Phil Muncaster

Novembre 2022

GUIDA ALL'ACQUISTO DEL SERVIZIO DI MANAGED DETECTION AND RESPONSE

Di che cosa si tratta e perché ne hai bisogno?

CONTENUTI

SOMMARIO

Il panorama dei rischi informatici per le aziende è in rapida evoluzione. Le superfici di attacco digitali si sono notevolmente ampliate in seguito agli investimenti implementati durante l'era pandemica. I sistemi cloud, i lavoratori in smart working distratti, le infrastrutture di accesso remoto, gli endpoint distribuiti e le complesse catene di fornitura sono tutti variegati e interessanti obiettivi di minacce informatiche. Allo stesso tempo, la criminalità informatica clandestina sta affinando le sue armi attraverso complesse catene di approvvigionamento, offerte di malware-as-a-service e tattiche, tecniche e procedure (TTP) sempre più innovative.

In questo contesto, la prevenzione delle minacce, pur essendo auspicabile, non è sempre possibile. Ecco perché le organizzazioni dovrebbero considerare di evolvere verso un approccio più olistico, basato su prevenzione, rilevamento e risposta. Così da consentire ai team di bloccare l'ingresso a soggetti malintenzionati ed evitare danni ai propri sistemi. Se la prevenzione fallisce, resta comunque la possibilità di rilevamento e risposta per individuare eventi sospetti e risolvere eventuali minacce prima che diventino troppo insidiose.

Ma qual è il giusto strumento di rilevamento e risposta per le organizzazioni? La soluzione Extended Detection and Response (XDR) può essere utile, ma aggiunge ulteriori sfide, come il reperimento e il costo del personale di sicurezza necessario per gestirlo per non ritrovarsi sovraccaricati da avvisi.

MDR (Managed Detection and Response) è un servizio di sicurezza che combina strumenti, tecnologie ed esperti di cybersecurity per fornire alle organizzazioni potenti capacità di rilevamento e risposta. Se gestito correttamente, l'MDR offre una modalità più efficace di gestire il rischio informatico. Ma il fattore critico è la scelta del fornitore a cui affidarsi.

Le organizzazioni dovrebbero prendere in considerazione fornitori con una comprovata esperienza, disponibilità di informazioni sulle minacce e tecnologie di alta qualità con un alto tasso di rilevamento, un basso tasso di falsi positivi e che sia al contempo poco ingombrante. Inoltre è importante considerare il servizio clienti e il grado di ottimizzazione dell'MDR per le esigenze specifiche della propria organizzazione.

XDR: COME FUNZIONA?

La soluzione XDR è un'evoluzione dell'EDR, che ottimizza il rilevamento, l'indagine, la risposta e la caccia alle minacce in tempo reale. XDR integra i dati relativi alla sicurezza degli endpoint con la telemetria proveniente da strumenti di sicurezza e 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

SFIDE ATTUALI

Nella continua corsa agli armamenti che è la sicurezza informatica, spesso sembra che i nostri avversari siano sempre una spanna avanti. Sono supportati da un sottosuolo criminale che vale trilioni di dollari l'anno e che fornisce tutti gli strumenti, le conoscenze e i dati necessari per sferrare attacchi con facilità. Gli autori delle minacce sono spesso protetti da stati ostili, il che garantisce che gli attacchi possano essere lanciati senza timore di ripercussioni da parte delle forze dell'ordine. Inoltre, le offerte SaaS (Software as a Service) malevoli hanno democratizzato la capacità di coordinare campagne azzardate, anche per soggetti con meno acume tecnico.

Dall'altra parte, i Chief Information Security Officer (CISO) e i loro team sono sempre più impegnati su diversi fronti contemporaneamente. Gli investimenti nella trasformazione digitale durante la pandemia hanno ampliato in modo significativo la superficie di attacco informatico delle aziende. Gli **ambienti di lavoro a distanza** rappresentano una lacuna di visibilità e controllo particolarmente pericolosa, che comprende tutto, dagli endpoint senza patch agli utenti distratti o negligenti. Eppure molti team di sicurezza sono sotto organico e sommersi da troppe soluzioni mirate inefficaci, che aggiungono complessità e riducono la produttività.

I potenziali danni economici e di immagine causati da una grave violazione della sicurezza non sono mai stati così rilevanti. Per di più la capacità delle organizzazioni di mitigare efficacemente i rischi associati a tali incidenti sta diminuendo. I costi derivanti dalle violazioni di dati a livello globale hanno raggiunto il massimo storico di oltre 4,2 milioni di dollari nel 2021. Secondo un assicuratore globale, un quinto delle aziende statunitensi ed europee che hanno subito un cyberattacco in quell'anno hanno rischiato di diventare insolventi.

In questo contesto, puntare **il 100% sulla prevenzione non è realistico**. Un criminale determinato troverà sempre un modo per compromettere degli obiettivi vulnerabili. L'attenzione deve quindi concentrarsi sull'integrare un approccio che preveda anche il rilevamento e la risposta. Anche in questo caso, però, le organizzazioni sono in ritardo. Il tempo medio necessario a livello globale per identificare e contenere una violazione nel 2021 è stato di 287 giorni.

XDR utilizza l'analisi comportamentale su endpoint, rete, cloud, e-mail e altri livelli per individuare attività sospette e bloccare gli aggressori prima che possano avere un impatto.

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

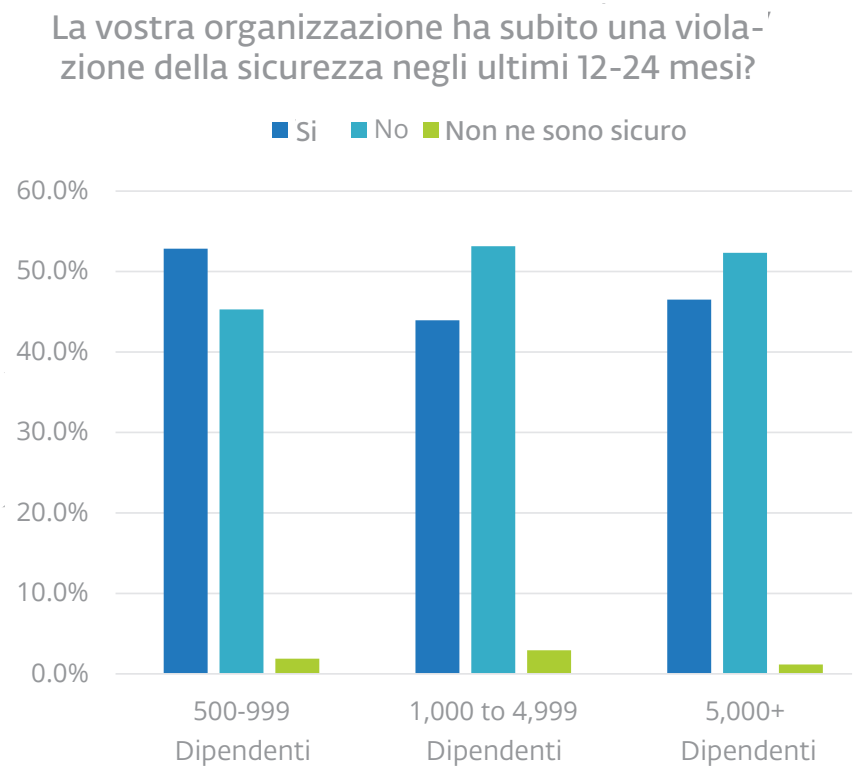
Per questo motivo, molte organizzazioni scelgono un servizio di sicurezza MDR, che combina strumenti, tecnologie ed esperti di cybersecurity. Secondo Gartner, entro il 2025 la metà delle organizzazioni a livello globale utilizzerà servizi MDR per il contenimento delle minacce. Tuttavia, mentre una soluzione XDR richiede che sia il cliente a occuparsi del monitoraggio, del rilevamento e della risposta, con il servizio MDR un fornitore di cybersecurity di fiducia si occuperà del lavoro pesante, permettendo al personale interno di concentrarsi su altre importanti attività.

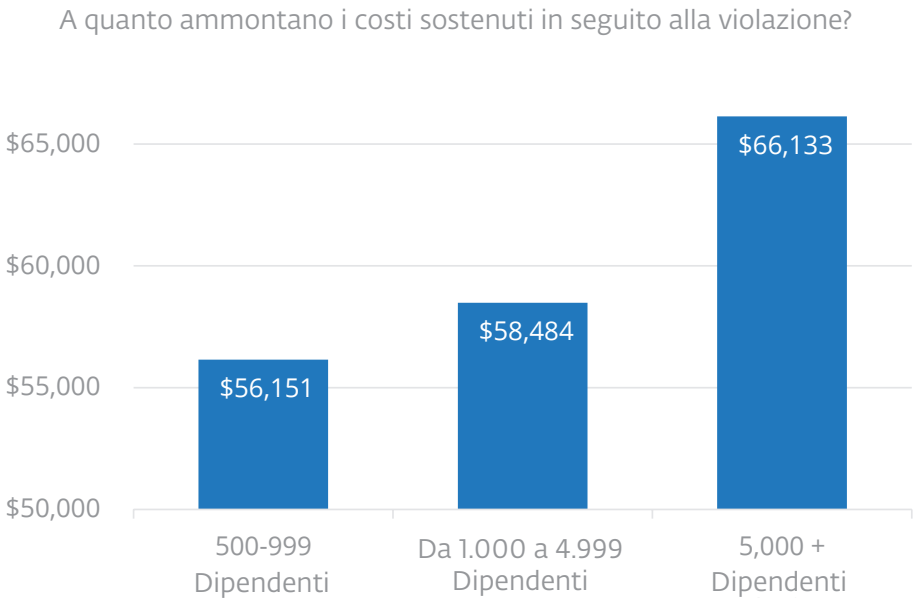
91%

le imprese a livello globale che si affidano o prevedono di avvalersi di servizi di distribuzione, assistenza tecnica, supporto alla cybersecurity e ricerca/monitoraggio delle minacce alla cybersecurity.

Fonte: Sondaggio interno di ESET Research su 404 intervistati di livello Enterprise.

LE VIOLAZIONI SONO UNA REALTÀ





Fonte: IDC, Security Services Market Update, 1Q22, Doc # US48907622, marzo 2022.

PERCHÉ AVVALERSI DI UN SERVIZIO MDR?

Sebbene la spesa media per la cybersecurity sia raddoppiata nel 2021 per le aziende con 250-999 utenti e sia aumentata del 65% per le imprese con più di 1.000 dipendenti, oggi le violazioni avvengono su scala monumentale.

Negli Stati Uniti, nel 2021 si è registrato un volume record di violazioni di dati rivelate pubblicamente, con un aumento del 23% rispetto al precedente massimo storico di 1.506. Nel Regno Unito, il 59% delle medie imprese[1] e il 72% delle grandi imprese[2] hanno dichiarato di aver rilevato violazioni o attacchi informatici nel 2021. La minaccia ransomware è particolarmente grave: un rapporto rivela che nel 2021 sono stati rilevati oltre 623 milioni di attacchi, con un aumento del 105% rispetto all'anno precedente.

La superficie di attacco delle aziende è in espansione

Perché le organizzazioni faticano a respingere gli avversari? In parte perché sono più esposte che mai in seguito agli investimenti in infrastrutture digitali e all'implementazione del luogo di lavoro ibrido. Secondo McKinsey, il COVID-19 ha spinto molte organizzazioni a superare il "punto di svolta tecnologico", cambiando per sempre il modo di lavorare. In alcuni casi, ha accelerato la trasformazione digitale di diversi anni. Ma se da un lato ciò ha contribuito a rendere queste aziende più efficienti e a offrire esperienze innovative a clienti e dipendenti, dall'altro ha aumentato in modo significativo la loro superficie di attacco digitale. Secondo uno studio, il 43% delle aziende globali ammette che la superficie di attacco digitale sta andando "fuori controllo". Lo si può notare nel:

Cloud computing

Le infrastrutture, le piattaforme e i software as a service (IaaS, PaaS, SaaS) offrono enormi vantaggi in termini di IT agility e di costi. Ma soprattutto quando si utilizzano IaaS e PaaS, le organizzazioni hanno difficoltà a proteggere i loro ambienti. Il fatto che molti gestiscano più cloud ibridi non fa che aumentare la complessità. L'errata configurazione è descritta come la prima causa di incidenti di sicurezza nel cloud nel 2021. Gli autori delle minacce cercano regolarmente sistemi esposti da compromettere.

---

1) Si considera un'azienda di medie dimensioni quando conta dai 50 a 249 dipendenti. Sono state intervistate 149 imprese di medie dimensioni.
2) Per grande impresa si intende un'azienda con almeno 250 dipendenti. Sono state intervistate 134 grandi imprese.

Lavoro a distanza

Molti sistemi domestici rimangono preoccupantemente sotto-protetti. I dipendenti potrebbero ritardare ingiustificatamente l'applicazione delle patch ai loro laptop aziendali o trascurare lo stato di sicurezza dei loro dispositivi personali. Un rapporto del 2021 afferma che il 45% dei responsabili IT è stato testimone di stampanti compromesse utilizzate per organizzare attacchi. L'ambiente di lavoro domestico è sempre più visto dai criminali informatici come un interessante vettore di attacco per compromettere le reti aziendali. E ora che il contesto lavorativo ibrido sta diventando una modalità sempre più consolidata, i lavoratori mobili che si connettono tramite hotspot Wi-Fi pubblici e computer condivisi potrebbero costituire un ulteriore minaccia.

Lavoratori a domicilio

Sebbene i dispositivi di lavoro remoto siano spesso bersaglio di attacchi, lo sono anche i loro proprietari. Secondo Microsoft, l'80% dei professionisti della sicurezza ha riscontrato un aumento delle minacce alla sicurezza da quando è iniziato il passaggio al lavoro da remoto. E di questi, il 62% sostiene che le campagne di phishing sono aumentate più di ogni altra minaccia. Si ritiene che i lavoratori a domicilio possano essere più distratti e disposti a correre rischi rispetto ai colleghi che lavorano in ufficio, il che li rende un bersaglio perfetto per l'ingegneria sociale. Il phishing può essere una porta d'accesso a ransomware, violazioni di dati e altre forme di compromissione. Più di un terzo (35%) delle aziende dichiara di aver visto dipendenti aggirare o disattivare le misure di sicurezza.

"Dal 2015 si è registrato un aumento del 25% nel numero di violazioni segnalate, un aumento del 500% nel numero di record violati e, dal 2017, un aumento del 231% nel numero di attacchi ransomware subiti".

Best Practice: Security Matters, Now What? Forrester Research Inc, 2 maggio, 2022

Infrastruttura di accesso remoto

L'avvento del lavoro remoto di massa ha comportato anche un'impennata nell'uso di strumenti come le reti private virtuali e il protocollo di desktop remoto (RDP), che consentono a chi è fuori dall'ufficio di accedere alle risorse interne. Il problema è che spesso vengono lasciati senza patch o mal configurati. Invece di utilizzare l'autenticazione a più fattori per proteggere ulteriormente l'accesso, molti account RDP sono protetti da credenziali deboli o condivise. Ciò consente agli aggressori di accedere abbastanza facilmente alle reti aziendali mascherandosi da utenti legittimi. L'RDP è uno dei tre principali vettori di attacco per il ransomware: i tentativi di compromissione hanno raggiunto il massimo storico di oltre 4,5 miliardi[3] il 10 gennaio 2022.

Grafico delle tendenze dei tentativi di connessione RDP e del numero di client singoli in T3 2021 - T1 2022, media mobile di sette giorni. fonte: Telemetria ESET)

3) Calcolato utilizzando una media mobile a sette giorni

Catene di approvvigionamento

Ciò può significare ecosistemi fisici o digitali di partner e fornitori. Nel mondo fisico, c'è un rischio persistente che i dipendenti e i fornitori con accesso alla rete vengano ingannati e costretti a cedere le loro password o a perdere le loro apparecchiature a causa dei ladri. Nella catena di fornitura del software, c'è probabilmente una minaccia ancora maggiore rappresentata da attori malintenzionati che contaminano i meccanismi e gli strumenti utilizzati per sviluppare, distribuire e aggiornare software con l'inserimento di malware. Il fornitore di software di gestione IT Kaseya è stato compromesso dal gruppo ransomware REvil, che ha sfruttato il suo accesso per inviare aggiornamenti software dannosi ai clienti MSP del fornitore. Oltre 1000 clienti a valle sono stati colpiti. Un'altra causa di preoccupazione è il codice open-source che, sebbene sia comunemente utilizzato dai team DevOps per accelerare il time to value, può introdurre rischi aggiuntivi difficili da gestire tra le complesse dipendenze del software. Secondo un rapporto, oltre due quinti (41%) delle organizzazioni non hanno fiducia nella sicurezza del software open-source che utilizzano e solo il 49% dichiara di avere una politica di sicurezza per il suo utilizzo.

49%

le organizzazioni che implementano una politica di sicurezza relativa ai software open source.

Fonte: State of Open Source Security Report, Snyk, 2022

Criminali informatici sempre più professionali e innovativi

Allo stesso tempo, negli ultimi anni sembrano essere aumentati gli attori di minacce pronti ad approfittare di queste lacune di sicurezza. Esiste persino un mercato in cui vendere dati rubati, acquistare accessi e strumenti e assumere nuove leve. A differenza della professione nell'ambito della cybersecurity, sembra esserci un flusso costante di talenti desiderosi di guadagnarsi da vivere con attività illecite.

L'innovazione è presente ovunque in questo mondo sotterraneo della criminalità informatica, il che è una cattiva notizia per i difensori della rete. Alcuni esempi:

1 Ransomware-as-a-service (RaaS)

Proprio come il SaaS ha reso popolare la distribuzione di software dal cloud, il RaaS ha reso molto più semplice l'attività di lancio e gestione degli attacchi ransomware. I gruppi affiliati possono guadagnare fino all'80% delle entrate derivanti dagli attacchi. In cambio, ricevono uno starter kit che include il payload del ransomware e l'infrastruttura di attacco, oltre a un sito di violazione su cui pubblicare i dati rubati.

2 Monetizzazione aggressiva

La maggior parte degli attacchi ransomware oggi prevede l'esfiltrazione e la fuga di dati per estorcere denaro. Ma i gruppi affiliati stanno sempre di più alzando il tiro contro le loro vittime con una serie di tattiche aggiuntive. Tra questi, gli attacchi denial-of-service distribuiti o i contatti con clienti, partner e giornalisti per informarli dell'accaduto. Un gruppo di ransomware deturpa i siti aziendali delle vittime per mostrare una nota di riscatto. Un altro crea siti su misura con le informazioni trafugate per ogni vittima, in modo che clienti e dipendenti possano verificare se i loro dati sono stati esposti.

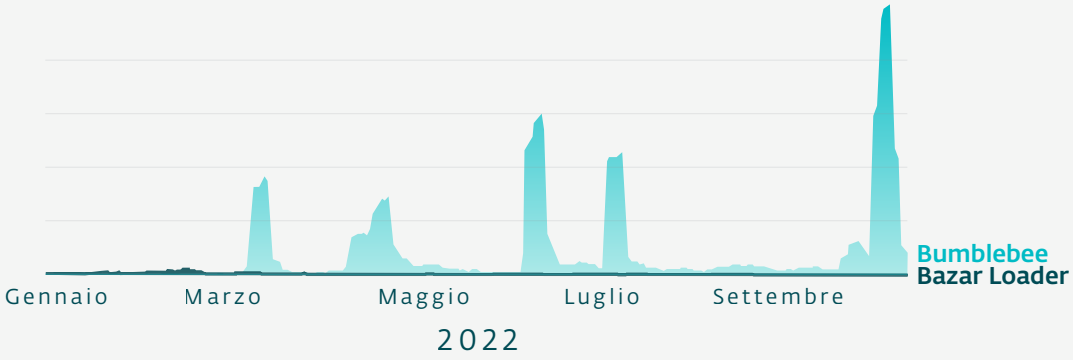
3 Rapido sfruttamento delle vulnerabilità

Il numero di vulnerabilità monitorate nel National Vulnerability Database (NVD) degli Stati Uniti ha raggiunto il massimo storico nel 2021. Questo rende sempre più difficile per gli amministratori della sicurezza tenere sotto controllo il numero spropositato di patch che vengono rilasciate. Come se non fosse già abbastanza difficile, i gruppi di criminali informatici stanno diventando sempre più capaci di reagire rapidamente ai bug zero-day per sfruttarli negli attacchi. A pochi giorni dalla distribuzione delle patch di Microsoft Exchange Server per risolvere le vulnerabilità di ProxyLogon, ben 10 gruppi APT le hanno sfruttate negli attacchi, colpendo oltre 5.000 server Exchange in più di 115 Paesi.

4 La catena di approvvigionamento delle minacce informatiche

La criminalità informatica clandestina è sempre più professionale e ricca di risorse. Stanno emergendo gruppi specializzati per soddisfare specifiche esigenze commerciali e operative. Ad esempio, per quanto riguarda l'accesso alla rete, si assiste a un aumento dei broker di accesso iniziale, esperti che compromettono gli obiettivi e poi vendono questo accesso all'ingrosso ad altri. Un team di ricerca nel 2021 ha rilevato un aumento del 57% nel numero di inserzioni di broker di accesso iniziale pubblicizzate nei forum di criminali informatici rispetto all'anno precedente. Poi c'è Bumblebee, un loader progettato per scaricare ed eseguire payload aggiuntivi. Si tratta del successore di TrickBot, una nota *bestia* altamente resistente che è sopravvissuta a due tentativi di takedown nel 2020 prima di essere disattivata dai suoi autori. Per un certo periodo, il posto di TrickBot è stato occupato da BazarLoader, che è stato attivo fino all'inizio del 2022, ma è stato rapidamente eliminato a favore di Bumblebee. Il loader Bumblebee, che si ritiene sia gestito dagli stessi attori delle minacce di TrickBot e BazarLoader, è tuttora attivo e ha lanciato le sue ultime campagne a metà agosto 2022.

TENDENZE DI RILEVAMENTO DI BUMBLEBEE E BAZARLOADER



5 Strumenti legittimi e malware senza file

Una volta che gli attori delle minacce si introducono nelle reti target, in genere utilizzano strumenti legittimi e malware senza file per aggirare gli strumenti di sicurezza tradizionali. L'idea è quella di utilizzare programmi non dannosi per svolgere attività dannose come movimenti laterali, esfiltrazione di dati, process discovery, dumping di credenziali e esecuzione di comandi shell arbitrari. Questi programmi includono PowerShell, PsExec e Cobalt Strike.

6 I progressi del phishing e dell'ingegneria sociale

A volte i vecchi metodi sono i più efficaci. Il phishing rappresenta ancora uno dei tre principali vettori di attacco per il ransomware, raggiungendo addirittura un livello record nel primo trimestre del 2022. I malintenzionati continuano a perfezionare le loro tecniche per stare un passo avanti rispetto ai filtri di posta elettronica e ai programmi di formazione sulla sicurezza. Tra i più diffusi c'è il thread hijacking delle e-mail, con cui gli aggressori compromettono una casella di posta e poi dirottano le conversazioni esistenti per diffondere link di phishing. Poiché un messaggio di risposta appare più autentico di uno non richiesto, è più probabile che i link inclusi vengano cliccati. Un'altra tecnica è lo smishing (phishing via SMS), che punta sul fatto che gli utenti sono più distratti quando guardano lo schermo dello smartphone e quindi più propensi a cliccare. Un fornitore ha registrato un raddoppio dei tentativi di smishing negli Stati Uniti nel 2021 e oltre 500 campagne di thread hijacking nello stesso anno, collegate a 16 diverse famiglie di malware.

Dalla prevenzione all'XDR

Il ransomware è certamente l'ambito in cui la criminalità informatica sta apportando grande innovazione Secondo gli esperti di sicurezza del governo britannico, questo ha permesso al ransomware di diventare il rischio informatico numero uno per le organizzazioni. È facile capirne il perché: un gruppo da solo (Conti) è riuscito a compromettere almeno 859 organizzazioni in soli due anni - di cui 40 in un solo mese - e a guadagnare miliardi in criptovalute nel processo. Secondo una stima, i rilevamenti di ransomware sono aumentati del 148% rispetto all'anno precedente, raggiungendo i 470 milioni nei primi tre trimestri del 2021, diventando così l'anno peggiore mai registrato.

Ma il ransomware non è affatto l'unica minaccia per le organizzazioni globali di oggi. Furto di dati, malware di cryptomining, trojan bancari e spyware, tra gli altri, si contendono tutti un posto a tavola.

L'impatto complessivo di queste tendenze dovrebbe far riflettere i responsabili della sicurezza informatica su una verità ineludibile. La **prevenzione delle minacce dovrebbe sempre essere preferita, ma a volte non è possibile**. Ci sono semplicemente troppi modi in cui i malintenzionati possono entrare nell'ambiente aziendale senza essere visti. Ecco perché le organizzazioni devono bilanciare la prevenzione con il rilevamento e la risposta. È su questo che si concentra l'approccio Prevention, Detection and Response (EPDR) di ESET, che fonde più livelli di tecnologia di sicurezza. In primo luogo, mira a proteggere bloccando il codice o gli attori dannosi dall'ingresso o dal danneggiare il sistema dell'utente. Ma se ciò fallisce, esistono potenti sistemi di rilevamento e risposta per mitigare le minacce avanzate in grado di compromettere un sistema.

Un po' come chiudere a chiave e a sprangare tutte le porte e le finestre, e installare ulteriori allarmi di rilevamento del movimento per individuare attività sospette se qualcuno riuscisse a entrare in casa. L'XDR è una risorsa fondamentale in questo caso. Consente ai team dedicati alle operazioni di sicurezza (SecOps) di ottenere una visibilità senza precedenti dell'ambiente IT da un unico pannello e di individuare le anomalie che indicano le minacce tramite avvisi affidabili. XDR[5] è un'evoluzione dell'EDR, che ottimizza il rilevamento, l'indagine, la risposta e la caccia alle minacce in

5) Definizione di XDR da parte di Forrester, 2021

tempo reale. XDR integra i dati relativi alla sicurezza degli endpoint con la telemetria proveniente da strumenti di sicurezza e 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.

L'XDR consente di rispondere a diverse domande chiave su un attacco informatico:

- **Come è iniziato?**
- **Da dove è iniziato?**
- **Quando è iniziato?**
- **Quali endpoint sono infetti?**
- **È stato contenuto?**
- **Come possiamo prevenirlo in futuro?**

Soprattutto, può aiutare a intraprendere azioni correttive rapide per risolvere gli incidenti prima che abbiano un impatto grave sull'organizzazione.

Quali sono i vantaggi dell'MDR?

Tuttavia, anche avvalendosi di una soluzione XDR, i team SecOps devono affrontare sfide importanti dal punto di vista organizzativo. Molte di queste, in particolare la mancanza di conoscenze, competenze e risorse interne, sono particolarmente rilevanti tra le PMI. Le sfide generali per le organizzazioni includono:

Carenza di talenti

Il settore della cybersecurity ha attualmente una carenza di 2,7 milioni di lavoratori e gli analisti dei centri operativi di sicurezza (SOC) sono probabilmente tra i più difficili da reperire e mantenere. Il problema è aggravato dall'imminente intenzione di molti analisti di smettere di lavorare nel 2023 a causa dello stress e del burnout associati al sovraccarico di allerte. I generalisti dell'IT spesso non possono dedicare diverse ore al giorno alla gestione di una soluzione XDR. La sfida è ancora più ardua tra le PMI, che in genere non dispongono delle conoscenze e delle competenze interne necessarie per gestire un SOC e potrebbero quindi trarre i maggiori benefici da un servizio MDR.

Costi

I responsabili della sicurezza non devono pensare solo al costo dell'assunzione e del mantenimento dei talenti per il SOC. Devono inoltre trovare la giusta combinazione di strumenti per fornire le informazioni di cui i loro analisti hanno bisogno. Questo può comportare un costo significativo sia in prima battuta che in seguito per il mantenimento delle licenze.

Il peso economico per le organizzazioni che scelgono di svolgere le SecOps internamente è in aumento. Secondo uno studio, in oltre la metà delle organizzazioni il ritorno percepito sugli investimenti è in calo a causa della complessità di gestione. Lo stesso rapporto afferma che i costi per la security engineering stanno raggiungendo i 3 milioni di dollari l'anno, ma solo il 51% ritiene che questi sforzi siano efficaci.

Falle nella sicurezza

A volte gli strumenti non sono all'altezza. Questo può portare a un sovraccarico di avvisi e alla conseguente difficoltà della loro gestione. Se il personale SOC è sommerso da falsi positivi, può finire per passare ore a inseguire vicoli ciechi, mentre i rischi reali vengono ignorati. Quando più strumenti confluiscono nel SOC, si possono creare falle nella copertura.

Management

L'acquisto, l'installazione e la corretta configurazione dei prodotti sono solo i primi passi. La gestione di più strumenti SOC e analisti in più sedi può rappresentare una sfida significativa. Quando le risorse sono già al limite, a volte si tralasciano compiti importanti. È facile sentirsi sopraffatti dalla battaglia contro le minacce in arrivo senza trovare il tempo per riflettere e pianificare strategie.

C'è la percezione che i team di sicurezza IT delle aziende vogliano e siano in grado di affrontare queste sfide in rapida evoluzione, che conoscano a fondo il software che acquistano e che possano costituire dei SOC interni abbastanza maturi per affrontare le minacce informatiche. Una ricerca condotta da ESET[4] mostra infatti che:

68% **le imprese che preferiscono che sia il proprio fornitore di sicurezza a distribuire i prodotti di sicurezza**

75% **si aspettano che il loro fornitore di sicurezza offra supporto, consulenza e risposta agli incidenti in materia di cybersecurity**

87% **richiedono servizi di supporto alla cybersecurity 24/7/365**

90% **vogliono che i fornitori forniscano servizi di monitoraggio, ricerca, risposta e risoluzione delle minacce**

4) Sondaggio interno di ESET Research su 404 intervistati di livello enterprise.

Quali sono i principali vantaggi dell'MDR?

È qui che l'MDR può apportare enormi vantaggi alle organizzazioni che vogliono mitigare il rischio informatico, ma non hanno le risorse interne per farlo in modo efficace. Sebbene un servizo MDR possa variare da fornitore a fornitore, dovrebbe includere almeno alcune delle seguenti caratteristiche:

Rilevamento delle minacce

Gli attori delle minacce hanno innumerevoli modi per eludere le difese perimetrali. Tuttavia, sfruttando l'analisi comportamentale, è possibile individuarli tempestivamente in modo che le organizzazioni possano intervenire per risolvere gli attacchi. La caccia proattiva alle minacce può essere utilizzata anche per cercare attacchi sofisticati che potrebbero essere in grado di eludere i controlli automatici.

Prioritizzazione

Le analisi intelligenti generano un contesto che consente ai sistemi MDR di trasformare i dati in informazioni attuabili e di rilevare gli allarmi con maggiore fedeltà. Si tratta di una fase critica del flusso di lavoro MDR, dato che molti team SOC si trovano a dover affrontare un sovraccarico di avvisi.

"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. IDC ritiene che un'offerta MDR debba andare oltre la semplice fornitura di indicazioni e raccomandazioni".

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

Analisi

L'analisi comportamentale automatizzata si combina con la valutazione umana per verificare se un allarme è un vero positivo e quali sono le misure da adottare per risolvere un problema.

Riscontro

Grazie alla precedente fase di analisi, il sistema capirà che tipo di risposta è necessaria per contenere ed eliminare la minaccia e rimediare a eventuali sistemi compromessi. Ciò potrebbe comportare la reimpostazione della password, il patching di endpoint specifici o persino il reimaging dei computer.

I vantaggi dell'esternalizzazione del rilevamento e della risposta sono semplici ma convincenti:

- Il fornitore di servizi MDR si occupa di tutta la gestione della tecnologia di back-end, liberando il personale che può concentrarsi su attività strategiche di alto valore anziché affogare negli avvisi.
- Il fornitore di servizi MDR può anche ottimizzare e gestire la tecnologia di back-end per allinearsi al profilo di rischio e all'infrastruttura di ciascun cliente.
- Con il rilevamento e la risposta gestiti da una terza parte, non sarà necessario pagare stipendi elevati per attrarre e trattenere i migliori talenti SOC.
- I clienti possono beneficiare delle economie di scala, della capacità di attrarre i migliori talenti e della conoscenza delle organizzazioni e degli ambienti di minaccia di altri clienti.

COSA CERCARE IN UN SERVIZIO MDR?

Con così tante offerte MDR che si affacciano sul mercato, può essere difficile capire da dove cominciare. Punta a un fornitore che possa fornire almeno quanto segue:

Eccellenza nella ricerca:
L'intelligence migliore della categoria costruita su una capacità di ricerca leader del settore.

Servizio clienti di alta qualità:
Compreso il supporto linguistico locale combinato con una presenza globale.

Personalizzazione:
Una soluzione su misura personalizzata in base alle dimensioni, la complessità informatica e il livello di protezione richiesto da ciascun cliente.

Capacità di rilevamento e risposta all'avanguardia:
Test indipendenti hanno premiato l'alto tasso di rilevamento, la bassa percentuale di falsi positivi e un impatto ridotto sulle risorse di sistema.

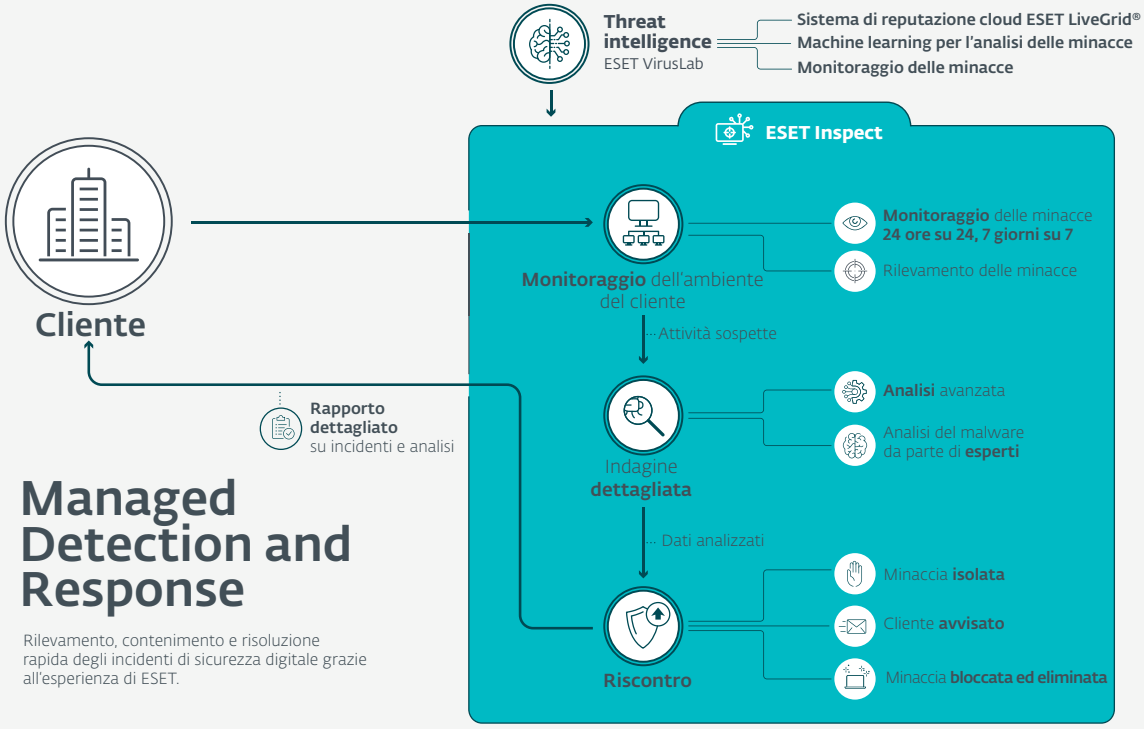
Rilevamento delle minacce informatiche:
Gli esperti analisti combinano la propria esperienza con strumenti avanzati per cercare in modo proattivo le sofisticate minacce che potrebbero nascondersi nella rete.

Operatività 24/7/365: I criminali informatici operano da tutto il mondo e in diversi fusi orari, quindi qualsiasi servizio deve essere vigile e attivo 24 ore su 24.

IN CHE MODO LA SOLUZIONE MDR DI ESET PUÒ AIUTARTI

Le capacità MDR di ESET combinano soluzioni **tecnologiche leader del settore**, tra cui XDR, con una ricerca sulla sicurezza di livello mondiale e un'intelligence sulle minacce basata su oltre **30 anni di esperienza**. Il risultato è un SOC di livello enterprise in grado di sfruttare le nostre **ricerche all'avanguardia** su malware, social engineering, tecniche di offuscamento, gruppi APT e molto altro.

Ma non si tratta di un servizio uguale per tutti. Ogni collaborazione inizia con una valutazione dell'ambiente, dell'infrastruttura, della composizione organizzativa e dell'atteggiamento generale alla sicurezza digitale del cliente. Questo ci aiuta a creare un **profilo di sicurezza su misura del cliente** e ci permette di inserirci come un'estensione interconnessa alle funzioni di sicurezza IT già in essere. ESET, infatti, vanta un'esperienza significativa nella **protezione di clienti in tutti i settori** e una competenza specializzata in una serie di ambiti e segmenti verticali. Affidarsi alla tecnologia ESET consente ai clienti di sfruttare questa esperienza.



Il servizio MDR di ESET, ESET Detection and Response Ultimate, fornisce una suite di prodotti e servizi completa e multi-regione che offre:

- **Un team di esperti di cybersecurity** pronto a gestire l'implementazione, l'ottimizzazione, il monitoraggio quotidiano, la caccia periodica alle minacce, l'analisi del malware e la risposta agli incidenti per una vasta gamma di organizzazioni di diverse dimensioni. I team locali lavorano a stretto contatto con il team globale di threat intelligence, che è il cuore pulsante dell'MDR e degli altri servizi gestiti.
- **Oltre 30 anni di ricerca sulle minacce informatiche** ci forniscono l'esperienza necessaria per monitorare gli ambienti dei clienti alla ricerca di minacce sofisticate e violazioni. E a fornire il servizio sono i nostri esperti il cui lavoro di ricerca è riconosciuto a livello internazionale e condiviso tramite WeLiveSecurity.
- **Indagine e risposta agli incidenti**, compresa l'analisi di base e dettagliata dei file, il reverse engineering, la digital forensics e l'assistenza per la risposta agli incidenti.
- **Una presenza locale su scala globale** fornita da un'ampia rete di partner, uffici regionali e diversi team di ricerca delle minacce informatiche presso la sede centrale di ESET e in tutto il mondo.
- **Assistenza per la sicurezza degli endpoint** per affrontare i mancati rilevamenti di malware, i problemi di pulizia, le indagini sui comportamenti sospetti e per mitigare gli attacchi ransomware.
- **Supporto ESET Inspect** per rispondere a qualsiasi domanda sul nostro strumento XDR, come ad esempio la creazione di regole ed esclusioni personalizzate.
- **Monitoraggio quotidiano delle minacce** disponibile 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, per garantire che l'ambiente sia sempre pulito e protetto e che le minacce vengano rilevate il più precocemente possibile.
- **Caccia alle minacce proattiva** una volta ogni tre mesi per impostazione predefinita, per garantire che l'ambiente rimanga protetto dalle minacce più recenti. Queste indagini sfruttano la vasta conoscenza di ESET degli indicatori di compromissione e delle potenziali minacce segnalate dai clienti.

Report mensile che include i risultati del nostro monitoraggio e dei servizi forniti. Contiene inoltre gli Avvisi di Sicurezza dei nostri analisti. Nei rapporti che abbiamo creato nel corso degli anni, è emerso che il numero di rilevamenti e di incidenti diminuisce nel tempo, man mano che i clienti prendono in carico gli avvisi. Questi non sono solo relativi ai prodotti e alle configurazioni di ESET, ma contengono consigli pratici sul tipo di attività che emergono all'interno dell'ambiente, come i rilevamenti Brute Force o il phishing, e su specifici utenti che tendono a cliccarli.

Il servizio ESET MDR (Detection and Response Ultimate) è un'opzione più completa che combina prodotti e servizi di prevenzione, rilevamento e risposta tutti gestiti da un unico pannello, che includono:

- Management Console (ESET PROTECT)
- Endpoint Protection Platform (ESET Endpoint Security)
- File Server Security (ESET Server Security)
- Advanced Threat Defense (ESET LiveGuard Advanced)
- Full Disk Encryption (ESET Full Disk Encryption)
- Extended Detection & Response (ESET Inspect)
- MDR Service (ESET Detection and Response Ultimate)
- Premium Support Service (ESET Premium Support Advanced)

QUALI SONO LE CARATTERISTICHE DI UN'IMPLEMENTAZIONE MDR EFFICACE?

IL CASO DI ROYAL SWINKELS BREWERY

Royal Swinkels è il secondo birrificio più grande dei Paesi Bassi, produce oltre 300 tipi di birre in più di otto birrifici in tutto il mondo che commercializza in oltre 130 paesi. Ha deciso di condividere la propria esperienza di implementazione del servizio MDR di ESET. Oggi la produzione di birra è un processo altamente automatizzato che dipende dall'IT e dall'OT (automazione industriale). Una violazione o un incidente potrebbero comportare un'interruzione della catena di fornitura e avere un forte impatto sulle consegne e sui ricavi. Il servizio MDR di ESET li aiuta a proteggersi da tali rischi. Il team ESET gestisce i rilevamenti e la risposta, filtra tutti gli avvisi, monitora l'ambiente, con un servizio 24/7 da parte di personale qualificato in sicurezza informatica.

"Ogni azienda delle nostre dimensioni dipende fortemente dall'IT al giorno d'oggi. Da un lato non siamo abbastanza grandi da avere un nostro Security Operations Center, ma dall'altro non siamo così piccoli da poter semplicemente aspettare che accada qualcosa. Non eravamo soddisfatti di questo atteggiamento reattivo, quindi abbiamo virato verso un approccio proattivo ed affidato la gestione a ESET tramite l'MDR. "

Robert Heines,
Royal Swinkels Family Brewers

Per saperne di più su come ESET può supportare il tuo percorso verso una prevenzione, un rilevamento e una risposta migliori, consulta le nostre risorse sui servizi MDR.

CONCLUSIONE

Gli addetti alle decisioni in materia di sicurezza si trovano ad affrontare un periodo difficile, caratterizzato da tendenze convergenti. Dopo gli anni di crisi globale, la superficie di attacco digitale delle aziende si è notevolmente ampliata. Allo stesso tempo, gli attori delle minacce sono sempre più forti, determinati e ben equipaggiati. I responsabili delle operazioni di sicurezza faticano a sventare attacchi sempre più sofisticati, quando i team sono sottoposti a un carico eccessivo, le soluzioni mirate sono poco efficaci e le risorse scarseggiano. Il costo di un SOC completo 24/7/365 in questo contesto è al di là delle possibilità della maggior parte delle imprese, ad eccezione di quelle più grandi.

Le violazioni sono inevitabili, ma non devono necessariamente comportare gravi danni finanziari e di reputazione se gli aggressori possono essere individuati e gli incidenti risolti rapidamente. La nostra soluzione MDR mira proprio a questo. Il lavoro pesante viene affidato a un fornitore dedicato, riducendo al minimo il rischio di sicurezza per l'organizzazione del cliente, consentendo al personale di lavorare su attività di alto valore e di destinare le risorse economiche ad scopi strategici.

"I fornitori di servizi possono implementare i servizi MDR con le competenze esistenti dei clienti, quali strumenti o servizi forniti dai partner di cybersecurity, e proprietà intellettuale privata. Questa partnership crea una potente combinazione di avanzate soluzioni EDR/extended detection response (XDR), esperienza umana, threat intelligence, threat hunting, console, dashboarding e reporting avanzati e varie forme di proprietà intellettuale sviluppate dal fornitore di servizi MDR".

Fonte: IDC, The Evolution of Managed Security Services, Doc # US48459521, dicembre 2021, P. D. Harris, CISSP, CCSK

Indipendenza, integrità, innovazione, competenza: queste sono le basi su cui ESET costruisce le sue pluripremiate soluzioni di cybersecurity.

Con ESET, la tua organizzazione può beneficiare di:

- Una soluzione su misura personalizzata in base alle dimensioni, la complessità informatica e il livello di protezione richiesto da ciascun cliente.
- Assistenza completa da parte degli esperti di cybersecurity di ESET che operano come partner silenziosi
- La tranquillità di sapere che qualsiasi informazione sensibile condivisa sarà gestita da un partner fidato
- Supporto linguistico locale in molti paesi
- Eccellenza nella ricerca costruita in 30 anni di esperienza nella cybersecurity
- Assistenza ransomware integrata, analisi del malware, digital forensics e risposta agli incidenti senza costi aggiuntivi.
- Leader del settore per la sicurezza degli endpoint, ottimizzazioni delle prestazioni e potente capacità di rilevamento.
- Un team di ricerca dedicato alle minacce informatiche che mette a disposizione decenni di esperienza per colmare le carenze di competenze dei clienti

SCOPRI DI PIÙ SUI SERVIZI DI MDR

INFORMAZIONI SU ESET

Per oltre 30 anni, ESET® ha sviluppato software e servizi di sicurezza IT tra i migliori del settore, offrendo soluzioni di protezione complete e multistrato 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 al malware. ESET è un'azienda privata che promuove la ricerca e lo sviluppo scientifico in tutto il mondo.

ESET IN NUMERI

1bn+
utenti internet protetti

400k+
clienti aziendali

Oltre 200
Paesi e territori

13
centri R&D globali

AFFIDATI A UN LEADER TECNOLOGICO GLOBALE PER PROTEGGERE LA TUA AZIENDA