kaspersky BRING ON THE FUTURE

Kaspersky Managed Detection and Response

La maggior parte dei security team adotta nei confronti degli incidenti di Cybersecurity un approccio di tipo "alert-driven", reagendo solo a incidente ormai avvenuto. Nel frattempo, nuove minacce si propagano senza essere rilevate, lasciando l'azienda con un falso senso di sicurezza. Di fatto, le imprese riconoscono in misura sempre maggiore la necessità di individuare e neutralizzare in modo proattivo le minacce IT che non sono state individuate, ma risultano ancora attive all'interno dell'infrastruttura aziendale.

Vantaggi offerti dal prodotto:

- La consapevolezza di essere costantemente protetti anche dalle minacce più complesse e avanzate
- Riduzione dei costi complessivi della sicurezza, avvalendosi di un servizio di management esterno
- Impiego delle risorse interne sui task di natura critica che ne richiedono un effettivo coinvolgimento
- Tutti i vantaggi di avere un SOC senza doverne effettivamente creare uno

Kaspersky Managed Detection and Response (MDR) assicura un'efficace protezione avanzata, 24 ore su 24, nei confronti del crescente volume di minacce informatiche, in grado di eludere i sistemi automatizzati di prevenzione e rilevamento. Fornisce un prezioso aiuto alle aziende con risorse interne limitate e a tutti coloro che si trovano in difficoltà nel reperire personale qualificato in ambito cybersecurity.

Le eccellenti capacità di rilevamento e risposta sono supportate da uno dei team di threat hunting migliori del settore, con oltre 20 anni di costante ricerca su malware e minacce informatiche. A differenza di offerte simili presenti sul mercato, Kaspersky MDR si avvale di modelli di machine learning di un'esclusiva Threat Intelligence e di comprovata esperienza nella ricerca di attacchi mirati. Rafforza automaticamente la resilienza aziendale alle cyberminacce, ottimizzando le risorse esistenti e i futuri investimenti nel campo della sicurezza IT.

Principali caratteristiche del prodotto

- Il deployment rapido e scalabile consente di implementare funzionalità di sicurezza IT senza dover investire in personale o competenze aggiuntive
- Una protezione avanzata, particolarmente efficace anche nei confronti delle minacce malwareless più complesse e sofisticate, previene qualsiasi interruzione delle attività aziendali e riduce al minimo l'impatto complessivo dell'incidente
- La risposta agli incidenti viene completamente gestita o guidata assicurando reazioni rapide mantenendo il controllo delle azioni di risposta agli attacchi
- La visibilità in tempo reale su asset e relativo stato di protezione garantisce una piena awareness dell'effettiva situazione, attraverso vari canali di comunicazione

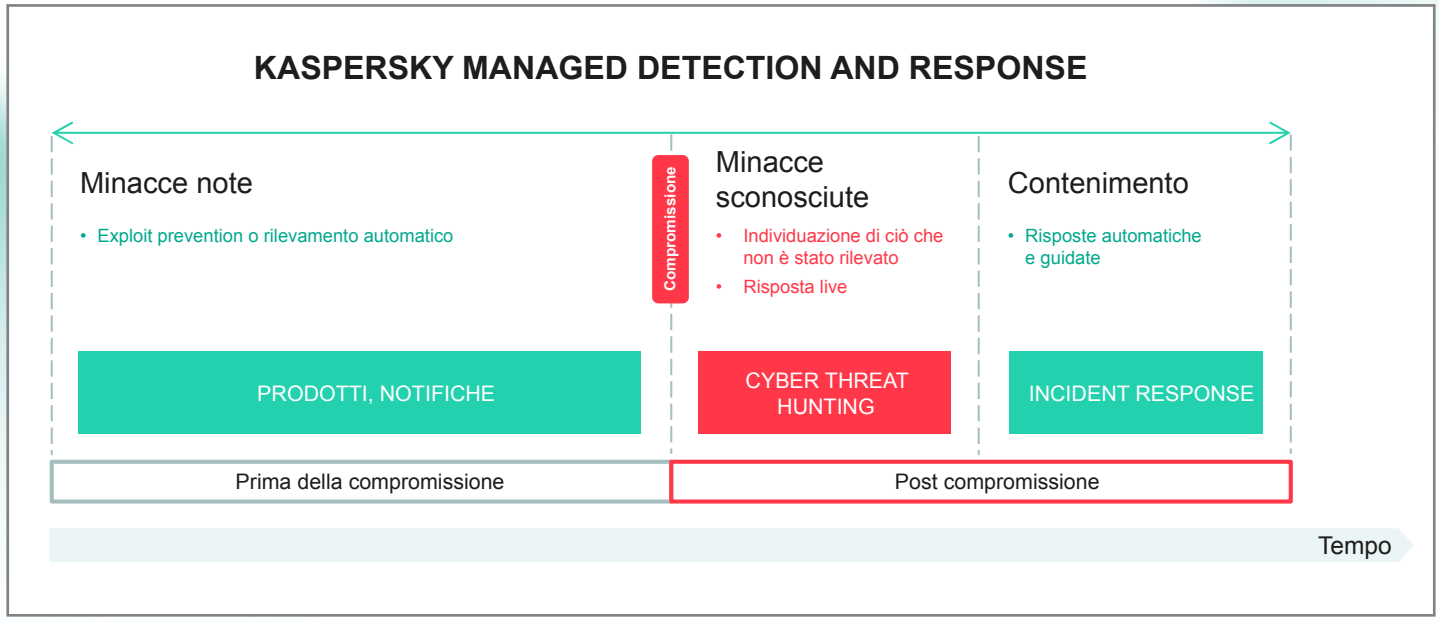

Figura 1. KASPERSKY MANAGED DETECTION AND RESPONSE

Prodotti supportati:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti-Targeted Attack

Come funziona

Kaspersky MDR convalida gli avvisi di sicurezza generati dal prodotto, al fine di garantire la piena efficacia delle funzionalità di prevenzione automatica; analizza inoltre in modo proattivo i metadati relativi all'attività di sistema, per rilevare eventuali comportamenti di un attacco attivo o imminente. I metadati vengono raccolti tramite l'infrastruttura Kaspersky Security Network, per poi essere automaticamente correlati in tempo reale con la Threat Intelligence di Kaspersky, allo scopo di identificare tattiche, tecniche e procedure utilizzate dagli autori dell'attacco. Gli Indicatori di Attacco proprietari consentono il rilevamento di minacce malwareless, in grado di emulare attività legittime. Nell'arco delle prime 2-4 settimane la soluzione si adatta pienamente all'infrastruttura IT aziendale, per garantire un tasso di falsi positivi pari a zero e determinare, assieme agli esperti di sicurezza IT interni, ciò che è legittimo e ciò che invece non lo è.

Kaspersky MDR presenta due diversi livelli, per soddisfare al meglio le esigenze che emergono nelle aziende di qualsiasi dimensione e in settori che denotano mutevoli livelli di maturità tecnologica in termini di sicurezza IT (Figura 2). **Kaspersky MDR Optimum** innalza istantaneamente il livello di sicurezza IT dell'azienda, senza dover investire in personale o competenze aggiuntive; assicura inoltre la massima resilienza agli attacchi, grazie al deployment rapido e scalabile. **Kaspersky MDR Expert** include tutte le funzionalità di Optimum e offre ulteriori funzionalità e maggior flessibilità per i team di sicurezza IT maturi, consentendo loro di assegnare i processi di investigation e triage degli incidenti a Kaspersky, consentendo alle risorse interne di focalizzarsi sulle strategie di risposta ai risultati forniti.

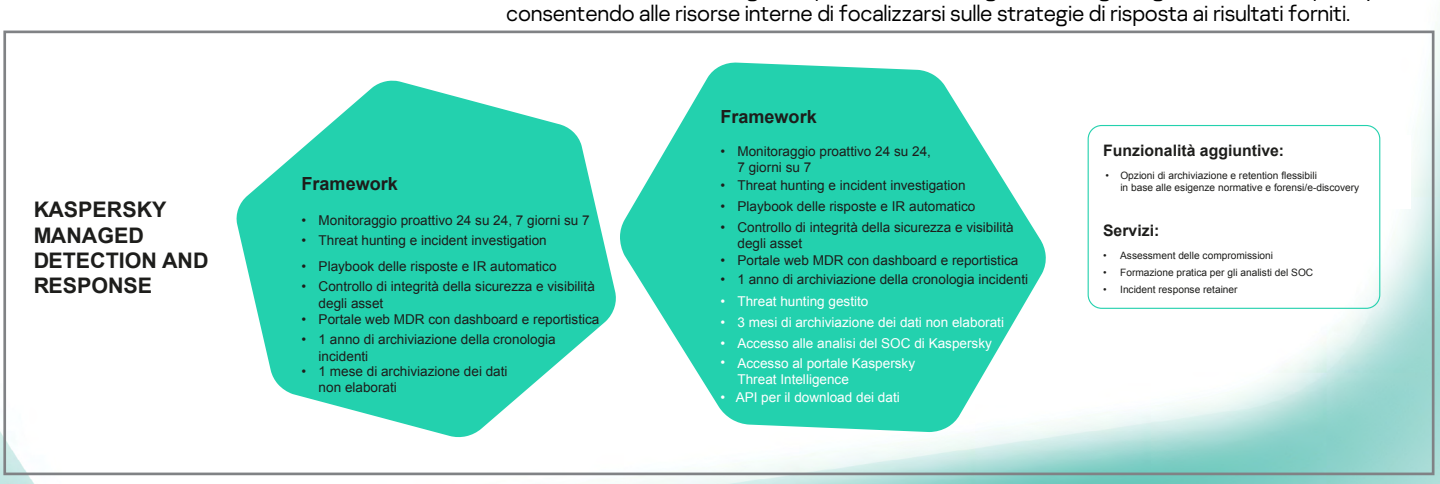

Figura 2. I due livelli di Kaspersky MDR

Il threat hunting automatizzato incluso in MDR Optimum si avvale dei rilevamenti automatici effettuati da Indicatori di Attacco proprietari per le ulteriori attività di validation, investigation e identificazione di nuove minacce. Il threat hunting gestito, disponibile con la soluzione MDR Expert, si basa sulle ricerche e findings del nostro team di esperti di Cybersecurity, alla costante ricerca proattiva delle minacce non individuate dai sistemi di rilevamento automatico.

Un'ampia serie di elementi opzionali complementari, consente di adattare perfettamente le funzionalità del prodotto alle esigenze specifiche di ogni azienda, fornendo un livello di flessibilità ancora maggiore in caso di necessità:

- Opzioni di archiviazione e retention flessibili in base alle esigenze normative e forensi/e-discovery
- Un incident response retainer, grazie al quale tutto il peso dell'esperienza di Kaspersky viene applicato alla risoluzione dell'incidente di sicurezza
- Un efficace e completo assessment delle compromissioni, per verificare che i controlli di sicurezza esistenti siano di fatto sufficienti
- Formazione pratica per gli analisti del SOC, per garantire le necessarie capacità reattive in presenza di incidenti

Per contrastare efficacemente gli attacchi mirati occorrono estese competenze, comprovata esperienza e la continua acquisizione di nuove conoscenze. Siamo stati ad esempio i primi ad allestire un centro dedicato alle investigation sulle minacce complesse: nessun altro provider di Cybersecurity è riuscito a rilevare un numero così elevato di attacchi mirati altamente sofisticati, come ha fatto Kaspersky nel corso di questo ultimo decennio. Kaspersky Managed Detection and Response, frutto di avanzate competenze in materia di sicurezza IT, ottimizza l'indiscusso valore delle soluzioni di sicurezza Kaspersky, offrendo funzionalità di rilevamento, assegnazione delle priorità, investigation e response completamente gestite e personalizzabili. Consente quindi di ottenere tutti i principali vantaggi derivanti dal disporre di un proprio SOC senza di fatto doverne creare alcuno.

* Il supporto per Kaspersky Endpoint Security for Mac è previsto nel Q1 2021. Kaspersky non rilascia alcuna dichiarazione, né si assume alcun obbligo in merito alle date previste per la release. Le stesse sono fornite esclusivamente a titolo informativo. Kaspersky si riserva il diritto di modificare in qualsiasi momento i piani relativi ai propri prodotti.

Novità sulle minacce informatiche: www.securelist.it
IT Security News: business.kaspersky.com
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security
Portale Threat Intelligence: opentip.kaspersky.com

www.kaspersky.it

Offriamo tecnologie di protezione comprovate. Siamo indipendenti e siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia migliori le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Bring on cybersecurity for a safer tomorrow.

Proven. Transparent. Independent.