bearIT

Potenzia le tue operazioni di sicurezza con XDR

Migliora l'efficienza del tuo team SOC (Security Operations Center) con un'intelligence sulle minacce senza pari e l'interruzione automatica di attacchi sofisticati come il ransomware

Inizia

Microsoft

Lo stato attuale delle operazioni di sicurezza

Frequenza, velocità e sofisticazione delle minacce in continua crescita

Il panorama della sicurezza informatica odierno vede un costante aumento degli attacchi in tutte le categorie: più phishing, più campagne ransomware, più minacce alle identità con una crescita anche nella velocità. Con la crescita della gig economy RaaS (Ransomware as a Service), chiunque può ora impossessarsi degli strumenti sviluppati dagli autori di attacchi degli stati-nazione più prolifici del mondo informatico, aumentandone le percentuali di successo e la capacità di scalare.

Le soluzioni isolate rallentano la risposta

La protezione degli endpoint e la presenza di una strategia di sicurezza e-mail completamente separata non sono più sufficienti. Gli attacchi prendono di mira le lacune tra tali soluzioni, a sé stanti e isolate, e il passaggio tra più domini, lasciando ai difensori la necessità di correlare manualmente i singoli avvisi per rilevare un attacco più ampio. Gli attacchi sofisticati si spostano su e-mail ed endpoint, fino alle identità degli utenti, alle applicazioni cloud e ai tuoi dati. Una strategia di soluzione a sé stante impone agli analisti della sicurezza di correlare manualmente gli avvisi per identificare gli attacchi perché non il quadro generale non è mai visibile. Ciò rallenta non solo il rilevamento, ma anche l'indagine e la correzione.

Secondo uno studio di Gartner, i responsabili delle decisioni in materia di sicurezza sono sempre più insoddisfatti delle inefficienze operative e della mancanza di integrazione derivanti dall'utilizzo di una vasta gamma di strumenti di sicurezza tradizionali e si dedicano quindi alla ricerca di soluzioni più efficaci e integrate.[1]

[1]Gartner: Top 5 Trends in Security Vendor Consolidation, 2022 (in inglese)

XDR: la risposta agli attacchi moderni

Per affrontare la natura degli attacchi moderni che si spostano tra più domini, i team di sicurezza hanno bisogno di una soluzione unificata che consenta loro di rilevare le minacce e di rispondervi in modo più efficiente in tutte le risorse digitali dell'organizzazione. Grazie a una potente intelligence che automatizza la correlazione e l'analisi dei dati, nonché le azioni di risposta, XDR può aiutare il Security Operations Center (SOC) a passare da un approccio reattivo a una strategia di difesa proattiva, migliorando al contempo il rilevamento delle minacce e i tempi di risposta e, soprattutto, consentendo agli analisti SOC di avere più tempo per concentrarsi sulla ricerca proattiva e sulla prevenzione.

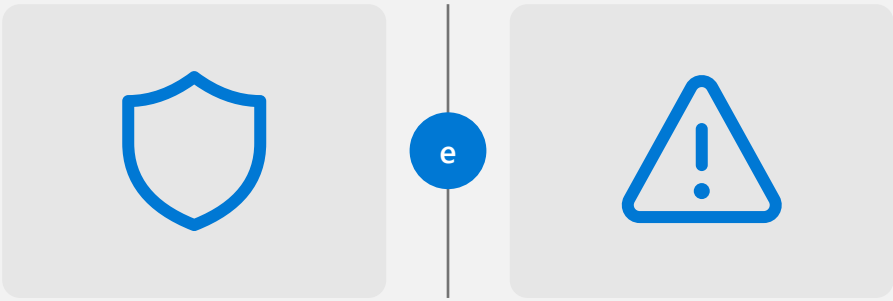
Funzionalità di rilevamento e reazione estese (XDR)

Le soluzioni sono progettate per offrire un approccio olistico, semplificato ed efficiente al fine di proteggere le organizzazioni dagli attacchi avanzati. Consentono ai team SOC di avere una visione più completa della catena di attacco per un'indagine più efficace e forniscono la correzione automatica in più domini grazie a vasti set di intelligence e intelligenza artificiale integrata.

Le soluzioni di rilevamento e reazione dagli endpoint (EDR) non sono sufficienti

XDR

- Sicurezza olistica e correlazione dei segnali tra identità, e-mail, endpoint, app cloud, sicurezza della prevenzione della perdita dei dati (DLP) e altro ancora
- Esperienza di indagine e risposta basata sugli incidenti
- Protezione da attacchi avanzati come ransomware e BEC (Business Email Compromise)



EDR

- Solo sicurezza degli endpoint
- Avvisi sugli endpoint isolati
- Può solo aiutare a respingere gli attacchi specifici agli endpoint e non offre una visione d'insieme per affrontare gli attacchi avanzati

Quando prendi in considerazione una soluzione XDR per l'organizzazione, i nostri esperti di sicurezza possono fornirti una valutazione del tuo ambiente attuale e consigliarti un nuovo modo per favorire l'efficienza dei processi e dei costi in tutte le tue operazioni. Ci concentriamo sul set critico di funzionalità seguente.

01. Visibilità della catena di attacco e protezione avanzate

Per salvaguardare un'azienda dagli attacchi avanzati, le soluzioni XDR devono coprire diversi tipi di risorse e unificare la sicurezza per i punti di ingresso critici delle minacce, come e-mail e identità, ma anche proteggere i punti più in basso nella catena di attacco, ad esempio endpoint, app cloud e dati DLP. Consolidando queste origini dati, le soluzioni XDR correlano gli avvisi di basso livello in un singolo incidente e aiutano a scoprire l'intera catena di un attacco sofisticato altrimenti trascurato dalle soluzioni di sicurezza a sé stanti.

02. Procedure di indagine e risposta unificate

Le soluzioni XDR efficaci sono progettate per consentire agli analisti della sicurezza di operare con maggiore incisività. L'indagine basata sugli incidenti che mostra la visione end-to-end dell'attacco, gli approfondimenti nel contesto e le guide alla risposta con le procedure consigliate sono tutti elementi fondamentali per semplificare ai team SOC l'indagine e la risposta più efficienti.

03. Automazione

La crescita del volume e della velocità degli attacchi avanzati mette alla prova la capacità della maggior parte dei team di sicurezza. Le soluzioni XDR consentono l'automazione in due modi. Da una parte, utilizzano l'ampiezza del segnale sottostante e l'intelligenza artificiale per fornire automazione integrata al fine di rispondere agli attacchi avanzati, dall'altra offrono anche opzioni alle aziende per creare automazioni personalizzate.

04. Intelligence ad ampio raggio e visibilità sui vettori delle minacce

Una soluzione XDR deve incorporare funzioni di intelligence e trarre informazioni da un'ampia gamma di origini per analizzare i segnali e comprendere meglio il panorama delle minacce, nonché da ricerche proprietarie che informano i meccanismi di prevenzione, rilevamento e protezione. Segnali in numero e diversità sempre maggiori migliorano la capacità di rilevare e comprendere più vettori di minacce, consentendo alla soluzione XDR di identificare rapidamente un attacco in una fase precoce e di ridurre la quantità di avvisi e incidenti, permettendo in tal modo al team SOC di rispondere alle minacce più recenti con migliore efficacia.

05. Costo totale di proprietà migliorato

XDR consente alle organizzazioni di consolidare i fornitori, integrando più strumenti di sicurezza isolati in una soluzione unificata. La soluzione elimina la necessità di acquistare da vari fornitori e il lavoro manuale richiesto per correlare i segnali. XDR fornisce invece una soluzione completa per il rilevamento, la risposta e la correzione, riducendo i costi di acquisizione e il sovraccarico dei processi.

Potenzia la tua esperienza SOC con Microsoft Defender XDR, la soluzione Microsoft XDR

In qualità di consulenti per la sicurezza di aziende come la tua, consigliamo Microsoft Defender XDR. Questa soluzione offre un'esperienza unificata di indagine e risposta e fornisce protezione nativa su endpoint, identità ibride, e-mail, strumenti di collaborazione e applicazioni cloud con visibilità centralizzata, analisi potenti e interruzione automatica degli attacchi. Con Microsoft Defender XDR, ottieni un set più ampio di protezioni, tra cui la sicurezza della posta elettronica e la gestione delle identità e degli accessi come soluzioni preventive critiche. Puoi inoltre beneficiare delle funzionalità di riparazione automatica per i problemi comuni ed espandere le potenzialità dei team SOC con interruzioni automatizzate XDR per proteggerti da ransomware e altri attacchi avanzati in modo più efficace, salvaguardando al contempo la continuità aziendale dell'organizzazione.

Microsoft Defender XDR offre ai difensori una serie di funzionalità chiave per stare un passo avanti agli utenti malintenzionati, con i vantaggi seguenti.

Consenti una risposta rapida grazie a incidenti con priorità XDR

1

Microsoft Defender XDR mette in correlazione i segnali nativi tra endpoint multipiattaforma, identità ibride, e-mail e strumenti di collaborazione, nonché app SaaS e informazioni dettagliate DLP per fornire una visione completa della catena di attacco. Questo contesto approfondito consente ai team SOC di indagare e rispondere a livello di incidente, semplificando la definizione delle priorità e accelerando la correzione.

Rimani al passo con gli attacchi avanzati

La capacità di correlare gli avvisi in modo efficiente è fondamentale per le operazioni quotidiane di un analista della sicurezza. Per questo motivo Microsoft Defender XDR offre un'indagine e una risposta unificate progettate al fine di offrire l'esperienza più efficiente per i team SOC per tempi di risposta più rapidi.

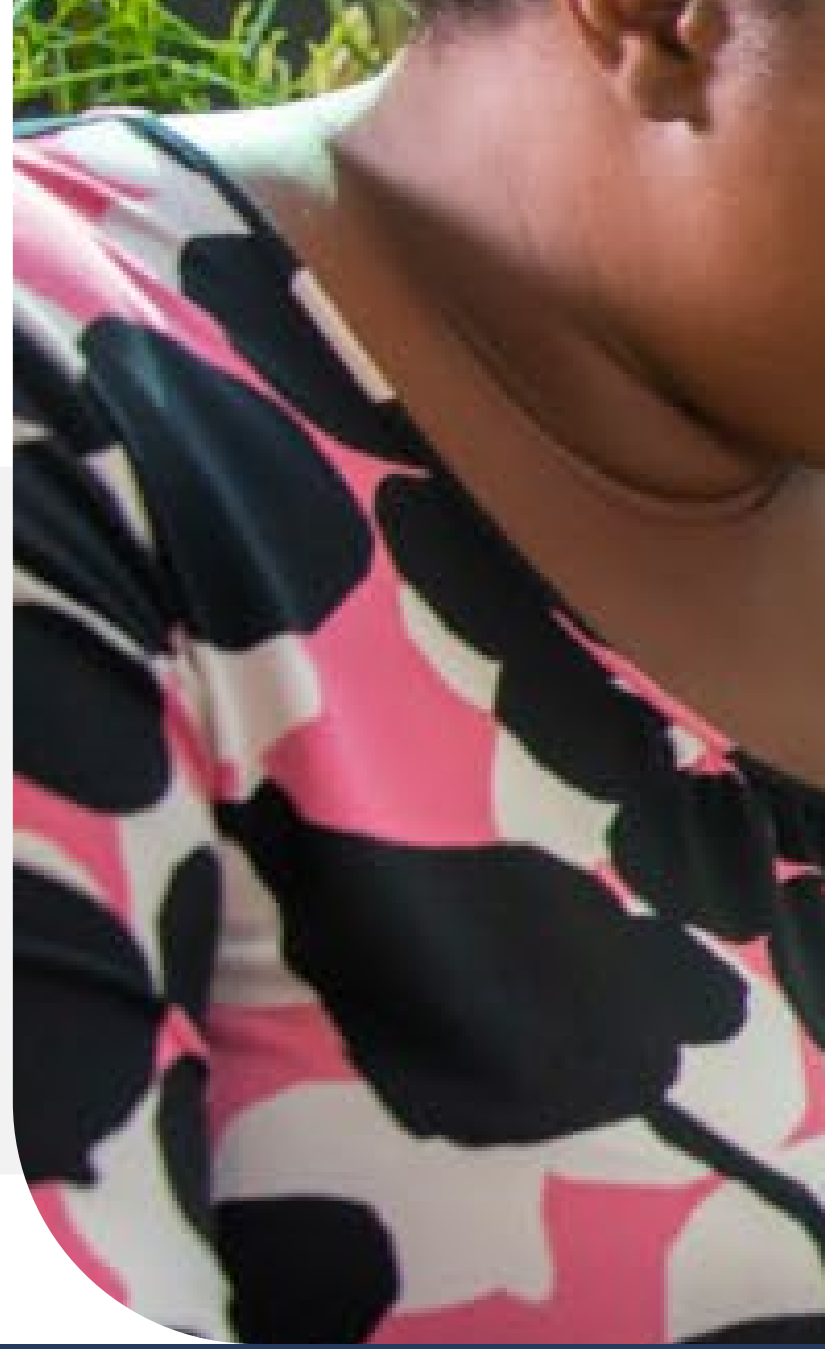
Per un'indagine semplificata, Microsoft Defender XDR fornisce un grafico visivo dell'attacco, che mostra tutte le entità interessate per aiutare il team SOC a capire facilmente il modo in cui l'utente malintenzionato sia passato dalla compromissione all'obiettivo.

Puoi analizzare gli avvisi nel contesto dell'intero incidente e utilizzare le guide integrate nel prodotto per rispondere rapidamente, in un'unica esperienza connessa senza dover cambiare contesto. Puoi anche esaminare in profondità in un unico linguaggio per la ricerca avanzata in tutti i servizi. Per assicurare che le automazioni ti aiutino a rispondere ancora più velocemente, Microsoft Defender XDR supporta inoltre rilevamenti personalizzati in tempo reale.

Abilita un team SOC incentrato sui dati con segnale DLP

La prevenzione della perdita dei dati (DLP) è fondamentale per le organizzazioni perché consente di proteggere le informazioni sensibili e di mitigare il rischio di perdita dei dati. L'integrazione degli avvisi DLP nell'esperienza di indagine sugli incidenti offre agli analisti SOC un modo completamente nuovo di stabilire le priorità, in base alla sensibilità dei dati interessati.

Microsoft Defender XDR offre la possibilità di comprendere rapidamente l'impatto di una violazione dei dati correlando gli avvisi DLP nella vista degli incidenti XDR, la possibilità di condurre ricerche avanzate e quella di intraprendere azioni correttive direttamente nel portale di Microsoft Defender XDR. L'aggiunta della centralità dei dati all'esperienza SOC semplifica la correlazione di un attacco con il rilevamento delle perdite di dati, in modo da comprendere più rapidamente l'impatto end-to-end e da rispondere in modo più efficace.



Interrompi gli attacchi avanzati alla velocità della macchina

2

Microsoft Defender XDR sfrutta l'ampiezza del segnale Microsoft XDR e le funzionalità di rilevamento basate sulla ricerca e sull'intelligenza artificiale per identificare attacchi avanzati come il ransomware e fornisce una risposta automatica a livello di incidente con interruzione automatica degli attacchi. L'interruzione consente di contenere gli attacchi in corso disabilitando o limitando automaticamente i dispositivi e gli account utente utilizzati in un attacco, interrompendone la progressione e riducendone l'impatto.

Espandi le potenzialità del tuo team SOC con il contenimento automatico delle risorse interessate

L'interruzione automatica è progettata per contenere gli attacchi in corso disabilitando o limitando automaticamente i dispositivi e gli account utente compromessi, arrestandone la progressione e riducendo l'impatto sulle organizzazioni. Si tratta di una grande innovazione: oggi la maggior parte dei team di sicurezza non è in grado di rispondere abbastanza velocemente ad attacchi sofisticati come ransomware o campagne BEC e in genere reagisce eseguendo operazioni di pulizia in base all'impatto. Con l'interruzione, gli attacchi sono limitati a un numero ridotto di risorse, diminuendo drasticamente l'impatto e migliorando la continuità aziendale.

Aumenta l'efficienza grazie alla più ampia conoscenza del settore sui vettori di attacco

Con 65.000 miliardi di segnali giornalieri e oltre 8.000 professionisti della sicurezza,[3] le soluzioni di sicurezza Microsoft danno visibilità su più vettori di minaccia rispetto a qualsiasi altro fornitore. Se abbinati alla piattaforma XDR di Microsoft integrata in modo nativo, i team SOC offrono una migliore protezione da minacce sofisticate in tempo reale e possono rispondere più rapidamente.

65.000 miliardi di segnali

sintetizzati quotidianamente, utilizzando sofisticate analisi dei dati e algoritmi di intelligenza artificiale per comprendere le minacce digitali e le attività informatiche criminali e proteggersi di conseguenza.[3]

3. Plan for the future with Microsoft Security | Microsoft Security Blog (in inglese)

Unifica la gestione della sicurezza, delle identità e degli accessi XDR

3

Le identità sono un vettore di minaccia critico perché la maggior parte degli attacchi include identità compromesse per spostarsi lateralmente. Microsoft combina le funzionalità di protezione delle identità della nostra piattaforma leader del settore[4] per la gestione delle identità e degli accessi con la nostra soluzione XDR, offrendo un'unica esperienza integrata per la protezione delle identità e la difesa dalle minacce. Questa potente combinazione offre funzionalità come l'accesso condizionale, incorporate direttamente nella piattaforma di identità Azure AD, fornendo al contempo l'intera gamma di funzionalità di protezione dalle minacce di Microsoft XDR. Ciò offre una soluzione unificata che protegge le identità ibride di utenti e carichi di lavoro e l'infrastruttura di identità sottostante.

Crea efficienze operative e riduci i costi

Microsoft Defender XDR offre un'esperienza unificata per la protezione delle identità in locale e nel cloud e combina questi segnali con tutte le altre origini per la vista XDR completa della catena di attacco, creando efficienze significative per il team SOC. L'acquisto di Microsoft Defender XDR, inoltre, è un approccio conveniente per consolidare i fornitori, offrendo funzionalità leader del settore sia per la gestione delle identità sia XDR in un unico pacchetto.

Le migliori della categoria, unificate in una soluzione XDR leader

Oltre a essere un fornitore di soluzioni per l'identità leader, Microsoft offre altre soluzioni unificate in XDR, le migliori della categoria, e una soluzione di sicurezza degli endpoint è spesso il punto di partenza per una discussione su XDR. Gartner ha nominato Microsoft leader nel Magic Quadrant di Gartner® per le piattaforme di protezione degli endpoint con protezione multipiattaforma tra cui Linux, macOS, iOS e Android del 2022.[4]

[4]Microsoft, "Microsoft is named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms", 2 marzo 2023 (in inglese)

Opinioni delle aziende

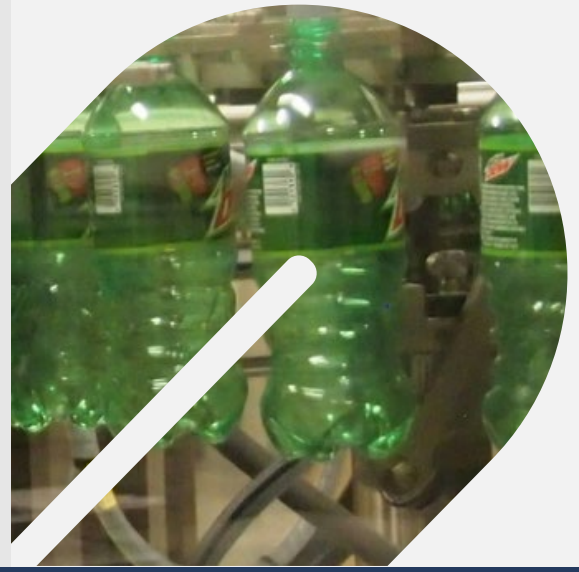
ING sfrutta l'intero ambito di Microsoft 365 Defender per reinventare i servizi bancari per un pubblico digitale. Il team IT è ora in grado di riconoscere meglio i tentativi di phishing e di bloccarli fin dall'inizio, basandosi sulla propria intelligence e utilizzando i dati delle query per identificare ulteriori rischi.

Un singolo livello di rilevamento non è abbastanza efficace ed è soggetto a una certa probabilità di falsi positivi...D'altra parte, Microsoft 365 Defender correla i segnali tra endpoint, e-mail, documenti, identità, app e altro ancora."

Consideriamo un punto di svolta il fatto che Microsoft 365 Defender combini i segnali per la ricerca delle minacce perché collega i dati dal punto di vista delle identità e degli endpoint per individuare eventi realmente dannosi."

– **Krzysztof Kuźnik**
Product Owner in ING

G&J Pepsi-Cola Bottlers ha distribuito Microsoft 365 Defender, ovvero la base di cui G&J Pepsi aveva bisogno per espandere la sicurezza dopo il recupero dall'attacco ransomware. Microsoft 365 Defender è l'unico strumento in grado di rilevare le minacce ransomware come quella che ha colpito G&J Pepsi nel 2021 e di rispondere di conseguenza.



L'adozione di una solida postura focalizzata sulla protezione della sicurezza fisica e dei dispositivi, delle identità e dei dati è fondamentale per la stabilità aziendale ed è stata una componente chiave per una difesa efficace contro gli attacchi informatici."

– **Eric McKinney**
Enterprise Infrastructure Director in G&J Pepsi-Cola Bottlers

Riepilogo

XDR è emerso come un approccio rivoluzionario per combattere le minacce informatiche e consentire a SecOps di ottenere di più con un'esperienza di rilevamento e risposta unificata. Gli attacchi avanzati come il ransomware pongono sfide significative e mettono in evidenza le carenze delle soluzioni di sicurezza isolate. La necessità di una soluzione più completa e integrata non è mai stata così evidente e XDR fornisce esattamente una soluzione di questo tipo.

Microsoft Defender XDR è riconosciuto come una soluzione XDR leader ed è definito dalla protezione unificata tra endpoint, identità ibride, e-mail, strumenti di collaborazione e applicazioni cloud integrata nel prodotto. Oltre all'indagine e alla risposta basate sugli incidenti, offre visibilità centralizzata, analisi potente e interruzioni automatiche degli attacchi al fine di promuovere l'efficienza SOC e garantire che le organizzazioni abbiano accesso alle più recenti protezioni basate sull'intelligence e sulla ricerca.

Infine, Microsoft Defender XDR è l'unico strumento che combina una piattaforma leader di gestione delle identità e degli accessi grazie alla sua soluzione XDR, per un'unica esperienza integrata che consente di proteggere le identità e difendersi dalle minacce, creando significativi vantaggi totali in termini di costi di proprietà e di efficienza dei processi, consolidando al contempo i costi con un unico fornitore.

XDR è una soluzione indispensabile per qualsiasi strategia di sicurezza moderna, quindi i team SOC sono avvantaggiati nel tenere il passo con il panorama degli attacchi in evoluzione, aiutati da un approccio alla protezione dalle minacce unificato e basato sull'intelligence.

Ottieni subito la protezione dalle minacce di cui hai bisogno

In qualità di partner Microsoft, possiamo aiutarti a difendere la tua azienda dalle minacce informatiche. Abbiamo una solida esperienza in materia di sicurezza nonché le competenze necessarie per assisterti in ogni fase della strategia di sicurezza. Se hai bisogno di una valutazione del tuo ambiente attuale o di aiuto nell'esaminare i piani di licenza, nella distribuzione o nei servizi gestiti, abbiamo le soluzioni appropriate.

Vuoi iniziare?

Contattaci subito.

www.bearIT.com

info@bearIT.com