Kaspersky Next XDR Expert

Ancora più potente,
veloce e all'avanguardia

kaspersky

XDR rappresenta un punto di svolta o è solo un'altra soluzione a un problema specifico?

A chi è destinato XDR?

XDR è destinato alle organizzazioni con un approccio maturo alla sicurezza, che necessitano di un'unica piattaforma da cui ottenere un quadro completo e coerente di quello che accade all'interno della loro infrastruttura.

XDR: Extended Detection and Response

Molti ne parlano ma, come per tutte le tecnologie relativamente recenti, non tutti sanno di cosa si tratta esattamente e quali vantaggi può comportare per un'azienda. Una cosa è certa: XDR implica un passaggio strategico da un approccio reattivo a quello proattivo. Perché quando si tratta di cybersecurity non si può semplicemente "stare a vedere". I meglio informati considerano XDR come una strategia, anziché come un semplice prodotto.

Quindi XDR è solo l'ennesimo tentativo di risolvere uno specifico problema tecnologico o rappresenta un potenziale punto di svolta? I problemi da risolvere certamente non mancano: dalla carenza di competenze a livello globale al sovraccarico del personale addetto alla sicurezza IT, da un panorama delle minacce in continua evoluzione al proliferare dei più disparati avvisi e strumenti, dalla scarsa intelligence sulle minacce alla crescente superficie di attacco. Secondo IDC, XDR sarà "una forza dirompente, che avrà un impatto sulla vendita delle soluzioni SIEM, EDR e SOAR e delle piattaforme di network intelligence e analisi delle minacce, oltre che sui fornitori di intelligence sulle minacce"[1]. Inoltre, Forrester ritiene che la tecnologia XDR differenziata "a breve termine sostituirà i sistemi EDR e a lungo termine usurperà il posto occupato dalle soluzioni SIEM"[2].

XDR sarà una forza dirompente - IDC

Più dispositivi, più applicazioni, più traffico di rete, più dati, più minacce...

A chi è destinato XDR e quali sfide può risolvere?

XDR è destinato alle organizzazioni con un approccio maturo alla sicurezza, che necessitano di un'unica piattaforma da cui ottenere un quadro completo e coerente di quello che accade all'interno della loro infrastruttura.

Le sfide legate alla cybersecurity che queste organizzazioni si trovano ad affrontare sono coerenti e consolidate. ESG Research ha condotto uno studio che ha coinvolto i professionisti IT e della cybersecurity[3] di alcune organizzazioni con 100 o più dipendenti, l'80% delle quali a livello enterprise, in diversi segmenti verticali. Ecco alcuni dei risultati principali:

Difficoltà a tenere il passo con i requisiti operativi delle tecnologie SOC

La gestione delle attività di sicurezza, o SecOps, è oggi più difficile di quanto non sia mai stata negli ultimi due anni, a causa delle difficoltà nel tenere il passo con le esigenze operative delle tecnologie SOC: scalabilità nella pipeline dei dati, bilanciamento del carico dei motori di elaborazione, maggiore capacità di archiviazione e così via.

[1] Fonte: IDC, Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now?, 2022

[2] Fonte: Forrester, Extended Detection and Response (XDR) - A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

[3] Fonte: ESG Research Report, SOC Modernization and the Role of XDR, 2022

Crescita e continua evoluzione della superficie di attacco e del panorama delle minacce in generale

Più dispositivi, più applicazioni, più traffico di rete, più dati, più minacce. Il panorama delle minacce non si ferma mai: con il proliferare di nuovi strumenti, anche le minacce informatiche si evolvono incessantemente in termini sia di quantità che di complessità. Allo stesso tempo, le barriere all'ingresso per i cybercriminali non sono mai state tanto basse. Da un lato ci si potrebbe trovare ad affrontare persone scarsamente competenti che acquistano a basso costo nel Dark Web attacchi già pronti da eseguire. E dall'altro hacker pazienti ed altamente qualificati che sviluppano attacchi complessi. E non vanno sottovalutate neanche le minacce interne e le vulnerabilità della supply chain.

Numero elevato di processi manuali necessari per la gestione della sicurezza

Le tecniche di elaborazione manuale risultano poco efficienti ed efficaci di fronte al volume crescente dei dati sulla sicurezza da raccogliere ed elaborare. Si crea così una tempesta perfetta che compromette la scalabilità, si traduce in un'eccessiva dipendenza dall'intervento umano e riduce l'efficacia della gestione delle minacce in generale.

Incapacità di sviluppare regole di rilevamento adeguate

La mancanza di tempo, risorse e competenze è all'origine dell'incapacità di sviluppare regole di rilevamento, mettere a punto i controlli di sicurezza e identificare e gestire le minacce in modo rapido ed efficiente: le organizzazioni, infatti, non sempre dispongono delle competenze o del personale necessario per stare al passo con le esigenze in termini di analisi e operazioni di sicurezza. Si passa così direttamente al problema successivo...

Carenza di personale competente a livello globale

Nonostante il massimo storico di 4,7 milioni di professionisti attualmente registrato dalla forza lavoro globale dedicata alla cybersecurity, c'è ancora un gap di 3,4 milioni di posti che deve essere colmato. E il divario si allarga a una velocità doppia rispetto a quella con cui cresce la forza lavoro, con un aumento su base annua pari al 26,2%.[4]

[4] Fonte: (ISC)², Cybersecurity Workforce Study, 2022

Per quanto poco efficaci, gli strumenti

impiegati dalle organizzazioni per il rilevamento delle minacce e le successive indagini in genere richiedono la presenza di figure competenti specializzate in grado di gestirli.

Strumenti non adeguati allo scopo

Se gli strumenti stessi sono parte del problema, qualcosa deve necessariamente cambiare. Per quanto poco efficaci, gli strumenti impiegati dalle organizzazioni per il rilevamento delle minacce e le successive indagini in genere richiedono la presenza di figure competenti specializzate in grado di gestirli. Dallo studio[5] è emerso che gli strumenti in uso risultano inefficaci nel mettere gli avvisi in correlazione e che il personale addetto alla sicurezza IT deve destreggiarsi tra molteplici strumenti diversi e disconnessi che gestiscono dati disparati. In sostanza, a fronte dei costi elevati regnano inefficienza, scarsa praticità e confusione. A questo si aggiunge un altro problema: gli strumenti attuali non offrono una scalabilità sufficiente per gestire l'espansione della superficie di attacco, né le necessarie capacità di rilevamento e risposta nel cloud.[6]

Non sorprende che i CISO sembrino sempre sotto stress...

La buona notizia è che il miglioramento delle operazioni di sicurezza è una priorità ed è finanziato: l'88% delle organizzazioni prevede un aumento della spesa per quest'anno, il 66% afferma che il consolidamento degli strumenti è una priorità e che lo sviluppo e l'implementazione di applicazioni moderne hanno registrato una maggiore velocità, richiedendo nuove competenze.[7]

88%

delle organizzazioni quest'anno prevede un aumento della spesa per il miglioramento delle SecOps

66%

afferma che il consolidamento degli strumenti è una priorità

Vantaggi di XDR

Ecco il modo in cui XDR consente di far fronte a queste sfide.

Migliore capacità di rilevamento delle minacce avanzate

Le funzionalità di rilevamento delle minacce offerte da XDR abbracciano endpoint, reti e ambienti cloud. L'utilizzo di algoritmi di machine learning e analisi del comportamento consente di identificare anche le minacce più sofisticate, come malware, ransomware e APT (Advanced Persistent Threat).

Automazione delle attività di risposta e correzione

XDR automatizza le azioni di risposta e correzione, consentendo alle organizzazioni di contenere rapidamente le minacce e ridurre al minimo i potenziali danni. È in grado di mettere in quarantena o isolare gli endpoint compromessi, bloccare le attività dannose e correggere le vulnerabilità, riducendo le operazioni manuali e i tempi di risposta.

[5] Fonte: ESG Research Report, SOC Modernization and the Role of XDR, maggio 2022

[6] Fonte: ESG Research Report, SOC Modernization and the Role of XDR, 2022

[7] Fonte: ESG Research Report, SOC Modernization and the Role of XDR, maggio 2022

Qual è il ruolo dei sistemi XDR nell'ecosistema delle soluzioni EDR, MDR, SOAR e SIEM?

La risposta si trova nella "X", che sta per "Extended". XDR (Extended Detection and Response) estende le funzionalità offerte da EDR (Endpoint Detection and Response) per rilevare proattivamente le minacce complesse a più livelli dell'infrastruttura, in modo da reagire e contrastare queste minacce automaticamente.

Importanza di un approccio integrato

Con l'integrazione di più strumenti e applicazioni di sicurezza e il monitoraggio dei dati su endpoint, reti, cloud, server Web, server di posta ecc... XDR va oltre il rilevamento e l'eliminazione delle minacce perché semplifica al tempo stesso la gestione della sicurezza delle informazioni grazie all'automatizzazione dell'interazione tra i prodotti.

Forrester ritiene che nella maggior parte dei casi XDR non sostituirà completamente le piattaforme di analisi della sicurezza, sottolineando che "XDR è in evoluzione e [noi] prevediamo che nei prossimi cinque anni le piattaforme di analisi della sicurezza e XDR entreranno in collisione".

Anche le soluzioni SIEM offrono casi d'uso che vanno oltre il rilevamento delle minacce e. Gli strumenti come i SOAR assicurano vantaggi indiscutibili. Tuttavia, quando sono in gioco il rilevamento e la risposta alle minacce, le avanzate capacità di analisi offerte dalla protezione ottimizzata di XDR non temono confronti.

Integrazione con gli strumenti di protezione degli endpoint

L'integrazione con gli strumenti EPP (Endpoint Protection) rappresenta una questione chiave: grazie ai dati sugli endpoint ricavati tramite telemetria e analisi del comportamento, XDR fornisce informazioni approfondite sulle attività degli endpoint. L'utilizzo di algoritmi avanzati di machine learning per identificare comportamenti sospetti e indicatori di attacco (IOA, Indicator of Attack) agevola il rilevamento precoce delle minacce sofisticate.

Assicura visibilità in tempo reale

XDR offre visibilità in tempo reale sullo stato della sicurezza dell'organizzazione. Raccogliendo e analizzando i dati provenienti da varie origini (come endpoint, server, firewall e piattaforme cloud), fornisce in un'unica console informazioni complete e approfondite sulle minacce in corso e sulle attività sospette. Rappresenta pertanto la soluzione ideale per chi intende adottare un approccio realmente proattivo, perché consente di rilevare automaticamente le minacce e di reagire più rapidamente agli incidenti, offrendo inoltre una visione olistica che aiuta i team di sicurezza a individuare attività sospette e potenziali incidenti di sicurezza con maggiore precisione.

Contestualizza i dati e l'intelligence sulle minacce

Basato su un potente database e sulle più avanzate tecnologie di intelligence sulle minacce, XDR fornisce informazioni contestuali estremamente utili tanto sulle minacce quanto sugli autori degli attacchi. Questo tipologia di threat intelligence semplifica la gestione degli avvisi relativi alle indagini e degli incidenti, consente ai team di sicurezza di comprendere meglio tattiche, tecniche e motivazioni dei responsabili delle minacce e agevola una più efficace risposta agli incidenti e l'implementazione di misure di difesa proattive.

Razionalizza le operazioni di sicurezza

Se opportunamente integrate, le migliori soluzioni si inseriranno senza problemi nell'infrastruttura già esistente consentendo di sfruttare appieno il potenziale dell'automazione e assicurando la massima visibilità e awareness senza richiedere la sostituzione delle soluzioni di sicurezza di terze parti in uso. È inoltre importante sottolineare che, fornendo una visione d'insieme degli incidenti di sicurezza e del comportamento degli utenti, l'integrazione favorisce anche il rispetto dei requisiti di conformità.

XDR soddisfa decisamente le aspettative, offrendo tutto quello che promette: controllo, stabilità e un fondamentale vantaggio competitivo. Ma non tutte le offerte XDR sono uguali... Come scegliere la più adatta per le proprie esigenze?

Cinque aspetti fondamentali da considerare quando si confrontano fornitori e soluzioni XDR

Ecco il modo in cui XDR consente di far fronte a queste sfide.

1

Esiste un collegamento diretto tra la qualità di una soluzione XDR e la capacità del fornitore di creare una sinergia tra i sistemi EPP ed EDR

Una soluzione EDR per il rilevamento avanzato e la risposta alle minacce informatiche sofisticate a livello degli endpoint è un elemento chiave per un efficace approccio XDR. Allo stesso tempo, la soluzione EDR necessita di una solida piattaforma di protezione degli endpoint (EPP) per individuare automaticamente le minacce. È importante esaminare attentamente le funzionalità EPP e verificare che sia disponibile il supporto per tutti i tipi di endpoint: PC, laptop, macchine virtuali, dispositivi mobili e i vari sistemi operativi.

2

Poter contare su informazioni aggiornate sulle minacce e su una visione completa delle tecniche e tattiche adottate dai cybercriminali è essenziale per contrastare le minacce informatiche

Non è fantascienza: qualsiasi soluzione XDR degna di questo nome offrirà entrambe queste funzionalità, con l'aggiunta di un contesto per migliorare e accelerare le attività di indagine e risposta agli incidenti.

3

L'integrazione con soluzioni di terze parti è più sostenibile ed economicamente vantaggiosa

La qualità dell'integrazione di una soluzione XDR con altre di terze parti è un'altra questione assolutamente critica, perché l'interoperabilità rende l'acquisto un investimento più sostenibile fin dall'inizio. Una soluzione XDR che offre numerose e autentiche opzioni di integrazione attingerà a più origini dati e fornirà un quadro più completo di ciò che accade all'interno dell'infrastruttura.

4

Le revisioni indipendenti, il riconoscimento globale e i risultati dei test indipendenti contano

Quando investite in qualcosa di così importante per la vostra azienda come la cybersecurity, non trascurate le valutazioni indipendenti. Richiedete i risultati dei test indipendenti. Verificate i riconoscimenti internazionali da parte di organizzazioni autorevoli come Forrester, IDC e altre. Le soluzioni vengono implementate a livello globale? Richiedete i case study.

5

Si tratta di un investimento a prova di futuro?

La tecnologia non si ferma mai. Pertanto, soprattutto nel caso delle tecnologie relativamente recenti come XDR, è importante scoprire cosa prevede la roadmap di un fornitore per lo sviluppo continuo del prodotto.

Perché Kaspersky

La più testata. La più premiata. Protezione Kaspersky.

Kaspersky è un'affermata azienda globale di cybersecurity con una solida esperienza in materia di sicurezza. Proteggiamo organizzazioni in tutto il mondo da oltre 25 anni e abbiamo ricevuto innumerevoli premi e riconoscimenti per i nostri prodotti e servizi. Tra il 2013 e il 2022, i prodotti Kaspersky:

587

si sono classificati 587 volte al primo posto

685

si sono classificati 685 volte nelle prime tre posizioni

827

hanno partecipato a 827 test e recensioni indipendenti

Nel 2023, Kaspersky è stata nominata Leader nel mercato delle soluzioni XDR dall'autorevole società di consulenza e ricerca tecnologica globale ISG. ISG definisce "leader" coloro che dispongono di un'offerta completa di prodotti e servizi e rappresentano la forza innovativa e la stabilità competitiva.

Per saperne di più

Kaspersky Extended Detection and Response

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture