

Guida all'acquisto

Guida all'acquisto di una soluzione di Extended Detection and Response

Che cos'è l'XDR e in che modo può rafforzare la sicurezza aziendale?

Rene Holt



Digital Security
Progress. Protected.

Marzo 2023



Digital Security
Progress. Protected.

© 1992–2023 ESET, spol. s r.o. – All rights reserved.
Tutti i marchi commerciali qui utilizzati sono marchi
commerciali o marchi registrati di proprietà di ESET,
spol. s r.o. o ESET North America. Tutti gli altri nomi e
marchi sono marchi registrati delle rispettive società.

Contenuti

Introduzione	4
Capitolo 1: Minacce attuali	6
La caduta dei ransomware e l'ascesa dei wipers	6
Violazione degli strumenti di gestione IT	7
Fuga di dati sensibili aziendali	7
Attacchi alla catena di approvvigionamento e rischi di terzi parti	8
Capitolo 2: Che cos'è l'XDR?	9
Previsioni di mercato	9
Definizione	9
EDR e sicurezza degli endpoint	9
XDR vs. EDR	10
MDR vs. XDR	11
Capitolo 3: Quali sono i vantaggi dell'XDR?	12
Vantaggi principali	12
Capitolo 4: Cosa ricercare in una soluzione XDR	14
Capitolo 5: La proposta XDR di ESET	19
ESET fa la differenza	19
Vantaggi della soluzione XDR di ESET	20
Distribuzione di una soluzione XDR: Uno scenario di vita reale	22
Il cliente	22
La sfida	22
La soluzione	23
Che cos'è l'MDR?	24
Quali sono i vantaggi del servizio MDR di ESET?	24
ESET leader 2023 nel settore MDR	24
Conclusione	26
Informazioni su ESET	28

Introduzione

Se sei il responsabile della sicurezza informatica della tua azienda, questa guida sulle soluzioni XDR (Extended Detection and Response) ha un duplice scopo.

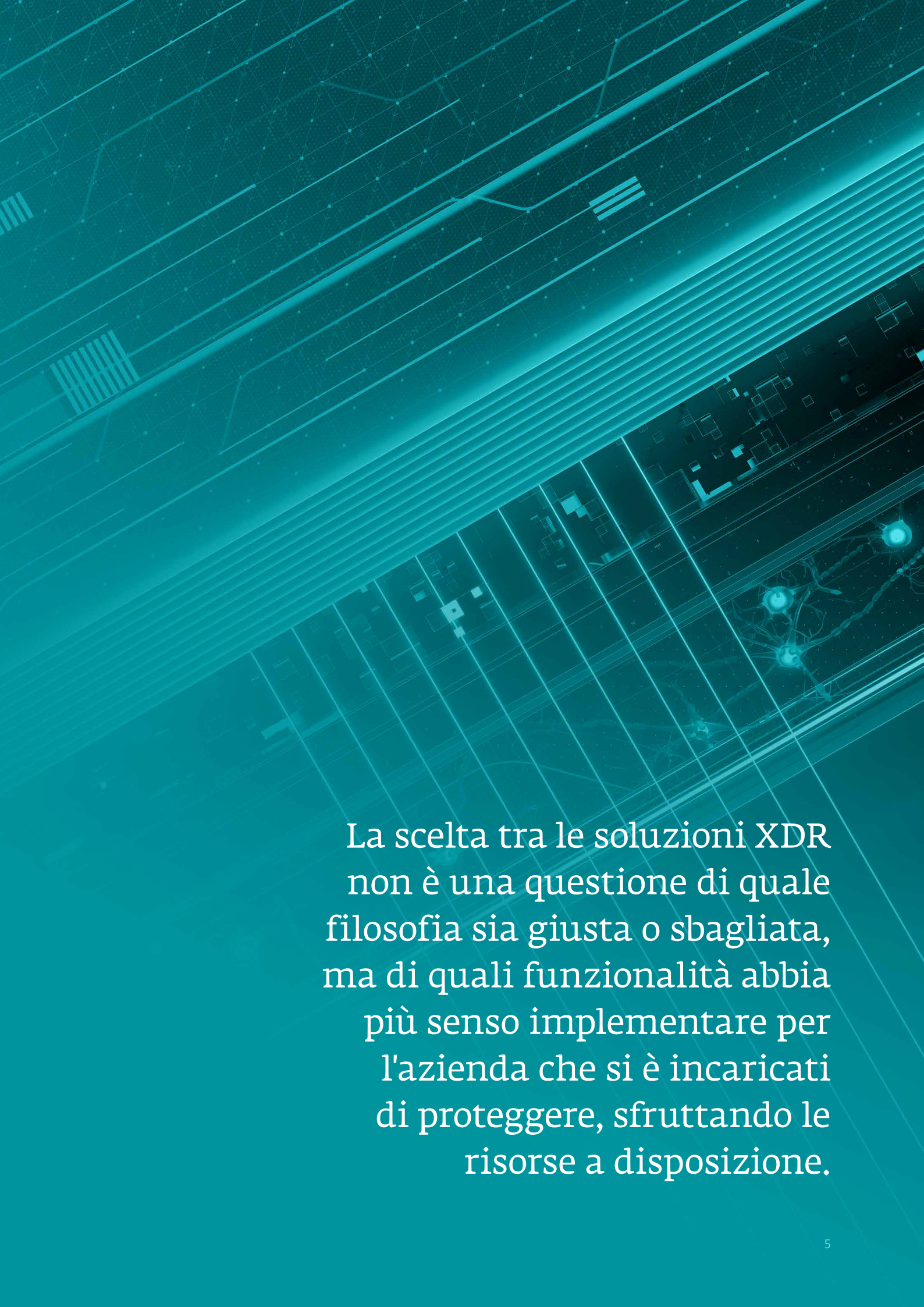
- **In primo luogo, capire come una soluzione XDR possa migliorare la sicurezza dell'azienda.**
- **In secondo luogo, presentare le caratteristiche di una soluzione XDR che valga la pena prendere in considerazione nella decisione di acquisto.**

La prima domanda da porsi prima dell'acquisto di una soluzione XDR è: Ne ho bisogno? I fattori che potrebbero innescare questa esigenza sono molteplici: l'aumento dei ransomware, il rischio di attacchi alla catena di fornitura, il continuo sfruttamento degli strumenti di gestione IT da parte degli aggressori, i requisiti normativi e assicurativi.

La scelta tra le soluzioni XDR non è una questione di quale filosofia sia giusta o sbagliata, ma di quali funzionalità abbia più senso implementare per l'azienda che si è incaricati di proteggere, sfruttando le risorse a disposizione.

I vendor hanno il dovere di presentare le proprie soluzioni in maniera chiara e trasparente, dando la possibilità di prendere una decisione basata su una visione accurata del servizio XDR proposto da ciascuno. Al termine di questa guida, speriamo di aver trasmesso almeno un messaggio significativo: il nostro componente abilitante XDR, ESET Inspect, restituisce all'organizzazione un maggior controllo sulla propria infrastruttura IT aziendale.

ESET Inspect fornisce agli esperti IT uno strumento tanto potente da raccogliere le informazioni necessarie a prendere decisioni in tutta tranquillità. I benefici combinati per la difesa includono una migliore valutazione del rischio, una riduzione delle spese per la sicurezza a lungo termine, una semplificazione dei processi di sicurezza e tempi più brevi per rilevare, identificare e risolvere le minacce.



La scelta tra le soluzioni XDR non è una questione di quale filosofia sia giusta o sbagliata, ma di quali funzionalità abbia più senso implementare per l'azienda che si è incaricati di proteggere, sfruttando le risorse a disposizione.

Capitolo 1: Minacce attuali

La guerra informatica tra difensori e nemici è una lotta senza fine.

Dal 2021 al 2022, la telemetria di ESET¹ ha registrato un aumento del 13% nel numero totale di minacce rilevate.

Sebbene la sicurezza degli endpoint sia stata un elemento indispensabile in questa lotta, alcune minacce sembrano sfidare anche questa protezione, soprattutto quando i sistemi rimangono esposti con falle nella sicurezza.

Per capire meglio come l'XDR può aiutare ad affrontare queste pericolose minacce, ne esamineremo quattro: ransomware e wipers, sfruttamento degli strumenti di gestione IT, fuga di dati sensibili aziendali e attacchi alla catena di approvvigionamento. Anche se queste non sono le uniche minacce che l'XDR aiuta ad affrontare, rappresentano sfide che possono essere particolarmente difficili da gestire.

LA CADUTA DEI RANSOMWARE E L'ASCESA DEI WIPERS

Nel 2022, la [telemetria di ESET](#) ha registrato una diminuzione dei ransomware e un [aumento dei wipers](#), in particolare in Ucraina. Questo calo è dovuto a un minor numero di attacchi ransomware? Oppure i potenziali attacchi ransomware sono stati individuati prima,

impedendo agli aggressori di avere l'opportunità di distribuire il ransomware?

Indipendentemente dalla risposta, i ransomware e i wipers sono un problema critico a causa dei danni catastrofici che potrebbero arrecare. Se gli autori del malware dovessero esfiltrare dei dati, possono anche tentare un doppio sfruttamento della vittima, promettendo di non far trapelare i dati se le richieste vengono soddisfatte. Anche se le probabilità sono basse, il danno potenziale è tanto significativo da giustificare un intenso controllo delle difese contro questo tipo di malware estremamente dannoso.

Un attacco sufficientemente sofisticato potrebbe sfruttare una lacuna o un punto debole nelle difese e quindi tentare di distribuire un ransomware o un wiper, eludendone il rilevamento. L'XDR può fornire ai difensori visibilità sulle fasi iniziali (e successive) di un attacco, aiutandoli a rilevare l'attacco prima di qualsiasi tentativo di distribuzione del malware. In altre parole, sfruttando l'XDR per la caccia alle minacce è possibile

ridurre significativamente il tempo di permanenza degli avversari nella rete.

VIOLAZIONE DEGLI STRUMENTI DI GESTIONE IT

Gli aggressori sono esperti nell'uso degli strumenti di gestione IT tanto quanto i difensori, il che significa che la violazione di questi strumenti può fornire una falsa idea di protezione. Alcuni degli strumenti utilizzati dagli aggressori sono [PowerShell](#), [certutil](#), [PsExec](#) e [SDelete](#).

Ad esempio, [LookingFrog](#), un gruppo di Hacker noto per aver preso di mira missioni diplomatiche, organizzazioni caritatevoli e aziende di produzione industriale, ha utilizzato [certutil](#) per fornire una shell web. [Agrius](#) - noto per aver preso di mira aziende di risorse umane, società di consulenza informatica, grossisti di diamanti e gioiellerie - ha utilizzato PsExec per eseguire il wiper Fantasy tramite un file batch di Windows. [NikoWiper](#), basato sullo strumento SDelete, un'utilità utilizzata per l'eliminazione sicura dei file, è stato rilevato in un'azienda del settore energetico ucraino.

Gli strumenti utilizzati dagli esperti IT hanno funzionalità che, nelle mani sbagliate, possono essere sfruttate per scaricare malware, riconfigurare i sistemi, disattivare le impostazioni di sicurezza, eseguire ricognizioni e persino distruggere i dati. Poiché questi strumenti sono considerati legittimi, il software di sicurezza degli endpoint è limitato nella

sua capacità di distinguere tra un uso corretto e una violazione.

Tuttavia, con l'XDR è possibile monitorare l'utilizzo degli strumenti di gestione IT e avvisare gli esperti IT in caso di azioni sospette o potenzialmente pericolose.

FUGA DI DATI SENSIBILI AZIENDALI

I ricercatori di ESET hanno [scoperto](#) con loro sorpresa che alcuni core router acquistati nel secondary market contenevano informazioni sensibili relative al loro precedente impiego nelle reti aziendali. Questo dato è sorprendente perché si suppone che le grandi organizzazioni abbiano a disposizione i processi e il personale per garantire che i dispositivi vengano ripuliti in modo sicuro prima di essere rivenduti.

Considerando che tali dispositivi hanno un costo piuttosto accessibile per gli aggressori, qualsiasi dato sensibile rimasto potrebbe dare una spinta ai progetti di violazione di tali reti.

Di fronte a una simile eventualità, si possono adottare almeno due misure. Per prima cosa, eliminare le chiavi crittografiche eventualmente memorizzate sui dispositivi rivenduti, in modo che non possano essere utilizzate per ottenere un accesso non autorizzato alla rete. In secondo luogo, dotarsi di una soluzione XDR per scovare gli aggressori che sfruttano i dati sensibili aziendali sulla rete.

ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO E RISCHI DI TERZI PARTI

Naturalmente, le aziende si affidano ai loro fornitori di software affinché gli aggiornamenti non si rivelino essere dei trojan. Gli aggressori che colpiscono gli sviluppatori di software possono sfruttare questa fiducia per ottenere l'accesso iniziale agli ambienti dei clienti.

In una [campagna Agrius](#), ad esempio, i server di aggiornamento di uno sviluppatore di software israeliano per l'industria dei diamanti sono stati compromessi e utilizzati per inviare ai clienti un aggiornamento dannoso contenente il wiper Fantasy.

Interessante è il caso di una [campagna Tick](#), in cui gli aggressori hanno

compromesso i server di aggiornamento di un'azienda di data-loss prevention per spostarsi lateralmente sulla rete, piuttosto che per eseguire un attacco alla catena di fornitura contro clienti esterni.

In un ulteriore colpo di scena di questa campagna Tick, gli installer affetti da trojan per Q-Dir - un file explorer multipane per Windows - sono stati trasferiti tramite strumenti di supporto remoto ai clienti dell'azienda compromessa, probabilmente durante le sessioni di supporto tecnico.

L'XDR è importante per contrastare minacce come queste perché può avvisare gli esperti di attività dannose in seguito allo sfruttamento di un rapporto di fiducia con un fornitore di software o un'altra terza parte.

I ransomware e i wipers sono un problema critico a causa dei danni catastrofici che potrebbero causare. Se gli autori del malware dovessero esfiltrare dei dati, possono anche tentare un doppio sfruttamento della vittima, promettendo di non far trapelare i dati se le richieste vengono soddisfatte.

Capitolo 2: Che cos'è l'XDR?

Dopo aver considerato alcune delle minacce che le organizzazioni devono affrontare e il ruolo dell'XDR nel rilevarle, diamo un rapido sguardo al mercato dell'XDR.

PREVISIONI DI MERCATO

Secondo [Gartner](#), se nel 2022 meno del 5% delle organizzazioni utilizzava un XDR, entro la fine del 2027 si prevede che oltre il 40% adotterà questa tecnologia. Si tratta di una crescita incredibile! Un'altra società di analisi, IDC, ha previsto una spinta altrettanto incredibile, ma a livello di fatturato. Un [rapporto IDC](#) del marzo 2022 prevedeva che il fatturato mondiale dell'XDR cloud-native avrebbe registrato un tasso di crescita annuale composto del 69,5% dal 2021 al 2026.

Mentre le organizzazioni cercano di migliorare le loro strategie contro gli avversari, l'XDR si è chiaramente imposto come soluzione di riferimento.

DEFINIZIONE

Come accennato nell'introduzione, l'XDR e i termini correlati, come endpoint detection and response (EDR) e managed detection and response (MDR), hanno definizioni diverse a seconda dei fornitori. A causa di una comprensione ambigua di questi termini, non è raro che vengano espresse critiche basate su diverse

definizioni, aspettative ed esperienze.

Una probabile fonte di confusione è il fatto che molti fornitori si avvicinano all'XDR da aree di competenza diverse. Per ESET, il viaggio è iniziato oltre trent'anni fa con la ricerca sulle minacce informatiche e lo sviluppo di software per la sicurezza degli endpoint, per poi passare all'EDR e ora all'XDR. Altri fornitori potrebbero avvicinarsi all'XDR con un'esperienza in security analytics o piattaforme di threat intelligence nel loro curriculum.

Forniremo di seguito una spiegazione rapida e basilare di come ESET intende questi termini.

EDR E SICUREZZA DEGLI ENDPOINT

Per proteggere i dispositivi, la sicurezza degli endpoint si avvale di tecnologie a più livelli, ognuno dei quali è stato messo a punto per rilevare e bloccare automaticamente le minacce. Per l'amministratore IT, l'esperienza con la sicurezza degli endpoint è in gran parte passiva e automatizzata. In un certo senso, questo è vantaggioso perché

l'amministratore IT non è gravato da problemi di sicurezza che vengono prontamente affrontati.

D'altro canto, al responsabile IT vengono solitamente fornite poche informazioni sul motivo per cui vengono rilevate determinate minacce, ovvero se non vi sia una causa sottostante più profonda dei sintomi rilevati. Una soluzione EDR offre all'amministratore IT una visibilità di tutti gli eventi che si verificano sugli endpoint, consentendo così di effettuare una diagnosi dei sintomi.

Una soluzione EDR può rilevare eventi specifici, o sequenze di eventi, che sono sospetti o necessitano di essere monitorati. I rilevamenti vengono attivati da un motore che analizza questi eventi e avvisa l'amministratore quando si verifica una corrispondenza comportamentale. Inoltre, l'EDR mette a disposizione degli esperti azioni di risposta, come l'eliminazione di un processo, l'isolamento di un computer dalla rete, il blocco di un eseguibile e così via.

In breve, l'EDR richiede un [approccio pratico e attivo alla sicurezza](#), perché consente ai difensori di monitorare e analizzare gli eventi low-level per individuare eventuali tecniche di attacco. Con l'EDR è più facile adottare anche altre misure proattive, come la simulazione degli avversari e l'attività di threat hunting.

XDR VS. EDR

Se una soluzione EDR è in grado di acquisire dati da altri dispositivi e fonti, come dispositivi di rete e servizi cloud,

Che cos'è l'EDR?

Tecnologia di rilevamento, investigazione e risposta che raccoglie dati di telemetria rilevanti per la sicurezza dagli endpoint, esegue il rilevamento delle anomalie, consente agli analisti di investigare a partire dalla telemetria raccolta e facilita la risposta da parte degli analisti sugli endpoint interessati.

Fonte: *Forrester, 2021*

allora è XDR. In altre parole, "extended" si riferisce a dati che vanno oltre gli endpoint. L'evoluzione dell'EDR in XDR richiede una maggiore integrazione con le soluzioni di sicurezza del fornitore e forse anche di terzi.

Una sfida che incentiva la crescita dell'XDR è la fatica causata da una molteplicità di strumenti, ognuno dei quali fornisce solo una visione frammentaria della sicurezza di un'organizzazione. Se più tipi di dati possono essere inseriti in un motore di rilevamento e forniti agli esperti di sicurezza in modo convincente e facile da capire, si ottiene una visione più ampia della sicurezza dell'organizzazione. A sua volta, questo può portare a una risposta più efficiente agli incidenti e a una maggiore automazione.

Tuttavia, l'acquisizione di questa visione d'insieme potrebbe non essere sempre vantaggiosa dal punto di vista dell'individuazione delle minacce, se i dati

Che cos'è l'XDR?

L'XDR è un'evoluzione dell'EDR, che ottimizza il rilevamento, l'indagine, la risposta e l'individuazione delle minacce in tempo reale. L'XDR integra i dati relativi alla sicurezza degli endpoint con la telemetria proveniente da strumenti di sicurezza aziendali come l'analisi e la visibilità della rete (NAV), la sicurezza delle e-mail, la gestione delle identità e degli accessi, la sicurezza del cloud e altro ancora. Si tratta di una piattaforma cloud-native costruita su un'infrastruttura di big data per offrire ai team di sicurezza flessibilità, scalabilità e opportunità di automazione.

Fonte: [Forrester, 2021](#)

provengono dall'esterno. Poiché le fonti di dati del fornitore sono in genere più ricche e standardizzate rispetto ai dati di terze parti, una maggiore integrazione con le

soluzioni del fornitore (definita anche XDR nativa) offre di solito un aiuto maggiore nella ricerca e nella risposta agli attacchi.

MDR VS. XDR

Poiché l'XDR è più efficace se gestito da personale altamente qualificato che ha tempo da dedicare al suo funzionamento, l'esternalizzazione della gestione dell'XDR può essere un'opzione preferibile. Come suggerisce il nome, MDR è un servizio di sicurezza che combina XDR con esperti di cybersecurity e altri servizi aggiuntivi offerti dal fornitore o da terze parti. Alcuni usano addirittura il termine MxDR per differenziarsi dal "vecchio" significato di MDR che faceva riferimento all'EDR.

L'MDR può aiutare le organizzazioni a superare alcune criticità per compiere il passaggio verso l'XDR che altrimenti non sarebbe possibile. Tali sfide includono la criticità nella gestione degli alert, la difficoltà di trovare e assumere personale di sicurezza di talento o esperto, i costi di gestione di un centro operativo di sicurezza interno e la richiesta di tempo per stare al passo con minacce in rapida evoluzione.

Possibili problemi legati alla funzionalità dell'XDR



Complessità dello strumento



Avviso di sovraccarico dello strumento



Mancanza di risorse IT qualificate



Tempo limitato per il monitoraggio delle minacce nell'XDR

Capitolo 3: Quali sono i vantaggi dell'XDR?

Sebbene il monitoraggio degli eventi low-level sugli endpoint possa sembrare interessante per gli analisti della sicurezza, facciamo un passo indietro e consideriamo i vantaggi per la sicurezza della vostra azienda. Il rilevamento di eventi sospetti può effettivamente migliorare le vostre difese?

VANTAGGI PRINCIPALI

Le organizzazioni che utilizzano soluzioni XDR per la prima volta potrebbero restare sorpresi da tutti gli eventi che attivano i rilevamenti. Può essere un momento di svolta per mettere in luce una serie di sistemi mal configurati, vulnerabilità o minacce. L'implementazione iniziale di una soluzione XDR può quindi portare rapidamente a un paio di vantaggi: la scoperta di pratiche di cyber-igiene inadeguate all'interno dell'organizzazione e la presenza di minacce in agguato nella rete.

Nel Capitolo 1 abbiamo preso in considerazione una serie di minacce contro le quali le organizzazioni potrebbero essere difficilmente in grado di difendersi senza l'XDR, il che significa che con l'XDR si ottengono i seguenti

vantaggi: maggiore sicurezza nel rilevare ransomware, wipers e attacchi alla catena di distribuzione e scoprire gli aggressori che sfruttano gli strumenti di gestione IT o i dati sensibili aziendali, magari sottratti da dispositivi dismessi.

Grazie alla visibilità garantita sugli eventi low-level, un altro vantaggio dell'XDR è che i responsabili IT possono testare la loro copertura dalle tattiche e dalle tecniche avversarie descritte nella [knowledge base MITRE ATT&CK®](#). Naturalmente, spesso esistono più modi per eseguire una tecnica, non tutti registrati in ATT&CK. Tuttavia, quelle registrate servono come indicazioni utili per scoprire i punti deboli e le lacune dei sistemi di difesa. Per facilitare l'emulazione degli avversari, le soluzioni XDR fanno riferimento alle tecniche ATT&CK per i rilevamenti.

Un altro vantaggio dell'XDR è il rilevamento delle minacce. Il flusso di notizie sulla sicurezza informatica rivelano spesso attacchi in corso, a volte su larga scala. Con i responsabili IT che agiscono sulle loro console per verificare gli attacchi appena segnalati e mettere a punto le adeguate difese, XDR offre il vantaggio di poter scrivere regole di threat hunting che effettuano ricerche su potenziali segni di compromissione.

Una volta scoperta una minaccia, l'XDR offre varie opzioni di intervento. Per ridurre il tempo medio di risposta alle minacce, l'XDR può attivare automaticamente le azioni di risposta.

Chi risponde agli incidenti è anche interessato a risalire agli attacchi fino al primo accesso. Poiché l'XDR tiene traccia dell'alberatura dei processi ed è in grado di correlare gli eventi, gli esperti sono in una posizione migliore per scoprire il vettore di attacco iniziale. Questa capacità è particolarmente importante per mitigare gli attacchi che iniziano con lo sfruttamento di una vulnerabilità zero-day o ancora senza patch, gli attacchi alla catena di approvvigionamento e le minacce interne.

L'XDR facilita anche la cooperazione tra gli esperti, incorporando funzioni di collaborazione ispirate alle piattaforme di risposta agli attacchi.

Il valore di una soluzione XDR

A partire dal 2023, IDC prevede che i vendor di soluzioni XDR saranno sempre più in grado di dimostrare in modo tangibile il valore reale di questa soluzione. La dimostrazione di tale valore consentirà di: migliorare la comprensione del rischio informatico da parte delle organizzazioni e i percorsi per ridurlo strutturalmente, migliorare le metriche di performance (ad esempio, il tempo medio di rilevamento, indagine e risposta) e ridurre l'impatto della dispersione tecnologica in termini di cybersecurity sulle spese complessive per la sicurezza e sulla complessità generale.

Fonte: IDC, *Worldwide Modern Endpoint Security Market Shares, luglio 2021-giugno 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth, Doc # US49982022, gennaio 2023*

Capitolo 4: Cosa ricercare in una soluzione XDR

Questo capitolo illustra ai potenziali acquirenti di una soluzione XDR i nove criteri da considerare prima dell'acquisto.



RILEVAMENTO

Per rilevare gli attacchi, l'XDR monitora gli eventi. Alcuni eventi possono, a seconda delle circostanze, indicare un intento malevolo o essere semplicemente un'attività innocua. Questa duplice natura comporta una maggiore possibilità di falsi positivi. Pertanto, una soluzione XDR dovrebbe essere dotata di un motore di rilevamento ben testato nella sua configurazione predefinita per ridurre al minimo i falsi positivi.

La strategia adottata da una soluzione XDR per ridurre al minimo i falsi positivi richiede un delicato equilibrio tra i criteri di security che vengono abilitati. A volte è meglio per un particolare ambiente non avere una regola XDR abilitata per gli eventi che sono frequentemente generati e osservati negli attacchi, ma affidarsi invece al rilevamento dell'attacco con un altro evento. L'attacco viene comunque rilevato, anche se l'utente potrebbe non essere stato avvisato di ogni fase. Ciò significa che non tutte le soluzioni XDR monitorano necessariamente gli stessi eventi per rilevare lo stesso attacco.

Un'ulteriore complicazione è rappresentata dal fatto che la frequenza

di un evento è influenzata dall'uso di particolari sistemi, applicazioni o strumenti in un'organizzazione. Ciò che è comune per un'organizzazione può non esserlo per un'altra. Lo stesso vale per i ruoli lavorativi all'interno di un'azienda.

Un'altra considerazione è che un numero eccessivo di rilevamenti di falsi positivi causa un affaticamento in termine di gestione, richiedendo l'ottimizzazione della soluzione XDR dopo l'implementazione iniziale. Se la tua organizzazione non è in grado di effettuare l'ottimizzazione iniziale, cerca un fornitore di soluzioni XDR che offra questo servizio.

Qualsiasi rilevamento deve offrire un contesto, come le possibili cause dannose e benigne, una stima della gravità e informazioni sugli eventi che lo hanno innescato. Dopotutto, l'XDR è stato progettato per aiutare il lavoro investigativo dei degli esperti di cybersecurity.

Infine, è necessario esaminare le fonti di rilevamento: questo aspetto influisce in modo critico sulla capacità di una soluzione XDR di rilevare le minacce.

Una soluzione XDR monitora gli eventi low-level, tra cui:

- Richieste HTTP
- Connessioni TCP/IP
- Richieste DNS Code injection
- Modifica ai valori di registro
- Chiavi di registro eliminate
- Operazioni sui file
- Chiamate API di Windows
- Eventi WMI
- Script
- Caricamento DLL
- Caricamento driver
- Caricamento del modulo del kernel
- Rilascio di eseguibili
- Creazione di named pipe
- Eventi nell'account utente
- Rilevamenti di sicurezza degli endpoint

I dati di telemetria includono rilevamenti dal monitoraggio delle API, dalla scansione della memoria, dagli script esposti da Windows Antimalware Scan Interface (AMSI) o anche dall'analisi dei contenuti del traffico di rete? Le fonti di rilevamento dovrebbero essere incrociate per garantire la sicurezza.



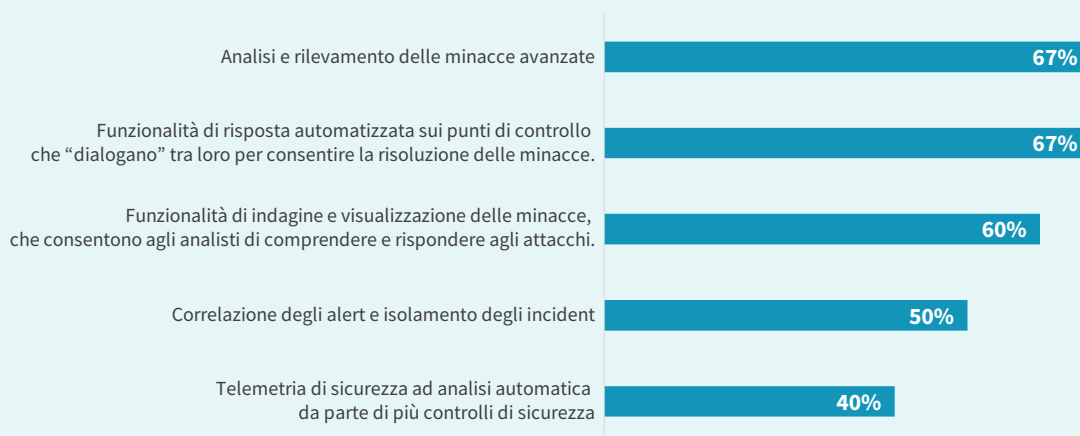
RISCONTRO

L'XDR dovrebbe presentare quali sono le fasi di indagine consigliate, quali le azioni di remediation da attuare e quali le risposte agli incident. Tali azioni possono comprendere il blocco dell'esecuzione di file eseguibili e del caricamento di librerie di collegamento dinamico (DLL), lo spegnimento o il riavvio del computer, il logout forzato, l'isolamento del computer, l'eliminazione dei processi e la pulizia dei file.

I potenziali acquirenti dovrebbero diffidare delle risposte automatiche troppo aggressive, che potrebbero compromettere il funzionamento dei sistemi nel loro ambiente. Una parte dei test sui falsi positivi per l'implementazione di una nuova regola dovrebbe includere la valutazione della gravità della minaccia associata al rilevamento e della probabilità che la causa sia dannosa prima di allegare risposte automatiche che bloccano l'esecuzione o bloccano un processo.

In un [sondaggio condotto nel 2022](#) tra le medie e grandi imprese del Nord America, i professionisti della cybersecurity hanno identificato il rilevamento e la risposta come le funzionalità più importanti di una soluzione XDR. (Si veda il grafico alla pagina successiva).

Quali sono le funzionalità essenziali che una soluzione XDR deve fornire perché la vostra organizzazione prenda in considerazione di dismettere la propria soluzione EDR? (Percentuale di intervistati, N=329, risposte multiple accettate)



Fonte: [Brief ESG: The Demise of EDR?, Aprile 2022, p. 2.](#)



EQUILIBRIO

Sebbene una maggiore visibilità degli eventi possa consentire di rilevare più fasi di un attacco, questa potrebbe rivelarsi un'arma a doppio taglio. È necessario avere una visione dettagliata per fermare un attacco, ma non così tanto da essere sopraffatti dai rilevamenti innescati dal normale comportamento dell'organizzazione.

Il ruolo di una soluzione XDR equilibrata non è quello di segnalare ogni singola procedura eseguita durante un attacco, ma piuttosto di avvisare che un attacco è in corso e di fornire assistenza nelle indagini.



TRASPARENZA

Alcuni fornitori di soluzioni XDR riducono la visibilità di analisi ai clienti in modo che gli esperti IT abbiano poca o nessuna visibilità su ciò che la soluzione sta monitorando. Sebbene non sia utilizzabile da tutte le organizzazioni, un set di regole

aperto consente al responsabile IT di visualizzare, controllare e analizzare gli eventi monitorati dalla soluzione XDR.



FLESSIBILITÀ

Una delle sfide dal punto di vista del rilevamento è rappresentata dai falsi positivi. Ma se il set di regole presente all'interno di una soluzione XDR è trasparente, gli esperti IT possono personalizzare la soluzione in base al proprio ambiente, riducendo così il numero di falsi positivi.

La personalizzazione è il cuore dell'ottimizzazione di una soluzione XDR, sia nella fase iniziale che in quelle successive. È utile prendere in considerazione una soluzione XDR che permetta di impostare esclusioni personalizzate, modificare le risposte automatiche con azioni diverse e stabilire le proprie regole. Ciò consente di utilizzare al meglio una soluzione XDR, ottimizzata in base a ciò che è "normale" in un dato ambiente.

In definitiva, è il personale IT dell'organizzazione ad essere nella posizione migliore per conoscere la configurazione più adatta per il motore XDR al fine di raggiungere l'equilibrio desiderato tra rischio e falsi allarmi.



INTEGRAZIONE

Una soluzione che si integri con i sistemi di sicurezza del fornitore e con quelle di terzi è una capacità cruciale per una soluzione XDR. L'integrazione comprende l'esportazione e l'importazione di dati nell'XDR, ad esempio tramite un'API (application programming interface). Verificate se è possibile esportare i rilevamenti per utilizzarli in un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) e importare gli hash dai feed di dati sulle minacce.

Per quanto riguarda le integrazioni native, molti fornitori offrono in genere sistemi di sicurezza degli endpoint e di reputazione e rilevamento basati sul cloud che, insieme, forniscono una capacità completa di prevenzione, rilevamento e risposta.

L'XDR si basa sulla protezione offerta dalla sicurezza degli endpoint e da altre soluzioni: non è una tecnologia a sé stante. Pertanto, è bene tenere presente che la qualità della telemetria degli endpoint generata dalle soluzioni dei diversi fornitori può variare. Le minacce bloccate dal software di sicurezza degli endpoint potrebbero essere un'occasione per approfondire le possibili cause con l'XDR e cercare modi per migliorare le difese.



COPERTURA MULTIPIATTAFORMA

Lato client, l'XDR dovrebbe supportare gli endpoint che eseguono i principali sistemi

operativi, come Windows, macOS e Linux. Con la copertura multiplatforma, è possibile tracciare più facilmente i movimenti laterali degli aggressori.

Lato server, l'acquisto e la manutenzione dell'hardware e del software necessari per gestire il server e il database sono costi potenzialmente proibitivi associati all'implementazione di una soluzione XDR. L'hardware deve essere in grado di gestire il numero abituale di eventi generati da tutti gli endpoint dell'organizzazione. Inoltre, se si desidera una maggiore visibilità, il costo dell'hardware potrebbe aumentare, perché l'archiviazione di molti eventi (soprattutto quelli generati di frequente) può diventare rapidamente un vero e proprio divoratore di risorse.

Se l'implementazione on-premise non è un'opzione possibile, cercate una soluzione XDR basata su cloud, in cui la responsabilità dell'hardware lato server è affidata al fornitore.



SERVIZI

L'investimento per una soluzione XDR non deve limitarsi al prodotto, ma deve includere anche i servizi. È importante accertarsi che il fornitore offra i seguenti servizi:

- **Servizi di implementazione e ottimizzazione**
- **Servizi di rilevamento e risposta gestiti, compresa la ricerca delle minacce.**
- **Controlli di sicurezza**
- **Un partner o un ufficio locale nella vostra zona**
- **Assistenza tecnica in lingua locale**



FORNITORE

Il valore dell'investimento nell'acquisto di una soluzione XDR dipende fortemente dalla stabilità e dalla reputazione del fornitore. È buona norma tenere in considerazione l'esperienza e la storicità del fornitore in materia di sicurezza, incluso l'intero portafoglio di prodotti e servizi offerti, la comprovata competenza nella prevenzione delle minacce, la capacità di intelligence sulle minacce e le ricerche pubblicate sulle minacce informatiche.

Inoltre, è bene esaminare le valutazioni di terze parti, come il [test Endpoint Prevention & Response \(EPR\)](#) di

AV-Comparatives. Questo test valuta la risposta di una soluzione XDR a diversi scenari di attacco in tre fasi: attacco iniziale, propagazione e violazione delle risorse.

Un'altra fonte indipendente è la [MITRE Engenuity ATT&CK® Evaluations](#) che mette a confronto le soluzioni XDR con note tecniche avversarie. Queste valutazioni indicano il livello di visibilità delle tecniche dannose e la completezza del contesto fornito da ciascun rilevamento. Va sottolineato che queste valutazioni non decretano una classifica finale, né testano i falsi positivi o l'impatto sulle prestazioni.

Una soluzione XDR offre numerosi vantaggi fra cui: maggiore sicurezza nel rilevare attacchi ransomware, wipers e alla catena di approvvigionamento, individuare gli aggressori che abusano degli strumenti di gestione IT o che sfruttano i dati sensibili aziendali, magari sottratti da dispositivi dismessi.

Capitolo 5: La proposta XDR di ESET

L'utilizzo di analisi comportamentali a livello di endpoint, rete, cloud, e-mail e altri livelli costituisce un quadro di riferimento per l'approccio e la metodologia di ESET.

Consente di individuare le attività sospette e di fermare gli aggressori prima che possano avere un impatto significativo sull'organizzazione. Per rendere possibile tutto ciò, ESET sfrutta le sue soluzioni tecnologiche leader del settore, come XDR.

[ESET Inspect](#), la nostra **soluzione che presenta la componente XDR**, offre ai team di sicurezza una straordinaria visibilità sulle minacce. Permette di eseguire un'analisi rapida e approfondita delle cause principali e di rispondere immediatamente agli incidenti. Abbinato alla comprovata potenza preventiva dei prodotti ESET per la protezione degli endpoint, ESET Inspect, il componente abilitante che consente l'attivazione dell'XDR, **in cloud**, è in grado di offrire:

- Individuazione delle APT (Advanced persistent threats)
- Protezione dagli attacchi fileless
- Blocco delle minacce "zero-day"
- Protezione contro ransomware
- Prevenzione contro le violazioni della politica di sicurezza aziendale

ESET FA LA DIFFERENZA

PREVENZIONE COMPLETA, RILEVAMENTO E RISPOSTA

ESET Inspect consente di analizzare e risolvere rapidamente qualsiasi problema di sicurezza nella rete. La sicurezza multilivello di ESET, in cui ogni singolo livello invia dati a ESET Inspect, analizza grandi quantità di dati in tempo reale per rilevare le minacce.

TUTTA L'ESPERIENZA DI UN LEADER DEL SETTORE

ESET da oltre 35 anni è impegnata nella lotta alle minacce informatiche. In qualità di azienda con una forte expertise tecnologica, è stata a lungo all'avanguardia nello sviluppo del machine learning, della tecnologia cloud e ora dello sviluppo di soluzioni XDR.

PREVENIRE È MEGLIO CHE CURARE

L'approccio di ESET nello sviluppare soluzioni XDR è strettamente connesso ai suoi pluripremiati prodotti di prevenzione. Grazie al nostro impegno nello sviluppo di tecnologie di rilevamento all'avanguardia, ESET è leader mondiale nel campo della prevention, detection and response.

VISIBILITÀ DI RETE DETTAGLIATA

Grazie a regole di rilevamento trasparenti (ESET Inspect ne ha più di 1250 e in continuo aumento), indicatori di compromissione (IoC) avanzati, capacità di ricerca, analisi approfondita di file eseguibili nella propria rete è possibile identificare qualsiasi elemento sospetto.

RISPOSTA IMMEDIATA

La soluzione di ESET è pronta all'uso ed è abbastanza potente da consentire modifiche granulari da parte di esperti.

FLESSIBILITÀ

Piena disponibilità di decidere come implementare la propria soluzione di sicurezza: ESET Inspect può essere eseguita tramite il proprio server in locale o sul cloud, consentendo di ottimizzare la configurazione in base agli obiettivi di TCO e alla capacità dell'hardware.

MITRE ATT&CK®

ESET Inspect fa riferimento ai rilevamenti framework MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) che in un click fornisce dati concreti anche su minacce molto complesse. ESET è una delle principali aziende indipendenti di software per la sicurezza informatica e rientra nella top 10 degli oltre 350 collaboratori di ATT&CK.

SISTEMA BASATO SULLA REPUTAZIONE

Il filtraggio esteso permette agli esperti di sicurezza di identificare ogni applicazione nota e affidabile, utilizzando il solido sistema di reputazione di ESET. Il sistema ESET contiene un database di centinaia di milioni di file non malevoli, usato per

permettere ai team di security di dedicare il tempo necessario ad analizzare file sconosciuti potenzialmente dannosi e non a falsi positivi.

AUTOMAZIONE E PERSONALIZZAZIONE

ESET Inspect permette di impostare facilmente i livelli di dettaglio e automazione sulla base delle proprie esigenze. Durante la configurazione iniziale, con l'aiuto di profili utente preimpostati, è possibile scegliere il livello di interazione desiderato e il tipo e la quantità di dati da archiviare, per poi lasciare che la Modalità di Apprendimento mappi l'ambiente dell'organizzazione e suggerisca esclusioni ai falsi positivi, dove necessario.

VANTAGGI DELLA SOLUZIONE XDR DI ESET

Oggi le aziende hanno bisogno di una maggiore visibilità sui loro endpoint, sui loro dispositivi e sulla loro rete per proteggere le minacce emergenti, i comportamenti rischiosi dei dipendenti e le applicazioni indesiderate. **ESET Inspect** è il componente della piattaforma ESET PROTECT **che consente l'attivazione dell'XDR in cloud**. Offre un rilevamento unico basato sul comportamento e sulla reputazione, completamente trasparente ai team di sicurezza, fornendo un feedback in tempo reale basato sulla threat intelligence fornita dal sistema di reputazione globale [ESET LiveGrid®](#). Optando per questa soluzione le organizzazioni potranno beneficiare di:

ESPERIENZA

Rilevamento e risposta da parte di un fornitore affidabile, che basa la propria attività su oltre 35 anni di esperienza all'avanguardia nella sicurezza digitale.

QUALITÀ

Strettamente integrato con i prodotti di prevenzione multilivello di ESET, basato su una tecnologia che ha vinto numerosi premi e che è riconosciuta a livello internazionale.

FLESSIBILITÀ

È facile da far funzionare, ma è sufficientemente potente per soddisfare

le esigenze di security di diverse organizzazioni, in quanto offre controlli granulari e si adatta in modo ottimale all'ambiente di ciascun utente.

TRASPARENZA

Regole di rilevamento trasparenti garantiscono una visibilità dettagliata su più livelli, tra cui e-mail, reti e server.

L'approccio e la metodologia di ESET consentono di individuare le attività sospette e di fermare gli aggressori prima che possano avere un impatto sui sistemi dell'organizzazione. Per rendere possibile tutto ciò, ESET sfrutta le sue soluzioni tecnologiche leader del settore, come l'XDR.

Distribuzione di una soluzione XDR: Uno scenario di vita reale

Il cliente

Il Gruppo Raicam è un'azienda automobilistica specializzata nella progettazione, nello sviluppo e nella produzione di freni, frizioni e attuatori. Raicam pone grande attenzione all'alta qualità e alla sicurezza dei prodotti e dei servizi che offre. Molti dei più noti costruttori di veicoli al mondo hanno scelto di lavorare con Raicam grazie alla qualità dei suoi prodotti.

La sfida

Con diverse sedi internazionali, Raicam aveva bisogno di una soluzione di cybersecurity in grado di fornire una copertura completa a livello globale, un sistema facile da gestire ma che garantisse un alto livello di protezione dai rischi digitali. Un altro fattore che ha spinto Raicam a prendere in considerazione una nuova soluzione è stata la necessità di un prodotto di protezione degli endpoint con **tecnologia XDR**, facile da integrare e con un basso consumo di risorse. L'obiettivo: una visione centralizzata da un'unica console, in cui gestire tutti i controlli di sicurezza senza aggiungere lavoro ai team interni.




La soluzione

Raicam ha affidato a **ESET** la sicurezza informatica dei suoi vari siti produttivi in Italia e all'estero. Ha adottato la [piattaforma ESET PROTECT](#), che incorpora diverse soluzioni sotto un'unica console di gestione, tra cui [ESET Inspect](#), la **soluzione che include la componente XDR**.

Grazie a questo approccio completo alla cybersecurity, gli endpoint e i server di Raicam sono protetti da attacchi ransomware, minacce

zero-day, violazioni dei dati e altro ancora, garantendo la continuità operativa e la salvaguardia dei dati aziendali sensibili. Il tutto con un'assistenza clienti, disponibile 24 ore su 24, 7 giorni su 7. L'adozione di una tecnologia tanto solida ha anche aiutato Raicam a soddisfare gli standard normativi.



"L'approccio multilivello alla sicurezza di ESET ci permette di rispondere positivamente alle verifiche di sicurezza richieste dai nostri clienti".

Antonella Bertola, Responsabile IS di Raicam

Che cos'è l'MDR?

È un servizio di **gestione della sicurezza** che combina strumenti, tecnologie ed esperti di cybersecurity per fornire alle organizzazioni potenti capacità di rilevamento e risposta.

L'MDR è di fatto una versione esternalizzata dell'extended detection and response (XDR), talvolta combinata con altri strumenti.

"I servizi MDR offrono già gran parte di ciò che l'XDR aspira a fare. L'MDR offre migliori risultati in termini di sicurezza fornendo strumenti e tecnologie quali threat intelligence, threat hunting, monitoraggio continuo 24 ore su 24, analisi avanzate, contenimento e rimozione di incidenti o violazioni in cui si sospetta o si è consapevoli dell'esfiltrazione e la distruzione dei dati."

Fonte: *IDC Global Security Products Analysis: From PowerPoint to Power Product, Where Is XDR Right Now?*, Doc # US47705821, 8 febbraio 2022, Ch. Kissel, M. Suby, F. Dickson

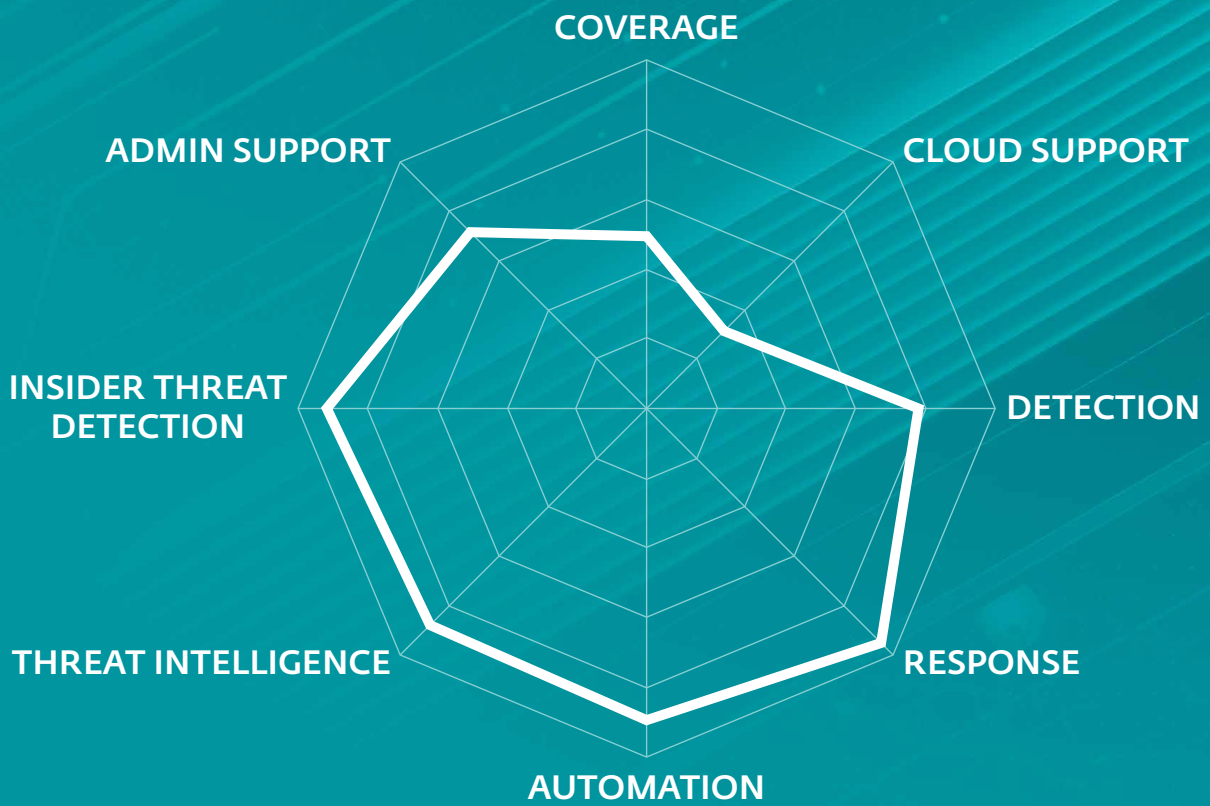
Quali sono i vantaggi del servizio MDR di ESET?

I servizi MDR ESET, che operano in collaborazione con l'intero parco tecnologico del vendor, supportano la gestione del rischio informatico fornendo visibilità sull'ambiente IT, gestito da un'unica console che può essere installata on-prem o in cloud, a seconda delle esigenze. Il servizio ESET MDR è una soluzione olistica che può essere acquistata come parte dell'offerta ESET PROTECT MDR. Si tratta di un'opzione più completa che combina prodotti e servizi di prevenzione, rilevamento e risposta

ESET LEADER 2023 NEL SETTORE MDR

KuppingerCole offre un confronto completo dei fornitori di MDR basato su criteri standardizzati nelle categorie Prodotto, Innovazione e Posizione di mercato. Il rapporto individua i leader complessivi tra i fornitori di MDR ed **ESET** è fiera di essere stata riconosciuta sia come **leader di mercato** che **leader assoluto** nella [MDR Leadership Compass 2023](#) grazie a [ESET PROTECT MDR](#).

ESET




Fonte: *KuppingerCole Leadership Compass 2023: Managed Detection & Response (MDR)*, Luglio 2023, p. 39.

Conclusione

L'XDR non è un elemento separato dal resto delle difese di un'organizzazione. Piuttosto, l'XDR svolge meglio il suo compito all'interno di un ecosistema di sicurezza proattivo che comprenda una moderna protezione degli endpoint, cloud sandboxing, machine learning, threat intelligence e un team di sicurezza dedicato.

Questo approccio multilivello alla sicurezza è fondamentale perché, se da un lato è importante avere una maggiore visibilità su un attacco che si sta verificando sulla rete, dall'altro è ancora più importante essere in grado di passare al setaccio una molteplicità di eventi per individuare un attacco. In questo modo è possibile passare più rapidamente alle fasi di intervento, impedendo all'attacco di progredire ulteriormente.

Naturalmente, il caso migliore è quello di bloccare un attacco al primo tentativo di accesso, o almeno subito dopo: una capacità che si può costruire se si dedica del tempo a testare a fondo le difese contro le tecniche avversarie con l'aiuto di una soluzione XDR.



Noi sosteniamo che l'unico
approccio possibile per
proteggere efficacemente i dati
della propria organizzazione è
quello di disporre di più livelli
di protezione.

Informazioni su ESET

Quando la tecnologia favorisce il **progresso**, ESET è qui per **proteggerlo**.

Per oltre 30 anni, ESET® ha sviluppato software e servizi di sicurezza IT tra i migliori del settore, offrendo soluzioni di protezione complete e multilivello contro le minacce di cybersecurity per aziende e consumatori di tutto il mondo.

ESET è da tempo all'avanguardia nello sviluppo di tecnologie di machine learning e cloud che prevengono, rilevano e reagiscono agli attacchi malware. ESET è un'azienda privata che promuove la ricerca e lo sviluppo scientifico in tutto il mondo.



Protetti da ESET dal 2016
più di 32,000 endpoint



Partner di sicurezza ISP dal 2008
2 milioni di customer base



Protetti da ESET dal 2016
più di 4.000 mailbox



**MITSUBISHI
MOTORS**

Drive your Ambition

Protetti da ESET dal 2017
più di 9,000 endpoint

30+

anni di esperienza

1bn+

utenti internet protetti

400k+

clienti aziendali

195

paesi e territori

13

centri R&D globali



30+ anni di
innovazione continua



Fornitore leader
nell'Unione Europea



Sempre rivolti alla
tecnologia



In crescita su base
annua sin dagli inizi

© 1992–2023 ESET, spol. s r.o. – All rights reserved. Tutti i marchi commerciali qui utilizzati sono marchi commerciali o marchi registrati di proprietà di ESET, spol. s r.o. o ESET North America. Tutti gli altri nomi e marchi sono marchi registrati delle rispettive società.