kaspersky

Kaspersky
Managed Detection
and Response

Wir stoppen Vorfälle, bevor sie ihr Geschäft stoppen

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

Kaspersky Managed Detection and Response ist ein Service von Experten, der rund um die Uhr Monitoring, Erkennung, Untersuchung sowie eine schnelle Reaktion auf komplexe Cyberangriffe bietet. Er ergänzt Ihre bestehenden Sicherheitskontrollen durch manuelle Erkennung und globale Bedrohungsinformationen. Der Service stärkt unmittelbar Ihre IT- und OT-Sicherheit, unabhängig von der Größe oder Branche Ihres Unternehmens.

Hauptvorteile

Von Anfang an genießen Sie kontinuierlichen, zukunftsweisenden Schutz für Ihre gesamte Angriffsfläche – Endgeräte, Netzwerk, Cloud und mehr.

Ein rund um die Uhr einsatzbereites SOC mit einem globalen Expertenteam: Sie müssen kein eigenes internes Sicherheitssystem entwickeln, pflegen oder Personal dafür bereitstellen.

Entlastung für Ihr internes Sicherheitsteam, da Sie Monitoring, Triage und Untersuchung an uns delegieren.

Ergebnisorientierte Sicherheit, die menschliches Fachwissen, Bedrohungsinformationen und KI kombiniert. So können Sie Vorfälle stoppen, bevor sich diese auf Ihr Unternehmen auswirken.

Unternehmen jeder Größe stehen unter Druck. Faktoren wie Homeoffice, die schnelle Entwicklung von Methoden zum digitalen Informationsaustausch, der weltweit zunehmende Mangel an Fachkräften und eine wachsende Zahl von Cyberbedrohungen, die traditionelle automatisierte Kontrollen umgehen können, tragen dazu bei. In diesem Umfeld ist es entscheidend, schnell und effektiv auf jeden Vorfall zu reagieren.

Ein Überblick über die Cyberbedrohungen von heute[1]

1 Erstangriffsvektoren

31 % gültige Konten

13 % vertrauensvolle Beziehung

39 % Ausnutzen einer öffentlich zugänglichen Anwendung

2 Dinge proaktiv erledigen

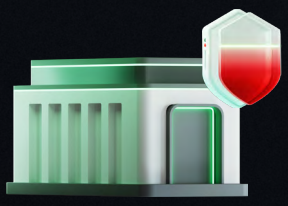
Angreifer verwenden häufig legitime Tools (wie Mimikatz, PsExec, SoftPerfect Network Scanner) in Infrastrukturen, in denen angemessene Kontrollen für die Systemkonfiguration fehlen.

3 Auswirkung

42 % verschlüsselte Dateien

17 % Datenlecks

11 % Persistenz installiert für künftige Auswirkungen



Es ist erwiesen, dass Angreifer nach einem erfolgreichen Angriff häufig zurückkehren.

Dauer des Angriffs

Schnell 45 %	Durchschnittlich 20 %	Lang andauernd 35 %
Bis zu 1 Tag	13 Tage	253 Tage

> Kaspersky MDR hat erfolgreich einen Zero-Day-Angriff erkannt und gestoppt. Andernfalls hätte dieser zu schwerwiegenden Störungen unseres Betriebs führen können.

GTO Grandeza de México

Daniel Huerta Santos
Cybersecurity Manager, Regierung des Bundesstaates Guanajuato, Mexiko

Weitere Informationen

1 Kaspersky MDR and Incident Response Report

Das bietet Kaspersky MDR

Kontinuierlicher Schutz vor komplexen Bedrohungen vom ersten Tag an

Kaspersky MDR ist in wenigen Minuten einsatzbereit, ohne dass zusätzliche Infrastruktur erforderlich ist. Der Service stützt sich auf unsere SOC-Analysten und Bedrohungsinformationen, um eine mehrschichtige Erkennung über verschiedene Domänen hinweg zu ermöglichen. Die Lösung basiert auf Milliarden von Telemetriesignalen und ermöglicht eine proaktive Bedrohungssuche, die Untersuchung der Ursachen sowie eine vollständige und schnelle Behebung. Somit bietet sie vom ersten Tag an Schutz vor bekannten Bedrohungen und Zero-Day-Angriffen.

Anwendungsfälle

- 24/7-Komplettschutz für Unternehmen ohne SecOps
- Gemeinsam verwaltete SecOps zur Unterstützung interner Cybersicherheitsteams
- Fortschrittlicher Schutz für OT-Infrastruktur
- Dedizierter kontinuierlicher Schutz für Embedded Systems

Durch Experten angeleitete Sicherheitsmaßnahmen, ergänzt durch Bedrohungsinformationen

Globale Experten mit umfassender Praxiserfahrung und branchenführenden Zertifizierungen verwalten Ihre Sicherheitsmaßnahmen mit Kaspersky MDR. Ihre Arbeit wird durch marktführende Threat Intelligence- und KI-Mechanismen ergänzt, die in den Service integriert sind. Diese tragen dazu bei, jede Warnmeldung mit Informationen anzureichen, die Erkennung zu beschleunigen und die mittlere Zeit bis zur Reaktion (MTTR) zu verkürzen.

30 Minuten
ist unsere durchschnittliche MTTR [2]

30 %
aller empfangenen Warnungen werden von AI Auto Analyst bearbeitet [1]

Betriebliche Effizienz und Vorhersagbarkeit von Kosten

- Kaspersky MDR beendet die Komplexität und die Kosten, die mit dem Aufbau eines vollständig neuen internen SOC verbunden sind. Dieser Prozess belastet Ihr Budget und verzögert sinnvolle Sicherheitsverbesserungen um Monate oder sogar Jahre.
- Wenn Sie bereits über ein eigenes SOC verfügen, übernimmt der Service die Rund-um-die-Uhr-Überwachung, die Priorisierung von Warnmeldungen und die Klassifizierung von Vorfällen. So können sich Ihre Analysten auf wertschöpfendere, strategische Aufgaben konzentrieren.

Bis zu 15 Minuten
dauert die Aktivierung von Kaspersky MDR

Bis zu 2 Jahre
dauert der Aufbau eines vollständig neuen internen SOC

70 %
der Sicherheitsteams haben Schwierigkeiten, mit der großen Anzahl von Warnungen Schritt zu halten, die von ihren Tools zur Sicherheitsanalyse generiert werden. [3]

Monitoring

- Endpoints
- Network
- ICS-Workstations
- Cloud
- Embedded Systems

Kompatibilität mit EPP-Anwendungen von Drittanbietern

Erkennung

Mehrschichtige Bedrohungserkennung

- Endpoint Detection-Technologien
- Anreicherung durch Threat Intelligence
- AI Auto Analyst
- Proaktives Threat Hunting

~30 %
aller empfangenen Warnungen werden von AI Auto Analyst bearbeitet [1]

>3.000
Regeln für die Bedrohungserkennung

Response

30 Minuten
Mittlere Zeit bis zur Reaktion*

Alle Reaktionsmodi

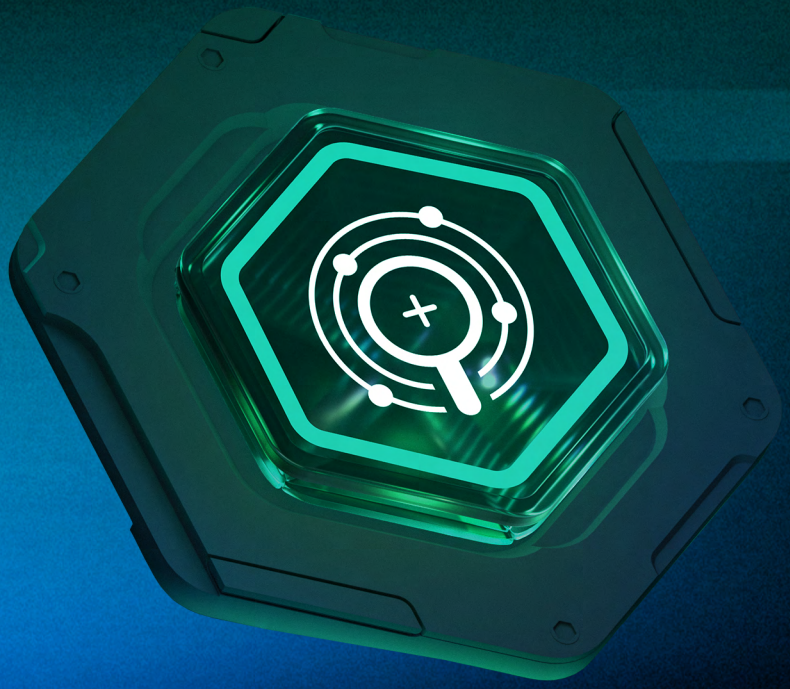
- Manuelle Genehmigung
- Vorab genehmigt
- Empfehlungen

Security Analysten | Detection Engineers | Incident Responder | Threat Researcher | Reverse Engineers | Threat Hunter | Digital Footprint Intelligence Analysts | Security Automation Engineers | Forensiker

24/7-Schutz durch Kaspersky SOC

2 Laut unseren jährlichen MDR-Analystenberichten

3 A portrait of the modern information security professional, 2024



Kaspersky Managed Detection and Response

Termin für Demo vereinbaren

www.kaspersky.de

#kaspersky
#bringonthefuture