

„Supply-Chain“-Angriffe:

**Wie schnell können Sie
diese erkennen?**

Was ist ein „Supply Chain“- Angriff ?...



Allgemein:

Supply-Chain-Angriff (Lieferketten-Angriff)
= meist Cyberangriff auf die Zulieferkette

Anstatt ein bestimmtes Unternehmen direkt ins Visier zu nehmen, werden Schwachstellen bei Lieferanten und Drittanbieter angegriffen.

- Angriff selbst geht gegen Dritte (indirekt)
- Kann sich gegen Personen/Firmen (via Social Engineering), Netzwerk, Hardware oder Software richten
- Nicht neu – bereits im militärischen Bereich wurden Nachschub-Linien angegriffen
- Im IT-Bereich wurde dies erstmals 1983 von Ken Thompson in seinem Paper *'Reflections on Trusting Trust'* beschrieben.

1

Warum sind „Supply Chain“- Angriffe gefährlich ?...

Besonders bedrohlich (bleiben oft unbemerkt, meist eine große Anzahl von Opfern)

Beispiele:

- **2017** Ransomware ExPetr (auch NotPetya) – kompromittiertes Updatesystem d. Buchhaltungssoftware M.E.Doc ¹
- **2020** SolarWinds Angriff – bössartiger Code und Backdoor im Update der NW-Mgmt.-Plattform "Orion" von SolarWinds
- **2021** Kaseya Angriff – REvil Verschlüsselungs-Trojaner getarnt als Sicherheitsupdate. Auch MSP's und deren Kunden betroffen
- **2023** 3CX-Angriff – trojanisierte Programmversion hatte legitimes Zertifikat von 3CX Ltd. ²
- auch Privat-Leute – z.B. **2018** Piriform CCleaner Attack – kompromittierte Kompilierungs-Umgebung der Entwickler ³
- auch HW – z.B. **2024** Pager-Attacke in Libanon (Hisbollah)

Quelle: (1) <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>

(3) <https://www.kaspersky.com/blog/ccleaner-supply-chain/21785/>

(2) <https://www.kaspersky.de/blog/supply-chain-attack-on-3cx/29961/>

SolarWinds-Hack

Der Spionagefall des Jahres

Experten sprechen von einem historischen Hack: Unbekannte haben die Computersysteme Tausender US-Behörden und Unternehmen kompromittiert. Auch in Deutschland gibt es Betroffene.

Von **Patrick Beuth**
18.12.2020, 18.37 Uhr

Angriff: kompromittierte Software-Update-Infrastruktur der IT-Management-Plattform *Orion* von SolarWinds

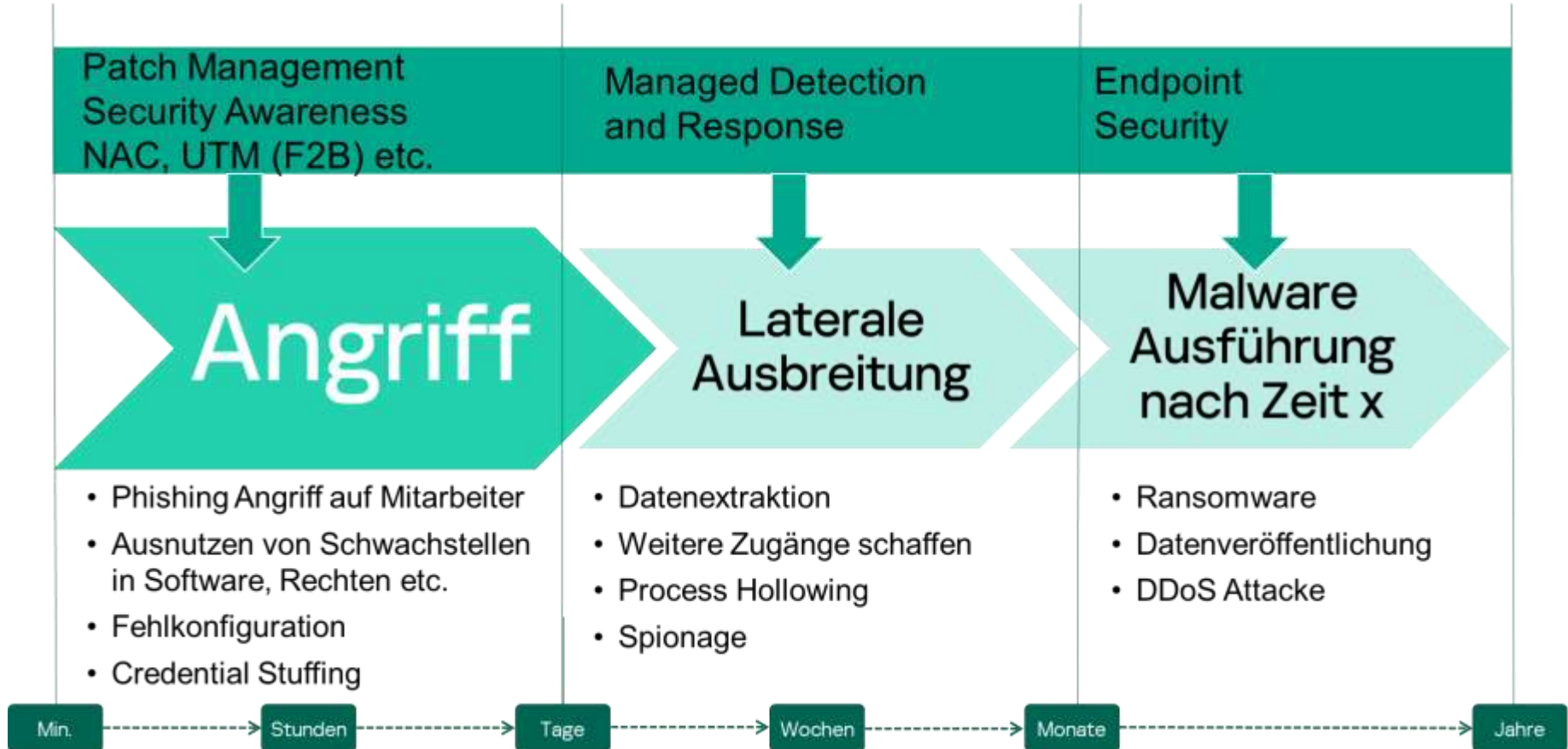
Durch infizierte Software-Updates wurden Malware in die Systeme von über 18.000 Kunden eingeschleust.

Auswirkungen: Betroffen waren u.a. Microsoft, Cisco, FireEye sowie Behörden wie z.B. US-Finanzministerium, Heimatschutzministerium

Ziel: Informationsdiebstahl und Cyber-Spionage, Verdacht auf staatlich geförderte Hacker aus Russland (APT29, auch als *CozyBear* bekannt)

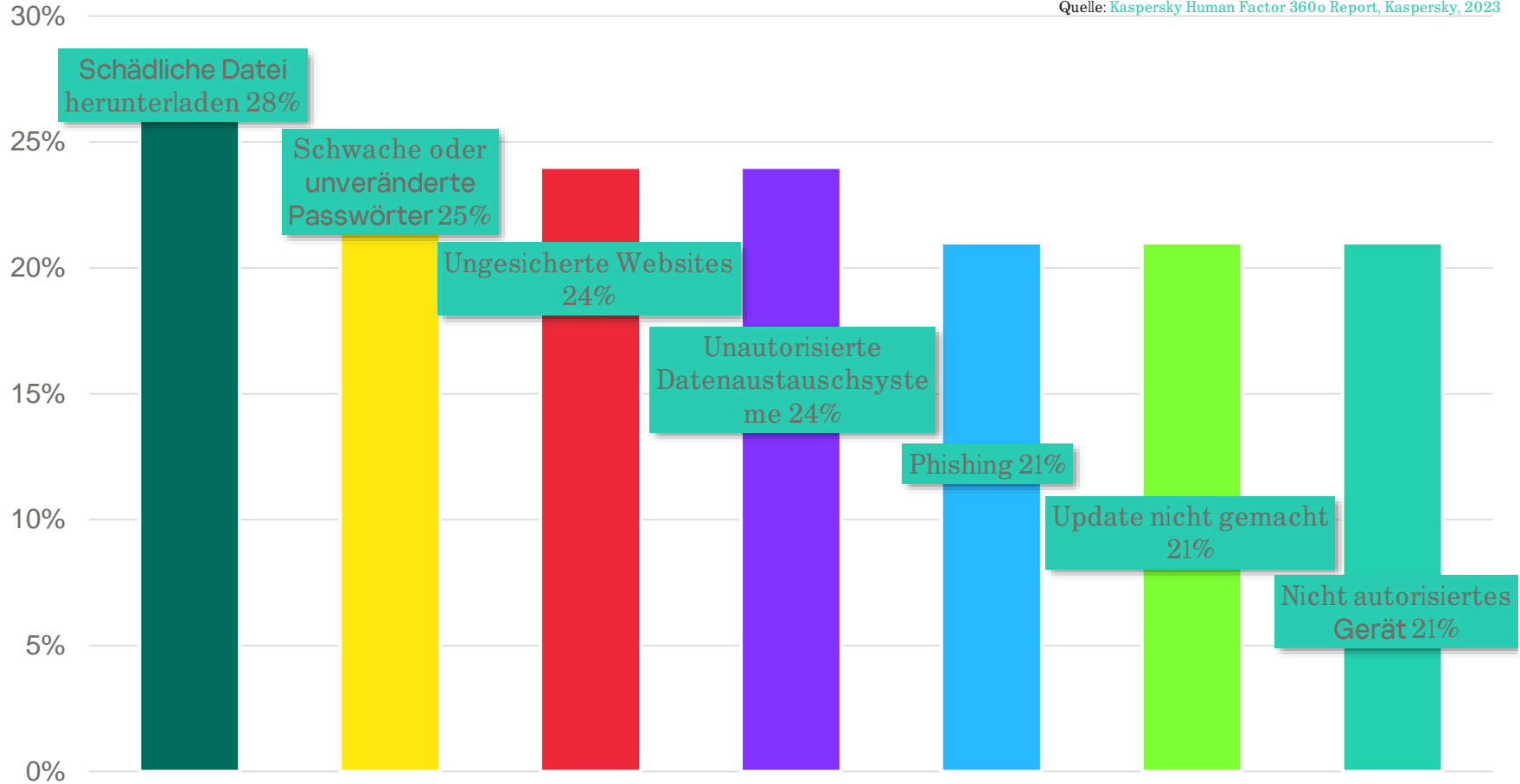
Kaspersky berichtete in seinem Blog:

<https://www.kaspersky.com/enterprise-security/mitre/apt29>



Wie haben Mitarbeiter Incidents verursacht? (Top 7 Gründe)

Quelle: [Kaspersky Human Factor 360o Report, Kaspersky, 2023](#)



„Supply Chain“- Angriffe und die Folgen



Finanzielle Verluste

- z.B. Betriebsausfälle, Datenverlust und finanziellen Einbußen → Unternehmen müssen ggf. für Wiederherstellungs-maßnahmen aufkommen

Betriebsstörungen

Reputationsschäden

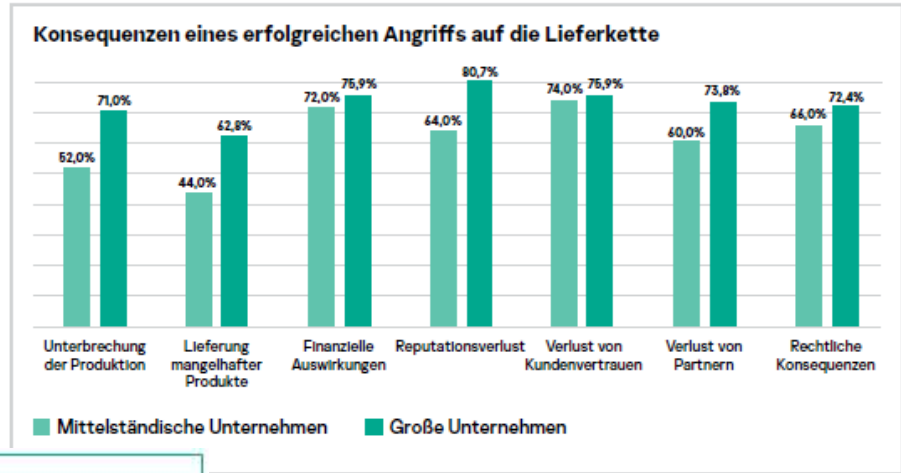
Datensicherheits-Verletzungen

- Angreifer können sensible Daten stehlen inkl. geistiges Eigentum, Kundeninformationen, Geschäftsgeheimnisse etc.
→ ggf. rechtliche Konsequenzen

Regulatorische Probleme

- Einhaltung von gesetzliche Vorschriften zur Meldung von Datenschutzverletzungen
→ Verstöße können hohe Strafen nach sich ziehen

„Supply Chain“- Angriffe und die Folgen



Anteil der Unternehmen, die nicht mit Partnern zusammenarbeiten würden, die bereits von einem Cyberangriff betroffen waren

50% der KMU

64% der Großunternehmen

kaspersky

Quelle: Kaspersky Studie „Cybersicherheit in der Supply Chain Deutschlands“

Schutz- Maßnahmen und Prävention gegen „Supply Chain“-Angriffe

Awareness

- z.B. Sensibilisierung der Mitarbeiter z.B. mit Kaspersky ASAP

Zero Trust Security

- z.B. Begrenzung des Zugriffs, Prinzip der geringstmöglichen Privilegien, Schutzfläche statt Angriffsfläche, Mikro-segmentierung, Trennung von OT- und IT-Systemen usw.

Risikomanagement, Zertifizierungen (z.B. SOC2)

- z.B. Zugriffs-Aufstellung aller Lieferanten/Partner, Audit, Überwachung externer Prozesse, Backup, Patches usw.

techn. Maßnahmen

- robuste Sicherheitslösung wie z.B. Kaspersky EPP, Kaspersky Endpoint Detection and Response (EDR), Kaspersky Managed Detection and Response (MDR) usw.

Notfallplan

- Vorbereitung auf den Fall eines erfolgreichen Angriffs, Unterstützung z.B. Kaspersky Incident Response



**Kaspersky
Next**



**Kaspersky Next
EDR Foundations**

Robuste Sicherheit für alle

Schützen Sie all Ihre Geräte

Wenn Sie Folgendes brauchen:

- Starker Endpoint-Schutz
- Grundlegende Sicherheitskontrollen
- Maximale Automatisierung



**Kaspersky Next
EDR Optimum**

Stärken Sie Ihre Abwehr

Erhöhen Sie Ihre Sicherheit durch wichtige Funktionen zur Untersuchung und Abwehr

Wenn Sie Folgendes brauchen:

- Verbesserte Sichtbarkeit und Reaktionsmöglichkeiten
- Hybrid Cloud Security
- Kontrollen auf dem Niveau von Großunternehmen



**Kaspersky Next
XDR Expert**

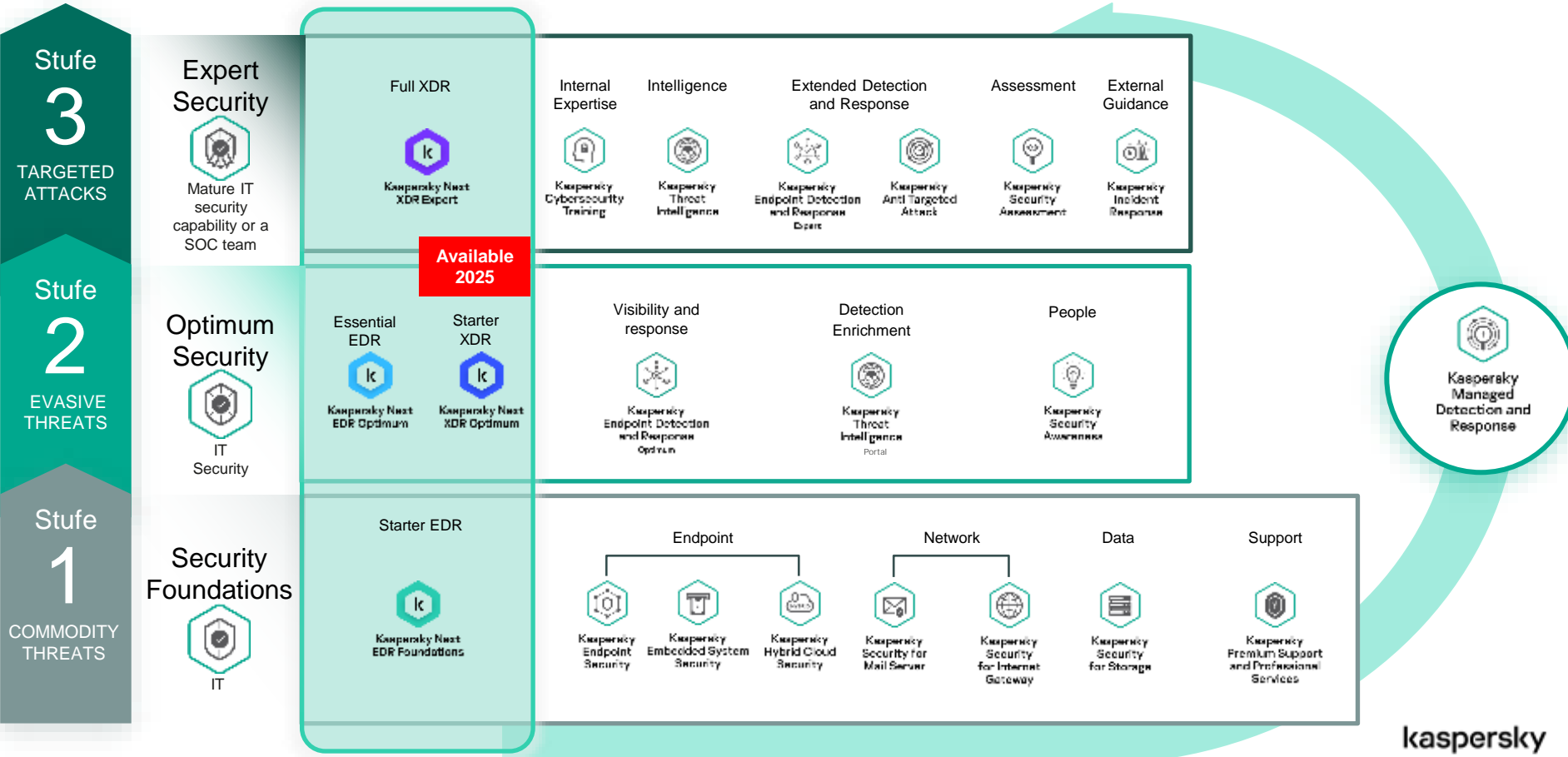
Tools für Ihre Experten

Schutz gegen komplexe, raffinierte Bedrohungen

Wenn Sie Folgendes brauchen:

- Fortschrittliche Threat Detection
- Nahtlose Integration
- Leistungsstarke Threat Hunting-Tools

Der stufenweise Ansatz von Kaspersky





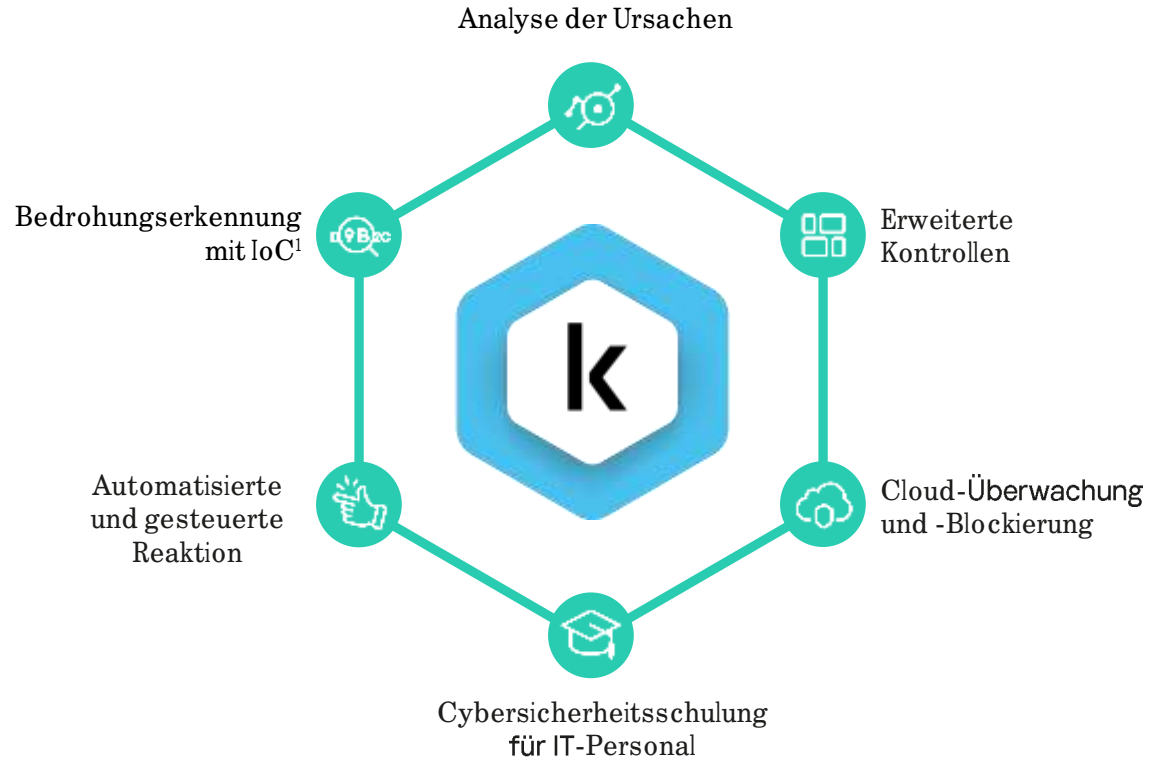
**Kaspersky Next
EDR Optimum**

Stärken Sie Ihre Abwehr

Erhöhen Sie Ihre Sicherheit durch wichtige Funktionen zur Untersuchung und Abwehr

Wenn Sie Folgendes brauchen:

- Verbesserte Sichtbarkeit und Reaktionsmöglichkeiten
- Cloud Discovery (CASB)
- Kontrolle auf dem Niveau von Großunternehmen



¹ Gefährdungsindikatoren



Kaspersky Managed Detection and Response

ist eine umfassende Lösung, die rund um die Uhr selbst vor den komplexesten Bedrohungen schützt.

- MDR als Add-on
- MDR inkludiert in **Kaspersky Next Complete**

24/7 Monitoring

für verdächtige Aktivitäten

Bedrohungserkennung und -analyse,

um zu verhindern, dass Systeme in Gefahr geraten

Priorisieren von Warnungen

So können Fehlalarme herausgefiltert und Ressourcen effizient eingesetzt werden

Threat Hunting und Vorfallsreaktion

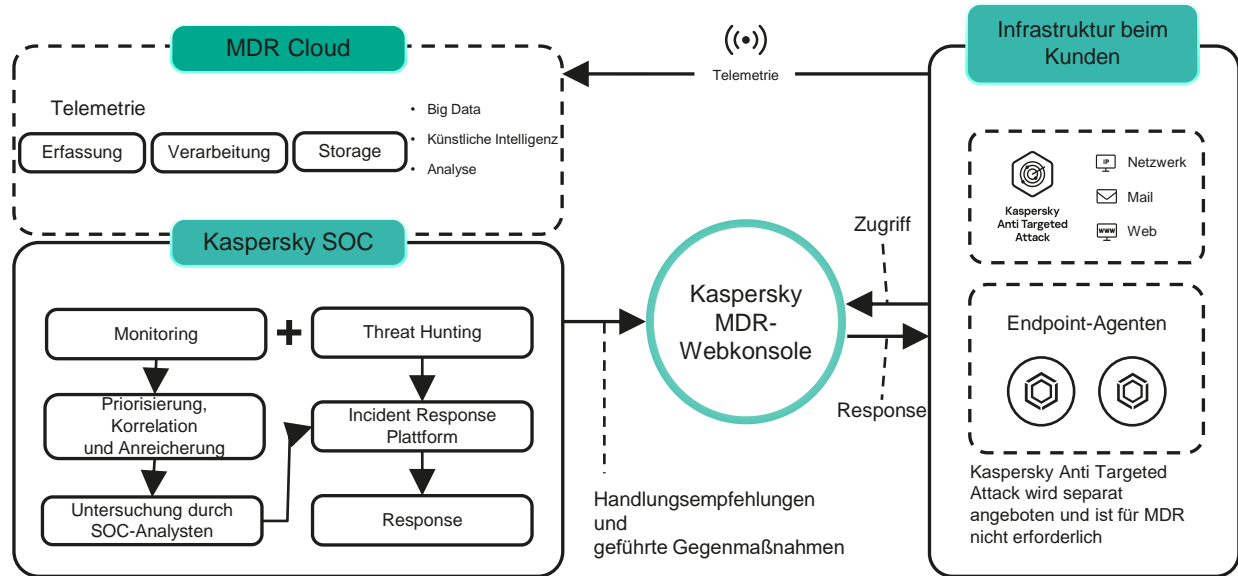
durch die Sicherheitsexperten von Kaspersky

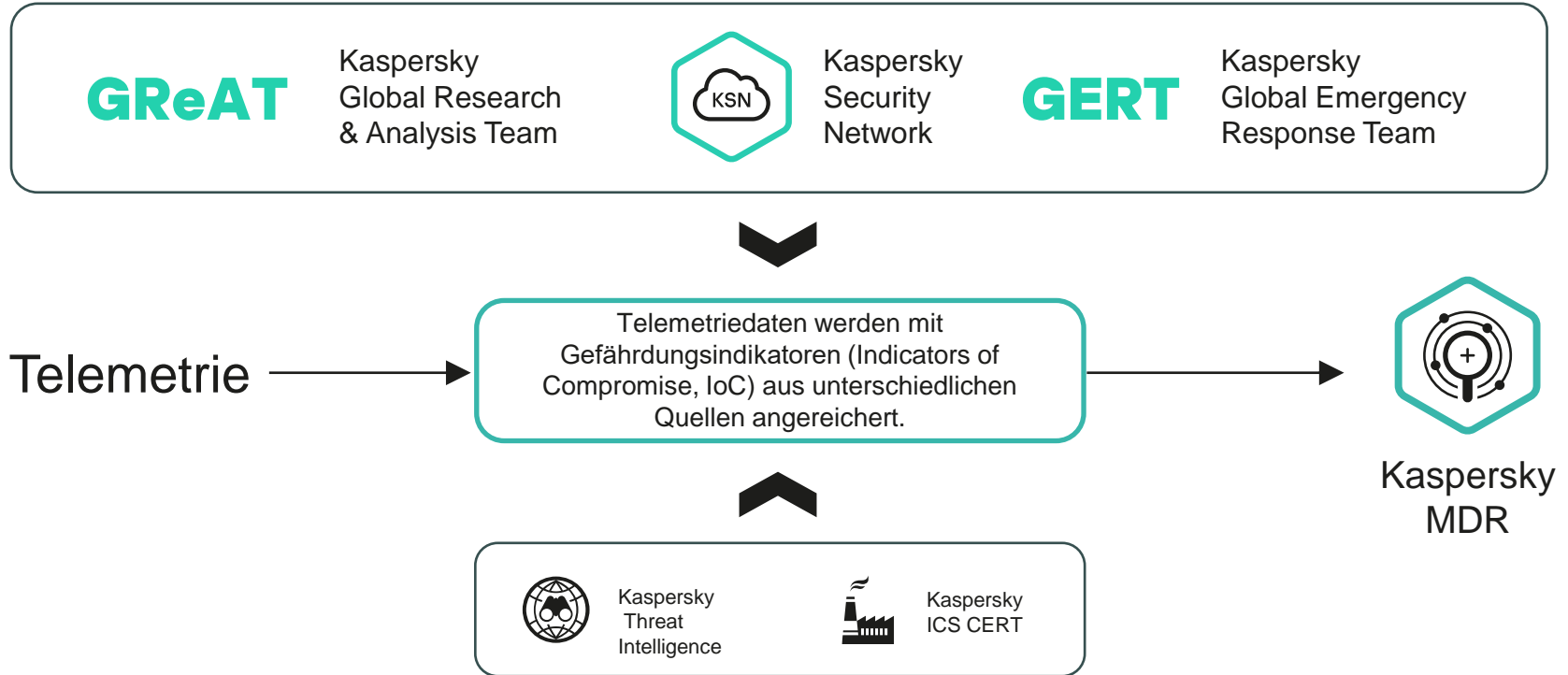
Funktionsweise von Kaspersky MDR

1 Kaspersky Endpoint Security-Lösung erfasst Telemetriedaten und leitet diese an das Kaspersky SOC weiter.

2 Die Telemetriedaten werden mit maschinellen Lernverfahren analysiert. Kaspersky SOC-Experten nehmen aktiv an der Analyse teil.

3 Das Kaspersky SOC-Team untersucht die Warnungen und informiert den Kunden über die schädlichen Aktivitäten. Es folgen Empfehlungen und eine Schritt-für-Schritt-Anleitung zur Abwehr.





Kaspersky Next Complete Security



...hilft bei der **schnellen und ressourcen-schonenden Abwehr** von Angriffen und bietet starken Endpunktschutz und -kontrolle, ergänzt durch optimale EDR-Funktionalität und Automatisierung.



...ist ein Service, der **rund um die Uhr (24x7)** Managed Protection vor Cyber-Bedrohungen und ausgeklügelten Angriffen bietet, die von automatisierten Sicherheitsmaßnahmen ggf. übersehen werden können.



**Kaspersky Next
XDR Expert**

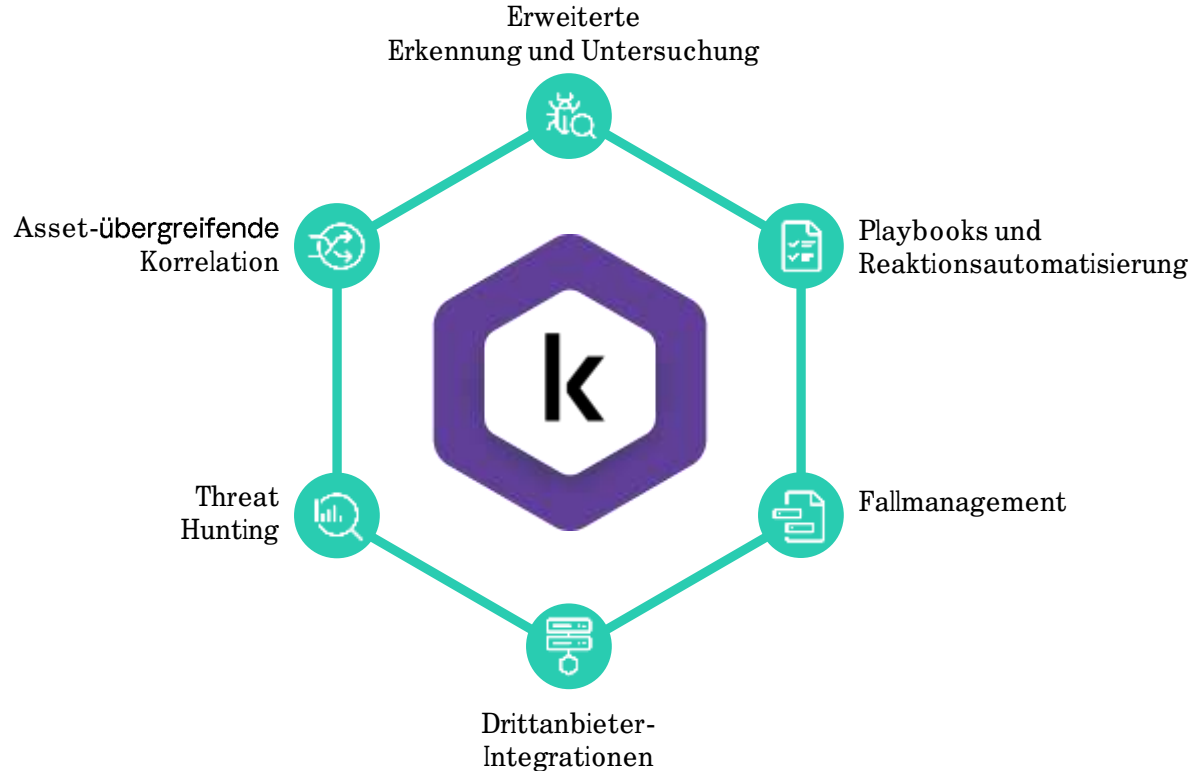
Tools für Ihre Experten

Schutz gegen komplexe, raffinierte Bedrohungen

Wenn Sie Folgendes brauchen:

- Fortschrittliche Threat Detection
- Nahtlose Integration
- Leistungsstarke Threat Hunting-Tools

Enthält
Kaspersky Next EDR Optimum-
Funktionen

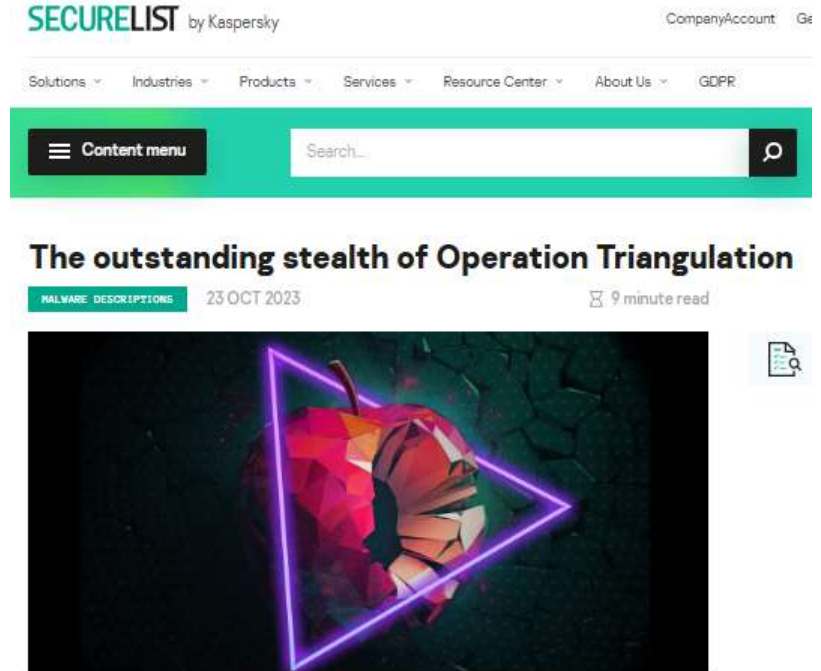


Ein paar Infos...

- High-Level APT auf **Apple iPhones** und **iPads**
- **0-Klick**-iMessage-Angriff (!) d.h. keine Benutzer Interaktion
- unsichtbare Nachricht auf dem Messengerdienst iMessage.
- Ausnutzung von 4 Zero-Day-Schwachstellen
- Kaspersky Researcher entdeckten auffällige Datenströme auf firmeneigenen iPhones und iPads
- Kaspersky veröffentlichte am 1. Juni 2023 eine erste Meldung zur „Operation Triangulation“

Weitere Details auf z.B. ...

- Kaspersky SECURELIST <https://securelist.com/triangulation-validators-modules/110847/>
- <https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/>



Vielen Dank
für Ihre Aufmerksamkeit !

Sprechen Sie mit uns in Halle 7, Stand 7-310

kaspersky