Come Varonis aiuta un team della sicurezza composto da una sola persona a risparmiare oltre 400 ore all'anno

CASO DI STUDIO

"Quando si tratta di investigazioni sui dati e analisi intensive, un piccolo team non ha il tempo sufficiente per occuparsene. Varonis offre un aiuto inestimabile: serve a estendere le capacità di una persona."

INFORMAZIONI SU QUESTO CASO DI STUDIO:

Il nostro cliente è un ospedale americano. Siamo lieti di soddisfare la loro richiesta di rendere anonimi tutti i nomi e i luoghi.

HIGHLIGHT

SFIDE

- Riduzione della minaccia del ransomware che potrebbe determinare problemi di sicurezza per i pazienti
- Protezione delle informazioni PHI e HIPAA dalle minacce interne ed esterne
- Remediation delle aree a rischio con un team di sicurezza composto da una sola persona

LA SOLUZIONE

La piattaforma di sicurezza dei dati più solida:

- **DatAdvantage** per scoprire i punti in cui gli utenti dispongono di accessi eccessivi e applicare in modo sicuro il privilegio minimo
- **DatAlert Suite** per il monitoraggio continuo e l'invio di alert relativi a dati e sistemi

RISULTATI

- Oltre 400 ore risparmiate annualmente
- Visibilità nei server on-prem che consentono a un team composto da una sola persona di rimanere in vantaggio sul ransomware
- Tranquillità dal 2009, grazie a una soluzione di sicurezza che cresce con le esigenze dell'ospedale

Sfide

Proteggere sistemi critici potrebbe salvare vite umane

Per gli ospedali e le organizzazioni sanitarie, fermare gli attacchi ransomware è letteralmente una questione di vita e di morte.

Nel settembre 2020, i soccorritori sono stati costretti a portare un paziente con lesioni potenzialmente letali in un altro ospedale, a 30 km di distanza, dopo che l'ospedale più vicino era stato compromesso da un attacco. Il paziente è deceduto e si ritiene che il ritardo di un'ora abbia contribuito all'esito fatale.

Comprendendo il rischio, un fornitore di servizi sanitari statunitensi (che rimane anonimo su richiesta) ha collaborato con Varonis nel 2009.

> "Uno dei nostri principali timori è il ransomware", spiega il Security Manager. "Il ransomware potrebbe segnare la nostra fine come azienda...o peggio. Siamo un ospedale e un attacco potrebbe trasformarsi in un problema di sicurezza del paziente. Se il ransomware interrompe la nostra attività per una settimana o due, è un grosso problema per i nostri pazienti.
>
> "Ma non si tratta solo del ransomware. Se non rimaniamo al passo con le insider threat e la data exfiltration, PII e PHI possono essere trattenute per chiedere un riscatto, unendosi alla minaccia dei file crittografati dannosi."

I team di sicurezza degli ospedali sono notoriamente composti da pochi collaboratori. In questo caso, un team composto da una sola persona è responsabile di proteggere i dati dagli attacchi ransomware e di garantire la conformità con HIPAA e PHI.

> "Molti dei nostri file contengono PHI e rientrano nella protezione delle norme di sicurezza HIPAA. Dobbiamo fare in modo che vi accedano solo le persone che ne hanno bisogno. Senza una soluzione come Varonis, non potremmo in nessun modo sapere chi accede e chi dovrebbe avere accesso ai file."

Anche per un team di grandi dimensioni, sarebbe un lavoro notevole. Per una persona, è un'impresa impossibile, motivo per cui hanno adottato Varonis.

> "Senza Varonis, non avrei tempo sufficiente nel corso della giornata per proteggere la nostra rete. Una sola persona non può svolgere tutto quel lavoro."

"Il ransomware potrebbe segnare la nostra fine come azienda...o peggio. Siamo un ospedale e un attacco potrebbe trasformarsi in un problema di sicurezza per i pazienti."

La soluzione

Visibilità e alert su tutti i file e sistemi critici

DatAdvantage per Windows aiuta il team della sicurezza composto da una sola persona a valutare, definire le priorità e ridurre i principali rischi per la sicurezza sui server on-prem dell'ospedale. Se un file è sovraesposto (ovvero aperto a tutti) o un utente inizia ad accedere, spostare o eliminare dati che normalmente non utilizza, Varonis avvisa il Security Manager in tempo reale.

In seguito, l'ospedale ha aggiunto ai propri strumenti di sicurezza **DatAdvantage per i servizi di directory**, che supporta Active Directory. Ora dispone di una visualizzazione panoramica dell'accesso ai dati nei sistemi più critici, e DatAdvantage fornisce aiuto rilevando e risolvendo in modo sicuro i problemi relativi ad autorizzazioni, gruppi nidificati ed ereditarietà.

> "Abbiamo iniziato con DatAdvantage e abbiamo aggiunto il supporto per servizi di directory, che controlla Active Directory per individuare eventuali modifiche. Ne avevamo sicuramente bisogno, perché fino a quel momento non sapevamo esattamente chi, cosa, dove o come si verificavano le modifiche".

L'ospedale ha inoltre aggiunto **DatAlert Suite** al proprio stack di sicurezza. Rilevando potenziali minacce nella kill chain prima che possano evolversi, DatAlert è fondamentale nella lotta contro il ransomware.

> "DatAlert rimane sempre al corrente di tutto ciò che accade nei nostri file server e in Active Directory. Se rilevasse un ransomware o se dovesse verificarsi una violazione effettiva, lo sapremmo immediatamente."

Ma anche con tutte queste soluzioni, un team di sicurezza con una sola persona avrebbe difficoltà a fermare un attacco concentrato da solo. Questo è il momento di chiamare i rinforzi: **il team di risposta agli incidenti di Varonis**.

"Il prodotto di un fornitore era stato compromesso. Il team di risposta agli incidenti ci ha aiutato a confermare che l'hacker non era arrivato oltre tale dispositivo. Senza Varonis, sarebbe stato molto più difficile e dispendioso in termini di tempo e lavoro."

"DatAlert rimane sempre al corrente di tutto ciò che accade nei nostri file server e in Active Directory. Se rilevasse un ransomware o se dovesse verificarsi una violazione effettiva, lo sapremmo immediatamente."

Risultati

Oltre 400 ore risparmiate annualmente

Secondo il Security Manager, il valore pratico di Varonis per un team composto da una sola persona è il risparmio di tempo: **almeno una giornata lavorativa completa ogni settimana o più di 400 ore all'anno.**

> "Quando si tratta di investigazioni sui dati e analisi intensive, un piccolo team non ha il tempo sufficiente per occuparsene. Varonis offre un aiuto inestimabile: serve a estendere le capacità di una persona."
>
> "Il risparmio di tempo mi permette di concentrarmi su altri problemi e di esaminare gli alert sui quali altrimenti non avrei il tempo di indagare."

Ma anche se il risparmio di tempo è notevole, la tranquillità è ancora meglio. Sapere che ora siamo in grado di bloccare i dati e che è sufficiente una rapida chiamata al team di risposta agli incidenti rappresenta un'iniezione di fiducia per il Security Manager e i dirigenti senior.

> "Nell'attuale ambiente della sicurezza, la tranquillità è difficile da raggiungere. Quasi ogni giorno si legge di un ospedale violato o infettato da ransomware. Avere gli strumenti per impedire l'escalation di una situazione negativa mi aiuta a dormire sonni tranquilli."

Mentre l'ospedale valuta i passi successivi, si impegna a prendere ulteriori precauzioni per proteggere i dati e le vite dei pazienti. A tale scopo, il Security Manager spera di aggiungere ulteriori soluzioni Varonis alla propria linea di sicurezza nel prossimo futuro.

"Varonis ha già trovato punti critici come account obsoleti, autorizzazioni errate e altre aree a rischio. Stiamo pensando di acquistare l'Automation Engine, seguito dal Data Classification Engine."

"Il risparmio di tempo mi permette di concentrarmi su altri problemi e di esaminare gli alert sui quali altrimenti non avrei il tempo di indagare."

Varonis aiuta i piccoli team a stare al passo.

Ottieni visibilità, sicurezza dei dati e la tranquillità che deriva dall'avere un team esperto a disposizione.

RICHIEDI UNA DEMO