementi indispensabili:

- **Monitoraggio proattivo.** Creando e registrando esplorazioni personalizzate, i tuoi team possono andare alla ricerca di esfiltrazioni di dati e attività rischiose. Le persone più attaccate o VAP (Very Attacked People), che sono inclini a fare clic su link o allegati o a interagire con applicazioni vulnerabili, possono essere monitorati per rilevare comportamenti insoliti, che possono indicare che si tratta di un utente compromesso. Lo stesso approccio può essere utilizzato per altri gruppi ad alto rischio come i collaboratori in uscita dall'azienda o gli utenti con accesso con privilegi. Poiché è impossibile identificare tutti gli utenti interni a rischio in anticipo, la soluzione ITM deve essere in grado di modificare in modo dinamico e flessibile la policy di monitoraggio di un utente in tempo reale se quest'ultimo fa scattare un avviso.
- **Controlli adattivi degli accessi.** Puoi applicare regole di accesso condizionali ai dati, come l'inserimento di paesi, reti o indirizzi IP ad alto rischio nell'elenco di quelli autorizzati e/o di quelli bloccati. Puoi anche limitare l'accesso ai dati sensibili a determinati utenti e gruppi con privilegi e autorizzare upload e download solo sui dispositivi gestiti. Grazie al controllo degli accessi basato sugli attributi, puoi rispettare i requisiti in termini di privacy.
- **Integrazioni.** Una soluzione ITM efficace completerà il tuo sistema di sicurezza, aggiungendo contesto agli eventi. Può essere integrata facilmente con diversi strumenti, tra cui:
  - Orchestrazione, automazione e risposta agli incidenti di sicurezza (SOAR)
  - Gestione degli eventi e delle informazioni di sicurezza (SIEM)
  - Risposta agli incidenti
  - Gestione dei ticket
- **Architettura moderna.** Il vantaggio di una piattaforma nativa nel cloud è che può supportare centinaia di migliaia di utenti. Una soluzione ITM deve acquisire i dati di telemetria attraverso un agent endpoint leggero che non ostacoli la produttività dell'utente o entri in conflitto con altre soluzioni.

Conclusione

Per proteggere la tua azienda dai rischi interni, intenzionali o meno, è necessaria una soluzione ITM che permette un approccio proattivo. Una soluzione di questo tipo deve avere visibilità sui comportamenti a rischio e la capacità di rispondere in modo automatico e dinamico. Data la collaborazione trasversale richiesta per gestire i rischi legati alle minacce interne, tale soluzione deve abilitare flussi di lavoro delle indagini e essere in grado di raccogliere prove irrefutabili, come le schermate, per supportare e velocizzare le indagini. Infine, una soluzione ITM deve essere in grado di scalare di pari passo con la tua azienda, sfruttare i tuoi investimenti esistenti e fornire accesso flessibile e controlli della privacy per assicurare la conformità. Grazie a una soluzione ITM con queste funzionalità richieste potrai assicurare la protezione della tua azienda dai rischi interni, sostenendo in modo efficace il tuo team della sicurezza.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.