kaspersky bring on the future

Kaspersky Partner Kick-Off 2026

Der Panoramablick auf die IT-Sicherheit Ihrer Kunden –

Kaspersky Next Managed XDR Optimum & Kaspersky KUMA inkl. Live-Demo

Angel Jodra
Senior Presales Engineer

Michael Hirschmann
Senior Presales Engineer

Kaspersky Next XDR/MXDR Optimum im Detail

Verfügbar seit Sep. 2025
On-Prem (Linux) & **Cloud**

Kaspersky Next EDR Foundations

Automated protection from mass threats

- Multi-layered anti-malware
- Behavior detection
- Exploit prevention
- Universal Linux Kernel Module (ULKM)
- Remediation engine
- File, email, web and network threat protection on endpoint level
- Firewall
- Host Intrusion Prevention
- AMSI protection
- BadUSB attack prevention
- Root cause analysis with an alert card
- Global threat intelligence via Kaspersky Security Network
- Mobile threat defense

System hardening

- Hardware and software inventory
- Application, web and device controls
- Mobile device management (MDM)
- Remote troubleshooting
- Third-party apps & OS installation

Cloud security

- Cloud discovery

+

Kaspersky Next EDR Optimum

Endpoint detection and response to complex threats

- Indicators of compromise (IoC) search with automatic cross-endpoint response
- Adaptive anomaly control
- Single-click and guided response
- System critical object check
- Move file to quarantine/recover file from quarantine
- Network isolation/remove network isolation
- Get/delete file
- Start/terminate process
- Critical areas scan
- Execution prevention
- Execute command

System hardening

- Patch management
- Remote wipe
- Encryption management
- Advanced MDM

Cloud security

- Cloud blocking
- Data discovery
- Security for Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams

IT training

- Cybersecurity

+

NEU

Kaspersky Next XDR Optimum

Extended detection and response to complex threats

- Alerts aggregation
- Active Directory Response from the alert card

Automated Security Awareness Platform

- Flexible security awareness training for employees
- Customizable courses available in 25 languages
- Security awareness dashboards and reports
- Simulated phishing campaigns
- Video and audio training formats
- Automated Security Awareness Platform response from the alert card

Kaspersky Cloud Sandbox

- Uploading and executing a file in Cloud Sandbox
- Uploading a file from a web address and then execute it in Cloud Sandbox
- Anti-evasion features to counter malware designed to avoid sandboxes
- Executing the extracted file from the Cloud Sandbox report
- Exporting the analysis results
- Automatic detection of file types
- Managing obsolete tasks for exec

+

NEU

Kaspersky Next MXDR Optimum

Managed protection

- 24/7 continuous monitoring and threat hunting
- Incident submitting for further investigation by Kaspersky SOC
- Direct communication with the SOC team about incidents
- Notifications about incidents via email/Telegram
- Guided and automated response scenarios
- REST API for integration with IRP/SOAR
- Artificial Intelligence mechanisms accelerating incident investigation
- Assets visibility with their current statuses
- Compatibility with third-party EPP applications
- User-friendly MDR portal dashboards
- Regular reports
- Raw telemetry storage for 3 months

EDR Optimum

- ✓ Schneller Einstieg, wenig Konfigurations-aufwand
- ✓ basiert auf mehrfach ausgezeichneten Endpoint-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 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**

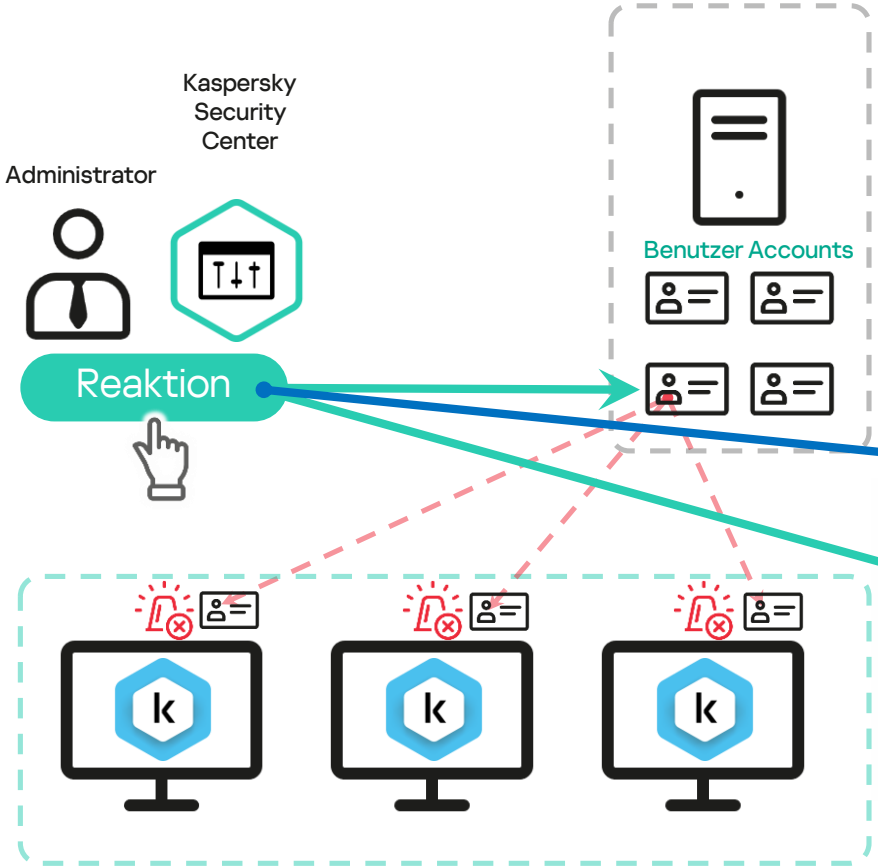
  → eingeschränkt (keine AD-, ASAP- und TIP Cloud Sandbox-Integration, keine neuen Web-Console Funktionen)
  - ASAP Standalone → Lizenz (20%) wird korrekt berechnet
  - TIP Cloud Sandbox Standalone

  (FYI: *von HQ keine Weiterentwicklung für KSC Windows geplant*)

- **KSC Cloud Console (KSCCC)**

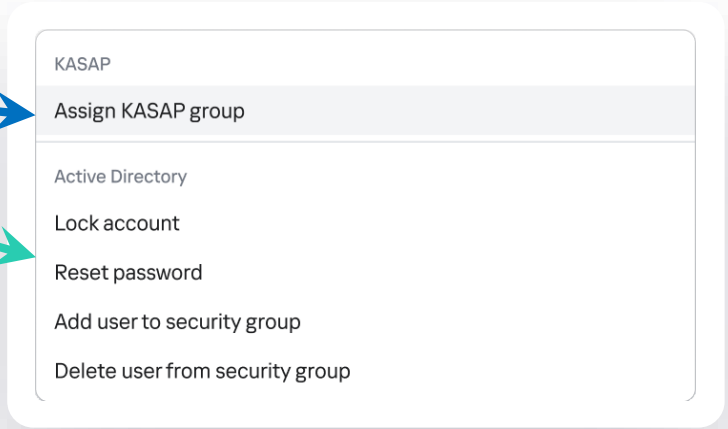
  → min. 300 User (MSP: 150 gesamt),
  nur Web GUI d.h. kein Linux Know-how notwendig

XDR/MXDR Optimum – AD & ASAP Integration



Active Directory Integration

ASAP Integration

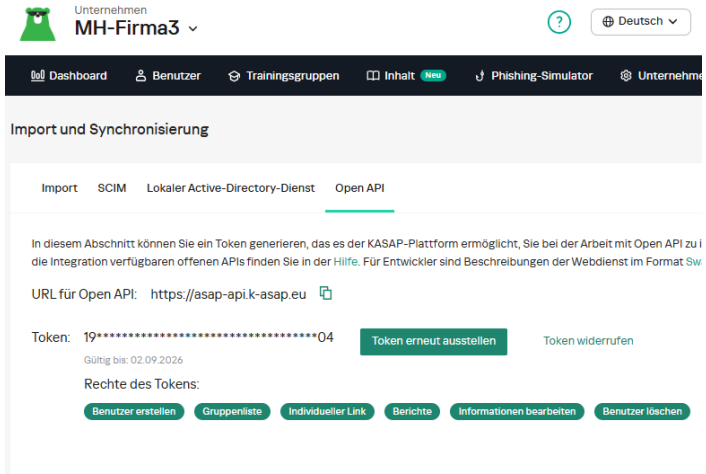


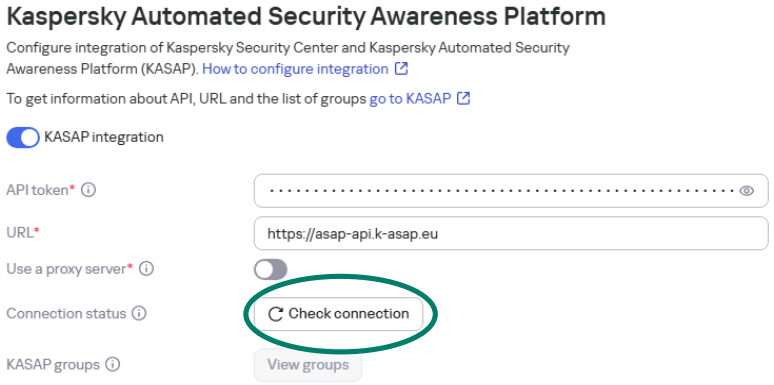
Voraussetzungen

- Account bzw. Zugriff auf das *Kaspersky Automated Security Awareness Platform* Portal (ASAP) ist erforderlich

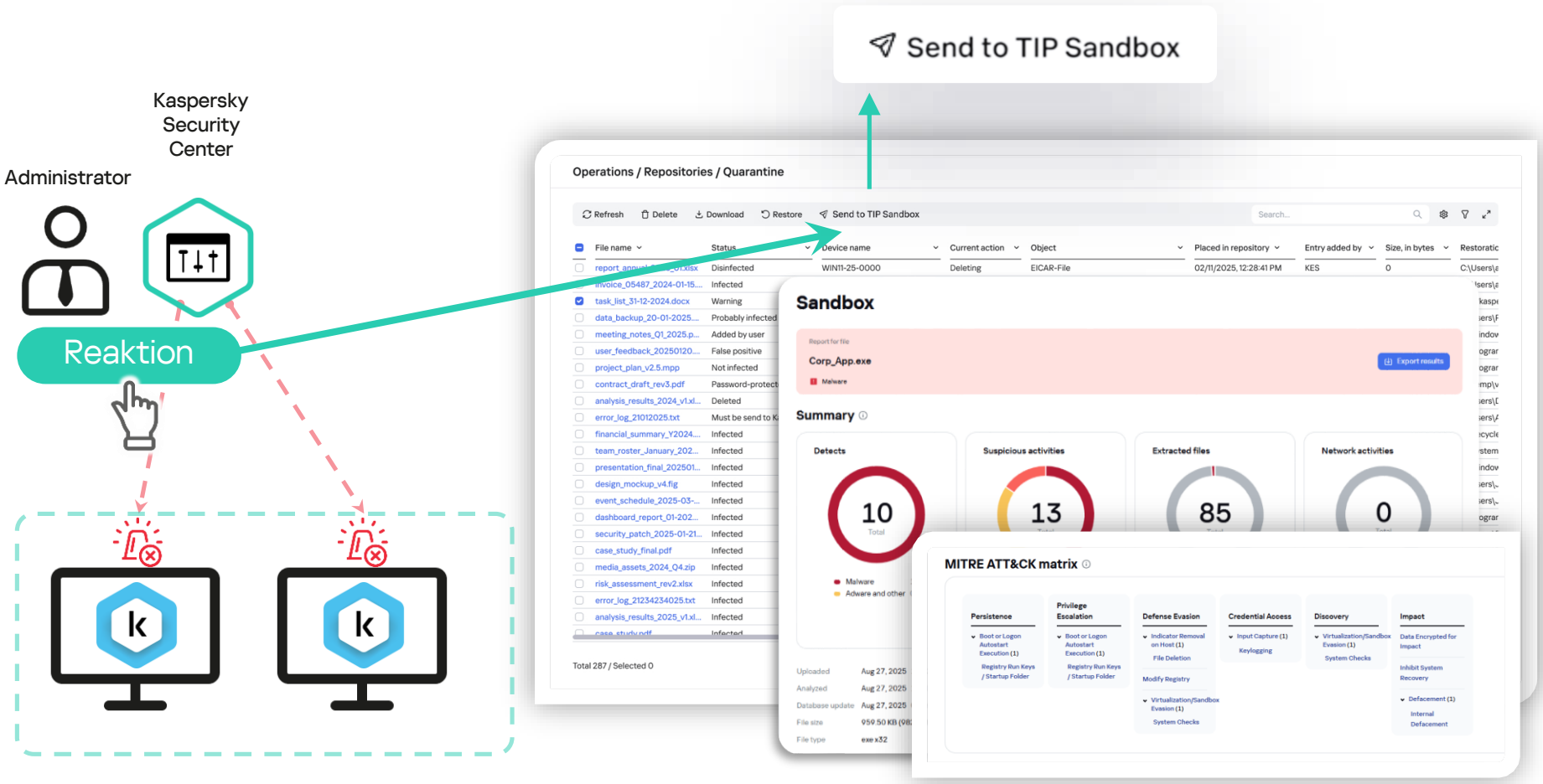
Integrations-Schritte (Überblick)

1. Login beim ASAP Portal (https://app.k-asap.eu/ bzw. https://www.k-asap.com/)
   → Dashboard-Screen anschl. Menü „*Import and Sync*“, „*Open API*“ und mit „*New Token*“ einen Token inkl. Rechte und Dauer erstellen. API Token und URL für OpenAPI kopieren.
2. KSC Web-Console → KSC „*Server Properties*“, unten „*KASAP*“ auswählen und die KASAP Integration aktivieren und den o.g. „API Token“ und URL zum ASAP-System (z.B. https://asap-api.k-asap.eu) hinzufügen





XDR/MXDR Optimum – TIP Cloud Sandbox Integration

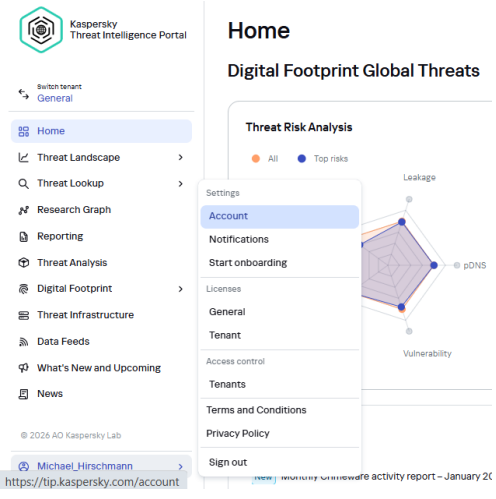


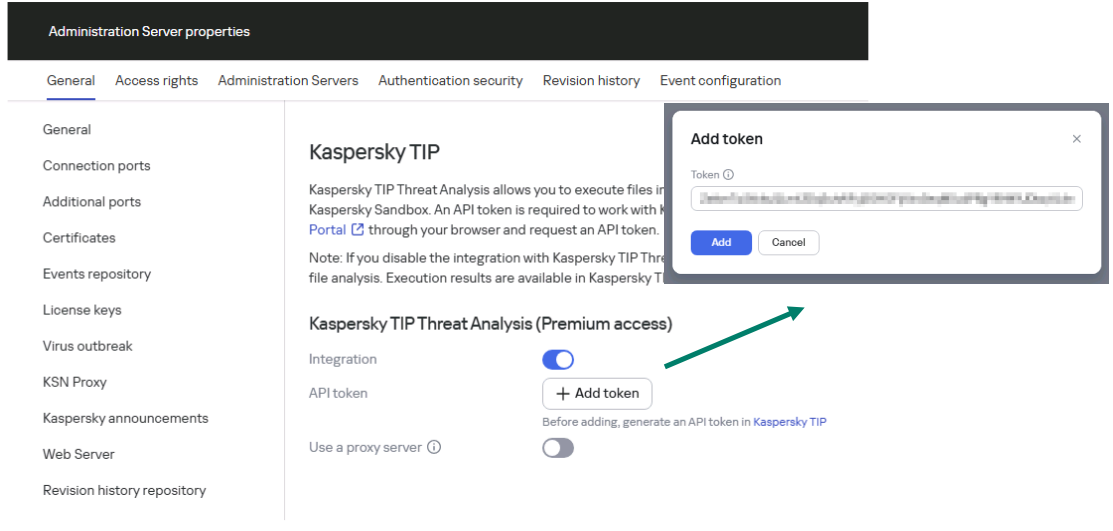
Voraussetzungen

- Account bzw. Zugriff auf das *Kaspersky Threat Intelligence Portal* (TIP) ist erforderlich

Integrations-Schritte (Überblick)

1. Login beim TIP Portal (https://tip.kaspersky.com/)
   → Mauszeiger über Benutzername und im Menü „*Account*“ auswählen und unten „*Request API token*“ mit entspr. Dauer
2. KSC Web-Console → KSC „*Server Properties*“, unten „*Kaspersky TIP*“ auswählen und die TIP Integration aktivieren und den o.g. „API Token“ hinzufügen





KSC 16.x On-Prem Installation unter Linux

Generelle Unterschiede von MS Windows vs. Linux

- Viele Linux Distributionen für KSC 16.x z.B. Debian, Ubuntu, Red Hat usw. ⇔ Microsoft OS
- Große DBMS Auswahl für KSC 16.x z.B. MySQL, MariaDB, PostgreSQL usw. ⇔ Microsoft SQL

Installations-Ablauf ab Linux OS Level… (nur Auszug)

- > *sudo apt install mariadb-server mariadb-client* (MariaDB unter Ubuntu/Debian)
- > *sudo apt install postgresql postgresql-client* (PostgreSQL unter Ubuntu/Debian)
- Konfigurations-Datei anpassen d.h. *my.cnf* bzw. (MariaDB)
  /etc/postgresql/<Version>/main/postgresql.conf (PostgreSQL)

- Erstellung der Gruppe "kladmins“ und von nicht-privilegierte Accounts
  - > *adduser ksc*
  - > *groupadd kladmins*
  - > *gpasswd -a ksc kladmins*
  - > *usermod -g kladmins ksc* usw.
- Erstellung der Datenbank
  - > *sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;* (PostgreSQL)
  - > *sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;“* (MariaDB)

KSC 16.x On-Prem Installation unter Linux

Installations-Ablauf ab Linux OS Level… (Fortsetzung… – nur Auszug)

- KSC 16.x Installation
  - Download entsprechendes KSC 16.x Linux Paket z.B. via GUI oder *sudo curl -O https://products.s.kaspersky-labs.com/…*
  - *> apt install /<path>/ksc64_ <Versions-Nr>_amd64.deb* (Ubuntu/Debian)
  - *> yum install /<path>/ksc64-<Versions-Nr>.x86_64.rpm –y* (Red Hat, CentOS)
- KSC 16.x Konfiguration
  - *> /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl*
    - Abfrage z.B. TCP Port-Nummer – Port 3306 (MariaDB/MySQL) – Port 5432 (PostgreSQL), FQDN Name des IAM-Servers etc.
- KSC 16.x Web-Console Installation
  - Download entsprechendes KSC 16.x Web-Console Paket
  - *> nano /etc/ksc-web-console-setup.json* (Antwort-Datei erstellen/anpassen im Json Format)
  - *> sudo dpkg -i ksc-web-console-<Versions-Nr.>.x86_64.deb* (DebianUbuntu)
  - *> sudo rpm -Uvh --nodeps --force ksc-web-console-<Versions-Nr.>.x86_64.rpm* (Red Hat)
  - *> systemctl restart KSC** (Restart der KSC Dienste)

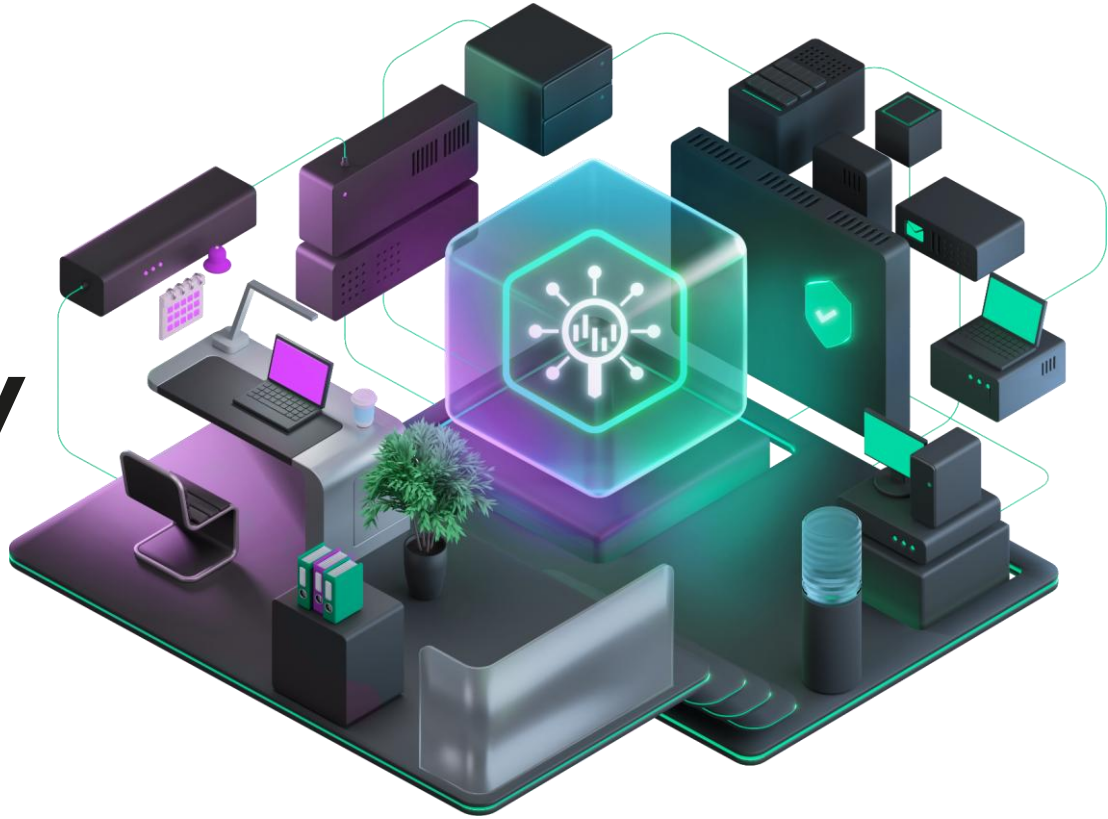
- **KSC 16.x Web-Console Konfiguraton** bzw. finale KSC Konfiguration via *https://<KSC-ServerFQDN>:8080/´*

Live-Demo...

KUMA

bzw.

Kaspersky SIEM



Live-Demo...

Vielen Dank !

Angel Jodra	Senior Presales Engineer /Presales Manager
Michael Hirschmann	Senior Presales Engineer /Presales Manager

kaspersky