kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Creazione di un'efficace strategia di protezione completa con risposte automatiche istantanee e un'analisi della root cause intuitiva

Il problema

Il 91% delle organizzazioni ha subito cyberattacchi nel 2019 e **1 su 10** è stata vittima di un attacco mirato[1].

Le minacce complesse creano instabilità

L'epoca del malware semplicistico è finita da tempo. Le minacce sono diventate molto più sofisticate e, con la complicità di tempi di rilevamento più lunghi, stanno generando disagi e perdite più pesanti per le aziende.

È in corso un attacco

Questo tipo di attacchi diventano sempre più economici e frequenti, perciò le organizzazioni che pensavano di esserne immuni ora si ritrovano a doverci fare i conti.

L'efficienza è fondamentale

La situazione è ulteriormente aggravata dalla mancanza di risorse, tra le quali spiccano il tempo e il personale qualificato, che le organizzazioni devono fronteggiare.

In che modo Kaspersky può essere d'aiuto

«Una soluzione EPP inefficace è destinata a distruggere il valore di uno strumento EDR»[2]

«Di conseguenza, le persone e il tempo diventano le nuove metriche ROI per lo strumento EDR»[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum protegge dalle minacce complesse e avanzate grazie a una funzionalità di rilevamento avanzato e a processi semplici e automatici di investigation e response.

Funzionalità innovative

Offre visibilità approfondita, semplici strumenti di investigation e opzioni di risposta automatica che consentono di rilevare la minaccia, scoprirne la reale portata e le origini e rispondere in tempo reale, evitando interruzioni alla business continuity.

Efficace strategia di protezione completa

Offre un toolkit di rilevamento e risposta intuitivo e altamente automatizzato, oltre all'ineguagliabile protezione endpoint e al rilevamento avanzato di Kaspersky Endpoint Security for Business, dando via a una soluzione unificata.

Strumento intelligente per un'efficienza garantita

Consente di risparmiare tempo e ottimizzare il lavoro del personale IT grazie a controlli centralizzati intuitivi e a un elevato livello di automazione. Flusso di lavoro snello da una singola console disponibile on-premise e su cloud[3].

Vantaggi chiave

- Protezione dalle minacce evolute e complesse più pericolose e frequenti
- Risparmio in termini di tempo e risorse grazie a uno strumento semplice e automatico
- Analisi della reale portata delle minacce sull'intera rete
- Individuazione della root cause e della modalità di attuazione della minaccia
- Esclusione di ulteriori danni grazie alla risposta automatica

Importanti use case di EDR

Risposte a domande importanti

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

Individuazione della reale portata della minaccia

Dopo aver compreso di essere di fronte a una potenziale minaccia globale, ad esempio nel caso in cui l'ente regolatore vi chieda di cercare uno specifico indicatore di compromissione (IoC), potete:

- Importare gli IoC da fonti attendibili ed eseguire scansioni periodiche per rilevare segni di un attacco
- Analizzare attentamente un avviso, generare IoC in base alle minacce rilevate ed eseguire scansioni di tutta la rete per scoprire l'eventuale coinvolgimento di altri host

Rispondere immediatamente alle minacce che si diffondono rapidamente

- Mettere automaticamente in quarantena i file associati a minacce complesse su tutti gli endpoint
- Isolare automaticamente gli host infetti dopo l'individuazione di un IoC associato a una minaccia che si diffonde rapidamente
- Impedire l'esecuzione di un file dannoso e la sua diffusione in rete nel corso dell'investigation

[1] Rapporto sui rischi globali IT, Kaspersky, 2019

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc US45794219, 2020

[3] Sono previste limitazioni alla gamma di funzionalità gestibili attraverso la console cloud. Per informazioni complete, consultate la pagina https://kas.pr/epp-management-options

Adesso è possibile:

Individuazione della reale portata della minaccia

È possibile individuare gli avvisi di sicurezza sugli endpoint e sottoporli a ulteriore analisi per comprendere la reale portata e gravità della minaccia. Ciò vi permetterà di gestire gli incidenti in modo efficace senza lasciare alcun segno della minaccia sull'endpoint.

Semplificazione del flusso di lavoro

Flusso di lavoro snello da una singola console on-premise e sul cloud, scenari e controlli EDR semplici, inclusa la visualizzazione dettagliata, opzioni di scansione e risposta agli IoC che non richiedono competenze particolari in ambito di Cybersecurity né un eccessivo dispendio di tempo.

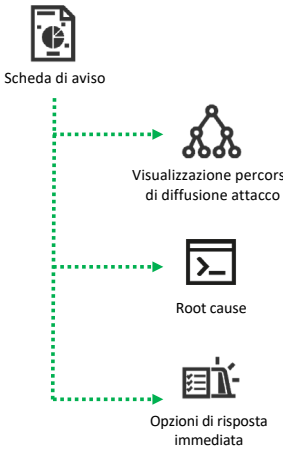
Ottimizzazione delle difese

L'aggiunta di Kaspersky Sandbox crea una soluzione per la sicurezza degli endpoint integrata e completa che offre una difesa multilivello semplice, efficace e altamente automatizzata contro le minacce commodity, complesse ed elusive.

Analisi dei dati dell'avviso dettagliati

Kaspersky EDR Optimum arricchisce gli incidenti con informazioni necessarie e vi aiuta a comprendere le connessioni tra i vari eventi tramite la visualizzazione del percorso di diffusione dell'attacco.

A tal fine, tutti gli host della rete vengono sottoposti a scansione al fine di rilevare indicatori IoC importati o generati.



Risposta automatica

È possibile impostare risposte automatiche alle minacce individuate su tutti gli endpoint in base alle scansioni IoC o rispondere immediatamente agli incidenti rilevati con un semplice clic.

Le opzioni di risposta includono: isolamento degli host, quarantena dei file, avvio della scansione dell'host e blocco dell'esecuzione dei file.

Altre opzioni di EDR

Kaspersky Endpoint Detection and Response Optimum è una delle numerose opzioni di EDR che offriamo, ciascuna personalizzata in base alle esigenze dei clienti. Altre soluzioni consigliate:

Kaspersky Endpoint Detection and Response

Soluzione EDR apprezzata dagli esperti del settore e dai clienti, perfetta per le organizzazioni IT con team di sicurezza IT specifici, che permette di risolvere gli attacchi mirati più evoluti e sofisticati. Offre rilevamento delle minacce avanzato, investigation efficace, threat hunting proattivo e incident response centralizzata.
https://www.kaspersky.it/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Soluzione completamente gestita e personalizzata che assicura operazioni continuative di rilevamento, assegnazione delle priorità, investigation e response. Supportata da più di 20 anni di attività di ricerca delle minacce, vi permetterà di sfruttare i maggiori vantaggi offerti da un centro per le attività di sicurezza senza doverne effettivamente crearne uno.
https://www.kaspersky.it/enterprise-security/managed-detection-and-response

Per maggiori informazioni sul modo in cui Kaspersky Endpoint Detection and Response Optimum affronta le minacce informatiche sfruttando al minimo il team responsabile della sicurezza e le vostre risorse, consultate la pagina
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Novità sulle minacce informatiche: www.securelist.it
Notizie di sicurezza IT: www.kaspersky.it/blog/
Sicurezza IT per grandi aziende: www.kaspersky.it/enterprise-security
Portale Threat Intelligence: opentip.kaspersky.com

www.kaspersky.it

Siamo testati. Siamo indipendenti. Siamo trasparenti. Ci impegniamo a costruire un mondo più sicuro. È per questo che lo proteggiamo, affinché chiunque, in ogni luogo, possa godere delle infinite opportunità che offre. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.