kaspersky BRING ON THE FUTURE

Kaspersky Managed Detection and Response

per Managed Service Provider

I processi aziendali sono ormai sottoposti a un'ampia automazione: le imprese dipendono in misura sempre maggiore dall'information technology. Ma più l'attività di un'azienda dipende dall'IT, più diventa attraente l'idea di hackerare i suoi sistemi informatici. Spesso le aziende hanno difficoltà a trovare le competenze necessarie per rilevare le minacce e affrontarle in modo appropriato. I team responsabili della sicurezza sono sopraffatti dalla gestione di sistemi e strumenti e non dedicano abbastanza tempo a indagini e analisi approfondite.

Pur portando ovvi vantaggi, adottare pratiche MDR richiede enormi investimenti in termini di personale, formazione specifica e tecnologie

La carenza di competenze in IT security ha ormai raggiunto livelli preoccupanti

Nel mondo vi sono 4,07 milioni di posizioni vacanti, contro i 2,93 milioni rilevate nello stesso periodo dello scorso anno. La crescente domanda di expertise in cybersecurity indica anche che, oltre alla difficoltà di trovare professionisti qualificati, c'è il problema di attirare e trattenere questi talenti. Quindi, se un'azienda non dispone già di un valido team di esperti di threat hunting, investigation e response, non può avere la certezza di riuscire a incrementarlo. Occorre trovare una valida alternativa.

I servizi di Managed Detection and Response (MDR) possono rappresentare una soluzione efficace per le aziende che desiderano creare o migliorare il proprio sistema di threat detection and response precoce, ma non hanno le competenze interne necessarie in materia di cybersecurity. Questi servizi rappresentano uno dei mercati in più rapida ascesa nell'ambito della cybersecurity. Gartner prevede che entro il 2024 il 25% delle aziende utilizzerà i servizi MDR, un incremento notevole rispetto al valore attuale, che è inferiore al 5%. Si tratta di un'enorme opportunità di profitto per i Managed Service Provider (MSP). L'aggiunta dei servizi MDR al vostro portafoglio di servizi vi aiuterà a risolvere i problemi di sicurezza dei vostri clienti e a consolidare relazioni durature con loro.

Pur portando ovvi vantaggi, adottare pratiche MDR richiede enormi investimenti in termini di personale, formazione specifica e tecnologie. Soprattutto, se non avete competenze in termini di threat hunting e incident response, avrete bisogno di molto tempo per far funzionare tutto. Nel frattempo, i vostri clienti attuali e potenziali probabilmente prenderanno in considerazione i servizi MDR forniti da altre aziende. Per trarre il massimo vantaggio dallo slancio del mercato, dovete agire rapidamente. Quali sono le opzioni a vostra disposizione?

Kaspersky MDR per MSP è una proposta estremamente semplice per voi e per i vostri clienti. Le eccellenti capacità di detection and response sono supportate da uno dei team di threat hunting migliori del settore. A differenza di offerte simili presenti sul mercato, Kaspersky MDR si avvale di tecnologie di sicurezza esclusive, di modelli di machine learning brevettati, di un'eccellente threat intelligence e di una comprovata esperienza nelle attività di ricerca di attacchi mirati. Questa soluzione vi permetterà di offrire ai vostri clienti attività proattive di threat hunting e un sistema di risposte guidate da remoto, anche se non disponete delle competenze necessarie. Inoltre, gli MSP che usano già un servizio MDR potranno ottimizzarlo con Kaspersky MDR, avvalendosi di una seconda preziosa opinione da parte di un partner specializzato e affidabile, che li aiuterà a verificare rapidamente le proprie attività di detection and respond per le minacce che potrebbero essere sfuggite.

[1] https://apt.securelist.com/

Vantaggi di Kaspersky MDR per i Managed Service Provider

Deployment rapido e scalabile senza dover investire nello staff e nella tecnologia

Le competenze di Threat Intelligence e Threat Hunting note in tutto il mondo, 24 ore su 24, 7 giorni su 7

Pagamenti flessibili, con subscription mensili a consumo oppure annuali

Funzionalità multitenancy per più clienti da una singola console di gestione

Prodotti supportati:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac[1]
- Kaspersky Security for Windows Server
- Kaspersky Security for Virtualization Light Agent[2]
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti-Targeted Attack

Come funziona

Il servizio monitora i dati di telemetria di sicurezza ricevuti dai prodotti Kaspersky. Convalida gli alert dei prodotti per garantire l'efficacia delle funzionalità di prevenzione automatica e analizza proattivamente i metadati dell'attività del sistema per rilevare eventuali segnali di un attacco attivo o imminente. I metadati vengono raccolti dal Kaspersky Security Network, vengono correlati automaticamente e in tempo reale con l'ineguagliabile threat intelligence di Kaspersky, per identificare tattiche, tecniche e procedure utilizzate dagli attaccanti.

Kaspersky MDR ha due livelli. **Kaspersky MDR Optimum** aumenta istantaneamente la capacità di threat hunting e incident response dell'azienda, senza necessità di investire in personale o competenze aggiuntive; assicura inoltre la massima resilienza agli attacchi elusivi, grazie al deployment rapido. L'agent EDR incluso consente azioni remote centralizzate per isolare gli host infetti, terminare i processi non autorizzati, mettere in quarantena ed eliminare i file dannosi; tutto questo può essere svolto da remoto con un solo clic.

Kaspersky MDR Expert include tutte le funzioni della versione Optimum, oltre a maggiori flessibilità e funzionalità, tra cui il contatto diretto con gli analisti di Kaspersky SOC per ricevere assistenza e indicazioni aggiuntive, tre mesi di archiviazione dei dati non elaborati per il threat hunting retrospettivo e l'accesso privilegiato a Kaspersky Threat Intelligence.

[1] Supporto previsto per il Q2 2021
[2] Supporto previsto per il Q1 2021

MDR a confronto

Optimum

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta da remoto guidati e non invasivi
- Controllo di integrità della sicurezza[1] e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- 1 mese di archiviazione dei dati non elaborati
- API per il download dei dati[2]

Expert

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta da remoto guidati, non invasivi e invasivi[3]
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- API per il download dei dati
- Threat hunting gestito
- 3 mesi di archiviazione dei dati non elaborati
- Accesso alle analisi del Kaspersky SOC
- Accesso al portale Kaspersky Threat Intelligence

Funzionalità aggiuntive:

- Opzioni flessibili di archiviazione e retention in base alle esigenze normative e forensi/e-discovery

Servizi:

- Valutazione di compromissione
- Formazione pratica per gli analisti del SOC
- Incident response retainer

Si tratta di una proposta semplice per voi e per i vostri clienti, che offre molti vantaggi immediati, tra cui:

- Competenze di threat hunting offerte da esperti a livello mondiale con oltre 20 anni di esperienza e successi nella ricerca di attacchi mirati
- Kaspersky MDR può essere facilmente integrato con i processi e i sistemi esistenti (IRP, SOAR, SIEM) attraverso le API del portale Kaspersky MDR
- Funziona con i sistemi di protezione AV di terze parti
- Funzionalità multitenancy per più client da una singola console di gestione

Il threat hunting automatizzato in MDR Optimum si avvale dei rilevamenti automatici effettuati da Indicatori di Attacco proprietari per eseguire ulteriori attività di convalida, investigation e identificazione di nuovi threat. Il threat hunting gestito di MDR Expert si basa sull'impegno pratico e scrupoloso del nostro rinomato team di esperti threat hunter, che esegue una ricerca proattiva dei threat che non vengono individuati automaticamente.

Il servizio utilizza il portale MDR web-based per fornire una visibilità completa di tutti i rilevamenti e fornisce alert e suggerimenti sulle attività di incident response. La sua architettura multitenant consente agli MSP di gestire tutti i client da una singola console. Il portale è dotato anche di API per l'integrazione con i sistemi esistenti (IRP, SOAR, SIEM) e i flussi di lavoro.

Una serie di elementi opzionali (forniti separatamente) consente di personalizzare le funzionalità del servizio in base alle specifiche esigenze, offrendo una maggiore flessibilità quando necessario.

[1] Sarà disponibile nel Q1 2021
[2] Sarà disponibile nel Q1 2021
[3] Sarà disponibile nel Q1 2021

Sottoscrivete Kaspersky MDR

Inserire Kaspersky Managed Detection and Response nel vostro portafoglio di servizi gestiti comporta notevoli vantaggi per l'azienda:

- Incentivare del rinnovo di Kaspersky Endpoint Security for Business con la protezione aggiornata di Kaspersky MDR per mantenere relazioni durature e ricorrenti con i clienti
- L'upselling della protezione avanzata 24/7 ai nuovi clienti di endpoint security consente di ottenere un numero di account maggiore e più redditizio

Sottoscrivete Kaspersky MDR e approfittate dei vantaggi del programma MSP di Kaspersky: sottoscrizioni mensili, a consumo o annuali, sconti per volumi elevati, margini di profitto più alti, opportunità di upselling/cross-selling e supporto tecnico e alle vendite di prim'ordine.

Per approfittare delle opportunità offerte dal mercato MDR in rapido sviluppo e iniziare a incrementare i vostri profitti, contattateci oggi stesso scrivendo a msp@kaspersky.com

News sui cyber threats: www.securelist.it
Notizie sulla sicurezza IT:
www.kaspersky.it/blog/category/business/
Sicurezza IT per le PMI:
www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise:
kaspersky.it/enterprise-security
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.it

We are proven. We are independent. We are transparent. Siamo pronti a costruire un mondo sicuro, dove le tecnologie migliorano le nostre vite. È per questo che lo proteggiamo, così che chiunque, in ogni luogo possa godere delle infinite opportunità che offre. Bring on cybersecurity for a safer tommorow.

Per saperne di più: kaspersky.it/transparency

Proven.
Transparent.
Independent.