Kontinuierliches Aufspüren, Erkennen und Ergreifen von Maßnahmen bei Cyberbedrohungen, die auf Ihr Unternehmen abzielen

Kaspersky Managed Detection and Response

kaspersky BRING ON THE FUTURE

Kaspersky MDR

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.

Bedrohungen müssen proaktiv gesucht werden

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, stets bestens vor den innovativsten Bedrohungen geschützt zu sein**
- **Geringere Gesamtkosten für die Sicherheit, ohne eigene Sicherheitsexperten einstellen zu müssen**
- **Konzentration der internen Ressourcen auf die kritischen Aufgaben, die tatsächlich menschliches Eingreifen erfordern**
- **Profitieren Sie von allen wesentlichen Vorteilen, die ein eigenes Security Operations Center bietet, ohne dass Sie ein solches tatsächlich einrichten müssen**
- **Unterstützung durch das globale SOC-Analystenteam von Kaspersky aus Europa, Lateinamerika und Russland**
- **Telemetriedaten von Kunden werden in unserem europäischen Rechenzentrum in Irland gespeichert**
- **Alle übertragenen Telemetriedaten werden verschlüsselt, um sie vor unbefugtem Zugriff durch Dritte zu schützen**

Service-Highlights

Die überlegenen Erkennungs- und Abwehrfunktionen von Kaspersky MDR 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. Dies stärkt die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberbedrohungen und optimiert gleichzeitig vorhandene Ressourcen und zukünftige Investitionen in die IT-Sicherheit.

Skalierbare Bereitstellung

Hochentwickelte, skalierbare IT-Sicherheitsfunktionen können sofort bereitgestellt werden, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss.

Incident Response

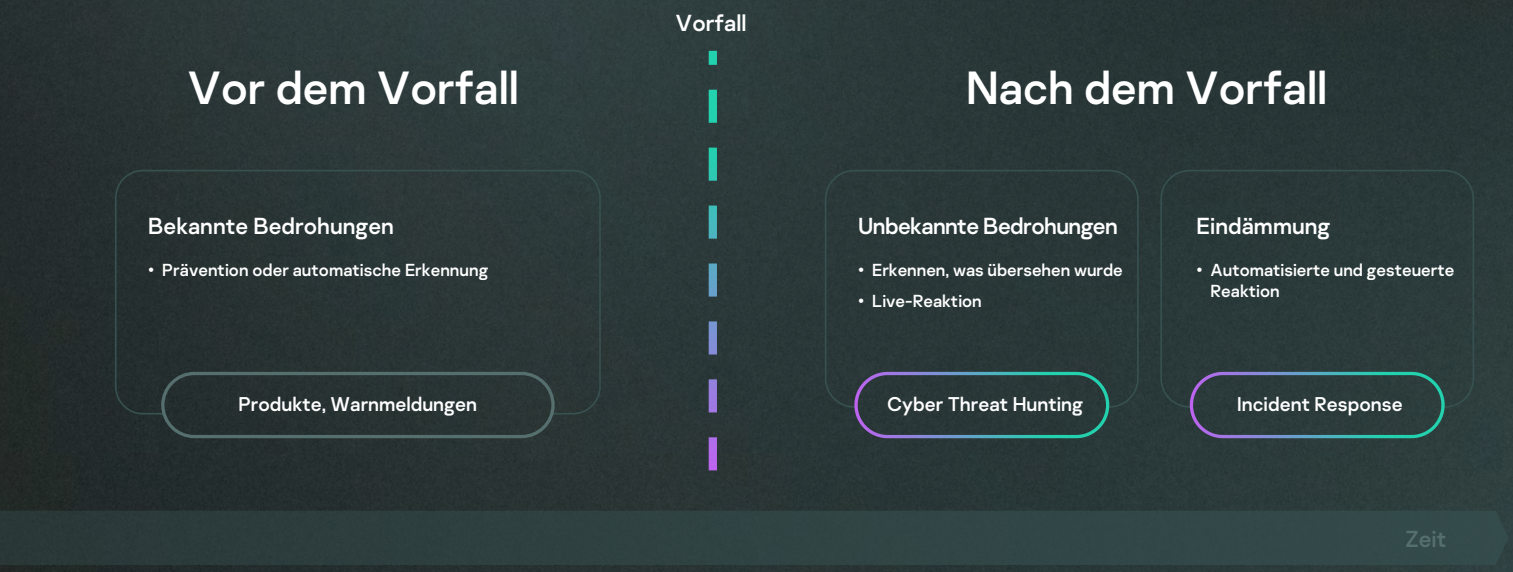
Vollständig gemanagter oder angeleiteter Umgang mit Vorfällen, damit schnell reagiert werden kann, wobei Sie stets die volle Kontrolle über sämtliche Maßnahmen behalten

Zuverlässiger Schutz

Zuverlässiger Schutz gegen sehr komplexe und innovative Bedrohungen abseits von Malware verhindert Unterbrechungen des Geschäftsbetriebs und reduziert die Gesamtauswirkungen auf ein Minimum

Echtzeit-Transparenz

Dank Echtzeit-Transparenz behalten Sie die aktuelle Situation aller Assets und deren Schutzstatus über verschiedene Kommunikationskanäle stets im Blick



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 wird mit Ihnen abgestimmt, was legitim ist und was nicht.

Unterstützte Produkte

- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Security for Mac
- Kaspersky Security for Windows Server
- Kaspersky Security Center
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Agent

Stufen von Kaspersky MDR

Kaspersky MDR wird in zwei Stufen angeboten, um den Ansprüchen von Organisationen jeder Größe und mit unterschiedlich ausgereiften IT-Sicherheitssystemen gerecht zu werden.

Automatisiertes Threat Hunting in MDR Optimum

MDR Optimum umfasst automatisiertes Threat Hunting, das automatische Erkennungsfunktionen einsetzt, die auf Indicators of Attack (IoA) basieren. Diese Erkennungen werden anhand von Echtzeit- und historischen Telemetriedaten erstellt. Unsere SOC-Analysten nutzen sie, damit sie Bedrohungen weiter identifizieren, bewerten und untersuchen können. Kaspersky SOC setzt über 700 selbst entwickelte Angriffsindikatoren ein, die 100 % aller bekannten Taktiken, Techniken und Prozeduren (Tactics, Techniques and Procedures, TTPs) abdecken.

Optimum

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.

- Sicherheitsüberwachung 24x7
- Automatisiertes Threat Hunting und Vorfallsuntersuchung
- Gesteuerte und verwaltete Reaktionen
- Zugriff auf Kaspersky SOC-Analyse
- Überprüfung der IT-Sicherheit u. Überblick über Ressourcen
- Zentrale Verwaltungskonsole (Kaspersky Security Center)
- Verläufe werden 1 Jahr lang gespeichert
- Rohdaten werden 1 Monat lang gespeichert

Managed Threat Hunting in MDR Expert

Gleichzeitig beruht Managed Threat Hunting im Rahmen von MDR Expert auf dem aktiven Einsatz unserer Experten und wird genau an Ihre individuellen Anforderungen angepasst. Unsere Threat Hunting-Experten spüren bisher unbekannte TTPs an, die in der automatischen Erkennung kein Ergebnis hervorgebracht haben. Das Team entwickelt im Fall der Identifizierung solcher TTPs neue oder angepasste bestehende Angriffsindikatoren für die weitere Verwendung auf beiden MDR-Stufen.

Expert

Kaspersky MDR Expert enthält sämtliche Features der Optimum-Version und bietet darüber hinaus weitere Funktionen für erfahrene IT-Sicherheitsteams, die die Auswahl und Untersuchung von Vorfällen an Kaspersky abgeben und den Fokus ihrer eigenen IT-Sicherheitsressourcen auf die Abwehr der kritischen Fälle richten können.

- Sicherheitsüberwachung 24x7
- Automatisiertes Threat Hunting und Vorfallsuntersuchung
- Gesteuerte und verwaltete Reaktionen
- Zugriff auf Kaspersky SOC-Analyse
- Überprüfung der IT-Sicherheit u. Überblick über Ressourcen
- Einzelne Verwaltungskonsole (Kaspersky Security Center) mit Dashboards und Reporting
- Verläufe werden 1 Jahr lang gespeichert

Nur in Expert

- Rohdaten werden 3 Monat lang gespeichert
- Managed Threat Hunting
- Erstellung benutzerdefinierter Vorfälle
- Zugang zum Kaspersky Threat Intelligence Portal
- API für Datendownload

Flexibler Service

Mit einer Reihe von optionalen Elementen können Sie die Funktionsweise des Dienstes flexibel an Ihre Anforderungen anpassen.

- Gefährdungs-Assessment
- Praktische Schulungen für SOC-Analysten
- Incident Response Retainer
- Tabletop Exercise

Nutzen Sie das einzigartige Know-how von Kaspersky

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.

Kaspersky Managed Detection and Response bietet eine vollständig verwaltete, individuell zugeschnittene kontinuierliche Erkennung, Priorisierung, Untersuchung und Reaktion und holt so 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.

www.kaspersky.de

#kaspersky
#bringonthefuture