Effektives Aufspüren, Erkennen und Ergreifen von Maßnahmen bei Cyberbedrohungen

Kaspersky Managed Detection and Response

kaspersky bring on the future

Aktuelle Herausforderungen für Unternehmen

55 %

der Unternehmen berichten von Malware-Infektionen ihrer Geräte[1]

20 %

der Unternehmen sind von Advanced Persistent Threats (APT) betroffen[2]

18 %

der Befragten nennen den Mangel an Fachpersonal im Bereich Cybersicherheit als Hauptursache für Vorfälle in ihrem Unternehmen[3]

2,5 Milliarden USD

Extreme Verluste durch einen erfolgreichen Cyberangriff[4]

Steigern Sie Ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen durch Managed Protection rund um die Uhr

Unternehmen jeder Größe stehen unter Druck. Dazu tragen Faktoren wie Homeoffice, die schnelle Entwicklung von Methoden zum Informationsaustausch, weltweit zunehmende Qualifikationslücken und eine wachsende Zahl von Cyberbedrohungen bei. Schnelle und effektive Abwehrmaßnahmen sind entscheidend.

Kaspersky Managed Detection and Response (MDR) bietet rund um die Uhr extern verwalteten Schutz vor Cyberbedrohungen und ausgefeilten Angriffen, die von herkömmlichen automatisierten Sicherheitsfunktionen nicht mehr erkannt werden.

Die Lösung bietet einen schlüsselfertigen Service für eine schnelle Implementierung und verbessert so das IT-Sicherheitsniveau von kleinen und mittleren Unternehmen, denen es an Fachwissen im Bereich Cybersicherheit mangelt. Erfahrene Teams mit viel Know-how im Bereich Cybersicherheit gewinnen an Flexibilität, wenn sie Aufgaben zur Erkennung und Einstufung von Vorfällen an Kaspersky-Experten delegieren oder eine zweite professionelle Meinung einholen können.

Kaspersky MDR stärkt und verbessert die Resilienz von Unternehmen gegenüber Cyberbedrohungen und optimiert den Einsatz von Ressourcen. So können Unternehmen vorhandene und künftige Investitionen in die IT-Sicherheit so effizient wie möglich nutzen.

Schlüsselfunktionen

- 24/7 Monitoring und Threat Hunting
- Übersicht über alle geschützten Ressourcen mit ihrem aktuellen Status
- Automatisierte und gesteuerte Reaktion
- Direkter Kontakt mit SOC-Analysten von Kaspersky
- REST API für die Integration mit IRP / SOAR
- Webkonsole mit Dashboards und Berichten
- 3 Monate Speicherung von Telemetrie-Rohdaten
- Meldung von Vorfällen
- Speicherung der Historie von Sicherheitsvorfällen für 1 Jahr

[1] IT Security Economics, 2022
[2] Kaspersky MDR Analyst Report, 2023
[3] Kaspersky Human Factor 360 Report, 2023
[4] Global Financial Stability Report. The Last Mile: Financial Vulnerabilities and Risks, 2024

Quellen der Telemetriedaten und Warnmeldungen für Kaspersky MDR

- **Kaspersky Endpoint Security for Windows**
- **Kaspersky Endpoint Security for macOS**
- **Kaspersky Endpoint Security for Linux**
- **Kaspersky Virtualization Light Agent**
- **Kaspersky Anti-Targeted Attack**

Funktionsweise

1

Die SOC-Analysten von Kaspersky untersuchen Sicherheitswarnungen und analysieren proaktiv Telemetrie-Ereignisse, die sie von Kaspersky-Lösungen aus dem Kundennetzwerk erhalten. Die Telemetriedaten werden mit den Cyberbedrohungsdaten von Kaspersky korreliert. Kaspersky hat mehr als 25 Jahre Erfahrung in der Untersuchung von Cyberbedrohungen; darunter befanden sich einige der weltweit bekanntesten Cyberangriffe und gezielten Kampagnen. So lassen sich bekannte, neue und aufkommende Taktiken, Techniken und Verfahren der Angreifer identifizieren. Eindeutige IoAs (Indicators of Attack) helfen, versteckte Bedrohungen zu erkennen, die keine Malware enthalten und legitime Aktivitäten vortäuschen.

2

Künstliche Intelligenz (KI) in Kaspersky MDR trägt dazu bei, die Anzahl von Fehlalarmen zu reduzieren und die Untersuchung von Vorfällen durch das SOC-Team zu beschleunigen.

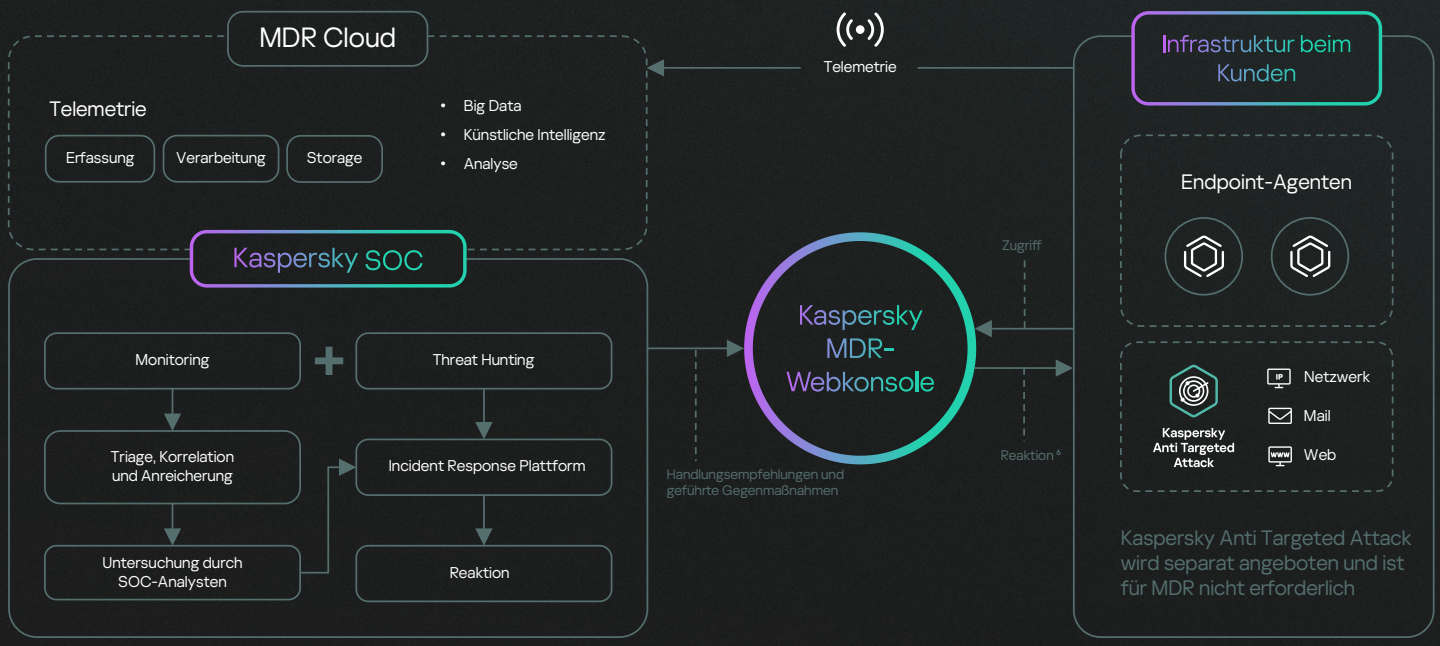
3

Wenn eine potenzielle Bedrohung erkannt wird, stuft Kaspersky MDR sie nach Schweregrad ein und benachrichtigt den Kunden per E-Mail und/oder Telegram. Die Ursachenanalyse hilft nach Möglichkeit, die Angriffsquelle zu identifizieren und gibt Empfehlungen, wie eine erkannte Bedrohung eingedämmt, abgewehrt und entschärft werden kann.

4

Kunden können die Reaktion auf Vorfälle[5] ganz oder teilweise an das Kaspersky SOC-Team auslagern. Fragen zu einem Vorfall können per Chat in der Kaspersky MDR-Webkonsole diskutiert werden.

Architektur von Kaspersky MDR



Kaspersky MDR ist mit Antiviren-Lösungen von Drittanbietern kompatibel.

[5] Ist eine eingehendere Analyse des Vorfalls erforderlich und ein aktives Abonnement von Kaspersky Incident Response vorhanden, kann der Vorfall zur weiteren Untersuchung an das Kaspersky GERT-Team weitergeleitet werden.

[6] Automatisierte Gegenmaßnahmen werden eingeleitet, falls der Kunde dies vorab im Kaspersky MDR-Portal freigeschaltet hat (andernfalls wird durch das MDR-Portal erst eine entsprechende Freigabe eingeholt).

Leistungsversprechen

Die Gewissheit, ständig vor den komplexesten und raffiniertesten Bedrohungen geschützt zu sein

Alle wesentlichen Vorteile eines Security Operations Center (SOC), ohne die Kosten und Mühen zur Einrichtung eines eigenen SOC

Insgesamt geringere Sicherheitskosten – es ist nicht nötig, mehrere teure IT-Sicherheitsexperten einzustellen und zu schulen, um verschiedene Bereiche abzudecken

Ihre eigenen IT-Sicherheitsressourcen können sich auf andere geschäftskritische Probleme fokussieren

Weltweit anerkannt

Kaspersky nimmt regelmäßig an unabhängigen Tests teil und arbeitet eng mit weltweit führenden Analystenfirmen zusammen. Kaspersky ist als führendes Unternehmen im Bereich Cybersicherheit weltweit anerkannt, und Kaspersky MDR hat, wie alle unsere Produkte, zahlreiche Auszeichnungen erhalten. Die leistungsstarken Erkennungs- und Abwehrfunktionen von Kaspersky MDR werden durch einzigartige Expertise ergänzt. Das hochqualifizierte Kaspersky SOC-Team ist eines der erfolgreichsten und erfahrensten Threat Hunting-Teams in der Branche.

Kaspersky Managed Detection and Response

Weitere Informationen

www.kaspersky.de

#kaspersky
#bringonthefuture