Kaspersky Endpoint Detection and Response

Le imprese stanno migliorando la propria strategia di sicurezza per fornire una risposta alle minacce avanzate e ai cyberattacchi moderni. Gli endpoint sono ancora il principale obiettivo dei cybercriminali. Oggi però le minacce puntano ad aggirare le tradizionali misure di sicurezza degli endpoint, interrompendo i processi critici di business, danneggiando la produttività e aumentando i costi operativi.

I ritardi costano denaro

Avviare il recupero una settimana dopo la scoperta di un incidente costa all'impresa il 200% in più rispetto alla risposta immediata.
Kaspersky Lab Corporate IT Risks Survey

Kaspersky EDR è ideale per le organizzazioni che desiderano:

- Automatizzare l'identificazione e la risposta alle minacce; senza interruzioni per l'attività
- Migliorare la visibilità degli endpoint e l'individuazione delle minacce; tramite tecnologie avanzate, come ML (Machine Learning), Sandbox, IoC scan e Threat Intelligence
- Potenziare il livello di sicurezza; con una soluzione di risposta agli incidenti, facile da utilizzare e destinata alle imprese
- Stabilire processi unificati ed efficaci per la ricerca di minacce, la gestione degli incidenti e i processi di risposta.

Riservatezza dei dati:

Condivisione di threat intelligence in tempo reale tramite Kaspersky Private Security Network on-premise.

- Nessun invio di dati in cloud grazie all'utilizzo di KPSN.
- Tutti i dati forensi vengono memorizzati centralmente all'interno di Kaspersky EDR nella rete aziendale.

Individuazione attiva di minacce

Con il servizio aggiuntivo Kaspersky Managed Protection - attivo 24 ore su 24 - in integrazione a Kaspersky EDR, le aziende possono trarre il massimo beneficio dalle attività di ricerca di minacce da parte dei nostri esperti a livello globale. I ricercatori di Kaspersky Lab possono:

- analizzare le informazioni relative alle minacce avanzate rilevate nella rete aziendale
- notificare rapidamente al team di Cybersecurity aziendale eventuali rilevamenti di attività dannose
- fornire consigli su come rispondere all'incidente e risolvere la problematica

Caratteristiche principali

Risposta adattiva alle minacce

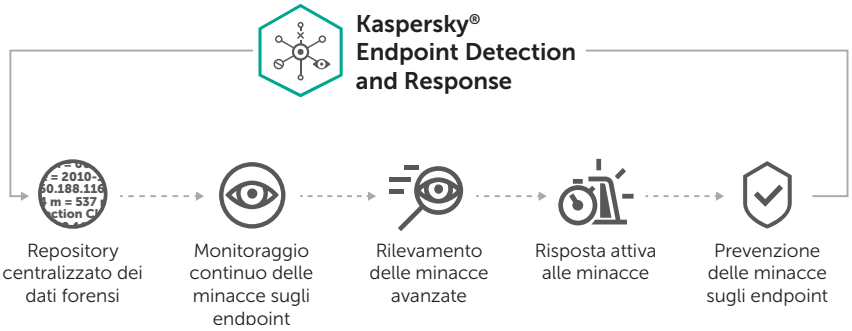
Kaspersky EDR include una vasta gamma di azioni di risposta automatiche che aiutano le imprese ad evitare i tradizionali problemi di remediation, quali il ripristino del sistema o la reinstallazione delle macchine, che possono comportare tempi di inattività e perdita di produttività.

Threat Hunting proattivo

Kaspersky EDR può cambiare radicalmente il flusso di lavoro dei team di cybersecurity grazie alla possibilità di ricercare indicatori di compromissione (IoC) sia all'interno di un database centralizzato che in tempo reale sugli endpoint gestiti. Invece di dover attendere la ricezione di alert, il team di cybersecurity può ricercare le minacce attraverso una scansione proattiva degli endpoint per individuare eventuali anomalie e violazioni di sicurezza.

Interfaccia web intuitiva

L'interfaccia intuitiva e web-based di Kaspersky EDR consente al personale addetto alla sicurezza una visibilità unificata e il controllo delle diverse fasi di analisi: individuazione, investigazione, prevenzione, alerting e reporting. Data la possibilità di monitorare e controllare una vasta gamma di funzioni tramite una singola interfaccia, il team di cybersecurity può eseguire le proprie attività in modo più efficace ed efficiente, senza dover districarsi tra strumenti differenti e console multiple.



Scoprire e contenere rapidamente le minacce avanzate

Kaspersky
Endpoint Detection and Response (Kaspersky EDR) aiuta le aziende a rilevare, analizzare e rispondere:

- Migliorando la visibilità sugli endpoint
- Automatizzando le attività di risposta
- Potenziando le capacità di indagine

... ed è compatibile con le tradizionali soluzioni di endpoint security.

Kaspersky EDR aiuta i team di cybersecurity, e anche i responder meno esperti, nell'effettuare il triage di un endpoint con la precisione di uno specialista di incident response. Con Kaspersky EDR, l'azienda può:

- MONITORARE in modo efficiente le minacce, oltre il malware generico
- RILEVARE in modo efficace le minacce, utilizzando tecnologie avanzate
- AGGREGARE i dati forensi a livello centrale
- RISPONDERE rapidamente agli attacchi
- PREVENIRE azioni dannose delle minacce rilevate

... il tutto attraverso una potente interfaccia web che semplifica l'indagine e la reazione.

Casi d'uso

- Ricerca proattiva e in tempo reale di intrusioni - compresi gli Indicatori di Compromissione (IoC) - a livello di rete
- Rilevamento rapido e remediation di un'intrusione - prima che l'attaccante possa causare danni e interruzioni di servizio
- Integrazione col SIEM - per supportare la correlazione degli eventi e le attività rilevate a livello endpoint
- Validazione degli alert e dei potenziali incident rilevati da altre soluzioni di sicurezza
- Analisi rapida e gestione centralizzata degli incidenti - anche su migliaia di endpoint - senza impatto sul business.
- Automazione delle operazioni di routine, per minimizzare le attività manuali, liberare risorse e ridurre la probabilità di "alert overload".

Sicurezza endpoint avanzata

Kaspersky Lab dimostra la propria costante leadership nella protezione degli endpoint con la combinazione di cinque elementi cruciali in un'unica soluzione:

- Un potente motore anti-malware di nuova generazione; con machine learning
- Endpoint detection and response (Kaspersky EDR)
- Un servizio di ricerca di minacce attivo 24 ore su 24: Kaspersky Managed Protection
- Accesso alla threat hunting in tempo reale, tramite Kaspersky Security Network
- Controlli endpoint avanzati (dispositivo/web/app, crittografia e altri).

Potenziamento delle tradizionali soluzioni di sicurezza degli endpoint.

Kaspersky EDR è compatibile con numerosi prodotti di endpoint security di terze parti e consente quindi di lavorare in affiancamento a tali soluzioni contribuendo ad aggiungere:

- Funzionalità Next-Gen, per rilevamento e prevenzione di minacce avanzate
- Centralizzazione dell'analisi e dei processi di risposta

...senza che l'azienda debba sostituire le soluzioni di sicurezza esistenti

Analisi degli oggetti in un ambiente virtuale e isolato.

Kaspersky EDR include una Sandbox avanzata on premise che effettua l'estrazione automatica di qualsiasi file, su qualsiasi endpoint, per un'analisi approfondita. Fornisce un'efficace "virus lab" interno, senza che alcun dato venga inviato all'esterno della rete aziendale.

Rilevamento avanzato: con machine learning.

Il motore di machine learning incluso in Kaspersky EDR - Targeted Attack Analyzer (TAA) - definisce una "baseline" del comportamento degli endpoint. Questo permette di creare uno storico dei log delle attività degli endpoint che può essere utilizzato per identificare come è avvenuto un data breach. Inoltre, tramite correlazione di dati forensi, threat intelligence e verdetti ricevuti dai moduli antimalware, Kaspersky EDR permette di rilevare i comportamenti anomali sugli endpoint.

I vantaggi di business in tutta l'impresa

Riduzione dei costi

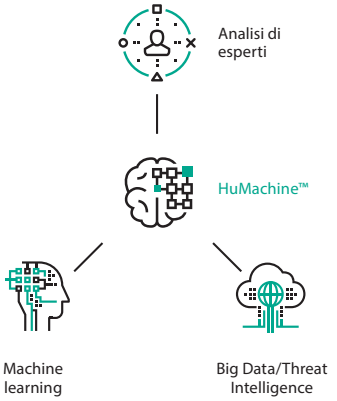
- Automatizzazione delle attività manuali; durante il rilevamento delle minacce e le azioni di risposta
- Aiuto nel velocizzare il contenimento della minaccia; finalizzato al risparmio di denaro e risorse
- Riduzione dell'effort del personale IT e di sicurezza, che può dedicarsi ad altre attività
- Riduzione al minimo dei disservizi durante l'investigazione

Ottimizzazione del ritorno di investimento

- Ottimizzazione dei flussi di lavoro
- Riduzione del tempo necessario ad identificare e rispondere alle minacce
- Supporto per il raggiungimento della conformità (PCI DSS e altre normative); tramite analisi dei log sugli endpoint, la revisione degli alert e la documentazione dei risultati delle indagini

Mitigazione dei rischi di attacco

- Supporto per l'individuazione ed il fixing delle falle di sicurezza e riduzione del "dwell time"
- Semplificazione dei processi di Threat Analysis e Incident Response
- Miglioramento delle soluzioni di sicurezza esistenti tramite "threat validation"



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Novità sulle minacce informatiche: www.securelist.it
Novità sulla sicurezza IT: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.it