kaspersky BRING ON THE FUTURE

Kaspersky Managed Detection and Response

Die meisten Sicherheitsteams verfolgen einen reaktiven Ansatz bei Cybersicherheitsvorfällen: Sie reagieren erst, nachdem ein Vorfall bereits eingetreten ist. In der Zwischenzeit bleiben neue Bedrohungen unter dem Radar und vermitteln ein falsches Gefühl von Sicherheit. Immer mehr Unternehmen erkennen, dass sie Bedrohungen, die unerkannt, aber noch immer aktiv in ihrer Unternehmensinfrastruktur lauern, proaktiv aufspüren müssen.

Servicevorteile:

- Die Gewissheit, dass Sie jederzeit vor den neusten Bedrohungen geschützt sind
- Geringere Gesamtkosten für die Sicherheit, ohne eigene Sicherheitsexperten einstellen zu müssen
- Konzentration der internen Ressourcen auf die kritischen Aufgaben, die tatsächlich menschliches Eingreifen erfordern
- Alle wesentlichen Vorteile, die ein eigenes Security Operations Center bietet, ohne ein solches tatsächlich einrichten zu müssen

Kaspersky Managed Detection and Response (MDR) bietet rund um die Uhr fortschrittlichen Schutz gegen die wachsende Zahl von Bedrohungen, die automatisierte Sicherheitsbarrieren umgehen können, und entlastet damit Organisationen, die keine spezialisierten Mitarbeiter finden oder auf beschränkte eigene Ressourcen angewiesen sind.

Die überlegenen Erkennungs- und Abwehrfunktionen dieser Lösung werden von den erfolgreichsten und erfahrensten Threat Hunting-Teams der Branche unterstützt. Im Gegensatz zu anderen Angeboten nutzt Kaspersky MDR patentierte ML-Modelle (maschinelles Lernen), ständig aktualisierte Threat Intelligence und Kasperskys langjährige Erfahrung aus der effektiven Erforschung von zielgerichteten Angriffen. So wird die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberbedrohungen gestärkt, während gleichzeitig vorhandene Ressourcen und künftige Investitionen in die IT-Sicherheit optimiert werden.

Service-Highlights

- Schnelle, skalierbare IT-Sicherheitsfunktionen können sofort als reife IT-Sicherheitseinrichtung bereitgestellt werden, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss.
- Zuverlässiger Schutz gegen sehr komplexe und innovative Bedrohungen abseits von Malware verhindert Unterbrechungen des Geschäftsbetriebs und reduziert die Gesamtauswirkungen auf ein Minimum
- Vollständig gemanagter oder angeleiteter Umgang mit Vorfällen, damit schnell reagiert werden kann, wobei Sie stets die volle Kontrolle über sämtliche Maßnahmen behalten
- Dank Transparenz behalten Sie die aktuelle Situation aller Assets und deren Schutzstatus in Echtzeit über verschiedene Kommunikationskanäle stets im Blick

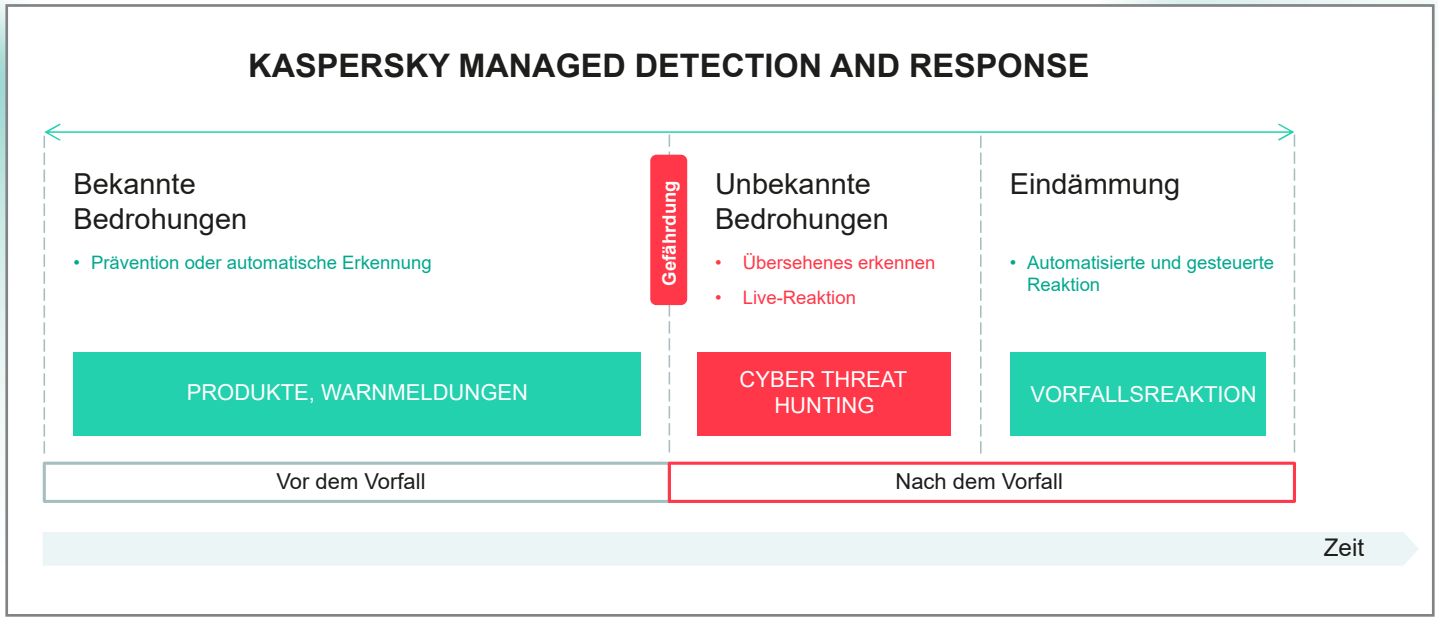

Abbildung 1. Kaspersky Managed Detection and Response

Unterstützte Produkte:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security für Linux
- Kaspersky Endpoint Security for Mac[1]
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

Funktionsweise

Kaspersky MDR überprüft die von den Produkten ausgegebenen Warnmeldungen, um die Wirksamkeit der automatisierten Prävention sicherzustellen, und untersucht proaktiv die Metadaten von Systemaktivitäten auf Anzeichen von aktiven oder bevorstehenden Angriffen. Diese Metadaten werden über das Kaspersky Security Network erfasst und in Echtzeit automatisch mit der stets aktuellen Threat Intelligence von Kaspersky abgeglichen, um Taktiken, Techniken und Vorgehensweise von Angreifern zu erkennen. Von Kaspersky selbst entwickelte Angriffsindikatoren sorgen dafür, dass im Verborgenen lauernde Bedrohungen abseits von Malware, die legitime Aktivitäten vortäuschen, erkannt werden. Innerhalb der ersten 2-4 Wochen passt sich der Service an Ihre Infrastruktur an, um auf eine False Positive-Rate von Null zu kommen. Dabei stimmt es mit Ihnen ab, was legitim ist und was nicht.

Um den Ansprüchen von Organisationen jeglicher Größe und unterschiedlich ausgereiften IT-Sicherheitssystemen gerecht zu werden, wird Kaspersky MDR in zwei Stufen angeboten (Abbildung 2). **Kaspersky EDR Optimum** erhöht unmittelbar den Sicherheitsstatus Ihrer IT-Systeme, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss, und bietet in einer schnellen, mühelosen Bereitstellung Resilienz gegenüber schwer erkennbaren Angriffen. **Kaspersky MDR Expert** enthält sämtliche Features der Optimum-Version und bietet darüber hinaus weitere Funktionen und Flexibilität für erfahrene IT-Sicherheitsteams, die die Auswahl und Untersuchung von Vorfällen an Kaspersky abgeben und ihre begrenzten eigenen IT-Sicherheitsressourcen auf die Abwehr der ihnen vorgelegten kritischen Fälle richten können.

Abbildung 2. Stufen von Kaspersky MDR

Zur weiteren Überprüfung, Untersuchungen und Identifizierung neuer Bedrohungen nutzt die Threat Hunting-Funktion von MDR Optimum eine automatisierte Erkennungsfunktion, die mit eigens ermittelten Angriffsindikatoren arbeitet. In MDR Expert basiert die Managed Threat Hunting-Funktion auf der manuellen Arbeit unserer Experten, die proaktiv solche Bedrohungen aufspüren, die die automatische Erkennung umgehen.

Mit einer Reihe von kostenlosen Zusatzelementen können Sie darüber hinaus die Funktionsweise des Services ganz flexibel an Ihre eigenen Bedürfnisse anpassen:

- flexible Optionen für Speicherung und Aufbewahrung entsprechend den gesetzlichen und ermittlungstechnischen/eDiscovery-Anforderungen
- ein Incident Response Retainer, um dem jeweiligen Sicherheitsvorfall machtvoll mit der gesammelten Expertise von Kaspersky zu begegnen
- ein umfassendes Gefährdungs-Assessment, um zu prüfen, ob Ihre vorhandenen Sicherheitskontrollen ausreichend sind
- praktische Schulungen für SOC-Analysten, damit Sie für jeden Vorfall gewappnet sind

Zur Abwehr zielgerichteter Angriffe, bedarf es neben viel Erfahrung auch der permanenten Weiterbildung. Kaspersky war der erste Anbieter, der vor fast zehn Jahren ein eigenes Center zur Untersuchung komplexer Bedrohungen eingerichtet hat und seitdem mehr hochentwickelte zielgerichtete Angriffe aufdecken konnte als jeder andere Anbieter von Sicherheitslösungen. Auf der Grundlage dieser spezifischen Expertise holt Kaspersky Managed Detection and Response mit seiner vollständig gemanagten, individuell zugeschnittenen stetigen Erkennung, Priorisierung, Untersuchung und Reaktion das Maximum aus Ihren Kaspersky-Sicherheitslösungen heraus. So können Sie alle wesentlichen Vorteile genießen, die ein eigenes Security Operations Center bietet, ohne ein solches tatsächlich einrichten zu müssen.

[1] Wird voraussichtlich ab dem 2. Quartal 2021 unterstützt

[2] Wird voraussichtlich ab dem 1. Quartal 2021 unterstützt

[3] Wird voraussichtlich ab dem 1. Quartal 2021 unterstützt

Neues über Cyberbedrohungen: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise
Threat Intelligence Portal: opentip.kaspersky.de

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen Möglichkeiten nutzen können, die Technologien mit sich bringen. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Proven. Transparent. Independent.