ENDPOINT DETECTION AND RESPONSE VON KASPERSKY

EDR

kaspersky

Kaspersky bietet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und neu aufkommenden Cyberbedrohungen. Die fortschrittlichen Kaspersky-Technologien wurden vielfach ausgezeichnet.

Endpoint Detection and Response, kurz EDR, fügt dem Endpoint-Schutz weitreichende Fähigkeiten der Datenkorrelation und Analyse hinzu. Mit diesen Informationen können intelligente Algorithmen, häufig als KI bezeichnet, trainiert werden und verdächte Vorgänge erkennen. Je nach Einstellungen bzw. Ausprägung wird verdächtiges Verhalten zur weiteren Analyse gemeldet oder automatisch unterbunden.

Doch warum ist das nötig? – Moderne Cyberbedrohungen sind so schnelllebig und vielseitig, sodass sowohl signatur- als auch verhaltensbasierte Schutzmaßnahmen an ihre Grenzen stoßen. Die Bedrohungen tarnen sich häufig, indem Sie legitime Tools, wie PowerShell, zur Erfüllung ihrer Aufgaben nutzen. Sie verschleiern so ihre wahren Absichten und können nur im Zusammenhang der einzelnen Vorgänge erkannt werden.

91 % aller Organisationen sind im Laufe des Jahres 2019 Opfer von Cyberangriffen geworden, wobei 1 von 10 einem gezielten Angriff[1] ausgesetzt war.

In den meisten Unternehmen fehlt die nötige Transparenz und das erforderliche Fachwissen. Auch reicht es nicht mehr, Bedrohungen einfach zu neutralisieren, ohne den Ursprung zu finden und zu beheben.

Stufenweiser Cyber-Sicherheitsansatz

Stufe 3 Integrierter Sicherheitsansatz

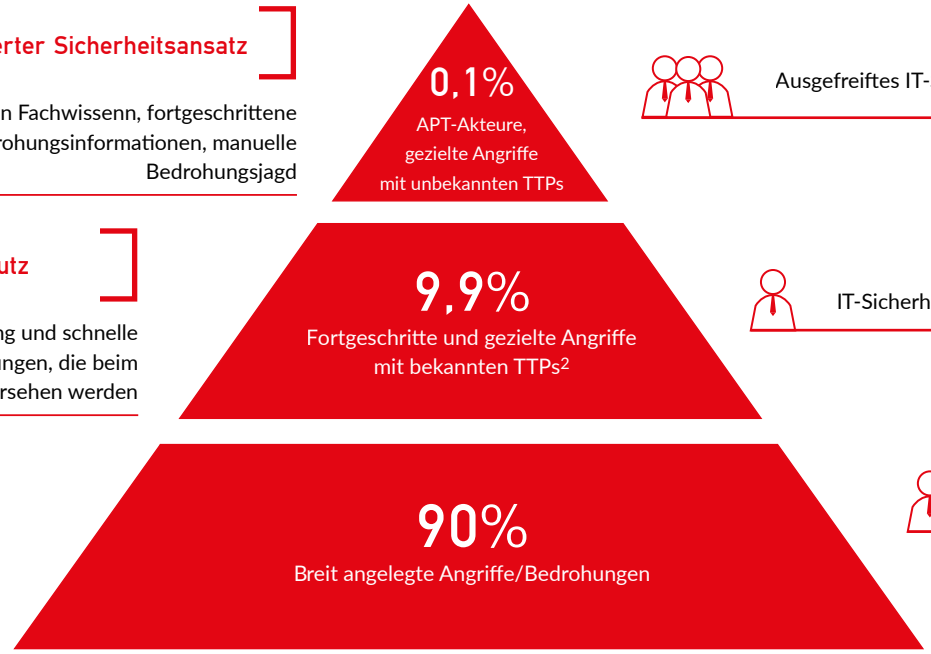
Hohes Maß an Fachwissenn, fortgeschrittene Nutzer für Bedrohungsinformationen, manuelle Bedrohungsjagd

Stufe 2 Erweiterter Schutz

Fokus auf automatische Erkennung und schnelle Reaktion auf komplexe Bedroungen, die beim präventiven Schutz übersehen werden

Stufe 1 Grundlagen der Sicherheit

Automatisierte Präventionstechnologien, um die größtmögliche Anzahl von Bedrohungen zu blockieren



Ausgefreiftes IT-Sicherheitsteam oder SOC

IT-Sicherheitsverantwortlicher/CISO

IT-Verantwortlicher

www.kaspersky.com

1 Der Kaspersky-Bericht zu globalen IT-Risiken, Kaspersky, 2019
2 Tactics, Techniques, and Procedures

8SOFT
Experts Security Distribution

Mit mehr als 18 Jahren Expertise sind wir Ihr kompetenter und zuverlässiger Cybersecurity Distributor mit Herz.

Sie erhalten von uns ausschließlich exklusive Produkte namhafter Hersteller, die unseren Praxistest bestanden haben. Aktuell sind dies:

APPTEC360,
C-IAM,
CLAVISTER
ESET,
FUDO SECURITY,
KASPERSKY
und SEP HYBRID BACKUP.

Mit unseren Lösungen und Services möchten wir Ihnen weitere Wachtsumschancen bieten, Sie in Ihrem täglichen Business unterstützen und dazu beitragen, Sie noch erfolgreicher zu machen.

Stellen Sie sich die Bausteine für Ihren Erfolg in unserem Partnerprogramm zusammen und profitieren von der Kraft der 8Soft-Gemeinschaft.

8Soft GmbH
Prymstraße 3
97070 Würzburg
T. +49 931 250 993 20
M. info@8soft.de

www.8soft.de

SO FUNKTIONIERT EDR

Vorfall

Indenfikation verdächtigen Verhaltens

Datenkorrelation

Vorfalls-/Warnhinweiskarte erstellen

Reaktion

Blockieren aller beteiligten externen IP-Adressen

Ursachen und Einfallstore identifizieren

Sicherheitsregeln anpassen

Wiederherstellung

Auflösen der Host-Isolation

TIPP

Entwickeln Sie Ihre eigene Fähigkeit zur Reaktion auf Vorfälle mit einem einfach zu bedienenden Endpoint Detection and Response (EDR)-Toolset, dass zu Ihnen passt und mitwächst.

Analyse

KES Bedrohungserkennung

Code Injection

Prozess, der einen anderen Prozess startet

Dateierstellung

Netzwerkverbindungen

Registry-Änderungen

Eingrenzung

Host isolieren

Scan des Hosts starten

Datei-Ausführung im Netzwerk verhindern

Hinzufügen der Datei zur Whitelist/Analyse in KL

Beseitigung

Scannen nach IOC

Automatische oder “Single-Click”-Aktionen

Datei löschen/ in Quarantäne

Prozess terminieren

www.kaspersky.com

8SOFT
Experts Security Distribution

8Soft-Services für Kaspersky-Partner

- Unterstützung bei Marketingkampagnen
- Persönliche vertriebliche Ansprechpartner
- Technischer Support, auch mehrsprachig
- Sales-Support für Angebote, Projektregistrierungen
- Kaspersky Schulungen (Vertrieb/Technik, online/ vor Ort)
- Durchführung von technischen & vertrieblichen Webinaren für Endkunden
- Technische Begleitung bei Terminen vor Ort
- Begleitung bei PoCs
- Umfangreiche technische Dienstleistungen, Installation, Konfiguration & Richtlinienerstellung

www.8soft.de

Funktionsumfang der EDR-Varianten

	Automated EDR	EDR Optimum	EDR Expert	XDR
Erweiterte Erkennung	Schutz gegen bekannte, unbekannte und dateilose Bedrohungen, Ransomware			
Reaktionen auf erkannte Bedrohungen	Automatisierte Reaktion (Blockieren von Bedrohungen, Verbindungen ins Internet, Client Isolation, Quarantäne,...) und Wiederherstellung (Roll-back)			
Suche nach IoC[1]	Nur Hash-basiert	Ja, verschiedene Arten von IoC, auch Import von Open IoC		
Suche nach IoA[2]	Nein		Ja	
Analyse und Reaktion	Nein	Ursachenanalyse mit vollständdger Ereigniskarte	Weitreichende Ursachenanalyse zum aktiven Threat Hunting	
Threat Hunting	Nein		Ja	
Datenerfassungsbereich	Endpoint			Enpoint, Netzwerk, Mail
Managed Detection and Respone Add-On	Vorbewertung und Behebung der Sicherheitsvorfälle durch das SoC Team des Herstellers in Abhängigkeit der eingesetzten Lösungen			

1 Indicator of compromise
2 Indicator of attack

DREIFACH MEHR SICHERHEIT DURCH EDR

Erweiterte Erkennung:
- Auf Maschine-learning basierende Verhaltensanalyse zur schnellen und präzisen Erkennung von verdächtigen Verhaltensweisen
- Automatische Bedrohungssuche basierend auf Angriffsindikatoren (IoCs)
- Automatischen Reduzierung der Angriffsfläche durch adaptive Anomaliekontrolle, angepasst an die Gewohnheiten der Mitarbeiter

Automatisierte Reaktion:
- Die 'Ein-Klick'-Reaktion ermöglicht das schnelle Eindämmen von Bedrohungen
- Geführte Reaktion mit der Erfahrung der Kaspersky-Experten, mit denen Sie auch komplexere und gefährlichere Bedrohungen abwenden
- Automatisierte und endpunktübergreifende Reaktion auf analysierte oder importierte Angriffsindikatoren (IoCs)

Vereinfachte Untersuchung:
- Alle Informationen zu einem Vorfall werden automatisch in einer einzigen Ereigniskarte zusammengefasst
- Visualisierung und Drill-Down-Menüs erlauben eine schnelle und effiziente Analyse des Vorfalls in einer einzigen Umgebung und über das weitere Vorgehen zu entscheiden

www.kaspersky.com

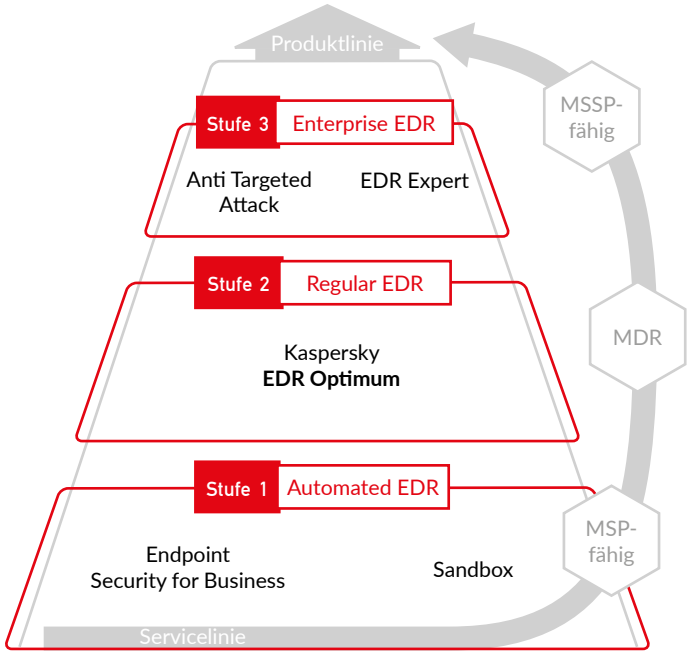
Genau die Lösungen, die für Ihre Kunden am besten passen und Services obendrein

Das Kaspersky Portfolio unterstützt Sie beim **Aufbau einer integrierten Verteidigungsstrategie gegen komplexe Bedrohungen**.

Die ressourcenschonende Lösung EDR Optimum ist ideal für kleine IT-Sicherheitsteams mit grundlegenden Fachkenntnissen, die die Unternehmenssicherheit verbessern wollen.

Kaspersky bietet darüber hinaus Tools, die die Übernahme manueller Threat-Hunting-Techniken durch ein ausgestattetes Team mit tiefem Wissen in spezifischen Themen wie digitale Forensik und Malware-Analyse bereits beherrschen. Alle Produkte können mit Managed Detection and Response Services (MDR) von Kaspersky unterstützt werden.

Mithilfe von **EDR in Kombination mit einer unübertroffenen fachlichen Beratung, Bewertung, Bedrohungsanalyse und Threat Intelligence und Schulungen durch führende Experten** erhalten Sie das Maß an Sicherheit, das zu Ihrer Organisation passt.



SOFT
Experts Security Distribution

8Soft-Services für Kaspersky-Partner

- Unterstützung bei Marketingkampagnen
- Persönliche vertriebliche Ansprechpartner
- Technischer Support, auch mehrsprachig
- Sales-Support für Angebote, Projektregistrierungen
- Kaspersky Schulungen (Vertrieb/Technik, online/vor Ort)
- Durchführung von technischen & vertrieblichen Webinaren für Endkunden
- Technische Begleitung bei Terminen vor Ort
- Begleitung bei PoCs
- Umfangreiche technische Dienstleistungen, Installation, Konfiguration & Richtlinienerstellung

www.8soft.de