Cos’è Managed Data Detection and Response (MDDR)?

Il mondo funziona grazie ai dati.

Indipendentemente dal settore (sanità, finanza, PA, istruzione, ecc.) tutte le organizzazioni lavorano con i dati.

Anche tutti gli attacchi informatici funzionano con i dati. Che la fonte sia esterna o interna, sofisticata o meno, le minacce hanno bisogno di dati per rubare un’identità o un segreto aziendale, compromettere una rete o condurre un attacco denial-of-service.

Tuttavia, nonostante i dati siano al centro delle operazioni aziendali e delle violazioni, le aziende continuano a pagare milioni per prodotti e servizi di rilevamento delle minacce che faticano a rispondere a domande importanti quando si verifica un incidente. Domande come… “Sono stati rubati dati?”

Varonis protegge prima di tutto i dati e l’offerta Managed Data Detection and Response (MDDR) è un servizio gestito per il monitoraggio e la protezione dei dati critici 24 ore su 24, 7 giorni su 7, 365 giorni all’anno.

Cos’è Varonis MDDR e come funziona?

Sin dalla fondazione di Varonis nel 2005, il rilevamento delle minacce è stato un componente fondamentale della sua Data Security Platform.

Varonis MDDR combina la tecnologia di rilevamento delle minacce leader del settore con il team di threat hunters di livello mondiale, con gli analisti forensi e gli addetti alla risposta agli incidenti che valutano, indagano e rispondono agli avvisi, così non deve farlo il cliente.

Questo servizio incorpora anche l'analisi comportamentale, l'apprendimento automatico, l'automazione basata su IA, decenni di esperienza nella security e un'esclusiva telemetria dei metadati per proteggere i clienti Varonis dalle minacce e dai percorsi di attacco che i servizi XDR ed EDR non possono rilevare.

MDDR è data-centric

I tradizionali servizi di rilevamento e risposta tendono ad essere incentrati sugli attori delle minacce. Rispondono a domande del tipo: "Chi era l'autore della minaccia? Quale CVE ha sfruttato? Quali strumenti sono stati utilizzati?"

Si tratta di domande importanti a cui rispondere, ma quando si tratta di comprendere l'impatto sui dati, si presentano in breve tempo e aumentano di settimane il tempo medio per rilevare una violazione.

A differenza dei tradizionali servizi XDR ed EDR, Varonis MDDR si concentra sui dati dell'azienda, quindi non ottiene solo informazioni incentrate sull'attore di un attacco.

Varonis può fornire informazioni su quali file sono stati interessati, se sono state prese di mira informazioni personali o proprietà intellettuale e altro ancora, per arrivare alla risposta principale: se i dati sono stati rubati e se la violazione deve essere segnalata.

Senza questo focus sui dati, le organizzazioni con stack di sicurezza avanzati possono comunque cadere vittime di violazioni da parte di minacce interne e attaccanti che aggirano i controlli degli endpoint e della rete.

Varonis MDDR risponde a domande a cui altre soluzioni di rilevamento e risposta non possono rispondere, ad esempio se i dati sono stati esfiltrati e se l'incidente costituisce una violazione materiale.

Investigazioni AI-driven

Quando viene rilevata un'attività anomala, Varonis esegue un'indagine iniziale per aggiungere un contesto critico sull'utente (i suoi colleghi, i dati con cui lavora, le tendenze degli avvisi, i dispositivi coinvolti e gli orari di lavoro generali) e attiva le risposte automatiche necessarie. Gli avvisi critici vengono inoltrati al team di esperti Varonis per ulteriori indagini e mitigazioni.

Nell'interfaccia Varonis, i clienti vedono su quali avvisi stanno lavorando gli analisti, leggono le loro note e rimangono aggiornati. I casi verranno inoltrati solo quando necessario.

Un avviso di ransomware, ad esempio, attiverà l'intelligenza artificiale di Varonis per indagare. Se i risultati indicano un vero positivo, l'analista MDDR viene coinvolto rapidamente per esplorare l'avviso e arrivare a una soluzione il prima possibile.

Le indagini Varonis basate sull'intelligenza artificiale rendono possibile mantenere lo SLA leader del settore, consentendo di rispondere agli avvisi di ransomware entro 30 minuti e ad altri avvisi entro 120 minuti. Il servizio include anche la ricerca proattiva delle minacce e valutazioni mensili della sicurezza per garantire che il livello di sicurezza dei dati aziendali sia in costante miglioramento.

Gli esperti Varonis rispondono rapidamente ed esaminano l'avviso per arrivare alla risoluzione il più rapidamente possibile.

Threat hunting proattivo

Il team di **Varonis Threat Labs (VTL)** ricerca in modo proattivo tendenze, minacce informatiche emergenti, autori di minacce e altro ancora, che prendono di mira determinati settori

verticali.

Questi risultati vengono inclusi nelle valutazioni mensili sullo stato di sicurezza per i clienti MDDR, con gli ultimi aggiornamenti in tempo reale di intelligence sulle minacce per ridurre continuamente la superficie di attacco.

Leggi l’ultima ricerca di VTL.

Varonis MDDR in azione

Nel 2018, Varonis ha costituito la sua organizzazione di risposta agli incidenti (IR) che ha ispirato l’offerta MDDR. Fin dalla sua nascita, Varonis IR ha indagato su oltre 10.000 incidenti.

Recentemente, presso un istituto sanitario, Varonis ha identificato tentativi di intrusione da parte del gruppo ransomware BlackCat, noto anche come ALPHV, e ha impedito la possibilità di un evento di crittografia malevolo. Dopo aver avvisato rapidamente il cliente, Varonis ha identificato il dispositivo vulnerabile e assistito con la mitigazione.

Varonis MDDR aiuta inoltre i clienti a combattere le minacce interne. In un caso, per esempio, la funzionalità EDR ha avvisato un cliente di un’attività insolita e il cliente ha contattato il team Varonis per indagare e identificare un file sospetto sulla rete.

Gli esperti Varonis hanno identificato rapidamente l’autore del file – un amministratore IT scontento – e hanno esaminato la sua attività sulla rete. È stato scoperto che non solo aveva creato il file sospetto, ma aveva anche creato oggetti non autorizzati per sfruttare probabilmente la persistenza nella rete, oltre ad accedere ai file delle risorse umane relativi a un partner che stava affrontando un’azione disciplinare verso l’organizzazione.

Ciò che era iniziato come un incidente EDR si è evoluto in

un’indagine sulle minacce interne molto più ampia e, senza l’attenzione del team IR di Varonis sui dati e sulla reale portata della minaccia, avrebbe portato a un risultato molto diverso.

Non attendere che si verifichi una violazione

Senza un monitoraggio continuo dei dati, le organizzazioni aumentano il rischio di esposizione quando si verifica una violazione. Varonis MDDR è la soluzione che fornisce il monitoraggio dei dati 24x7x365. Per saperne di più: https://www.varonis.com/it/

A cura *di* **Mike Thompson***, Security Architect Manager, Varonis*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cose-managed-data-detection-and-response-mddr/