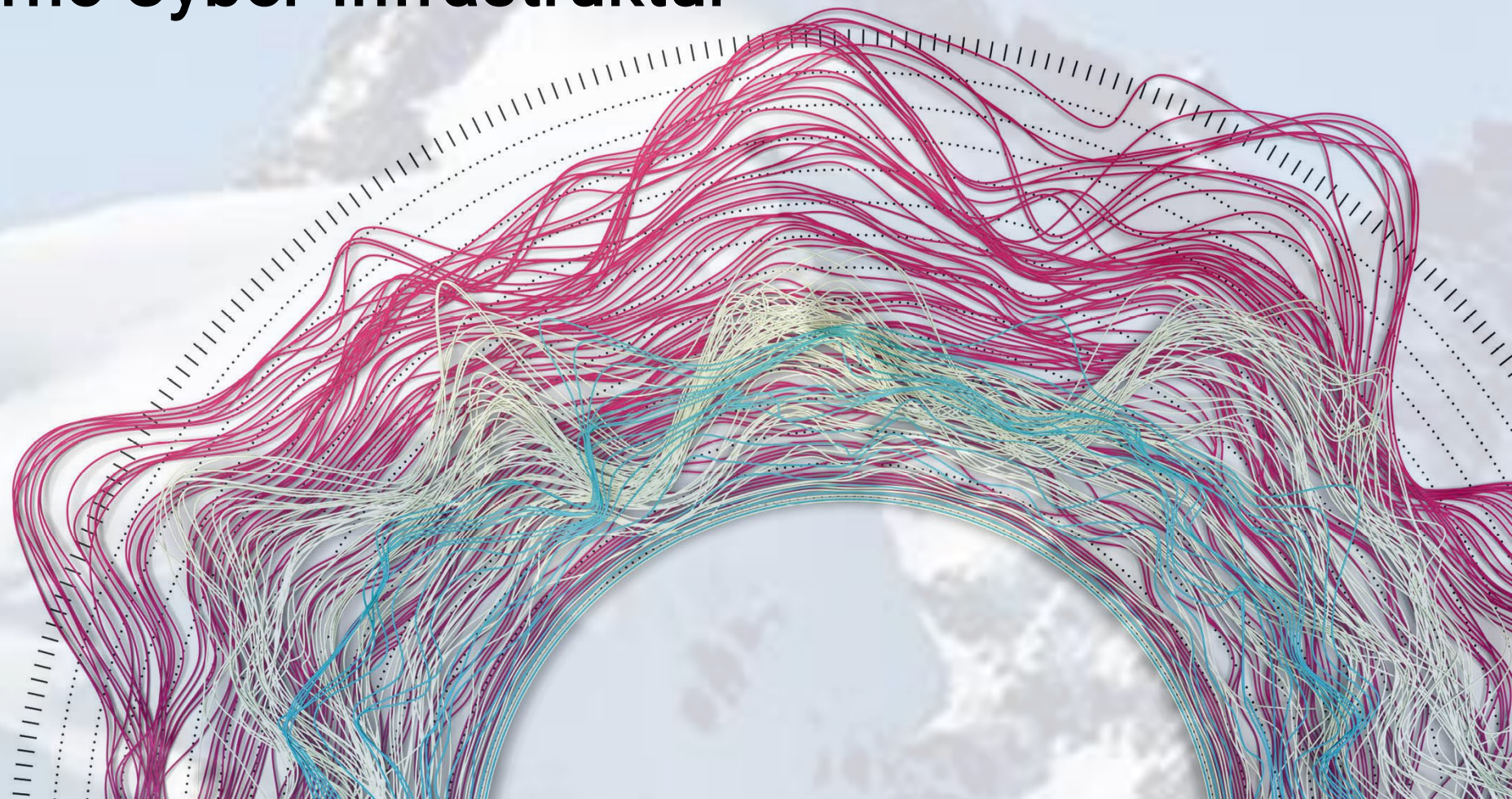
3 Banken IT

exeon
Smart Cyber Security.

Die Zukunft der Cybersicherheit: Was eine moderne Cyber-Infrastruktur ausmacht



Denis Matosevic
Sales Director DACH

Dietmar Kolasch
Abteilungsleiter Infrastruktur & Applikationen

3 Banken IT

exeon
Smart Cyber Security.

Network Detection and Response (NDR) in der Cyber-Infrastruktur

Prävention

- Anti-Viren Software
- Firewall
- Sicheres Web-Gateway (“Proxy”)
- Awareness-Training
- Phishing- Erkennung

- Etablierte Technologien
- In der Regel manuell konfiguriert
- Stoppen viele Angriffe
- Aber einige Angriffe gehen durch...

Erkennung & Reaktion

- … Stoppt Angriffe, die nicht verhindert wurden!

Network Detection and Response (NDR)

- Sichtbarkeit & Erkennung **ohne Agenten**
+ Vogelperspektive auf die IT-Aktivität aller Geräte, unabhängig von Agenten
+ Aggregierte, qualitativ hochwertige Warnungen durch eine Kombination von Datenquellen

SIEM

- Allgemeine Protokolldaten-Erfassung
- Eingeschränkte Unterstützung für Analyse und Erkennung
- Eine Preisgestaltung nach Volumen kann teuer werden

Endpoint Detection and Response (EDR)

- Detaillierte Endpunktansicht **mit Agenten**
- "Blind" auf nicht unterstützten Geräten

ExeonTrace
Zukunftssichere NDR

3 Banken IT

exeon
Smart Cyber Security.

Die SOC-Transparenz-Triade (SOC Visibility Triad)

> Endpoint Detection & Response (EDR)

Agenten auf allen Systemen, die detaillierte Informationen sammeln
Fortgeschrittene Malware schaltet diese Agenten leider oft aus!

> **Network Detection & Response (NDR)**

Sichtbarkeit und Erkennung ohne Agenten: Funktioniert für **jedes Gerät** und kann von Angreifern kaum deaktiviert werden
Vogelperspektive auf **alle IT-Aktivitäten** und Datenflüsse

> SIEM/UEBA

Allgemeine Analyse von Protokolldaten
Keine spezialisierten Algorithmen für EDR/NDR
Notwendigkeit einer Entwicklung und Pflege von Anwendungsfällen

Detection im Aufbau

Detection Erweiterung

3 Banken IT

exeon
Smart Cyber Security.

Hauptvorteile ExeonTrace

Umfassende Visibilität

Visibilität über Ihr gesamtes IT-/IoT-/OT-Netzwerk und alle seine Schnittstellen, um Schwachstellen (ungeschützte Dienste, Schatten-IT usw.) und bösartige Angriffsmuster in Echtzeit zu erkennen.

Netzwerk-Verhaltensanalyse

Dank Machine-Learing entdeckt ExeonTrace auffällige oder abweichende Kommuniationsverhalten in allen Netzwerke. Damit können Advanced Persistent Threats frühzeitig entdeckt werden.

On-prem oder Cloud

ExeonTrace kann on-prem oder in der Cloud betrieben werden. Für die Analyse der Daten verlassen keine Informationen die ExeonTrace Instanz.

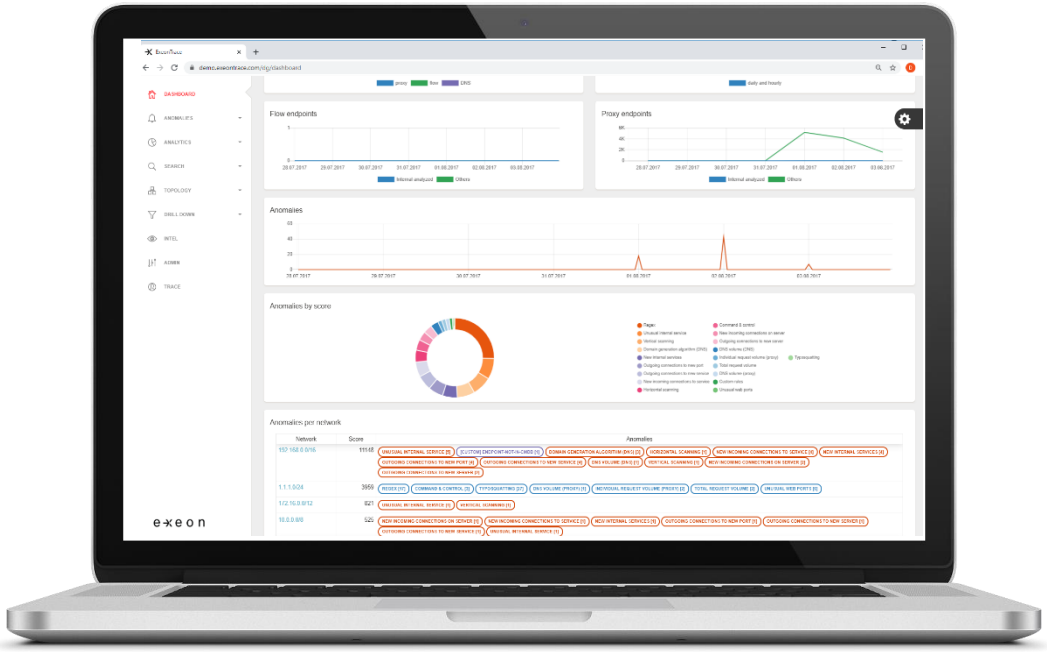
Entwickelt in der Schweiz

Als etablierte Schweizer NDR-Lösung, die auf einem Jahrzehnt Forschung an der ETH Zürich basiert, verfügen wir über ein hohes Maß an Innovation und Datenschutz, das kontinuierlich in unsere ExeonTrace-Plattform eingearbeitet wird.

3 Banken IT

exeon
Smart Cyber Security.

Exeon: Next Generation NDR/XDR aus der Schweiz



Gegründet von **Security Analysten und Researchern** des ETH Zürich Information Security & Privacy Center (ZISC)

Die Exeon NDR/XDR **Lösung**:

- Software Appliance (VMware)
- ML der unterschiedlichen Kommunikation
- Visuelles Abbild der Netzkommunikation
- Lokale Datenspeicherung für Detection und Forensik
- Geringer Speicherbedarf durch Verwendung von Logdaten
- Einfache Integration in die bestehende Umgebung

PostFinance

BonnNetz
Ein Unternehmen der Stadtwerke Bonn

SWISS

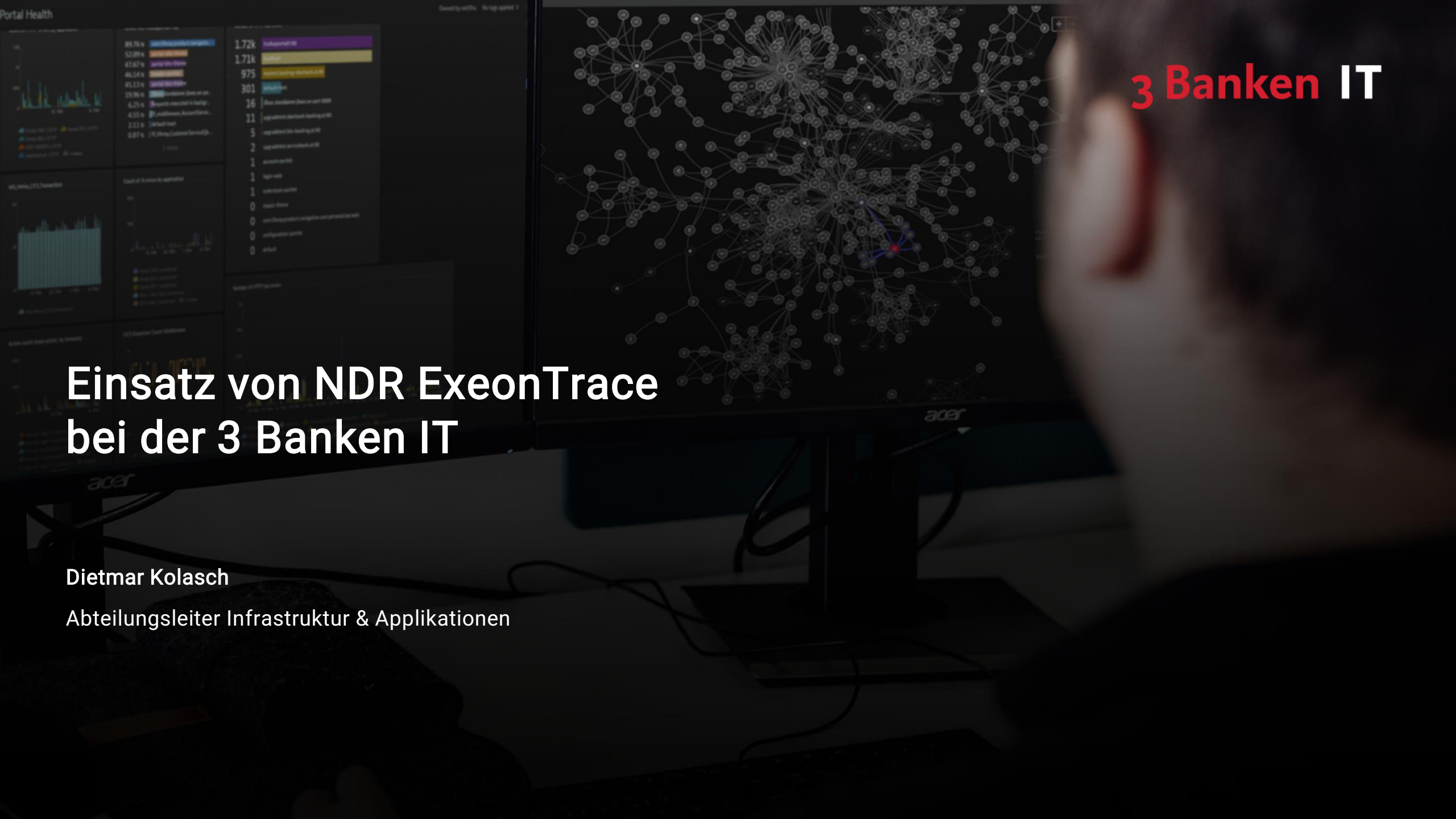
PLANZER

University of St.Gallen

3 Banken IT

solothurner spitäler SOH

HAAG-STREIT DIAGNOSTICS



Einsatz von NDR ExeonTrace bei der 3 Banken IT

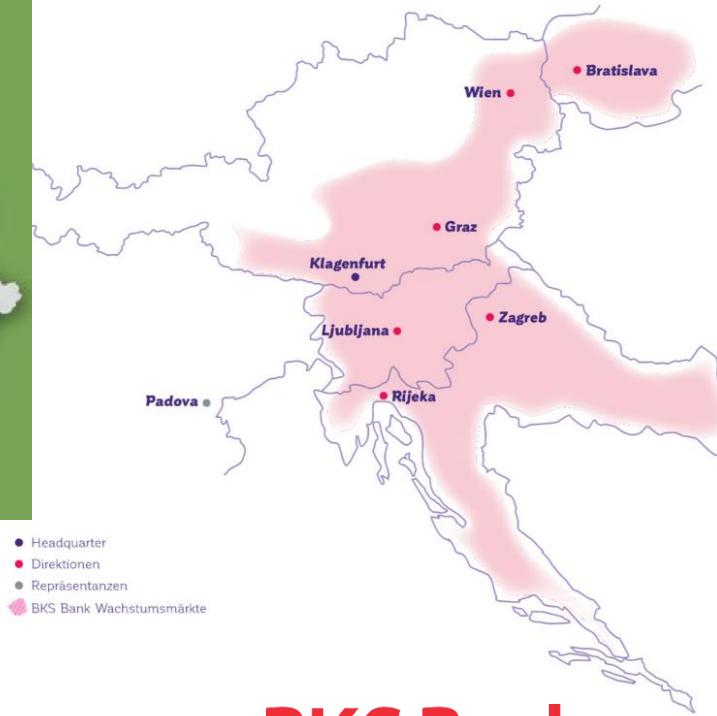
Dietmar Kolasch

Abteilungsleiter Infrastruktur & Applikationen

3 Banken IT

exeon
Smart Cyber Security.

Kurzüberblick 3 Banken Gruppe - Marktgebiet 3 Banken IT



BKS Bank
3 Banken Gruppe

Stand 31.12.2022	BTV	OBK	BKS	Gesamt
MitarbeiterInnen (FTE)	888	2.134	986	**4.008**
Anzahl Geschäftsstellen	35	180	64	**279**

3 Banken IT

exeon
Smart Cyber Security.

Unternehmen

3 Kompetenzzentren:
Linz, Innsbruck, Klagenfurt

3 Banken IT GmbH	2014	2015	2016	2017	2018	2019	2020	2021	2022
MitarbeiterInnen (per 31.12.)	210	226	232	253	271	307	326	350	369
Umsatz (in Mio.€)	51,56	51,47	54,73	56,62	60,29	67,52	73,23	79,66	85,10

3 Banken IT

exeon
Smart Cyber Security.

Leistungsportfolio

Was wir machen?

Applikationsarchitektur und Entwicklung

IT-Security

Rechenzentrums- und IT-Infrastruktur-Dienstleistungen

Kennzahlen	2021	2022
Online Transaktionen (in Mio. / Jahr)	ca. 3.000	ca. 3.160
Helpdesk-Tickets	36.000	32.300
Bearbeitete **Projekte**	197	179
Betreute **Applikationen**	800	812
Desktops, Notebooks, Tablets	7.200	7.250
IP-Phones	7.950	7.970
Betreute **Server** (Windows, Linux)	2.238	2.423

3 Banken IT

exeon
Smart Cyber Security.

IT – Security - Regulatorien

- Anforderungen aus staatlichen Behörden und Gesetzen und branchenspezifischen Regulativen mit denen sich eine Bank auseinandersetzen muss

#ICT Guideline (EBA)

#Croe für FMI (EZB)

#Leitfaden IKT-Sicherheit (FMA)

#BWG (AT)

#DSGVO (EU)

#NIS2-Richtlinie (AT)

#PSD2 (EU)

#MiFiD2 (AT)

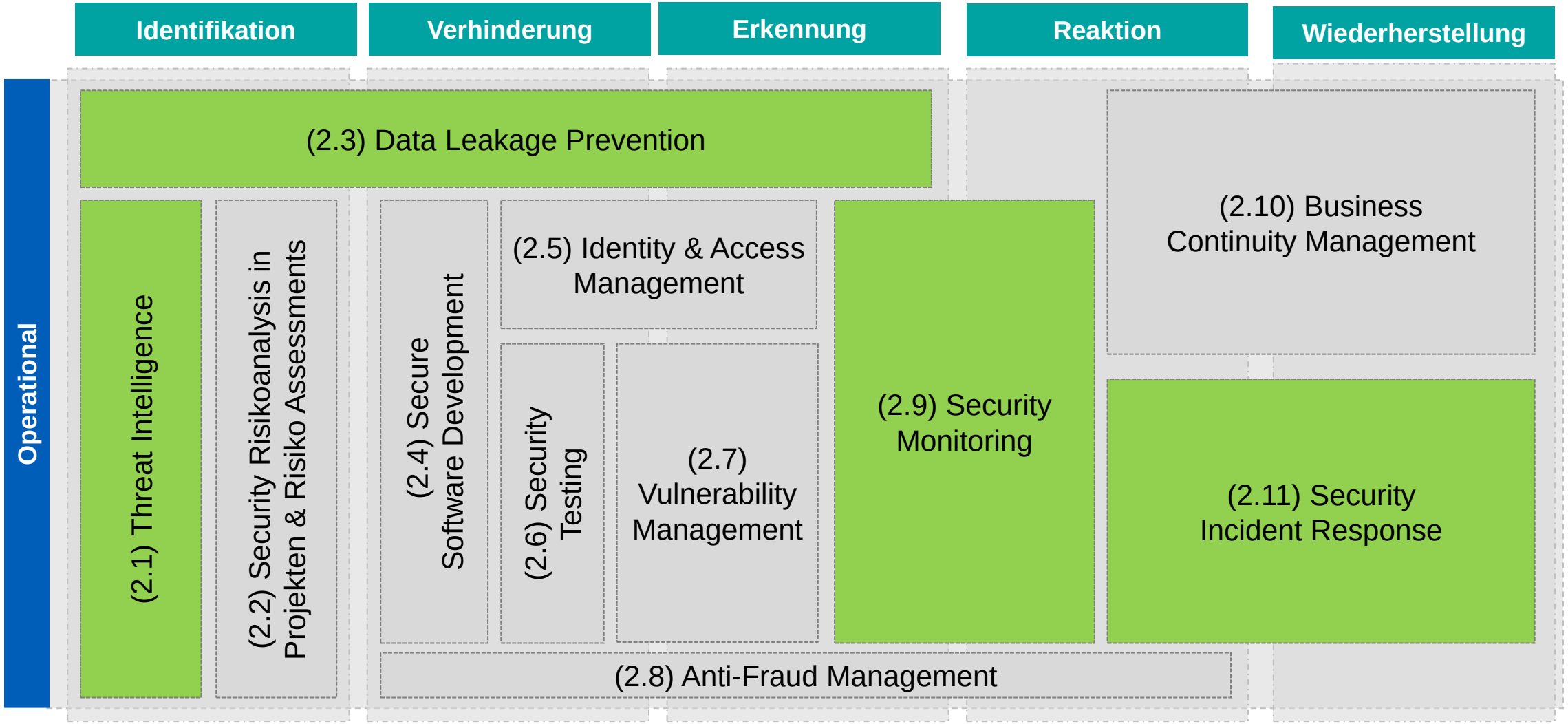
#Basel II, III u. IV (AT)

#Zadig (AT)

3 Banken IT

exeon
Smart Cyber Security.

Security Strategie



3 Banken IT

exeon
Smart Cyber Security.

IT – Security

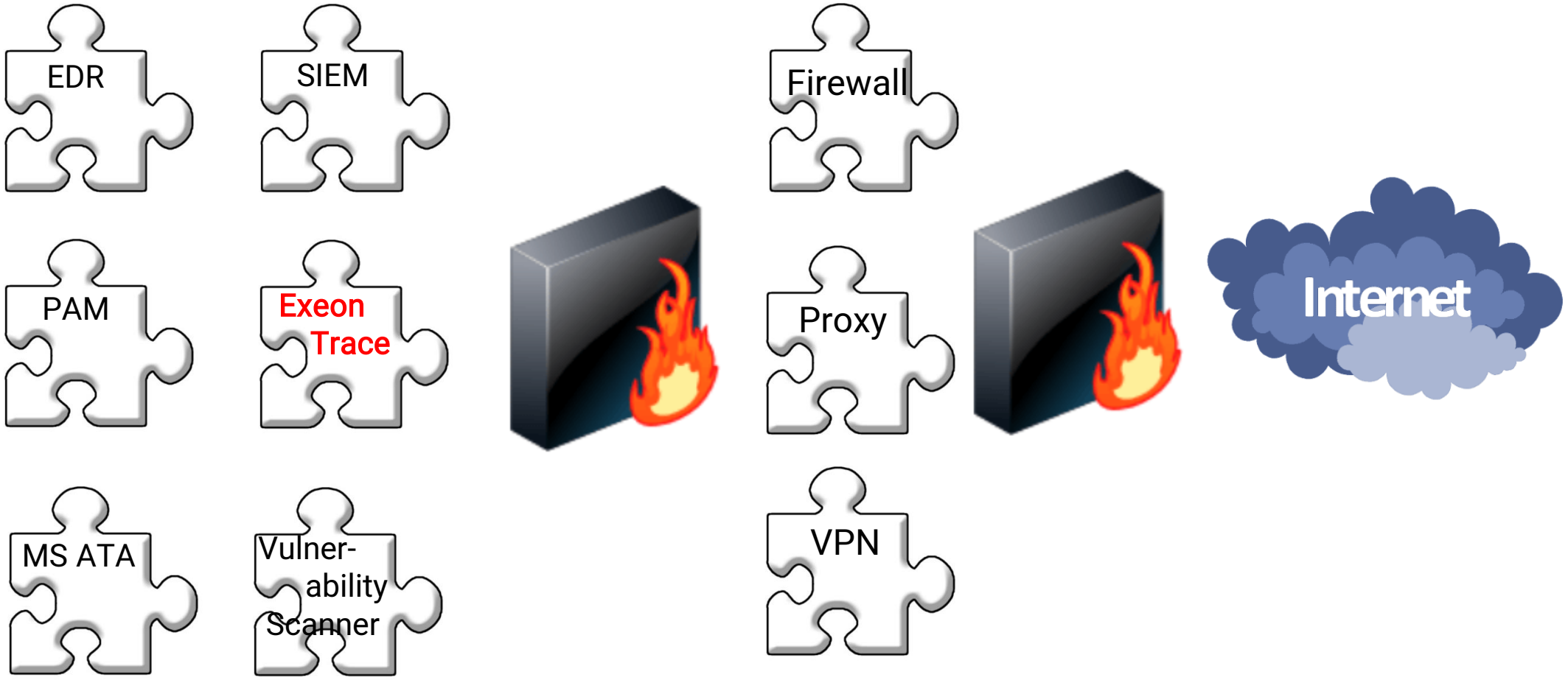
Einsatzgebiet von NDR:

- Kontrolle von Verbindungen nach außen (2.9 Security Monitoring)
- Übertragung ungewöhnlicher Datenmengen ins Internet (2.3 DLP)
- Analyse der Verbindungen und Übertragungen nach außen, bei Bedrohungsinformationen im Kontext mit zusätzlichen Security Tools (2.1 Threat Intelligence, 2.11 Incident Response)

3 Banken IT

exeon
Smart Cyber Security.

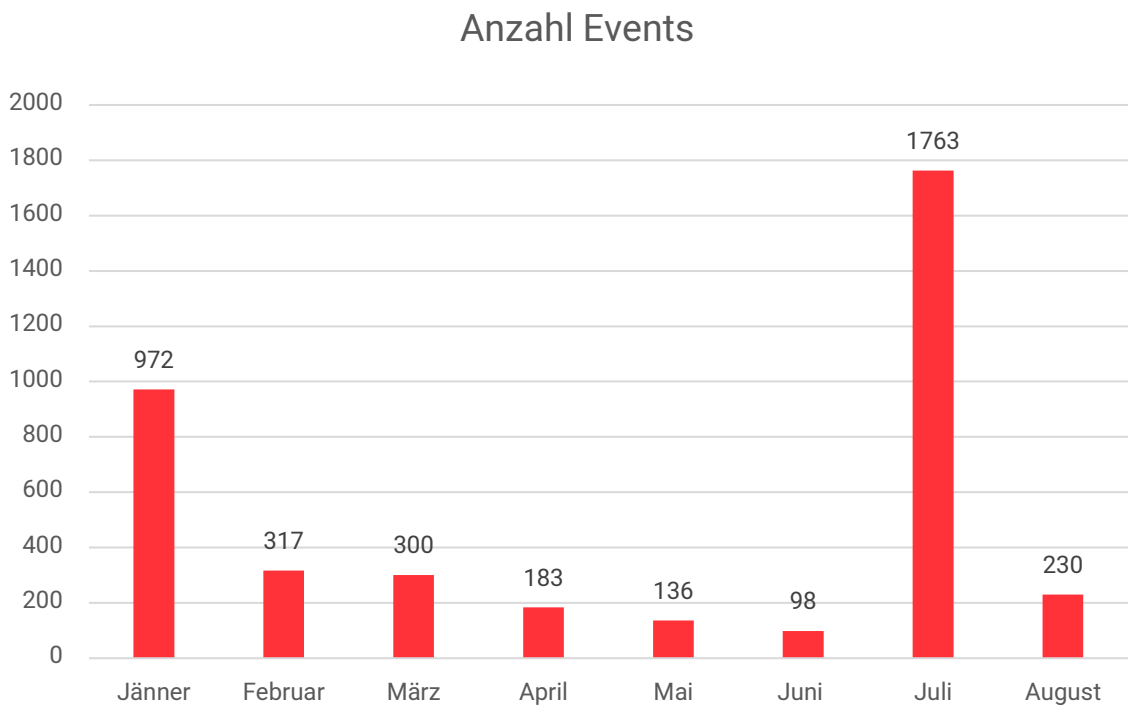
IT – Security - Tools



3 Banken IT

exeon
Smart Cyber Security.

IT – Security



Skills / Aufwand:

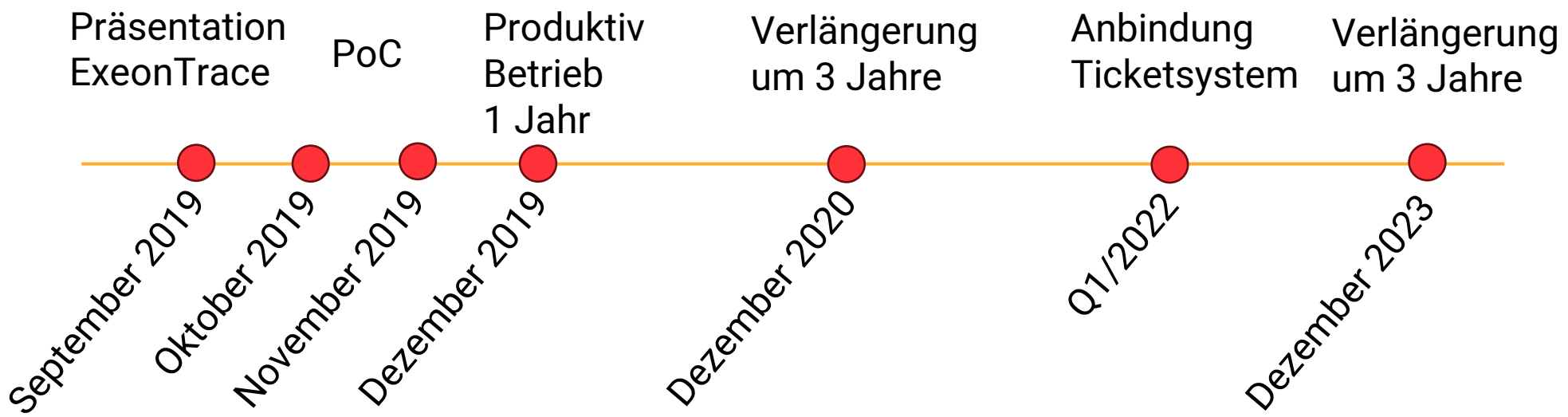
- Erfahrene MitarbeiterInnen mit Know-How über die Netzwerkinfrastruktur
- Bearbeitung der Events über Ticketssystem
- Täglicher Aufwand für die Eventkontrolle: ca. 1h

3 Banken IT

exeon
Smart Cyber Security.

IT – Security

Umsetzung:

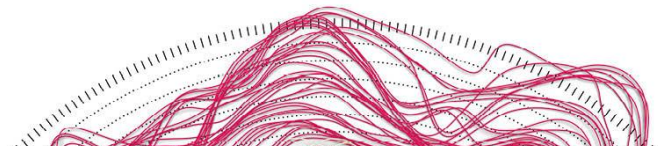


3 Banken IT

exeon
Smart Cyber Security.

Diskussionsrunde

- Eindringlinge bleiben oft lange Zeit unentdeckt. Verfügen Sie über Detektion-Tools, um diese zu erkennen?
- Ist eine Kombination mehrerer Detektion-Tools sinnvoll?
- Sind False Positives und eine grosse Anzahl an Alerts eine Herausforderung bei Ihnen?



3 Banken IT

exeon
Smart Cyber Security.

Take-Away

?