I megatrend della cybersecurity e le implicazioni per la protezione dalle minacce informatiche

Ripensare EPP,
EDR e XDR

kaspersky

Introduzione

Ogni anno, i principali analisti, commentatori, associazioni di categoria e così via presentano i "megatrend" che, secondo le previsioni, plasmeranno il loro settore nel breve periodo.

E la cybersecurity non è da meno. Per quanto queste informazioni possano essere essenziali per aiutare i top manager ad anticipare i principali trend e a pianificare il futuro delle loro organizzazioni, quando si parla di Chief Information Officer (CIO), Chief Information Security Officer (CISO), team IT e della sicurezza IT, quello che conta veramente è come gestirne le implicazioni in termini pratici.

Per assistervi in questo processo, il nostro e-book riepilogherà alcuni dei trend di sicurezza più di spicco che attualmente si ripercuotono sul settore IT. In particolare, verranno descritte le implicazioni per l'uso da parte delle organizzazioni di soluzioni che vanno dalle piattaforme di protezione degli endpoint (EPP) alle soluzioni Endpoint Detection and Response (EDR) ed Extended Detection and Response (XDR).

Sommario

Voi dite megatrend. Io dico superficie d'attacco estesa

Anche per chi lavora nel settore IT, a volte può essere difficile apprezzare pienamente l'importanza della cybersecurity

La Security Industry Association (SIA), ad esempio, è la principale associazione di categoria per i provider di soluzioni di sicurezza globali, con oltre 1400 membri. Nell'introduzione all'edizione 2023 della sua visione per il settore, la SIA afferma che "non è in alcun modo sorprendente trovare ancora la cybersecurity del regno della sicurezza fisica nel nostro elenco dei megatrend per la sicurezza del 2023".

> "L'intelligenza artificiale e la cybersecurity continuano a contendersi il primo posto tra i trend che influenzano il settore della sicurezza, ma i dati sono chiari: la cybersecurity è il primo pensiero delle aziende leader nel settore della sicurezza." E "l'intelligenza artificiale e la cybersecurity rappresentano ordini di grandezza tenuti maggiormente in considerazione rispetto alle tendenze successive."

Per contestualizzare queste affermazioni, i professionisti del settore della sicurezza considerano la cybersecurity e l'intelligenza artificiale molto più critiche rispetto ai megatrend che si potrebbe altrimenti pensare che dominino il settore, come lo sviluppo della forza lavoro, le variazioni delle condizioni economiche e l'uso etico/sicuro di dati e tecnologie.

I trend più specifici dell'IT

Da report analoghi dei principali analisti come Gartner, IDC e Frost & Sullivan, emergono chiari riferimenti a tutto quello che va dall'aumentato dinamismo degli ambienti di rete che rende più difficile difendersi dalle vulnerabilità al costante incremento del volume e della sofisticatezza dei cyberattacchi che sfruttano queste vulnerabilità.

In Cybersecurity Megatrends 2022, ad esempio, IDC evidenzia i "sette trend della realtà della cybersecurity" tra cui:

- Digital transformation, lavoro ibrido e morte del perimetro
- Carenza di professionisti della sicurezza informatica
- Sofisticatezza in rapida crescita dei cybercriminali
- Proliferazione dei set di strumenti di sicurezza e piattaformizzazione
- Crescita ininterrotta delle normative in materia di conformità
- Nuovi acquirenti e vecchi acquirenti con nuove priorità
- Fiducia

Dal report di Gartner Top Trends in Cybersecurity 2023, nel frattempo, risulta evidente che "i principali trend nella cybersecurity di Gartner di quest'anno indicano un aumentato riconoscimento dell'importanza del coinvolgimento del personale nel programma di sicurezza per gestire i rischi di cybersecurity e sostenere un'efficace funzionalità di cybersecurity. La natura sempre più distribuita del lavoro amplifica l'adozione del cloud. A sua volta, questo aumenta la dipendenza dalla visibilità end-to-end degli ecosistemi digitali in espansione e dalla disponibilità di supply chain resilienti. Inoltre, i CIO stanno modificando i modelli operativi IT per promuovere una maggiore agilità dell'attività aziendale. L'ambiente normativo continua a evolversi, obbligando il management ad assumere un ruolo più attivo nella gestione dei rischi di cybersecurity. Se da una parte i pagamenti dei riscatti sono in diminuzione, gli attacchi ransomware su larga scala e gli attacchi ai sistemi di protezione delle identità continuano.

Questi trend globali vedono i principali leader che si occupano di gestione della sicurezza e del rischio concentrare i propri sforzi nei seguenti modi:

1. Focalizzandosi sul ruolo essenziale delle persone per il successo e la sostenibilità del programma di sicurezza.
2. Implementando capacità di sicurezza dal punto di vista tecnico che assicurano una maggiore visibilità e reattività nell'intero ecosistema digitale dell'organizzazione.
3. Ristrutturando il modo in cui opera la funzionalità di sicurezza per garantire l'agilità senza compromettere la sicurezza.

Per risolvere questi problemi, Gartner suggerisce che "i responsabili della gestione dei rischi e della sicurezza dovrebbero:

- Adottare il modo di pensare dell'autore di un attacco per determinare le priorità degli sforzi di mitigazione dei rischi informatici acquisendo una visione end-to-end della superficie d'attacco e consolidare i portfolio dei vendor, dove appropriato.
- Ottimizzare l'allineamento delle capacità di cybersecurity a nuove modalità di lavoro distribuite adottando nuovi modelli operativi di sicurezza e approcci architettonici che promuovano l'agilità e integrino la sicurezza per progettazione.
- Determinare le priorità e ottimizzare gli investimenti per il miglioramento del comportamento del personale allo scopo di migliorare e sostenere l'efficacia della sicurezza aziendale."

Tutte queste raccomandazioni sono chiaramente consigli affidabili. Quindi, come procedere per renderli operativi all'interno dell'organizzazione?

Per rispondere a questa domanda, occorre iniziare ad analizzare in maggiore dettaglio il panorama in costante evoluzione delle minacce e le sue implicazioni nell'ambito dell'infrastruttura, degli strumenti e dei controlli di sicurezza IT esistenti.

"Raramente le vulnerabilità zero-day sono la causa principale di una violazione. In altre parole, le violazioni potrebbero essere impedite se le organizzazioni correggessero la loro esposizione a una minaccia prima che un cybercriminale possa sfruttarla. Tuttavia, correggere ogni vulnerabilità nota è sempre stato irrealizzabile a livello operativo."

Gartner: Top Trends in Cybersecurity 2023

In che modo gli ultimi megatrend influenzano il panorama delle minacce

Rispetto solo a qualche anno fa, il panorama delle minacce si sta evolvendo molto più rapidamente di prima. Oggi è raro, ad esempio, che passi una settimana senza un report sull'ultimo attacco ransomware, data breach o truffa di alto profilo e non solo i cyberattacchi aumentano di numero, sono anche più sofisticati, più mirati e più difficili da rilevare.

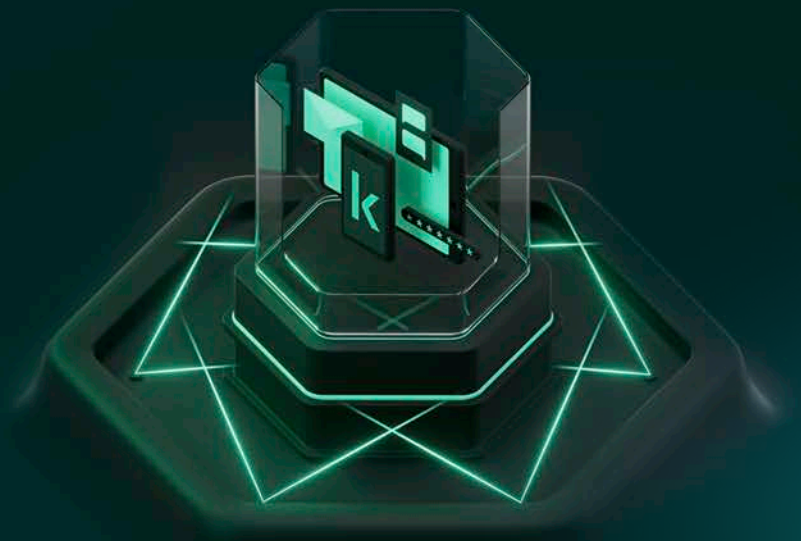
Molte delle persone coinvolte nei cyberattacchi sono criminali di professione e l'esperienza implica il successo. Il falso mito secondo cui gli hacker sono leoni da tastiera isolati non è più applicabile.

Prendendo come esempio il ransomware, i gruppi coinvolti si comportano sempre più come organizzazioni decentralizzate, con reti complesse di affiliate responsabili delle singole fasi del processo, da ricognizione, accesso, creazione del malware, distribuzione ed esfiltrazione dei dati a negoziazione del riscatto, pubblicazione dei dati rubati online e riciclaggio dei pagamenti dei riscatti.

La stragrande maggioranza degli attacchi ora ha tempi di permanenza che si misurano in ore anziché in giorni. I gruppi offrono anche un modello Ransomware-as-a-Service e mettono in atto attacchi che assomigliano più a minacce APT (Advanced Persistent Threat) in termini di portata. E gli hacktivisti e gli stati sovrani possono ricorrere al ransomware e ad altre tecniche (come i wiper) per scopi distruttivi o geopolitici invece che puramente commerciali.

Come se non bastasse, le tattiche, tecniche e procedure (TTP) utilizzate dai cybercriminali stanno diventando sempre più sofisticate. Tra gli esempi rientrano l'uso di funzionalità di auto-diffusione e auto-propagazione, lo sfruttamento di applicazioni pubbliche, account compromessi ed e-mail dannose e l'uso di strumenti come PowerShell che vengono ampiamente utilizzati nelle normali operazioni IT, rendendo così questi attacchi più difficili da individuare.

La conseguenza è che determinare il livello ottimale di protezione per la vostra organizzazione, sia che utilizziate soluzioni EPP, EDR e/o XDR, non è mai stato così importante.



Come siamo passati dall'EPP all'EDR e all'XDR?

Tradizionalmente, oltre a difendere i perimetri aziendali con firewall e protezione e-mail, le organizzazioni hanno concentrato i propri sforzi sugli endpoint, nella fattispecie PC, laptop, server (fisici e virtuali) e workstation, come misura di difesa principale contro le cyberminacce, al punto che le piattaforme di protezione degli endpoint (EPP) sono diventate uno strumento fondamentale per contrastare attacchi complessi.

Più di recente, le organizzazioni hanno iniziato anche a distribuire strumenti più avanzati per difendersi dagli attacchi. Possono essere utilizzati per identificare e rispondere a comportamenti anomali sugli endpoint, attraverso l'EDR (Endpoint Detection and Response), o in rete, tramite l'NDR (Network Detection and Response).

Ma come abbiamo appena visto, i cybercriminali perfezionano continuamente le loro tattiche e mettono in atto metodi sempre più sofisticati per prendere di mira le organizzazioni. Attualmente, gli autori degli attacchi stanno adottando sempre di più un approccio multi-vettore per sferrare i loro attacchi, spesso coinvolgendo più punti di accesso nell'infrastruttura e una vasta gamma di tattiche e tecniche differenti.

Gli autori degli attacchi sfruttano tecniche avanzate come social engineering (tra cui phishing e Business Email Compromise), account compromessi, app pubbliche ed exploit zero-day per violare le difese organizzative, rendendo particolarmente problematico proteggere le aziende da queste minacce in evoluzione.

Le minacce APT, ad esempio, eludono i tradizionali strumenti di rilevamento degli endpoint e possono rimanere attive per settimane o mesi, spostandosi lateralmente all'interno della rete, ottenendo autorizzazioni, esfiltrando dati e raccogliendo informazioni dai diversi livelli dell'infrastruttura IT in previsione di un attacco su larga scala o di un data breach.

La complessità e il volume enorme di questi attacchi rendono difficile per le organizzazioni stare sempre un passo avanti. E la superficie di attacco in continua espansione, inclusi dispositivi mobili, ambienti cloud e lavoro da remoto, per non parlare dei server, aggrava ulteriormente queste difficoltà.

Oltretutto, le organizzazioni devono confrontarsi con minacce interne, vulnerabilità della supply chain, requisiti normativi e di conformità, cercando di gestire allo stesso tempo la costante penuria di professionisti esperti nel settore della cybersecurity. E il potenziale danno a sistemi, processi operativi e reputazione dell'azienda derivante da data breach, ransomware, attacchi DDoS (Distributed Denial of Service), minacce APT, cyberspionaggio e così via può essere enorme.

Una strategia di protezione efficace contro queste minacce richiede pertanto un approccio proattivo e completo basato sull'uso di tecnologie avanzate, rigidi criteri, monitoraggio vigile, formazione costante e molto altro, che è esattamente la visione a 360° del panorama delle minacce che XDR intende offrire.

Eliminando la suddivisione in silos tra soluzioni specializzate per i diversi livelli, XDR garantisce ai Security Operations Center (SOC) e ai team addetti alla sicurezza IT la visibilità e l'integrazione end-to-end necessarie per identificare più rapidamente le minacce, rispondere tempestivamente, risolverle con maggiore efficacia e ridurre al minimo i danni causati.

Il 51% delle organizzazioni ha difficoltà a rilevare le minacce avanzate e a condurre indagini con gli strumenti a disposizione.

ESG Research Report, SOC Modernization and the Role of XDR, giugno 2022

Chi ha bisogno di quale tipo di sicurezza?

Per anni, le piccole e medie imprese (PMI) e le aziende di fascia bassa si sono affidate alle EPP per proteggersi da una vasta gamma di minacce commodity. Ma come abbiamo già accennato, ormai gli autori degli attacchi prendono di mira le organizzazioni di tutte le dimensioni, i settori e i livelli di preparazione, pertanto le PMI e le aziende più piccole sono sempre più a rischio di essere vittime delle minacce elusive più avanzate che prima colpivano solo le organizzazioni di dimensioni maggiori.

Per far fronte a questa situazione i team di sicurezza IT hanno integrato le soluzioni EPP con servizi EDR e/o Managed Detection and Response (MDR) che consentono di rilevare e analizzare gli incidenti di sicurezza, circoscrivere le minacce all'interno dell'endpoint e ricevere una response automatica e/o le istruzioni per la remediation.

La soluzione ideale è quella che integra la protezione degli endpoint con una sicurezza di livello EDR capace di alleggerire in modo significativo il carico di lavoro: più minacce si prevengono, meno materiale dovrà essere analizzato dal team di sicurezza. Questo consente a sua volta ai team IT di ottimizzare le risorse chiave e di concentrarsi sull'IT invece di rincorrere quantità spropositate di alert e falsi positivi.

La soluzione ideale è quella che integra la protezione degli endpoint con una sicurezza di livello EDR capace di alleggerire in modo significativo il carico di lavoro: più minacce si prevengono, meno materiale dovrà essere analizzato dal team di sicurezza.

Salendo di un livello rispetto a EDR e MDR, l'"extended" in Extended Detection and Response rispecchia il fatto che in XDR una soluzione EDR è supportata e strettamente integrata con un'ampia gamma di altri strumenti di sicurezza non necessariamente progettati per l'uso congiunto. Invece di utilizzare vari strumenti di sicurezza come soluzioni isolate, XDR consente alle organizzazioni di creare un ecosistema di sicurezza completo, flessibile e scalabile che sfrutti al massimo i vantaggi degli strumenti esistenti, possa essere personalizzato in base alle esigenze dell'organizzazione, riduca i rischi e garantisca la sicurezza.

Quindi per rispondere alla domanda "Quale tipo di sicurezza è più adatta?", i punti chiave da tenere in considerazione sono che:

- Tutte le organizzazioni hanno bisogno di una solida base per le moderne soluzioni di sicurezza degli endpoint.
- Gli ulteriori livelli di sicurezza richiesti dipenderanno in gran parte da una combinazione dei tipi di attacchi informatici a cui l'organizzazione è potenzialmente esposta e delle competenze di sicurezza IT del team IT addetto all'implementazione e all'utilizzo degli strumenti richiesti per prevenirli.

Analizzeremo ora cinque step fondamentali che vi aiuteranno a valutare e a rendere operativi i vostri requisiti di sicurezza in relazione a queste considerazioni.

Come valutare i vostri requisiti di sicurezza a mano a mano che si evolvono: EPP, EDR e MDR

Step 1:

Esaminate l'attuale protezione degli endpoint

Con così tante soluzioni avanzate di cybersecurity in commercio, è facile dimenticare il ruolo cruciale svolto dalla protezione degli endpoint. Perché gli endpoint sono così importanti? Non si tratta solo dei punti di ingresso più comuni nell'infrastruttura di un'organizzazione - e dell'obiettivo principale dei criminali informatici - ma anche delle principali fonti di dati per un'indagine efficace sugli incidenti complessi.

Di conseguenza, ogni impresa dovrebbe scegliere una soluzione EPP in grado di offrire protezione automatizzata da tutti i possibili incidenti causati dalle minacce commodity, comprese quelle fileless e il ransomware.

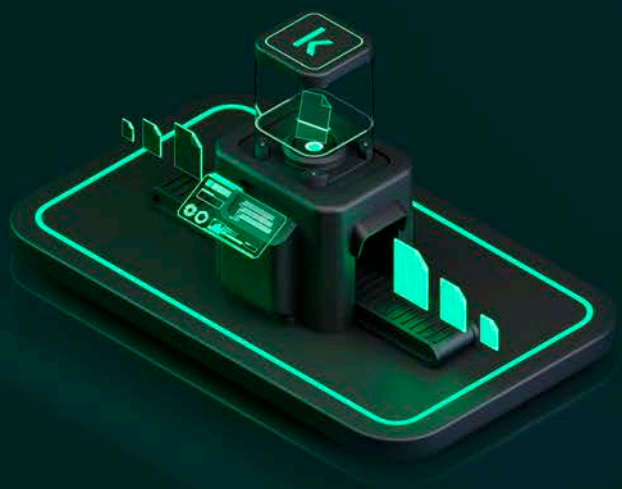
Dato che questa configurazione richiede conoscenze o personale di sicurezza relativamente limitato, soddisfa le esigenze di sicurezza degli endpoint delle PMI e delle imprese più piccole che non dispongono di un team di sicurezza dedicato o delle organizzazioni con livelli molto bassi di esperienza in cybersecurity.

Si tratta inoltre di un passaggio fondamentale per le aziende di medie e grandi dimensioni in cui, attraverso la gestione automatizzata di un gran numero di minacce minori, la soluzione consente ai team di sicurezza di concentrarsi sulle strategie di difesa più avanzate in caso di necessità.

Considerazioni chiave

Quando esaminate la soluzione EPP per valutare se garantisce prestazioni all'altezza delle aspettative, tenete in considerazione:

- Quanto è efficace?
- Quanti falsi positivi ricevete?
- Offre funzionalità efficaci di riduzione della superficie di attacco come anti-virus file, Web e posta, protezione di rete, Antimalware Scan Interface (AMSI), prevenzione degli exploit, remediation, rilevamento del comportamento e Host Intrusion Prevention (HIPS)?
- Aiuta ad automatizzare le attività di routine?
- È facile da gestire e aiuta a ridurre al minimo i costi e le spese generali del team IT?
- È di supporto in attività critiche come valutazione delle vulnerabilità, inventario software/hardware, firewall, controlli di applicazioni, dispositivi e Web e discovery delle attività sul cloud?



Step 2:

Individuate eventuali lacune critiche nelle difese degli endpoint

Perché le moderne soluzioni EPP richiedono funzionalità EDR

Come abbiamo discusso in questo e-book, la costante evoluzione del panorama delle minacce implica che, nel tempo, minacce sempre più sofisticate che in precedenza colpivano solo le grandi organizzazioni ora si ripercuotano sulle PMI e sulle aziende più piccole che non dispongono delle risorse interne necessarie per contrastarle in modo efficace.

In particolare, l'avvento delle minacce elusive, che utilizzano strumenti legittimi negli attacchi, includono scenari pronti all'uso per aggirare l'EPP, sono economiche e immediatamente disponibili sul Dark Web, ha notevolmente aumentato i rischi in termini di cybersecurity per le organizzazioni che usano le soluzioni EPP tradizionali.

Questi problemi sono ulteriormente aggravati dalla mancanza di trasparenza associata all'EPP tradizionale. Queste soluzioni, di fatto, offrono solo una rappresentazione semaforo rosso/verde del fatto che un attacco abbia luogo o meno. Invece, quello di cui un team IT con competenze di sicurezza di base ha bisogno è la visibilità su quello che accade nei singoli endpoint, in modo che possa essere analizzato in maggior dettaglio per aumentare la comprensione della minaccia.

Le moderne soluzioni EPP che integrano semplici funzionalità EDR fungono pertanto da porta di accesso tra l'EPP tradizionale e le soluzioni EDR più avanzate e complete.

Per quanto l'EPP possa proteggervi da una vasta gamma di minacce commodity, non dovete tralasciare le misure di difesa dalle minacce nuove, sconosciute ed elusive che aggirano la soluzione EPP.

Per i criminali informatici la preparazione di un attacco sta diventando sempre meno costosa, fattore che espone al rischio più imprese. Oltre a verificarsi con maggiore frequenza, questi tipi di attacchi sono diventati molto più efficaci grazie alla capacità dei criminali di combinare, testare e utilizzare varie tecniche per eludere con successo la sicurezza degli endpoint.

Anche l'urgenza di affrontare queste minacce è diventata sempre più critica a causa di cambiamenti quali la scomparsa dei perimetri aziendali dovuta al rapido aumento del lavoro da remoto. Insieme, questi trend stanno alimentando il bisogno di una soluzione EPP le cui capacità vadano oltre quelle fornite dalle soluzioni EPP tradizionali e includano in particolare funzionalità EDR di base come la root cause analysis semplificata.

Considerazioni chiave

Ecco alcuni elementi che indicano che è ora di espandere le proprie difese oltre l'EPP tradizionale:

- EPP non è in grado di bloccare un numero crescente di minacce nuove, sconosciute ed elusive.
- Avete una visibilità limitata rispetto a ciò che accade nei vostri endpoint, quindi non riuscite, ad esempio, a eseguire in tempo reale la root cause analysis, le attività di investigation e response alle minacce, oppure dovete svolgerle manualmente, caso per caso, con gli strumenti standard del sistema operativo: un processo lento, complesso e con un elevato rischio di errori.
- Non avete le competenze in termini di sicurezza IT necessarie per affrontare minacce sempre più sofisticate.
- Siete preoccupati per le potenziali sanzioni o per i danni alla reputazione della vostra azienda derivanti da un grave incidente di sicurezza informatica.

Per implementare una soluzione di difesa efficace contro queste minacce, dovete anche valutare vari aspetti della vostra azienda, tra cui le dimensioni, il profilo aziendale, la preparazione rispetto alla sicurezza, le risorse e le competenze esistenti e, in particolare, il livello di competenza del vostro team IT o di sicurezza IT.

Step 3:

Definite con precisione ciò che volete ottenere

Molte imprese hanno tempo e risorse limitati (o un piccolo reparto di sicurezza IT che non intendono espandere), ma hanno l'esigenza di capire che cosa sta succedendo alla loro infrastruttura ed essere in grado di rispondere alle minacce elusive prima che queste arrechino danni.

L'aggiunta di funzionalità EDR appropriate alla moderna soluzione EPP può garantire una difesa altamente efficace contro le minacce elusive più avanzate. Questo dovrebbe consentire la formulazione di risposte automatizzate e/o rapide e precise "single-click", come la messa in quarantena dei file, l'isolamento degli host, l'arresto di un processo, l'eliminazione di un oggetto e così via. E, se avete un team di specialisti della sicurezza IT, dovrebbe fornire loro le informazioni, gli approfondimenti e gli strumenti necessari per condurre un'indagine efficace, come root cause analysis, creazione di indicatori di compromissione (IoC) personalizzati, importazione di IoC e relativa scansione in tutti gli endpoint.

Inoltre avrete bisogno di una soluzione che vi consenta di sfruttare in maniera ottimale tutte le funzionalità di cui avete effettivamente bisogno, anziché pagare parecchie funzioni superflue e ritrovarsi a reclutare esperti di sicurezza IT con le competenze necessarie per poterne beneficiare.

Cinque luoghi comuni sull'EDR

1 La nostra soluzione di protezione degli endpoint funziona: non ci serve l'EDR

Luogo comune: i cybercriminali non sono interessati ad aziende come la nostra: siamo immuni ai tipi di attacchi da cui offre protezione l'EDR.

Realtà: nonostante si possa pensare che i cybercriminali tendano a non prendere di mira le piccole aziende, la realtà è che le PMI devono affrontare gran parte delle minacce a cui sono soggette le grandi aziende. Anche se la stragrande maggioranza dei cyberattacchi si basa su minacce commodity, il resto è costituito in larga parte da attacchi nuovi, sconosciuti ed elusivi che aggirano l'EPP tradizionale. Queste minacce sono difficili da rilevare, a causa delle varie tecniche di elusione che adottano, in particolare l'impiego di strumenti legittimi e nativi del sistema. Passando a lungo inosservate, hanno anche il tempo di esplorare e di infiltrarsi nell'infrastruttura di un'azienda causando danni maggiori, che si tratti di un data breach, di un attacco ransomware, spyware o dell'override diretto.

2 Abbiamo bisogno dell'EDR per compensare soluzioni EPP inefficaci

Luogo comune: la nostra soluzione EPP non è abbastanza efficace, quindi abbiamo bisogno dell'EDR per rafforzarla.

Realtà: cercare di rafforzare la sicurezza dei vostri endpoint investendo in una soluzione EDR senza prima affrontare i problemi con la soluzione EPP è come costruire un castello di sabbia. Una soluzione EPP inefficace può effettivamente minare l'EDR, rendendolo incapace di garantire i risultati richiesti. Inoltre, se la soluzione EDR è eccessivamente specifica per le vostre effettive esigenze, potrebbe anche risultare troppo costosa e difficile da comprendere e utilizzare per il vostro team.

3 Per utilizzare EDR è necessario un team esperto di sicurezza IT

Luogo comune: le PMI e le aziende di fascia bassa non hanno abbastanza specialisti della sicurezza con le competenze per comprendere e utilizzare gli strumenti necessari per rilevare, indagare e reagire alle minacce elusive.

Realtà quando l'EDR è stato introdotto inizialmente, i sistemi erano complicati e difficili da usare. Ma con le soluzioni moderne, ogni volta che riceverete un alert, la soluzione EDR vi aiuterà a capire da dove proviene la minaccia, come si è sviluppata, qual è la sua root cause, se ha interessato altri host e, di conseguenza, qual è la sua portata. Dovrebbe inoltre guidarvi attraverso un semplice processo di gestione degli incidenti che comprende fasi quali l'identificazione, il contenimento, l'eliminazione, il ripristino e l'analisi di quanto appreso per prepararsi a futuri attacchi.

4 Non è possibile combinare EDR e MDR

Luogo comune: se desiderate una sicurezza di tipo EDR, dovete investire in soluzioni EDR utilizzabili dal vostro team interno o lasciare che sia un fornitore specializzato a occuparsi dell'MDR.

Realtà: la sicurezza di tipo EDR non esclude altre soluzioni. Le soluzioni EDR e MDR hanno ciascuna i propri vantaggi e l'opzione migliore è spesso quella di combinarle. Una PMI o un'azienda di fascia bassa potrebbe ad esempio utilizzare l'MDR per aumentare istantaneamente la propria capacità di sicurezza IT e proteggersi dalle minacce elusive, senza la necessità di investire in altro personale o risorse aggiuntive; mentre un'azienda di dimensioni maggiori potrebbe utilizzare queste soluzioni per trasferire i processi di valutazione e indagine sugli incidenti 24 ore su 24, 7 giorni su 7, e concentrarsi maggiormente sulle risorse di sicurezza IT interne utilizzando l'EDR per processi di investigation e response dettagliati.

5 EDR aumenta l'impegno associato agli alert e non risulta quindi vantaggioso

Luogo comune: è risaputo che l'EDR genera un gran numero di alert e falsi positivi che i team IT non hanno né il tempo né le risorse per gestire o risolvere.

Realtà: le moderne soluzioni EDR non solo automatizzano molte attività, ma l'EDR e/o l'MDR hanno il potere di portarvi da una situazione di rischio significativo di attacco evasivo a una situazione di rinnovata fiducia nella sicurezza dei vostri endpoint. Anziché non avere certezze su ciò che sta accadendo nel vostro ambiente, avrete visibilità e controllo su tutti gli endpoint. E anziché essere riluttanti a eseguire upgrade di sicurezza a causa della loro complessità, avrete una soluzione semplificata e consolidata che vi aiuterà a ottimizzare le risorse.

Provate il nostro gioco di simulazione del ransomware interattivo per scoprire come proteggere meglio l'infrastruttura IT:
https://www.kaspersky.com/response-game/en/

Step 4:

Pensate ai vostri use case

Prima di individuare la protezione più adatta alle vostre esigenze, dovete stabilire requisiti ben definiti. Ciò significa considerare gli aspetti critici delle prestazioni e dell'utilizzo standard della soluzione, come gli use case a cui si rivolge e i risultati che vi aspettate che fornisca.

Per esempio, quando ricevete un alert di sicurezza, EDR e/o MDR dovrebbero consentirvi di rispondere a domande fondamentali come:

- Qual è il contesto dell'alert?
- Quali azioni sono già state intraprese in relazione all'alert?
- La minaccia rilevata è ancora attiva?
- Vi sono altri host sotto attacco?
- Da dove ha avuto origine l'attacco?
- Qual è la root cause della minaccia?

Queste soluzioni dovrebbero inoltre aiutarvi a comprendere la portata complessiva della minaccia. Ad esempio:

- Se rischiate di essere vittime di una minaccia nota, probabilmente il vostro team di gestione vorrà avere la certezza di non essere sotto attacco in questo momento, pertanto avrete bisogno di trovare un indicatore di compromissione (IoC) online, eseguire una scansione e rispondere correttamente a tutte le domande.
- Se un'autorità di regolamentazione vi chiedesse di eseguire una scansione per un IoC specifico, dovreste essere in grado di importare gli IoC da fonti attendibili ed eseguire scansioni periodiche per rilevare potenziali indicatori di un attacco.
- Se avete esaminato a fondo un avviso e generato un IoC in base alla minaccia rilevata, dovrebbe iniziare automaticamente la scansione nell'intera rete per scoprire se sono stati interessati altri host.

Analogamente, dovreste essere in grado di rispondere rapidamente alle minacce con un'elevata velocità di replicazione e movimento nei seguenti modi:

- Contenendo la minaccia tramite l'isolamento dell'host, la messa in quarantena dei file o il blocco dell'esecuzione dei file durante l'indagine.
- Utilizzando una risposta automatica trasversale tra più endpoint basata sulle scansioni IoC, che vi consente di rispondere alle minacce elusive non appena vengono rilevate, o scenari di risposta guidata e da remoto se utilizzate l'MDR.

Alcuni dei risultati principali che dovreste quindi aspettarvi dalla soluzione sono:

- Protezione dalle minacce elusive più frequenti e dannose.
- Risparmio in termini di tempo e risorse grazie a uno strumento semplice e automatico.
- Valutazione della portata di un attacco attraverso la scansione IoC in tutti gli endpoint.
- Individuazione della root cause di ciascuna minaccia e della relativa modalità di attuazione.
- Prevenzione di ulteriori danni grazie alla response automatica rapida.

Cinque luoghi comuni sull'MDR

1 L'MDR è solo un servizio di sicurezza gestito come tanti

Luogo comune: l'MDR si comporta come qualsiasi altro servizio di sicurezza gestito (MSS) che prevede la gestione dell'infrastruttura IT da parte del vendor.

Realtà: i servizi MSS includono in genere una gamma di servizi generici di sicurezza informatica tra cui la valutazione della compliance normativa, tecnologie come VPN e firewall, penetration test, offerta di suggerimenti e così via. L'MDR si concentra invece sulla detection avanzata e sulla risposta rapida a minacce nuove, sconosciute ed elusive che aggirano le piattaforme EPP automatizzate, attraverso una combinazione di ricerca, detection e analisi delle minacce basati su TTP.

2 L'MDR è solo per le grandi aziende

Luogo comune: poiché l'MDR si occupa di funzionalità complesse come il threat hunting e gli Indicatori di attacco (IoA), è adatto solo alle esigenze delle grandi aziende.

Realtà: l'MDR non è una soluzione universale. Offre funzionalità diverse per diversi tipi di organizzazioni. Una PMI o un'azienda di piccole dimensioni potrebbe utilizzare l'MDR per migliorare istantaneamente la propria sicurezza IT e proteggersi dalle minacce elusive, mentre un'azienda di dimensioni maggiori potrebbe utilizzare queste soluzioni per trasferire la valutazione e l'indagine sugli incidenti e concentrarsi maggiormente sulle risorse di sicurezza IT interne.

3 L'MDR basato sull'intelligenza artificiale non ha bisogno di personale esperto

Luogo comune: l'intelligenza artificiale (IA) e le tecniche di machine learning hanno raggiunto livelli talmente avanzati che l'uso di personale esperto in MDR sarà presto un ricordo del passato.

Realtà: intelligenza artificiale, machine learning e IoA proprietari consentono l'elaborazione automatica di un numero elevato di alert, automatizzando la classificazione iniziale degli incidenti, riducendo al minimo il tempo medio di rilevamento (MTTD) e di reazione (MTTR) mediante l'aumento significativo del throughput degli analisti MDR e assicurando protezione continua anche dalle minacce non-malware più innovative. Ma per TTP precedentemente sconosciute o condotte da esseri umani che non si traducono in una detection automatica, il threat hunting gestito si basa ancora sul lavoro meticoloso, proattivo e concreto dei threat hunter esperti.

4 L'MDR è difficile da implementare

Luogo comune: dal momento che l'MDR è spesso commercializzato per offrire le capacità di un SOC 24 ore su 24, 7 giorni su 7, è scontato che sia complicato da utilizzare.

Realtà: come evidenziato in precedenza, l'MDR può essere utilizzato per diverse finalità, tra cui prevenire le minacce che aggirano le difese informatiche esistenti o avere una seconda opinione o consentire agli esperti interni di concentrarsi su attività più importanti. Può essere considerato un servizio pronto all'uso facilmente implementabile che offre notevoli miglioramenti in ambito MTTD e MTTR. Più MTTD e MTTR sono rapidi, minori sono le interruzioni causate dagli incidenti e i costi associati.

5 Anche in presenza dell'MDR, tuttavia, le attività di competenza del vostro team rimangono molte

Luogo comune: l'ambito d'azione dei servizi MDR si ferma all'indagine sugli incidenti, offrendo ai clienti report tecnici e consigli da applicare ai sistemi e aumentando ulteriormente la pressione sulle risorse di sicurezza IT.

Realtà: mentre questo avveniva sicuramente in passato, con i moderni servizi MDR potete scegliere di autorizzare il fornitore a reagire automaticamente per conto vostro, avviare azioni di response consigliate (ad esempio isolamento dell'host, spostamento dei file in quarantena, rimozione dei file, arresto dei processi, richiesta di file o esecuzione di un programma nell'host, scansioni IoC e così via) o applicare scenari di remediation gestiti che è possibile approvare preventivamente o manualmente per ciascun alert.

Il Security Operations Center (SOC) e il Global Emergency Response Team (GERT) di Kaspersky hanno analizzato un anno di incidenti di sicurezza in ogni settore per produrre un'istantanea senza confronti del panorama delle minacce.

Accedete ai report: https://go.kaspersky.com/mdr-and-ir-reports-2022.html

Step 5:

Scegliete la protezione più adatta alle vostre esigenze

Molte aziende potrebbero non disporre di risorse dedicate specificamente dedicate alla sicurezza IT. Alcune potrebbero avere appena iniziato a creare il proprio reparto di sicurezza IT, mentre altre potrebbero già disporre di team di sicurezza IT formati e qualificati.

Molte aziende potrebbero non disporre di risorse dedicate specificamente dedicate alla sicurezza IT. Alcune potrebbero avere appena iniziato a creare il proprio reparto di sicurezza IT, mentre altre potrebbero già disporre di team di sicurezza IT formati e qualificati. La qualità dell'esperienza di queste aziende con la threat defense varierà quindi notevolmente, così come la quantità di tempo che potranno dedicare a questa attività.

Per far fronte a queste diverse circostanze, le aziende senza personale di sicurezza IT dedicato, o quelle il cui personale di sicurezza IT è sovraccaricato dalle attività di routine, dovranno fare un uso strategico dell'automazione per contrastare le più recenti minacce elusive.

Questo vuol dire integrare il proprio EPP con strumenti EDR aggiuntivi che, pur proteggendo da queste minacce, incorporano anche livelli appropriati di automazione (totale o parziale).

In alternativa, anziché investire in una soluzione EDR eccessivamente complessa per la quale potrebbero non avere il tempo o le competenze necessarie, l'MDR permette alle organizzazioni di accedere a funzionalità come il monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7 da parte di esperti del settore, il threat hunting automatizzato e gestito e scenari di response guidata da remoto, tramite un vendor, un Managed Service Provider (MSP) o un Managed Security Service Provider (MSSP).

Una terza opzione è quella di combinare EDR e MDR. Molte aziende non hanno le competenze necessarie per il threat hunting, in questi casi è spesso una soluzione ideale esternalizzare queste operazioni implementando in-house le funzionalità di detection and response. Può rivelarsi particolarmente vantaggioso anche per quelle aziende che desiderano sviluppare il proprio team di cybersecurity, ma non dispongono delle risorse, del personale e/o delle competenze per una detection and response specializzata.

Cosa fare se si dispone solo di risorse interne limitate?

Supponiamo che disponiate di risorse interne limitate in materia di sicurezza IT o di un piccolo team di uno o due specialisti della sicurezza. Supponiamo inoltre che stiate cercando di decidere se integrare la vostra soluzione EPP con EDR e/o MDR. Che tipo di vantaggi potete aspettarvi e quale sarebbe la soluzione giusta per voi?

Se preferite un approccio più pratico (e il vostro team IT dispone di competenze di sicurezza IT sufficienti), l'EDR può aiutarvi a prevenire interruzioni e danni al business eliminando i rischi rappresentati da minacce nuove, sconosciute ed elusive e dando al personale di sicurezza la visibilità necessaria per la threat investigation, la root cause analysis e la response.

Questo può ottimizzare i costi consentendo al team di sicurezza di lavorare in modo più efficiente, senza doversi destreggiare tra più strumenti e console, e di massimizzare le attività automatizzando una vasta gamma di processi. Il monitoraggio e la detection delle minacce, nonché la response e la prevenzione degli attacchi, risulteranno semplificati.

Se intendete espandere le vostre competenze IT interne mediante l'offload delle attività di detection and response, MDR può offrire una protezione avanzata e continua dalle minacce che altrimenti potrebbero eludere le barriere di sicurezza automatizzate. Questo può aiutare a rendere più efficiente l'azienda, rimediando alla mancanza di personale IT specializzato e assicurando i principali vantaggi di un SOC operativo 24 ore su 24, 7 giorni su 7.

L'MDR può inoltre ottimizzare i costi lasciando che le risorse interne si concentrino sulle attività critiche che richiedono davvero il coinvolgimento del team IT o di sicurezza IT e sfruttando modelli avanzati di ML per aumentare significativamente il livello di produttività degli analisti e ridurre al minimo l'MTTR. Inoltre, può offrire il monitoraggio della sicurezza continuo da parte degli esperti del settore, insieme al threat hunting automatizzato e gestito, che comprende l'analisi di minacce complesse differenti dai malware, pericolose e difficili da rilevare perché sferrano l'attacco abusando di strumenti legittimi del sistema operativo.

La combinazione di EDR e MDR, nel frattempo, vi consente di adattare le funzionalità EDR alle vostre specifiche esigenze, per esempio esternalizzando il threat hunting (per il quale potreste non avere l'esperienza necessaria) e implementando in-house le funzionalità di endpoint detection and response.

Come valutare i vostri requisiti di sicurezza a mano a mano che si evolvono: XDR

Il 40% delle organizzazioni avrà implementato una piattaforma XDR entro il 2027, rispetto al 5% nel 2021

Secondo il Cyber Resilient Organization Study 2021 di IBM, il 32% delle organizzazioni ha affermato di avere utilizzato dai 21 ai 30 strumenti di sicurezza per rispondere alle singole minacce, mentre il 13% ha dichiarato di aver fatto ricorso a più di 31 strumenti.

Proprio a causa del numero di strumenti coinvolti, le organizzazioni impiegano troppo tempo a identificare e contenere le minacce avanzate.

Dal report Cost of a Data Breach 2022 di IBM è emerso che il data breach medio richiede 277 giorni per essere rilevato e risolto, quindi una violazione verificatasi in data 1 gennaio potrebbe non risolversi fino al 4 ottobre.

XDR in breve

Se la vostra è una media impresa o una grande azienda e il SOC o il team di sicurezza IT non vi ha ancora assillato riguardo alla necessità dell'XDR, è solo questione di tempo prima che accada.

Come evidenziato dal CRN (15.2.23), "quando si parla di threat detection e response, limitarsi a guardare l'endpoint o la rete non basta più. L'approccio verso cui stanno transitando molte delle più grandi aziende di cybersecurity al mondo in questo ambito è l'XDR, o Extended Detection and Response. Attualmente una delle categorie in più rapida crescita nel campo della cybersecurity, XDR punta a garantire una sicurezza superiore mettendo in correlazione i dati provenienti dagli ambienti e dai dispositivi di un'organizzazione, assegnando quindi le priorità alle minacce più serie per una risposta.

"Indipendentemente da come si definiscono esattamente, le piattaforme XDR sono tutte focalizzate a sostenere i team di sicurezza a corto di personale, allo scopo di migliorare la qualità del rilevamento delle minacce riducendo al tempo stesso il sovraccarico negli alert."

Con XDR, le soluzioni di sicurezza che non sono necessariamente progettate per l'uso congiunto possono interagire perfettamente per la prevenzione, il rilevamento, l'indagine e la risposta alle minacce. Ed eliminando le falle di visibilità tra i livelli e gli strumenti di cybersecurity, XDR permette ai team IT già sovraccarichi di individuare e risolvere le minacce in modo più rapido ed efficiente, nonché di acquisire dati contestuali più completi per prendere decisioni più efficaci per la sicurezza e prevenire futuri attacchi.

Quindi cosa fa esattamente XDR, quali sono i vantaggi e perché potenzialmente è uno degli investimenti più significativi in termini di sicurezza che la vostra organizzazione possa mai fare?

Confronto tra EDR, MDR e XDR

EDR
Endpoint Detection and Response

- Identifica le minacce nuove, sconosciute ed elusive che aggirano la protezione degli endpoint e automatizza le attività di sicurezza di routine

MDR
Managed Detection and Response

- Esternalizza il rilevamento delle minacce, il threat hunting e l'investigation sugli incidenti o integra le misure esistenti assicurando una protezione avanzata contro le minacce, 24 ore su 24, 7 giorni su 7

XDR
Extended Detection and Response

- Rileva in modo proattivo le minacce complesse su più livelli di infrastruttura e risponde automaticamente a tali minacce per contrastarle

Come funziona

- Migliora la visibilità e la visualizzazione delle minacce
- Fornisce meccanismo di detection avanzati (ad es. IoC, IoA)
- Semplifica la root cause analysis e supporta il threat hunting
- Fornisce una risposta rapida e automatizzata

- Fornisce una protezione continua contro le minacce malwareless più complesse e innovative

- Si integra con più strumenti di sicurezza, applicazioni e con l'infrastruttura di cybersecurity esistente
- Monitora i dati provenienti da più fonti per rilevare ed eliminare le minacce complesse

Valore aziendale

- Consente ai team responsabili della sicurezza IT di lavorare in modo più efficiente, senza spostarsi tra più strumenti e diverse console
- Automatizza una vasta gamma di processi per evitare di affidarsi ai processi di remediation tradizionali che potrebbero comportare tempi di inattività
- Semplifica il monitoraggio e il rilevamento delle minacce, l'aggregazione dei dati forensi a livello centrale e la risposta e la prevenzione degli attacchi

- Consente alle risorse interne qualificate di concentrarsi sulle attività critiche che richiedono realmente l'intervento del team di sicurezza IT
- Sfrutta i modelli proprietari di machine learning per migliorare in modo significativo la produttività degli analisti e ridurre al minimo MTTD e MTTR
- Risolve la crisi di talenti nel campo della cybersecurity
- Offre tutti i principali vantaggi di un SOC disponibile 24 ore su 24, 7 giorni su 7

- L'approccio basato sull'ecosistema ottimizza l'efficienza degli strumenti di cybersecurity coinvolti, consente di risparmiare risorse e riduce i rischi
- Semplifica il lavoro degli specialisti della sicurezza IT e fornisce loro il contesto aggiuntivo necessario per indagare sugli attacchi multi-vettore
- Riduce al minimo MTTD e MTTR, fondamentali per contrastare minacce complesse e attacchi mirati
- Fornisce una protezione olistica contro il panorama delle minacce in evoluzione

Per chi è più indicato?

- Aziende avverse al rischio e conservative dal punto di vista tecnico che desiderano aggiungere visibilità alla protezione automatica
- Utenti IT standard che intendono sviluppare processi di incident response
- Organizzazioni che utilizzano l'IT come vantaggio competitivo e devono mettere i propri esperti in condizione di trovare e neutralizzare minacce complesse

- Aziende che intendono espandere la capacità della sicurezza IT interna, alleggerendo il carico dei task di rilevamento e risposta
- Organizzazioni che potrebbero non disporre del budget o del personale specializzato per creare un proprio SOC interno

Organizzazioni con risorse di sicurezza significative che desiderano un'unica piattaforma in grado di offrire:

- Un quadro coerente di ciò che sta accadendo nell'infrastruttura
- Ricerca delle minacce e threat intelligence integrate
- Migliore definizione delle priorità degli incidenti e meno avvisi di falsi positivi

Capacità e vantaggi specifici che dovreste aspettarvi da una piattaforma XDR

Un'unica piattaforma integra diversi strumenti di sicurezza

Con XDR, le soluzioni di sicurezza che non sono necessariamente progettate per l'uso congiunto possono interagire perfettamente per la prevenzione, il rilevamento, l'indagine e la risposta alle minacce.

- Possono includere, ad esempio, soluzioni pensate per proteggere posta, Web, rete, infrastruttura cloud, applicazioni, identità e così via, consentendo il rilevamento e l'indagine su ulteriori tipi di scenari di attacco e rafforzando il processo di contrastare le minacce complesse.
- XDR può anche includere strumenti di threat intelligence, come feed di dati sulle minacce e la piattaforma utilizzata per la gestione di questi dati, per fornire ai team SOC un ulteriore contesto, che si rivela fondamentale quando si indaga su incidenti informatici complessi.
- Inoltre, a seconda dei requisiti e del settore di un'organizzazione, XDR può integrare strumenti di sicurezza OT (Operational Technology) e IoT (Internet of Things), sviluppando una soluzione di sicurezza completa per gli ambienti IT/OT.

Unisce più tipi di telemetria

Consentendo l'analisi in tempo reale del comportamento e dei dati di telemetria tra più livelli di sicurezza, inclusi endpoint, rete e cloud, i security analyst possono visualizzare meglio le cyberminacce, individuandole ed eliminandole sulla base della gravità con cui possono ripercuotersi sull'infrastruttura IT dell'organizzazione.

Offre una visibilità delle minacce end-to-end

Eliminando la suddivisione in silos tra soluzioni specializzate per i diversi livelli, XDR garantisce al SOC e ai team addetti alla sicurezza IT la visibilità e l'integrazione end-to-end necessarie per identificare più rapidamente le minacce, rispondere tempestivamente, risolverle con maggiore efficacia e ridurre al minimo i danni causati.

Dal momento che XDR può collegare ogni passaggio all'interno di una kill chain presentandola come un unico alert con una descrizione dettagliata del contesto completo dell'attacco, si riduce il volume degli alert aumentandone la qualità e si consentono una orchestration e una response end-to-end.

Semplifica e centralizza la raccolta dei dati e aumenta l'efficienza

Un unico data lake consente la raccolta, la gestione e l'archiviazione complete dei log, fornendo una piattaforma centralizzata per raccogliere, indicizzare e analizzare i log da diverse origini, tra cui soluzioni di sicurezza (EPP, FW, NGFW, IAM, SIEM, SOAR e così via), sistemi operativi, applicazioni aziendali (sistemi HR, strumenti per ufficio), sicurezza fisica (sistemi di controllo degli accessi automatizzati) e altri dispositivi.

Questo consente al SOC e ai team di sicurezza IT di ottenere informazioni preziose, rilevare anomalie e identificare potenziali incidenti di sicurezza utilizzando i dati dei log relativi a eventi passati e presenti (in tempo reale). L'integrazione con altri strumenti e piattaforme di sicurezza ottimizza inoltre l'efficienza operativa centralizzando la gestione della sicurezza e fornendo una visione unificata degli incidenti e degli eventi di sicurezza.

Accelera threat detection, investigation e response

Eliminando le falle di visibilità tra i livelli e gli strumenti di cybersecurity, XDR permette ai team IT già sovraccarichi di individuare e risolvere le minacce in modo più rapido ed efficiente, nonché di acquisire dati contestuali più completi per prendere decisioni più efficaci per la sicurezza e prevenire futuri attacchi.

Automatizzando le attività di routine come la classificazione, il contenimento e la correzione delle minacce, le organizzazioni possono ottimizzare le risorse di sicurezza e concentrarsi su attività più strategiche.

Riduce MTTD e MTTR

XDR aiuta a ridurre il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR), essenziali per affrontare minacce complesse e attacchi mirati, per cui le azioni tempestive messe in atto dagli esperti di sicurezza IT riducono il tempo di permanenza e le possibilità che gli aggressori raggiungano il loro obiettivo di causare danni finanziari o alla reputazione per l'organizzazione.

Migliora il threat hunting

Sfruttando l'ultima intelligence sulle minacce, XDR ottimizza il threat hunting e la discovery, mentre l'automazione delle attività di routine, i processi di indagine guidata e i rilevamenti personalizzabili promuovono tutti una rapida risoluzione degli incidenti. Le minacce avanzate vengono rilevate e neutralizzate con più velocità e accuratezza, aspetto fondamentale per attacchi complessi e APT.

Aiuta a risolvere la carenza globale di esperti di sicurezza IT

Tra una carenza a livello globale di esperti di sicurezza IT, XDR fornisce una protezione olistica per l'infrastruttura IT in espansione contro un panorama delle cyberminacce in rapida evoluzione. XDR semplifica il lavoro degli specialisti di sicurezza IT che dispongono di risorse scarse, riduce la necessità che siano coinvolti nelle attività di routine e li rende liberi di impegnarsi nel processo di gestione di incidenti complessi.

Supporta la conformità normativa e la gestione dei rischi

Sfruttando la visibilità completa, la threat intelligence e le capacità di reporting, le organizzazioni possono dimostrare la propria conformità ai framework e alle normative del settore come GDPR, PCI DSS, HIPAA e molto altro. Così facendo, potranno mitigare i rischi finanziari e legali associati alla mancata conformità.

Anche la gestione dei log svolge un ruolo cruciale nel garantire la conformità alle normative e agli standard regionali o del settore, facilitando l'archiviazione e la retention di dati e log per la durata prescritta e permettendo alle organizzazioni di recuperare e analizzare facilmente i log in caso di necessità.

Consente una gestione intuitiva attraverso un'unica console

Le intuitive soluzioni XDR forniscono informazioni complete sulle minacce in atto e le attività sospette attraverso un'unica console. Questo consente un threat hunting proattivo e una risposta più rapida agli incidenti e fornisce una visione olistica che aiuterà i team SOC a identificare le attività sospette e i potenziali incidenti di sicurezza in modo più efficiente.

Opzioni di piattaforma aperta e nativa

Open XDR supporta l'integrazione con soluzioni di terze parti per raccogliere specifici formati di dati di telemetria per consentire il rilevamento, il threat hunting e l'indagine sulle minacce su origini dati differenti e mettere in atto azioni di risposta. Il risultato è l'assenza di vincoli con il vendor e la possibilità da parte delle organizzazioni di sfruttare gli strumenti di sicurezza di terze parti già implementati e scegliere i prodotti più adatti dai diversi vendor.

XDR nativo è una soluzione di un unico vendor progettata per integrarsi con i prodotti di quello specifico vendor.

Distribuzione nel cloud e/o on-premises

Mentre buona parte delle piattaforme XDR sono aperte e basate sul cloud, la distribuzione on-premises è l'ideale per le organizzazioni che intendono consentire la massima sovranità dei dati e assicurarsi di rispettare i requisiti normativi e di conformità.

Integrazione con Zero Trust

Se usati insieme, XDR e Zero Trust offrono una potente difesa contro le cyberminacce. Zero Trust impedisce l'accesso non autorizzato a risorse e applicazioni o revoca l'accesso già concesso in caso di variazione delle condizioni, mentre XDR aiuta a rilevare e a rispondere alle potenziali minacce che riescono a eludere quei controlli di accesso iniziali.

Confronto tra XDR, SIEM e SOAR

XDR
Extended Detection and Response

- Rileva in modo proattivo le minacce complesse su più livelli di infrastruttura e risponde automaticamente a tali minacce per contrastarle

SIEM
Security Information and Event Management

- Raccoglie, aggrega, analizza e archivia i dati dei log dell'intera infrastruttura IT per casi d'uso che includono governance/conformità e correlation matching basato su regole per il rilevamento delle attività sospette

SOAR
Security Orchestration and Automated Response

- Acquisisce dati da una varietà di fonti nell'infrastruttura, inclusi sistemi di gestione e piattaforme di threat intelligence, e fornisce analisi delle priorità
- Consente ai team di sicurezza di configurare risposte automatizzate multi-fase e multi-soluzione alle minacce in arrivo

Come funziona

- Integra più strumenti e applicazioni di sicurezza
- Monitora i dati su endpoint, reti, cloud, server Web, server di posta e così via per rilevare ed eliminare le minacce complesse

- Cerca eventuali modelli o eventi che potrebbero indicare comportamenti sospetti e genera un alert per il SOC o il team di sicurezza IT

- Utilizza playbook per automatizzare un'ampia gamma di flussi di lavoro, tra cui la scansione delle vulnerabilità, l'analisi dei log, la gestione degli accessi degli utenti, la classificazione delle minacce e altro ancora
- Coordina più strumenti e processi in un flusso di lavoro più ampio, raccogliendo tutti i dati rilevanti in un'unica piattaforma per informazioni consolidate e utilizzabili

Quali sono le differenze?

- L'approccio basato sull'ecosistema ottimizza l'efficienza degli strumenti di cybersecurity coinvolti, consente di risparmiare risorse e riduce i rischi
- Semplifica il lavoro degli specialisti della sicurezza IT e fornisce loro il contesto aggiuntivo necessario per indagare sugli attacchi multi-vettore
- Riduce al minimo MTTD e MTTR, fondamentali per contrastare minacce complesse e attacchi mirati
- Fornisce una protezione olistica contro il panorama delle minacce in evoluzione

- L'enorme set di dati fornito da SIEM può comportare troppi alert che devono essere filtrati, elaborati e analizzati manualmente
- Non fornisce il contesto necessario per gestire gli attacchi nuovi, complessi o sofisticati
- La soluzione passiva non include capacità di blocco, messa in quarantena o risposta
- Funziona al meglio se usato in combinazione con soluzioni di indagine e risposta proattive come XDR o SOAR

- Mantenere una piattaforma SOAR ben configurata che si integra con gli strumenti dei partner richiede l'impegno continuo di un SOC maturo e altamente qualificato
- Senza una manutenzione così qualificata e attenta, gli analisti SOAR possono ritrovarsi con troppi alert a bassa priorità, falsi positivi e un set di dati generalmente incoerente come risultato di tutti i vari strumenti isolati che forniscono dati alla piattaforma: esattamente quello che stavano cercando di evitare

Come giustificare l'investimento nell'XDR

Oltre ai vantaggi tecnici, ci sono valide ragioni commerciali per investire nell'XDR, come quelle correlate alla mitigazione degli attacchi, al rilevamento delle minacce interne, al cloud e alla conformità, all'investigation e response agli incidenti e molto altro.

Mitigazione degli attacchi

Nel caso di un'organizzazione che è stata vittima di un attacco ransomware con il conseguente criptaggio dei dati critici e l'arresto delle operazioni, le funzionalità di threat detection proattiva di XDR avrebbero potuto contribuire a identificare e prevenire questo tipo di attacco prima che creasse scompiglio, grazie alla capacità di rilevare comportamenti sospetti, isolare gli endpoint infetti e fornire una risposta agli incidenti in tempo reale, riducendo notevolmente l'impatto dell'attacco e ripristinando rapidamente la continuità aziendale.

Rilevamento delle minacce interne

Le minacce interne, che siano deliberate o meno, sono tra le preoccupazioni principali di quasi tutte le organizzazioni. Ma offrendo la massima visibilità su endpoint, reti, applicazioni e cloud, XDR è in grado di rilevare i segnali che indicano la presenza di minacce interne come comportamenti anomali degli utenti, tentativi di esfiltrazione dei dati e accesso non autorizzato. Inoltre, mettendo in correlazione e analizzando i dati provenienti da più fonti, XDR aiuta a identificare e mitigare le minacce interne, a proteggere le informazioni sensibili e a mantenere l'integrità dei dati.

Cloud e conformità

Mentre sempre più organizzazioni adottano le tecnologie cloud, garantire la conformità e una solida protezione sta diventando fondamentale. Fornendo una visibilità e una threat detection unificate tra ambienti ibridi e multi-cloud, XDR consente alle organizzazioni di monitorare i workload nel cloud, rilevare gli errori di configurazione e identificare le attività sospette, mantenendo così un'infrastruttura cloud sicura e conforme e mitigando al tempo stesso i rischi associati agli attacchi basati su cloud.

Investigation e incident response

Risposte tempestive e investigazioni approfondite sono critiche nel ridurre al minimo i danni e prevenire incidenti futuri. XDR semplifica i processi di risposta agli incidenti automatizzando i flussi di lavoro di rilevamento delle minacce, classificazione degli alert e investigazione e fornendo ai team di sicurezza una visione completa degli incidenti in modo da rispondere in modo rapido ed efficace. Il risparmio di tempo e risorse risultante dalle capacità di risposta automatizzata di XDR ne fa un vero e proprio punto di svolta per la gestione degli incidenti.

Si integra con EPP, EDR, SIEM e molto altro

Avere la possibilità di impedire i tipi di minacce descritti in precedenza giustifica assolutamente l'investimento nell'XDR, mentre per gli utenti di EPP, EDR, SIEM e così via, XDR consolida le prestazioni di tutte queste soluzioni.

- In ambito EPP, XDR ottimizza le funzionalità di protezione degli endpoint fornendo threat detection avanzata, automazione della risposta e visibilità migliorata sugli ambienti cloud e di rete, rappresentando il passaggio logico successivo nelle roadmap per la sicurezza e consentendo alle organizzazioni di ottenere un livello superiore di protezione dalle minacce in continua evoluzione.
- In ambito EDR, XDR (che spesso si basa su EDR) estende le capacità della soluzione oltre le attività di detection e response focalizzate sugli endpoint, fornendo visibilità olistica nell'infrastruttura protetta, inclusi rete, macchine virtuali, applicazioni e ambienti cloud, e consentendo capacità di incident response più efficienti e threat hunting ottimizzato.
- In ambito SIEM, XDR integra la soluzione fornendo threat detection in tempo reale, capacità di risposta avanzate e visibilità e correlazione migliorate degli eventi di sicurezza tra endpoint, reti e cloud, assicurando risposte più rapide agli incidenti e tempi di indagine ridotti.

Per chi intende investire nella tecnologia XDR nell'immediato futuro, la semplicità d'uso è di gran lunga il vantaggio più importante percepito per l'organizzazione, sia che si pianifichi di integrare la tecnologia con gli strumenti di sicurezza esistenti o si definisca un'infrastruttura di un unico vendor pronta per l'XDR. Gli intervistati hanno anche indicato che altri investimenti a breve termine in soluzioni per unificare la detection e la response e migliorare la visibilità tra i prodotti/servizi di sicurezza potrebbero essere per Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Security Information and Event Management (SIEM) e threat intelligence.

CRA Business Intelligence, XDR Poised to Become a Force Multiplier for Threat Detection, marzo 2022

Gestione del più ampio panorama delle minacce

In molte aziende, gli analisti della sicurezza trascorrono più di metà del proprio tempo a occuparsi dei falsi positivi, invece di eseguire threat hunting e rispondere in modo proattivo, con un significativo aumento dei tempi di rilevamento

Threat intelligence

Per molte organizzazioni, e soprattutto quelle vulnerabili ad attacchi mirati e minacce APT, la threat intelligence è uno strumento fondamentale per la difesa proattiva dalle minacce. Se tuttavia gli usi e i vantaggi della threat intelligence sono molteplici, lo sono anche le sue fonti, il che significa che identificare la soluzione migliore per la propria organizzazione può essere una sfida in sé.

Oggi, in molte aziende, gli analisti della sicurezza trascorrono più di metà del proprio tempo a occuparsi dei falsi positivi, invece di eseguire threat hunting e rispondere in modo proattivo, con un significativo aumento dei tempi di rilevamento. Fornire informazioni sulle minacce irrilevanti o imprecise per le operazioni di sicurezza farà aumentare ulteriormente il numero di falsi alert, con un impatto notevolmente negativo sia sulle capacità di risposta che sulla sicurezza complessiva. Come si può evitare questa situazione?

Sebbene non esistano criteri universalmente condivisi per valutare le offerte commerciali di threat intelligence, gli aspetti da tenere in considerazione sono:

- Nell'ampia rosa di provider tra cui scegliere, le organizzazioni dovrebbero cercare una threat intelligence che consenta di avere una visione più dettagliata del panorama specifico delle minacce, ad esempio attraverso un'analisi approfondita delle minacce passate ed emergenti che colpiscono il loro particolare settore, area geografica o singola attività, per migliorare le prestazioni di funzioni quali la gestione delle vulnerabilità, il threat hunting, l'incident response e molto altro.
- Per combinare in modo efficace la threat intelligence con i processi, i controlli e gli strumenti di sicurezza che un'organizzazione utilizza e conosce già, vanno cercati metodi di distribuzione, meccanismi di integrazione e formati che supportino la perfetta integrazione della threat intelligence con le attività di sicurezza già esistenti.
- È anche importante identificare una threat intelligence con portata globale. Poiché gli attacchi non hanno confini, il vendor raccoglie informazioni a livello globale e riunisce attività apparentemente disgiunte in campagne coerenti, dal momento che questo tipo di intelligence aiuterà a prendere misure più appropriate?
- Le organizzazioni alla ricerca di contenuti più strategici per definire la pianificazione della sicurezza a lungo termine dovrebbero cercare un provider di threat intelligence con una comprovata esperienza nell'individuazione e nelle indagini sulle minacce complesse nella loro area geografica e/o settore specifico.
- Anche la capacità del provider di adattare le proprie capacità di ricerca alle specifiche dell'organizzazione è fondamentale.

La threat intelligence (TI) è una risorsa in continua evoluzione. Perché sia efficace, inoltre, devono esserlo anche i programmi di threat intelligence interni che la utilizzano. Stabilite un benchmark per le vostre prestazioni attuali con il nostro strumento di valutazione TI interattivo per avere raccomandazioni di miglioramento personalizzate: https://go.kaspersky.com/ti_tool_2023.html

Inoltre, utilizzare Kaspersky Threat Intelligence Portal aiuta un'organizzazione ad aggregare, gestire e rendere operativa la threat intelligence, un aspetto fondamentale quando gli strumenti di sicurezza utilizzano informazioni provenienti da più origini. Nello specifico, Kaspersky Threat Intelligence Portal dovrebbe consentire all'organizzazione di:

- Rispondere alle minacce in modo più efficiente controllando ogni indicatore di minaccia considerato sospetto, che si tratti di un file, un hash di file, un indirizzo IP o un indirizzo Web.
- Analizzare i file per individuare le minacce comuni, elusive e APT avanzate.
- Inviare indirizzi IP, hash di file, domini o indirizzi Web considerati sospetti per convalidare e stabilire rapidamente la priorità di alert e incidenti utilizzando i livelli di rischio e supportando le informazioni contestualizzate per individuare le minacce reali.
- Ricevere report periodici sul comportamento di file o indirizzi Web specifici.
- Automatizzare i flussi di lavoro di sicurezza collegando le applicazioni rilevanti con Kaspersky Threat Intelligence Portal.

Security awareness

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani, anche perché, considerando che le soluzioni di cybersecurity si sviluppano e si adattano rapidamente alle minacce complesse, questo rende la vita più difficile per i cybercriminali che si rivolgono all'elemento più vulnerabile della cybersecurity, il fattore umano. Alcuni esempi dell'impatto che questo può avere sono che:

- Il 52% dei top manager afferma che i dipendenti rappresentano la più grande minaccia per la sicurezza operativa.
- Il 43% delle piccole aziende ha subito un incidente di sicurezza a causa di una violazione dei criteri di sicurezza IT da parte dei dipendenti.
- Il 60% dei dipendenti custodisce dati di natura riservata sul proprio dispositivo aziendale (dati finanziari, database di posta elettronica e così via).
- Il 30% dei dipendenti ammette di condividere con i colleghi i dati di accesso e le password del proprio PC di lavoro.

Una cultura di comportamenti informatici sicuri, basata su abilità e consapevolezza di cybersecurity diffuse in tutta l'azienda, è pertanto la chiave per ridurre la superficie d'attacco e il numero di incidenti che il team IT si trova a gestire.

Il contributo di Kaspersky

Kaspersky Next EDR Foundations

La potente protezione degli endpoint basata su tecniche di machine learning di Kaspersky Next EDR Foundations, i controlli di sicurezza flessibili e la root cause analysis EDR offrono alle organizzazioni il modo più semplice per costruire un nucleo solido per la cybersecurity. La semplicità della console, la distribuzione nel cloud o on-premises e un'ampia gamma di funzionalità che promuovono la qualità della vita lavorativa riducono la complessità e aumentano l'efficienza.

Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum assicura una solida soluzione di protezione degli endpoint, controlli ottimizzati, formazione, gestione patch e molto altro, il tutto supportato dalle funzionalità EDR essenziali. La visibilità delle minacce, l'indagine e la risposta sono semplici, rapide e guidate per consentire ai team IT e della sicurezza IT di vanificare gli attacchi velocemente e con l'impiego di risorse minime.

Kaspersky Next XDR Expert

Kaspersky Next XDR Expert si integra perfettamente con l'infrastruttura di sicurezza esistente di un'organizzazione, fornendo visibilità in tempo reale e informazioni approfondite sulle cyberminacce in evoluzione per offrire rilevamento avanzato delle minacce e azioni di risposta automatizzate, oltre alle funzionalità XDR essenziali descritte in questo e-book.

Kaspersky Managed Detection and Response

Kaspersky MDR fornisce una protezione avanzata e continuativa contro le minacce in grado di eludere le difese di sicurezza automatizzate, in costante aumento, e offre un valido aiuto alle aziende che faticano a trovare personale specializzato o possono contare solo su risorse interne limitate. Le sue eccellenti capacità di detection and response sono supportate da uno dei migliori team di threat hunting del settore. A differenza di offerte simili, Kaspersky MDR si avvale di modelli di ML brevettati, di un'esclusiva threat intelligence (TI) e di comprovata esperienza nella ricerca di attacchi mirati. Rafforza automaticamente la resilienza aziendale alle cyberminacce, ottimizzando le risorse esistenti e i futuri investimenti in sicurezza IT.

Kaspersky Threat Intelligence

Il portfolio di TI di Kaspersky copre una gamma completa di scenari di sicurezza, tra cui prevenzione, rilevamento, indagini, risposta e report strategici, tutti personalizzabili in base alle esigenze delle singole organizzazioni. Il nostro Global Research and Analysis Team (GReAT) è un gruppo d'élite di esperti che, riuscendo a introdursi con successo nelle community chiuse e nei forum underground di tutto il mondo, ha scoperto e analizzato oltre 50 dei più sofisticati attacchi mirati al mondo. Le nostre conoscenze, esperienze e informazioni approfondite su ogni aspetto della cybersecurity hanno fatto di noi uno dei partner di fiducia delle più importanti agenzie governative e forze dell'ordine, comprese Interpol e i principali CERT.

Esempi dei nostri servizi e soluzioni TI innovativi includono oltre 20 tipi di feed di dati sulle minacce, un'ampia gamma di report TI, una sandbox sviluppata internamente per rilevare minacce sofisticate ed elusive, un Threat Intelligence Portal aperto e servizi quali analisi del panorama delle minacce specifico per il cliente, oltre a Kaspersky Digital Footprint Intelligence, che analizza i dati sul footprint digitale per identificare potenziali minacce e vulnerabilità.

Kaspersky Security Awareness

Kaspersky Security Awareness offre una gamma di soluzioni di formazione altamente coinvolgenti ed efficaci, che aumentano la consapevolezza della cybersecurity del personale a tutti i livelli, in modo che contribuiscano alla sicurezza informatica dell'azienda. Poiché le modifiche comportamentali sostenibili richiedono tempo, il nostro approccio si basa sulla creazione di un ciclo di apprendimento continuo che include più componenti, tra cui simulazioni di protezione interattive per un'ampia gamma di scenari specifici di settore, strumenti di valutazione sotto forma di gioco, una piattaforma Automated Security Awareness con campagne di phishing simulate, formazione per i top manager e molto altro.

Kaspersky Professional Services

Il portfolio di Kaspersky Professional Services di servizi di valutazione, implementazione, manutenzione e ottimizzazione aiuta le organizzazioni a soddisfare le specifiche esigenze, ridurre al minimo i rischi di sicurezza, massimizzare il ritorno sugli investimenti, minimizzare il carico sulle risorse, rispondere rapidamente alle nuove minacce alla sicurezza e trarre il massimo vantaggio dalle soluzioni Kaspersky.

Fiducia

Proven. Transparent. Independent.

Nel 2017 Kaspersky ha lanciato la Global Transparency Initiative. Questo significa che, a differenza di quanto accade con altri vendor simili, in caso di dubbi sui nostri prodotti chiunque può esaminare liberamente il nostro codice sorgente, gli aggiornamenti software e le regole di rilevamento delle minacce, oltre che i nostri processi per la sicurezza in tutto il ciclo di vita di sviluppo e le strategie di mitigazione dei rischi per il software e la supply chain. A supporto di questa iniziativa abbiamo aperto più di dieci Transparency Center in tutto il mondo, che hanno ricevuto la visita di autorità di controllo, provider di infrastrutture critiche, clienti, partner, media e molto altro. E per i clienti che lo richiedono, siamo conformi allo standard SOC2 e certificati ISO/IEC 27001.

Kaspersky Next EDR Foundations — Per saperne di più

Kaspersky Next EDR Optimum — Per saperne di più

Kaspersky Next XDR Expert — Per saperne di più

Novità sulle minacce informatiche: securelist.com
IT Security News: kaspersky.it/blog/category/business
Sicurezza IT per PMI: kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security

kaspersky.it

Scoprite di più su Kaspersky Next all'indirizzo: https://go.kaspersky.com/next

Scegliete il livello più adatto alle vostre esigenze partecipando a un breve sondaggio nel nostro strumento interattivo: https://go.kaspersky.com/Kaspersky_Next_Tool