kaspersky bring on the future

Kaspersky Partner Kick-Off 2026

Sicherheit mit System – ein Kompass für Prävention, Reaktion und Abwehr

Roland Haberl
Detlev Narr
Mike Ritter
Michael Hirschmann
Frank Jonas
Angel Jodra

kaspersky bring on the future

Kaspersky Partner Kick-Off 2026

1. Vorbeugung – Risiken aufspüren, bevor sie zum Problem werden

Detlev Narr
Sr. Consultant Threat Intelligence

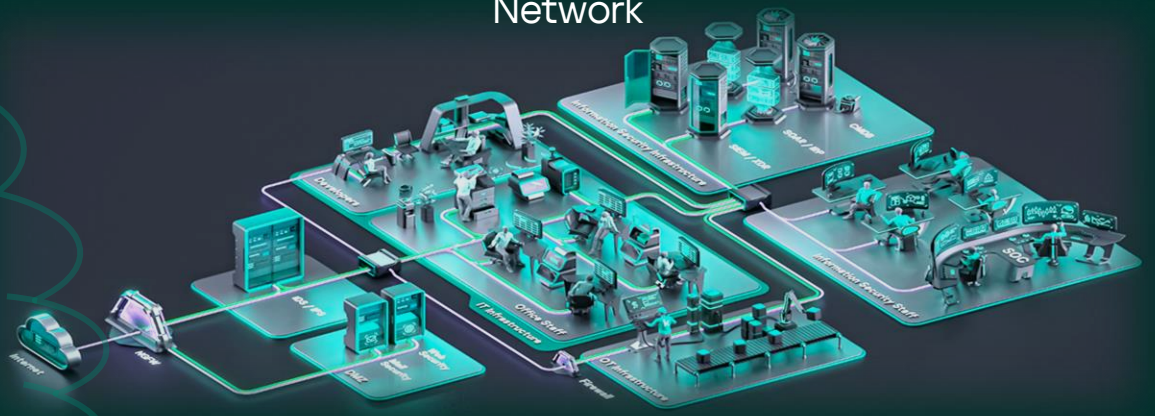
Roland Haberl
Head of B2B Germany

Attacks & Counter Measurement Options

Internet, DeepWeb, Darknet

Gateway

Client „internal“ Network



Cyberangriff Vorbereitung

Angriffs-entwicklung

Erkennung

DFI
DFM
ein EASM (inkl. Historie)

TDF

KUMA

MDR
XDR

EASM = External Attack Surface Monitoring

Digital Footprint Monitoring DFM

Wenn Dich Hacker automatisiert beobachten –
wieso machst Du das nicht?
Heutige Angreifer handeln strategisch, opportunistisch und verstörend methodisch!

Verstehen, wie eine Organisation von Angreifern gesehen wird und Kontrolle **übernehmen!**

→ Partner können dies als Service für ihre Kunden anbieten
starte mit
2nd-Level-Domains & eigenen, externen IPs o. IP-Ranges

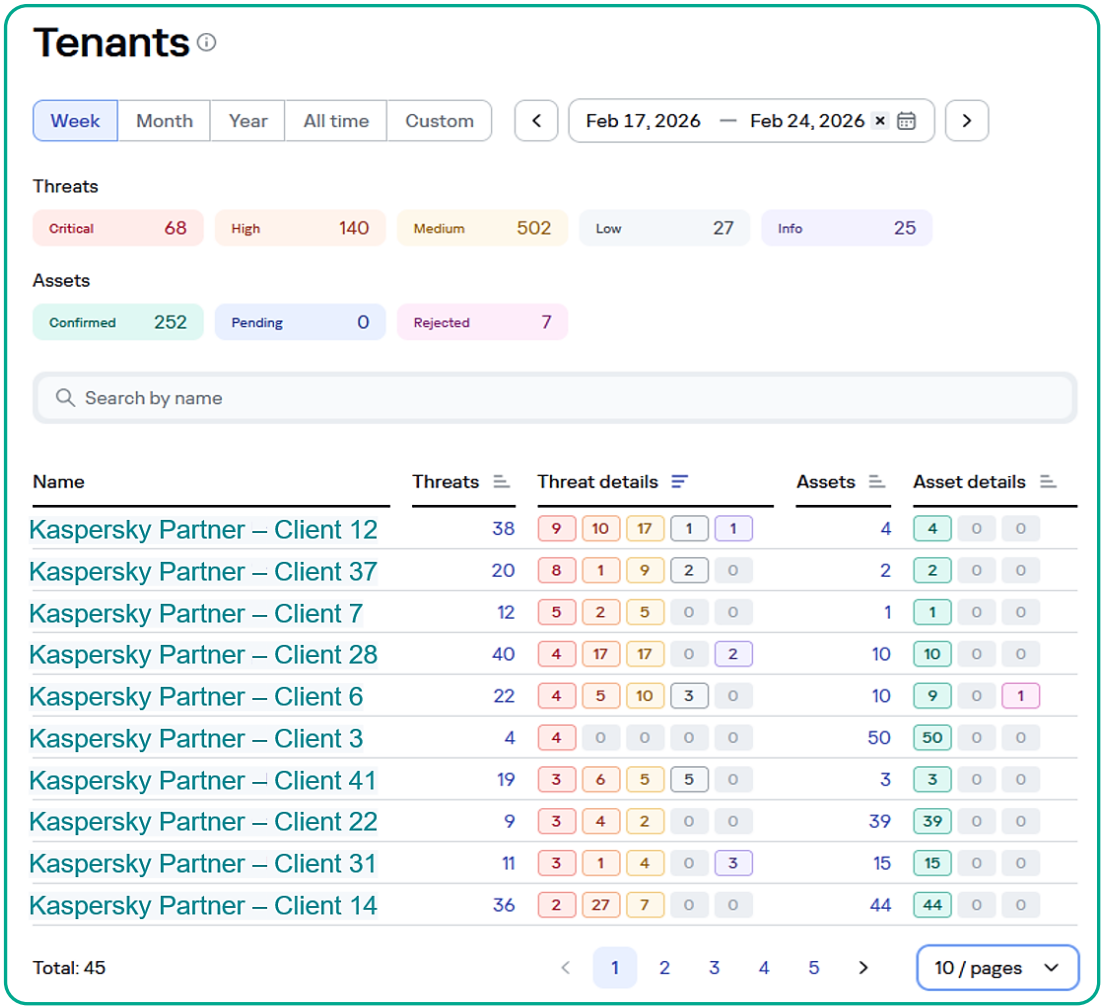
DFM

- **identifiziert, analysiert** und **überwacht** öffentlich zugängliche digitale Assets sowie die Präsenz einer Organisation
- **meldet** mögliche Datenlecks &
- **berät** hinsichtlich notwendiger Aktionen

→ PenTests zeigen eine Momentaufnahme
DFM überwacht regelmäßig

DFM im TIP – Tenant Center

- MSSP – Überblick über alle Kunden
- MSSP – Priorisiere Deine Arbeit für die Kunden
- MSSP – effektiver Einsatz der eigenen Spezialisten
- MSSP – Status-Historie



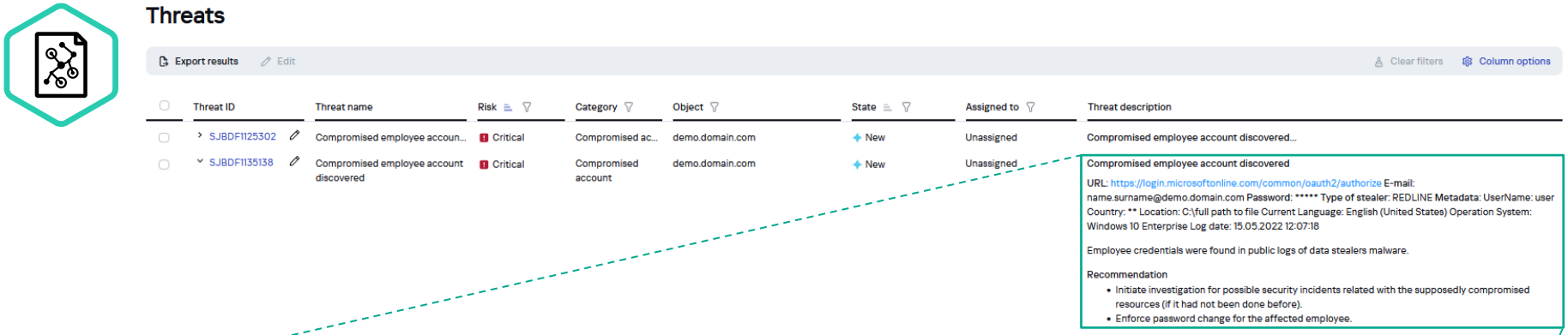
DFM / DFI – Threat-Übersicht

Threats

Export results | Edit | Clear filters | Column options

Threat ID	Risk	Date	Threat name	Category	Object	State
...F1036803	Medium	Mar 21 2025 18:22	New post on Darknet	Darknet	Database AND sell AND "USA / Europe"	Active
...F1036802	Medium	Mar 21 2025 18:22	New post on Darknet	Darknet	sell AND RDP AND access AND " sql injections"	Pending
...F1036330	Critical	Mar 21 2025 18:22	Compromised employee ac...	Compromised ...	domain2.com	New
...F1036329	Critical	Mar 21 2025 18:22	Compromised employee ac...	Compromised ...	domain.com	New
...F1036328	Medium	Mar 21 2025 18:22	Compromised credentials f...	Compromised ...	www.domain2.com	Pending
...F1036327	Medium	Mar 21 2025 18:22	Compromised credentials f...	Compromised ...	domain.com	New
...F1036326	Critical	Mar 21 2025 18:22	Vulnerable version of Open...	Vulnerability	*.*.*.*	New
...F1036325	Low	Mar 21 2025 18:22	SMB version 1 is used	Vulnerability	*.*.*.*	Pending
...F1036324	High	Mar 21 2025 18:22	SMB service is publicly avail...	Vulnerability	*.*.*.*	New

DFM / DFI – Threats im Detail



Compromised employee account discovered → **Threat-Beschreibung**
„kompromittierter Mitarbeiterzugang entdeckt“

[...]

Recommendation → **Handlungsempfehlung**

- Initiate investigation for possible security incidents related with the supposedly compromised resources (if it had not been done before)
- Enforce password change for the affected employee

DFM / DFI - USPs

Unbegrenzte Anzahl an Assets

Asset-Management mit
unbegrenzter Asset-Anzahl

Dark Web Monitoring

Analyse z. B. von Log-Daten

Handlungsempfehlungen zu fast jedem Threat

Priorisierung der Threats nach Kritikalität sowie
detaillierte Handlungsempfehlungen

Regelmäßiges Screening

Regelmäßiges Screening der festgelegten
Assets ➔ schnelle Reaktion auf aktuelle
Bedrohungen

DFM / DFI – Proof of Concept

→ Welche Infos werden benötigt?

Kundenliste mit **URLs & IPs**,
spätestens 1 Woche vor PoC-Start

→ Wie viele Kunden sollten integriert werden?

40 – 50 (mindestens 20-25)

Und warum?

PoC **Erfolgsrate knapp 50 %**
➔ Ziel von mind. 10 zahlenden Kunden,
um verhandelte Preise zu bekommen

→ 3 erfolgreiche PoCs 2025

→ 2 aktuelle PoCs

→ Mehrere geplante PoCs für 2026

➔ Ein initialer PoC ist essentiell, um den Umgang mit dem TIP zu erlernen und dieses Wissen bei aktuellen sowie bei künftigen Kunden als Verkaufshilfe zu nutzen

DFM / DFI – Wie profitieren Reseller

Umsatz und Marge!

- → Enduserpreis 2/3 unter Listenpreis, wenn 10 oder mehr Kunden zeichnen
- → Preis hängt nicht von Kundengröße ab ➔ flexible Mischkalkulation
- → Jährlich wiederkehrende Umsätze
- → White Labeling! Erstelle Deinen eigenen gebrandeten Service
- → Anschlussgeschäfte & Services (Takedown Services, Incident Response, …)

Expertenpositionierung beim Kunden!

- Beratung statt nur Produktverkauf
- Stärkung des Vertrauens → Trusted Advisor

➔ Erhöhe Deinen Umsatz mit jährlich wiederkehrenden DFM Renewals

➔ Nutze den TIP Tenant Center, um Deine Kunden strukturiert und priorisiert zu unterstützen

Vielen Dank!

Detlev Narr
Roland Haberl

Sr. Consultant Threat Intelligence
Head of B2B Germany

kaspersky

kaspersky bring on the future

Kaspersky Partner Kick-Off 2026

2. Reaktion – Gefahren erkennen und gezielt handeln

Michael Hirschmann
Senior Presales Engineer / Presales Manager

Mike Ritter
Territory Channel Manager MSP

Cyber Kill Chain in 3 Phasen

1. Phase 1 – Aufklärung / Prävention

2. **Phase 2 – Ausführung / Erkennung & Abwehr**
   Lösungen z. B.
   Kaspersky MXDR / MDR / EDR,
   Threat Hunting,
   Kaspersky Threat Data Feeds

3. Phase 3 – Incident Response / Aufräumen & Recovery

Beispiel-Phasen eines Cyber-Angriffs

Allgemein: (abhängig vom Angriff)

1. Aufklärung (Reconnaissance)
2. Vorbereitung (Weaponization)
3. Erstzugriff (Initial Access z. B. via Phishing, USB)
4. Laterale Bewegung (Lateral Movement)
5. Rechteausweitung (Privilege Escalation)
6. Persistenz (Persistence)
7. Daten-Exfiltration (Exfiltration)
8. Auswirkung (Impact, Schaden, Zielaktion)

Kaspersky Next

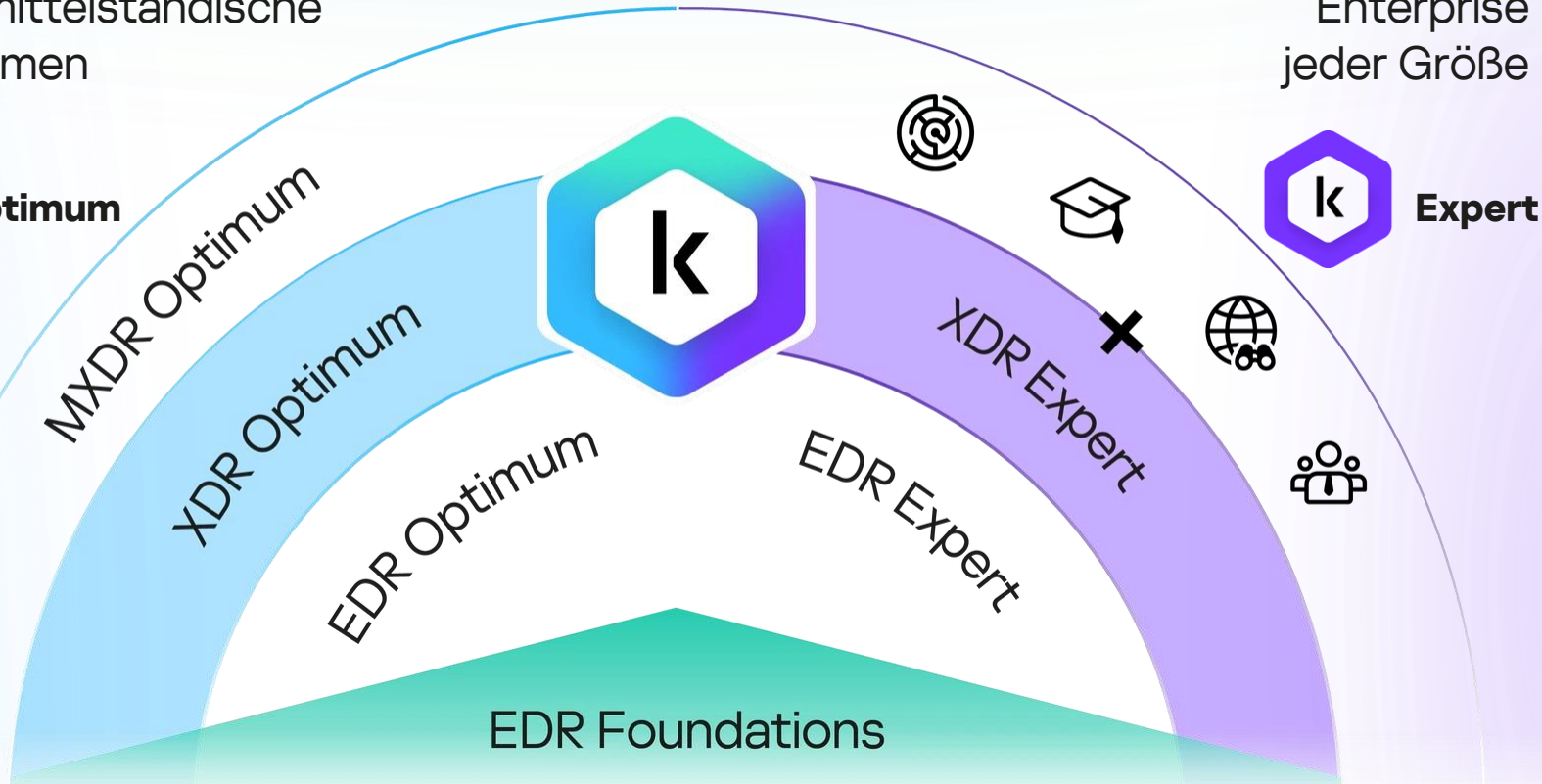
Maßgeschneiderte Sicherheit für jedes Unternehmen

Kleine & mittelständische Unternehmen

Enterprise jeder Größe

Optimum

Expert



EDR Optimum

- ☑ Schneller Einstieg, wenig Konfigurations-aufwand
- ☑ basiert auf mehrfach ausgezeichneten EP-Schutz + Device Control + AAC usw.
- ☑ Patch-Management
- ☑ Cloud Discovery & Blocking
- ☑ Data Discovery
- ☑ Microsoft Office 365-Schutz
- ☑ Cybersicherheits-Trainings für Admins (CITO)

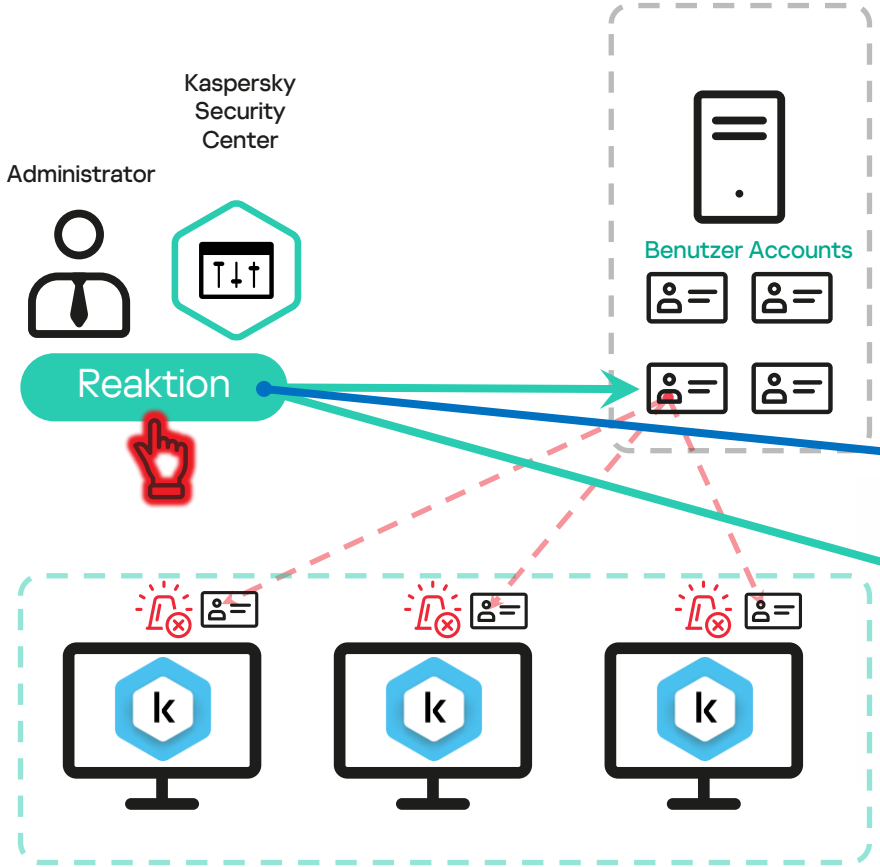
XDR Optimum

- ☑ alle „*EDR Optimum*“ Features **plus** …
- ☑ Ganzheitliche Sicht auf Bedrohungen inkl. **Alert Aggregation**
- ☑ TIP **Cloud Sandbox** für schnelle Datei-Analyse und Erkennung komplexer Angriffe
- ☑ **Active Directory** Integration
- ☑ Security **Awareness** (**ASAP**) Integration
- ☑ Zentrale Reaktion aus der KSC Alert Card

MXDR Optimum

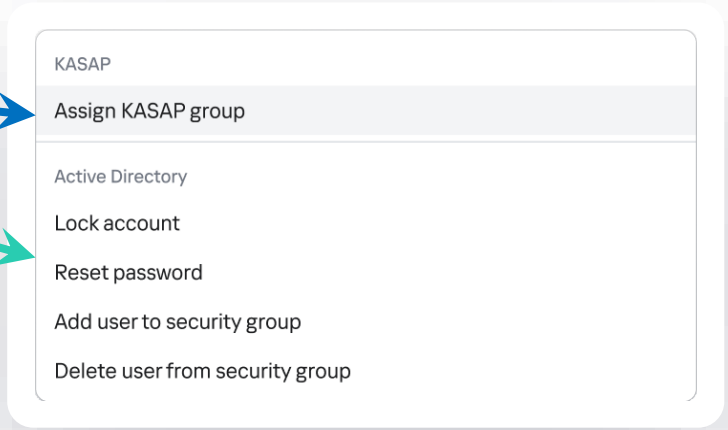
- ☑ alle „*XDR Optimum*“ Features **plus**…
- ☑ 24/7-Überwachung & Threat Hunting & IR-Reaktionen auf Angriffe, d. h. MDR

XDR/MXDR Optimum – AD- & ASAP-Integration

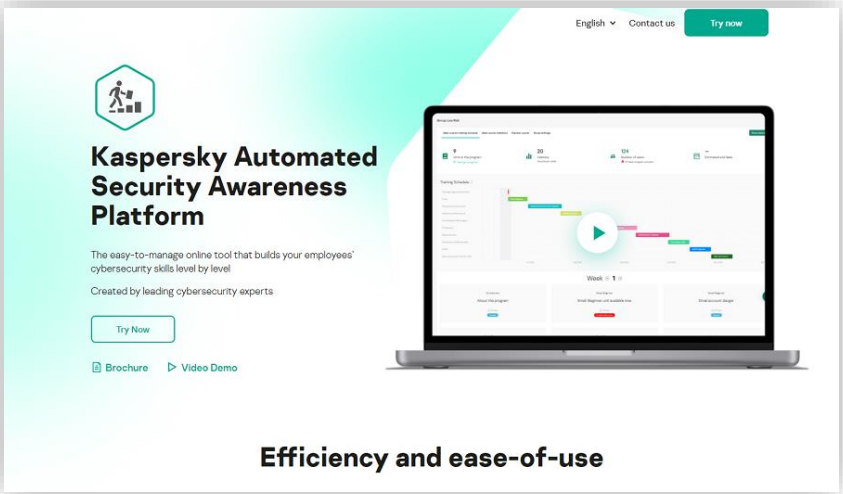


Active Directory Integration

ASAP Integration



ASAP: Überblick & News



ASAP = **A**utomated **S**ecurity **A**wareness **P**latform
Integrierte Plattform für Schulung, Assessments, Reporting und Simulierte Phishing-Angriffe

Für Organisationen jeder Größe als...

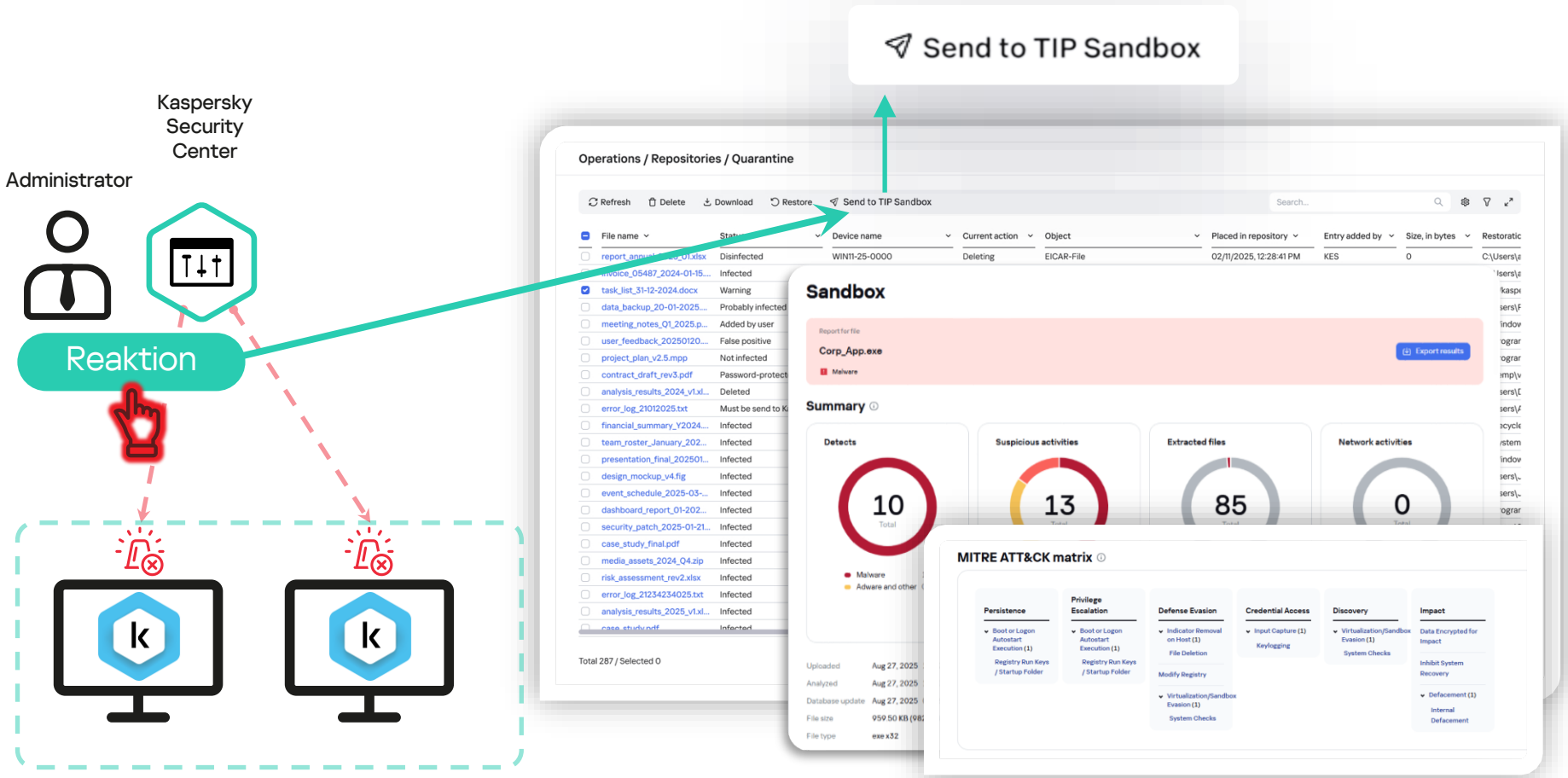
- Cloud/SaaS-Plattform (Flaggschiffprodukt)
- oder SCORM-Module (SCORM bei vorhandenen LMS)
- oder On-Premise (**NEU**)

- Einfache Einrichtung und Automatisierung
- 26 Sprachen & bis zu 4 Level (Haupt-Kurse)
- 13 Sprachen (Intensiv-/Express-Kurse)
- seit **Jan. 2026:** Hinzufügen von benutzerdefinierten, externen Inhalte z. B. Arbeitssicherheit (SCORM, .pdf)
- MSP-fähig

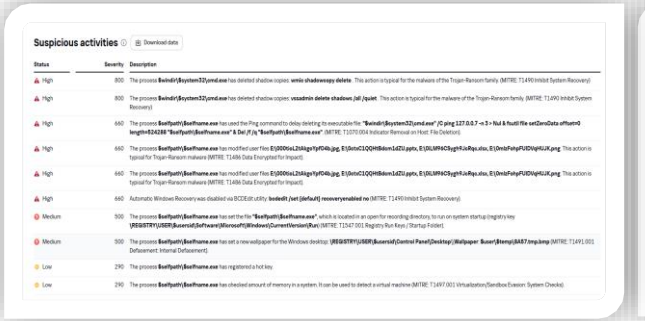
Kostenloses Trial

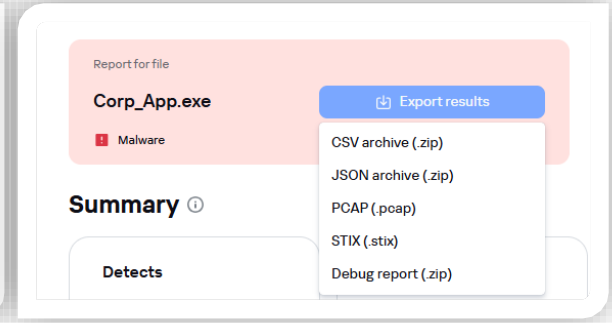
k-asap.com

XDR/MXDR Optimum – TIP Cloud Sandbox Integration



Threat Hunting mit TIP Cloud Sandbox





Überwachung verdächtiger Aktivitäten

Systemaktivitäten:

- File Operationen
- Registry Operationen
- Prozess Operationen
- Laden portabler Executables
- Netzwerk Aktivitäten (HTTP/s, FTP, IRC, DNS und andere Protokolle)

Screenshots

Die TIP Sandbox erstellt während des Emulationsprozesses entsprechende Screenshots und liefert so eine visuelle Darstellung gefährlicher Aktivitäten in einer kontrollierten Umgebung.

Exportieren von Ergebnissen

Maximieren Sie den Wert der "File Emulation Daten", indem Sie techn. Details und IOCs in verschiedenen Formaten (CSV, JSON, PCAP, STIX) exportieren, um sie mit Systemen von Drittanbietern zu teilen.

* Verfügbare Emulations-Umgebungen inkl. Windows XP, 7, 10 and Android x86, ARM

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 MXDR Optimum**

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

Mehr Details: https://www.kaspersky.com/enterprise-security/managed-detection-and-response

Lizenzierung – kurz zusammengefasst

Kaspersky NEXT Produkte werden pro Benutzer lizenziert
Je nach Next-Stufe umfasst **1** Benutzer…

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	**Kaspersky Next XDR Optimum**
Desktop und Server	x1		
Mobile Geräte	x2		
Microsoft Office 365 Mailboxen	–	x1.5	
Cybersecurity Training für IT Administratoren (CITO)	–	Nach Anzahl der Administratoren	
Security Awareness Platform Benutzer (ASAP)	–	–	x0.2
Cloud Sandbox Anfragen	–	–	x0.5

XDR/MXDR Optimum Lizenz
...und die technischen Einsatz-Optionen...

- **KSC 15.x/16.x On-Prem – Linux**

  → voller Funktionsumfang, d. h. mit AD-, ASAP- und TIP Cloud-Sandbox-Integration und Alert Aggregation

- **KSC 15.x On-Prem – Windows**

  → eingeschränkt (keine AD-, ASAP- und TIP Cloud Sandbox-Integration, keine neuen Web Console-Funktionen)
  - ASAP Standalone → Lizenz (20 %) wird korrekt berechnet
  - TIP Cloud Sandbox Standalone
  (FYI: *von HQ keine Weiterentwicklung für KSC Windows geplant*)

- **KSC Cloud Console (KSCCC)**

  → voller Funktionsumfang, min. 300 User (MSP: 150 gesamt), nur Web GUI, d. h. kein Linux Know-how notwendig

Kaspersky Threat Data Feeds

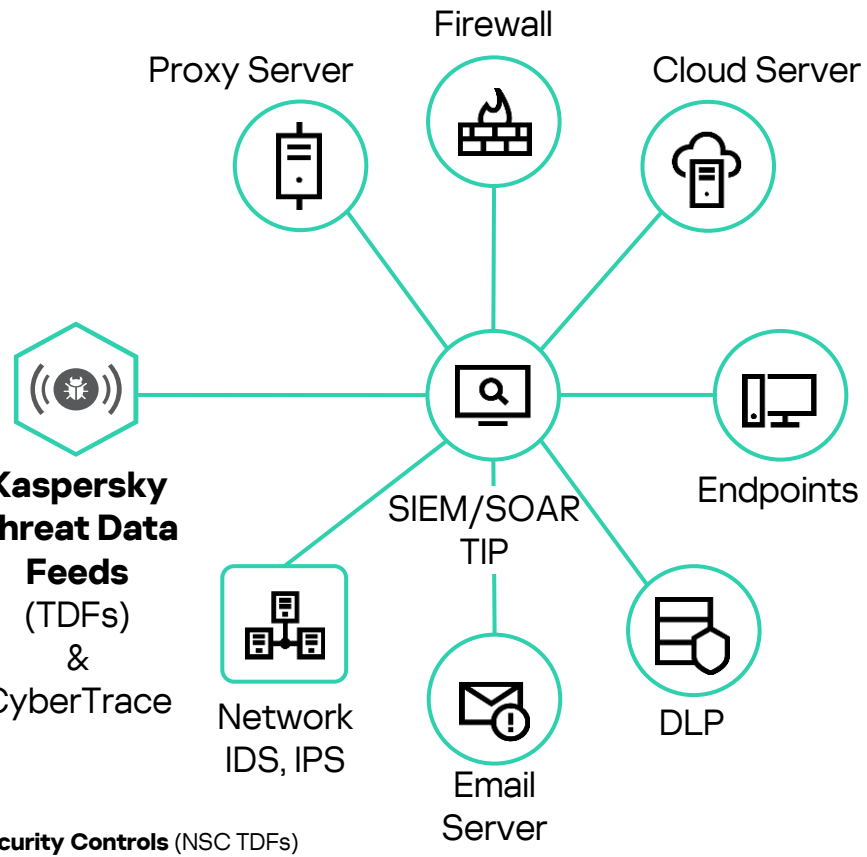
APT
APT & Crimeware Feeds (URL, IP, Hash, Yara)

Rules
Suricata Rules, Yara Rules (part of APT Reporting)

URL
URL Feeds (Malicious, Phishing and C&C)
Ransomware URL Feed
IoT URL Feed
Exact URL Feed (Malicious, Phishing, Botnet)
Mobile Botnet URL Feed

IP
IP Reputation / **IP Block List**
Passive DNS (pDNS) Feed

Hashes
Malicious Hash Feed
Malicious Hash Feed for ICS
Mobile Malicious Hash Feed
File Reputation Feed
Vulnerability Data Feeds



Network Security Controls (NSC TDFs)

Threat Data Feeds bzw. Network Security Controls – Integration, z. B. NGFW

Name	Type	Description	URI	Update frequency
Dangerous IPs	IPs	IP List of dangerous IP addresses	https://tip.kaspersky.com/api/feeds/dangerous_ips	20
Malicious URLs	URL	List of malicious domains	https://tip.kaspersky.com/api/feeds/malicious_domains	20
Phishing URLs	URL	List of phishing domains	https://tip.kaspersky.com/api/feeds/phishing_domains	20
Botnet CnC URLs	URL	List of botnet C&C domain	https://tip.kaspersky.com/api/feeds/botnet_domains	60

Integrations-Überblick:

- oben genannten dynamische IoC-Listen (Network Security Controls) auswählen – je nach Anforderung
- API-Token via Kaspersky Threat Intelligence Portal
- Herunterladen der Listen, z. B. mit dem Dienstprogramm cURL inkl. evtl. **Limit**-Parameter (optional), z. B. **curl -v -u api_token:< *YOUR API TOKEN*> https://tip.kaspersky.com/api/feeds/dangerous_ips?limit=9000**
- Integration in die jeweilige NGFW Web-Console, z. B. Cisco Firewall Management Center

Vielen Dank!

Mike Ritter — Territory Channel Manager MSP
Michael Hirschmann — Senior Presales Engineer / Presales Manager

kaspersky

kaspersky bring on the future

Kaspersky Partner Kick-Off 2026

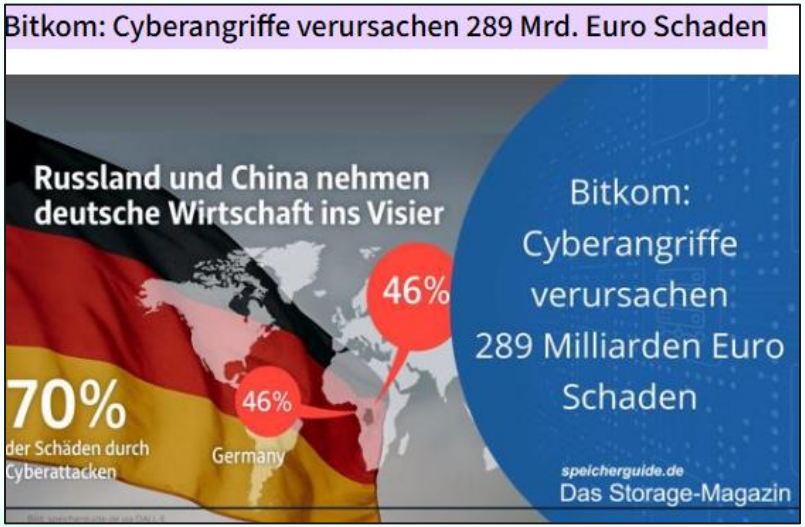
3. Abwehr – Bedrohungen stoppen, bevor sie Schaden anrichten

(Kuma – ein SIEM als Schlüssel zur NIS-2- und GDPR-Compliance)

Angel Jodra
Presales Consultant

Frank Jonas
Head ENT Sales DACH

Hintergrund der NIS 2 Richtlinie



Steigende Cyberangriffe und regulatorischer Druck

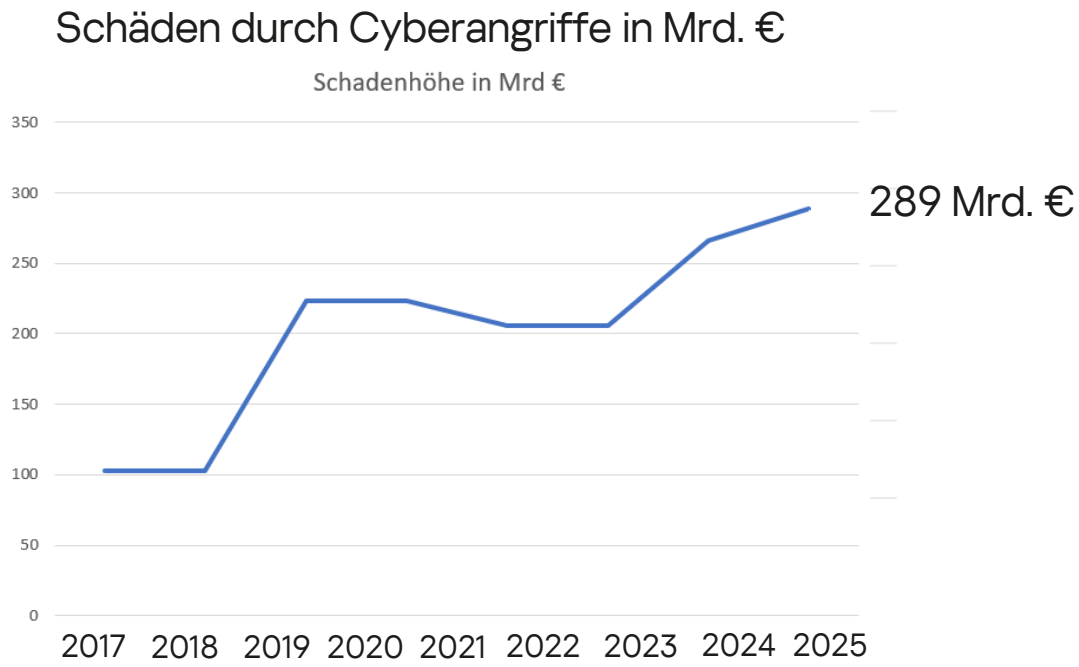
- Laut BITKOM: in 2025 Schäden in Höhe von 289 Mrd. € bei deutschen Unternehmen;
- 87 % Unternehmen sind betroffen

GDPR: Meldungen innerhalb von 72h

NIS 2: Erstmeldung schwerwiegender Vorfälle innerhalb von 24h, erweiterte Meldung nach 72 Stunden, Abschlussbericht nach 4 Wochen.

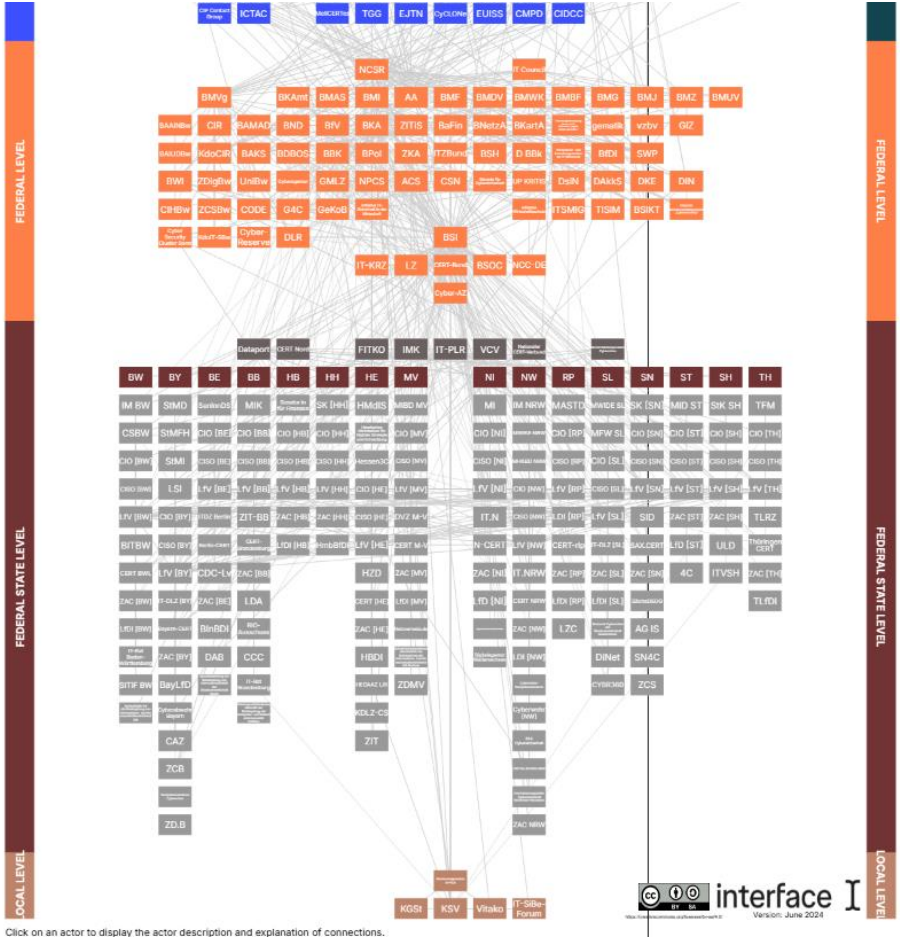
Strafen bis zu 20 Mio. € / 4 % vom jährlichen Umsatz

Schäden durch Cyberangriffe – Deutsche Unternehmen



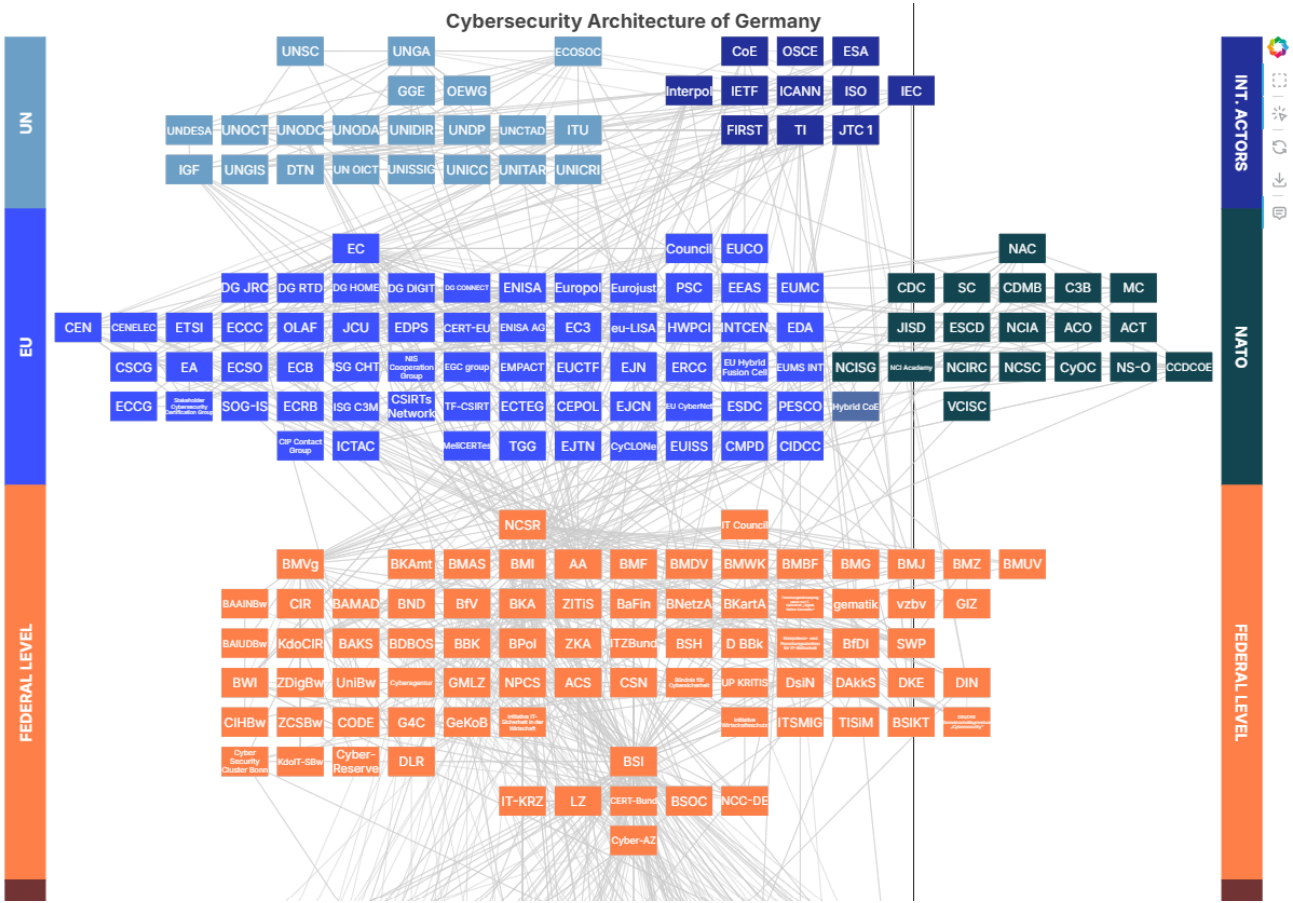
Quelle: BITKOM

Cybersecurity-Architektur in Deutschland



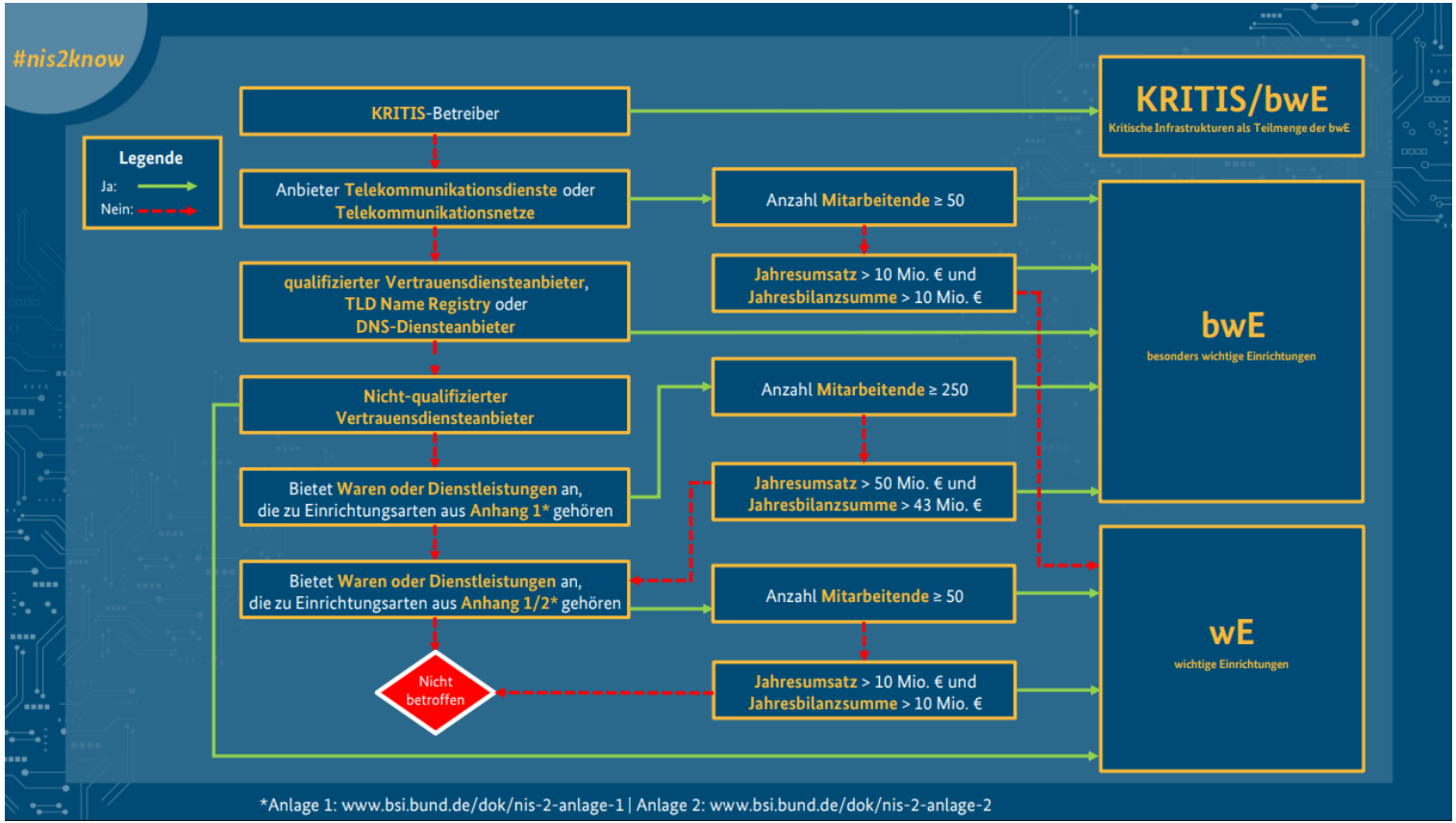
Quelle: interface-eu.org

Cybersecurity-Architektur in Deutschland – Verbindungen zu EU, NATO und UN



Quelle: interface-eu.org

Wen betrifft die NIS 2 Richtlinie?



Quelle:bsi.de

Wen betrifft die NIS 2 Richtlinie?

- **Energie:** Elektrizität, Fernwärme/-kälte, Erdöl, Erdgas, Wasserstoff
- **Verkehr:** Luftfahrt, Schienenverkehr, Schifffahrt, Straßenverkehr
- **Bankwesen:** Kreditinstitute
- **Finanzmarktinfrastrukturen:** Betreiber von Handelsplätzen, zentrale Gegenparteien
- **Gesundheitswesen:** Gesundheitsdienstleister, EU-Referenzlabore, Hersteller von pharmazeutischen Produkten
- **Trinkwasser:** Wasserversorgung und -verteilung
- **Abwasser:** Entsorgung und Behandlung
- **Digitale Infrastruktur:** Anbieter öffentlicher elektronischer Kommunikationsnetze/-dienste, Rechenzentren, Top-Level-Domain-Registries, DNS-Dienste, Cloud-Computing, Content-Delivery-Netze
- **Verwaltung von IKT-Diensten:** Managed Service Provider (MSP)
- **Weltraum:** Betreiber von Bodeninfrastruktur

Schwellenwerte Unternehmensgröße:

ab 50 Beschäftigten ODER über 10 Millionen Euro Jahresumsatz/Jahresbilanzsumme

Betroffene Branchen (Wichtige Einrichtungen – NIS 2 Anlage 2):

- **Post- und Kurierdienste:** Anbieter von Postdiensten (Art. 2 Nr. 1a der RL 97/67/EG)
- **Abfallbewirtschaftung:** Unternehmen, die Abfallbewirtschaftung betreiben (ohne reine Entsorger)
- **Chemie:** Herstellung und Vertrieb von chemischen Stoffen
- **Lebensmittel:** Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- **Produktion:** Herstellung von Waren (Maschinenbau, elektrische Ausrüstung, Fahrzeuge/Automobilindustrie)
- **Digitale Dienste:** Anbieter von Online-Marktplätzen, Suchmaschinen, Cloud-Computing-Diensten
- **Forschung:** Einrichtungen, die Forschung betreiben

Unternehmensentscheider werden in die Pflicht genommen

Quelle:bsi.de

Überblick über die NIS 2 Anforderungen

- **Risikomanagement & Sicherheit:** Implementierung von Sicherheitskonzepten, Verschlüsselung, Backup-Management, Zugriffskontrollen und Business Continuity Plänen.
- **Lieferkettensicherheit:** Prüfung der Cybersicherheit bei Zulieferern und Dienstleistern.
- **Meldepflichten:** Ein dreistufiger Prozess: 24h-Vorabmeldung, 72h-Bericht, einmonatiger Abschlussbericht bei signifikanten Vorfällen.
- **Meldeportal:** Registrierungspflicht beim BSI (Bundesamt für Sicherheit in der Informationstechnik).
- **Cyber-Hygiene & Schulung:** Regelmäßige Mitarbeiterschulungen und Sicherheitsupdates.
- **Verantwortung der Leitung:** Die Geschäftsführung haftet persönlich für die Einhaltung und muss Schulungen absolvieren.

Logmanagement: Warum herkömmliche Ansätze scheitern

- Logs sind verteilt auf viele Systeme
- Keine zentrale Sicht auf Bedrohungen
- Hoher manueller Aufwand → Langsame Reaktion
- Fehlende Nachweisbarkeit gegenüber Behörden

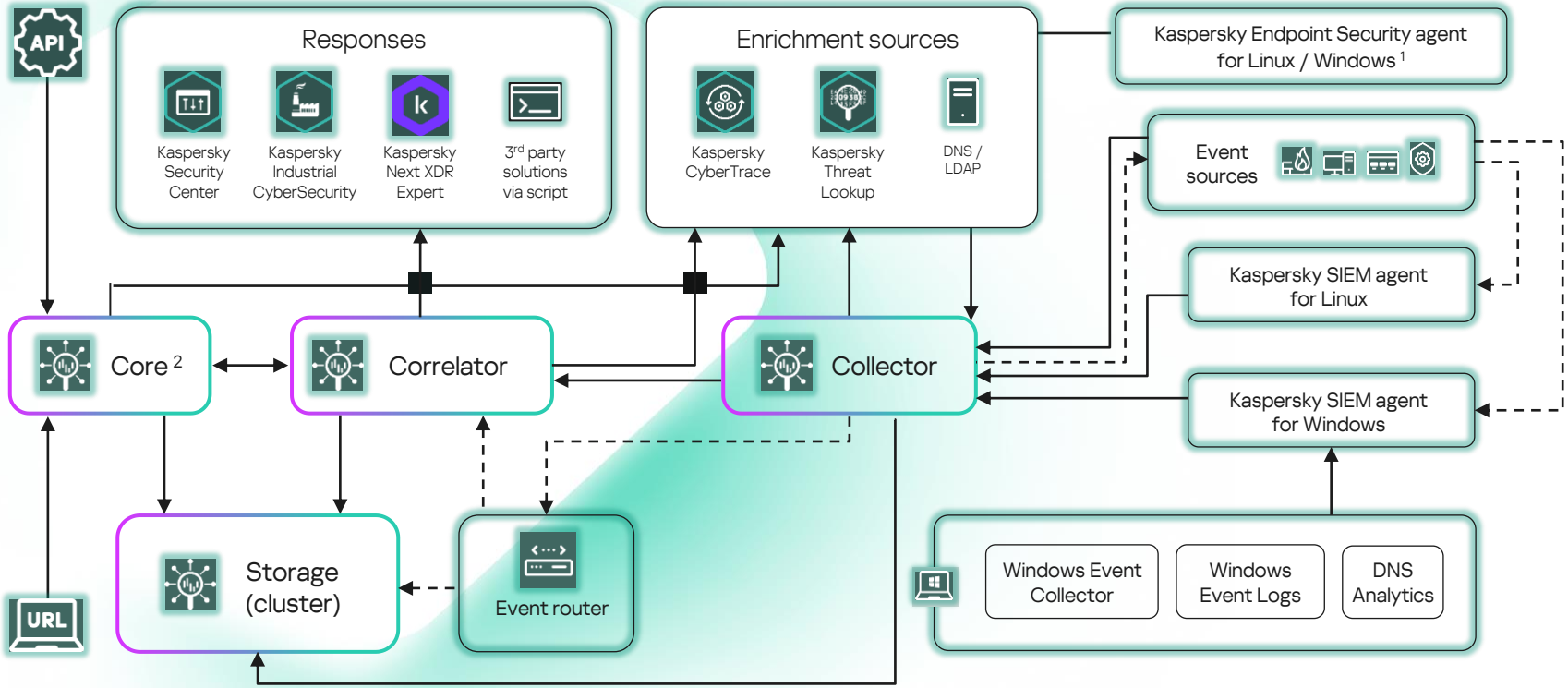
FAZIT:
Zentralisiertes Monitoring und weitgehende Automatisierung erforderlich → **SIEM**

Kaspersky SIEM:

KUMA – Kaspersky Unified Monitoring and Analysis Plattform

Eine State-of-the-Art SOC-Plattform basierend auf KI-Technologien und unterlegt mit führenden Threat Intelligence-Informationen

Erweiterte Ansicht der Architektur



[1] If a workstation has a Kaspersky Endpoint agent (KES Win 12.6 or Linux 12.2) , it can be used to forward events to SIEM without setting up an additional data source

[2] The Core component can be deployed as a cluster of 3 or 5 servers for high availability. Fault tolerance is now ensured not only by the Kubernetes cluster but also by the Raft algorithm.

Threat Intelligence

- Verbessert die Datenrelevanz für genauere Analysen
- Beschleunigt Erkennungs- und Triageprozesse
- Nutzt taktische, operative und strategische Bedrohungsinformationen

Enge Integrationen

- Umfangreiche Integration von Kaspersky- und Drittanbieterprodukten
- Integrierte Antwortoptionen
- Unübertroffene nahtlose Integration mit den eigenen Produkten von Kaspersky

Multitenancy

- Native Unterstützung für Mandantenfähigkeit innerhalb einer einzigen SIEM-Installation
- Ermöglicht die Erstellung isolierter SIEM-Instanzen für einzelne Mandanten
- Jeder Mandant kann seine eigenen Ereignisse unabhängig empfangen und verarbeiten

Synergie zwischen SIEM und Threat Intelligence

SIEM

+

TI

Kaspersky SIEM

Event collection | Normalization | Enrichment | Correlation | Storage

Kaspersky CyberTrace

Aggregiert Indicators of Compromise (IoC) aus verschiedenen Quellen und integriert Bedrohungsdaten-Feeds in SIEM-Systeme.

Kaspersky Threat Data Feeds

Ransomware URL | Malicious URL | IP Reputation

Botnet URL | Phishing URL | and more on demand

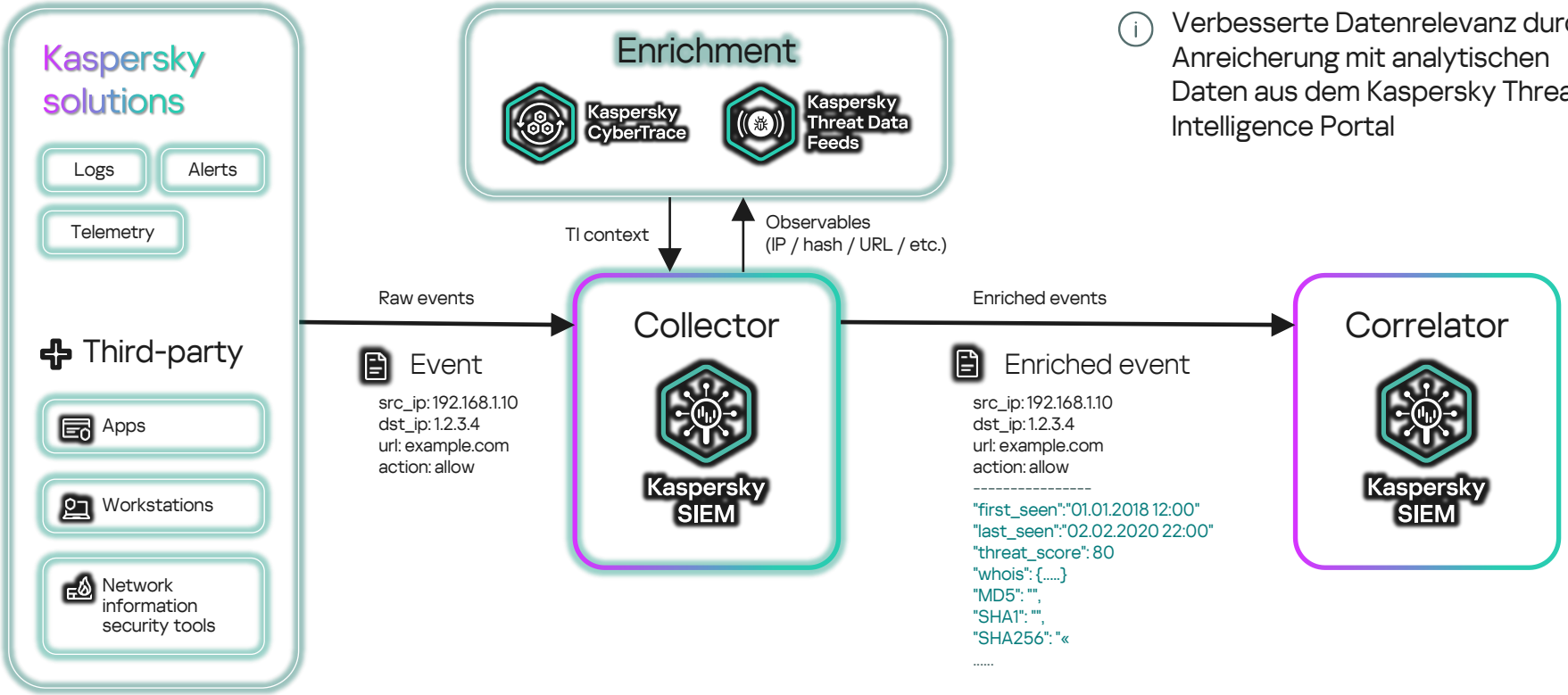
Kaspersky Digital Footprint Intelligence

Ein umfassender digitaler Risikoschutzdienst, der Kunden dabei hilft, ihre digitalen Assets zu überwachen und Bedrohungen aus dem Surface-, Deep- und Dark-Web zu erkennen.

Kaspersky Threat Lookup

Stellt das gesamte Wissen von Kaspersky über Cyberbedrohungen und deren Zusammenhänge in einem einzigen leistungsstarken Webdienst zur Verfügung.

Streaming Enrichment

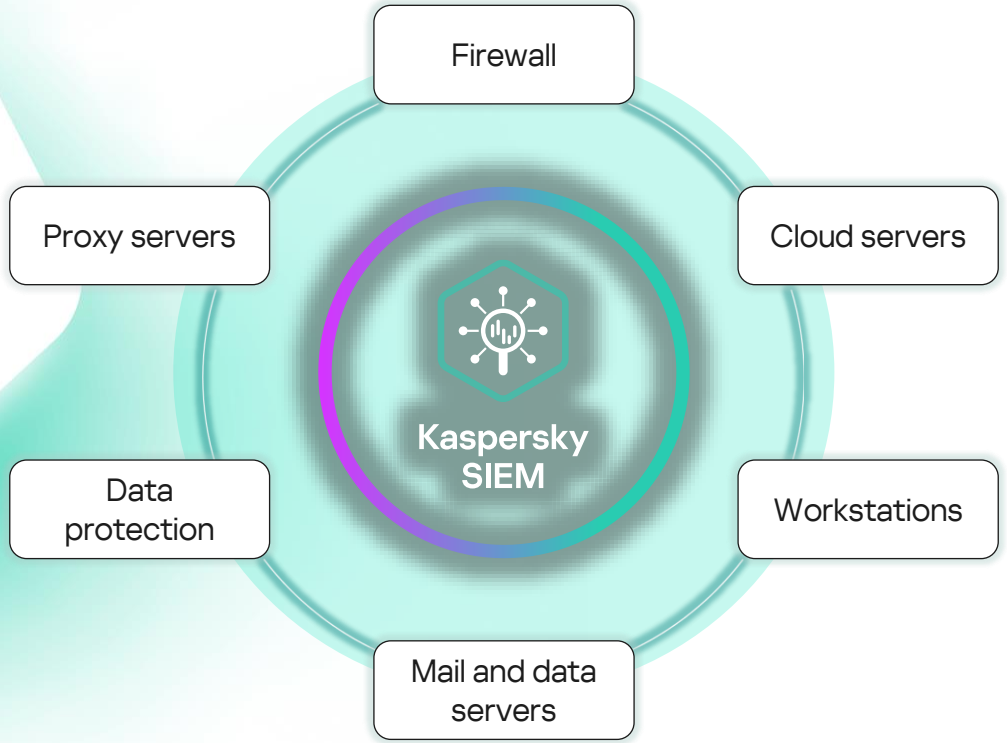


ⓘ Verbesserte Datenrelevanz durch Anreicherung mit analytischen Daten aus dem Kaspersky Threat Intelligence Portal

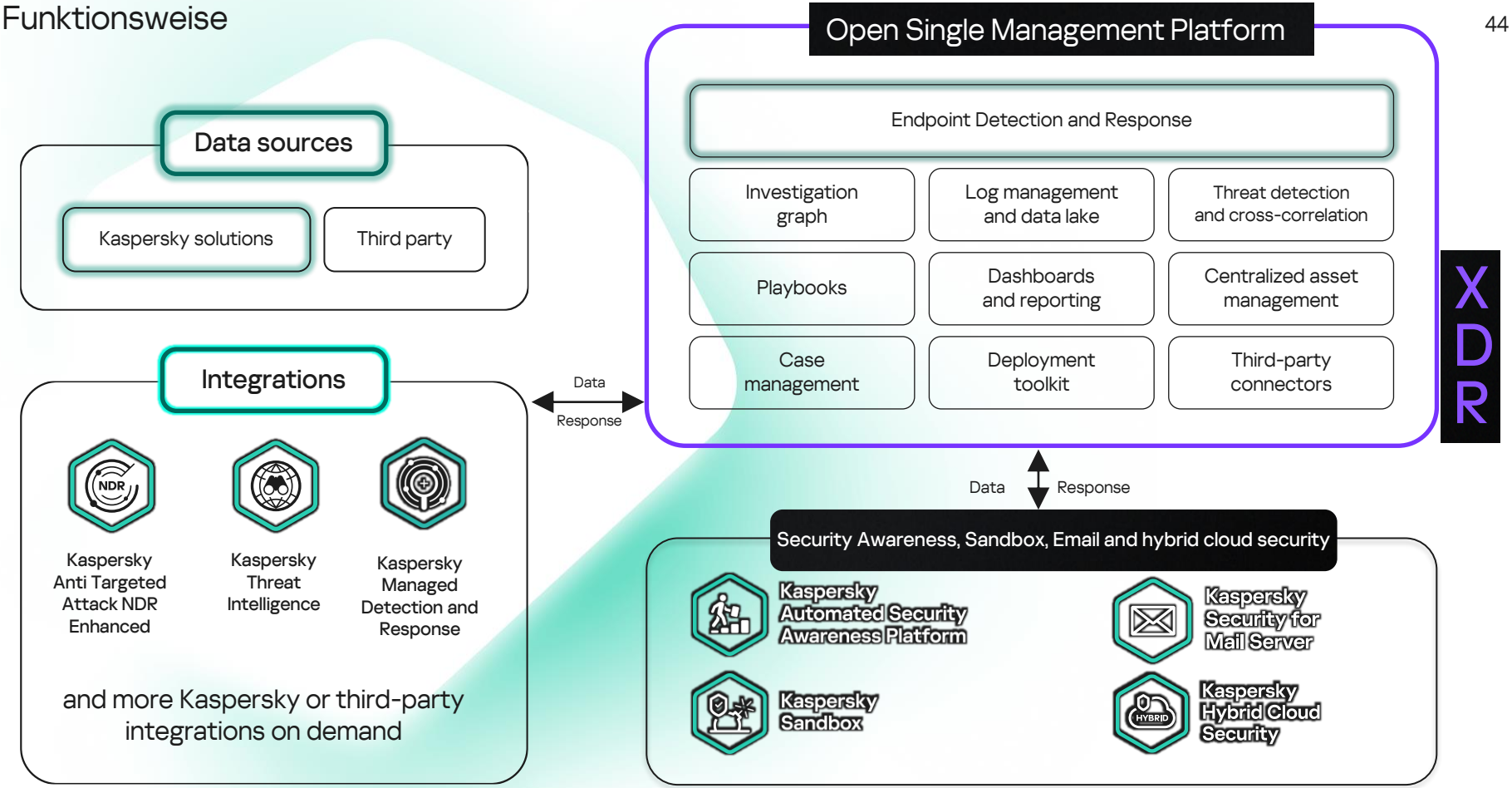
Threat Data Feeds

Kaspersky Threat Data Feeds

- IP reputation feed
- Hash feed (Win / *nix / MacOS / Android OS / iOS)
- URL feeds (malicious, phishing and C&C)
- Ransomware URL feed
- APT IoC feeds
- Vulnerability feed
- Passive DNS (pDNS) feed
- IoT URL feed
- Whitelisting feed
- ICS hash feed
- and more



Funktionsweise



Integrationen

By vendor (300+ sources supported out-of-the-box*) Full list

Kaspersky
Absolute
AhnLab
Aruba
Avigilon
Ayehu
Barracuda Networks
BeyondTrust
Bloombase
BMC
Bricata
Brinqa
Broadcom
Check Point
Cisco
Citrix
Claroty
CloudPassage
Corvil
Cribl
CrowdStrike
CyberArk
Deep Instinct
Delinea
EclecticIQ
Edge Technologies
Eltex
ESET
F5 BIG-IP
FireEye
Forcepoint
Fortinet
Gigamon
Huawei
IBM
Ideco
Illumio
Imperva
Orion soft
Intralinks
Juniper Networks
Kemp Technologies
Kerio
Lieberman Software
MariaDB
Microsoft
MikroTik
Minerva Labs
NetIQ
NETSCOUT
Netskope
Netwrix
Nexthink
NIKSUN
Oracle
PagerDuty
Palo Alto Networks
Penta Security
Proofpoint
Radware
Recorded Future
ReversingLabs
SailPoint
SentinelOne
SonicWall
Sophos
ThreatConnect
ThreatQuotient
Trend Micro
Trustwave
VMware
Vormetric
WatchGuard
Windchill FRACAS
Zettaset
Zscaler
and more.

By security domain

Endpoint Security
- EPP & EDR solutions

Network & Web & Email Security
- Email Protection
- Network Detection and Response (NDR)
- Firewalls (FW) and Next-Gen Firewalls (NGFW)
- Unified threat management (UTM)
- Intrusion Detection Systems (IDS)

Cloud Security
- Cloud Access Security Brokers (CASB)
- Cloud Workload Protection Platforms (CWPP)

Threat Intelligence
- Cyber Threat Intelligence (CTI)

Identity Security
- Identity and Access Management (IAM)
- Privileged Access Management (PAM)

Data Loss Prevention (DLP)
OT / IoT Security
Security Awareness

By transport type Full list

TCP
UDP
NetFlow
sFlow
NATS JetStream
Kafka
HTTP
SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse)
File
Diode
FTP
NFS
WMI
WEC
SNMP
SNMP Traps
VMware API
Elasticsearch
and more.

By data type

XML
Syslog
CSV
JSON
SQL
IPFIX
CEF
NetFlow v5
NetFlow v9
Key-Value
RegExp

Kaspersky products

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Security Center
- Kaspersky Secure Mail Gateway
- Kaspersky Web Traffic Security
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial Cyber Security for Networks
- Kaspersky Industrial Cyber Security for Nodes
- Kaspersky Automated Security Awareness Platform
- Kaspersky Managed Detection and Response
- etc.

* 200+ normalizers enable receiving of events from more than 300+ sources

24+ host-based response

- Terminate process
- Run program
- Isolate host
- Manage services
- Run YARA scan
- Run IOC scan
- Retrieve file
- Delete file
- Quarantine file
- Restore file from quarantine
- Get process list
- Get autostart entries
- Get file list
- Get NTFS metafiles
- Get registry key
- Get process memory dump
- Get RAM dump
- Get disk image
- and more.

Third-party response

- Active Directory
- Redmine
- Check Point NGFW
- Sophos Firewall
- FortiGate
- Palo Alto Networks (NGFW)
- And more.

Kaspersky response

- Kaspersky Automated Security Awareness Platform
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Threat Intelligence
- Kaspersky NGFW
- And more.

Built-in response options using Kaspersky products increases security efficiency

- Reaktionsmaßnahmen können manuell oder automatisch erfolgen, wenn Kaspersky SIEM beispielsweise mit Kaspersky Endpoint Detection and Response oder Active Directory gekoppelt wird, um die Reaktionsmöglichkeiten an Endpunkten zu erweitern..

- Die automatisierte Erfassung von Bestandsinformationen hilft bei der Kontextualisierung von Informationssicherheitsereignissen und unterstützt die Untersuchung von Vorfällen.

- Über Skripte können weitere Reaktionsoptionen hinzugefügt werden.

- Die Verwaltung von Workplace-Agenten erleichtert die Reaktion auf erkannte Bedrohungen.

Neu

Über die SIEM-Benutzeroberfläche können Analysten EDR-Reaktionsmaßnahmen auf KES-Endpunkten durchführen, die von EDR/XDR Optimum über Skripte und Open API verwaltet werden – so können sie Bedrohungen untersuchen und eindämmen, ohne die Konsole wechseln zu müssen.

Kaspersky EDR

- Host isolation and de-isolation
- Blocking md5 and sha256 hash on host
- Run executable files on host using full path
- Logging responses in the system log

Active Directory

- Lock and unlock accounts
- User logout from active sessions
- Add and remove accounts to and from groups

Kaspersky Web Traffic Security

- IP Blocking
- URL Blocking
- Domain Blocking

NGFW

- IP Blocking
- URL Blocking
- Domain Blocking

Telegram

- Alerts via Telegram

Kaspersky Secure Mail Gateway

- Blocking by email address
- Blocking by IP

Automatisierung und Orchestrierung von Reaktionen

In Kaspersky Next XDR Expert stehen zwei Arten von Playbooks zur Verfügung:

Das erste ist vorinstalliert, wurde von Kaspersky-Experten entwickelt, und das zweite ist ein benutzerdefiniertes Playbook.

Der Benutzer kann den automatischen oder manuellen Start des Playbooks konfigurieren.

Die Art und Weise, wie das Playbook gestartet wird, hängt vom ausgewählten Betriebsmodus ab: automatisch, manuell oder Test.

Playbooks beschleunigen Routinevorgänge, entlasten IT-Sicherheitsexperten, sodass diese sich komplexeren Untersuchungen widmen können, und tragen dazu bei, Fehler in gängigen Situationen zu minimieren, wodurch die Geschwindigkeit und Genauigkeit der Reaktion auf Vorfälle erhöht wird.

Kaspersky SIEM & AI

- AI detection of account theft
- Kaspersky AI Asset Scoring
- UEBA technology
- DLL hijacking
- Kaspersky Investigation and Response Assistant

Vielen Dank!

Frank Jonas — Head ENT Sales DACH
Angel Jodra — Presales Consultant

kaspersky