

Guida

9 ASPETTI DA VALUTARE NELLA SCELTA DI UN SERVIZIO MDR



Digital Security
Progress. Protected.

L'MDR può aiutare a colmare le lacune in termini di capacità e competenze in materia di sicurezza, ma la scelta del fornitore giusto è fondamentale.

Le aziende di tutte le dimensioni riconoscono sempre più la necessità di una sicurezza più proattiva. La continua adozione del cloud computing, la diffusione del lavoro ibrido e la catena di fornitura digitale hanno aumentato la superficie di attacco e gli attori delle minacce sono diventati ancora più ingegnosi nella ricerca di modi per penetrare nelle reti.

Tuttavia, solo le imprese più grandi operano su una scala tale da potersi permettere l'allestimento di un centro operativo di sicurezza completo e dotato di analisti di sicurezza impiegati a tempo pieno. Anche se si dispone dei fondi necessari, gli specialisti di cybersecurity scarseggiano. Se la vostra è un'organizzazione di medie o piccole dimensioni, è probabile che sia più difficile identificare e mantenere al vostro interno esperti in cybersecurity e quindi spesso potete affidarvi solo a "generici" esperti IT anche per gestire la sicurezza della vostra infrastruttura aziendale.

I servizi di Managed Detection and Response (MDR) colmano le lacune aziendali in termini di capacità e competenze di sicurezza. Consentono infatti di affidarsi a professionisti della cybersicurezza esperti nel svolgere questo compito.

Tuttavia, il termine MDR viene impiegato per descrivere un'ampia varietà di modelli di fornitura di servizi. Se avete deciso che è arrivato il momento di rafforzare la sicurezza e di affidarvi a un servizio MDR in outsourcing, dovete analizzare l'offerta per individuare il fornitore più adatto alla vostra organizzazione. Di seguito le domande più importanti da porre.

1. QUAL È IL PROCESSO DI ONBOARDING E TUNING DEL FORNITORE?

I tempi di onboarding variano, così come gli strumenti e i modelli di servizio dei vari fornitori di MDR. Fate chiarezza sul processo di onboarding e sul grado di coinvolgimento del vostro team IT, in modo da evitare sorprese.

Le regole di rilevamento, esclusione e i parametri devono essere personalizzati per adattarsi alle esigenze dell'ambiente IT e alle minacce specifiche a cui è esposta l'organizzazione. Sebbene un onboarding rapido sia sempre auspicabile, in questo caso potrebbe essere utile raggiungere un compromesso tra l'attivazione celere del servizio MDR e l'offerta di prestazioni di rilevamento ottimali fin dal primo giorno.

Occorre inoltre tenere presente che la protezione offerta dal servizio MDR migliora nel tempo. E' necessario un periodo iniziale di analisi e ottimizzazione, durante il quale gli strumenti e gli analisti umani acquisiscono esperienza pratica e imparano a distinguere correttamente le anomalie nel vostro ambiente.

2. IL SERVIZIO È 24/?

Gli aggressori sono attivi da Paesi e fusi orari di tutto il mondo, ragion per cui il servizio MDR deve essere operativo 24 ore su 24, 7 giorni su 7. Gli indicatori di compromissione e di attacco devono essere analizzati immediatamente, in tempo reale, in modo da poter avviare una risposta adeguata.

Un servizio locale presenta alcuni vantaggi, che tuttavia vengono rapidamente vanificati in assenza di personale adeguato durante le ore notturne. L'opzione migliore potrebbe essere quella di un servizio dotato di un rappresentante locale, ma anche di centri operativi di sicurezza attivi in tutto il mondo, per un'operatività 24 ore su 24, 7 giorni su 7.

3. QUAL È LO STACK TECNOLOGICO? QUALI FEED VENGONO UTILIZZATI?

Il servizio MDR si basa su uno stack tecnologico fornito dal provider che gestisce il rilevamento, l'indagine, la mitigazione e la risposta. Può trattarsi di un insieme di tecnologie sviluppate dal fornitore o di strumenti di terze parti collegati da API. Tra gli strumenti più comuni si annoverano l'Endpoint o eXtended Detection and Response (EDR o XDR), Security Information and Event Management (SIEM) e la Security Orchestration and Response (SOAR). Tali strumenti dovrebbero integrarsi con la piattaforma di protezione degli endpoint.

Il tratto distintivo di un sistema XDR rispetto a un sistema EDR è dato dall'incorporazione di feed provenienti dall'esterno degli endpoint, tra cui il traffico di rete e vari file di log. Chiedete quali feed verranno utilizzati nell'ambito del monitoraggio. Avvalersi di un fornitore di servizi di protezione degli endpoint ha il vantaggio di offrire una piattaforma degli endpoint che non solo alimenta direttamente l'XDR, ma fornisce anche dati telemetrici unici sugli attacchi.

Gli aggressori informatici stanno diventando sempre più abili nell'utilizzare i servizi cloud come vettore di attacco o parte della catena di attacco. Pertanto, verificate che il vostro fornitore MDR sia in grado di rilevare e monitorare le attività nel cloud.

4. QUALI RUOLI SVOLGE L'AUTOMAZIONE NELL'OFFERTA? QUALI RUOLI SVOLGONO I TEAM DI ANALISTI?

Un solido stack tecnologico è importante, ma ciò che rende un servizio MDR tale è l'attenzione degli analisti di cybersecurity human-in-the-loop.

L'intelligenza artificiale può svolgere un ruolo prezioso nell'identificazione di comportamenti anomali e nel vagliare azioni apparentemente isolate per riconoscere le correlazioni e i segnali di compromissione o attacco. L'automazione può eseguire rapidamente una serie di azioni che isolano i sistemi o fermano un attacco sul nascere. Si tratta di strumenti di assistenza che non sostituiscono le competenze degli analisti umani.

Nella fretta di arrivare sul mercato o di rendere i loro servizi più accessibili, alcuni fornitori di MDR fanno eccessivo affidamento sull'automazione per alcune parti delle loro offerte (per saperne di più, vedere "Chi gestisce la mitigazione e la risoluzione?"). Alcuni offrono servizi differenziati, con servizi più avanzati ai livelli superiori, come team dedicati alla risposta agli incidenti, risposta agli incidenti forensi digitali (DFIR) e analisi avanzata delle minacce informatiche.

5. QUALI FONTI DI INTELLIGENCE SULLE MINACCE VENGONO UTILIZZATE?

Un'intelligence aggiornata sulle attività degli aggressori informatici globali è una componente fondamentale di un servizio MDR di massima efficacia. Gli aggiornamenti basati sui dati telemetrici e sulle analisi dei team di threat intelligence rivelano i metodi di attacco e le rispettive contromisure.

I feed di informazioni sulle minacce possono essere generati dal fornitore di servizi MDR o da terze parti. È utile conoscere le fonti dell'intelligence del fornitore, il modo in cui sono raccolte le informazioni e come vengono rese utilizzabili all'interno del servizio.

È fondamentale sottoporre informazioni regolarmente aggiornate e attuali sulle minacce agli analisti della sicurezza affinché possano scoprire le minacce latenti all'interno del vostro ambiente (argomento successivo).

ESET

Managed Detection and Response

I servizi MDR di ESET poggiano su solide basi: la pluripremiata protezione ESET per gli endpoint; la tecnologia XDR (eXtended Detection and Response) di ESET, che fornisce strumenti pratici per l'analisi dell'intera infrastruttura aziendale; i team di esperti di sicurezza che operano direttamente attraverso la console unica di gestione. Attraverso una rete globale di centri operativi, i servizi MDR di ESET monitorano l'infrastruttura aziendale, identificando e bloccando le minacce e analizzando le informazioni raccolte in modo da attuare le azioni di remediation necessarie.

Il servizio è disponibile in due livelli, uno pensato per le piccole e medie imprese e un SOC di classe enterprise. Entrambi i livelli includono le componenti chiave di un servizio MDR, tra cui il rilevamento continuo, il monitoraggio, il contenimento e l'eliminazione concreta delle minacce. Il livello superiore offre servizi personalizzati o specializzati da parte degli esperti informatici di ESET.

ESET MDR offre:

Ricerca, monitoraggio e risposta alle minacce per clienti di qualsiasi dimensione e livello di sicurezza

Un servizio sempre attivo, 24 ore su 24, 7 giorni su 7, che applica una combinazione di automazione basata sull'intelligenza artificiale e competenze umane

Una libreria già pronta di modelli di rilevamento del comportamento, ulteriormente personalizzata e adattata all'ambiente del cliente

Un team di Global Threat Intelligence che tiene traccia degli incidenti critici in corso e intraprende azioni coordinate per contrastare le minacce.

6. QUALI TIPI DI RILEVAMENTO DELLE MINACCE SONO OFFERTI?

L'obiettivo dell'avversario è introdurre una presenza sconosciuta nella rete utilizzando tattiche, tecniche e procedure che eludono i meccanismi di rilevamento esistenti. Individuare queste minacce nascoste è il compito del rilevamento proattivo.

L'offerta e la portata di tale rilevamento delle minacce sono uno dei principali elementi di differenziazione tra i servizi MDR. Un rilevamento delle minacce continuo e sistematico dovrebbe essere tra i requisiti di base del servizio MDR.

Alcuni fornitori offrono un rilevamento personalizzato, pianificato o ricorrente, incentrato sui trend attuali oppure basato su ipotesi fondate sui dati storici dei rilevamenti e metodi di attacco passati.

7. CHI GESTISCE LA MITIGAZIONE E LA RISOLUZIONE?

Tra i fornitori di MDR non esiste una visione condivisa su quale parte - il fornitore di servizi o l'acquirente - sia responsabile della componente "risposta" dell'MDR. Mentre il rilevamento di sistemi compromessi e di attacchi attivi è universalmente parte dei servizi MDR, questi variano dal punto di vista degli approcci alla mitigazione della minaccia (contenimento per prevenire ulteriori danni) e alla risoluzione (ripristino dei dati e della funzionalità del sistema).

Alcuni fornitori intraprendono azioni di risposta solo se possono essere automatizzate, altrimenti si limitano ad assistere il personale IT del cliente. Altri offrono la risposta nell'ambito di un servizio di livello superiore, con un contratto di consulenza o a un prezzo maggiorato.

I clienti sono diversi anche per quanto riguarda l'atteggiamento nei confronti delle modifiche apportate da terzi. Alcuni sono infatti riluttanti a consentire al servizio MDR di intervenire sui propri sistemi in quanto non possiede una conoscenza approfondita del potenziale impatto sui processi aziendali. Potrebbero preferire, ad esempio, affidarsi al servizio MDR per contenere la minaccia e rimuoverla, riservando invece il ripristino completo al proprio personale IT.

8. IN CHE MODO L'APPROCCIO DEL FORNITORE È IN LINEA CON LA VOSTRA ATTIVITÀ?

Quando si verificano incidenti, l'impatto del servizio MDR va al di là della sicurezza e coinvolge altre parti dell'azienda. Esaminate l'approccio del fornitore al contenimento e valutate come le azioni intraprese si allineino ai requisiti della vostra attività.

Dal punto di vista operativo, considerate come e se le sue attività e i suoi output possano o debbano essere integrati con i vostri sistemi di gestione dei ticket e con i flussi di lavoro interni.

Il fornitore deve anche essere in grado di fornire o permettere di generare rapporti sugli incidenti in corso e risolti, sullo stato del vostro ambiente e su qualsiasi altro aspetto gestito per vostro conto.

9. SE AVETE PARTICOLARI REQUISITI NORMATIVI O DI CONFORMITÀ, IL SERVIZIO È IN GRADO DI SODDISFARLI?

Se avete requisiti di privacy, gestione o conservazione dei dati, verificate che il fornitore di servizi MDR sia in grado di rispettarli. Potrebbe essere necessario adattare o fare eccezioni speciali ai suoi processi standard per conformarsi agli statuti locali.

Se state cercando o avete una copertura assicurativa per la cybersecurity, confrontate gli elementi del servizio del fornitore con i requisiti assicurativi. I controlli informatici aggiuntivi che fanno parte del servizio MDR possono essere rilevanti per il risarcimento o ridurre il premio.

CONCLUSIONE

I servizi MDR sono una categoria di mercato in rapida crescita. Secondo Gartner, esistono più di 600 fornitori di servizi MDR (o servizi definiti tali); il 30% delle organizzazioni utilizza attivamente l'MDR e questo numero è destinato a raddoppiare entro il 2025.

In generale, i fornitori di servizi MDR che si sono fatti avanti per soddisfare la crescente domanda si dividono in due categorie: (1) aziende che forniscono servizi IT gestiti in outsourcing e che hanno aggiunto l'MDR alla loro offerta e (2) aziende di software di sicurezza che hanno aggiunto una componente di servizi. Al di là di questa ampia categorizzazione, esistono modelli molto diversi tra loro per quanto riguarda l'architettura e l'erogazione di un servizio MDR. Comprendere queste differenze è importante.

Ad ogni modo, riconoscere la necessità di un servizio MDR è già un importante passo nella giusta direzione. Ci auguriamo pertanto che questa guida vi sia utile per trovare la soluzione più idonea per la vostra organizzazione.

Continuate a leggere per conoscere i servizi MDR di ESET.

ESET

PREVENZIONE AI-NATIVE PER LE MINACCE DI DOMANI

Rimanete un passo avanti rispetto alle minacce informatiche note ed emergenti con il nostro approccio AI-native, orientato alla prevenzione. ESET combina la potenza dell'intelligenza artificiale e l'esperienza umana per rendere la protezione semplice ed efficace.

Sviluppata nel corso di 30 anni, la protezione best-in-class di ESET attinge alla nostra intelligence interna sulle minacce informatiche globali, avvalendosi di una vasta rete di ricerca e sviluppo guidata da ricercatori rinomati nel settore.

ESET PROTECT, la nostra piattaforma di cybersecurity XDR scalabile e cloud-first, combina funzionalità di prevenzione, rilevamento e threat-hunting proattive di nuova generazione con un'ampia gamma di servizi di sicurezza, tra cui managed detection and response (MDR). Le nostre soluzioni altamente personalizzabili e pronte per l'integrazione supportano tutti i metodi di distribuzione, includono il supporto locale e hanno un impatto minimo sulle prestazioni. Identificano e neutralizzano le minacce emergenti prima che possano essere eseguite, garantiscono la continuità aziendale e riducono i costi di implementazione e gestione.

La nostra missione non è solo quella di fermare gli attacchi sul nascere, ma anche di evitare che si verifichino. ESET protegge la vostra azienda per consentirvi di sfruttare appieno il potenziale della tecnologia.



Digital Security
Progress. Protected.