esko
XDR & SOC

esko systems.de
part of connexta

# esko XDR und SOC – Warum XDR auf Servern teurer und komplexer ist

Mit Sicherheit gut beraten.

FORTINET

info@esko-systems.de | www.esko-systems.de

## EXECUTIVE SUMMARY

Server sind das Herzstück jeder IT-Infrastruktur und betreiben zentrale Dienste wie Active Directory, Datenbanken, Applikationsserver, Webservices oder Dateifreigaben. Ein erfolgreicher Angriff auf einen Server kann massive Auswirkungen auf das gesamte Unternehmen haben. Im Gegensatz zu Clients erfordert die Überwachung von Servern mit XDR eine höhere Präzision, individuelle Anpassungen und intensivere Ressourcen.

Dieses Whitepaper beleuchtet, warum XDR auf Servern komplexer und kostenintensiver ist und wie **esko XDR** in Verbindung mit dem **esko SOC** diese Herausforderungen effektiv adressiert.

## DIE BESONDERE ROLLE VON SERVERN IN DER IT-SECURITY

- **Zentrale Dienste:** Authentifizierung, Datenhaltung, Applikationsbereitstellung
- **Hohe Angriffsfläche:** Kritische Systeme sind bevorzugte Ziele von Angreifern
- **Große Auswirkung:** Kompromittierte Server können Geschäftsprozesse unterbrechen und sensible Daten freilegen

## WARUM XDR AUF SERVERN KOMPLEXER IST

**Vielschichtige Prozesse und Dienste**

- Automatisierte Aufgaben (Scheduled Tasks, Cronjobs)
- Hintergrunddienste (Backup, Monitoring, Datenbank-Replikation)
- Legacy-Software mit untypischem, aber legitimen Verhalten

***-> Diese Faktoren erschweren die Baseline-Bildung und erhöhen die Gefahr von False Positives.***

**Individuelle Anforderungen je Serverrolle**

- Maßgeschneiderte Sicherheitsrichtlinien statt Standardprofilen
- Ausnahmen für bestimmte Verzeichnisse oder Prozesse
- Abhängigkeiten zwischen Applikationen erfordern tiefes Fachwissen und umfangreiche Koordination/ Kommunikation und Planung

***-> Höherer Administrationsaufwand bei Einrichtung und Betrieb.***

**Hohe Datenvolumen und Performance-Herausforderungen**

- Große Mengen an Telemetriedaten (DB-Abfragen, Webanfragen, Dateioperationen)
- Erhöhte Speicher- und Analyseanforderungen
- Notwendigkeit von Datenselektion, um Signal statt Rauschen zu liefern

## WIE ESKO XDR UND SOC DIE KOMPLEXITÄT REDUZIEREN

**Hoher Schutz Status**
Wir gewährleisten auf allen Server-Systemen einen hohen Schutzstatus und reduzieren Fehlalarme durch gezielte Anpassungen sowie Kundenberatung.

**Überwachung durch das SOC**
Unser Security Operations Center übernimmt die kontinuierliche Analyse und reagiert umgehend auf bestätigte Bedrohungen – entlastet interne IT-Teams und verkürzt Reaktionszeiten.

**Intelligente Datenerfassung**
Sicherheitsrelevante Ereignisse werden erfasst und analysiert, wodurch Speicherbedarf und Analysezeit optimiert werden.

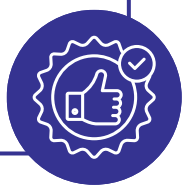
## BEST PRACTICES FÜR XDR AUF SERVERN

**Rollenbasierte Richtlinien:**
Passgenaue Policies für jede Serverfunktion.

**Regelmäßiges Tuning:**
Baseline-Erkennung anpassen, um Fehlalarme zu minimieren.

**SOC-Nutzung:**
Echtzeit-Überwachung und Incident Response durch Experten.

**Performance-Optimierung:**
Relevante Daten selektieren, Systemressourcen schonen.



## FAZIT

Server erfordern einen deutlich höheren Aufwand bei der Implementierung und dem Betrieb von XDR-Lösungen als Clients. Die Kombination aus **esko XDR** und **SOC-Services** bietet:

- Höhere Erkennungsgenauigkeit
- Geringere False Positives
- Schnellere und gezielte Reaktionen

So lässt sich die Sicherheit von Servern signifikant erhöhen und geschäftskritische Prozesse werden nachhaltig geschützt.

# esko-systems GmbH

Ortsstraße 45
89359 Kötz
Tel. (+49) 8284 996 90 - 0





esko systems.de
part of connexta


**info@esko-systems.de | www.esko-systems.de**