Herzlich Willkommen zu Securing the Future 2.0

Managed Services vom Endpoint bis zum 24/7 SOC

Das Wichtigste zuerst:

Danke!

Teilnehmende

Sprechende

Sponsoring

Orga-Team

Agenda: Ein intensives Programm

Securing the Future

08:30-08:45 Willkommen + CyberCompare Blick auf den Markt

Virtuelles Zusammentreffen und Willkommen

08:45-09:00 Keynote Speech Daniel Brettschneider

Daniel Brettschneider ist CISO bei Miele und Mitglied im CyberCompare Advisory Board

09:00-09:30 Warm-Up

In 60 Sekunden Pitches stellen die Speaker Ihre Session vor

09:30-12:25 Experten Sessions

12:30-12:45 Schlussworte

Offene Diskussion und Verabschiedung

Managed Security Services sind kundenseitig die **Top 1** nachgefragte Kategorie bei CyberCompare Ausschreibungen und Angebotsvergleichen

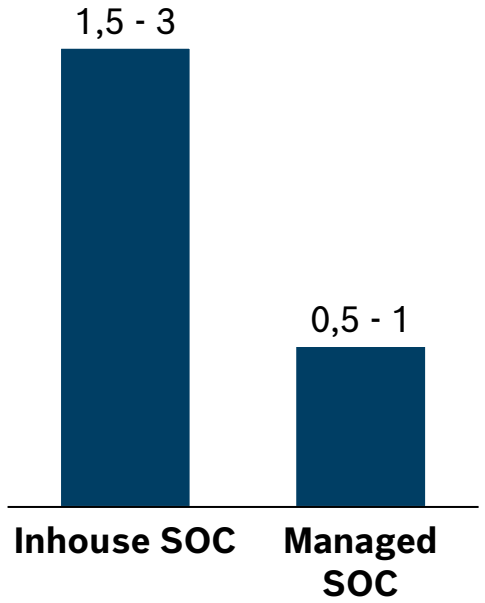
Effektivität der 24/7 Überwachung und Reaktion

- Gesunder Menschenverstand: Ohne Überwachung und ohne schnelle Reaktion haben Angreifer es einfach(er)
- „Best Practices“ und Empfehlungen
- Anforderungen von Cyberversicherungsträgern
- Standards + Regulatorische Anforderungen (z.B. ISO 27002 12.4; NIST CSF SI-4; KRITIS Systeme zur Angriffserkennung)

+

Skaleneffekte durch Bündelung

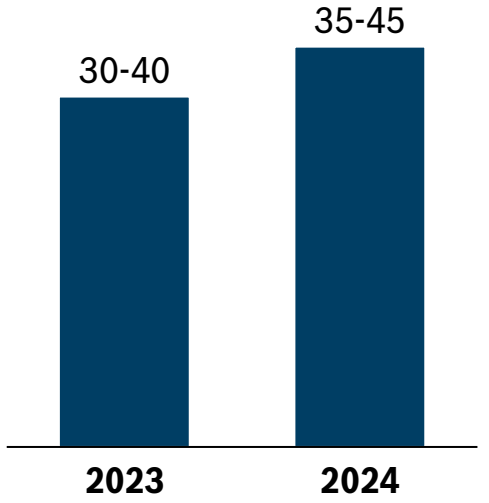
Kostenindikation, Mio. EUR/Jahr



=

Hohe Kundennachfrage

Globaler Markt für Managed Security Services, Mrd. USD



Quellen der Abschätzungen und Wachstumsraten: Mordor Intelligence, Allied Market Research, Gartner

Typische Fragestellungen bei Managed Detection and Response (MDR) / Managed Security Operations Center (MSOC)

- Tech-Stack: XDR vs. EDR+SIEM
- Priorisierung weiterer Log-/Eventquellen oder Zusatzmodule neben AV/EDR: Z.B. AD / Identity Protection, Firewalls, DHCP/DNS Server, NDR, Mobile, Email
- Unabhängiger MSSP oder XDR-Hersteller
- Microsoft E3/E5
- Reaktionsmöglichkeiten
- SLA (Reaktionszeiten)
- Follow-the-sun / Schichtmodelle
- DSGVO
- Umgang mit „Indeterminates“
- Wann beginnt „Incident Response“ vs. „Security Incident-Analyse + Reaktion“?
- Umgang mit OT und Enterprise IoT
- Pricing: Lizenzen / Preismodelle z.B. abhängig von # Endpunkte oder #Logvolumen oder #M365-Nutzer

Agenda

Securing the Future

08:30-08:45 Willkommen + CyberCompare Blick auf den Markt
Virtuelles Zusammentreffen und Willkommen

08:45-09:00 Keynote Speech Daniel Brettschneider
Daniel Brettschneider ist CISO bei Miele und Mitglied im CyberCompare Advisory Board

09:00-09:30 Warm-Up
In 60 Sekunden Pitches stellen die Speaker Ihre Session vor

09:30-12:25 Experten Sessions

12:30-12:45 Schlussworte
Offene Diskussion und Verabschiedung

Agenda: Ein intensives Programm

Securing the Future

08:30-08:45 Willkommen + CyberCompare Blick auf den Markt
Virtuelles Zusammentreffen und Willkommen

08:45-09:00 Keynote Speech Daniel Brettschneider
Daniel Brettschneider ist CISO bei Miele und Mitglied im CyberCompare Advisory Board

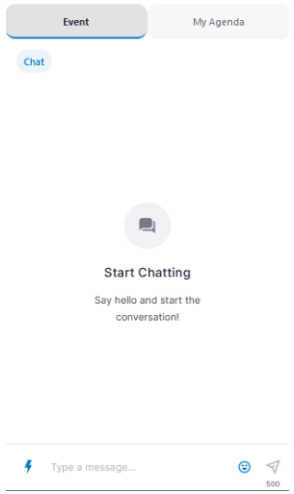
09:00-09:30 Warm-Up
In 60 Sekunden Pitches stellen die Speaker Ihre Session vor

09:30-12:25 Experten Sessions

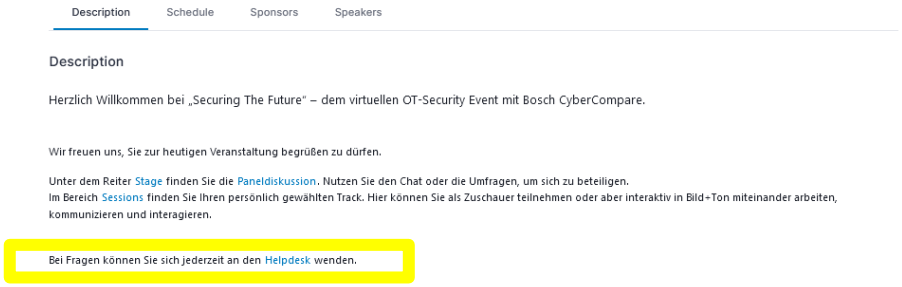
12:30-12:45 Schlussworte
Offene Diskussion und Verabschiedung

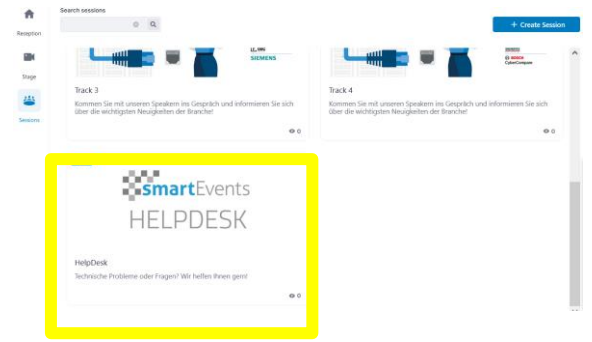
Wir hoffen auf eine angeregte Diskussion

- Fragen stellen gerne über Chatfenster an Seite:



- Help Desk finden Sie auf der Startseite:

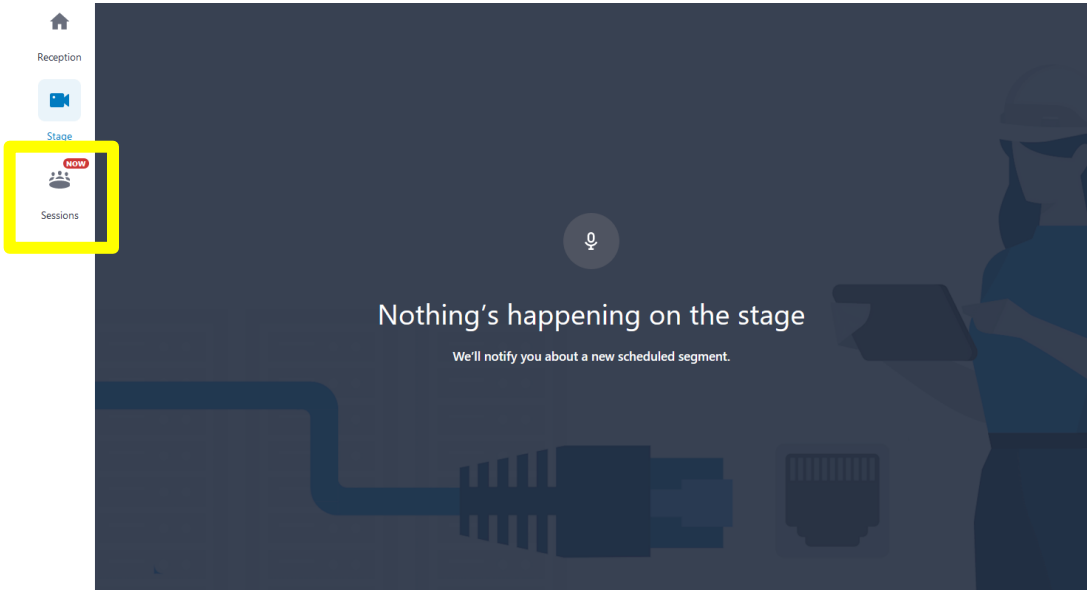




CyberCompare BOSCH

Wir hoffen auf eine angeregte Diskussion

- Wir sind nun auf der Main Stage, um in Ihren Track zu gelangen, bitte auf die jeweiligen Sessions klicken



- Wir stellen alle Präsentationen, eine Aufzeichnung der Paneldiskussion und Kontaktdaten der Sprecher im Nachgang bereit

Für Sie heute dabei: Unsere Sprechenden mit Erfahrung aus der Praxis

Securing the Future

Sprechende

Thino Ullmann
sure[secure]

Mathias Fuchs
infoGuard SWISS CYBER SECURITY

Terence Canaday
ARCTIC WOLF

Götz Schartner
8COM CYBER SECURITY

Christian Bohr
controlware

Alexander Schmidt
OBRELA

Zrinka Maslic
KUDELSKI SECURITY

Peter Klein
W/T H secure

Philipp Rieblinger
orange Cyberdefense

René Odermann
telent service • commitment • value

Nicolas Wehmeyer
CROWDSTRIKE

Thomas Maxeiner
paloalto NETWORKS

Olaf Müller-Haberland
<TEHTRIS>

Friedrich von Jagwitz
graylog

Thomas Jupe
orange Cyberdefense

Christopher Johannes
orange Cyberdefense

Richard Wieneke
corelight

Stefan Linning
W/T H secure

Michael Veit
SOPHOS

Für Sie heute dabei: Moderation

Securing the Future

Moderation

Jannis Stemmann
CyberCompare

Christine Schwanebeck
CyberCompare

Philipp Pelkmann
CyberCompare

Simeon Mussler
CyberCompare

Agenda

Securing the Future

08:30-08:45 Willkommen + CyberCompare Blick auf den Markt
Virtuelles Zusammentreffen und Willkommen

08:45-09:00 Keynote Speech Daniel Brettschneider
Daniel Brettschneider ist CISO bei Miele und Mitglied im CyberCompare Advisory Board

09:00-09:30 Warm-Up
In 60 Sekunden Pitches stellen die Speaker Ihre Session vor

09:30-12:25 Experten Sessions

12:30-12:45 Schlussworte
Offene Diskussion und Verabschiedung

Expert Sessions

Securing the Future

SOC/MDR 1

Moderation

Jannis Stemmann
CyberCompare

Thino Ullmann
SureSecure

Götz Schartner
8com

Mathias Fuchs
Infoguard

Christian Bohr
controlware

Terence Canaday
ArcticWolf

Alexander Schmidt
Obrela

SOC/MDR 2

Moderation

Christine Schwanebeck
CyberCompare

Zrinka Maslic
Kudelski Security

Philipp Rieblinger
Orange Cyberdefense

Olaf Müller-Haberland
Thetris mit Nomios

René Odermann
Telent

Peter Klein
withsecure

Nicolas Wehmeyer
Crowdstrike

CyberCompare BOSCH

Expert Sessions

Securing the Future

SIEM/XDR

Moderation

Philipp Pelkmann
CyberCompare

Logpoint

Olaf Müller-Haberland
Thetris

Götz Schartner
8com mit Logpoint

Friedrich von Jagwitz
graylog

Thomas Maxeiner
Palo Alto

Thomas Jupe
Orange Cyberdefense

EDR/NDR

Moderation

Simeon Mussler
CyberCompare

Thomas Maxeiner
Palo Alto

Ontinue

Christopher Johannes
Orange Cyberdefense

Stefan Linning
WithSecure

Richard Wieneke
Corelight

Michael Veit
Sophos

Agenda

Securing the Future

08:30-08:45 Willkommen + CyberCompare Blick auf den Markt
Virtuelles Zusammentreffen und Willkommen

08:45-09:00 Keynote Speech Daniel Brettschneider
Daniel Brettschneider ist CISO bei Miele und Mitglied im CyberCompare Advisory Board

09:00-09:30 Warm-Up
In 60 Sekunden Pitches stellen die Speaker Ihre Session vor

09:30-12:25 Experten Sessions

12:30-12:45 Schlussworte
Offene Diskussion und Verabschiedung

Verabschiedung

Securing the Future

Was nehmen Sie aus dem heutigen Tag mit?

Wie sehen Sie die Zukunft der MSSP?

Was sind Ihre nächsten Security Schritte ?

LOGPOINT CROWDSTRIKE KUDELSKI SECURITY SOPHOS paloalto NETWORKS Ontinue Cyberdefense InfoGuard SWISS CYBER SECURITY OBRELA

8COM CYBER SECURITY sure[secure] controlware graylog corelight ARCTIC WOLF <TEHTRIS> telent service • commitment • value WITH secure

Vielen Dank für Ihre Teilnahme.

Bis zum nächsten Mal!


KORAMIS
Cybersecurity by telent

FACTS & FIGURES

Geschäftsbereiche

Kommunikationsnetze, 5G-/IoT-Campusnetze, Campus & Data Center, Professioneller Mobilfunk, Cybersecurity, Technology Services

Kunden

KRITIS-Betreiber, öffentliche Hand, Industrieunternehmen insb. aus den Branchen Verkehr, Energie, ITK

Team

550 Mitarbeiterinnen & Mitarbeiter

Standort

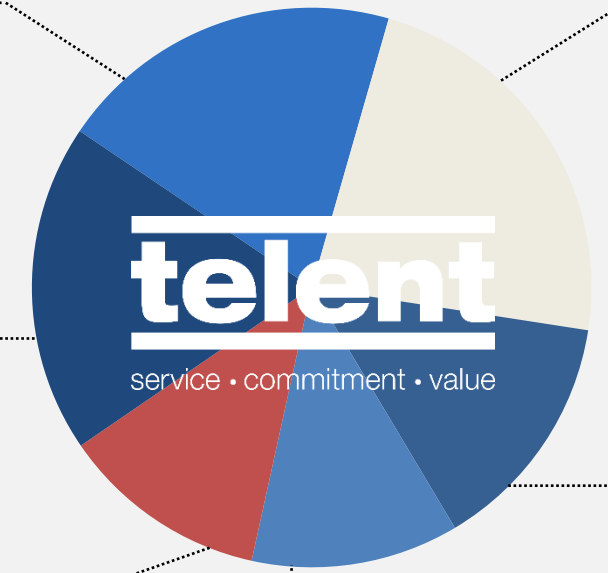
Firmensitz Backnang (Baden-Württemberg)

bundesweit Regionalbüros & 24/7 Servicepoints

Tochter der GZS Digital

KORAMIS
Cybersecurity by telent

Kundensegmente



Bahn & ÖPV

DB · ASEAG · gevb · Schönbuchbahn

Transport & Luftfahrt

TOLL COLLECT service on the road · Die Autobahn · DFS Deutsche Flugsicherung · WSV.de

Behörden

Industrie

Mercedes-Benz · Merck · DOW · spier Fahrzeugwerk · RIVA Engineering · LSU Schäberle Logistik & Speditions-Union

Versorgungsunternehmen

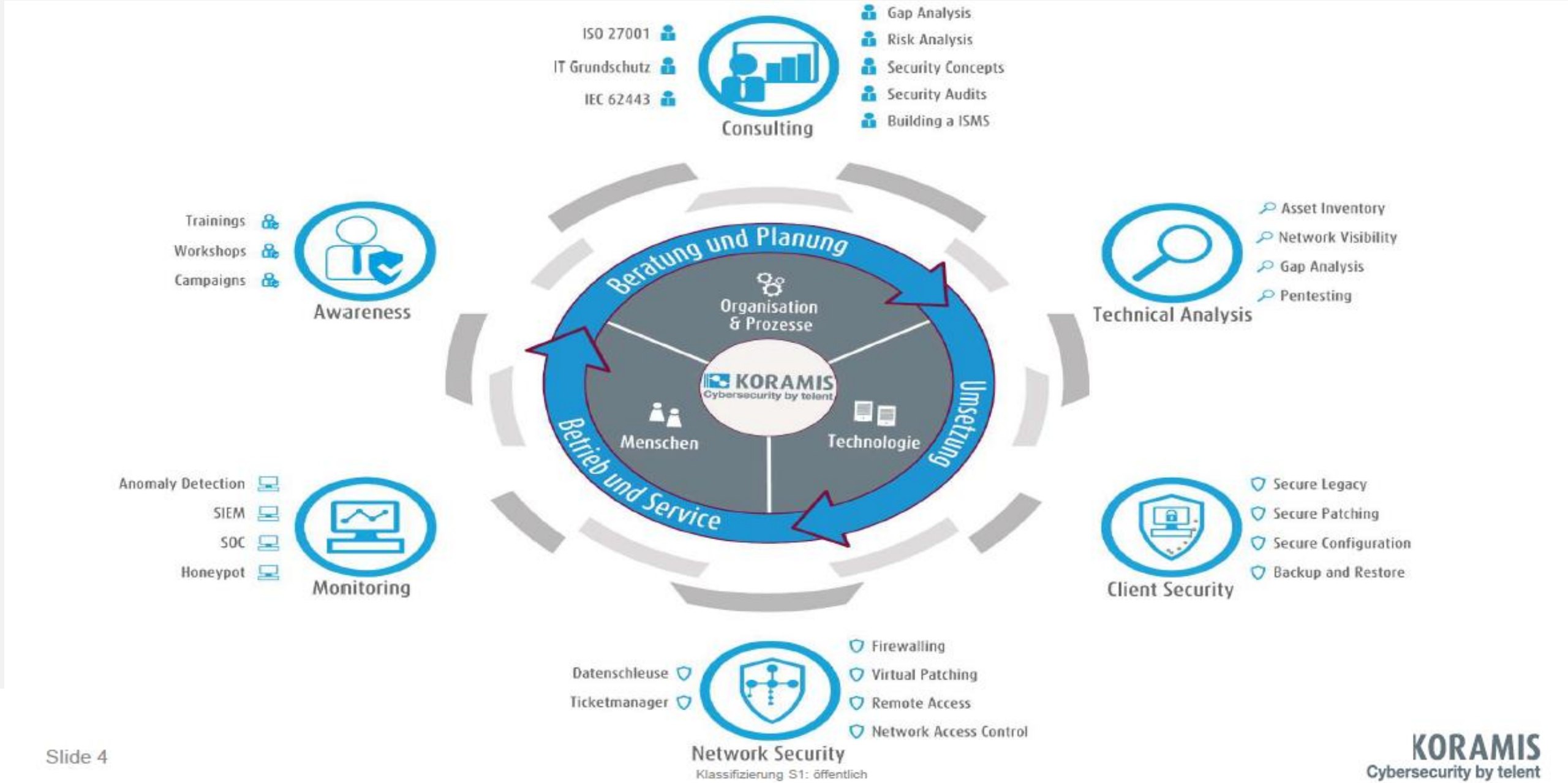
e·on · 50hertz · TRANSNET BW · westenergie · EnBW · TenneT · EnergieDienst · SW//M · RHEIN-RUHR · FWF · bayerngas

Telekommunikation & Medien

Deutsche GigaNetz · colt · Thüringer Netkom · PŸUR · NetCom BW · vodafone · BT · SWR · BR · ropa carrier solutions · Stadtwerke Münster · fibernet.rn · NHF

KORAMIS Cybersecurity by telent

Unser Leistungsspektrum



KORAMIS
Cybersecurity by telent

…ber zehn Jahre Erfahrung…

…n der
…rmations-
…erheitsberatung

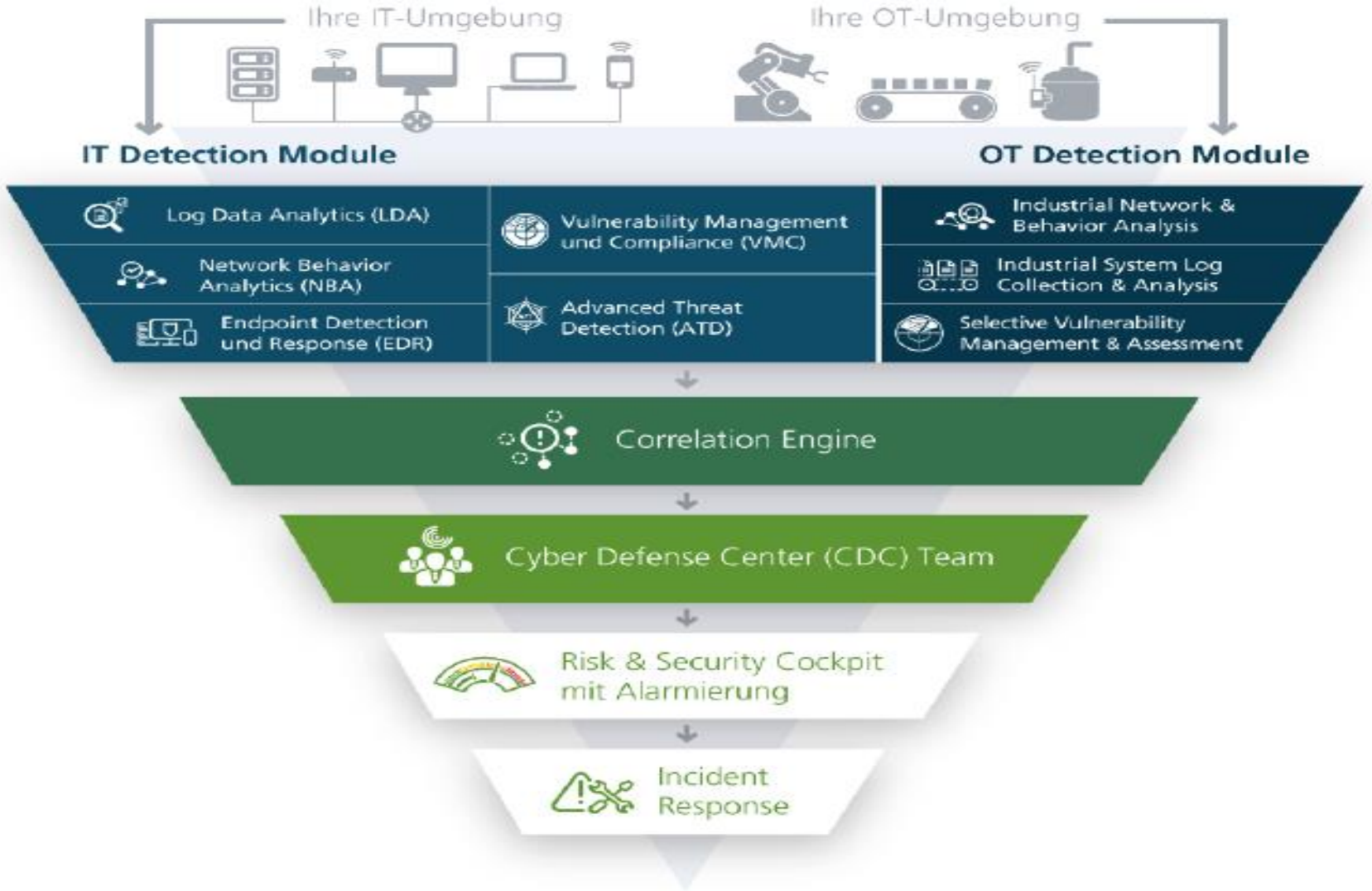
… in der
Implementierung
von Cyber Defence
Centern (CDC)

…n der
…ringung
SOC as a Service

… mit
Cyber Security
Technologien

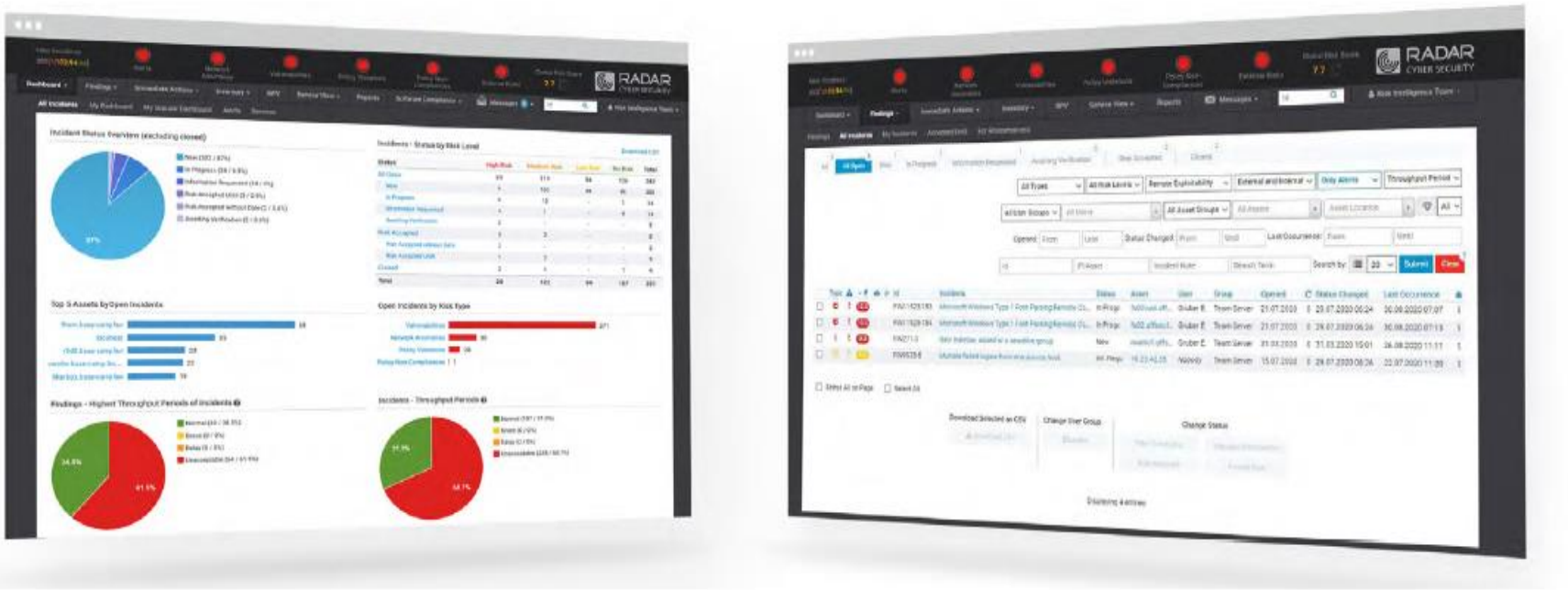
MATERNA
RADAR
CYBER SECURITY

Security Operation Center



12

KORAMIS
Cybersecurity by telent



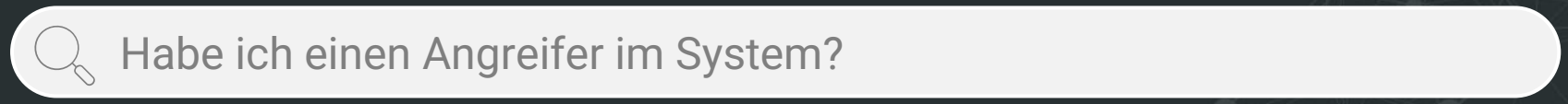
Risk & Security Cockpit

Im Risk & Security Cockpit werden Ergebnisse aus der Sicherheitsanalyse und -bewertung dargestellt. Diese dienen als Grundlage für die Festlegung von Gegenmaßnahmen im Fall von gemeldeten Cyberangriffen. Analysierte Risiko- und Sicherheitsbenachrichtigungen werden zentral im Risk & Security Cockpit präsentiert. Maßgeschneiderte und leicht verständliche Risikoberichte und Statistiken sind auf Knopfdruck verfügbar.

sure[secure]

CyberCompare - SOC/MDR

IT-Security made with


Habe ich einen Angreifer im System?

PAINS & NEEDS

SOC AS A SERVICE - HERAUSFORDERUNGEN

Ressourcen

- Fachkräfte
- 24x7 Monitoring

Anforderungen

- NIS2, IT-SiG 2.0, BSI
- Datenschutz
- Cyberversicherung

Komplexität

- Plan-Build-Run-Optimize
- IT, OT, IoT

Geschwindigkeit

- People
- Process
- Products

Aufwand für den SOC-Aufbau (intern/extern)

- Aufbau notwendiger SOC-Strukturen etwa einer 24x7 Überwachung, bindet viele Ressourcen und Budget. Dazu kommt die ständige Gefahr der Technologie-Obsoleszenz, welche den Aufwand weiter erhöht.

	INTERN AUFBAUEN	EXTERN VERGEBEN
Kosten	↑	→
Anpassungs-fähigkeit	↑	↗
Expertise	↘	↑
Skalierbarkeit (abhängig vom Betriebsmodell)	→	↑
Implementierungs- und Zeitaufwand	↑	↘

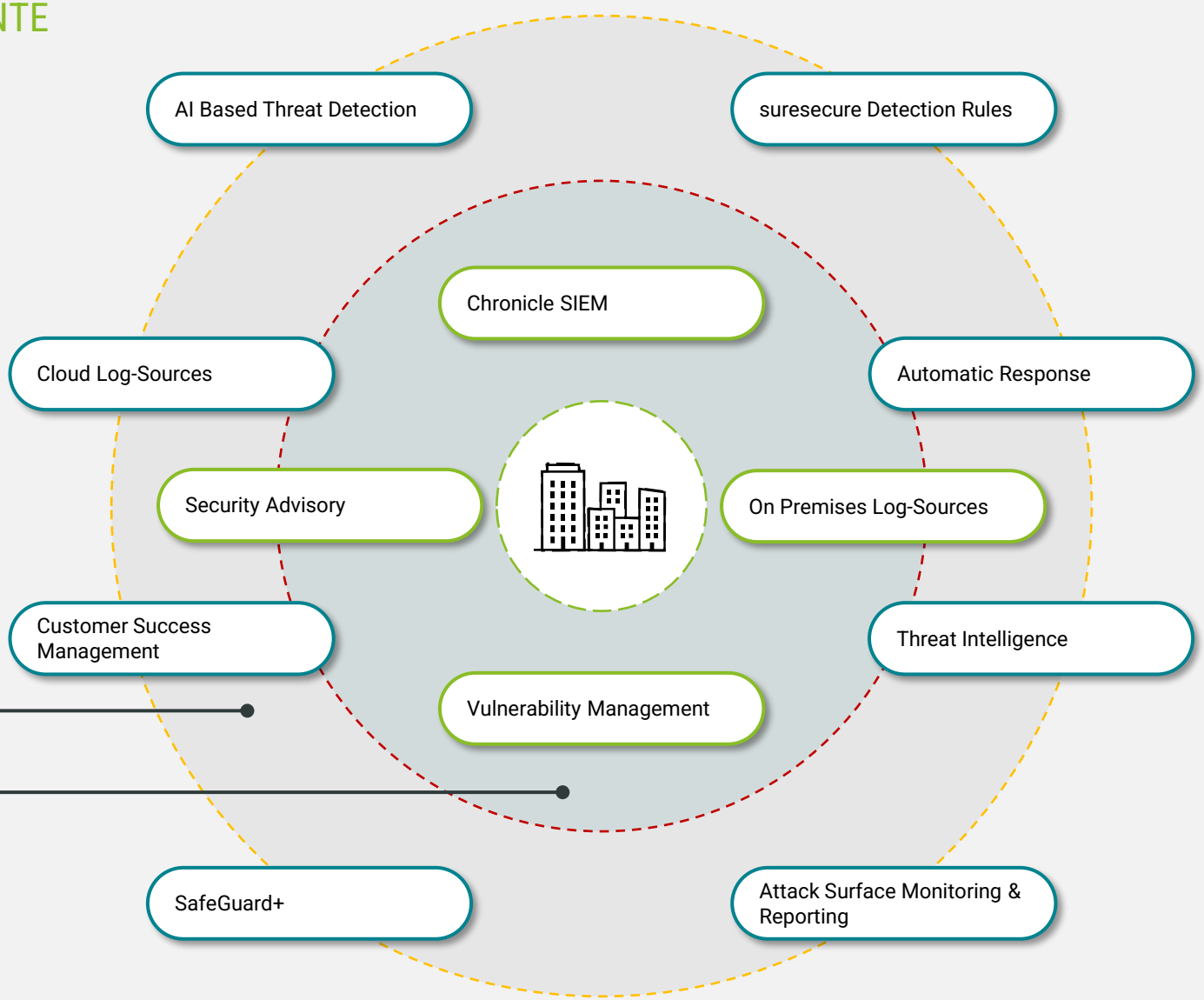
Shared Responsibility Model

PRODUCTS – VIELFÄLTIGE, KOMPLEXE ANGRIFFSVEKTOREN

SOC AS A SERVICE - ELEMENTE

PRODUCTS – DEFENSE LAYER

SOC AS A SERVICE - ELEMENTE



1st DEFENSE LAYER

2nd DEFENSE LAYER

Tools & Technology

VIRUSTOTAL

Chronicle

MANDIANT

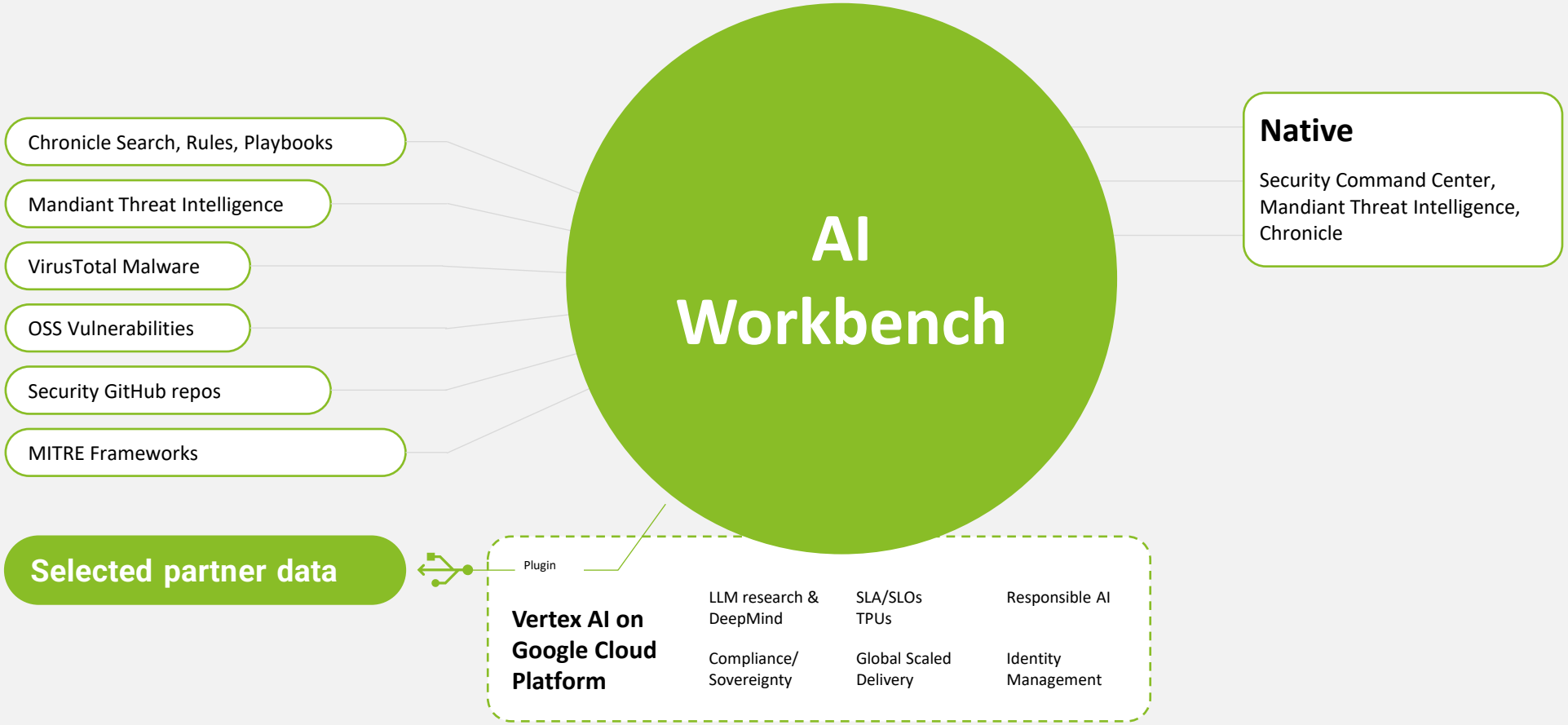
Google Cloud Partner

splunk>

Qualys.

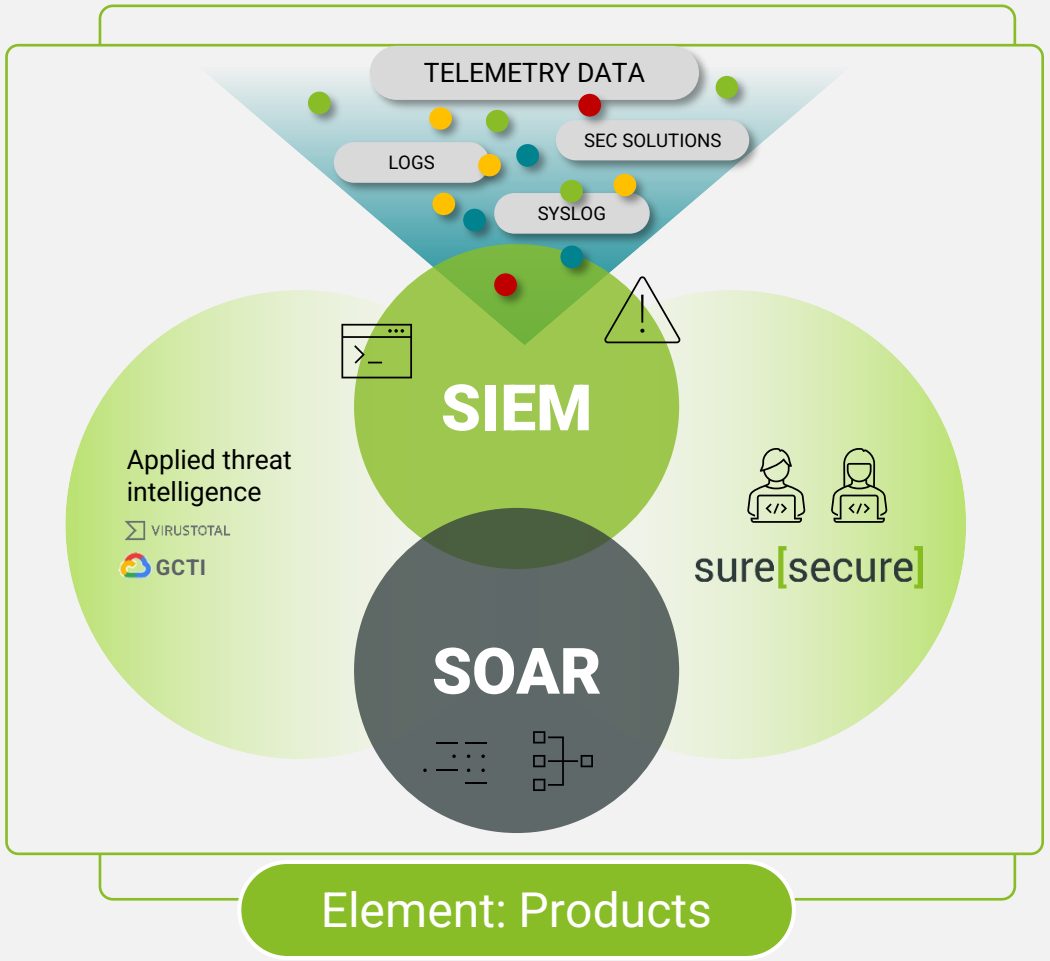
PRODUCTS – SECURITY AI-WORKBENCH

SOC AS A SERVICE - ELEMENTE



PRODUCTS – KONZEPT

SOC AS A SERVICE - ELEMENTE



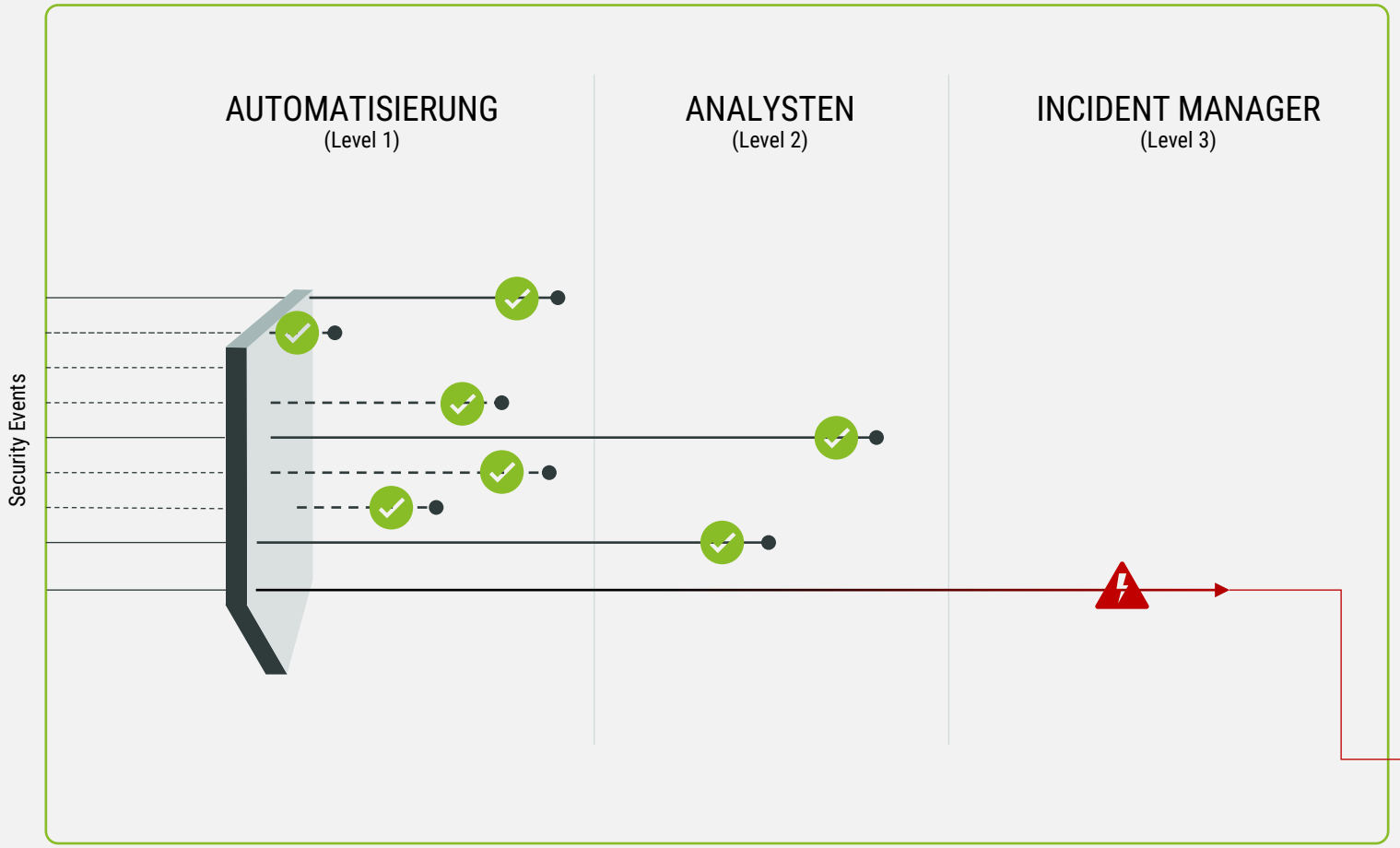
Moderne SaaS-Architektur mit Google

- Anbindung von Cloud-Lösungen und on-premise IT- und OT-Systemen
- Suchen und analysieren mit Google-Geschwindigkeit
- Cloud-First Ansatz, um Betriebskosten zu minimieren
- Mehr als 700 umfangreiche Custom Use-Cases + Curated Rules durch Google
- Eigene und hersteller-basierte Playbooks
- Security AI-Workbench

Google Cloud Partner

PROCESS - HERZSTÜCKE EINES SOCS

SOC AS A SERVICE - ELEMENTE

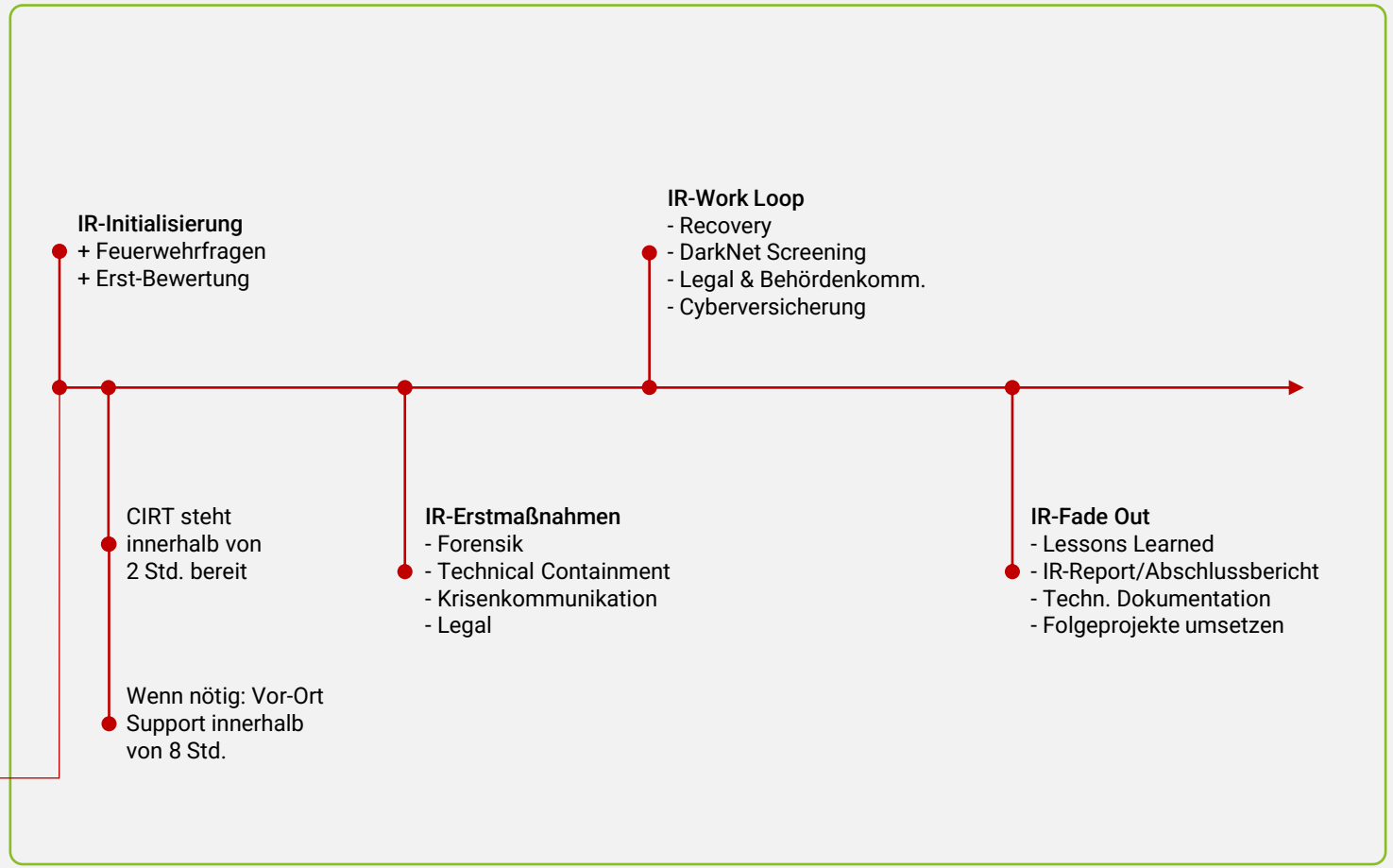


Standards sorgen für konstante Qualität

- Eindeutige Prozesse und klare Eskalationsstufen
- Hoher Grad an Automatisierung durch Detection Rules & Playbooks
- Im Falle eines Incidents: sofortige Bereitstellung eines Managers sowie CIRT
- Erfahrungen, Erkenntnisse und Angriffsmuster aller SOC-Partner werden Verarbeitet

PROCESS - HERZSTÜCKE EINES SOCS

SOC AS A SERVICE - ELEMENTE



Security Incidents

- **Geschwindigkeit**
  Wir wissen um die Situation, deshalb reagieren wir sofort
- **Ganzheitliche Betreuung**
  Unser Framework steht bei Bedarf sofort und komplett zur Verfügung
- **Transparenz**
  Tägliche Reportings über Budgetplanung und Progress
- **Erfahrung und Expertise**
  Als First Mover im Bereich Incident Management haben wir einen hohen Reifegrad

SOC mit Speed

- Kontinuierliches Monitoring der Security Events
- Hoher Automatisierungsgrad sorgt für hohe Kosteneffizient
- Schnelle Reaktion auf Security Incidents
- Verbesserte Threat Intelligence
- Skalierbar und flexible Lösung
- Next-Generation SOC mit modernster Technologie
- Cloud-based mit Google Geschwindigkeit

LinkedIn

[s]

sure[secure]

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de

/suresecure.gmbh

/suresecure-gmbh

/SuresecureD

/suresecuregmbh

/suresecure GmbH

/the world of it security

/suresecure_de

IT-Security made with

Ist alles nur noch XDR & SIEM?

Wie Orange Cyberdefense mit EDR Ihre IT-Security stärken kann.

Christopher Johannes, Portfolio Manager

orange™ Cyberdefense

Agenda

- „Wer bin ich – und wenn ja, wie viele?“
- Orange Cyberdefense im Überblick
- Ist alles nur noch XDR & SIEM?
- EDR mit Orange Cyberdefense

„Wer bin ich – und wenn ja, wie viele?“

- Name: Christopher Johannes
- Alter: 37
- Status: verheiratet, 1 Kind
- Karriere: 17 Jahre in der IT, 1 Jahr bei Orange Cyberdefense

Orange Cyberdefense

Führender europäischer MSSP

The Forrester Wave™: European Managed Security Services Providers (MSSPs), Q3 2022

"Top-Anbieter für Managed Detection und Response"

Gartner

Security-Umsatz 2022

ca. € 977 Mio.

3.600+
Hoch-qualifizierte Cyber-sicherheits-experten einschließlich

1.000
Security Consultants

Competence and Training Center ISH Flughafen München

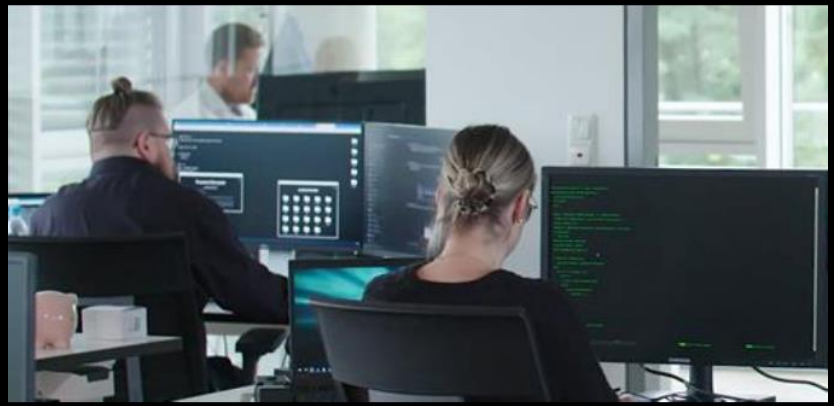
Cybersecurity Experience Center Antwerpen

OT Demo Center Lyon

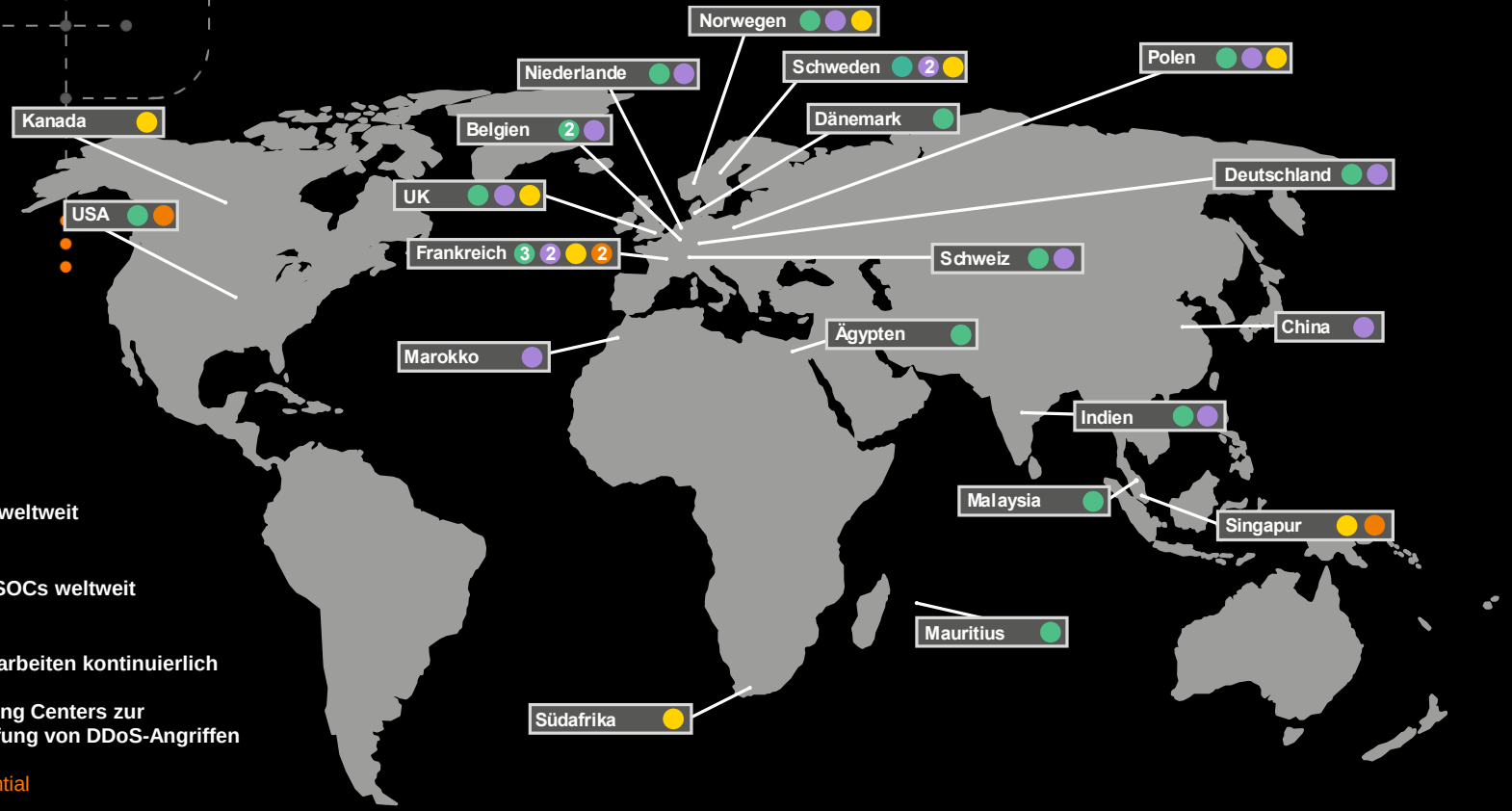
Weltweit
18 SOC's
8 CERT's
4 Scrubbing Centers

24/7/365
Kontinuierliches Monitoring von sicherheits-relevanten Systemen

Wo finden Sie uns?



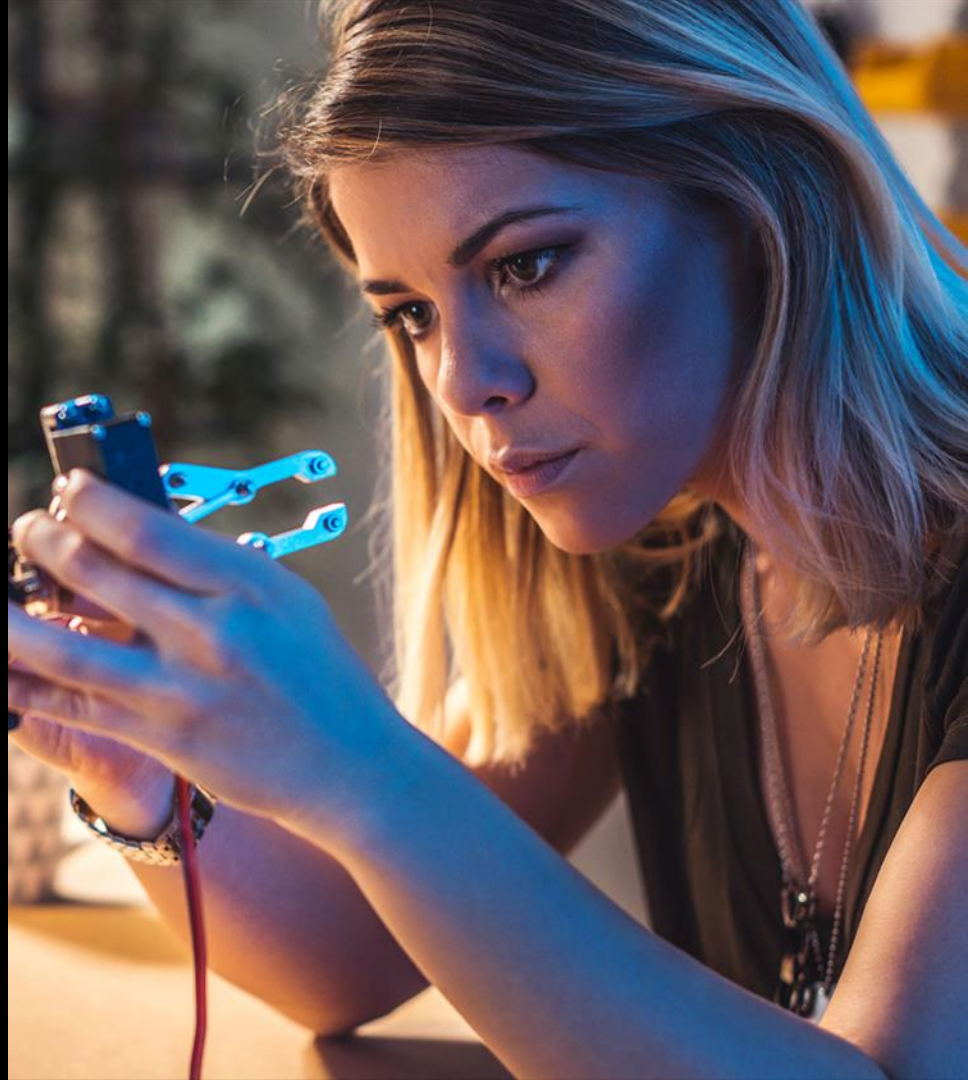
Wir sprechen Ihre Sprache

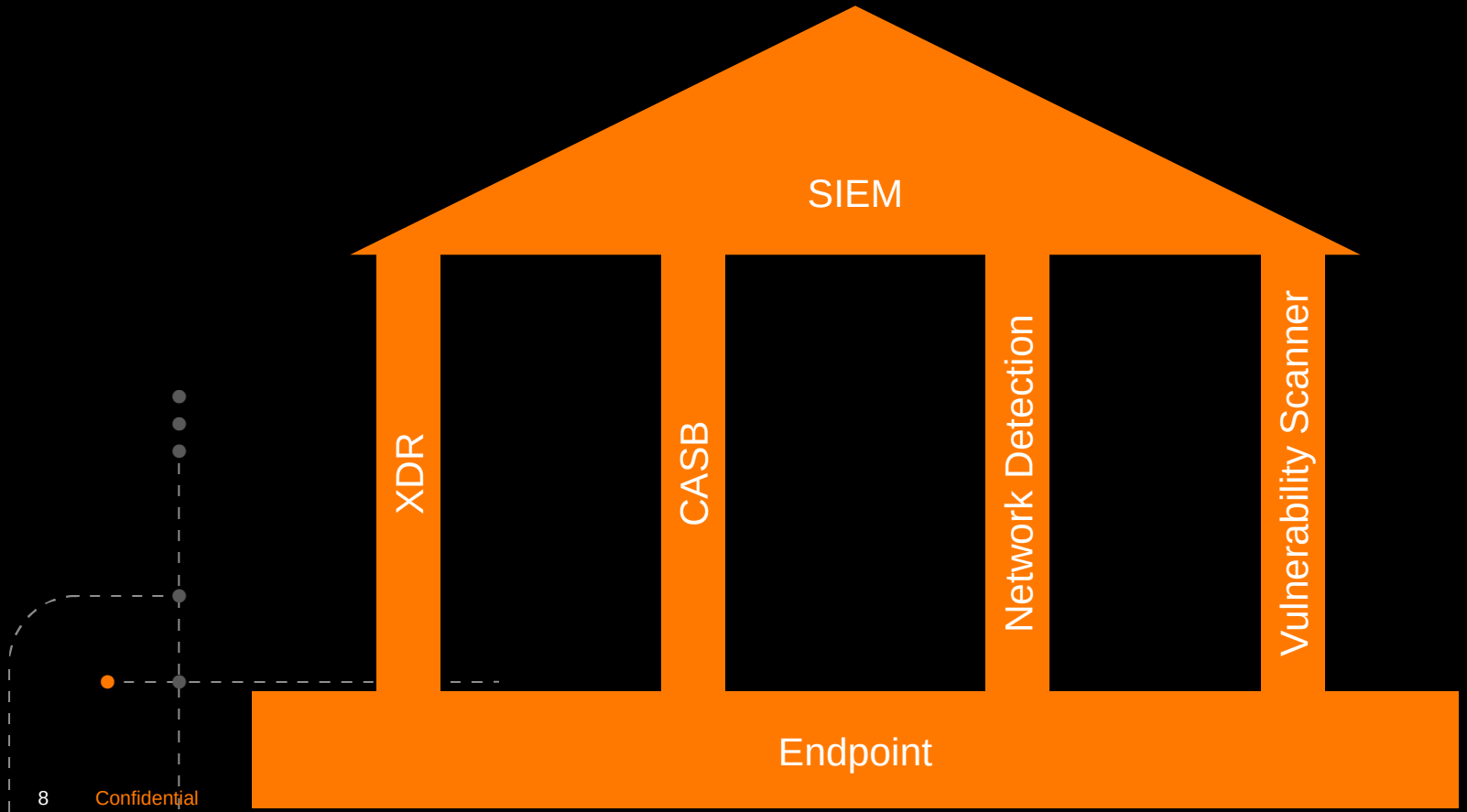


- 18 SOCs weltweit
- 14 CyberSOCs weltweit
- 8 CERTs arbeiten kontinuierlich
- 4 Scrubbing Centers zur Entschärfung von DDoS-Angriffen

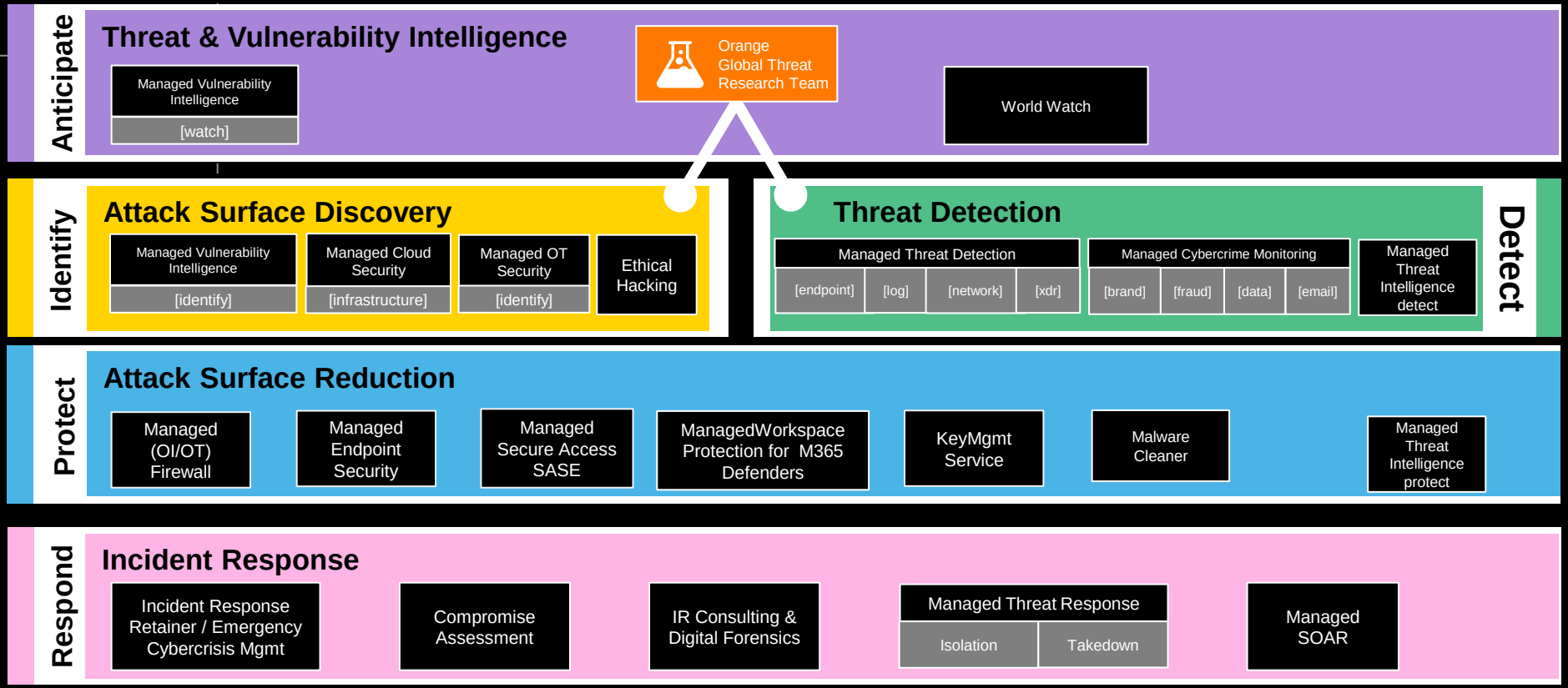
Ist alles nur noch XDR & SIEM?

NEIN!

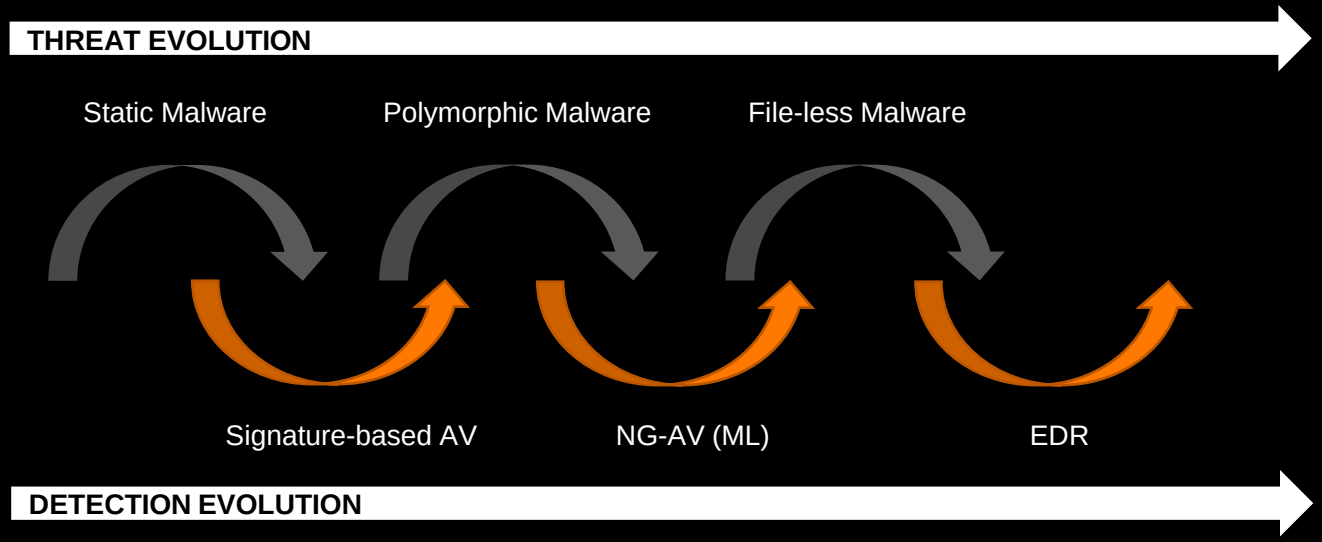



SIEM
XDR
CASB
Network Detection
Vulnerability Scanner
Endpoint

Intelligence-led Managed Services



Traditional tools are not sufficient



80%

of successful attacks use file-less malware*

60%

of attacks are not effectively blocked by traditional AV tools*

* Ponemon 2020 Endpoint Security Statistisc Trends

Challenge

How to efficiently protect endpoints against known and unknown threats?

Cutting complexity

Securing endpoints in an ever-growing environment without increasing complexity, costs and the number of endpoint security solutions.

Combating the threat landscape

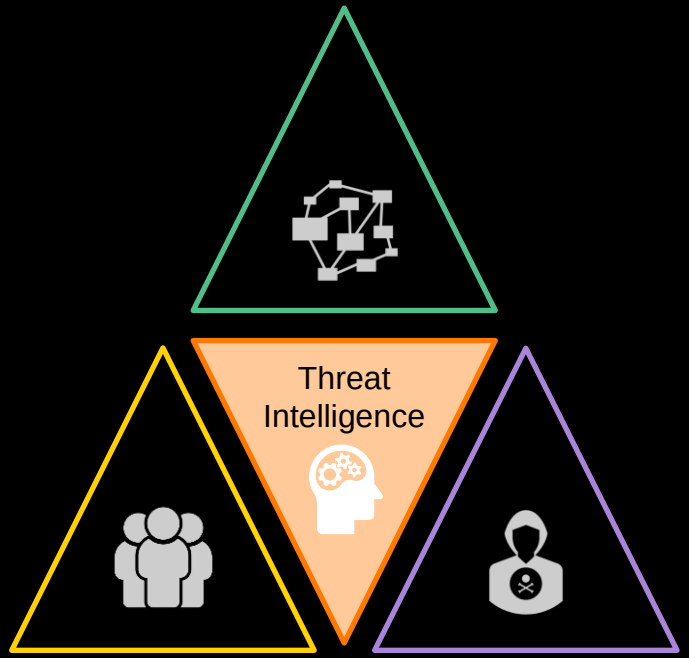
Protecting endpoints from known threats, detecting unknown sophisticated attacks and quickly take appropriate response actions.

Lack of expertise and resources

Effectively configure and manage tools to reduce alert fatigue, professionally investigate and respond to incidents and proactively hunt threats.

Our managed endpoint security approach

End-to-end intelligence-led endpoint security



End-to-End endpoint security

Effective endpoint security combines prevention, detection and response in one solution with cross-machine correlation for an enterprise-wide view.

Intelligence-led security

Powered by our unique threat intelligence to enrich detection context providing fast and effective analysis, reduce alert fatigue and to enable efficient threat hunting.

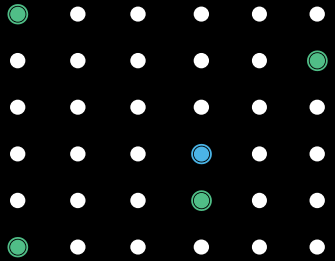
Fast Detection & Response

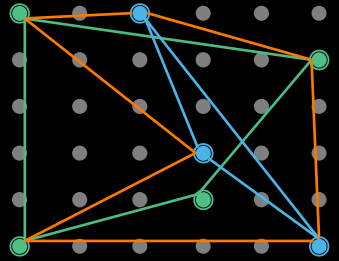
Security Analysts on hand 24x7 to isolate threats and limit the impact of breaches.

Skilled resources

Combining highly skilled Security Analysts and specialized Endpoint Engineers with the ability to optimize configurations and query a huge set of endpoint telemetry to utilize endpoint tools efficiently.

Managed Threat Detection [endpoint]





Isolated endpoint security solutions

- Data is stored on disk
- Data analysis is manual
- Generates redundant alerts
- One alert for each affected machine

Multi-layered endpoint security solutions

- Data **remains in memory**
- Data is **enriched and correlated**
- Aggregates **the whole attack**
- One alert for **all affected machines**

Managed end-to-end endpoint security service

- ✓ All endpoint events in a single pane of glass
- ✓ Faster and more accurate security analysis
- ✓ Combined service and license costs
- ✓ One endpoint agent for endpoint security

End-to-End endpoint security

Prevention, Detection, Response

Preventive Actions

- Malware Prevention
- Memory Exploit Prevention
- Script Prevention
- Device usage policy enforcement
- Anti-Ransomware
- Endpoint controls

Proactive EPP Agent Monitoring

Deliverables are either Monthly, Quarterly or Yearly based on the contract:

- Remove deprecated endpoints
- Remove duplicate endpoints
- Groups- and policy review
- Endpoint software EOL
- Customer user review

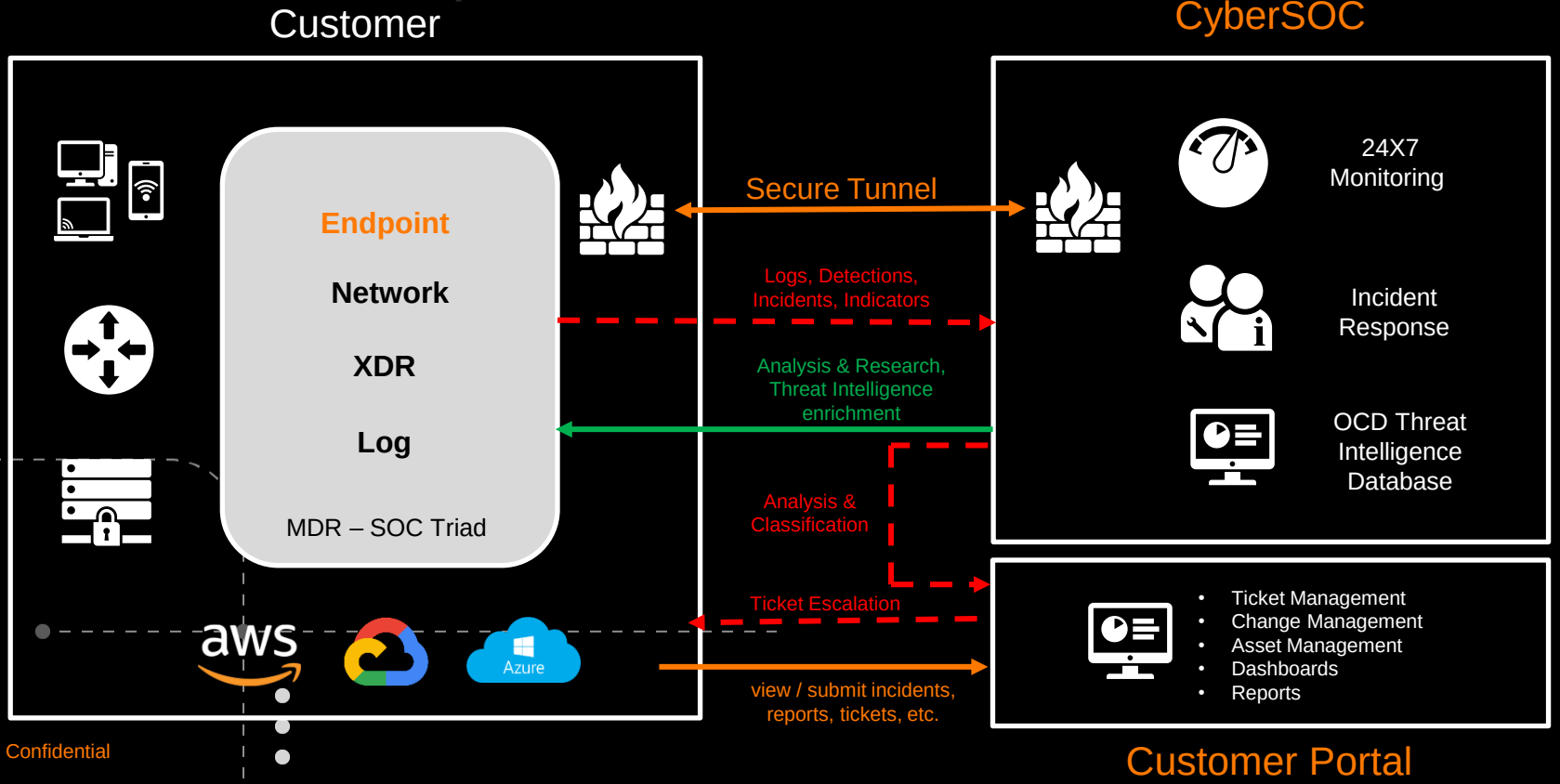
The Threat Clean Service

A structured approach for deployment, cleaning up existing threats and tuning the EPP agents for your specific environment and delivering:

- Policy that aligns with your business
- Identifies and allows approved software to run
- Implements enhanced features

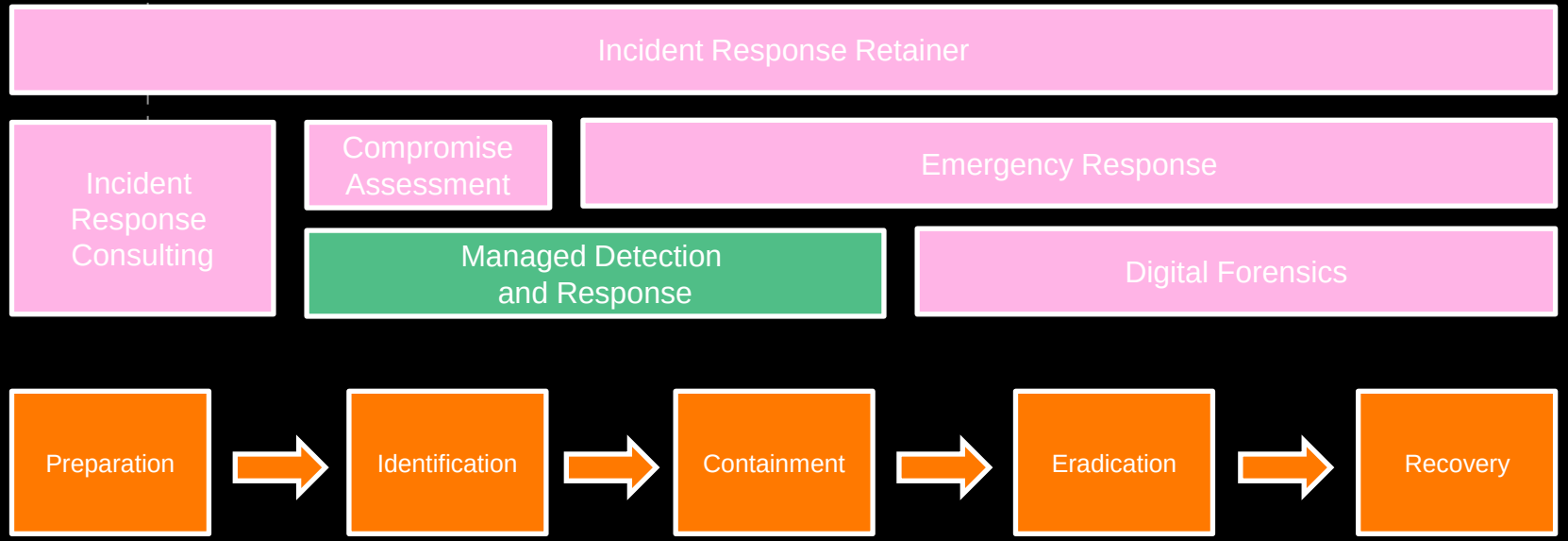
End-to-End endpoint security

Prevention, Detection, Response



End-to-End endpoint security

Prevention, Detection, **Response**



Operational synergies via Core Fusion

Teams

CERT

SOC

CyberSOC

Core Fusion Platform

Alert Flow Normalization

Data Enrichment

Case Proximity Routing

Security Orchestration

Guided Response Actions

Data Analysis & Reporting

Portal

Threat Intelligence Platform

SOAR Platform

Case Management

Proprietary Malware Analysis Tools

Proprietary Cybercrime Analysis Tools

Customers

Services

Public Cloud Services

Private Cloud Services

OnPrem / Endpoint Services

OT / ICS Services

Vielen Dank!

„Wer bin ich – und wie erreichen Sie uns?“

Call: 089 2000 148 00 oder 1428

Mail: info@de.orangecyberdefense.com oder
christopher.johannes@orangecyberdense.com

Web: https://www.orangecyberdefense.com/de/

orange™ Cyberdefense

SOC as a Service in Aktion!

Ein Blick durch das Schlüsselloch.

Philipp Rieblinger, Security Consultant

orange™ Cyberdefense

Wie betreibt man SOC als Service?

Was unser Soc as a Service ausmacht

Detect and Respond: Bausteine

Leute

Prozesse

Technologie

Informationen

Was unser Soc as a Service ausmacht

Detect and Respond: Bausteine

Leute

Was unser Soc as a Service ausmacht

Detect and Respond: Bausteine

Technologie

Was unser Soc as a Service ausmacht

Detect and Respond: Bausteine

Prozesse

Was unser Soc as a Service ausmacht

Detect and Respond: Bausteine

Informationen

Core Fusion: taking operational synergies further

Teams

CERT

SOC

CyberSOC

Core Fusion Platform

Alert Flow Normalization

Data Enrichment

Case Proximity Routing

Security Orchestration

Guided Response Actions

Analysis & Reporting

Threat Intelligence Platform

SOAR Platform

Case Management

Proprietary Malware Analysis Tools

Proprietary Cybercrime Analysis Tools

Portal

Customers

Services

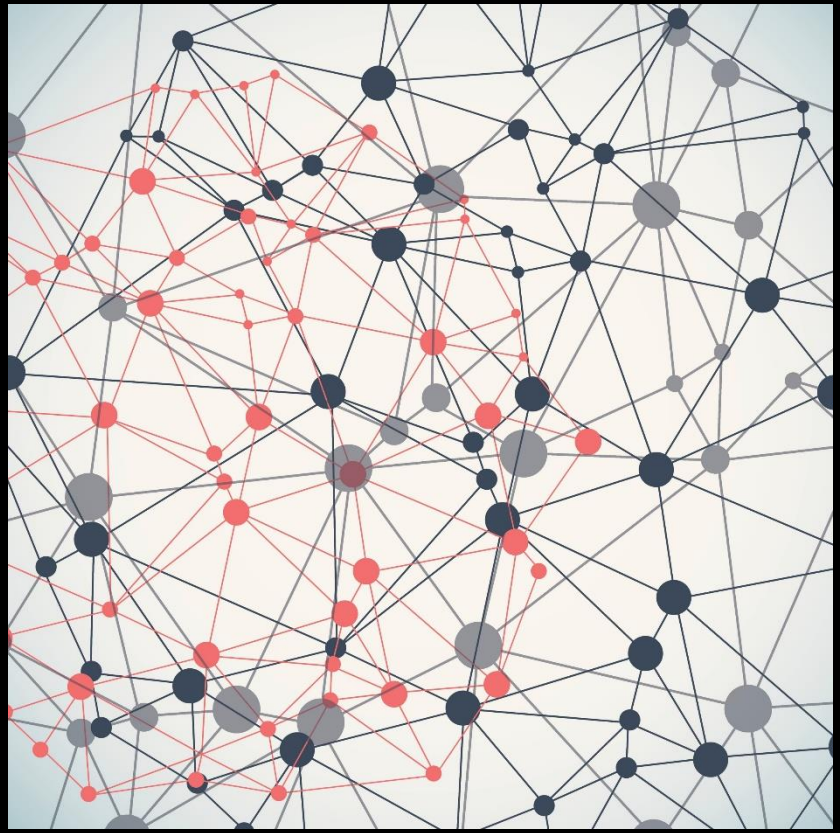
Public Cloud Services

Private Cloud Services

OnPrem / Endpoint Services

OT / ICS Services

Trends in Managed Security Services



- Mehr Nachfrage nach SOC-as-a-Service
- SaaS aus der Cloud
- Aufschwung von XDR
- Integration von Threat Intelligence

Vielen Dank!

Cyberdefense

WithSecure™ Elements Detection & Response der Cybercop

Stefan Linnig

Sales Engineer

WithSecure™ früher F-Secure

Instinctive technologies + Proven expertise

35 Year history

1,300 Employees

7,000+ Partners

135m Revenue ’22

The largest European cyber security vendor

> 2.5 M Endpoints secured

> 7.5 M Monthly ransomware detections

Continuously high partner satisfaction: Net promoter score of **72**

Listed on the NASDAQ OMX Helsinki Ltd

We are here to build and sustain trust in a digital society.

WITH secure

WithSecure product and service offering

Predict	Prevent	Detect	Respond
Insights consulting – Establishing strategic priorities, building governance models, resilience and detection capability development			
Security Assurance - Assess the security posture of assets, applications, embedded systems, OT and networks		**Incident Response –** Live attack response, and readiness preparation and testing	
CSPM and ASM - Continuous monitoring to enable proactive response to vulnerabilities and emerging threats		**Countercept MDR** – 24/7 Managed Detection and Response services for legacy and cloud	
Elements vulnerability management – Harden your attack surface		**Elevate** – Hybrid services, expert support for tough cases	
Elements endpoint protection – for Windows, Mac, Linux, iOS, and Android		**Co-monitoring –** 24/7 or out-of-office hours version	
Elements collaboration protection – for MS365		**Elements endpoint detection & response** – Critical external threat protection	
Elements cloud security posture management – for AWS and Azure cloud environments			
Cloud protection for Salesforce (CPSF)			
Partner services – Competence development, service design, integration support, co-marketing, sales & technical support			

W/Consulting W/Managed service W/Elements and CPSF Partner services

WITH secure

Elements endpoint detection & response –
Critical external threat protection

WITH secure

Problem?

Lösung?

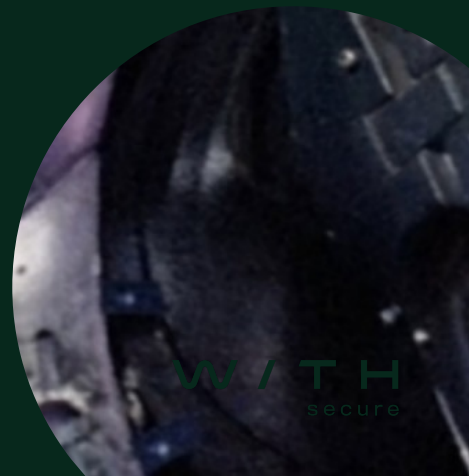
KI - schon wieder...

Worin sind Computer gut?

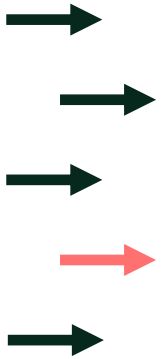
- Große Datenmengen verarbeiten – Computer skalieren

Worin sind Menschen gut?

- Entscheidungen treffen



Broad Context Detection™ in action



Events

Capturing behavioral events

500 mln data events/month

Collected by ~325 endpoint sensors deployed across the organization

Real-time behavioral analysis

225,000 suspicious events

After WithSecure's real-time behavior analysis of the raw data events

Broad context detection™

24 detections

After WithSecure's real-time behavior analysis of the raw data events

Broad context detection™

7 Real threats

Confirmed as real threats

WITH secure

Need for self-learning AI and machine learning

Supervised ML modules

- Detecting threats based on training data
- Learning from expert feedback

Unsupervised ML modules

- User/host profiling
- Anomaly detection

Data transformation

- Advanced visualization
- Intelligently clusters anomalies

Home
ENDPOINT PROTECTION
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions
Downloads
Reports
Settings
Support
Subscriptions
VULNERABILITY MANAGEMENT
CLOUD SECURITY POSTURE MANAGEMENT
COLLABORATION PROTECTION
Management - Collaboration Protection
MANAGEMENT

Dashboard

Devices at risk

Device	Company	Open Detections
DESKTOP-V0738FC	FR IT-Central	1 - 1
win2016dc.training.f-secure.local	RS GlobalCorp Inc	1 - 1
DESKTOP-TLFMF7L	FR IT-Sec	- 3 2
DEMOCBServer.DEMOCB.local	FR IT-Central	- 2 3
WithSecure-Labo.stilabs.local	FR IT-Sec	- 1 4

Recent detections (5 out of 28 devices at risk)

See all devices ›

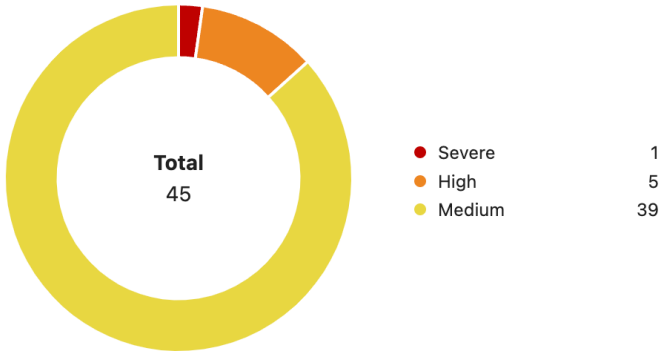
Overview

Last 30 days

50 Devices	4.1M Total Events	46 Detections
168 Software	0 Potentially unwanted software	0 Harmful software

Open detections by risk

Last 30 days



Detections by status

Last 30 days

Open Closed

Home
ENDPOINT PROTECTION
Dashboard
Devices
Software updates
Reports
Subscriptions
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions

Back to Detections list

Broad Context Detection 2 of 2

2495210-773

Go to old Broad Context Detection view

Privilege escalation

Severe risk (100), High confidence, High criticality Response Walkthrough

Created: 23.10.2023 22:36:15 UTC+02:00
Modified: 10.11.2023 09:08:17 UTC+01:00

New

Quick actions

Isolate affected device
Scan device
Collect forensics package

More response actions

Elevate to WithSecure

Elevate

Company

RS GlobalCorp Inc

Affected devices (1)

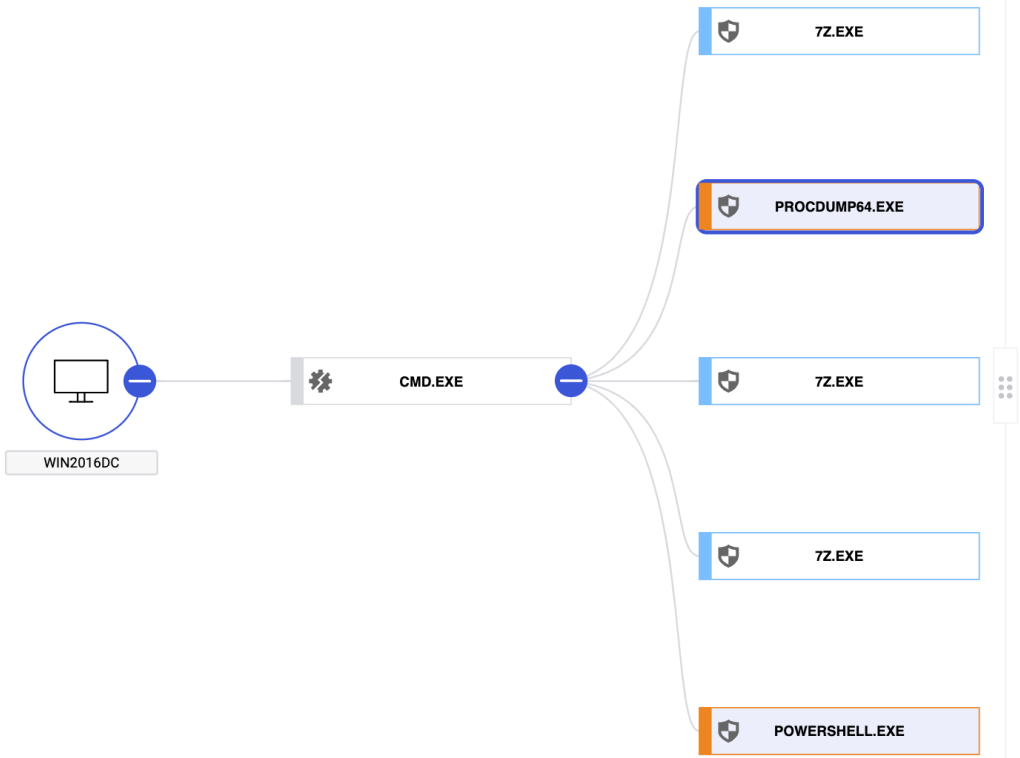
win2016dc.training.f-secure...

Identical detections (0)

Similar detections (0)

Summary Analysis Comments Log

Info and above (default)



Overview Process details

win2016dc.training.f-secure.local
2 processes added
Remove all

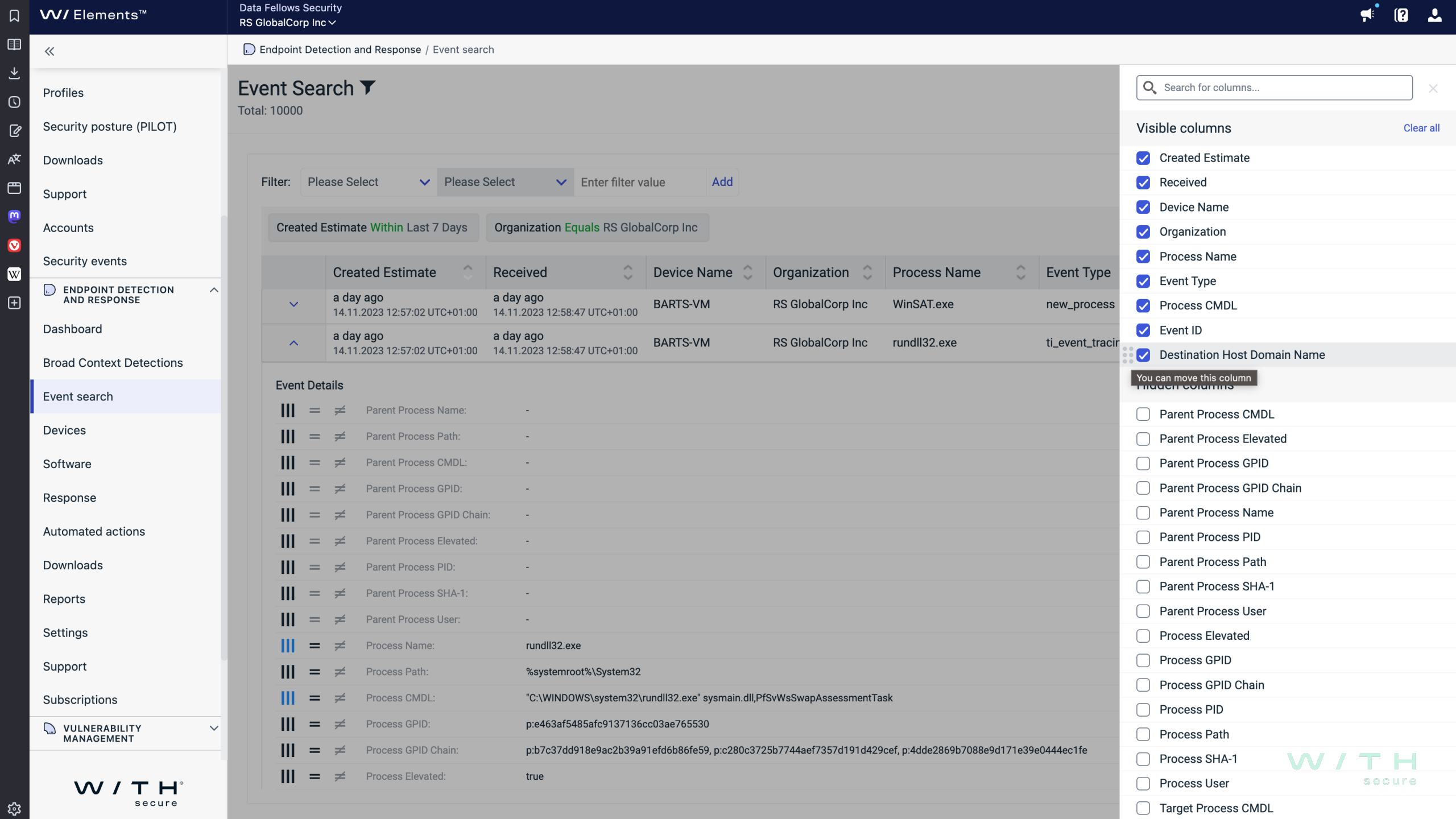
procdump64.exe Remove

Username	TRAINING\admin
Command line	"C:\Users\Public\procdump64.exe" -accepteula -ma lsass.exe "C:\TMP\somethingwindows.dmp"
Path	%profiles%\public
PID	5260
SHA1	4bed038c66e7fdbbfb0365669923a73fbc9bb8f4
Execution start	23.10.2023 22:34:40 UTC+02:00
Execution end	23.10.2023 22:34:40 UTC+02:00

Detections: Expand all Collapse all

Detection 1/2 : Lsass process dumped High
23.10.2023 22:34:40 UTC+02:00

Description: Dumped the lsass.exe memory. This may be an attempt to access passwords or hashes.


Elements™
Data Fellows Security
RS GlobalCorp Inc
Endpoint Detection and Response / Event search
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions
Downloads
Reports
Settings
Support
Subscriptions
VULNERABILITY MANAGEMENT
Event Search
Total: 10000
Filter: Please Select Please Select Enter filter value Add
Created Estimate Within Last 7 Days
Organization Equals RS GlobalCorp Inc
Created Estimate
Received
Device Name
Organization
Process Name
Event Type
a day ago 14.11.2023 12:57:02 UTC+01:00
a day ago 14.11.2023 12:58:47 UTC+01:00
BARTS-VM
RS GlobalCorp Inc
WinSAT.exe
new_process
rundll32.exe
Event Details
Parent Process Name: -
Parent Process Path: -
Parent Process CMDL: -
Parent Process GPID: -
Parent Process GPID Chain: -
Parent Process Elevated: -
Parent Process PID: -
Parent Process SHA-1: -
Parent Process User: -
Process Name: rundll32.exe
Process Path: %systemroot%\System32
Process CMDL: "C:\WINDOWS\system32\rundll32.exe" sysmain.dll,PfSvWsSwapAssessmentTask
Process GPID: p:e463af5485afc9137136cc03ae765530
Process GPID Chain: p:b7c37dd918e9ac2b39a91efd6b86fe59, p:c280c3725b7744aef7357d191d429cef, p:4dde2869b7088e9d171e39e0444ec1fe
Process Elevated: true
Search for columns...
Visible columns
Clear all
Created Estimate
Received
Device Name
Organization
Process Name
Event Type
Process CMDL
Event ID
Destination Host Domain Name
You can move this column
Parent Process CMDL
Parent Process Elevated
Parent Process GPID
Parent Process GPID Chain
Parent Process Name
Parent Process PID
Parent Process Path
Parent Process SHA-1
Parent Process User
Process Elevated
Process GPID
Process GPID Chain
Process PID
Process Path
Process SHA-1
Process User
Target Process CMDL

Home
ENDPOINT PROTECTION
Dashboard
Devices
Software updates
Reports
Subscriptions
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions

Back to Detections list

Broad Context Detection 2 of 2

2495210-773

Go to old Broad Context Detection view

Privilege escalation

Severe risk (100), High confidence, High criticality Response Walkthrough

Created: 23.10.2023 22:36:15 UTC+02:00
Modified: 10.11.2023 09:08:17 UTC+01:00

New
- New
- Acknowledged
- In progress
- Monitoring
- Closed
  - Confirmed
  - Unconfirmed
  - False positive

More response actions

Elevate to WithSecure

Elevate

Company

RS GlobalCorp Inc

Affected devices (1)

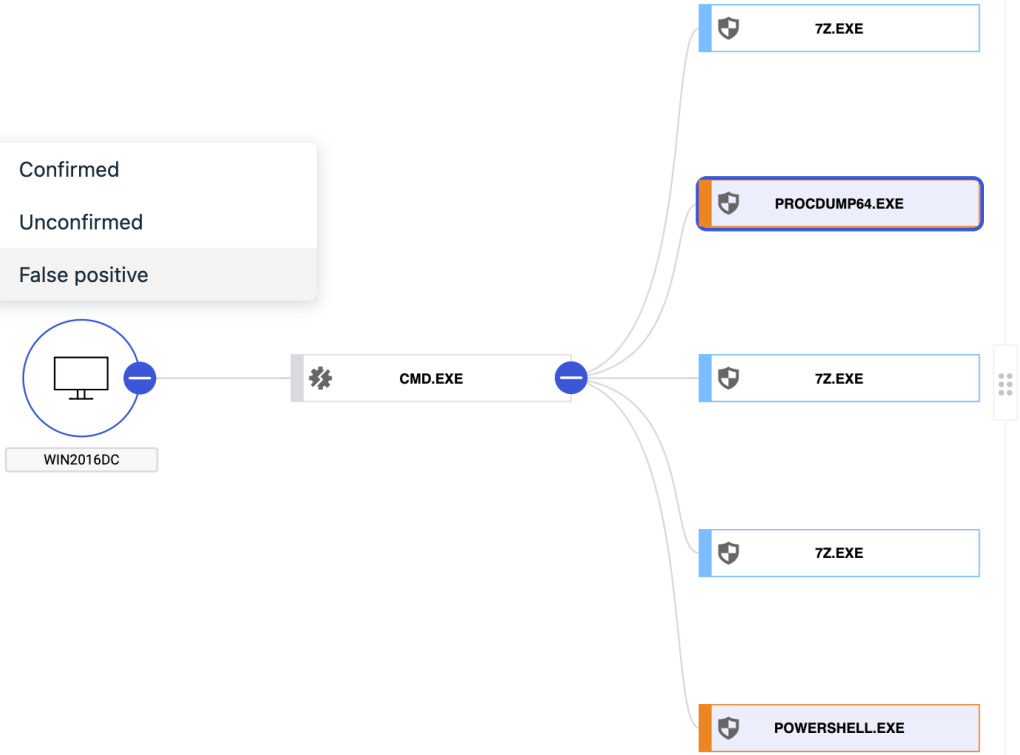
win2016dc.training.f-secure...

Identical detections (0)

Similar detections (0)

Summary Analysis Comments Log

Info and above (default)



Overview Process details

win2016dc.training.f-secure.local
2 processes added
Remove all

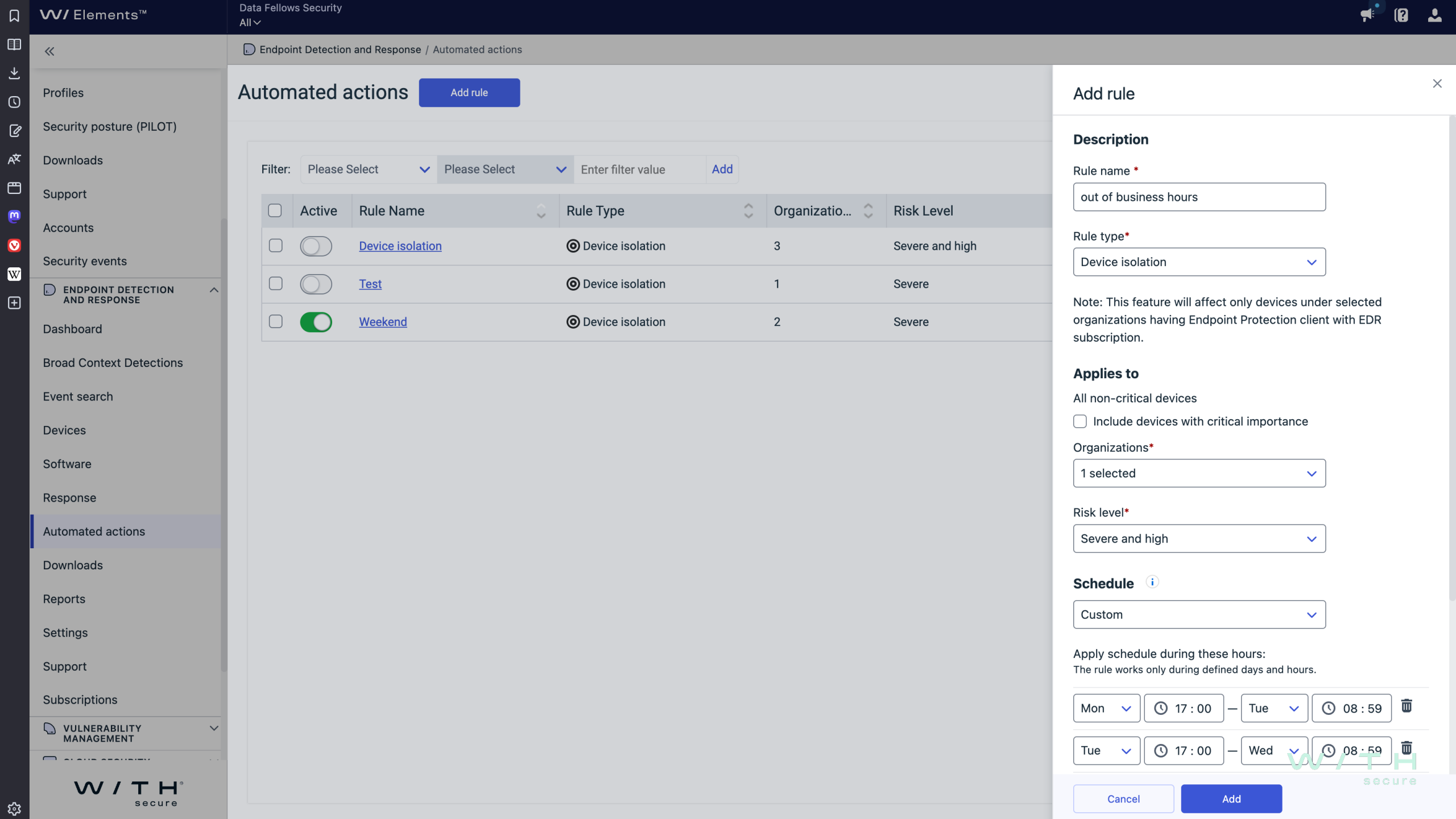
procdump64.exe Remove

Username	TRAINING\admin
Command line	"C:\Users\Public\procdump64.exe" -accepteula -ma lsass.exe "C:\TMP\somethingwindows.dmp"
Path	%profiles%\public
PID	5260
SHA1	4bed038c66e7fdbbfb0365669923a73fbc9bb8f4
Execution start	23.10.2023 22:34:40 UTC+02:00
Execution end	23.10.2023 22:34:40 UTC+02:00

Detections: Expand all Collapse all

Detection 1/2 : Lsass process dumped High
23.10.2023 22:34:40 UTC+02:00

Description: Dumped the lsass.exe memory. This may be an attempt to access passwords or hashes.


Elements™
Data Fellows Security
All
Endpoint Detection and Response / Automated actions
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions
Downloads
Reports
Settings
Support
Subscriptions
VULNERABILITY MANAGEMENT
Automated actions
Add rule
Filter:
Please Select
Please Select
Enter filter value
Add
Active
Rule Name
Rule Type
Organizatio...
Risk Level
Device isolation
Device isolation
3
Severe and high
Test
Device isolation
1
Severe
Weekend
Device isolation
2
Severe
Add rule
Description
Rule name *
out of business hours
Rule type*
Device isolation
Note: This feature will affect only devices under selected organizations having Endpoint Protection client with EDR subscription.
Applies to
All non-critical devices
Include devices with critical importance
Organizations*
1 selected
Risk level*
Severe and high
Schedule
Custom
Apply schedule during these hours:
The rule works only during defined days and hours.
Mon
17 : 00
Tue
08 : 59
Tue
17 : 00
Wed
08 : 59
Cancel
Add

Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions
Downloads
Reports
Settings
Support
Subscriptions
VULNERABILITY MANAGEMENT

Advanced responses support English language only. View details

New response action

1 Devices — 2 Actions — 3 Parameters — 4 Summary

Actions

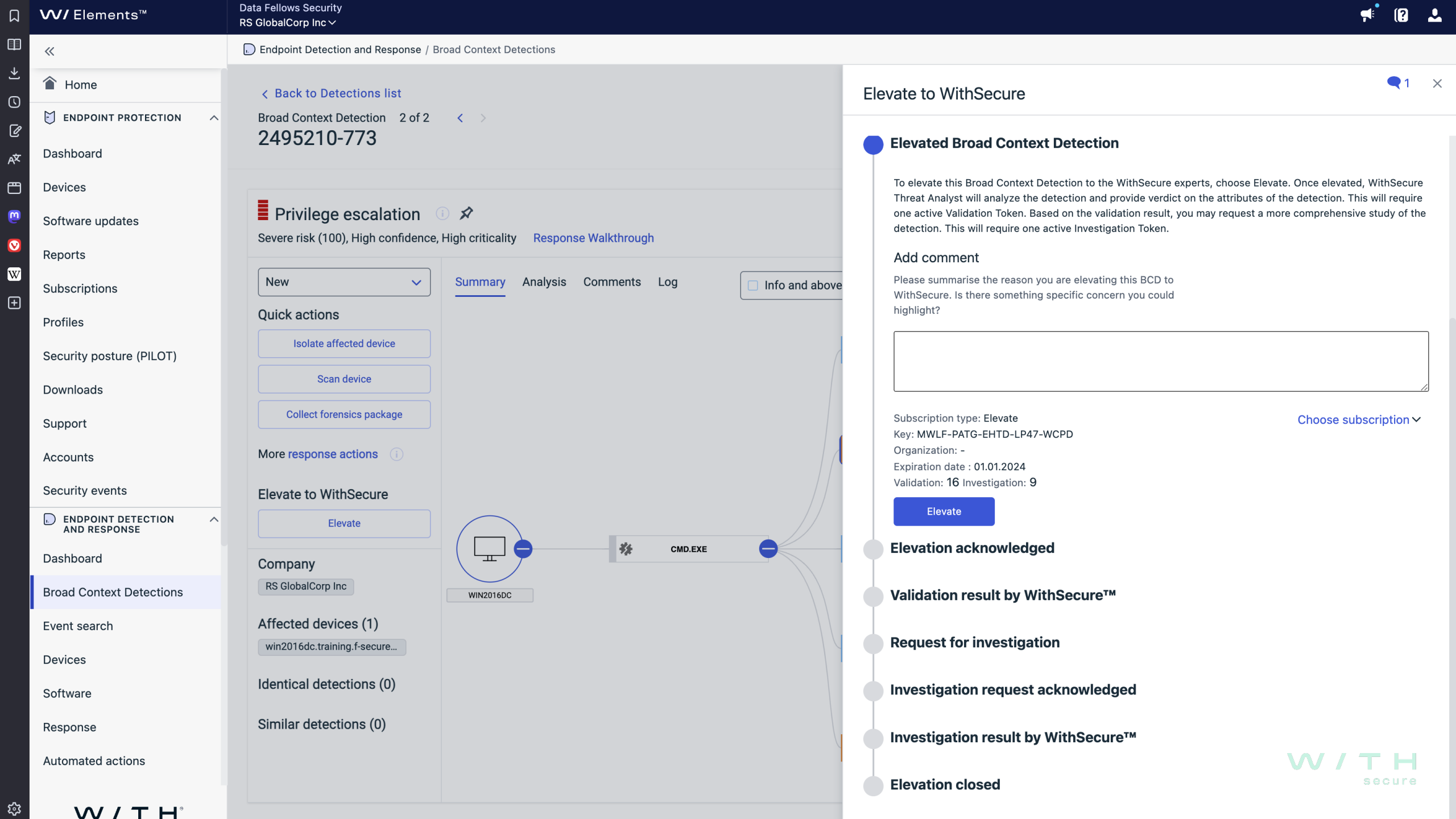
Search

Retrieve rdp cache files from (USERHOME)\(AppData\Local|Local Settings\Application Data)\Microsoft\Terminal Server Client\Cache\.*

- [ ] **Retrieve prefetch**
  Retrieve all prefetch (*.pf) files from %SYSTEMROOT%\Prefetch
- [ ] **Map registry ***
  Retrieves a listing of all registry keys under the given path.
- [ ] **Retrieve anti-virus logs**
  Retrieves anti-virus log files (.log/.txt/.html/.evtx format).
- [ ] **Retrieve event log entries ***
  Retrieves Windows event log entries in a format viewable from within the frontend.
- [ ] **Retrieve files**
  Retrieves files.
- [x] **Full memory dump (Windows)**
  Uploads a full memory dump. Warning: this job uploads large files and will thus block subsequent jobs, consider running this job last.
- [ ] **Netstat ***
  Retrieves network connections, routing tables, interface statistics, masquerade connections, multicast memberships and associated process information for each entry from the selected endpoints.
- [ ] **Delete WMI persistence**
  Removes persistence achieved through WMI Event subscription by deleting the matching instances of EventConsumer, EventFilter and FilterToConsumerBinding. If a single search term is provided then all the related instances will be removed. For example, if the EventConsumer name is only entered, then the matching EventConsumer, all the FilterToConsumerBindings that reference it, and the EventFilters referenced by the binding instances, are removed. Providing additional search terms help narrow down the results to delete only matching instances. An error is raised if any deleted instance is found again after the specified time delay.

* The output for these actions is in jsonl. Find out more.

Back | Next | Please enter correct parameters to create response action.


Elements™
Data Fellows Security
RS GlobalCorp Inc
Endpoint Detection and Response / Broad Context Detections
Home
ENDPOINT PROTECTION
Dashboard
Devices
Software updates
Reports
Subscriptions
Profiles
Security posture (PILOT)
Downloads
Support
Accounts
Security events
ENDPOINT DETECTION AND RESPONSE
Dashboard
Broad Context Detections
Event search
Devices
Software
Response
Automated actions
Back to Detections list
Broad Context Detection 2 of 2
2495210-773
Privilege escalation
Severe risk (100), High confidence, High criticality
Response Walkthrough
New
Summary
Analysis
Comments
Log
Info and above
Quick actions
Isolate affected device
Scan device
Collect forensics package
More response actions
Elevate to WithSecure
Elevate
Company
RS GlobalCorp Inc
Affected devices (1)
win2016dc.training.f-secure...
Identical detections (0)
Similar detections (0)
WIN2016DC
CMD.EXE
Elevate to WithSecure
1
Elevated Broad Context Detection
To elevate this Broad Context Detection to the WithSecure experts, choose Elevate. Once elevated, WithSecure Threat Analyst will analyze the detection and provide verdict on the attributes of the detection. This will require one active Validation Token. Based on the validation result, you may request a more comprehensive study of the detection. This will require one active Investigation Token.
Add comment
Please summarise the reason you are elevating this BCD to WithSecure. Is there something specific concern you could highlight?
Subscription type: Elevate
Key: MWLF-PATG-EHTD-LP47-WCPD
Organization: -
Expiration date : 01.01.2024
Validation: 16 Investigation: 9
Choose subscription
Elevate
Elevation acknowledged
Validation result by WithSecure™
Request for investigation
Investigation request acknowledged
Investigation result by WithSecure™
Elevation closed

WithSecure Co-Monitoring service

- Monitoring (24/7 or out-of-hours) of severe-risk detections by WithSecure
- Validation and investigation of severe-risk detections by a human threat analyst
- Confirmed attacks are escalated directly to partners or customers on-call
- Threat Analyst provides containment advice for fast and effective remediation
- Possible to escalate to Incident Response services with or without IR Retainer

Outcome

- Improved resilience
- Minimized disruption and unplanned expense
- Customer trust

WITH secure

WITH secure

Stefan Linnig
Sales Engineer
stefan.linnig@withsecure.com

Zukunftssichere IT-Sicherheit
– welche Rolle spielen Mensch und KI?

Michael Veit
Technology Evangelist, SOPHOS

November 2023

SOPHOS

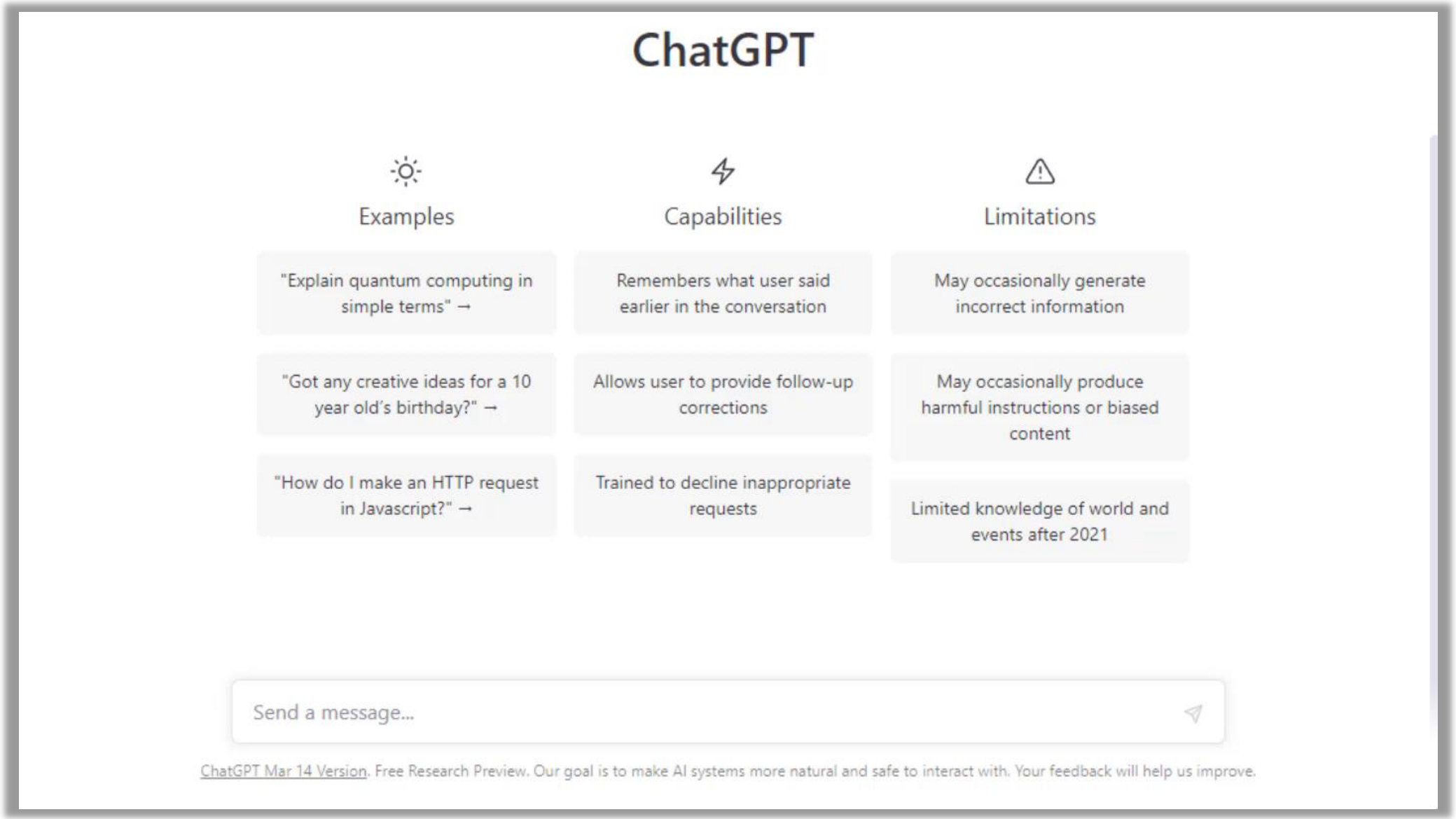
Delivering Optimal Cyber Security Outcomes

SOPHOS

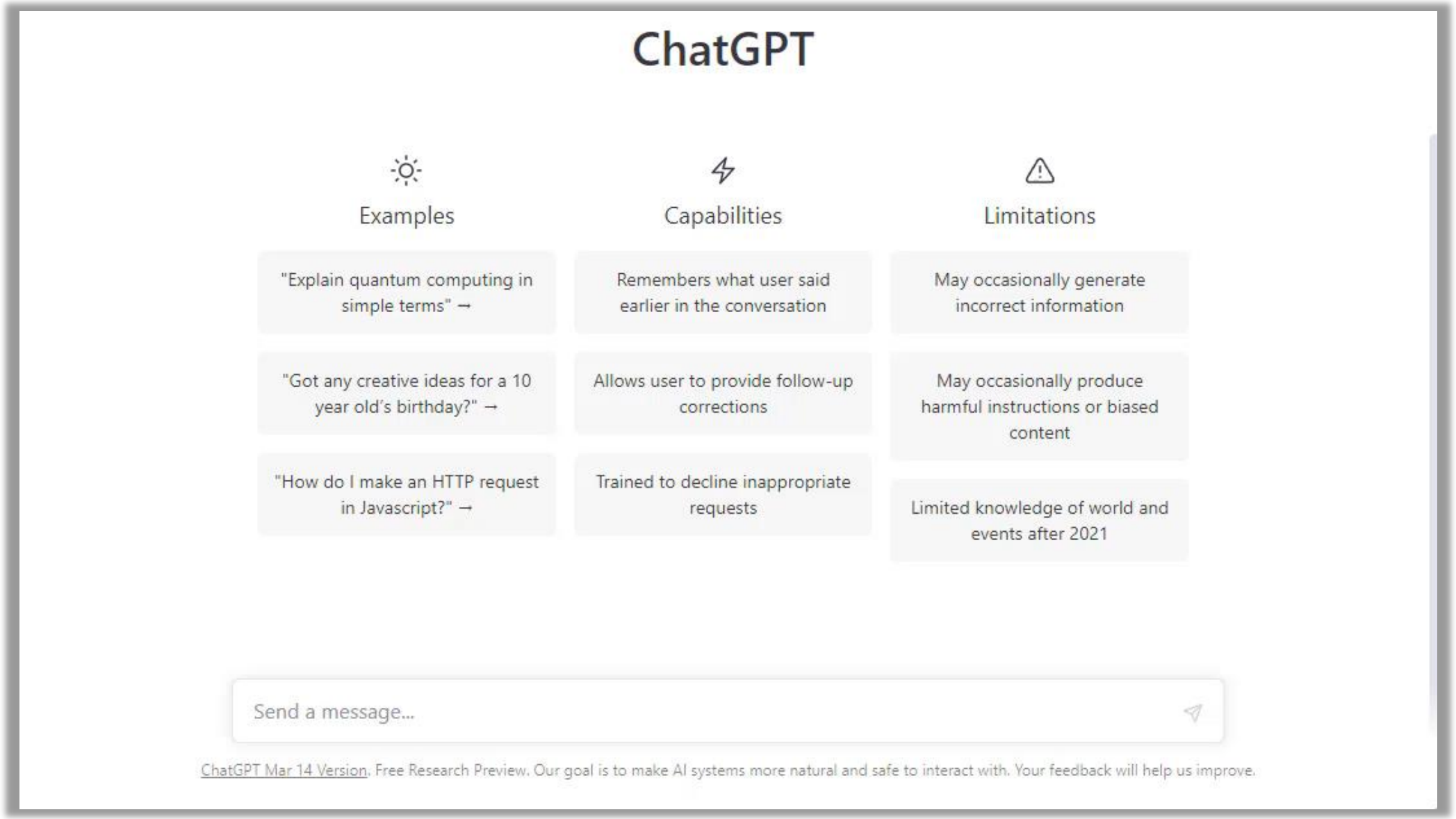
KI verändert die IT-Sicherheit

SOPHOS

Phishing-Email



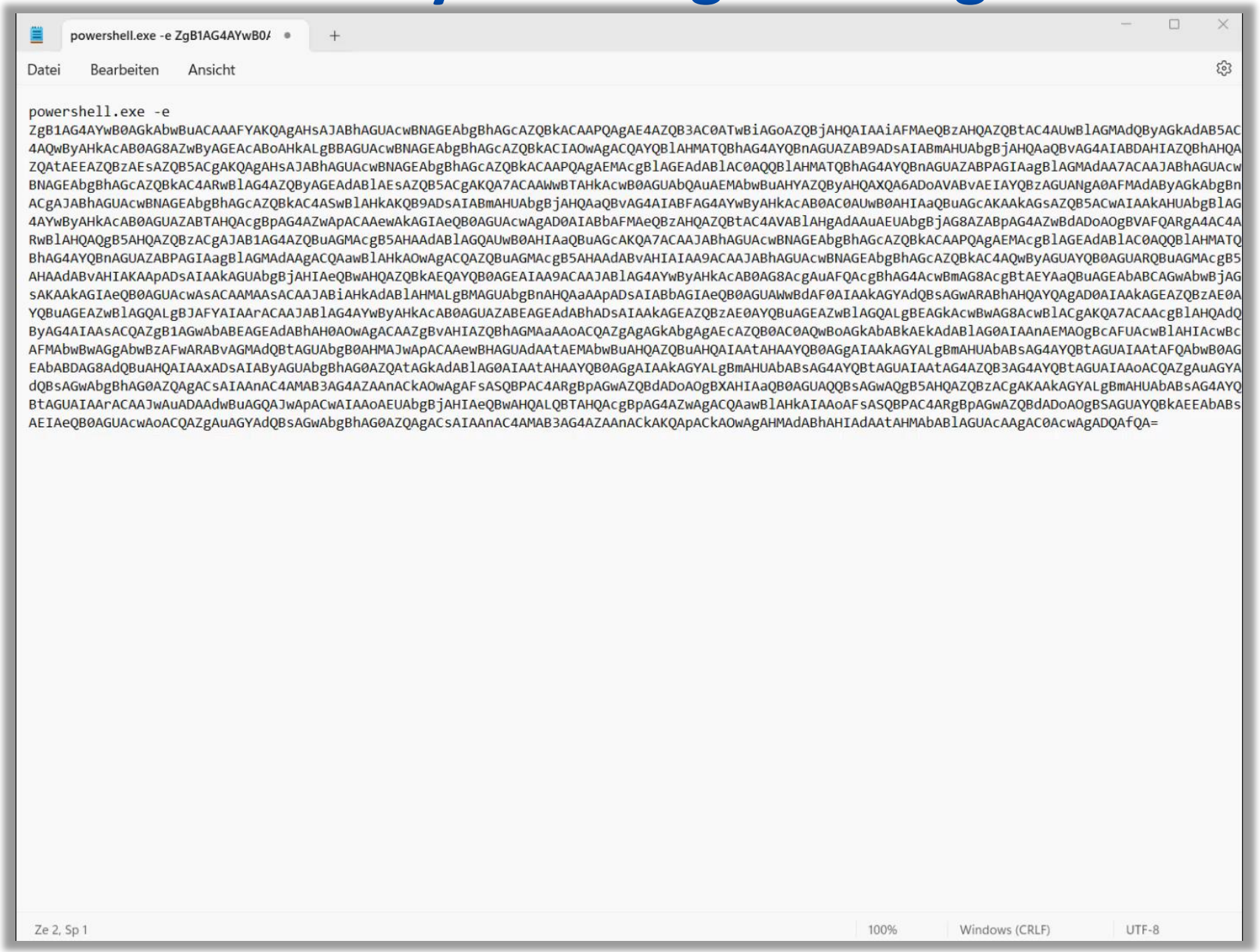
Ransomware


ChatGPT
Examples
"Explain quantum computing in simple terms" →
"Got any creative ideas for a 10 year old's birthday?" →
"How do I make an HTTP request in Javascript?" →
Capabilities
Remembers what user said earlier in the conversation
Allows user to provide follow-up corrections
Trained to decline inappropriate requests
Limitations
May occasionally generate incorrect information
May occasionally produce harmful instructions or biased content
Limited knowledge of world and events after 2021
Send a message...
ChatGPT Mar 14 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

Wo kann KI + ChatGPT eine Bedrohung sein?

- Phishing Emails Reloaded
- Skript-Malware schreiben
- Code Debugging -> Exploits finden
- Für Profis ändert sich wenig
- Amateure bekommen mächtige neue Werkzeuge

ChatGPT übersetzt Analysten mögliche Angriffsaktivität

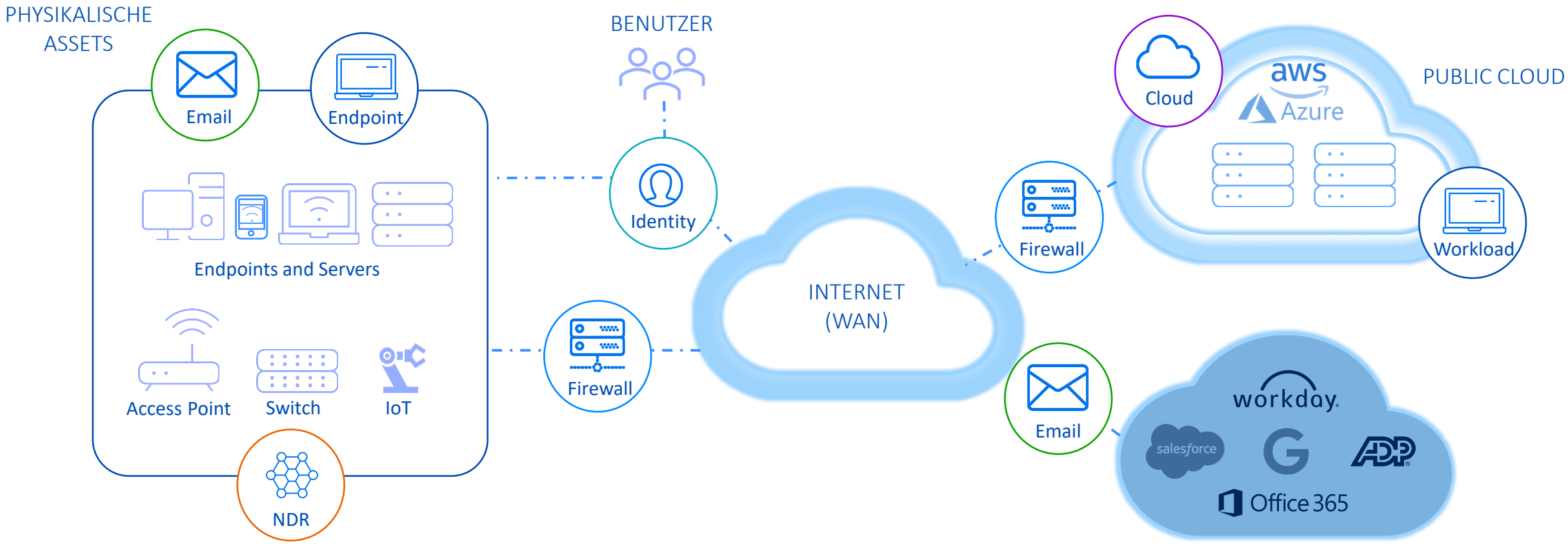


SOPHOS

Telemetrie + KI zur Verteidigung

SOPHOS

Sicherheitslösungen verteilt in der gesamten Umgebung



NDR

Ungeschützte und fremde Geräte

- Privatgeräte
- Altes OS / Telefonanlage
- Fremdgeräte

IoT / OT Geräte

- Medizinische Geräte
- Produktionsstraßen
- Drucker

Insider-Bedrohungen

- Datenabfluss

Umfassendere Sichtbarkeit

- Verschlüsselte C2-Kommunikation

Synergie mit MDR + XDR

- Technologieübergreifende Analysen + Korrelation

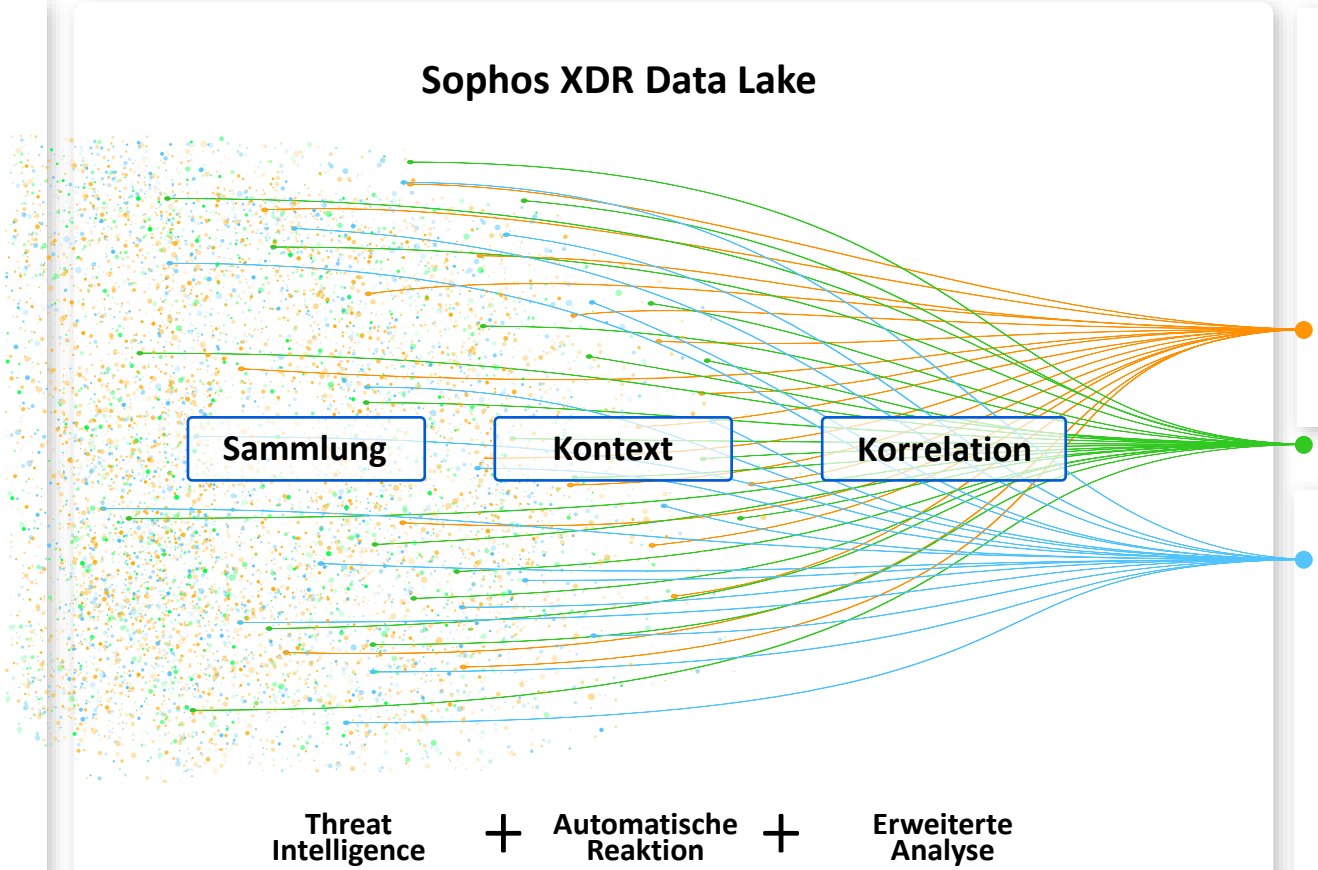
SOPHOS

Analyse und Reaktion – eigenes SOC oder Sophos MDR

Telemetriequellen

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identität
- Microsoft

Bedrohungsanalyse und Korrelation



Untersuchung und Reaktion

24/7 Managed Detection and Response Services

Sophos MDR Experten für Bedrohungssuche, Analyse und Reaktion

38 Min Ø Zeit bis zur Behebung

Investigation and Response Platform für das eigene SOC

Sophos Central als zentrale Plattform für Untersuchung, Reporting und Management

Selbst verwaltet oder zusammen mit dem Sophos MDR Team

SOPHOS

Sophos MDR – mit Telemetrie von Drittanbietern

Telemetriequellen

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identität
- Microsoft

Endpoint

Sophos Endpoint

SentinelOne · TREND MICRO · Microsoft · BlackBerry CYLANCE · CROWDSTRIKE

Firewall

Sophos Firewall

paloalto NETWORKS · FORTINET · CHECK POINT · CISCO · WatchGuard · SONICWALL

Email

Sophos Email

Microsoft 365 · mimecast · proofpoint.

NDR

Sophos NDR

DARKTRACE · Forcepoint · CANARY · Skyhigh Security

Cloud

Sophos Cloud

aws · Azure · orca security

Identität

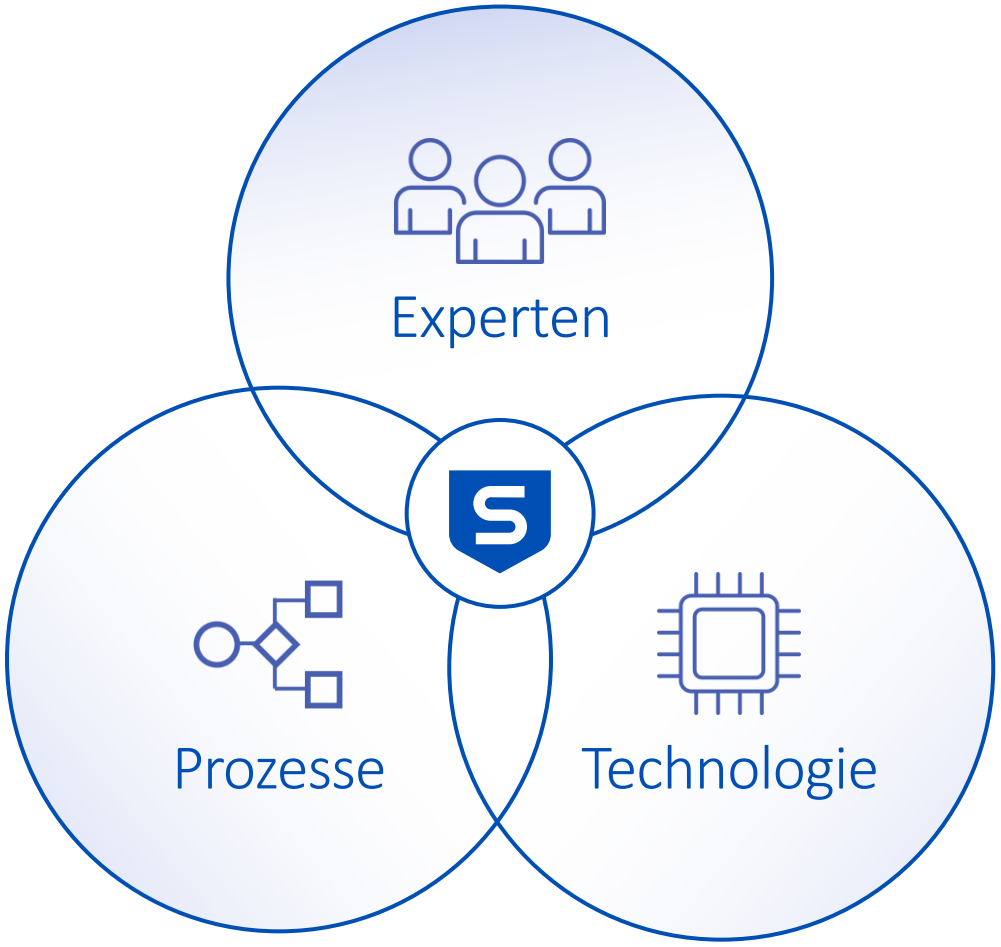
okta · DUO · Auth0 · Microsoft

Microsoft

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- O365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

SOPHOS

SOPHOS MDR - Cybersecurity as a Service



- Proaktive Bedrohungssuche
- 24/7 Erkennung und Reaktion durch Analysten
- Vollständige Ursachenanalyse + Incident Response
- Mehr als 18.000 MDR Kunden
- Telemetrie von mehr als 580.000 Unternehmenskunden
- All-inclusive Service – keine versteckten Kosten
- Bestmögliches Ergebnis für Ihre IT-Sicherheit

14.3.2023
MS Outlook

[Security Advisory] CVE-2023-23397 - Outlook Elevation of Privilege

// Overview

On Tuesday, March 14, Microsoft disclosed a vulnerability in Microsoft Outlook for Windows that enables NTLM credential theft. CVE-2023-23397 is triggered when an attacker sends a message with an MAPI property that includes a UNC path to a threat actor controlled SMB share (TCP port 445). No user interaction is required to exploit this vulnerability.

Note: Online services, such as Microsoft 365, do not support NTLM authentication and are not vulnerable to being attacked by these specifically crafted messages.

Microsoft is aware of targeted attacks against a limited number of organizations in government, transportation, energy, and military sectors in Europe. This vulnerability was disclosed in coordination with the Computer Emergency Response Team of Ukraine (CERT-UA).

At this time, the Sophos MDR team have not identified exploitation in our customers' environments. However, we highly recommend applying patches if you are on an affected version.

// What Sophos MDR (Managed Detection and Response) is doing

SophosLabs is actively investigating detection opportunities for exploitation of this vulnerability. In addition, the Sophos MDR team has detections that cover a variety of actions that an attacker would use these stolen credentials for.

If you find any indication of emails crafted to exploit your users and gain their credentials, please submit them to SophosLabs for analysis. You can follow the instructions found here:

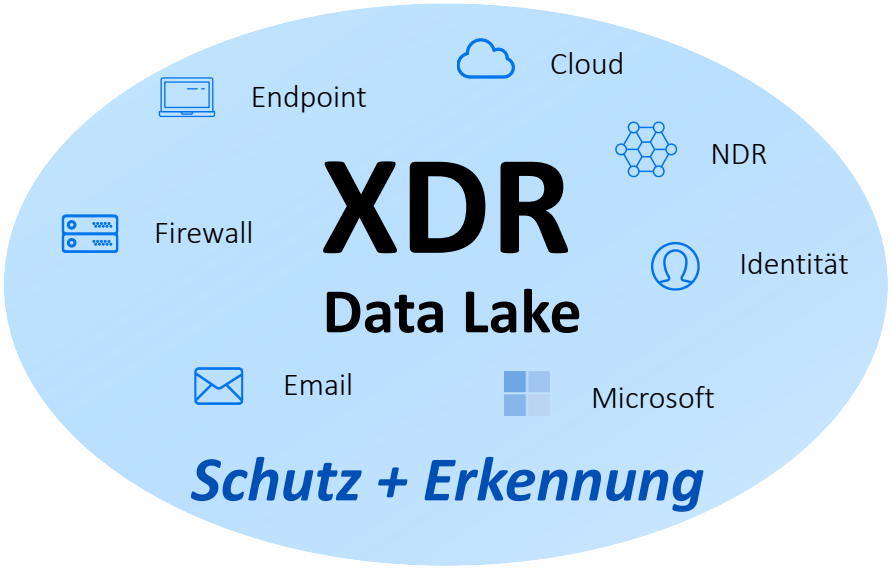
- https://support.sophos.com/support/s/article/KB-000033422?language=en_US

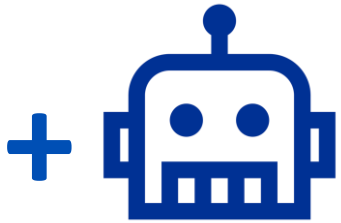
We are continuing to perform threat hunts to identify potential indicators of related suspicious activity and for signs of post-exploitation tactics. We will notify you should any suspicious or malicious behaviour is observed in your estates. The Sophos MDR Threat Intelligence team will continue to monitor private and public threat intelligence.

SOPHOS

Ist KI jetzt Gefahr oder Chance?

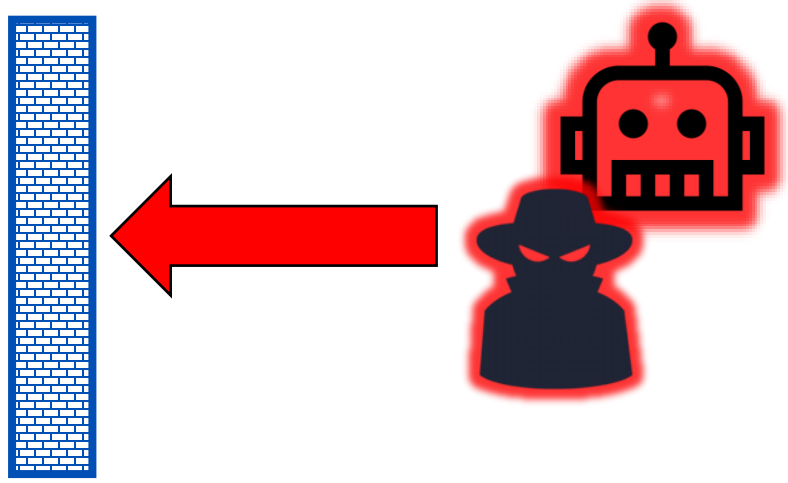
Ist KI also eher Gefahr oder Chance?

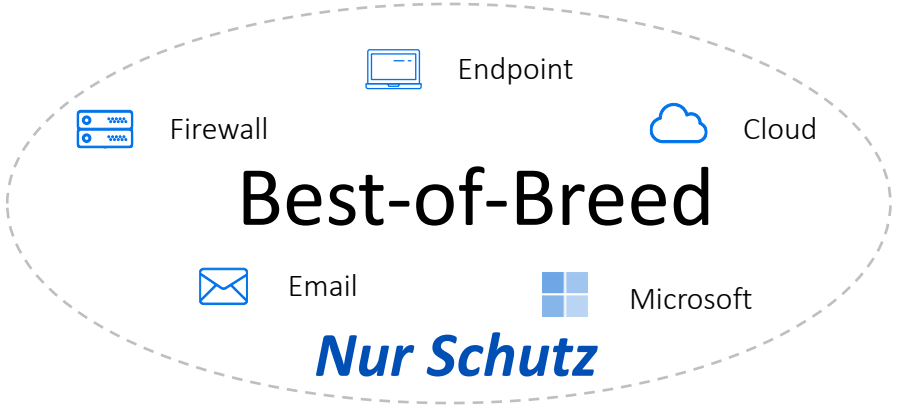




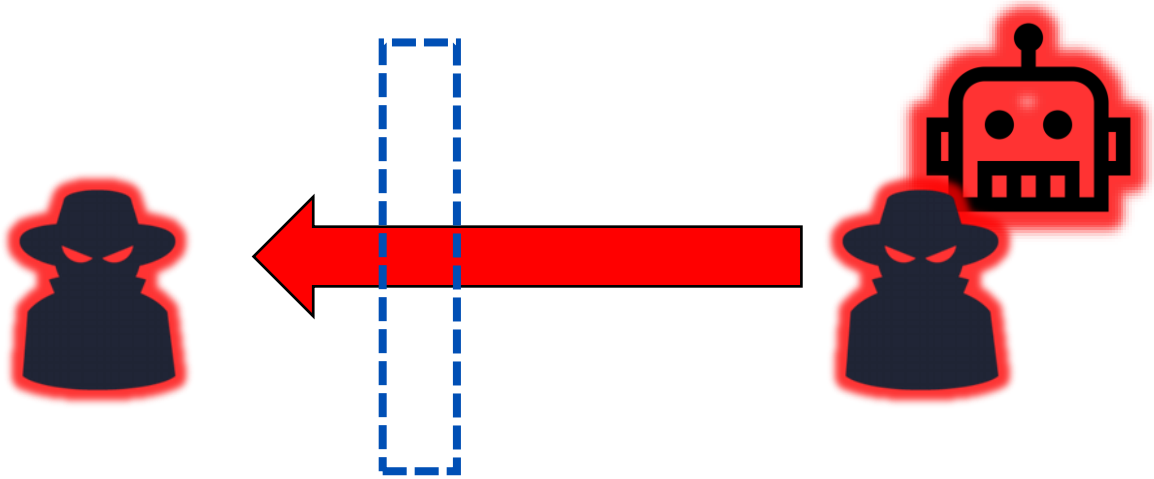
KI

Experten
24/7



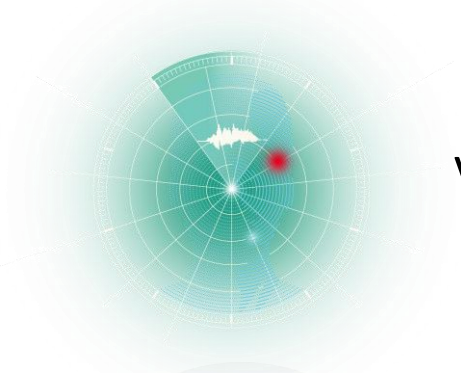


IT
8/5



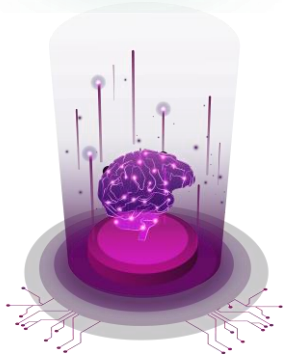
Sophos KI - ai.sophos.com/projects/

Next-Gen Web



Verhaltenserkennung

Infrastruktur



KI Forschung

Phishing Erkennung

XDR / MDR:

- Korrelation von Ereignissen
- Analyst Experience/Assistance

Die nächsten Schritte

Sophos Intercept X Advanced with XDR

Sophos Intercept X Advanced with XDR erfasst neben Endpoint- und Server-Informationen auch Netzwerk-, E-Mail-, Cloud- und mobile Datenquellen und bietet Ihnen so ein noch umfassenderes Bild Ihrer Cybersicherheit

Zum Datenblatt

Sophos AI

Sophos hat bereits seit einigen Jahren Maschine Learning in Lösungen integriert. Die weitere Entwicklung mit AI in den Bereichen Next Gen Web, Behavioral Detection, Infrastucture, Interpretable ML als auch Phishing Detection können Sie live mit verfolgen.

ai.sophos.com/projects/

Sophos MDR

24/7 Schutz vor Cyberangriffen – mit Ihrem persönlichen MDR-Service: Weitere Informationen zu unserer Lösung Sophos MDR erhalten Sie auf unserer Produktseite.

sophos.de/mdr

Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

sophos.de/kontakt

SOPHOS

Cybersecurity as a Service

paloalto NETWORKS | CORTEX

We have to look beyond the Endpoint.

The importance of the XDR

Thomas Maxeiner
Director EMEA Central | Cortex Area Sales Executive

What is the best approach?

EDR

Endpoint Detection and Response

XDR

eXtended Detection and Response

SIEM

Security Incident and Event Management

Digital Transformation is creating new Attack Surface Risks

Digital Transformation is creating new Attack Surface Risks

Workplace Transformation

Working from Anywhere

- Windows 10 / 11
- Mobile
- MAC OS / Linux
- Legacy OS

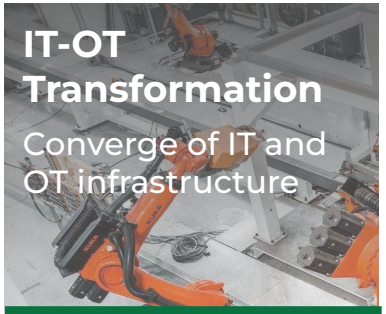
Cloud Transformation

Half of the attacks are Cloud Native

- Cloud (SaaS, IaaS)
- Shadow IT
- SDN
- Cloud Storage

R&D and Innovation

- Collaboration
- Container
- M&A Infrastructure
- Supply Chain



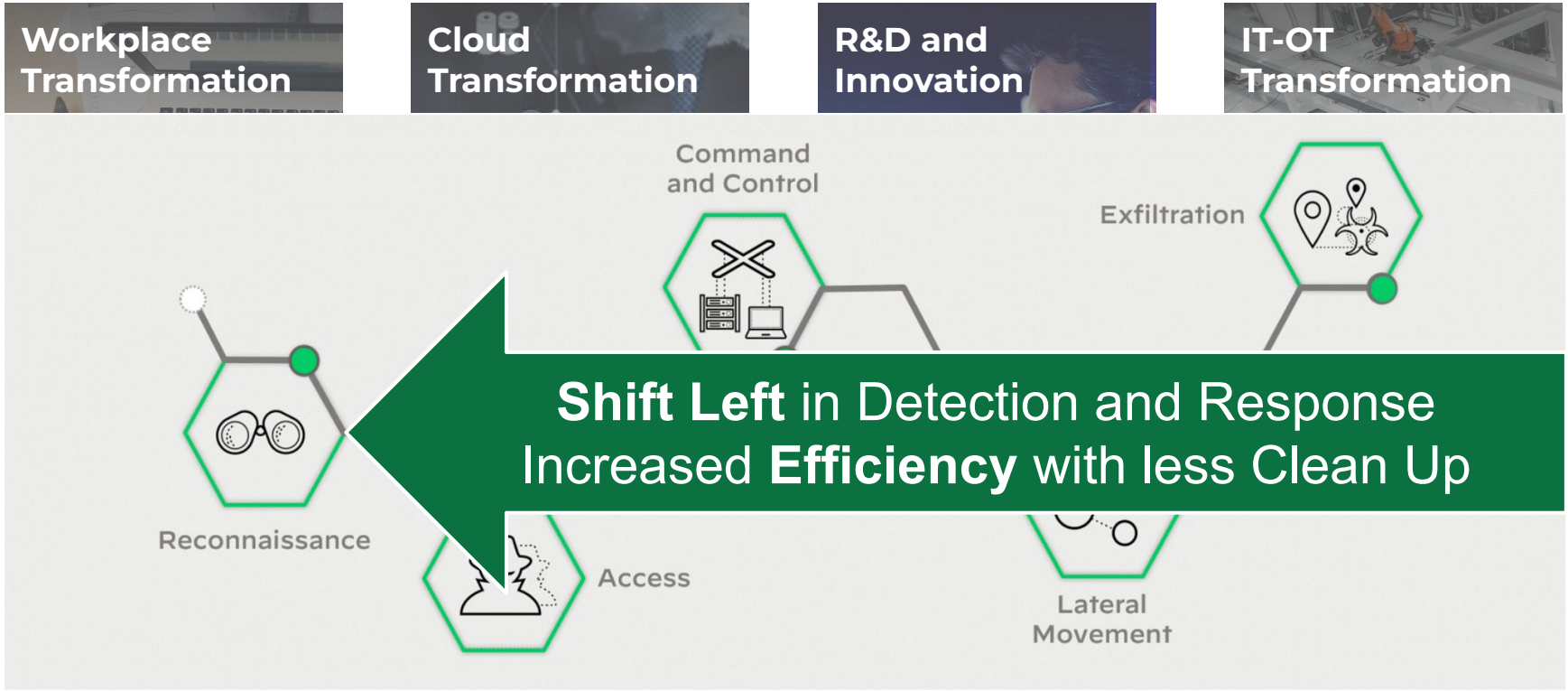
IT-OT Transformation

Converge of IT and OT infrastructure

- Critical Infrastructure
- SCADA
- Manufacturing
- Medical Devices

NGFW Network Segmentation

Digital Transformation is creating new Attack Surface Risks



Have you locked all your doors?
Ransomware Attacks do not start on the Endpoint anymore!

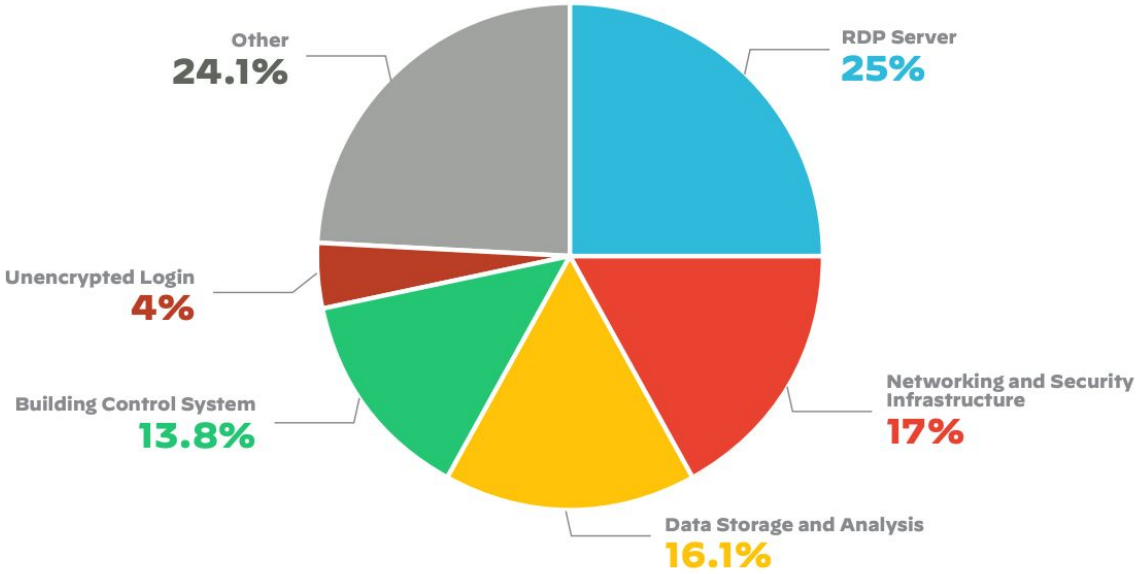


Figure 3: Distribution of risks across the global attack surface

- Nearly **1 out of 4** issues found on the attack surface was related to RDP servers
- **Networking equipment** related vulnerabilities were the second largest type of issues found on the attack surface.
- Exposed Data Storage and Analysis systems are also prevalent and could **lead to data leaks** and **exfiltration**.

R = 1

Risk equals One

Key Security Principles to reduce Risk and increase Efficiency

Analysts need the right context to stop sophisticated Attacks

EDR and SIEM Products Have Not Adequately Solved the Problem

EPP / EDR

Deep analytics and threat detection

Lacks coverage and context for entire environment

EDR

Endpoint

Lack of Analytics

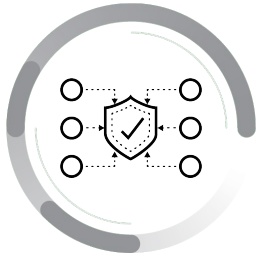
Lack of Data and Context

SIEM

No Endpoint

Lack of Analytics

SIEM



SIEM / SA

Mile-wide, inch-deep understanding of data

Deficient analytics and detection

Lack of workflows

Lack of control points to remediate

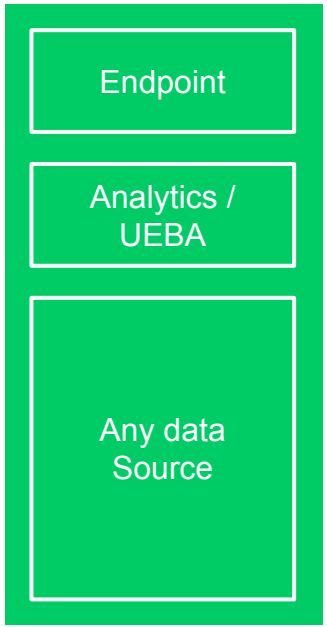
XDR is designed to increase SOC efficiency

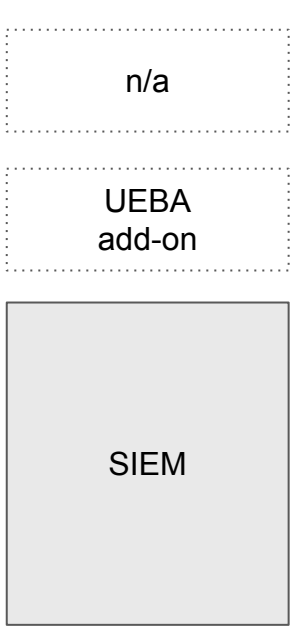
Protection
- Modern EPP Platform

Detection
- Data Stitching to tell the complete attack story “Causality Chain”

Investigations
- Complete Incident, instead of multiple Alerts
- Build-in analytics will stitch anomalies over multiple days

Response
- Native Actions (Endpoints, Firewalls, Cloud, OT)
- Live terminal and Host Restore





Protection
- Not available

Detection
- Static Correlation Rules only triggered if all criteria is met (if, then, else conditions)

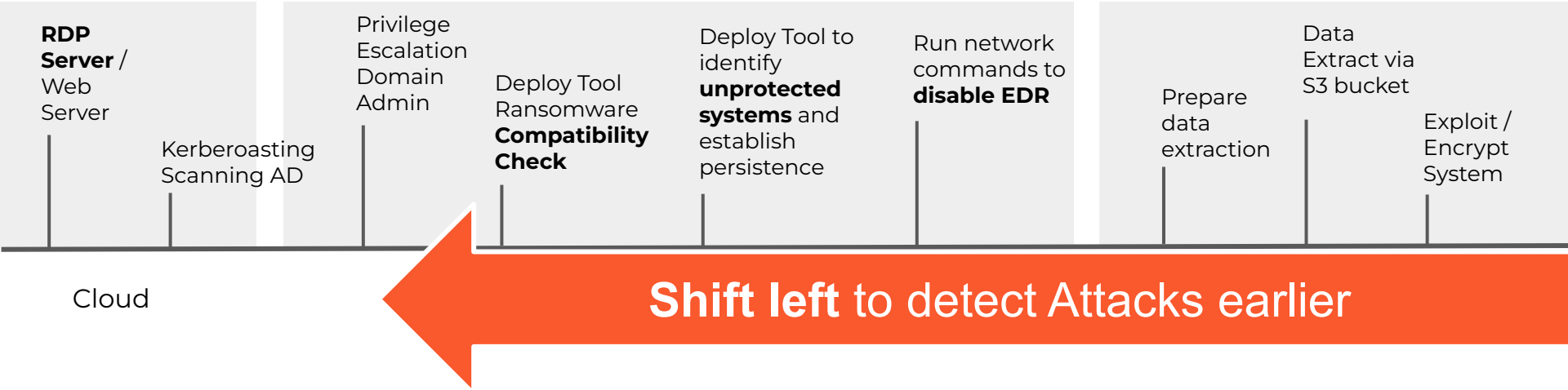
Investigations
- Lack of analytics means investigations are manual to put alerts in context

Response
- API based integrations with Endpoint vendors
- Limited actions

Lack of visibility and complexity is creating a huge Blind Spot

BUT WHAT HAPPENED BEFORE?

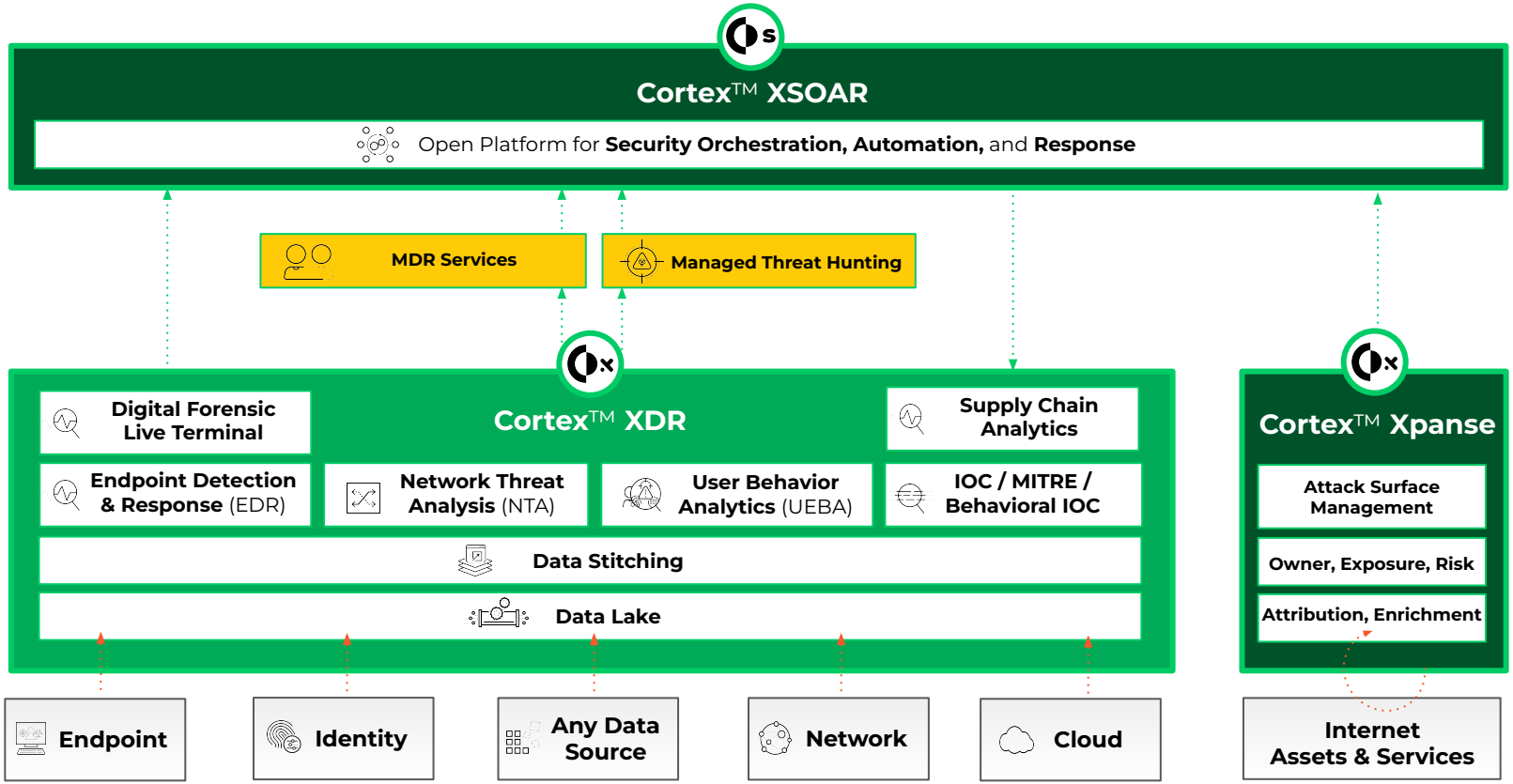
Unit42 Insights: Starting on the Endpoint is way too late



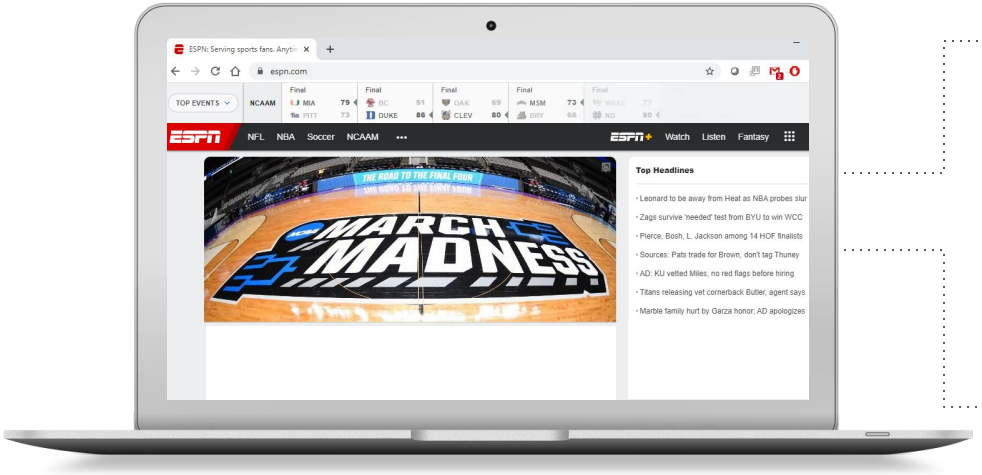
Cortex XDR Sensor Network

Endpoint | **Identity** | **Any Data Source** | **Network** | **Cloud** | **Internet Assets & Services**

Cortex Is A Holistic Platform For Delivering SOC Services



What Does it Mean to Stitch Data Together?



A user did **one** thing: accessed a website.

Network data

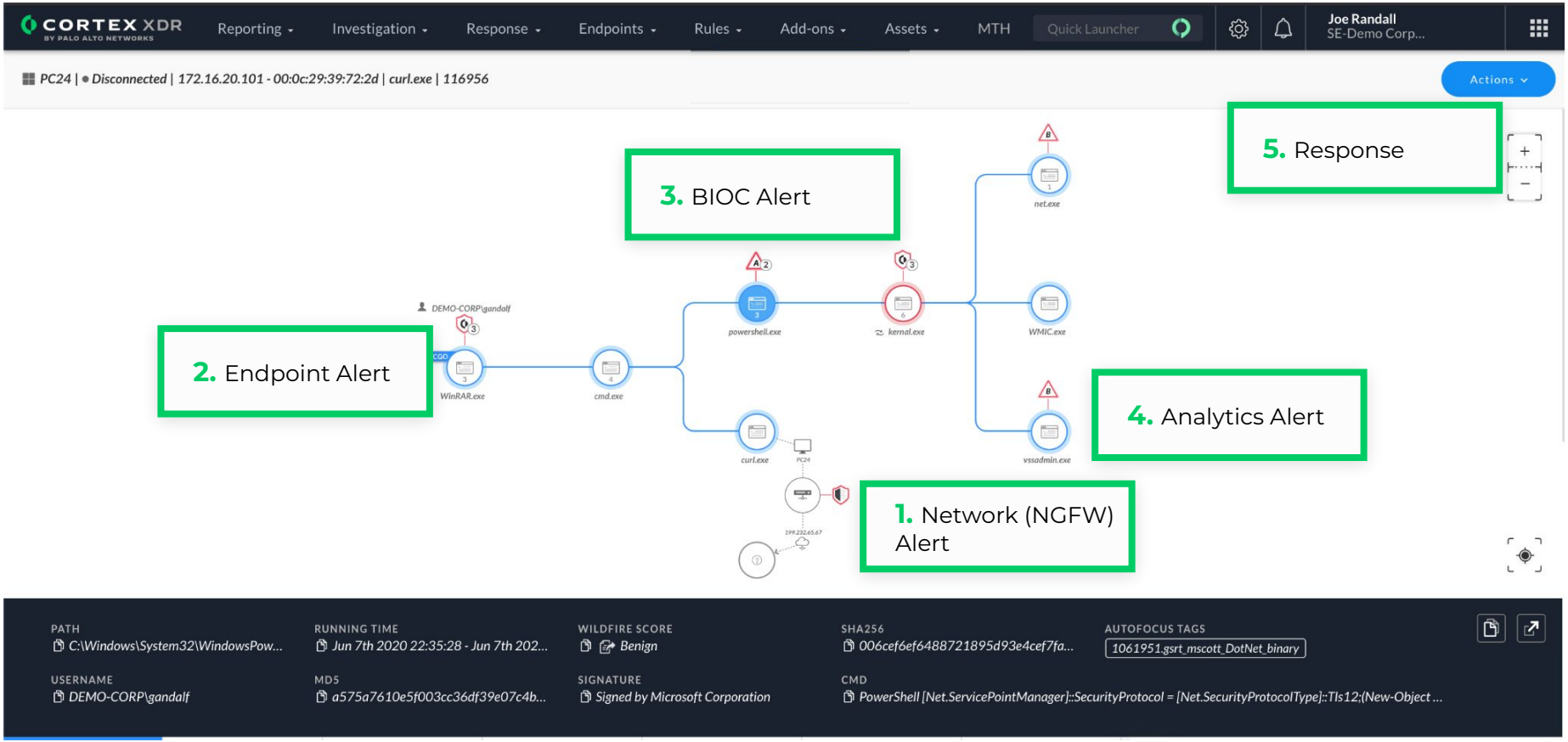
Two (or more) logs were generated from three different points of view.

Endpoint data

Cloud data

One unified and clear “story” in XDR

Cortex XDR Stitching for Faster Context & Faster Response



The Value of an integrated platform approach providing better security outcomes

paloalto NETWORKS | CORTEX

The Value of an integrated platform approach providing better security outcomes (EDR vs XDR)

Endpoint Detection & Response (EDR)

- Attacks will most likely **hit the endpoint**
- Endpoint Data only which **limits the context** of an attacks
- **Lack of visibility** into all the touchpoints the adversary had; add to investigation time
- **High risk** hackers are still **persistent** somewhere on the network

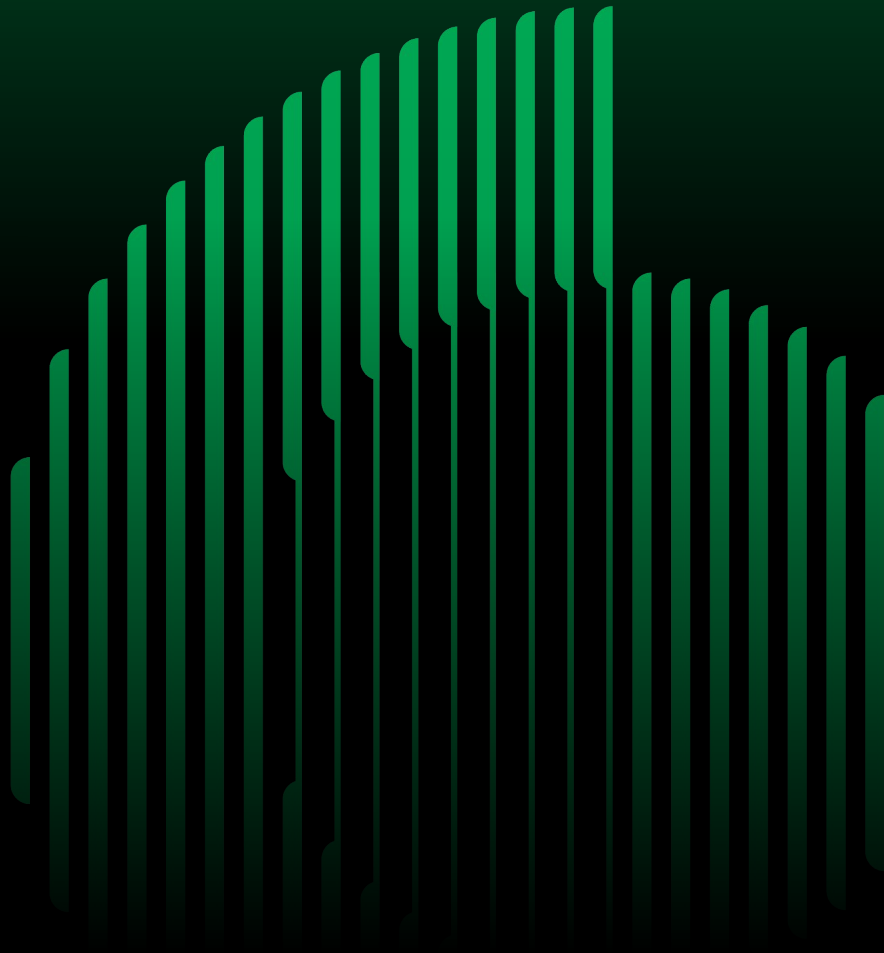
eXtended Detection & Response (XDR)

- Attackers do **NOT think in Silos**
- Additional Data Sources to drive better **Attack Context**
- **Shift Left** in detection to stop attacks earlier
- Increased **operational efficiency** as less touch points means less clean up
- **Analytics** across **Data Sources**, e.g. NGFW, Prisma, SASE, third Party
- Understanding the full attack causality chain is critical for **complete recovery**

paloalto NETWORKS | CORTEX

Thank You

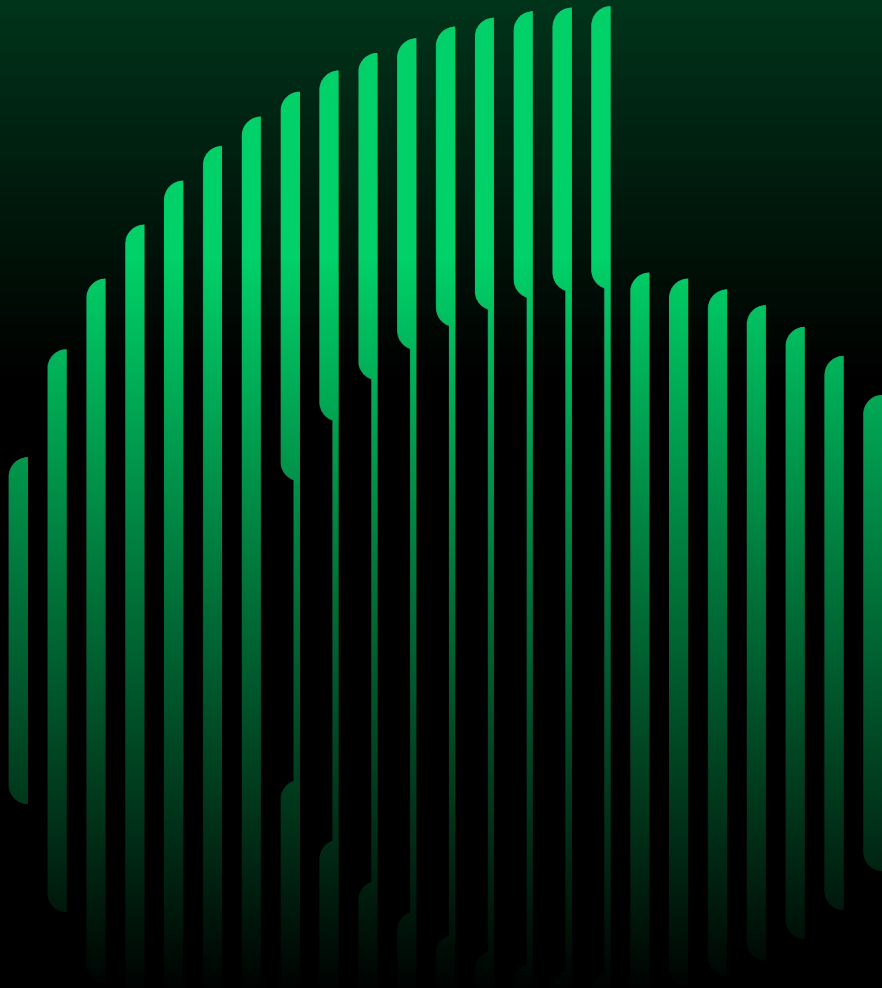
paloaltonetworks.com



paloalto NETWORKS | CORTEX

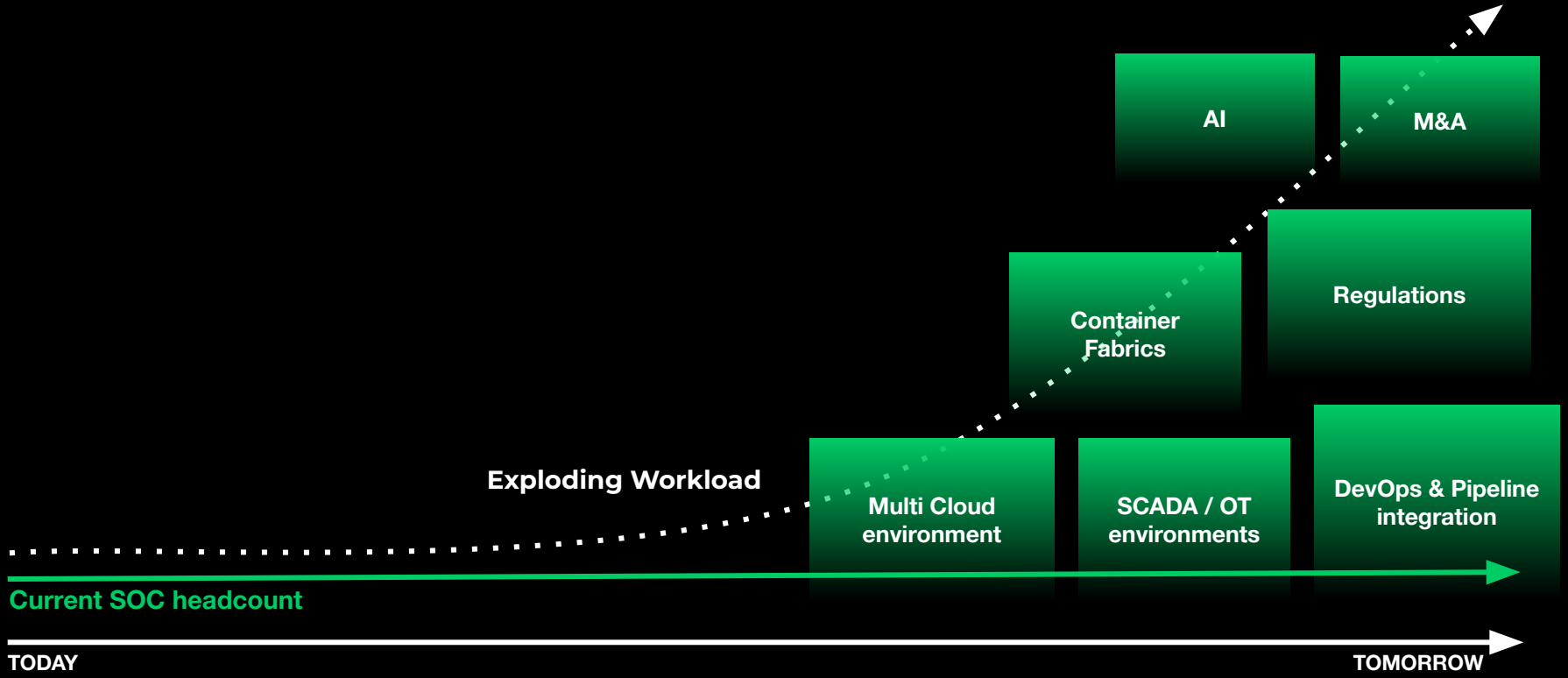
Transform the SOC by re-thinking the SIEM.

A Journey to the Modern SOC with Cortex XSIAM

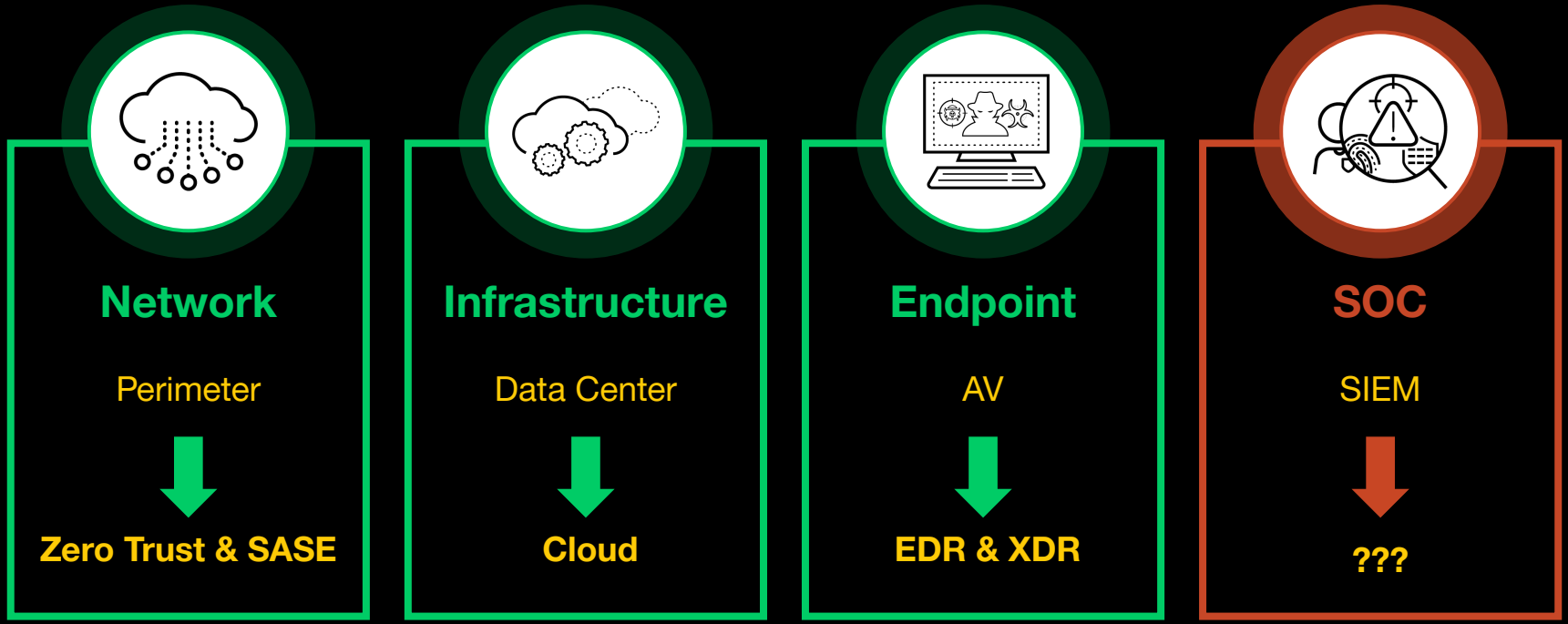


Thomas Maxeiner
Director EMEA Central | Cortex Area Sales Executive

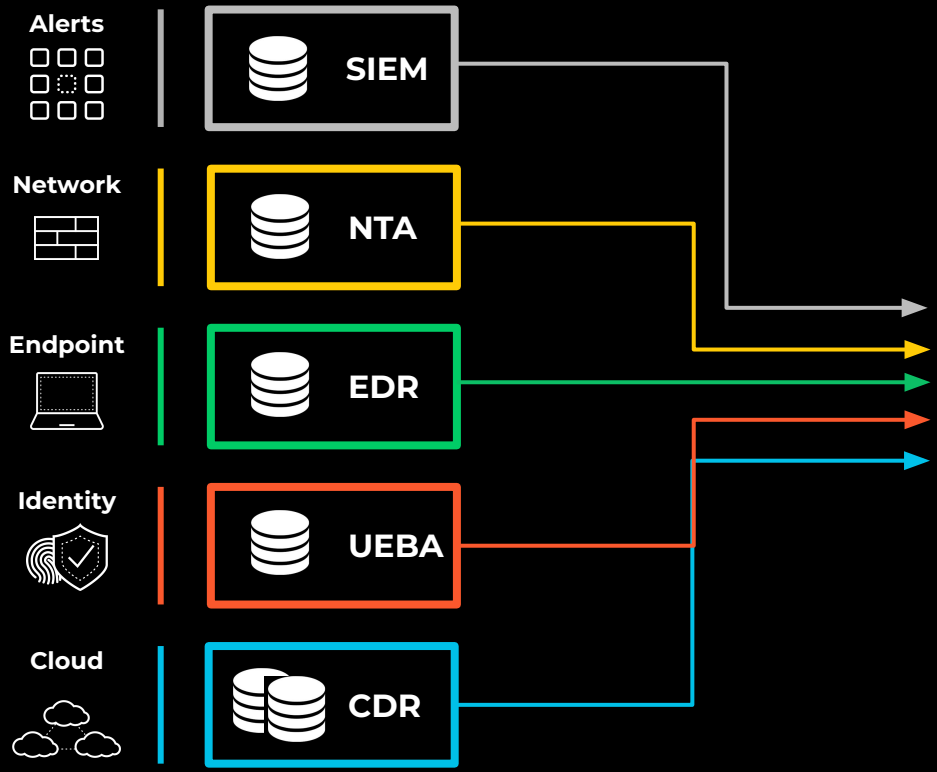
The SOC Challenge: Scalable and Adaptive to new Business Demands as part of the Digital Transformation Journey



Today's dilemma: Most IT domains have been transformed. But in the SOC we are still problem driven



The Result: Too Much Info, Too Many Silos, Too Many Alerts



~11K
alerts per day

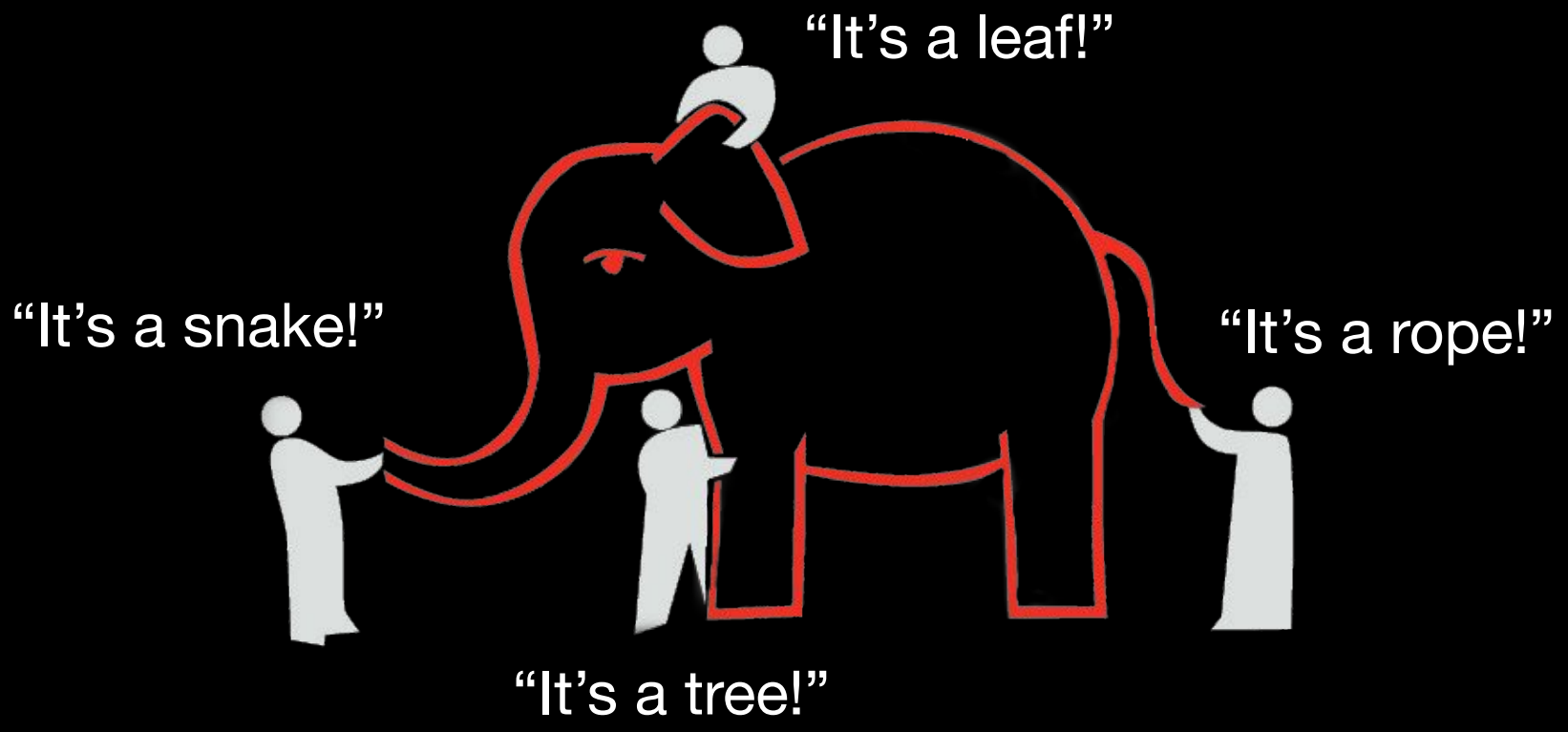
4+
days to investigate

> 30%
of Alerts are untouched / day

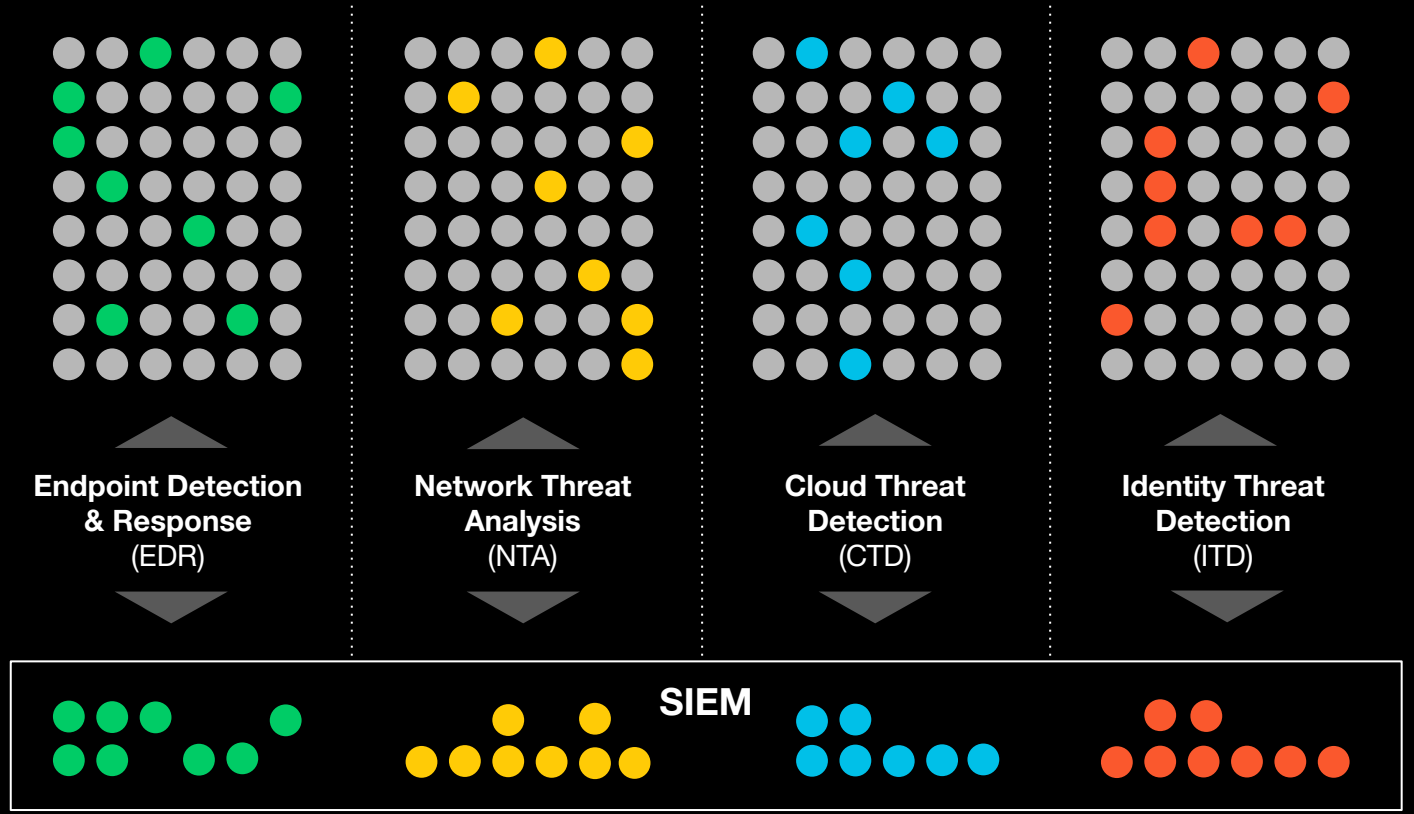
212
days of dwell time

Source: Forrester (The 2021 State of Security Operations), Demisto (The State of SOAR Report, 2018), Ponemon (The Cost of a Data Breach, 2021)

Why: A siloed Detection approach leads to the “The Elephant Problem”



Siloed Detections create “Opinions” (Alerts) bases on limited context

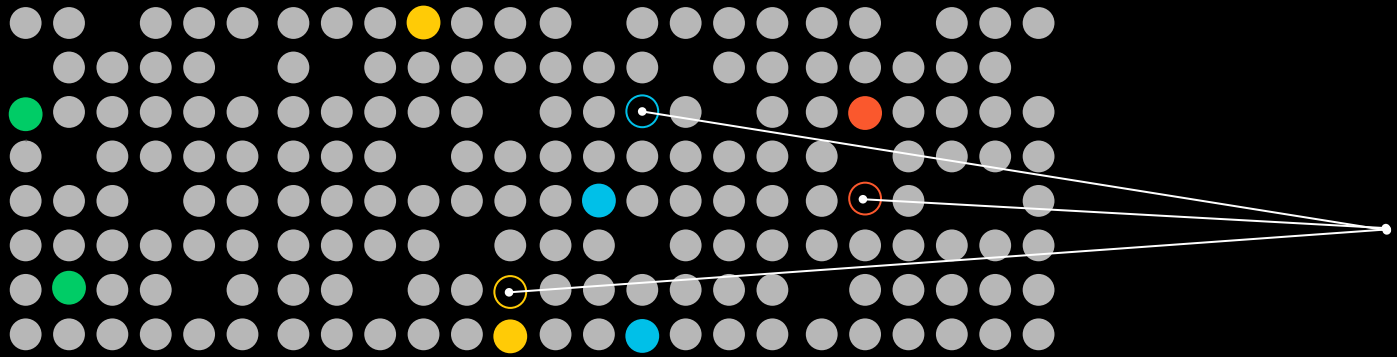


Data is split across technologies

Product based detections

Sileod Product Alerts send to SIEM based on limited Data visibility

Analytics across all Data Sources as Hackers do not think in Silos



Open Data Model to Parse and Normalize

Eliminate False Positives through Atomic Alert Playbooks

XSIAM

Endpoint Detection & Response (EDR)

Network Threat Analysis (NTA)

Cloud Threat Detection (CTD)

Identity Threat Detection (ITD)

Apply multiple Detection Rules and ML Engines on full raw Data

Auto-Stitched Dataset to tell the Attack Story

Our Approach: XSIAM Designed Around Three Key Concepts

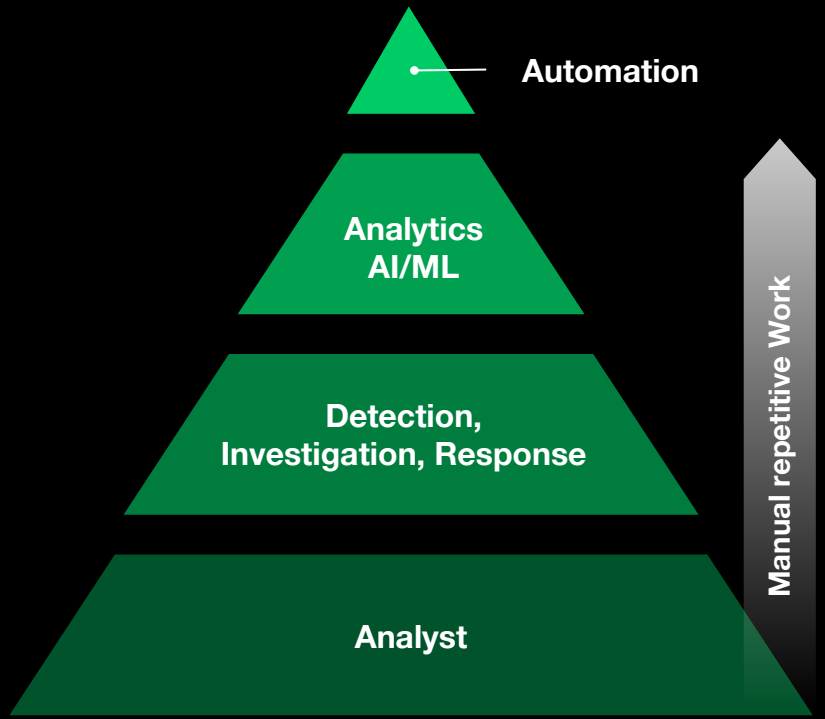
Intelligent Data & Analytics

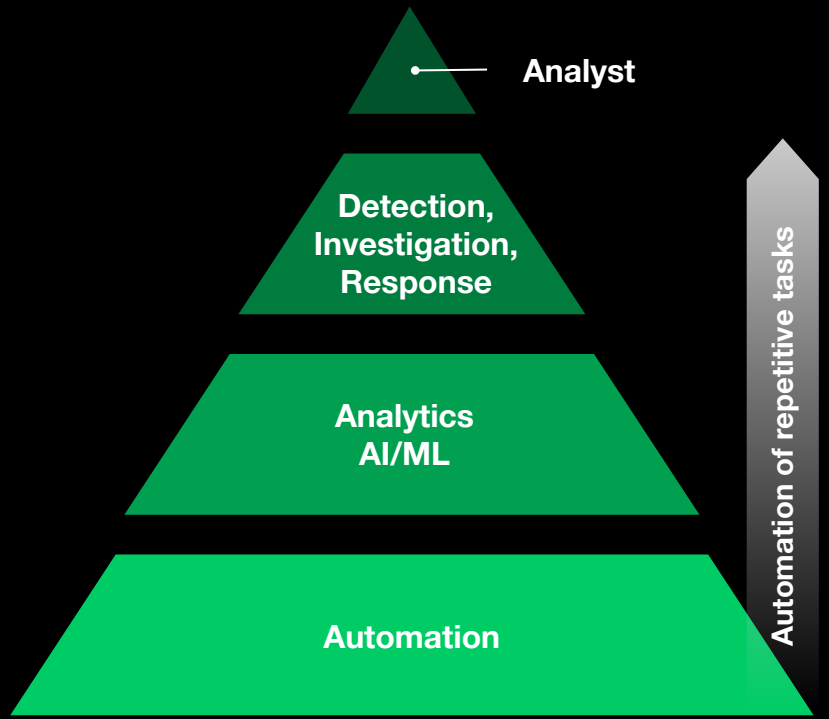
Automation First

Proactive Security

XSIAM delivers a transformation in detection and response, analyst experience, and continuous risk reduction.

With XSIAM we are changing the Focus





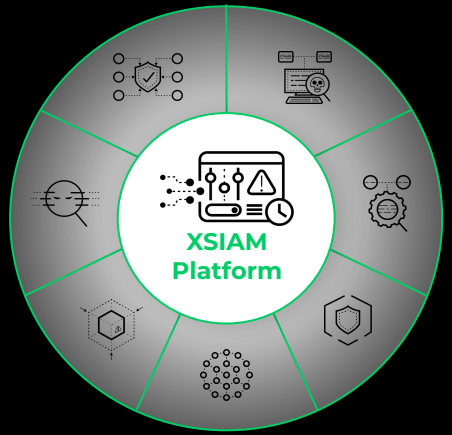
Redesigning the SOC: Single platform to implement, configure, manage all key capabilities in a single UI

- Endpoint Protection
- User Behavior Analytics
- Threat Intelligence Platform
- Endpoint Detection & Response
- Network Detection & Response
- Cloud Detection & Response
- Identity Detection & Response
- SIEM, SOAR
- Attack Surface Management

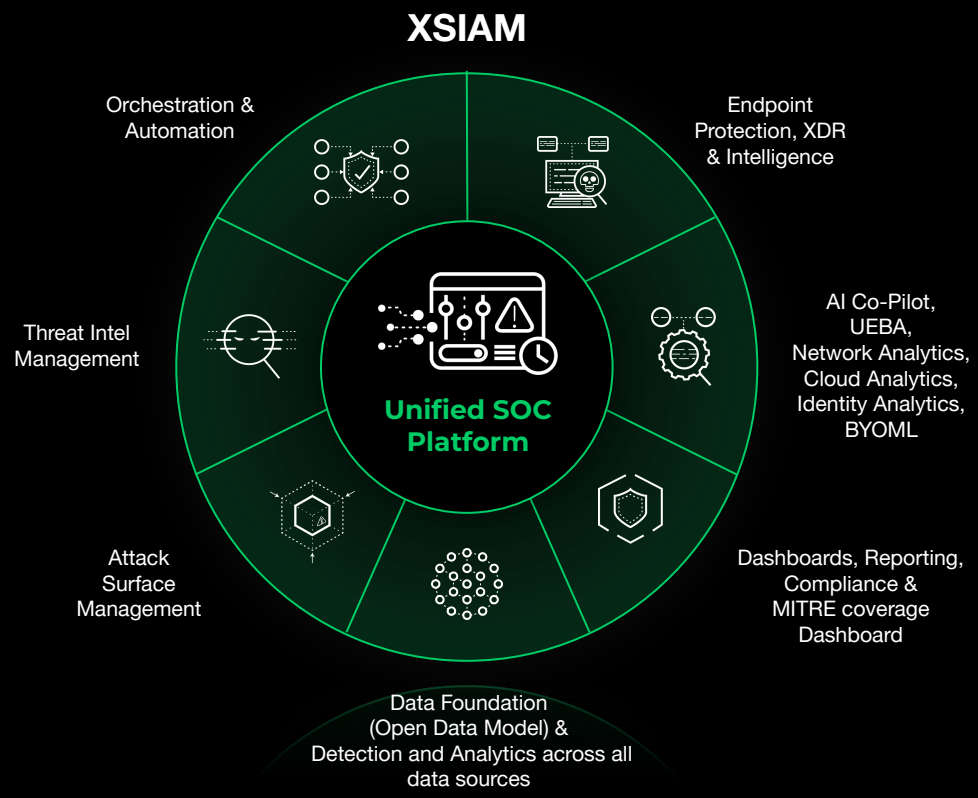
Protection

Investigation
Detection
Response

Attack Surface Management



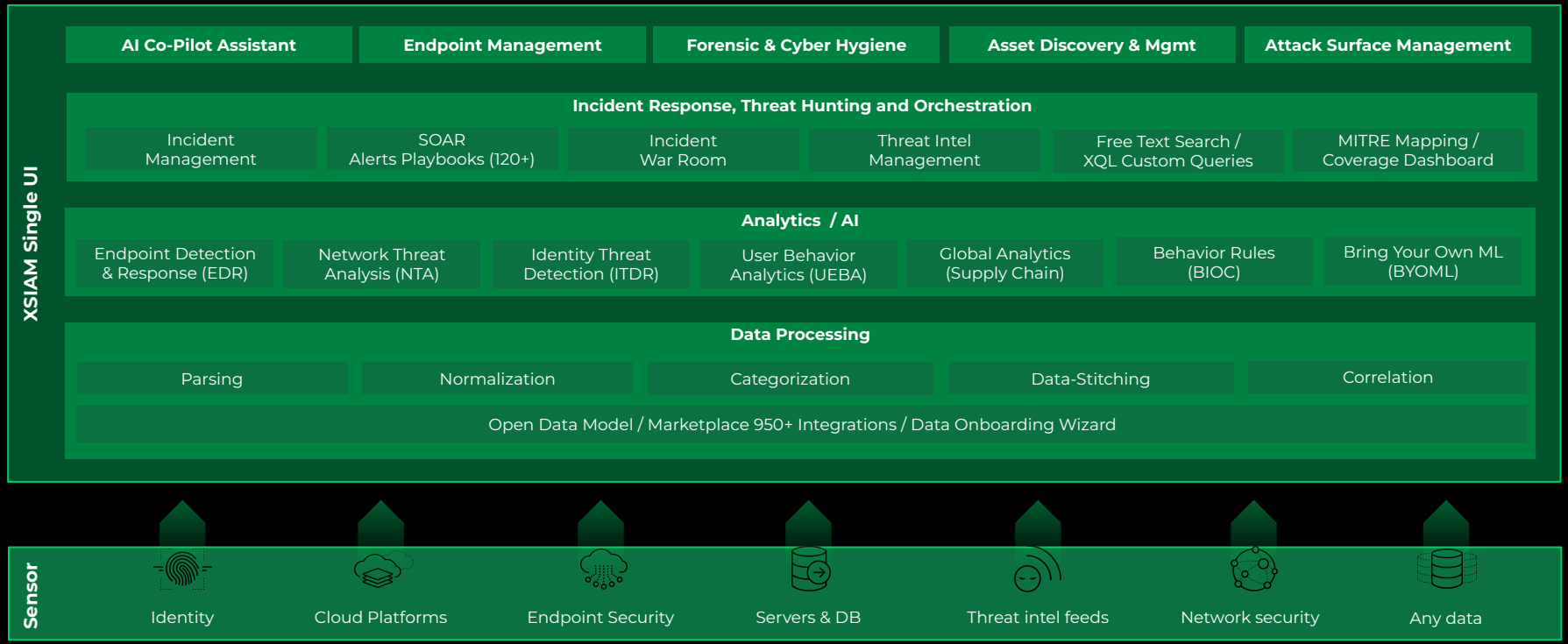
XSIAM Is the Next Big Transformation in Security Operations



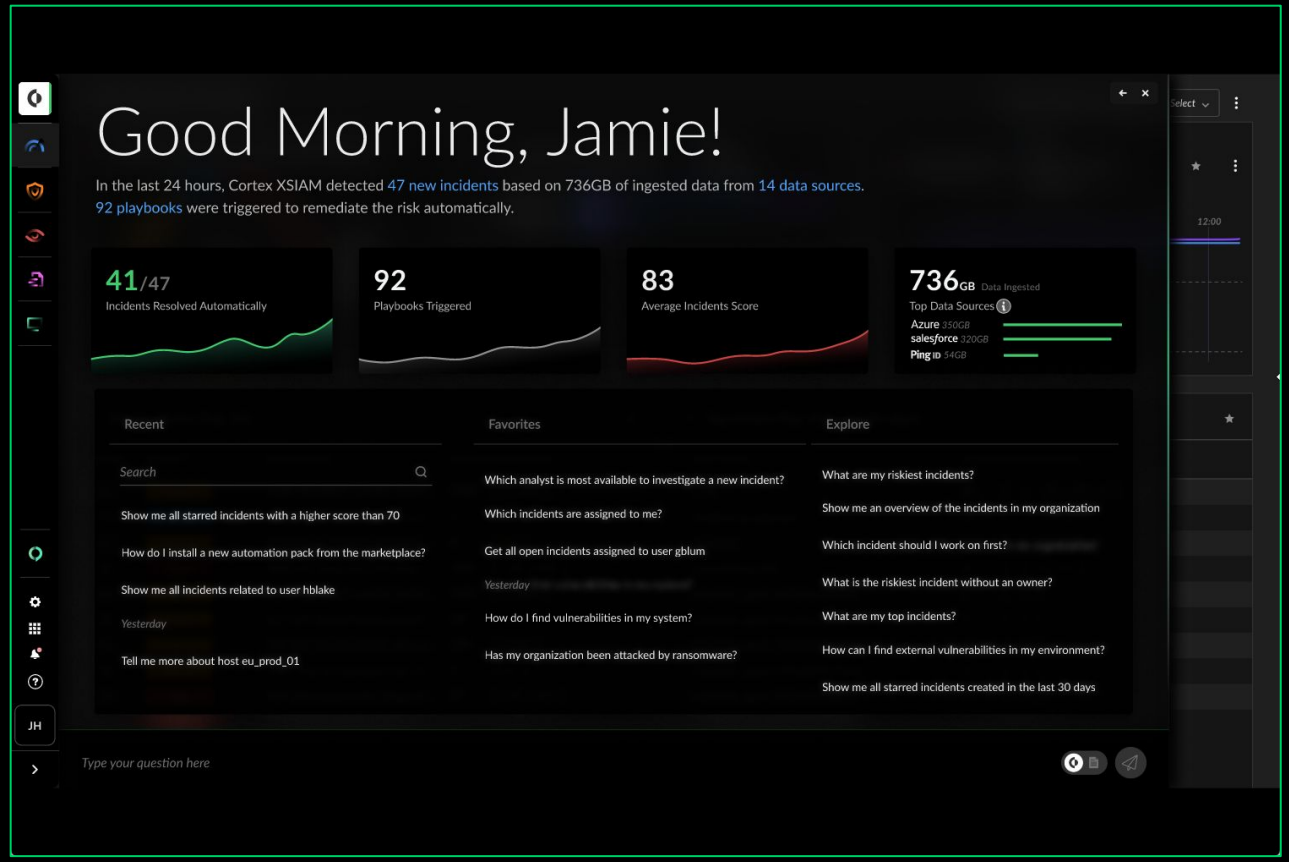
A new design for security operations:

- **Redefines** SOC architecture into an automation-first approach
- **Unifies** best in class SOC functions to improve analyst experience
- **Integrates** multiple products into a single platform (unified back- and frontend)
- **Extends** the SOC to the cloud, for complete visibility

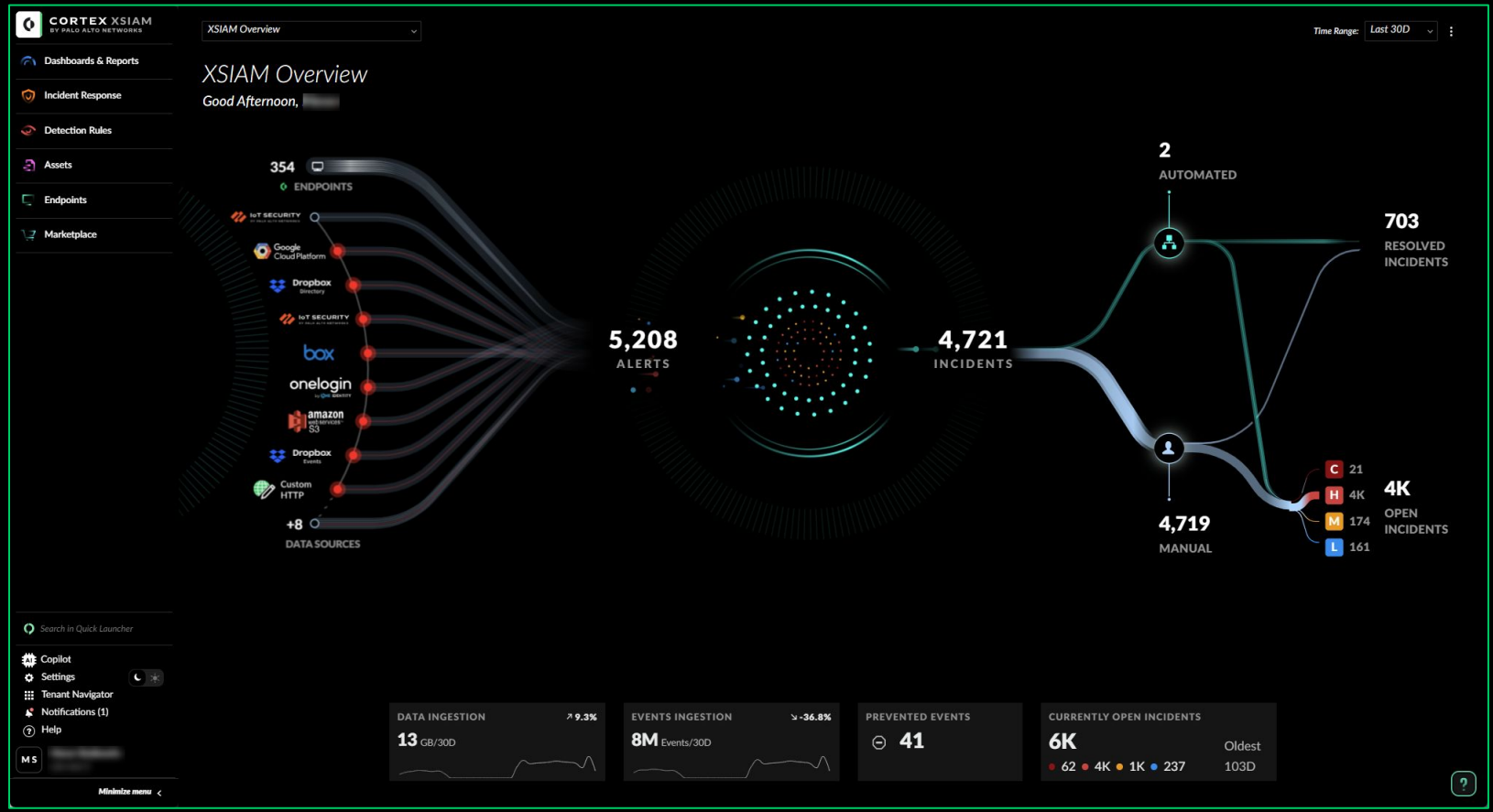
XSIAM is a modular, integrated and AI Data driven SOC Platform



Co-Pilot Assistant (Generative AI)



XSIAM Command Center



Automation First

Bring in Automation where it Matters

Bring in Automation where it Matters

Incidents are unique.

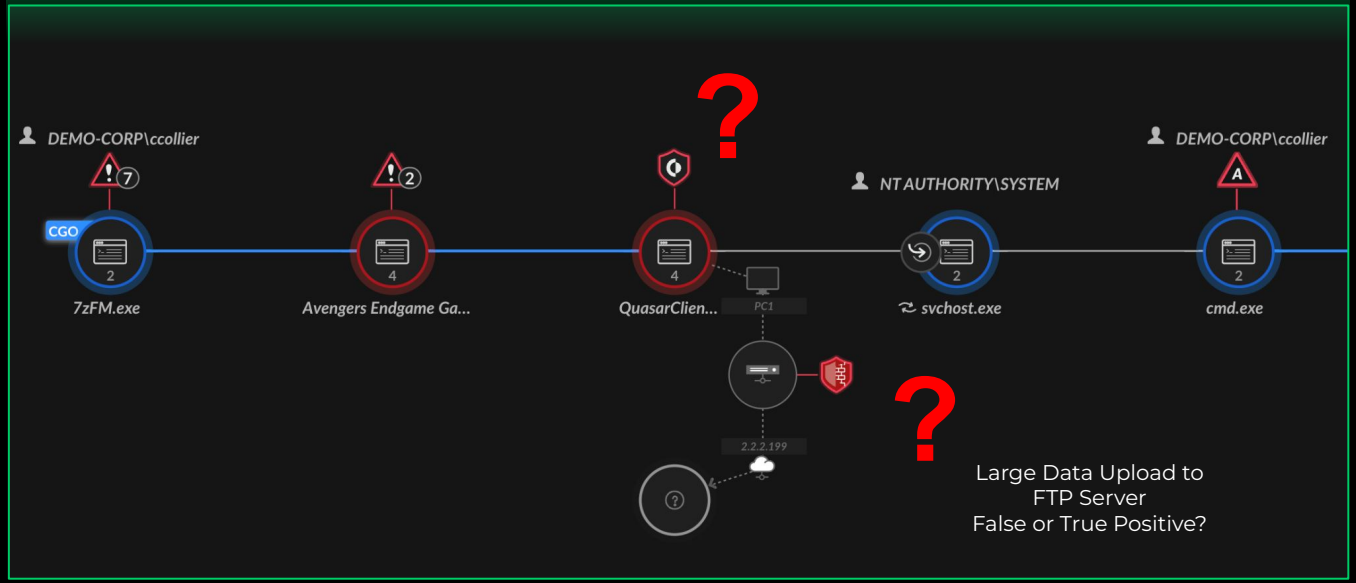
Alerts are the same.

Every Day Alerts…

- Several failed Logins for Locked-Out Account
- Large Upload to FTP Server
- Failed Connections
- New Administrative Behavior / Lateral Movement
- Local Analysis Malware / WIldFire Malware
- Greyware Detection
- Adversary scanning internet-connected assets

Bring in Automation where it Matters: Combing Incidents with Playbooks to auto-resolve Alerts

Auto-Data Stitching to build Causality Chain



Playbooks to auto-resolve open Alerts

AUTOMATION

1 Playbook waiting for analyst

M 27626 - Fortigate - Machine Scanning The Network

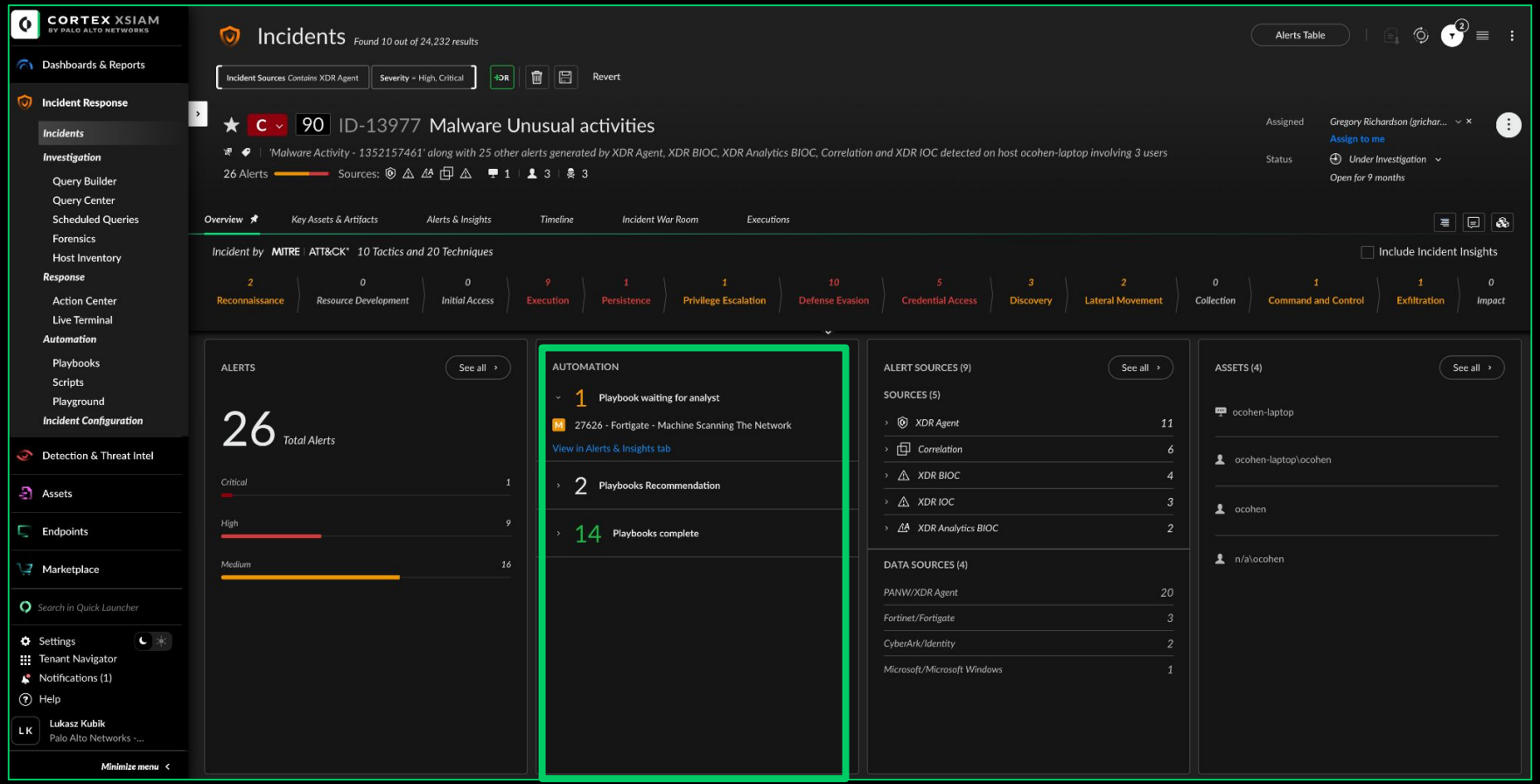
View in Alerts & Insights tab

2 Playbooks Recommendation

14 Playbooks complete

paloalto NETWORKS | CORTEX

Automation in the Incident View to auto-resolve Alerts



Daily Log & Alert Volume in the Palo Alto Networks SOC

Log Events
Includes all log events ingested to XSIAM

Raw Alerts
All out-of-the-box alerts generated by security logs

Alerts
After grouping, exclusions, deduping

Analysis
Automated fully or partially

Incidents
Any alert that requires SOC action

10
SECONDS
Mean Time to Detect

1
MINUTE
Mean Time to Respond
(High priority)

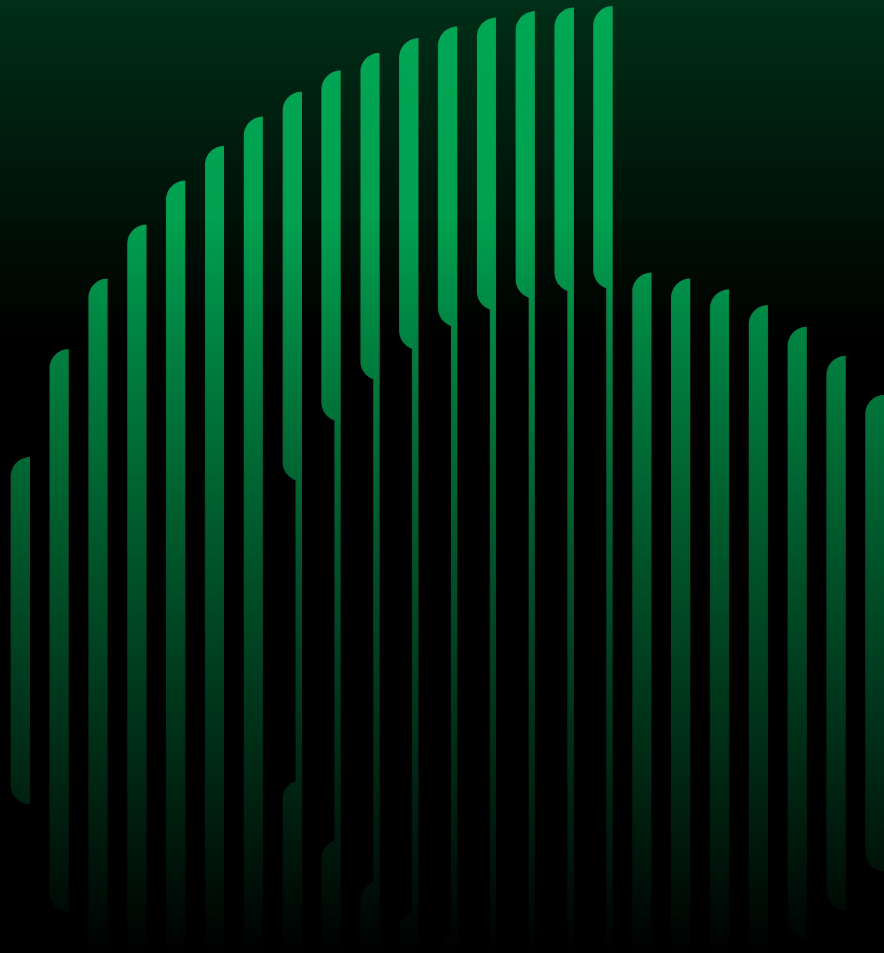
16
FTE
Staff automation efficiency saving
(per annum)

paloalto NETWORKS | CORTEX

paloalto NETWORKS | CORTEX

Thank You

paloaltonetworks.com



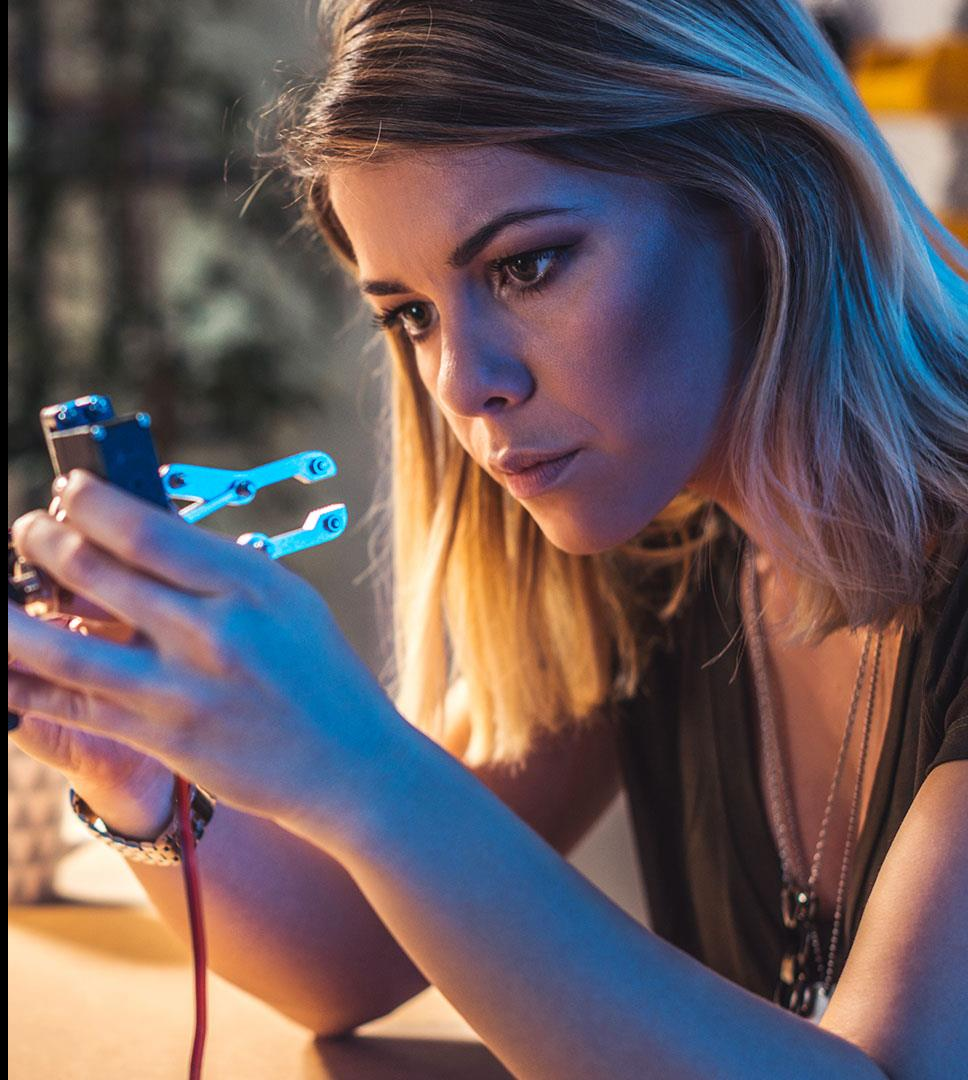
Orange
Cyberdefense

XDR unter der Lupe:

Welche Lösung passt zu Ihnen? Finden Sie Ihren perfekten Match!

Thomas Jupe, Business Development
Thomas.Jupe@Orangecyberdefense.com
https://www.linkedin.com/in/thomas-jupe-67604593/

XDR-Systeme bieten zahlreiche Funktionen in Bezug auf Sicherheit, Bedrohungsschutz und Abwehr



Grundsätzlich
Evolution

Orange Cyberdefense

EDR

- Überwachung von Benutzer- und Softwareaktivitäten
- Proaktive Erkennung und Untersuchung fortschrittlicher Bedrohungen
- Bewertung von Schwachstellen
- Zuverlässige Alarmierung und Reaktion
- Automatisierungsfunktionen / Integrierbarkeit

Vor allem **Advanced Persistent Threats (APTs)** und **Ransomware** im Netzwerkverkehr bleiben mit klassischen EDR-Tools **häufig** unentdeckt.

XDR

- Transparenz über Endpunkte, Netzwerke, Server, Applikationen sowie Cloud
- Erkennung von unbekannten Bedrohungen und Lateral Movement
- AI - Threat Intelligence zur ganzheitlichen Überwachung
- Schwachstellenerkennung und Bewertung
- Konsolidierung von Incidents und Aktivitäten über unterschiedliche Systeme

Mehrwerte einer XDR – Lösung

Was kann ich grundsätzlich von XDR erwarten?

Orange Cyberdefense

- Zentrale Sicht auf Bedrohungen
- Reduzierte Mean Time To Detect (MTTD)
- Einheitliche Orchestrierung der Bedrohungsreaktion
- Einsatz ohne spezifische Konfiguration

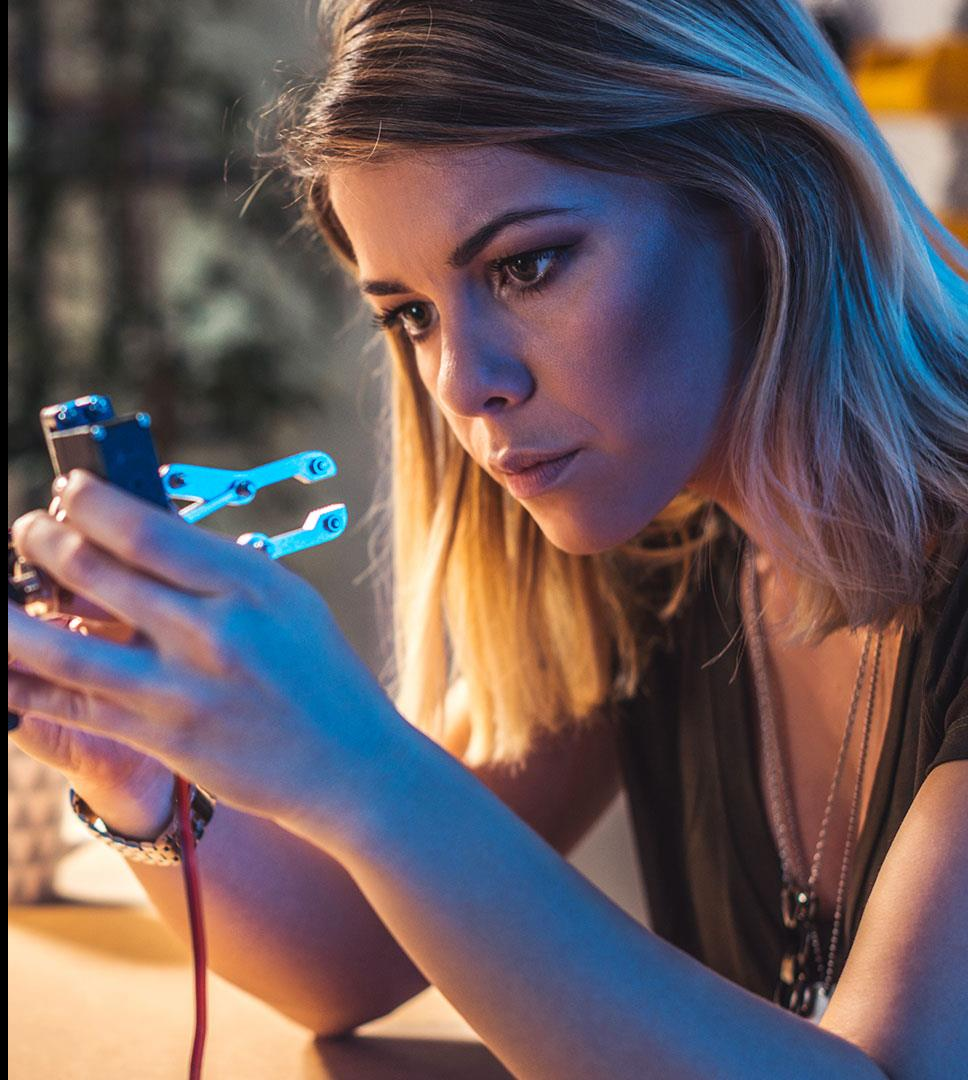
Aber wo genau liegt der Unterschied?

Vergleich zwischen SIEM, EDR und XDR

Orange Cyberdefense

FEATURES	SIEM	XDR	EDR
Description	Security Information & Event Management / Security Analytics	eXtended Detection & Response	Endpoint Detection & Response
Data sources	Any log data	Endpoint telemetry, network traffic and selected log data	Endpoint telemetry
Time-to-value	Months	Weeks	Days
Customization	High	Low	Low
Data model	Flexible	Fixed	Fixed
Use Cases	Threat Detection, Data Analytics, Operational analysis	Threat Detection & Response	Threat Detection & Response

Wie komme ich nun zu einem perfekten Match?

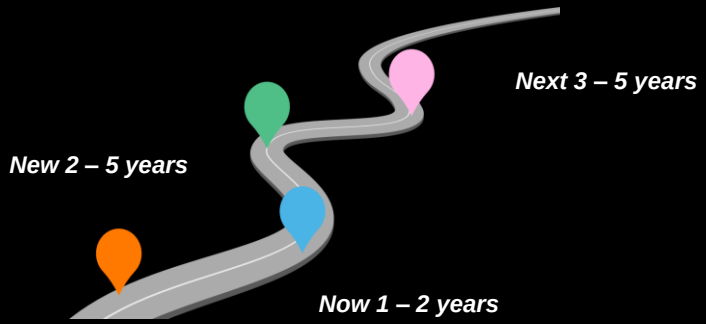


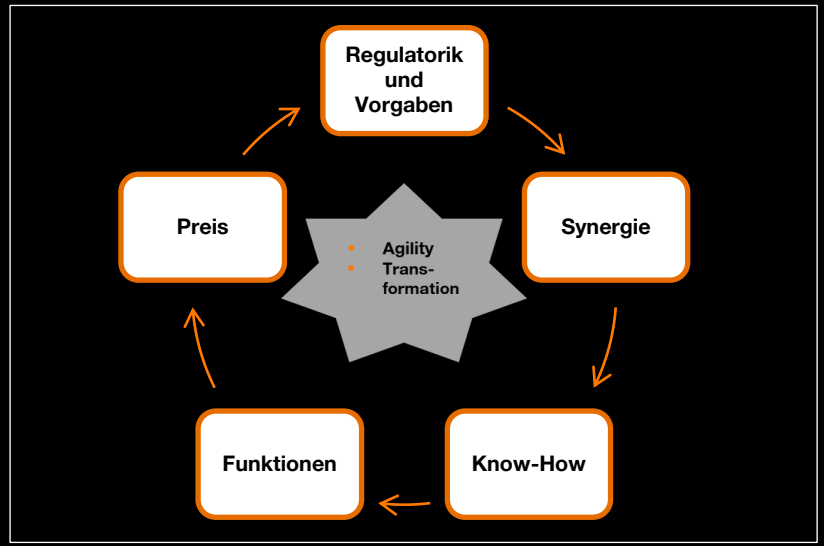
Ein strategischer Ansatz sollte immer die Basis sein!
Der Anfang aller Entscheidungen!

Orange Cyberdefense

Zitat:

Wer das Ziel kennt, kann entscheiden;
wer entscheidet, findet Ruhe;
wer Ruhe findet, ist sicher;
wer sicher ist, kann überlegen;
wer überlegt, kann verbessern.





Nicht jeder Angreifer ist gleich

Vor welchen Angreifern möchte ich mich schützen?

Orange Cyberdefense

Zitat: „Kennst du dich selbst und den Gegner, / ist der Sieg dir unbenommen; / kennst du Himmel und Erde, / ist der Sieg vollkommen.

Skilled Hacker mit definierten Zielen (Level 3)

High Skilled und Funded Attacker (Level 4)

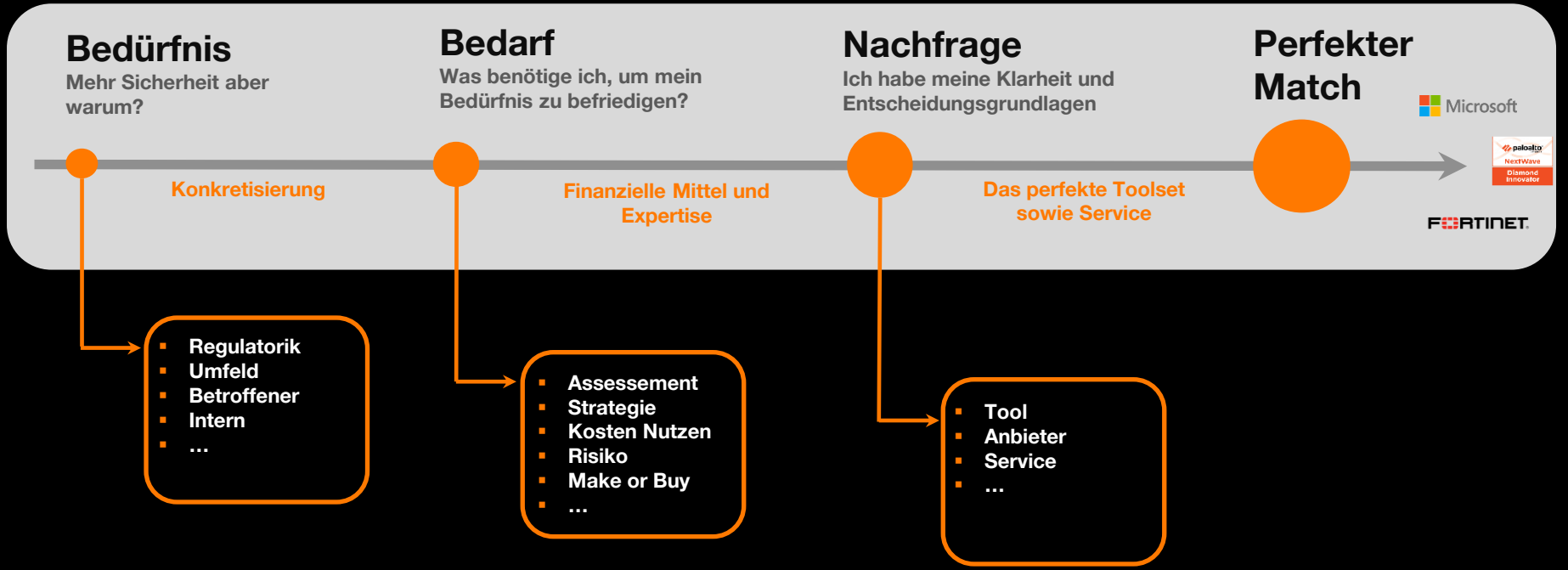
Nation State Sponsored (Level 5)

Von einem Bedürfnis zum perfekten Match

Ein XDR nur weil der Markt sagt, dass es die Zukunft ist?

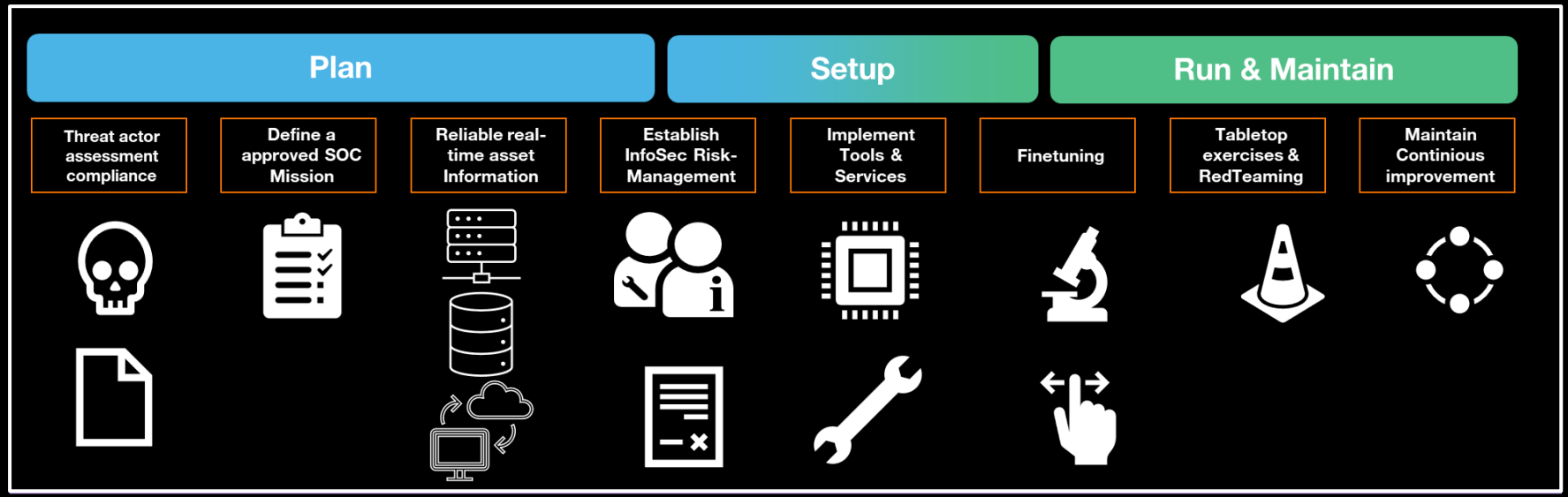
Orange Cyberdefense

Lieber rational denkend, anstatt dritten und Trends blind zu vertrauen!



Geführte Umsetzungsstrategie
- ein schrittweiser Ansatz

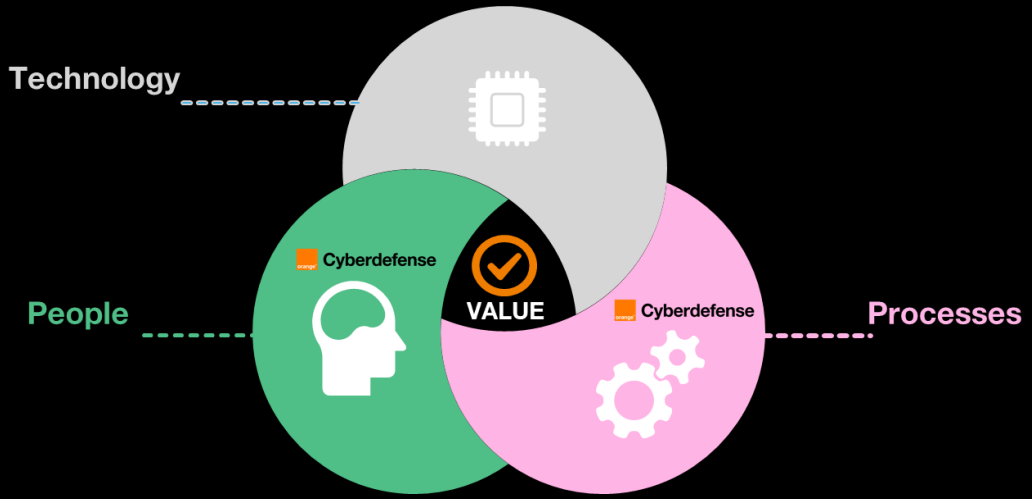
Orange Cyberdefense



Ensure adequate knowledge

Implement mature processes

Lassen Sie uns gemeinsam Ihren individuellen perfekten Match finden!



Orange Cyberdefense

Build a safer digital society.

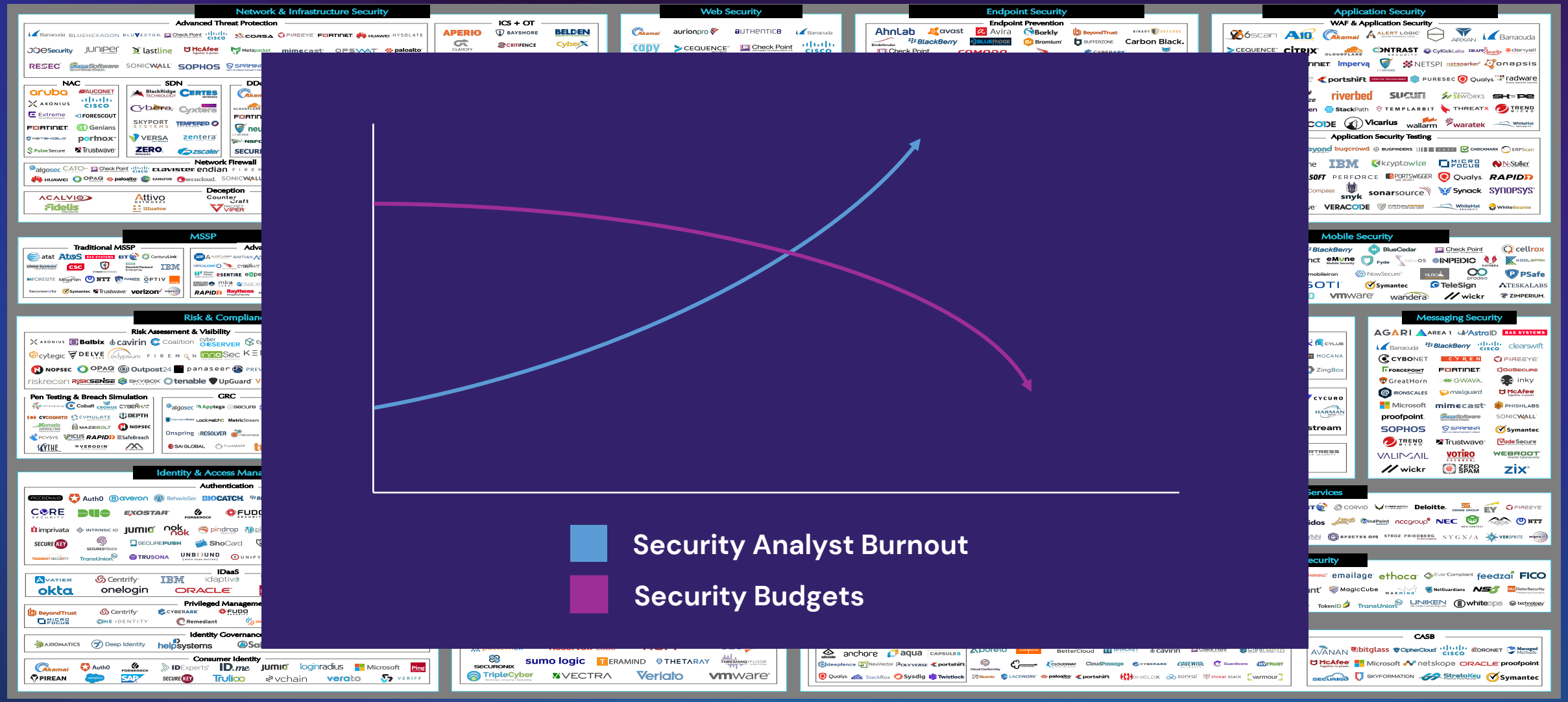
Make Microsoft Defender work smarter and harder

with AI-Powered MXDR

Alexander Luig
Senior MXDR Specialist

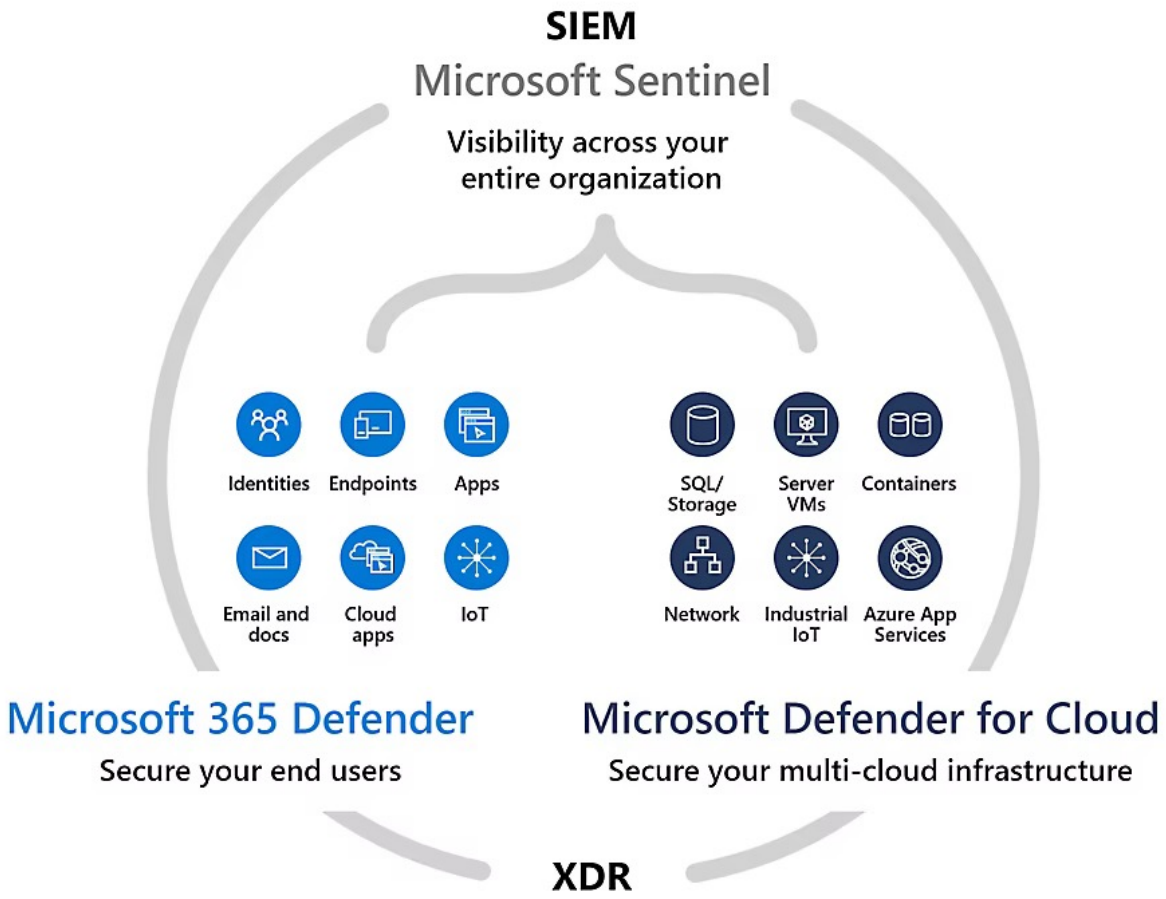
Ontinue

More products isn't the answer.



Source: Momentum Cyber

Microsoft simplifies the problem.



Leader in 4 Magic Quadrants

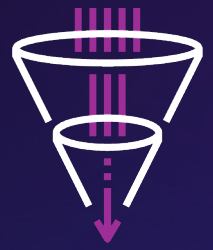
Access Mgmt.

Ent. Information Mgmt.

SIEM

Endpoint Protection

Operationalizing can be challenging.



Benign vs. True Positives

They filter false positives but struggle to distinguish benign vs. true positives.

Poor Collaboration

Different people, systems, and consoles make collaboration hard and slow.

Lack of Specialization

Support for diverse technologies limits ability to maximize your existing investments.

Take a tour of Ontinue ION

Collab. Respond. Resolve.

Alexander Luig
Senior MXDR Specialist

Ontinue

Ontinue ION

Microsoft

AI-Powered MXDR for Microsoft Security customers

People

Data scientists, Microsoft MVPs, and security experts

Process

A continuous, closed loop assess-prevent-detect-respond process delivered from dedicated advisors and a global set of SOCs

Technology

AI-Powered platform that natively integrates into Microsoft

What is needed?

AI-Powered

AI that models defenders and defended environments to localize protection and drive automation.

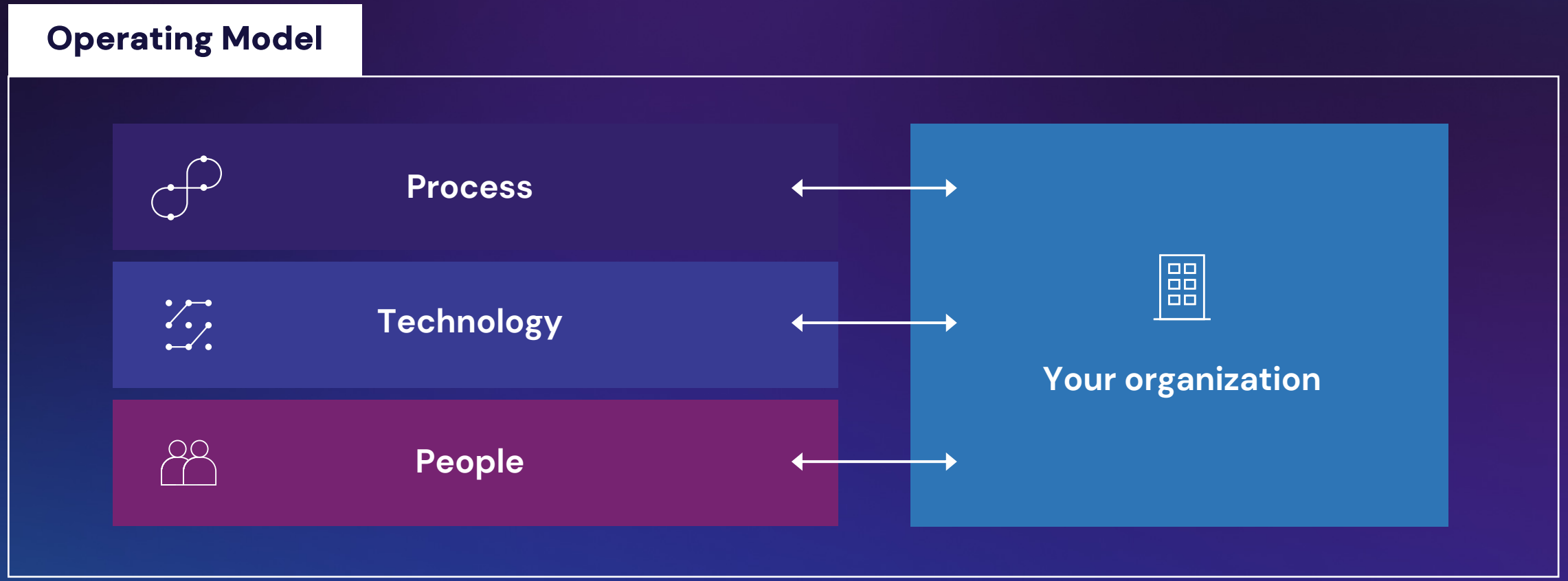
Collaboration

Streamlined communication between Security, IT, and providers using collaboration systems.

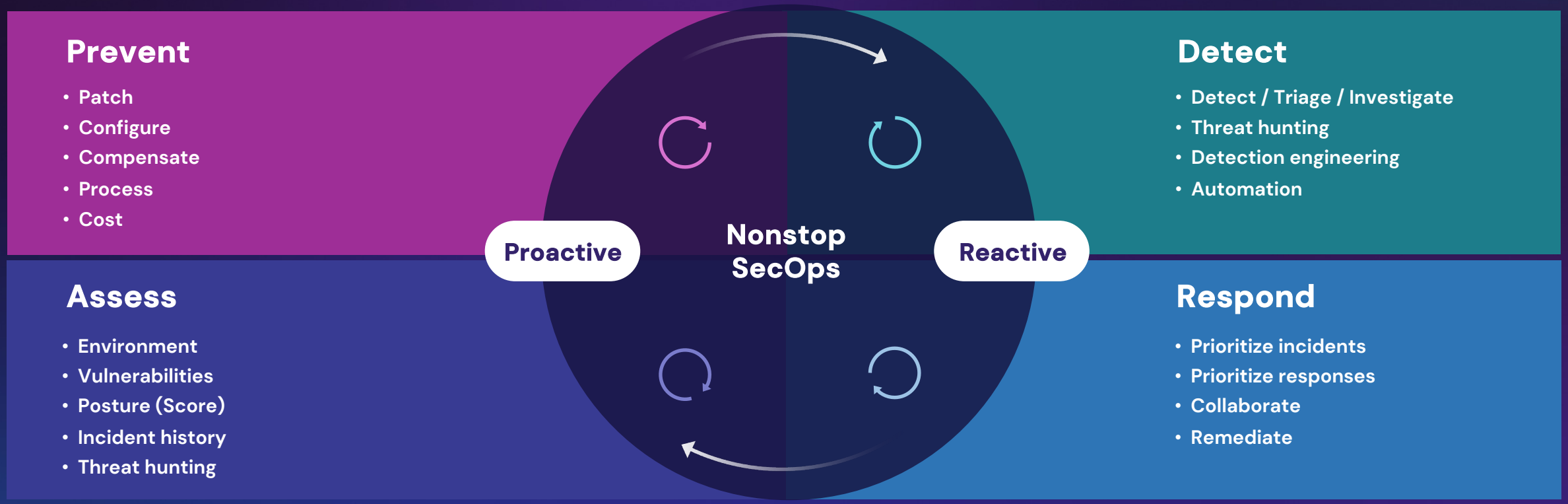
Specialization

Deep Microsoft expertise and focus to enable tool consolidation and cost optimization.

Ontinue's Service Approach



Combining pro- and reactive processes



Cyber Advisors

Cyber Defenders

Power of dedicated Ontinue teams

Ontinue teams that support security operations with intelligence, automation, and engineering

- Data Science Team
- Automation Team
- Detection Engineering Team
- Threat Intel Team

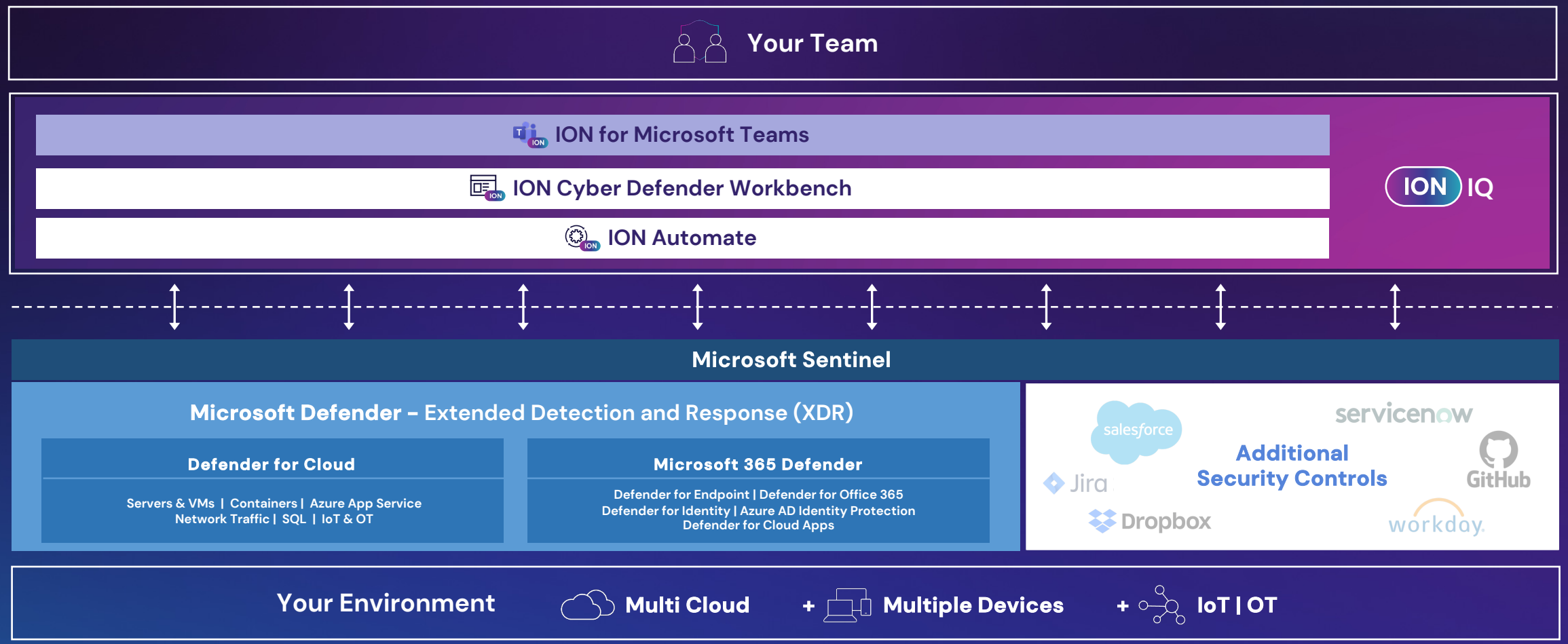
Your Team

Ontinue teams responsible for day-to-day security operations

- Cyber Advisors
- Cyber Defenders
- Threat Hunters
- Vulnerability Analysts

ION Cyber Defense Center

Enabling existing Microsoft technology



Live Demo

Collab. Respond. Resolve.

Alexander Luig
Senior MXDR Specialist

Ontinue

Q&A

Thank you!

Alexander Luig
Senior MXDR Specialist

Ontinue

Reach out on LinkedIn.

Collab. Respond. Resolve.

Alexander Krebs
Senior Sales Cybersecurity

Alexander Luig
Senior MXDR Specialist

Ontinue

Ein SOC ist ein SOC! Wirklich?

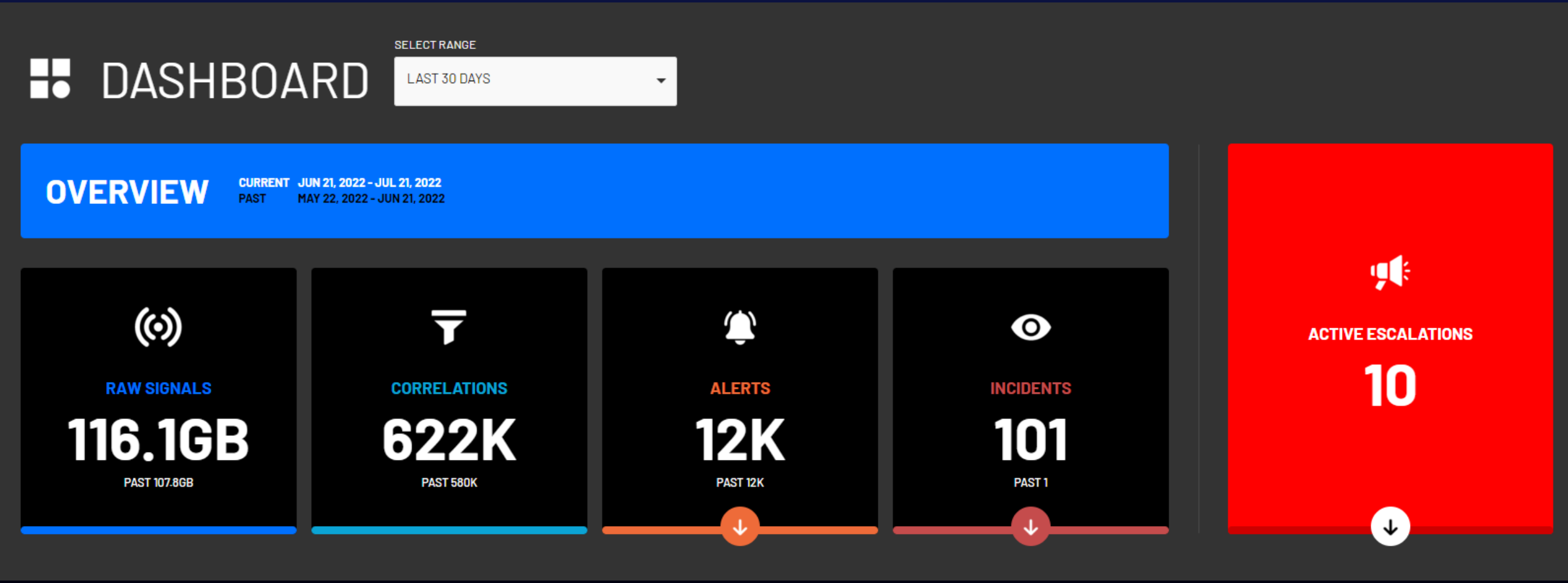
Securing the Future - Managed Services vom Endpoint bis zum 24/7 SOC

Alexander Schmidt
Director Sales | 21.11.2023

OBRELA

Alexander Schmidt
a.schmidt@obrela.com
+49 (0) 152 33 98 86 43

Von Rohdaten zur aktiven Eskalation in 30 Minuten



Überwachen. Nachforschen. Jagen. Reagieren.

ENDPOINT | NETWORK | ON PREMISES | CLOUD

Detect

DETECTION
Erkennung basierend auf IP-Inhalten von Algorithmen, Nutzung von Tausenden von Korrelationsregeln, Watchlists, Bedrohungsdaten und fortschrittlicher Analytik (statistische Analyse, maschinelles Lernen)

Investigate

VALIDATION
SOC-Analysten untersuchen unter Berücksichtigung zusätzlicher Kontextinformationen und Anreicherung.

INVESTIGATION
Die Empfehlungen der SOC-Analysten und die Leitlinien für den Umgang mit Vorfällen werden innerhalb von Swordfish bereitgestellt

Respond

SOC THREAT RESPONSE
Von SOC-Analysten ermöglichte softwaregesteuerte Maßnahmen oder automatisierte Playbooks zur Eindämmung der Bedrohung.

EMERGENCY INCIDENT RESPONSE
Bereitgestellt von einem hochqualifizierten, zertifizierten Incident-Response-Team..

THREAT INTELLIGENCE
Integration mehrerer Threat-Intelligence-Feeds.

PROACTIVE THREAT HUNTING
Threat Hunting wird bei unseren Kunden wöchentlich durchgeführt.

24x7 Analyst-Analyst-Access
Via Swordfish, Email, Telefon

The Power of „The UseCase“

Praxisorientierte Szenarien stärken die Effektivität von SIEM und SOC bei der Identifizierung, Analyse und Reaktion auf Sicherheitsvorfälle.

UseCases sind essenziell für SIEM und SOC. Sie ermöglichen präzise Regeln zur Bedrohungserkennung.

- Sicherheitsteams reagieren proaktiv
- Ressourcenwerden effizient genutzt
- Compliance-Anforderungen werden erfüllt
- Automatisierte Reaktionen ermöglicht

Und Ihr MDR und SOC as a Service Partner?

Für einen MDR-Provider wie Obrela sind klar definierte UseCases entscheidend:

- sie ermöglichen eine effiziente Erkennung und Reaktion auf Sicherheitsvorfälle in Echtzeit
- standardisieren Sicherheitspraktiken
- passen sich an individuelle Kundenanforderungen an
- ermöglichen schnellere Reaktionszeiten
- verbessern die Skalierbarkeit der Dienstleistungen

Durch die präzise Anwendung von UseCases kann OBRELA effektiv auf unterschiedliche Kundenbedürfnisse reagieren und einen konsistenten Schutz bieten.

Obrela UseCases

Im Standard stehen sofort über 1.000 UseCases zur Verfügung, mehr als 75% davon in den letzten 13 Jahren von Obrela entwickelt

Als integraler Bestandteil des Onboarding-Prozesses und darüber hinaus arbeiten wir daran, kundenspezifische UseCases zu identifizieren

Während der Vertragslaufzeit können Sie pro Jahr die Erstellung von bis zu 12 von individuellen UseCases abrufen

UseCase Beispiele für ein Kundenszenario

- Für 'Bind' sind 4 'Device-spezifische' UseCases verfügbar
- Im 'Active Directory' stehen 2 erweiterte Sicherheitskorrelation und 4 Device-spezifische UseCases zur Verfügung
- Darüber hinaus bieten wir mehr als 15 UseCases für Linux-Betriebssysteme sowie 2 UseCases für MySQL-Datenbanken

Zusammenspiel UseCases / Playbooks am Beispiel: Ransomware

2023 Vorfall bei einem Obrela Kunden, Deutsches Dienstleistungsunternehmen, Rechtsberatung

- 800 überwachte Systeme
- Angriff identifiziert 2023
- Threat Intelligence als Impulsgeber

In diesem Fall wurde verdächtiger oder bösartiger Inhalt auf einem Endgerät identifiziert. Die Analyse zielt darauf ab, die Natur der Inhalte zu verstehen, ihre Herkunft zu ermitteln und geeignete Maßnahmen zur Eindämmung und Bereinigung zu ergreifen. Dabei kommen verschiedene Analysemethoden und Sicherheitswerkzeuge zum Einsatz, um die Bedrohung genau zu charakterisieren und die Auswirkungen auf das betroffene Endgerät sowie das gesamte Netzwerk zu bewerten.

Kurze Beschreibung eines Falles - Verdächtige/bösartige Inhalte auf einem Endpunkt

Malicious activity detected on an internal host (13:46)

Regelwerk wurde mehrmals durch Aktivitäten ausgelöst:

- Rundll32 führt eine verdächtige DLL aus dem Benutzer-Temp-Ordner aus.
- Mehrere verdächtige PowerShell verschleierte Befehle.
- Skriptausführung in Verbindung mit einer verdächtigen .zip-Datei.
- Verdächtige Netzwerk-C2-Kommunikation (blockiert).

Die SOC-Analysten haben die Warnungen auf weitere verdächtige Befunde überprüft und die Artefakte mit Hilfe von "Technologie" eingehend analysiert

Acknowledged & Action Initiated

Der Kunde hat den Fall in der Swordfish-Plattform bestätigt.

Reported Case (14:03)

Der SOC-Analyst berichtete über Swordfish und eskalierte die Ergebnisse telefonisch, wobei angemessene Maßnahmen für den Vorfall vorgeschlagen wurden.

- Der Host wurde remote durch Technologie isoliert.
- Die Angriffs-IOCs wurden für die gesamte Unternehmensumgebung durch Technologie gesperrt.
- Die Analyse wurde fortgesetzt.
- Es wurde eine erweiterte Infektion zur gleichen Zeit auf mehreren Hosts und einem Server identifiziert. Weitere Mitglieder des L2 wurden hinzugezogen.

Further Analysis and Investigation

Unsere Analysten setzten ihre Untersuchung über Technologie auf dem Host fort und machten dabei mehrere zusätzliche Entdeckungen.

Die Analyse zeigte eine Verbindung zur Qakbot-Malware-Familie. Link: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/qakbot

Zusätzliche Technologie-Agenten wurden bereitgestellt.

Die Herkunft der Infektion deutete auf eine ausgedehnte Phishing-Kampagne gegen den Kunden hin.

Es wurde eine Analyse der E-Mail durchgeführt, die die Quelle des Angriffs und den Arbeitsmechanismus aufdeckte. HTML-Anhang, der eine Zip-Datei herunterlädt.

.

Continuous communication and Investigation

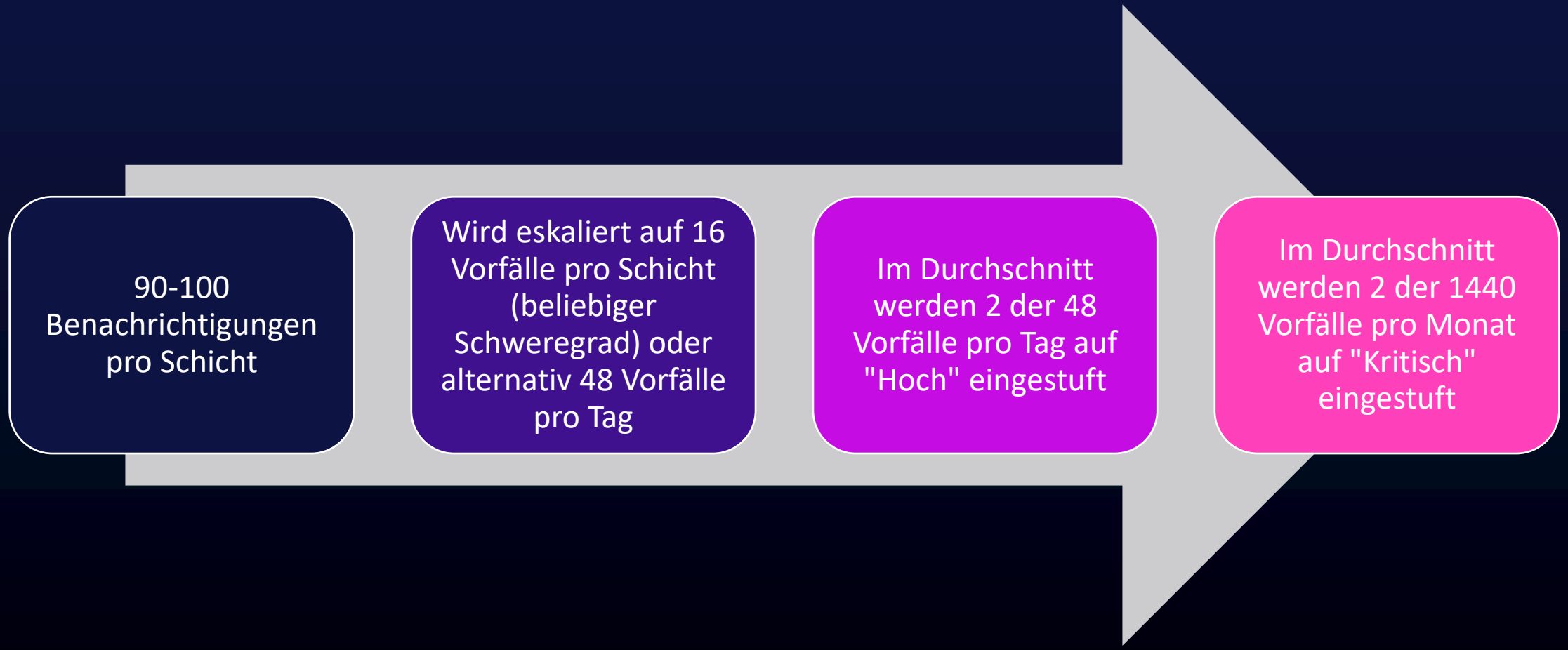
Zusätzliche Warnungen und Befunde wurden erkannt und gemeldet.

In den nächsten Stunden folgten mehrere Telefon-Eskalationen.

Case Close (22:27)

Kontinuierliche Kommunikation und Unterstützung des Kunden, um alle erforderlichen Schritte des Incident-Response-Zyklus zu verfolgen. Mehrfache Wiederholung des IR-Zyklus und Bedrohungssuche in der Umgebung mit der Erstellung von IOCs aus dem TI-Zyklus. Ein weiterer Fall wurde erstellt und anschließend mit diesem anfänglichen Fall korreliert.

Was leistet 1 Analyst pro Schicht?



CASE 1 – Suspicious Internal Activity

- SOC escalated the Incident Case.
- Analysis continued by the analysts.

- Server was isolated.
- Obrela's Incident Response Team was involved to investigate further and provide their analysis regarding the Incident.

AUG 28, 12:45 (UTC+3)

AUG 28, 13:01 (UTC+3)

AUG 28, 18:14 (UTC+3)

Detection → Report & Escalation → Detection #2 → Continuous communication & Investigation → Operations Resume

A Suspicious sequence of exploration activities was identified on the host "XXXX". Multiple commands were executed.

- An outbound connection to IP related to malicious site was detected.
- Malicious files were identified.
- No connections to other clients/servers within the organization were identified.
- No data exfiltration was observed.

CASE 2 - Suspicious Internal Activity

- SOC proceeded with case escalation.
- The analysts requested BTS contribution in order to decode the encoded string.
- The Customer and Obrela were in contact through various communication channels concerning the course of the Incident.

Further Analysis and Investigation:

- The decoded command used the rundll32.exe utility to invoke a function within the comsvcs.dll file.
- It retrieved the process ID of the lsass process using the Get-Process cmdlet and passed it as an argument.
- The command also included the path to a shortcut file

- The customer confirmed that the activity was part of Internal Pentest audit.
- The case was closed following the customer's feedback.

T0 = JUL 8, 20:47 | JUL 8, 21:15 | JUL 8, 21:16 | JUL 12, 10:06

Detection → **Report & Escalation** → **Further Analysis and Investigation** → **Continuous communication & Investigation** → **Operations Resume**

MDR CORE (XDR) detected suspicious activity on the host XXXX from user YYYY, which is a Domain Admin account.

WmiPrvSE.exe spawned the process powershell.exe, which executed an encoded command.

Continuous communication and Investigation:

- CMD was then invoked an ran a command that iteratively retrieved the list of running processes filtered to only include the process with the image name "lsass.exe" and then searched for the specific string within the output. It then invoked rundll32.exe and instructed it to execute comsvcs.dll with specific command line arguments.

- The aforementioned command sequence was identified as "Process Memory Dump" and overall suspicious behavior by MDE.

CASE 3 –Host Infection

SOC detected that the host 'XXXX' is possibly infected by a malicious file.

T0 = MAR 9, 09:50

Detection

- SOC proceeded with case escalation.
- According to Threat Intelligence information, the file in question had malicious reputation.
- The Customer and Obrela were in contact through various communication channels concerning the course of the Incident.

MAR 9, 10:03

Report & Escalation

Further Analysis and Investigation:

- The file was flagged as Trojan:Java/Adwind" and categorized as a "RAT" by MDATP (MDR CORE).
- This type of file can be possibly used by attackers to collect information from an infected machine.
- Defender failed to quarantine the malicious file.
- Suspicious outbound communication has been detected

MAR 9, 10:15

Further Analysis and Investigation

2nd Alert Received:

- More malicious files with bad reputation have been identified residing in different paths of the host.
- TECHNOLOGY also failed to quarantine them.

MAR 10, 2:37

Detection #2

Continuous communication and Investigation:

- Suspicious connections have been identified, as the process "WinSCP.exe" is performing connections and likely file transfer to "ping-pong.gr."
- In addition, multiple outbound connections to various websites on port 69 have been identified. It is found that all of them are directed towards IP XXXX but with many different request URLs and from various processes including browsers, viber.exe, others.

Continuous communication & Investigation

- SOC suggested to verify the activity with the user, scan the host and block the hash, while the host remains isolated.
- Customer confirmed that the pc has been checked.
- The case was closed after the customer's request.

MAR 11, 11:23

Operations Resume

Obrela UseCase SLAs

ACTION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
Time to Acknowledge Ticket	1 working day	1 working day	1 working day
Time to Analyze and Validate	5 working days	4 working days	3 working days
Time to Develop (Standard)	15 working days	5 working days	3 working days
Time to Test	2 working days	1 working day	1 working day

Die Kritikalität von Vorfällen

INCIDENT SEVERITY	CATEGORIES
CRITICAL	The incident creates grave concern affecting the systems and/or services in scope.
HIGH	An incident that creates concern in terms of the target system security in scope.
MEDIUM	An incident that creates potential concern in terms of the target system security in scope.

Rund um die Uhr Echtzeitschutz für Applikationen, Infrastruktur und Cloud

24x7 Managed Detection and Response:
Rund um die Uhr Erkennen und Reagieren auf Bedrohungen.

Umfangreiche Sichtbarkeit und Handlungsbereitschaft:
Ausführliche Überwachung und sofortige Handlungsfähigkeit bei sicherheitsrelevanten Ereignissen.

Skalierbarer Threat-Detection-Technologie-Stack:
Anpassungsfähige Technologie-Infrastruktur für die Erkennung von Bedrohungen, die mit dem Umfang wächst.

SOAR (Automatisierung und Orchestrierung):
Integration von Security Orchestration, Automation, and Response für eine effiziente automatisierte Reaktion auf Vorfälle.

MITRE ATT&CK Framework:
Verwendung des MITRE ATT&CK Framework als Referenz für die Identifizierung, Kategorisierung und Reaktion auf Angriffstechniken.

Threat Intel MDR:
Nutzung von TI für eine datengesteuerte und proaktive Herangehensweise an Bedrohungen.

Umfangreiche Tiefe und Breite:
Tiefgreifende und umfassende Abdeckung von Sicherheitsmaßnahmen, um eine breite Palette von Bedrohungen zu bewältigen

SOCaaS

Obrela SOC-as-a-Service (SOCaaS) bietet Echtzeit-Lagebewusstsein und Schutz durch:

- 157 hochqualifizierte IT-Sicherheits- und Bedrohungsanalysten
- 24/7/365 Überwachung
- Event-Management
- Reporting, Analysen und Service-Reviews
- Dediziertes Service Delivery und Client Success

THREAT HUNTING

- Obrela kombiniert Wissen, Erfahrung, Automatisierung und die proaktive Suche nach Kompromittierungen mithilfe von fortschrittlicher Analyse und Threat Intelligence
- Das Threat-Hunting-Team von Obrela führt proaktive Threat Hunts durch, um Bedrohungsakteure und Schwachstellen zu identifizieren.
- Das Threat-Hunting-Framework von Obrela konzentriert sich auf eine hypothesegetriebene Suche und Profilierung und umfasst die folgenden Ansätze:
  - System Based: Durchführung von Bedrohungs-Hunting-Iterationen, um verdächtige Aktivitäten oder Indicators of Compromise (IOCs) systematisch zu identifizieren
  - Mission Based: Reaktiver Ansatz, bei dem Threat-Hunting aktiv dazu beiträgt, Angriffsaktivitäten zu stoppen

Dankeschön!

Alexander Schmidt

a.schmidt@obrela.com

+49 (0) 152 33 98 86 43

BackUp Slides

MDR Service Metrics / KPIs

Incident Management KPIs

- Anzahl der Vorfälle pro Arbeitsstunde eines Sicherheitsanalysten
- Anzahl der Ereignisse pro Arbeitsstunde eines Sicherheitsanalysten
- Zeitaufwand für die Analyse pro identifizierten Vorfall
- Anzahl der eskalierten Warnungen
- Falschpositive pro Monat
- Identifizierte der False-Positives pro Monat
- Trend der False-Positives pro Monat
- Warnungen/Vorfälle, die gemäß SLA basierend auf der Schwere geschlossen wurden
- Reaktionszeit gemäß SLA basierend auf der Schwere
- Support-Tickets, die gemäß SLA geschlossen wurden

Platform Maintenance KPIs

- Uptime und Nutzung der Komponenten der Swordfish-Plattform (stündlich)
- Anzahl der verlorenen Ereignisse während der Weiterleitung pro Tag
- Anzahl der Ereignisse pro Sekunde pro Protokollquelle und Spitzenwerte (EPS-Überwachung und Berichterstattung)
- Anzahl der Gesamtereignisse im Vergleich zu korrelierten Ereignissen (Ereignisreduktionsrate)
- Anzahl der Korrelationsregeln / Ereignisreduktionsrate
- Anzahl der überwachten Geräte/Protokollquellen pro Monat
- Anzahl der GB/Tag
- Problemmanagement und -lösung basierend auf der Kritikalität
- Anzahl der Änderungsanfragen
- Anzahl der für die Plattform geöffneten Problemfälle

BLUE TEAM

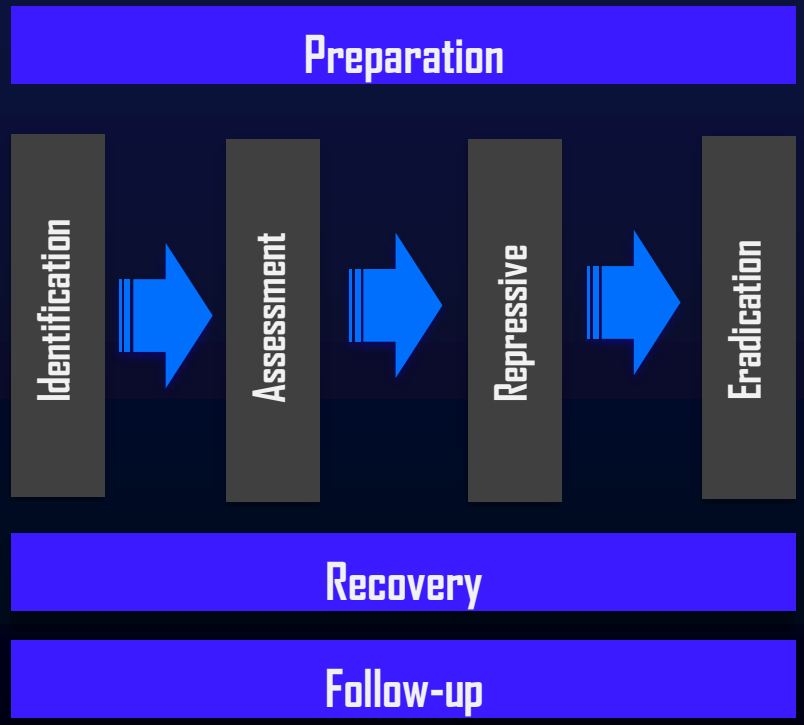
Unterstützt das Security Operation Center mit effizientem Vorfallsmanagement, Eskalierung, und Mitigierung

- Security Operations Support
- Security Posture Assessment
- Vulnerability Scanning
- Vulnerability Management
- Advanced Content Development
- Training

SIRT - INCIDENT RESPONSE

Obrelas Security Incident Response Team (SIRT) ermöglicht dem Kunden eigene Mitigierung / Eindämmung durchzuführen:

- Remote Security Incident Support bis zum Abschluss
- Remote-Untersuchung veranlasst durch Services Requests
- Remote Endpunkt-Untersuchung und Malware-Analyse
- Active Responses/ Playbooks
- Domän-Ausschaltung



Obrela: Dienstleistungsorientiert durch “MDR Native”

- Unsere Customer Success Manager gewährleisten, dass Kunden ihre Ziele nicht nur während der erfolgreichen Implementierung erreichen, sondern auch darüber hinaus. Dies fördert die Zusammenarbeit mit den Experten innerhalb von Obrela.
  - Unser Customer Success Management umfasst die Planung, das Onboarding und die erfolgreiche Kundenbindung,
  - m Dienstleistungsmanagement verfolgen wir wichtige Meilensteine und Metriken, um sicherzustellen, dass der Kunde seine Ziele erreicht
  - Quartärliche Service Reviews

- Der Service Delivery Manager ist Ihr technischer Ansprechpartner
  - Ein Onboardingspezialist, der den Prozess gut kennt und dem Kunden bei technischen Angelegenheiten, wie der Installation von VMs, hilft
  - Er bleibt auch nach dem Onboarding der Ansprechpartner für technische Fragen
  - Quartärliche Service Reviews

Threat Intelligence

- Die Obrela-Plattform ist mit mehr als 20 Anbietern von Threat Intelligence integriert, darunter Emerging Threats, LookingGlass, Alien Vault, Openphish, Zeustracker, IBM und viele weitere. Insgesamt sind über 60 Threat-Intelligence-Feeds in die Plattform eingebunden:
  - Bösartige URLs & IP-Adressen
  - Malware-Seiten
  - Phishing-Adressen
  - C2-Domänen und -Adressen
  - Ransomware-Auslieferungs-URLs und –Adressen
  - Kompromittierte Adressen und Server
  - TOR-Adressen
  - Spam-Absender
  - Zeus C2-Domänen und -Adressen

- Microsoft Threat Intelligence
- IBM Xforce
- STIX
- TAXII
- Quad9 (mnemonic, 360Netlab, Anti-Phishing Working Group, Bambenek Consulting, F-Secure, Hybrid Analysis, Proofpoint, RiskIQ, ThreatSTOP)
- cinsscore.com
- feodotracker.ause.ch
- hosts-file.net

- malc0de.com
- openphish.com
- osint.bambenekconsulting.com
- ransomwaretracker.abuse.ch
- reputation.alienvault.com
- rules.emergingthreats.net
- svn.code.sf.net
- torstatus.blutmagie.de
- blocklist.de

- dan.me.uk
- dshield.org
- joewein.net
- malwaredomainlist.com
- nothink.org
- talosintelligence.com
- zeustracker.abuse.ch
- … plus 40 more feeds

Obrela in Zahlen

OPERATIONAL METRICS 2023 (YTD)

6.1PB
Logs Collected & Analyzed*

299K
Devcies & Endpoints Monitored

12.3'
Actual Response Time**

1.3M
Triaged Alerts Managed

99,9%
Availability SLA

20+
Countries

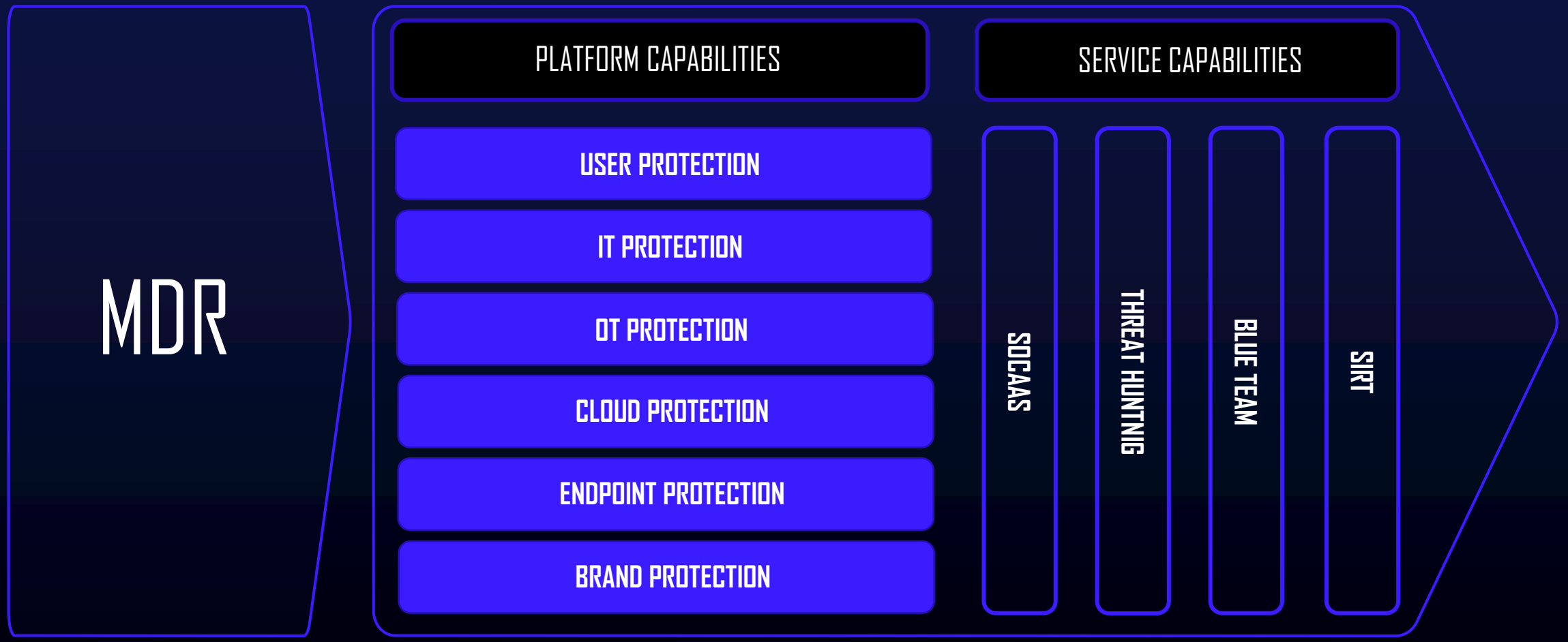
250+
Customers

250+
Employees

* 2023 FIGURES YEAR TO DATE

Obrela is recognised, again, in the 2023 Gartner® Market Guide for MDR Services.

MANAGED DETECTION AND RESPONSE



People, Process and Technology Integrated

PROCESS

Threat Hunting
- Kill Chain Analysis
- What-if Analysis
- Incident Discovery
- Threat Intelligence Mapping with Customer Environment

Threat Intelligence
- New Threats Discovery
- IOC Collection
- Targeted Intelligence
- Collective Intelligence
- Cyber Adversary Characterization

Risk Management
- Vulnerability
- Asset
- Incident
- Policy
- Vendor Security
- Privacy
- Compliance
- Reporting

Cyber Ops
- Rules of Engagement
- Case Management
- Intelligence Analysis
- 24/7/365 Monitoring
- Incident Response
- Client Onboarding

Platform & Content Management
- IR Playbooks
- Alert Management
- Continuous Improvement
- HardCore Content Development
- Integration & Connectors Development

PEOPLE

Service Management
- Service Delivery Manager

SOC Operations
- L1/L2 Analysts
- SOC Officers

Blue Team Support
- Threat Intelligence Experts
- Threat Detection & Response Experts

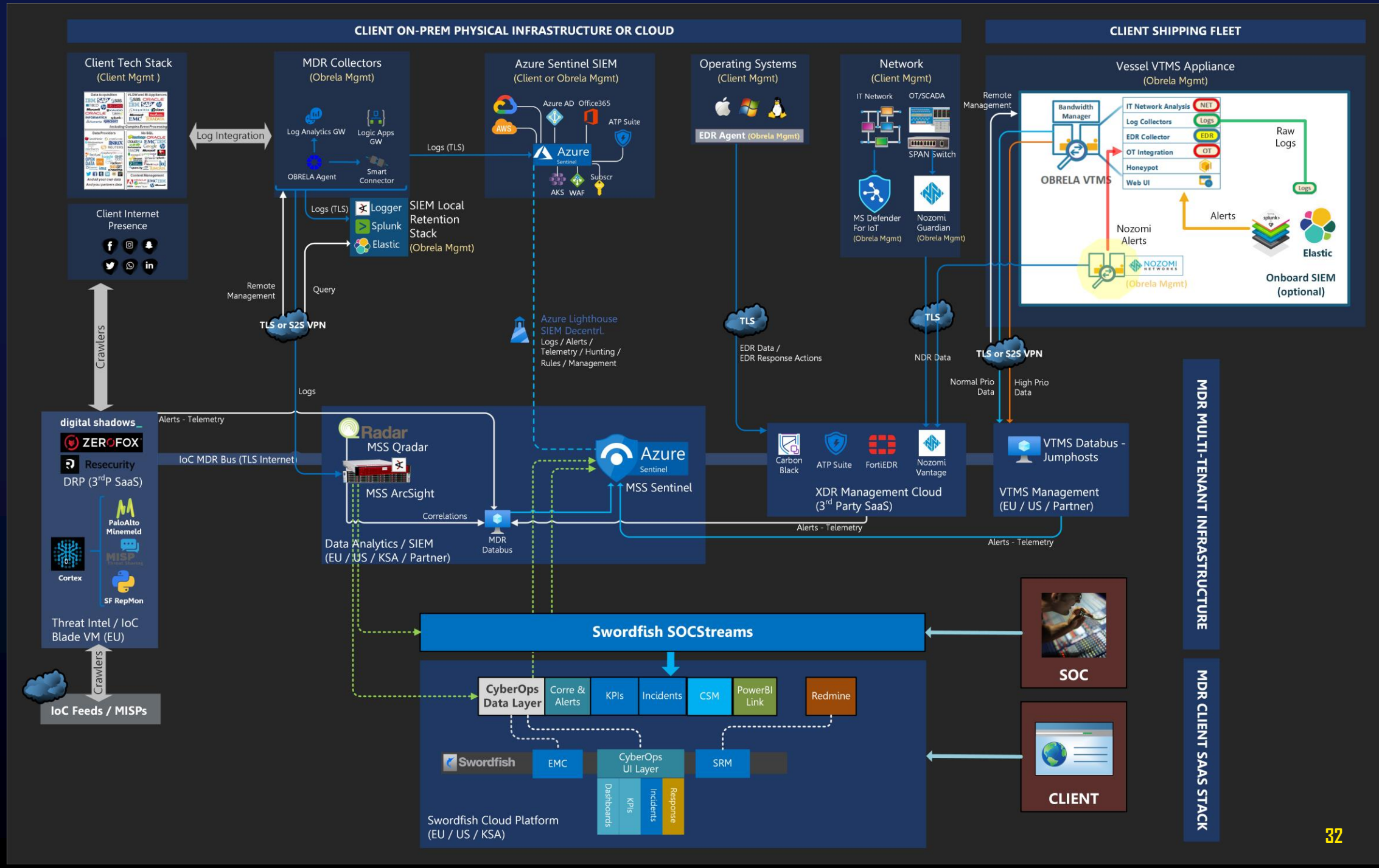
Threat Hunting & Incident Response
- Threat Hunters
- CSIRT

Devops
- Security Engineers
- Data Engineers
- Content Developers
- Network/System Engineers

Customer / Partner
- Customer Side Security Team
- Partner Security Team

SOCaaS

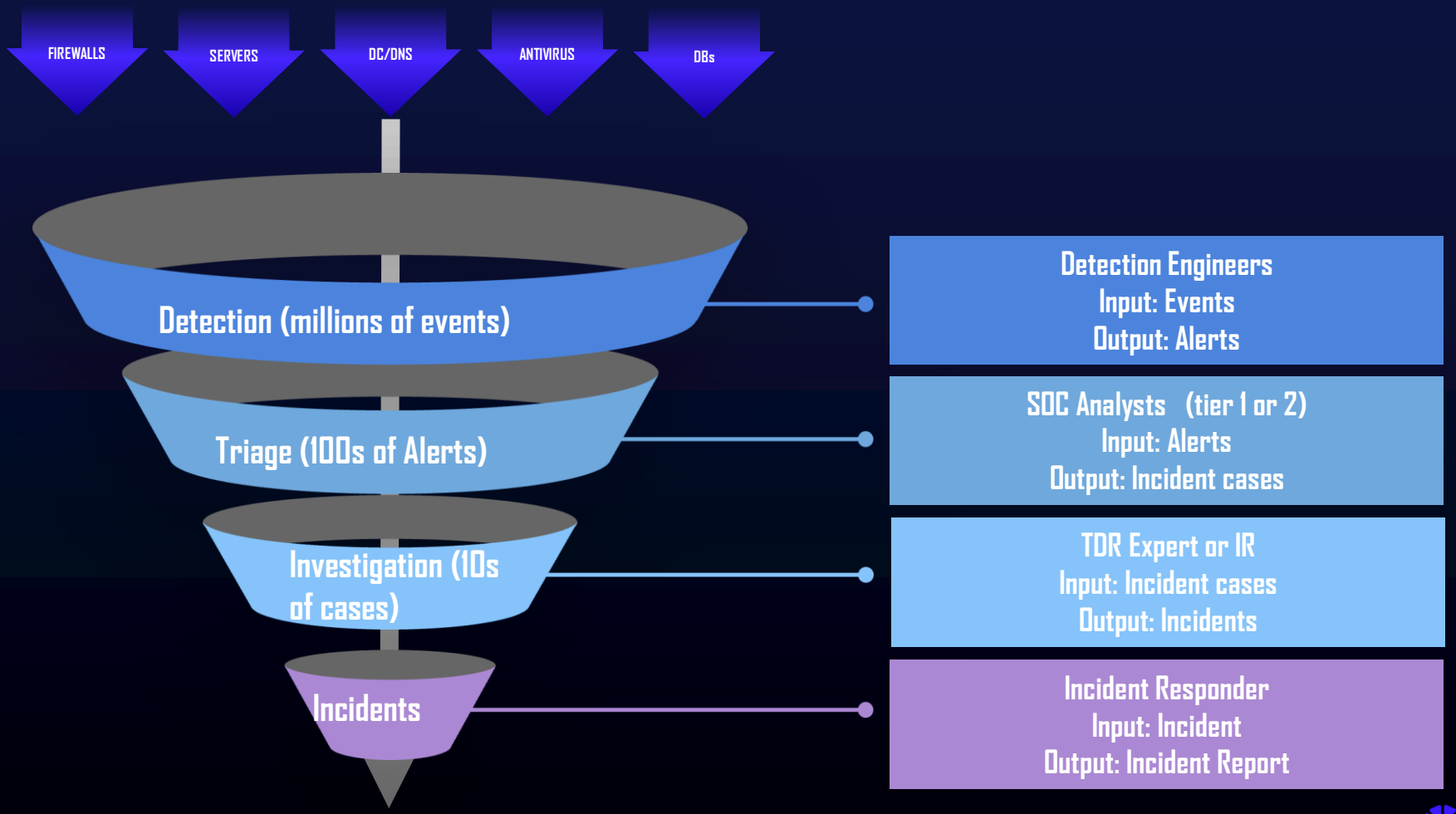
OBRELA


CLIENT ON-PREM PHYSICAL INFRASTRUCTURE OR CLOUD
CLIENT SHIPPING FLEET
Client Tech Stack
(Client Mgmt)
Log Integration
MDR Collectors
(Obrela Mgmt)
Log Analytics GW
Logic Apps GW
OBRELA Agent
Smart Connector
Logs (TLS)
Azure Sentinel SIEM
(Client or Obrela Mgmt)
Azure AD
Office365
ATP Suite
AWS
Azure Sentinel
AKS
WAF
Subscr
Operating Systems
(Client Mgmt)
EDR Agent (Obrela Mgmt)
Network
(Client Mgmt)
IT Network
OT/SCADA
SPAN Switch
MS Defender For IoT
(Obrela Mgmt)
Nozomi Guardian
(Obrela Mgmt)
Vessel VTMS Appliance
(Obrela Mgmt)
Remote Management
Bandwidth Manager
OBRELA VTMS
IT Network Analysis
Log Collectors
EDR Collector
OT Integration
Honeypot
Web UI
Raw Logs
Logs
Alerts
Nozomi Alerts
NOZOMI NETWORKS
(Obrela Mgmt)
Elastic
Onboard SIEM (optional)
Client Internet Presence
Logger
Splunk
Elastic
SIEM Local Retention Stack
(Obrela Mgmt)
Remote Management
Query
TLS or S2S VPN
Crawlers
Azure Lighthouse
SIEM Decentrl.
Logs / Alerts / Telemetry / Hunting / Rules / Management
TLS
EDR Data / EDR Response Actions
NDR Data
TLS or S2S VPN
Normal Prio Data
High Prio Data
Logs
digital shadows_
ZEROFOX
Resecurity
DRP (3rdP SaaS)
Alerts - Telemetry
IoC MDR Bus (TLS Internet)
Radar
MSS Qradar
MSS ArcSight
Azure Sentinel
MSS Sentinel
Correlations
MDR Databus
Data Analytics / SIEM
(EU / US / KSA / Partner)
Carbon Black
ATP Suite
FortiEDR
Nozomi Vantage
XDR Management Cloud
(3rd Party SaaS)
VTMS Databus - Jumphosts
VTMS Management
(EU / US / Partner)
Alerts - Telemetry
Alerts - Telemetry
PaloAlto Minemeld
MISP
Cortex
SF RepMon
Threat Intel / IoC Blade VM (EU)
Crawlers
IoC Feeds / MISPs
Swordfish SOCStreams
CyberOps Data Layer
Corre & Alerts
KPIs
Incidents
CSM
PowerBI Link
Redmine
Swordfish
EMC
CyberOps UI Layer
SRM
Dashboards
KPIs
Incidents
Response
Swordfish Cloud Platform
(EU / US / KSA)
SOC
CLIENT
MDR MULTI-TENANT INFRASTRUCTURE
MDR CLIENT SAAS STACK

CyberOps

- 360° security view across MDR subscriptions
- Issues classification and context review
- Investigation facilitation and intelligence
- Tailor made workflows based on your organizational structure
- Assisted escalation and monitoring
- Graphical and visual representation in real time
- Reporting and dashboards

Real Time Threat Management



Detection Engineers
Input: Events
Output: Alerts

SOC Analysts (tier 1 or 2)
Input: Alerts
Output: Incident cases

TDR Expert or IR
Input: Incident cases
Output: Incidents

Incident Responder
Input: Incident
Output: Incident Report

Risk Assessment factors

Incident categories

- Phishing
- Malware / Ransomware
- BruteForce
- DDoS / Availability
- Web attacks
- Zero Day Exploit / Vulnerability Exploit
- Lateral Movement
- Reconnaissance / Suspicious communication (TI)
- Policy Violation / Data Exfiltration
- OT Attack
- Brand Attack

Criticality

- Critical
- High
- Medium
- Low

Closing reason

- False Positive
- True Positive
- Benign (non-issue)

Investigation & Incident Response example

Pentest tools and Kali Linux download detected

Proxy traffic served as detection means.

Acknowledged & Action Initiated

The Customer and Obrela were in contact through Swordfish & Phone concerning the course of the incident

Further Analysis and Investigation

Identification of the network segment where the action took place, and the responsible user. Further investigation and containment actions (EDR).

Continuous communication and Investigation

CSIRT provided further threat eradication recommendations to the customer and provided root cause analysis report.

Case Closed

The case was closed with Obrela's summary report.

Blue Team Support

Blue Team Support

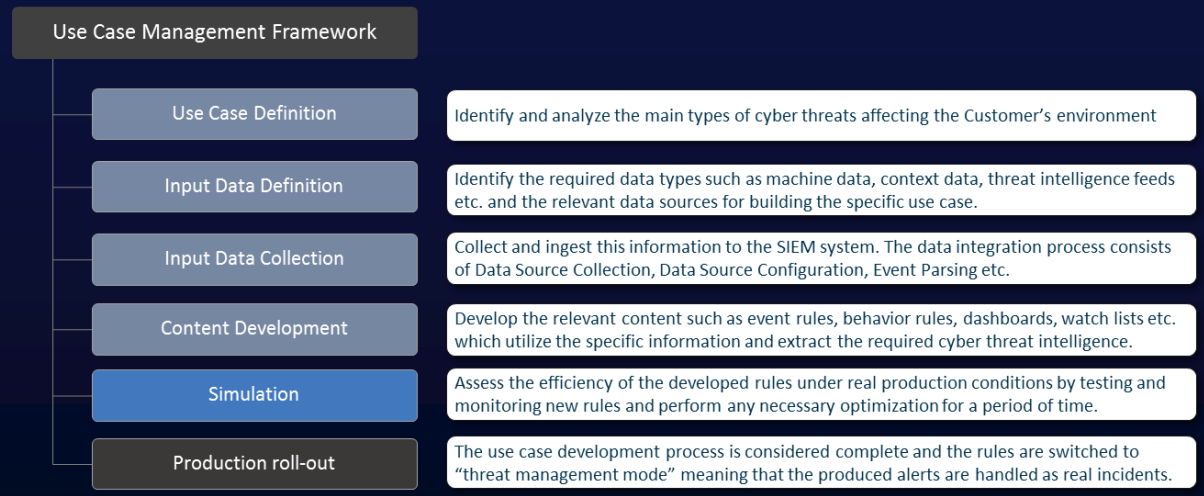
Goal-driven team of Threat Detection & Response experts who prepare for, simulate & hunt against any kind of cyber threat, by performing:

- Security Operations Support
  - Content management (use case management, incident case management, creation of customized dashboards, searches, design and implementation of playbooks, etc.)
  - Service Level Management
- Security Posture assessment
- Vulnerability Scanning / Vulnerability Management
- Advanced Content Development (identify and create additional custom use cases based on our Use Case Lifecycle Management framework)
- Training

Advanced Content Development

Blue team Support services deliver a vast library of optimized correlation rules and behavior analysis/profiling use cases including:

- Out of the box rules: This built-in ruleset is activated from day one to the Client and is further optimized using Client-focused false positive / false negative elimination techniques.
- Correlation rules: Use cases addressing current and past security threats and non-compliance issues are included.
- Industry/Infrastructure Specific Rules: to take advantage of threats and security implications that target specifically the former have been developed.
- Intelligence Services Rules: Integrate with the complete ecosystem of intelligence services, that bring external intelligence to the correlation engine in order to identify Advanced Persistent Threats, Data Leakage, configuration inconsistencies have been developed.
- Client-Based Rules: OBRELA's BlueTeam optimizes and develops new content for each Client based on new attack threats that are emerging but also based on Client detection and monitoring and use case requests.



Threat Hunting

Threat Hunting Team Overview

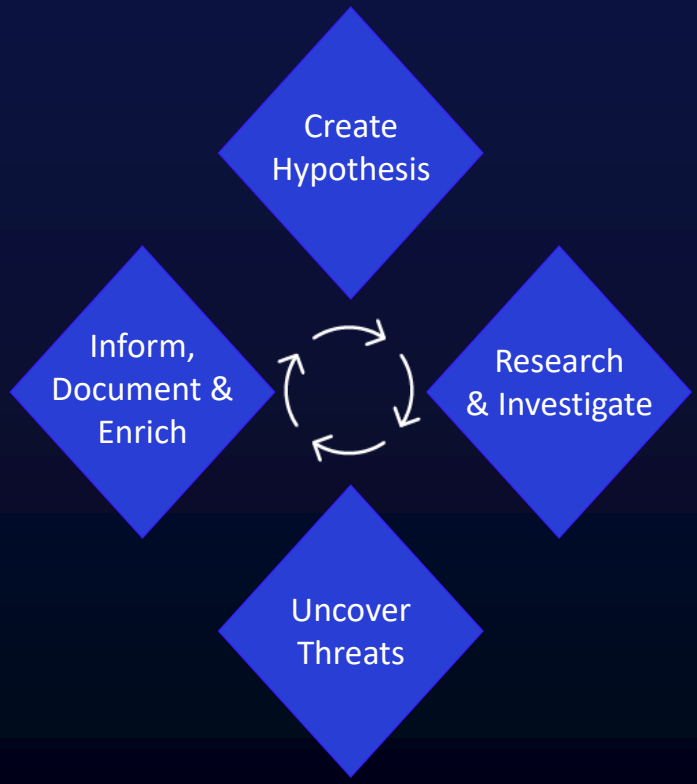
OBRELA's Threat Hunting team provides complete proactive and reactive hunts.

Threat hunting is the practice of searching activities for threats through networks, endpoints and systems that might remain undetected. This practice combines proactive methodologies and threat intelligence to find and stop malicious activities.

The Hunt Cycle Framework

Threat hunting is focused on advanced active searches in order to identify gaps in the organization infrastructure and security areas of further fine tuning and optimization of onboarded devices through the MDR service.

Threat hunts are organized through a cyclic system. Revolving between research and hunting for the duration of the hunt. This cycle continues until the hunt hypothesis is either proven or disproven.



Hunt Triggers

OBRELA's Threat Hunting framework focuses on proactive hypothesis-driven threat profiling and covers two functional streams of work:

1. Systemic based. Following a hypothetical approach, threat hunting cycles to systemically uncover and identify malicious activity or emerging IOCs that are in progress.
2. Mission Based. Following a reactive approach, threat hunting is actively engaged to "lock" attack behavior and malicious activity that has been reported from threat intelligence or the security operations.

There are many ways to trigger a hunt, the most common of which are as follows:

Lead-based

Start with a lead such as previous alerts or suspicious traffic.

Attack Lifecycle

Hunt for behaviors that are often seen during different stages of the Attack Lifecycle. E.g. Mitre ATT&CK framework

Internal

Focus on departments, users, or tools that are likely to be targets of an attack.

Emerging Threats

Search for evidence of attacks and techniques based on threat intelligence and trends.

Freestyle

Pick data at random to investigate, such as a single department or type of system.

Threat Hunting Requirements

Hunts can take advantage of all available platforms such as SIEMs, EDRs and NDRs.

Due to this, the quantity, quality and enrichment of data available to a hunter is of high importance.

Whilst hunts can be conducted with either SIEMs, EDRs and NDRs. The success and maturity of a hunt relies on data depth, with EDR/NDR platforms giving a hunter access to specific process or flow data which may be required to complete an investigation.

For example, an EDR solution would provide the hunter access to system artefacts such as files modified by a malicious process, which would be lost to a SIEM alone.

Each of these platforms provide an extra layer of detection and analytics which is taken into consideration when creating a hypothesis for a hunt.

Example Hunts

Hunt Trigger	Example Scenario
Lead based	Alert, Indicator of Compromise, Threat Intelligence – Traffic to IP relating to specific threat actor
Attack Cycle	MITRE ATT&CK – Common Persistence methods
Internal Investigation	Behaviors on machines or crown jewels, usage of programs etc
Emerging threats	COVID 19 phishing, Russian/Ukraine geopolitical conflict, new APT targets
Freestyle	Processes communicating with external IP addresses/domains

Incident Response (CSIRT)

Cyber Security Incident Response Team

OBRELA CSIRT provides complete Emergency Incident Response supporting all types of incidents from compromise of internal threats, BECs to full breach and ransomware. Incident response can be requested directly to CSIRT via the account manager or initiated through the MDR SOC service.

Scoping

Stakeholder interviews & scoping of IR engagement

Incident Triage

Identification & analysis of compromise

Remediation

Eradication of threats; Attack containment and root cause analysis

Follow-up

Recovery, reporting, recommendations, and post-incident security hardening

Cyber Security Incident Response Team

Emergency Incident Response

Emergency Incident Response

- Remote Incident Response
- Digital Forensic Analysis
- Malware Analysis and Reverse Engineering
- Initial Contact: Best Effort
- Incident Triage: Best Effort
- Pay-As-You-Go

IR Retainers

Basic

- Remote Incident Response
- Initial Contact & Incident Triage: 8 hours
- Predefined tiers
  - 40 hours
  - 100 hours
  - 200 hours
  - Custom

Advanced

- Incident Response, Remote and On-site (when necessary)
- Initial Contact & Incident Triage: 4 hours
- Bi-Annual Workshop
- Predefined tiers
  - 40 hours
  - 100 hours
  - 200 hours
  - Custom

Emergency SLAs*

Initial Contact & Triage	4 / 8 hours
Remote Support	4 / 8 hours
On-site Support	48 hours

** Depending on IR Retainer level*

IR Cross-Functional Expertise

Initial Contact

Understand & Expand Visibility
Within hours

Incident Triage, Analysis, Remediation

Full-Scale Emergency Incident Response & Recovery

Identify & Analyze

- Capturing Data
- Iterative Forensics & Threat Analysis
- Plan for Remediation

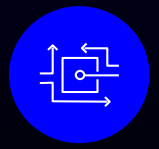
Remediate

- Containment
- Evict Threat Actor
- System and Data Recovery
- Monitor for threat actor re-entry

Follow-up

- Recovery and reporting
- Lessons learned and recommendations
- Security Hardening

Threat Intelligence Unit



Security Testing

Emergency IR Phases

Scoping, Initiation And Kick-off

- Initial call to identify scope and objectives
- Scope of engagement defined
- Kickoff after signing the IR SOW and Approval Form sent by the IR or Account team
- IR team resources assigned

Collection and Deployment

- Remote assistance provided to capture forensic data
- Deployment of engagement technology (endpoint, network)

Technical Analysis

- Based on available artifacts, the extent of compromise, attack vectors, and timeline of intrusion activity are iteratively captured and analyzed
- Threat eradication including root cause analysis
- Recurring status reports including facts, findings, recommendations, and action plans

Incident Follow-up

- Baseline reporting format is provided for technical and non-technical stakeholders
- Draft incident report delivered no later than three (3) weeks from the end of incident

Service Management

Service Governance

The MDR Service Governance typically includes regular performance review sessions, reporting through dashboards for the executive management and SOC officer, constant update of the HardCore content, operational updates regarding the SOC activities and technologies, weekly operations meetings, periodic use case review/design meetings and monthly service review meetings with the customers.

The typical topics to be constantly reviewed include:

- Open tickets and issues
- Preventable actions
- Threat intelligence updates
- Service delivery status
- Awareness, knowledge transfer & procedural updates
- Updates on assigned tasks incl. incidents, tickets closure, review of SOC processes/ playbooks etc.
- Uses cases management, activity tracking, development, and fine-tuning
- Log source management
- Security procedural runbook
- Incidents business impact
- Critical issues, findings, and recommendations
- Assistance to prepare for audit (internal, external etc).

Indicative Service KPI/metrics

- Platform components uptime and utilization (hourly)
- Number of events per second per log source and peak values (EPS monitoring and reporting)
- Number of total events over correlated ones (event reduction rate)
- Number of incidents per security analyst work hours
- Number of alerts per security analyst work hours
- Time spent on analysis per offense identified
- Number of alerts escalated
- False positives / month
- False positives trend/month
- Alerts/Incidents closed as per SLA based on severity
- Response time as per SLA based on severity
- Support tickets closed based on SLA
- Number of change requests
- Number of platform problem cases opened

Service Delivery Manager

The Service Delivery Manager (SDM) is Focused on Ensuring Success by Understanding Customer's Business Goals and Providing Guidance.

The designated Service Delivery Manager (SDM) will consult and help the Customer's security team achieve the greatest value from the Service. Each SDM has in-depth security knowledge and experience to keep the Customer informed and help navigate any threats uncovered in the environment but also handle any operational issues that may come up.

01

Provides Continuity Throughout Customer's Journey Lifecycle.

02

Maintains Proactive and Personal Communications to Drive Results with Our Software and Services.

03

Helps the Customer Achieve their Security Program Goals as They Manage and Mature Their Program.

OBRELA

THANK YOU

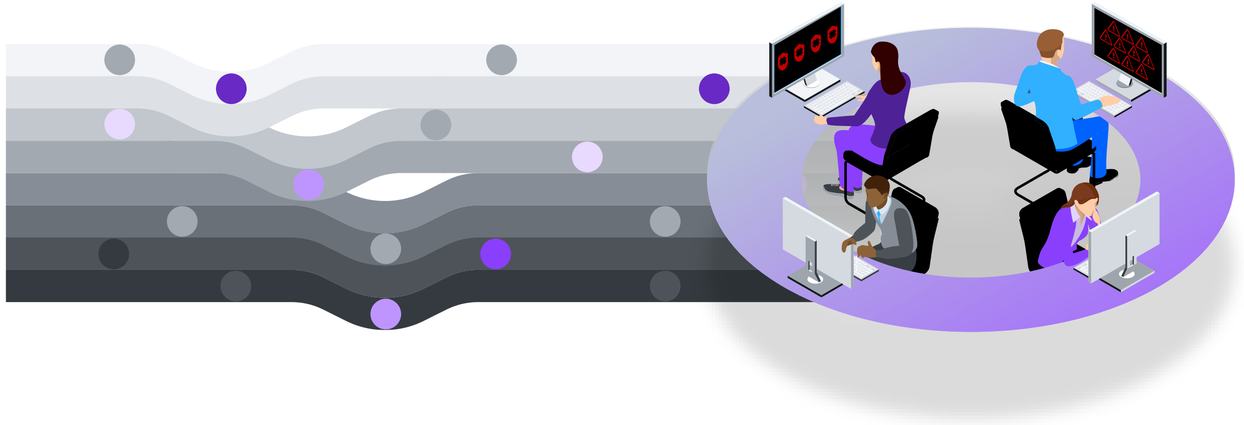
London | Athens | Dubai | Frankfurt | Riyadh

www.obrela.com

Modernized security operations

IBM **Security**

Security operations needs major improvement



The move to cloud and IT modernization has expanded the attack surface, creating increased security complexity

Poor visibility
2 out of 3 organizations' external attack surface has expanded in the last year[2]

Disconnected tools
80% of organizations use at least 10 disparate solutions to manage security hygiene[2]

Keeping up with attackers
29% of security operations processes are immature and need reengineering before they can be automated[1]

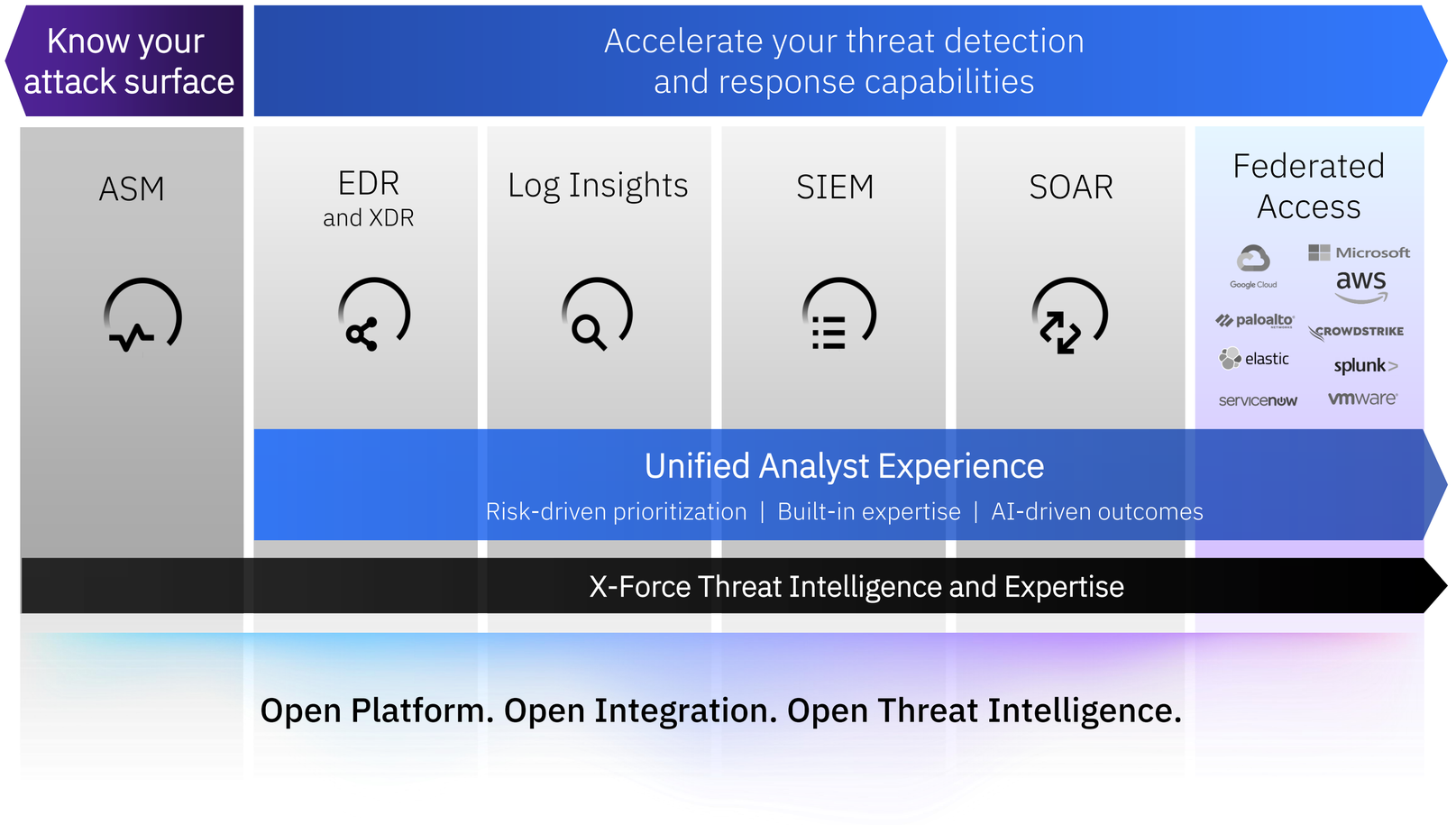
Information overload
52% of security environments have become more difficult to manage over the last two years[2]

51% of organizations struggle to detect and respond to advanced threats[1]

Current SecOps	Modernized SecOps
Technology focused	Analyst focused
Dependent on experts and heroes	Scale with expertise and AI
Proprietary ecosystems	Community collaboration

Modernize security operations with greater speed and visibility

The evolution of the IBM Security QRadar Suite



Designed around the analyst experience
Enable better decisions quickly using a common, streamlined, Unified Analyst Experience (UAX)

Gain accurate insights quickly
Streamline workflow with automation and AI designed for analysts, continuously updated threat X-Force threat detection and response expertise

Work with what you already have and expand to where you want to go
Built to meet you where you are using an open modular platform, standards, and ecosystem, with bi-directional integrations including federated search

Designed around the analyst experience

Enable better decisions quickly using a common set of Unified Analyst Experience (UAX) capabilities

Traditional Experience

8+ security UI's

30+ hours of tool training

2+ days of response time

Manual investigation

Unified Analyst Experience

1 common UX

Continuous learning

< 30-minute response time[1]

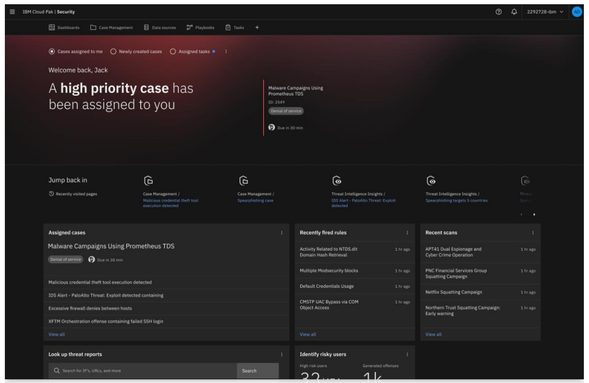
Automated investigation

– What?
– When?
– Where?
– Who?
– How?

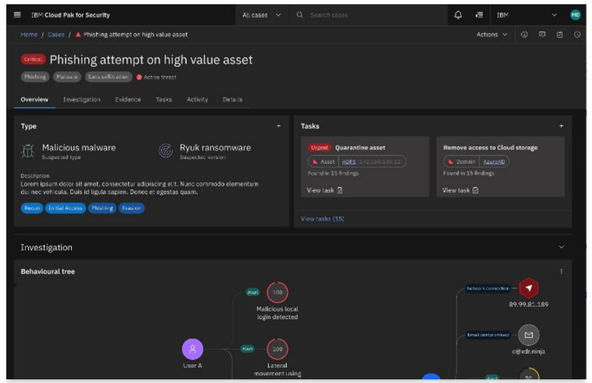
Take action

90%+ analyst time saved on investigating an incident[2]

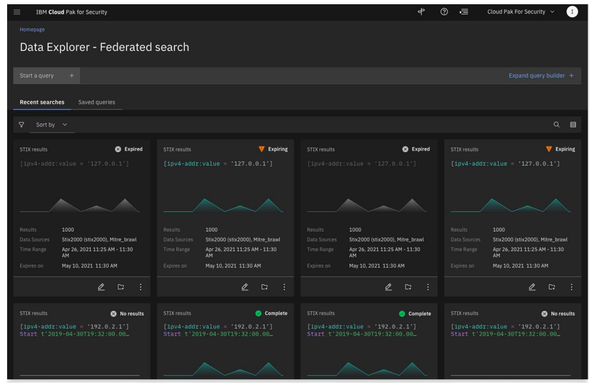
" I equate the UAX to five additional FTEs, it was easier to get better data out of my tools with AI, than investing in more people. It made my people faster and better at their job."[1]



Enrich, correlate, and prioritize



Automated investigation and response recommendations



Federated search and threat hunting

Work with what you already have and expand to where you want to go

An open approach with federated search gives you flexibility to access data where it is, or consolidate when necessary

3,000+ Open Sigma SIEM rules

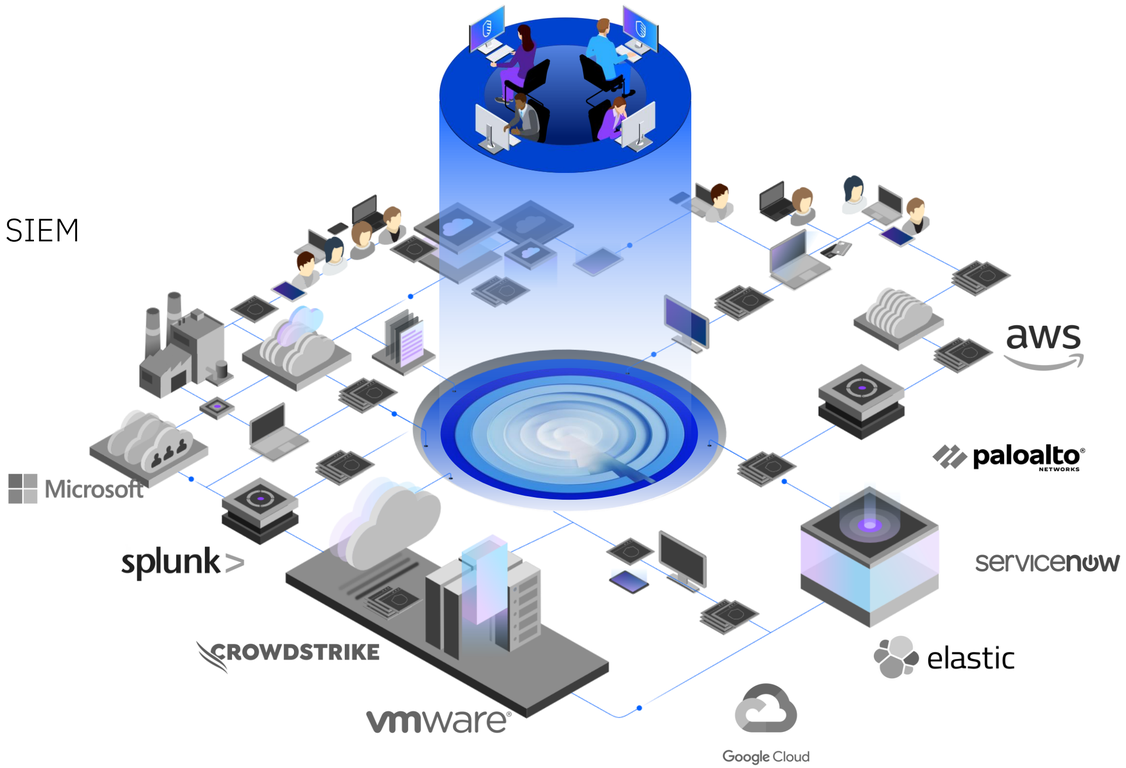
550+ Log adapters and apps for QRadar SIEM

300+ QRadar SOAR integrations

40+ Federated search sources

10+ Threat intelligence sources

150+ Open ecosystem vendors



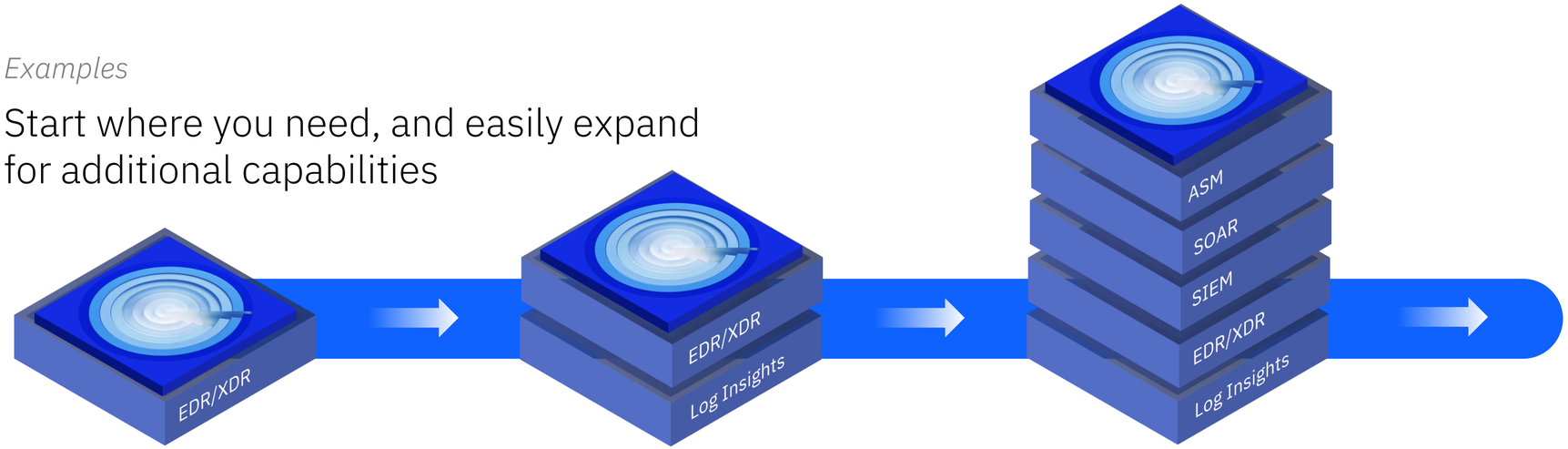
"QRadar can be deployed and quickly start working from day one."[1]

"The extensive information captured in QRadar provides insights and time savings for users beyond the security team."[2]

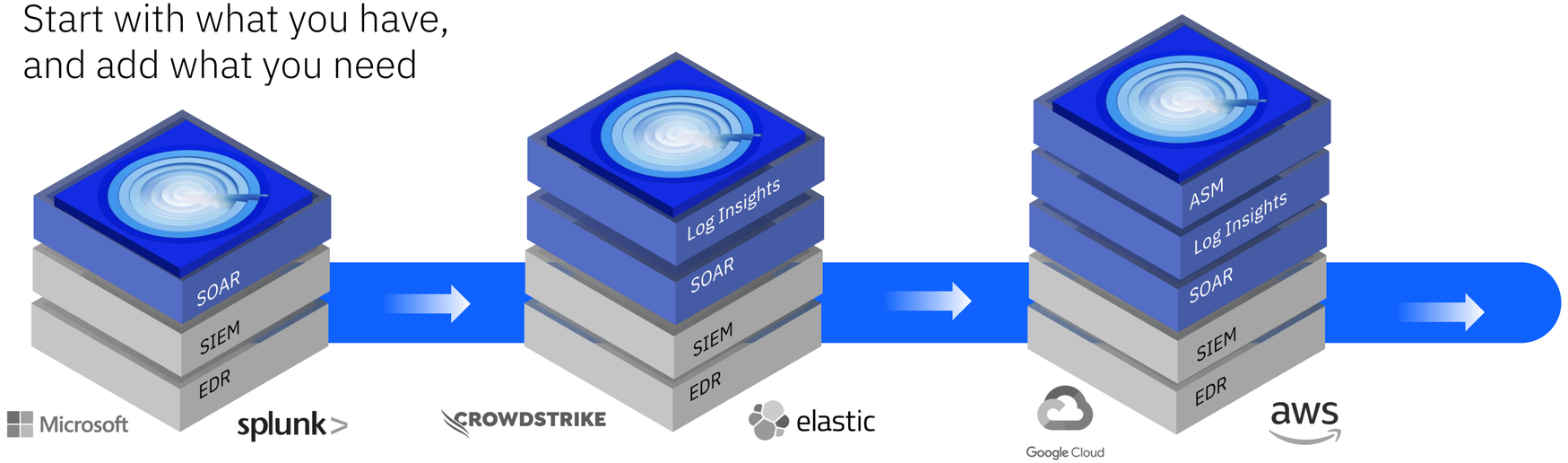
Accelerate your security, starting where you need to

Examples

Start where you need, and easily expand for additional capabilities



Start with what you have, and add what you need



- Wide set of integrations available to work with existing solutions to allow stepwise adoption
- Broader adoption of IBM solutions adds capabilities, context, insights and automation to the analyst experience with little incremental training or integrations
- Available as licensed software or SaaS

Thousands of open integrations at the center of your ecosystem

Open source and open community

OPEN CYBERSECURITY ALLIANCE

Open Cybersecurity Schema Framework

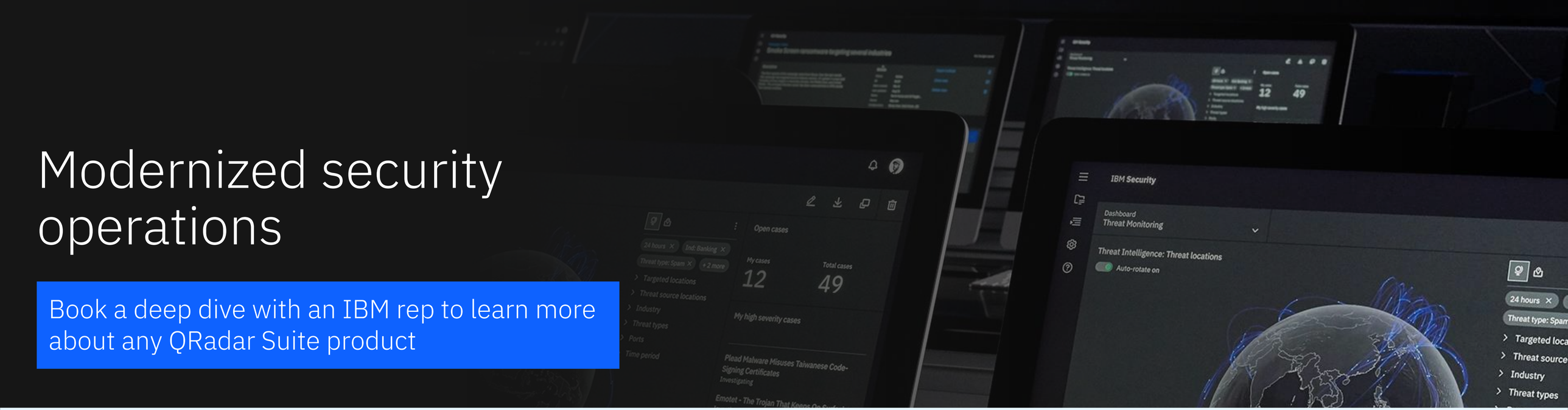
MITRE ATT&CK

fido ALLIANCE

quad9

Modernized security operations

Book a deep dive with an IBM rep to learn more about any QRadar Suite product



If you are experiencing cybersecurity issues or an incident, contact X-Force to help

US hotline 1-888-241-9812

Global hotline (+001) 312-212-8034

Schedule

A QRadar Suite Demo
Click here

Contact

An IBM Rep to schedule a QRadar Suite Demo

Schedule

A no-cost QRadar Value Assessment through your IBM Rep

DATA. INSIGHTS. ANSWERS.

graylog

GRAYLOG

Cybersecurity & Protokollierung

“Egal, womit man beginnt,

Protokollierung ist immer ein Thema…”

Regulierungswut?

- **ISO 27001** Annex A.12.4
- §76 **BDSG**
- Art. 33 **DSGVO**
- § 8 **BSIG** (Mindeststandard BSI)
- **KRITIS**
- Art. 56, **NIS2**
- **Telekommunikationsgesetz**, 3.7
- Krankenhauszusatzgesetz (**KHZG**)
- uvm...

Ein **altes**

Vorgehensmodell

01 Detektion

02 Reaktion

03 Prävention

Was zu schützen wäre

Daten

Identitäten

Motive...

NACH RANSOMWARE-ATTACKE

Hacker reichen Beschwerde bei der SEC ein

Ein Unternehmen aus den USA meldete einen Cyberangriff mehrere Tage nicht an die Behörden. Nun haben die Angreifer ein wenig nachgeholfen.

in Pocket speichern | merken

16. November 2023, 11:59 Uhr, Marc Stöckel

Daten von Polizisten in Nordirland aus Versehen freigegeben

09.08.2023, 12:34 Uhr

Die Lage für Polizisten in Nordirland bleibt gefährlich. Einige Beamte erwähnen ihre Arbeit nicht einmal innerhalb der eigenen Familie. Wegen eines gewaltigen Datenleaks könnten nun viele gefährdet sein.

Neue Zürcher Zeitung

Russland schaltet mit einem Hackerangriff in der Ukraine den Strom aus. Gefährlich ist das neuartige Vorgehen – auch für den Westen

Ein neuer Bericht zeigt, wie russische Angreifer viel rascher als früher die ukrainische Stromversorgung sabotieren konnten.

Nordrhein-Westfalen

Cyberangriff auf Südwestfalen IT: Noch mehr Kommunen betroffen

Stand: 16.11.2023 17:01 Uhr

Bis zu 103 Kommunen seien laut Siegens Bürgermeister Steffen Mues vom Cyberangriff auf die Südwestfalen IT in Hemer betroffen - rund 30 mehr als bisher angenommen. Die Verwaltungen in den Kreisen Siegen-Wittgenstein und Olpe seien am stärksten betroffen.

…und Zielsetzung

Auskunftsfähigkeit

Angriffserkennung

Ein kreativer Job?

- Verschiedenste Vorgaben und Empfehlungen für Protokollierung sind vorhanden
- Ein Ausgleich zwischen Datenerhebung und Datenschutz muss gefunden werden
- Organisationen und Prozesse müssen den neuen Herausforderungen angepasst werden

Ein kreativer Job?

- Detektion, Reaktion und Prävention: Wie genau ist die eigene IT bekannt?
- Welche spezifischen Faktoren können zur Detektion beitragen, was sind relevante Use Cases?
- Wie viele Personen werden für diese Aufgaben zusätzlich benötigt?
- **Wo fange ich an?**

Bundesamt für Sicherheit in der Informationstechnik

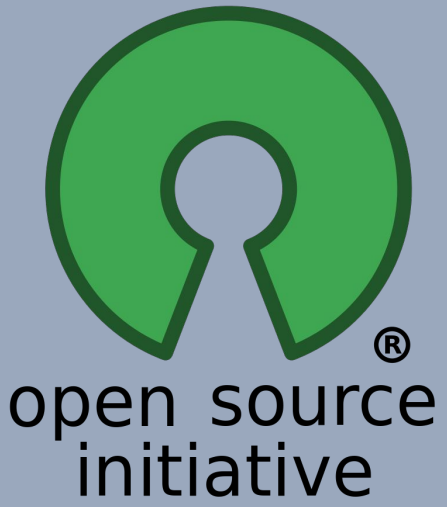
Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen

Iterativ ans Ziel

- Sensibilisieren der Mitarbeiter für Protokollierung / Detektion
- Priorisieren: Quick-Wins in der Protokollierung berücksichtigen
- Zentralisieren der Protokollierungsdaten zur Herstellung der Auskunftsfähigkeit und Detektion

Iterativ ans Ziel

- Absichern, ggf. Abschotten der Protokollierungssyteme
- Normalisieren von Protokolldaten entscheidet über Verwendbarkeit - offene Formate verwenden
- Standardisierte Methodik zum Einsatz von Detektoren - offene Formate verwenden

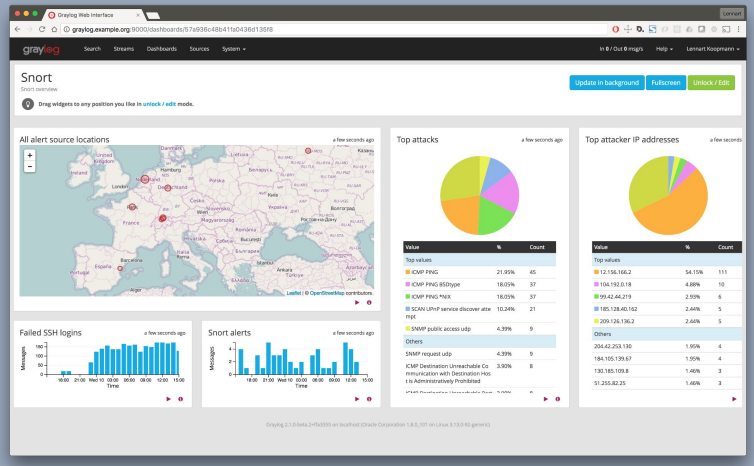


Iterativ ans Ziel

- Bekannte Schwachstelleninformationen mit den Protokolldaten abgleichen - offene Formate verwenden
- Identitäten, Systeme und Daten nach Schutzbedarf klassifizieren und überwachen
- Prozesse und organisatorische Maßnahmen etablieren

Iterativ ans Ziel

- Erste Erfahrungen mit zentraler Protokollierung zu sinnvollen Kosten - Opensource
- Erweiterung und Produktauswahl für eine langfristige Strategie auf Basis eigener Erfahrungen



Friedrich von Jagwitz
fvj@graylog.com

graylog

Graylog Open Source: https://graylog.org/products/source-available/

Dankeschön

corelight

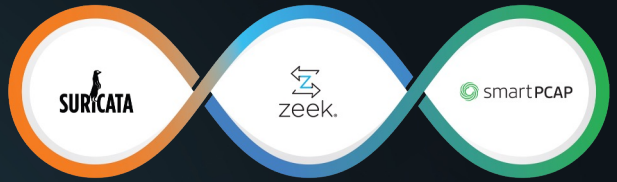
Richard Wieneke- Regional Sales Director
Timo Jobst - Systems Engineer

NETWORK DETECTION AND RESPONSE

Open NDR Platform I on premise - Cloud - SaaS

WHY CORELIGHT

- Industry's fastest growing network and detection response company.
- Founders and maintainers of open source Zeek, the world's most widely deployed network security monitoring tool with over 10,000 deployments.
- Deployed by large enterprises across finance, healthcare, tech, IT/OT as well as government agencies - at scales of up to 1 Tbps.
- Dedicated Technical Account Manager (TAM) and industry recognized customer support/success
- Tool of choice for elite defenders:
    - Only NDR vendor used by CrowdStrike and Mandiant IR teams.
    - Embedded technology in Microsoft Defender Endpoints.
    - Used in both the BlackHat NOC and Splunk's Boss of the SOC.

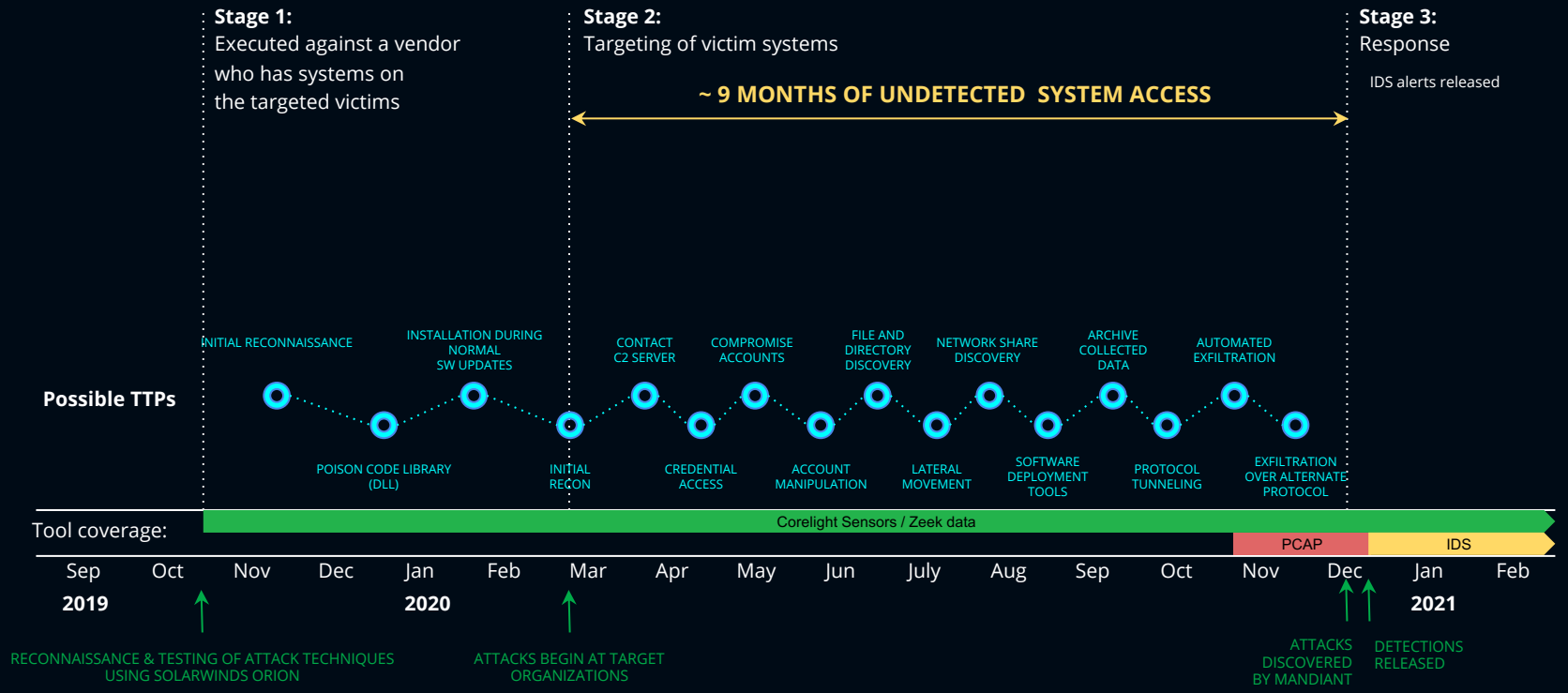


2023 CRN Top 100 Security Vendor
2023 CRN Top 20 Coolest Security Companies
2023 Enterprise Security Tech Winner
2023 Cyber Security Tech Winner
2023 Global InfoSec NDR Category Winner
2023 Forrester Strong Performer (NAV WAVE)

corelight

SUNBURST was the wake-up call for all SOC team

solarwinds

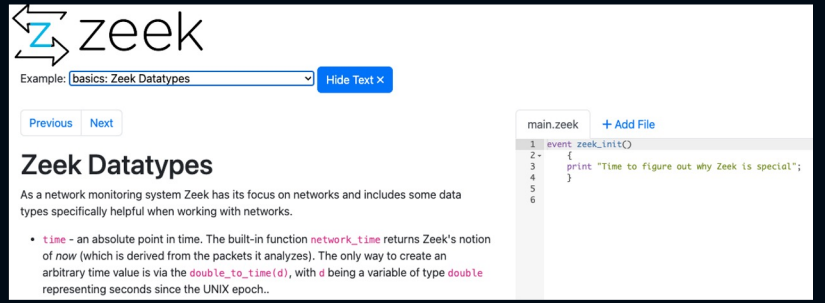


corelight

Threat Hunting with zeek also known as “Bro”

Zeek has a long history in the open source and digital security worlds. Vern Paxson began developing the project in the 1990s under the name “Bro” as a means to understand what was happening on his university and national laboratory networks. Vern and the project’s leadership team renamed Bro to Zeek in late 2018 to celebrate its expansion and continued development.

- 60+ log files provided by default
- 3,000+ underlying network events tracked
- 10,000+ deployments worldwide
- 5,500+ GitHub stars
- 20+ years of federally-funded R&D
- 240+ community-contributed packages



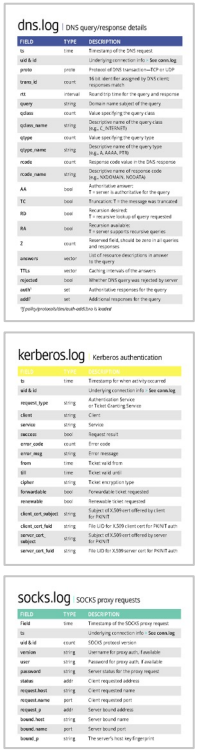
https://try.zeek.org

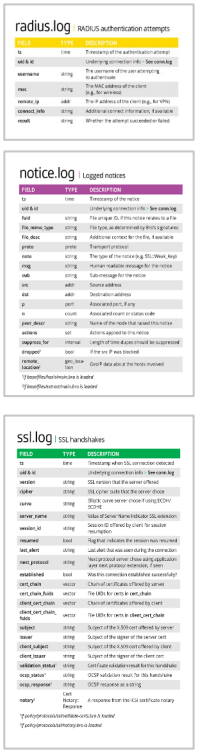
corelight

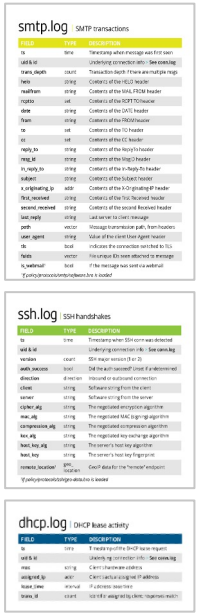
Zeek outputs dozens of logs, hundreds of data elements

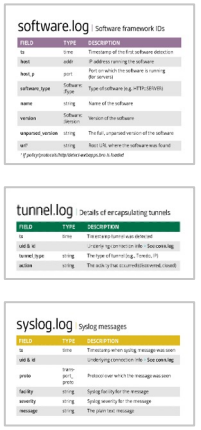
conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoint addresses
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see **conn.log** > **conn_state**)
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missing (packet loss)
history	string	Connection state history (see **conn.log** > **history**)
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)
tunnel_parents	table	If tunneled, connection UID of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of originator
resp_l2_addr	string	Link-layer address of responder
vlan	int	Outer VLAN for connection
inner_vlan	int	Inner VLAN for connection



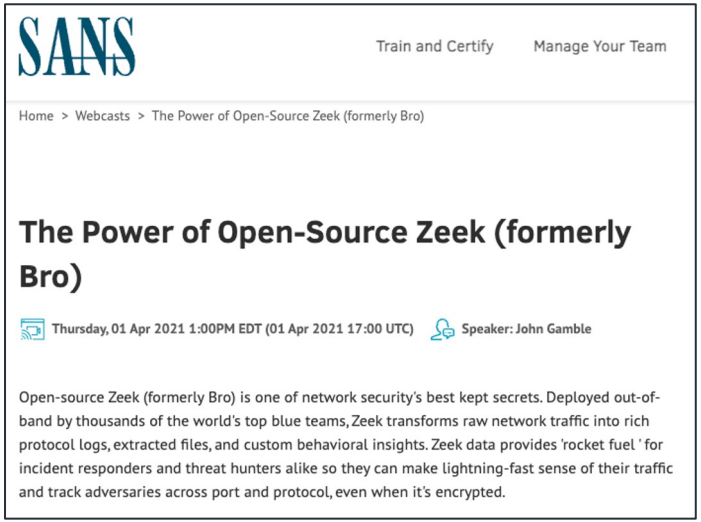






corelight

Zeek provides the best Network Metadata for Elite Defender



SANS

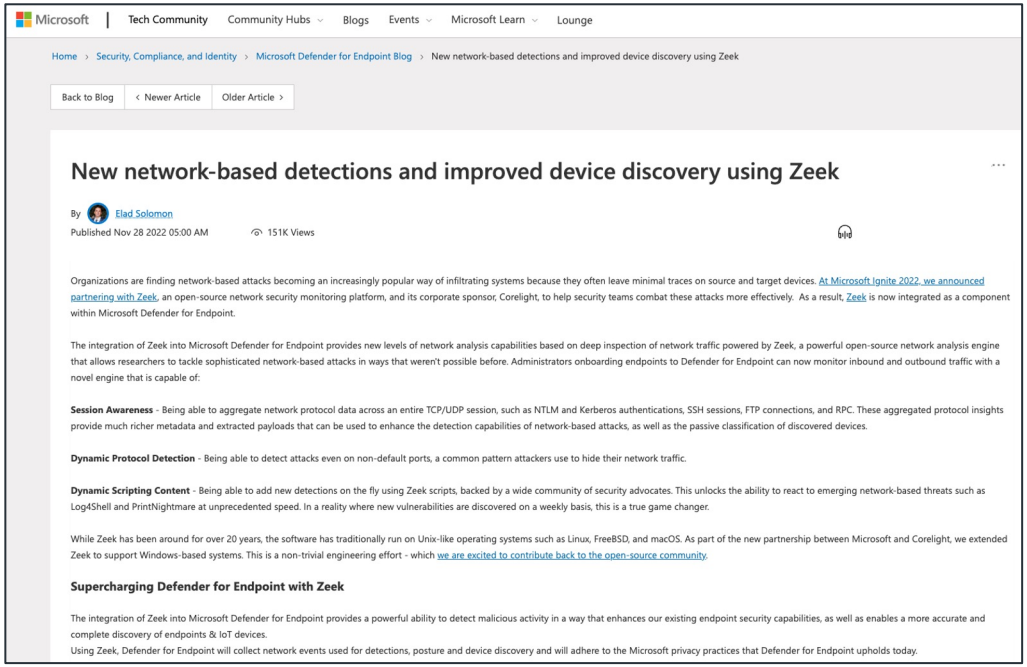
Train and Certify Manage Your Team

Home > Webcasts > The Power of Open-Source Zeek (formerly Bro)

The Power of Open-Source Zeek (formerly Bro)

Thursday, 01 Apr 2021 1:00PM EDT (01 Apr 2021 17:00 UTC) Speaker: John Gamble

Open-source Zeek (formerly Bro) is one of network security's best kept secrets. Deployed out-of-band by thousands of the world's top blue teams, Zeek transforms raw network traffic into rich protocol logs, extracted files, and custom behavioral insights. Zeek data provides 'rocket fuel ' for incident responders and threat hunters alike so they can make lightning-fast sense of their traffic and track adversaries across port and protocol, even when it's encrypted.



Microsoft | Tech Community Community Hubs Blogs Events Microsoft Learn Lounge

Home > Security, Compliance, and Identity > Microsoft Defender for Endpoint Blog > New network-based detections and improved device discovery using Zeek

Back to Blog < Newer Article Older Article >

New network-based detections and improved device discovery using Zeek

By Elad Solomon
Published Nov 28 2022 05:00 AM 151K Views

Organizations are finding network-based attacks becoming an increasingly popular way of infiltrating systems because they often leave minimal traces on source and target devices. At Microsoft Ignite 2022, we announced partnering with Zeek, an open-source network security monitoring platform, and its corporate sponsor, Corelight, to help security teams combat these attacks more effectively. As a result, Zeek is now integrated as a component within Microsoft Defender for Endpoint.

The integration of Zeek into Microsoft Defender for Endpoint provides new levels of network analysis capabilities based on deep inspection of network traffic powered by Zeek, a powerful open-source network analysis engine that allows researchers to tackle sophisticated network-based attacks in ways that weren't possible before. Administrators onboarding endpoints to Defender for Endpoint can now monitor inbound and outbound traffic with a novel engine that is capable of:

Session Awareness - Being able to aggregate network protocol data across an entire TCP/UDP session, such as NTLM and Kerberos authentications, SSH sessions, FTP connections, and RPC. These aggregated protocol insights provide much richer metadata and extracted payloads that can be used to enhance the detection capabilities of network-based attacks, as well as the passive classification of discovered devices.

Dynamic Protocol Detection - Being able to detect attacks even on non-default ports, a common pattern attackers use to hide their network traffic.

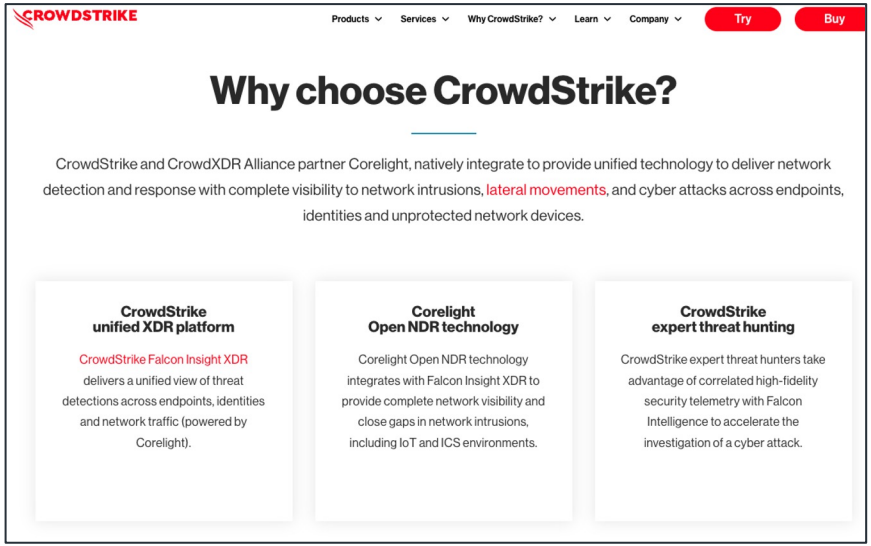
Dynamic Scripting Content - Being able to add new detections on the fly using Zeek scripts, backed by a wide community of security advocates. This unlocks the ability to react to emerging network-based threats such as Log4Shell and PrintNightmare at unprecedented speed. In a reality where new vulnerabilities are discovered on a weekly basis, this is a true game changer.

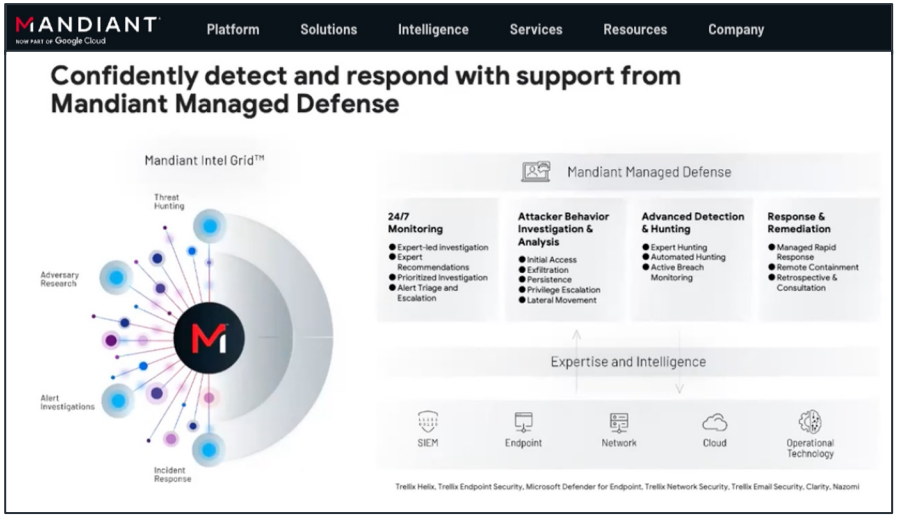
While Zeek has been around for over 20 years, the software has traditionally run on Unix-like operating systems such as Linux, FreeBSD, and macOS. As part of the new partnership between Microsoft and Corelight, we extended Zeek to support Windows-based systems. This is a non-trivial engineering effort - which we are excited to contribute back to the open-source community.

Supercharging Defender for Endpoint with Zeek

The integration of Zeek into Microsoft Defender for Endpoint provides a powerful ability to detect malicious activity in a way that enhances our existing endpoint security capabilities, as well as enables a more accurate and complete discovery of endpoints & IoT devices.
Using Zeek, Defender for Endpoint will collect network events used for detections, posture and device discovery and will adhere to the Microsoft privacy practices that Defender for Endpoint upholds today.

The best Incident Response Teams using Corelight





"I'm excited to support our strengthened partnership with Corelight," said **Marshall Heilman, CTO of Mandiant**. "Corelight's products are based on battle-tested open source technology deployed in some of the world's most critical environments. Their detection and network analytics capabilities will enable our Managed Defense and Incident Response businesses to identify and resolve incidents faster and more accurately. In addition, Corelight's integration across our Chronicle SecOps suite helps our customers maximize the value from our mission-focused organizations, with the incorporation of streamlined detections and solutions that are budget friendly for organizations of all sizes."

ELITE DEFENDERS LEVERAGE OUR PLATFORM

OPEN NDR PLATFORM

Transform network and cloud telemetry to detect suspicious behaviors and disrupt future attacks.

Complete platform includes:

- AI/ML workflow automation
- Intrusion detection
- Network security monitoring
- Packet Capture

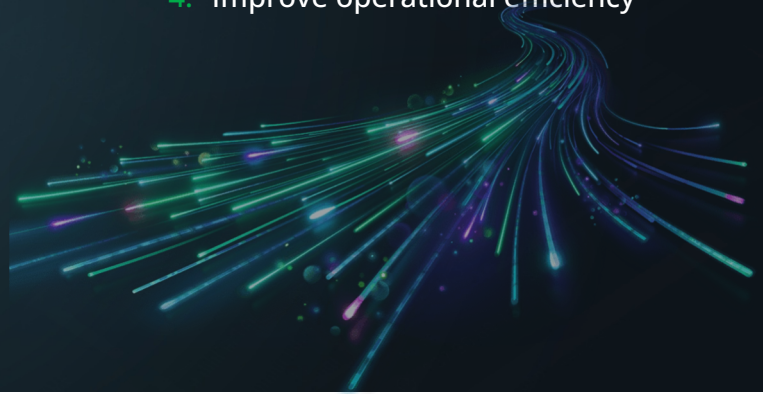
Available on-prem, in the cloud or via SaaS.

TOP USE CASES

1. MITRE coverage and detection initiatives
2. Tech stack modernization and consolidation
3. SOC automation + efficiency
4. XDR/SOC triad strategy implementation
5. Zero Trust + Compliance monitoring

TOP CUSTOMER OUTCOMES

1. Accelerate Incident Response
2. Improve detection coverage and accuracy
3. Expand network + cloud visibility
4. Improve operational efficiency



Centralized alerting and intelligence

corelight

THE CORELIGHT OPEN NDR PLATFORM

AUTOMATION

- AI-assisted investigation
- Alert tuning and triage
- 1-click pivots from alerts to logs to files to PCAP
- Alert aggregation, including IDS
- Integrated with existing SOC tooling and workflows

ANALYTICS

- Machine learning, behavioral models, signatures and queries
- 75 MITRE ATT&CK TTPs across Recon, C2, lateral movement, exfil
- Attacker tooling and technique detections

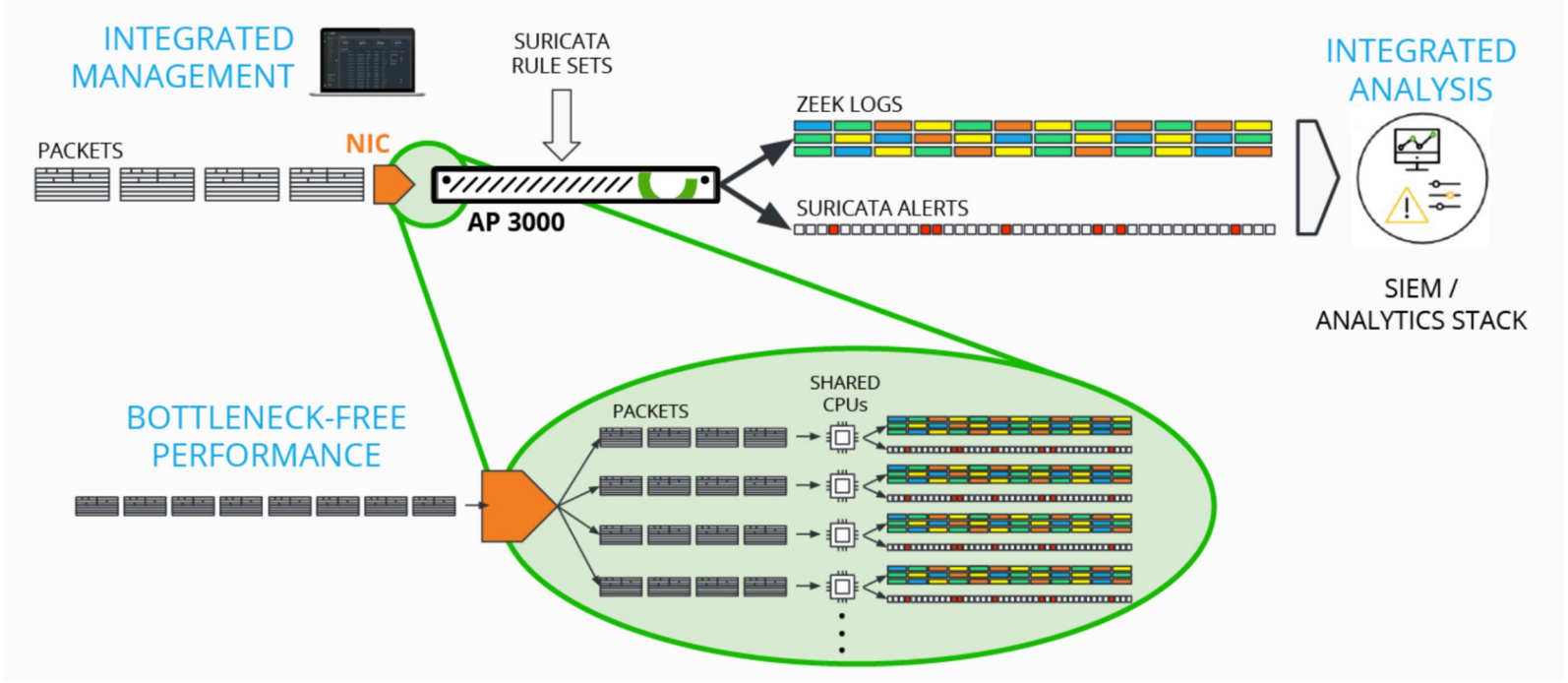
EVIDENCE

- Interlinked data for a single of truth across port and protocol
- 100s of unique insights for encrypted traffic, applications and entities
- Compact format allows for storage of months and years worth of date
- Single architecture delivers NSM, IDS and PCAP functionality

SENSORS

- Monitor low speed to high-speed (100 Gbps) with a 1U Sensor
- Centralized sensor management
- Virtual, cloud and physical sensors provide complete coverage

Corelight natively integrates



corelight

Collections: Behavioral analytics, detections and insights

corelight

CORE

Log enrichment, additional detections, and data reduction capabilities

ENCRYPTED TRAFFIC

Insights into encrypted traffic

C2

Detections of command and control activity

ENTITY

Identify, detect, and aggregate entity information

+

ZEEK COMMUNITY

zeek

Third party Zeek package support

+

CUSTOM SCRIPTS

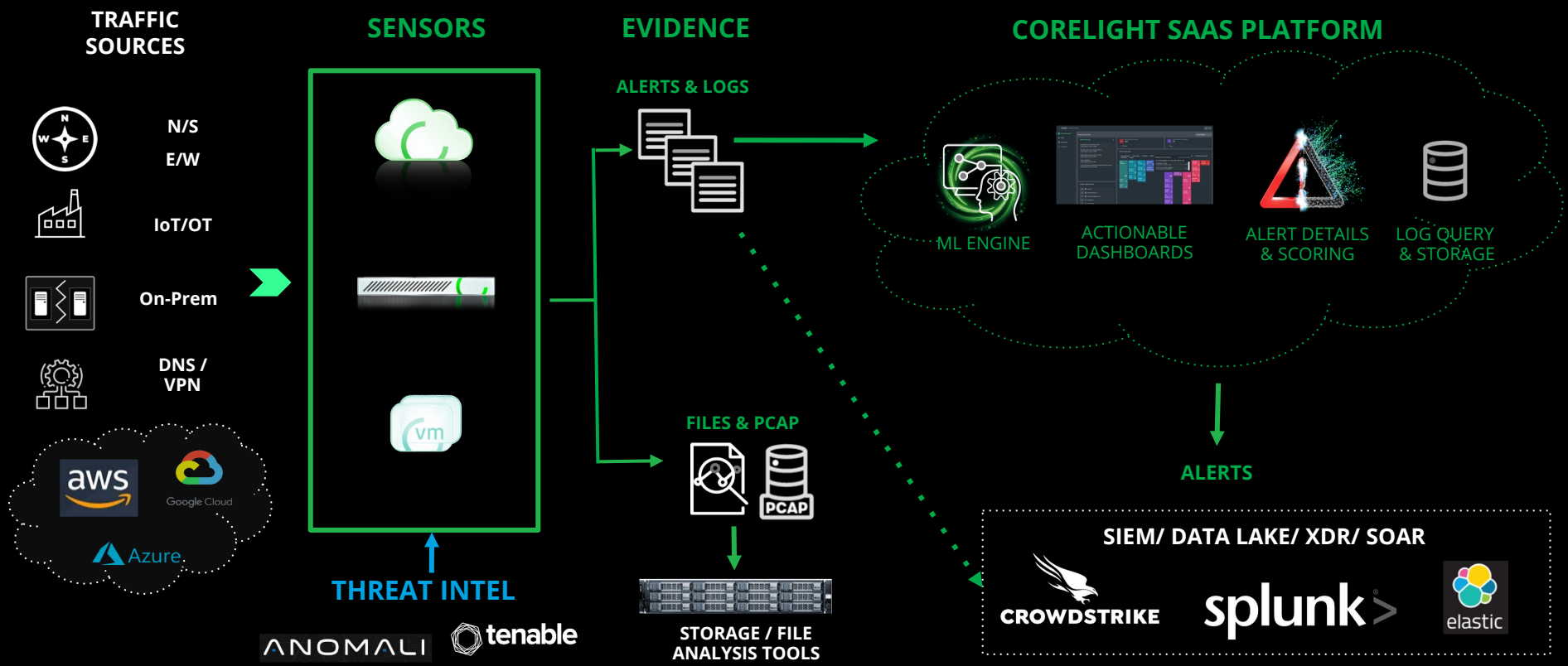
Full support for the Zeek scripting language

Extending visibility through our new ICS/OT collection

- BACnet: Protocol for building automation and control systems
- DNP3: Protocol for utility industry control system communication
- Ethercat: High-speed industrial Ethernet protocol for real-time control
- Ethernet/IP and CIP: Protocols for industrial automation and device integration
- Modbus: Widely used protocol for serial communication between devices
- PROFINET: Ethernet-based protocol for industrial automation and process control
- S7Comm: Siemens' protocol for communication with S7 programmable logic controllers
- TDS: Tabular Data Stream, a protocol used by Microsoft SQL Server for database communication

https://corelight.com/blog/extending-visibility-with-new-ics-ot-collection

CORELIGHT OPEN NDR | DEPLOYMENT MODELS



OPEN NDR PLATFORM CONSUMPTION

Corelight is the only NDR provider to support all three major SOC architectures

I consume evidence and detections directly into my SIEM, Data lake or XDR where I've built the workflows I need

ADVANCED SOC FOCUS

- Deploy on-prem and in cloud to scale up in minutes.
- Focus on evidence, not instances.
- Built-in detection, monitoring, and enrichment.

I need the ability to add, tune, and triage advanced detections but will do full investigations in my SIEM/xDR

DETECTION FOCUS

- Leverage your SIEM as primary investigation tool and data repository.
- Leverage SaaS to add advanced analytics and tunability

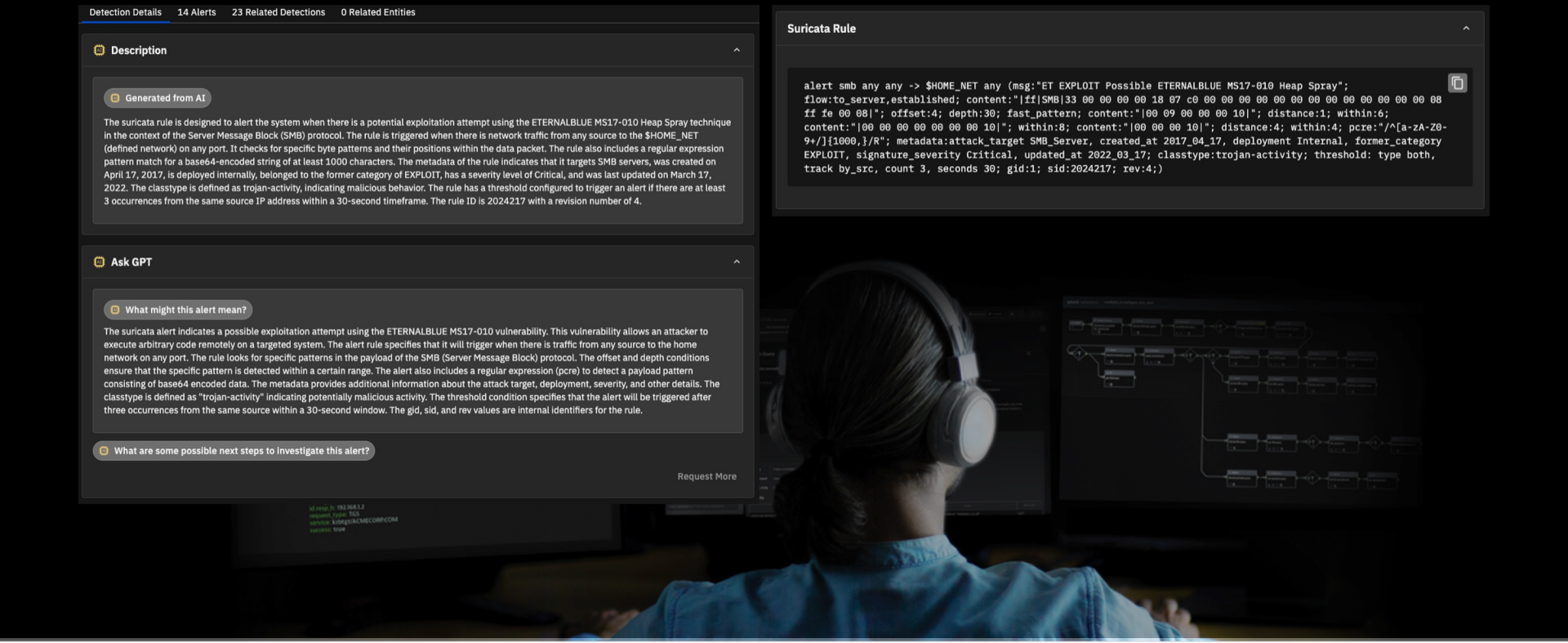
I need a dedicated product for network-centric analysis, threat hunting and investigation.

SIEM COST FOCUS

- Complete visibility, detections, in the Open NDR UI
- Leverage our platform data repository to lower SIEM cost and complexity

Full data export and a range of IR workflows across all SOC architectures

AI-assisted (OpenAI's GPT-4) triage for alert context and explainability



corelight

CORELIGHT TECHNOLOGY PARTNER ECOSYSTEM

SIEM/SOAR/XDR

elastic splunk> paloalto NETWORKS
snowflake RAPID7 Chronicle
Microsoft CROWDSTRIKE
exabeam DEVO
SWIMLANE Secureworks

CLOUD + VIRTUALIZATION

vmware Azure
kubernetes aws docker Google Cloud

PACKET BROKERS + TAPS

cpacket NETWORKS endace KEYSIGHT
ARISTA CUBRO NETWORK VISIBILITY Gigamon

THREAT INTEL

MISP TALOS ANOMALI
proofpoint. Recorded Future

SASE/SSE

paloalto NETWORKS netskope

VULNERABILITY MANAGEMENT

RAPID7 tenable Qualys.

MALWARE ANALYSIS

paloalto NETWORKS FORTINET VIRUSTOTAL
CROWDSTRIKE Microsoft

COMMUNITY

zeek. SURICATA MITRE ATT&CK. WIRESHARK SIGMA
jupyter kafka amazon salesforce

CAPABILITIES THAT DRIVE BUSINESS OUTCOMES

Expand Visibility	**Network coverage** **Duration / Time**	• Ground truth evidence from 25 years of elite defender IR • Compact, interlinked data for broad network coverage • Asset discovery, app identification, ICS / IoT insight
Improve Detection Coverage	**MITRE coverage** **Alert volume**	• Broadest range of detection capabilities: ML, behavioral, signature, queries and threat intel • Continuously updated content • Unique insights on encrypted traffic
Accelerate Incident Response	**MTTR** **Case closure rate**	• Only vendor powered by generative AI • Tie alerts to rich evidence history to accelerate response • Fast, chainable search to discover the entire kill chain
Reduce Operational Cost	**Direct cost** **Talent / turnover**	• Only complete visibility solution: metadata + files + IDS + PCAP • Only vendor supporting all three analytic architectures (XDR, SOC Triad, Datalake) • Only vendor with pooled license model

KEY NDR SELECTION CRITERIA

- Single-sensor architecture
- Open core evidence & alert standard
- Configurable Selective PCAP
- File extraction capabilities
- Encrypted threat detection
- SIEM/XDR data export controls
- Pooled capacity-based licensing
- AI-assisted IR workflows
- Machine learning model transparency

Gartner

*"**Security and risk assessment leaders should prioritize NDR** as complementary to their detection tools, focusing on **low false positive rates** and **detection of anomalies** that other controls don't cover"*

- Gartner Market Guide for Network Detection and Response

Follow design principles of Elite Defenders using Corelight Open NDR

Corelight DACH Team

richard.wieneke@corelight.com
timo.jobst@corelight.com

Cyber Defense Services

SOC 2.0 – Wie unser Controlware SOC Sie mittels EDR/XDR wirklich vor Cyber Gefahren schützt!

Christian Bohr, christian.bohr@controlware.de

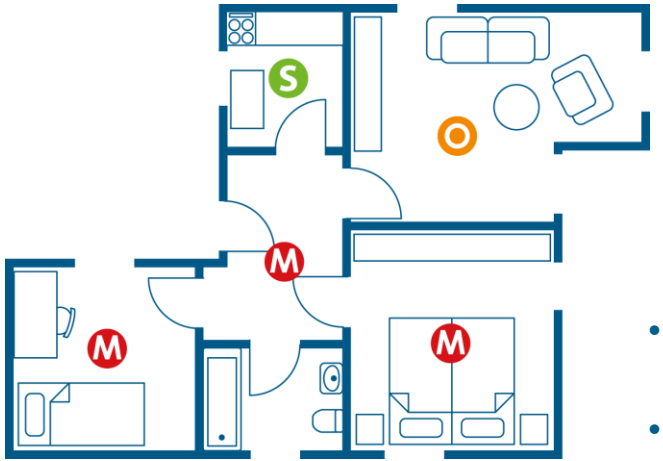
Warum EDR/XDR als Erkennungsplattform?

Endpoint
Detection &
Response

e**X**tended
Detection &
Response

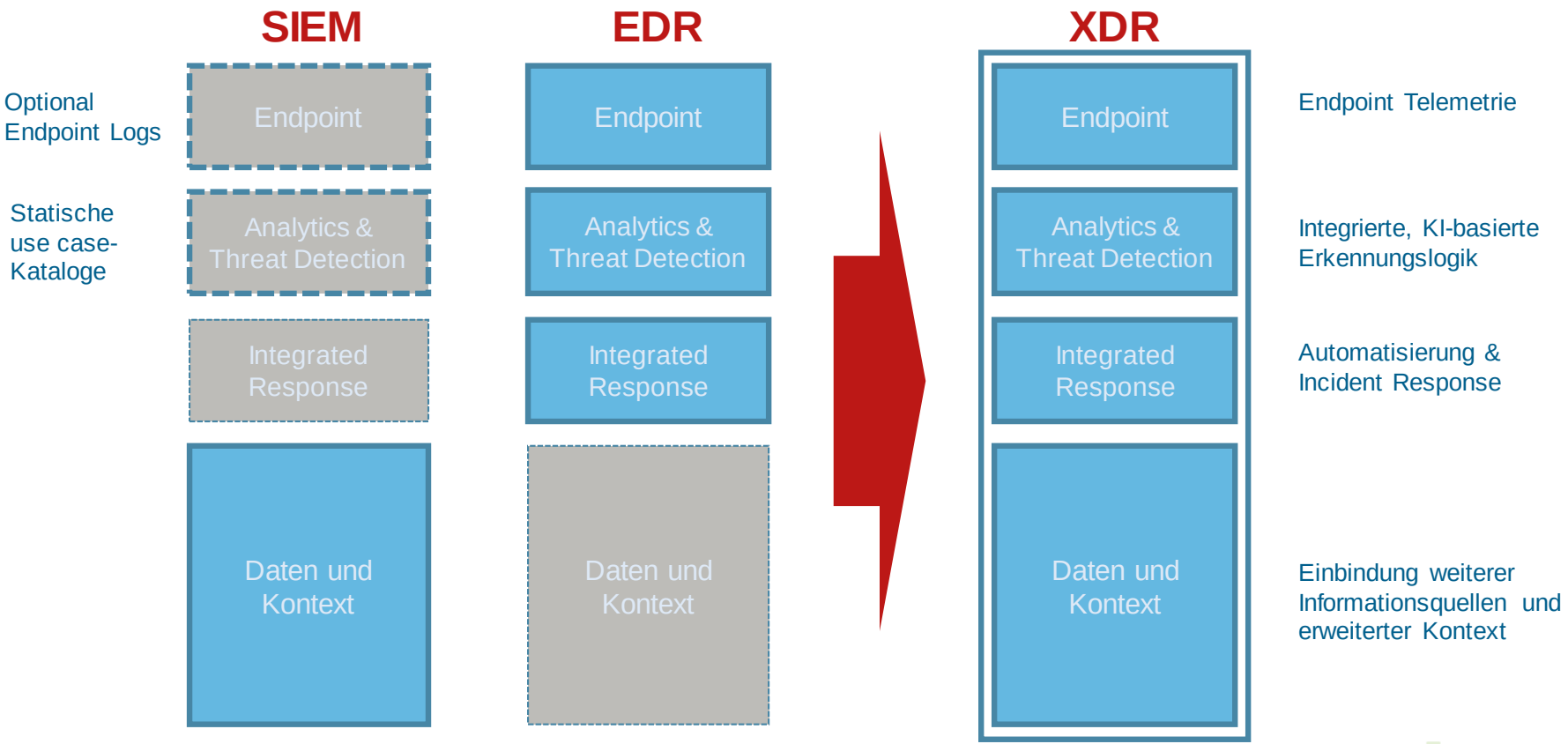
- EDR/XDR-Lösungen kombinieren **Erkennung** und **Reaktion**
- Sie stellen die **modernste Variante** der Gefahrenerkennung dar und sind klassischen Ansätzen überlegen, auch hinsichtlich der Wirtschaftlichkeit
- Sie sind leicht zu implementieren und damit **schnell wirksam**
- Aus diesen Gründen basiert das **Controlware Managed SOC** auf **Endpoint-basierte Risikoerkennung**

Wie arbeiten EDR-Lösungen - Analogie Brandverhütung



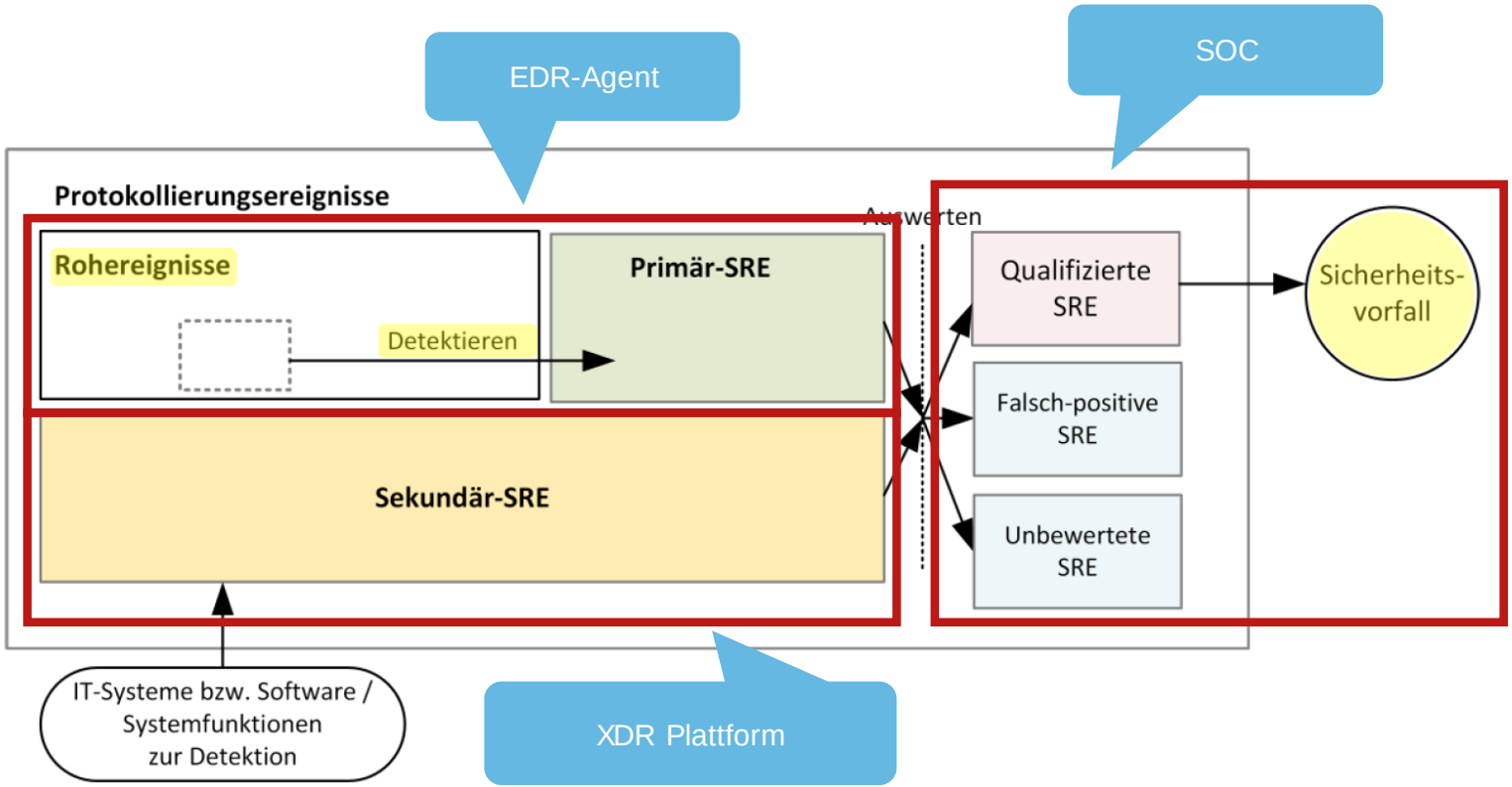
- Es ist ratsam, alle Räume auszustatten, um die Entstehung eines Brandes **frühzeitig erkennen und alarmieren** zu können.
- Sprinkleranlagen löschen gezielt am Brandherd und können die **Ausbreitung verhindern**, sind aber **nicht überall unbedenklich** einsetzbar.
- EDR/XDR-Lösungen arbeiten nach dem gleichen Konzept und **kombinieren Erkennung und Reaktion** am **Ausgangspunkt** der Gefahr, dem Endpoint (Client/Server).
- Das **SOC** unterstützt **gezielt reaktiv**, sucht aber auch **präventiv** nach Verdachtsmomenten

Entwicklung SIEM > EDR > XDR



Unser Managed SOC-Service erfüllt die BSI Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen

controlware



Auszug aus „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen Version 1.0a“

Unterstützte Lösungen zur EDR/XDR Angriffserkennung:

Lizenzen bereits vorhanden?

Falls Sie bereits eine dieser Lösungen einsetzen, können Sie den Managed SOC-Service **ohne zusätzliche Plattform-Kosten** nutzen!

Empfehlungen aus über 40 Managed SOC-Projekten (1)

controlware

- Beginnen Sie mit **Endpoint Detection und Response** in Verbindung mit **Managed SOC**

- **Warum?**
  - Schneller Rollout
  - Unmittelbarer Schutz
  - Kein interner Aufwand für die Analyse und Bewertung von Security Incidents

Empfehlungen aus über 40 Managed SOC-Projekten (2)

controlware

- **Separieren Sie** ggf. Bereiche, in denen EDR nicht möglich ist, z.B. OT-Umgebungen, über Netzwerksegmentierung

- Damit haben Sie bereits einen **umfassendes Schutzniveau** erreicht, das **annähernd 100% aller Angriffe** erkennt und die Ausbreitung verhindert

Empfehlungen aus über 40 Managed SOC-Projekten (3)

controlware

- Ergänzen Sie **im zweiten Schritt** sukzessive weitere **sinnvolle** Log-Quellen (XDR)
- **Warum?**
  - Erweiterte Log-Quellen erlauben **weitergehende Untersuchungen** und helfen **false positives** zu vermeiden
  - Sie dienen aber **eher selten** der initialen Erkennung von Cyber-Gefahren
  - Wir beraten Sie, welche Logquellen aus SOC-Sicht **sinnvoll** sind und einen **Mehrwert** für das SOC bieten

Empfehlungen aus über 40 Managed SOC-Projekten (4)

controlware

- Versuchen Sie **nicht**, im ersten Schritt gleich **100% aller denkbaren Szenarien** abzudecken

- **Warum?**
  - Sie verlieren viel Zeit für die Implementierung und erreichen einen ausreichenden Schutz erst **deutlich verzögert**
  - Sie erzeugen **hohe Kosten**, z.B. für die Speicherung von Log-Daten, die Sie vielleicht nie benötigen
  - Starten Sie pragmatisch!
    (siehe Key-Note Dr. Daniel Brettschneider)

Was zeichnet unseren Managed SOC Service aus?

controlware

- **24/7** SOC-Leistungen **ausschließlich aus Deutschland**
- **Deutsch- und englischsprachiger** Service durch **Qualifizierte SOC-Analysten**
- **Unmittelbare Incident Response-Leistungen** auf Basis der XDR-Plattform
- **Konkrete Handlungsempfehlungen**, falls Eingriffe in die Infrastruktur notwendig sind
- **Monatliche Threat Reviews**
- **entspricht den Empfehlungen des BSI** zur Protokollierung und Detektion von Cyber-Angriffen

Leader in Managed Security Services

controlware

Quelle: ISG Research Studie Cyber Security Solutions & Services 2023

Das sagt ISG über uns

Managed Security Services - SOC

Leader

„Mit seinem modularen Angebot und SOC-Services aus Deutschland geht Controlware zielgerichtet auf die Bedürfnisse seiner mittelständischen Kunden ein."

Frank Heuer

Controlware

Übersicht

Controlware ist ein deutscher IT-Dienstleister mit Hauptsitz in Dietzenbach in Hessen, beschäftigt mehr als 800 Mitarbeiter und unterhält ein Vertriebs- und Servicenetz mit 16 Standorten in Deutschland, Österreich und der Schweiz. Neben Strategic und Technical Security Services bietet Controlware auch Managed Security Services an, mit denen Kunden, vom gehobenen Mittelstand bis zu Großunternehmen und großen öffentlichen Kunden, adressiert werden. Die Managed Security/SOC Services sind Teil der Cyber Defense Services von Controlware.

Stärken

Große Manpower: Speziell auch gemessen an der Anzahl der Kunden unterhält Controlware in Deutschland ein großes Expertenteam für seine Managed Security Services.

Fokus auf Wachstumssegment: Controlware hat hinsichtlich seiner Managed-Security-Services einen starken und klaren Fokus auf das Segment der mittelständischen Unternehmen – eine Zielgruppe mit besonders hohem Wachstumspotenzial.

Delivery aus Deutschland: Controlware betreibt in Deutschland ein dediziertes Security Operations Center. Dies entspricht klar den Erwartungen vieler mittelständischer Kunden, dem wichtigsten Kundensegment von Controlware.

Flexible, kundenorientierte Services: Die Leistungen von Controlware sind kundenorientiert. Controlware offeriert seinen Kunden modulare Managed Security Services, was besonders interessant für Kunden ist, die keine alle Leistungen und Themen abdeckende Lösung benötigen. Dies gilt vor allem für viele mittelständische Unternehmen. Als Systemintegrator ist Controlware zudem dazu in der Lage, mittel- bis langfristige Lösungen für Cybersicherheitsprobleme anzubieten, die über das SOC-Sicherheitsvorfallmanagement hinausgehen, sowie Vorfälle zu entschärfen und die Infrastruktur von Kunden umzugestalten.

Herausforderungen

Controlware adressiert bisher mit seinen Managed Security Services nicht das Themen Data Leakage/Data Loss Prevention. Der punktuelle Ausbau des Angebotes könnte sich lohnen, da Datenschutz ein wichtiges und aktuelles Thema ist.

ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

BOSCH
CyberCompare

Arctic Wolf

END CYBER RISK

Terence Canaday, Senior Sales Engineer

Wahrscheinlichkeit eines Cyberangriffes

1 zu 2.700.000

Bärenattacke

- Nach Angaben des Yellowstone Nationalparks beträgt die Wahrscheinlichkeit für Besucher, von einem Grizzly angegriffen zu werden, 1 zu 2,7 Millionen (**3,7037037 x 10^{-5} Prozent**).

1 zu 16.000.000

Tödlicher Flugzeugabsturz

…teigender …en sinkt die Zahl der …ontinuierlich. Betrug die …hkeit, bei einem …eben zu kommen, in **…ahren noch 1:264.000**, … bei 1:16.000.000.

1 zu 4

Cyberangriff

- Im Jahr 2017 wurden geschätzte **8,4 Milliarden Geräte von Cyberkriminellen** angegriffen.
- Die Security-Spezialisten des Ponemon Institute schätzen die Wahrscheinlichkeit, Opfer eines Datendiebstahls zu werden, auf **25 Prozent** ein.

1 zu 354

Wohnungs-einbruch

- Im Jahr 2017 wurden in Deutschland **116.540 Einbrüche** gemeldet.
- Bei rund 41,3 Millionen Haushalten in Deutschland ergibt sich daraus eine **Wahrscheinlichkeit von 0,28 Prozent**.

1 zu 140.000.000

Lottogewinn

- Die Wahrscheinlichkeit, beim Lotto 6 aus 49 die **sechs Gewinnzahlen samt Superzahl** richtig zu tippen, beträgt 1 zu 139.838.160. Die Wahrscheinlichkeit für einen Dreier beträgt immerhin nur 1:63, ist damit aber immer noch knapp 16 Mal höher als die eines Cyber-Angriffs.

https://blog.wiwo.de/look-at-it/2019/03/26/die-wahrscheinlichkeit-eines-cyberangriffs-im-vergleich-mit-einbruch-blitzschlag-mehr/

Wahrscheinlichkeit
eines Vorfalls

Auswirkung
eines Vorfalls

Lösegeld

Innerhalb weniger Stunden geht die Lösegeldforderung ein. Dies geschieht immer mittels Fristsetzung und der Drohung kritische Daten zu verkaufen.

Verschlüsselung

Fileserver, Datenbanken und sogar Virtualisierungsbereiche werden verschlüsselt.

Datendiebstahl

Es werden Unternehmeskritische Daten ins Darkweb geladen. Dies können Konstruktionspläne, personenbezogene oder kundenbezogene Daten sein

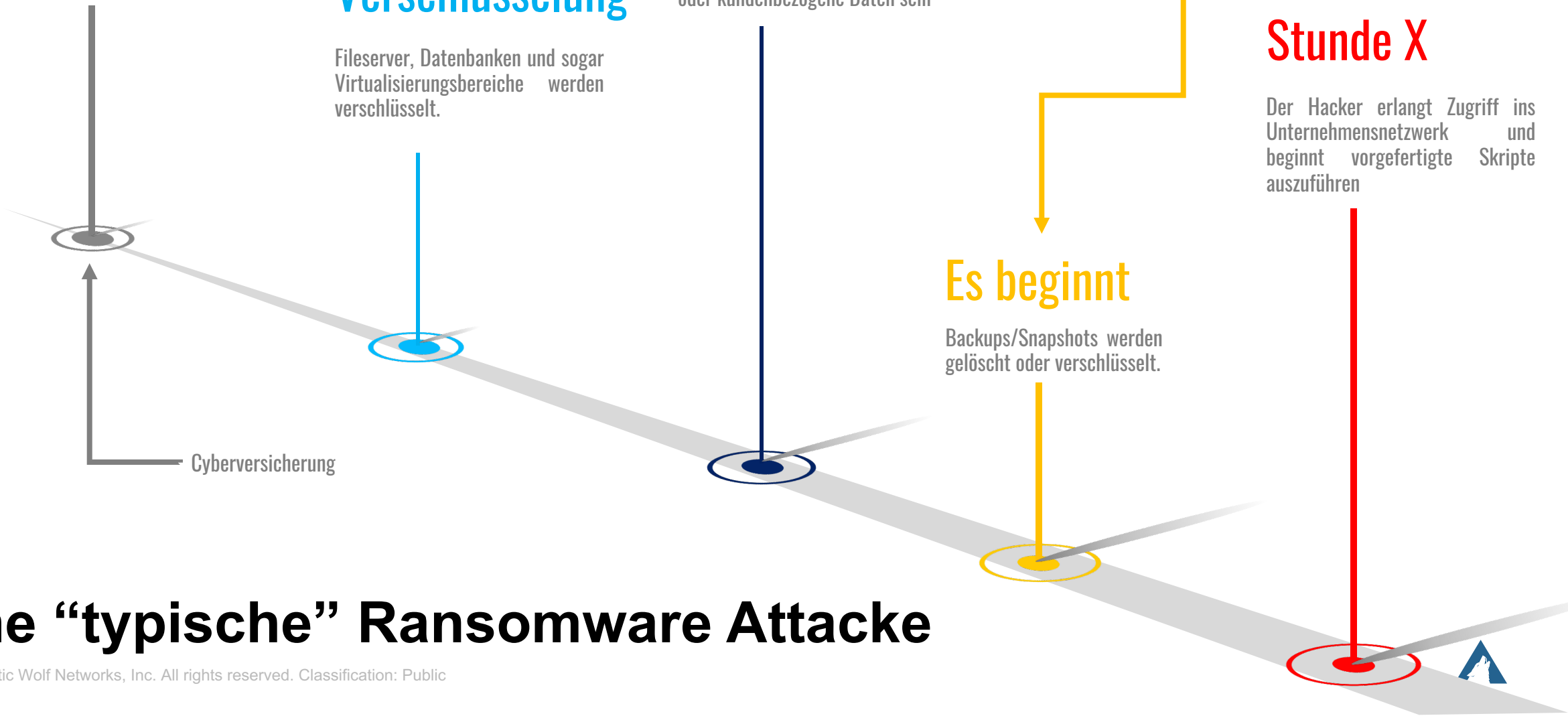
Immutable Backups/Snapshots

Es beginnt

Backups/Snapshots werden gelöscht oder verschlüsselt.

Stunde X

Der Hacker erlangt Zugriff ins Unternehmensnetzwerk und beginnt vorgefertigte Skripte auszuführen



Eine “typische” Ransomware Attacke

Stunde X

Der Hacker erlangt Zugriff ins Unternehmensnetzwerk und beginnt vorgefertigte Skripte auszuführen

Rahmenparameter

Durch öffentlich zugängliche Internetseiten wie Google und Bundesanzeiger werden Lösegelder festgesetzt.

Spionage

Kritische Komponenten warden gescannt. Infrastrukturkomponenten werden inventarisiert.

Es beginnt

Nötige Programmkomponenten für die Spionage werden in die Kundenumgebung platziert.

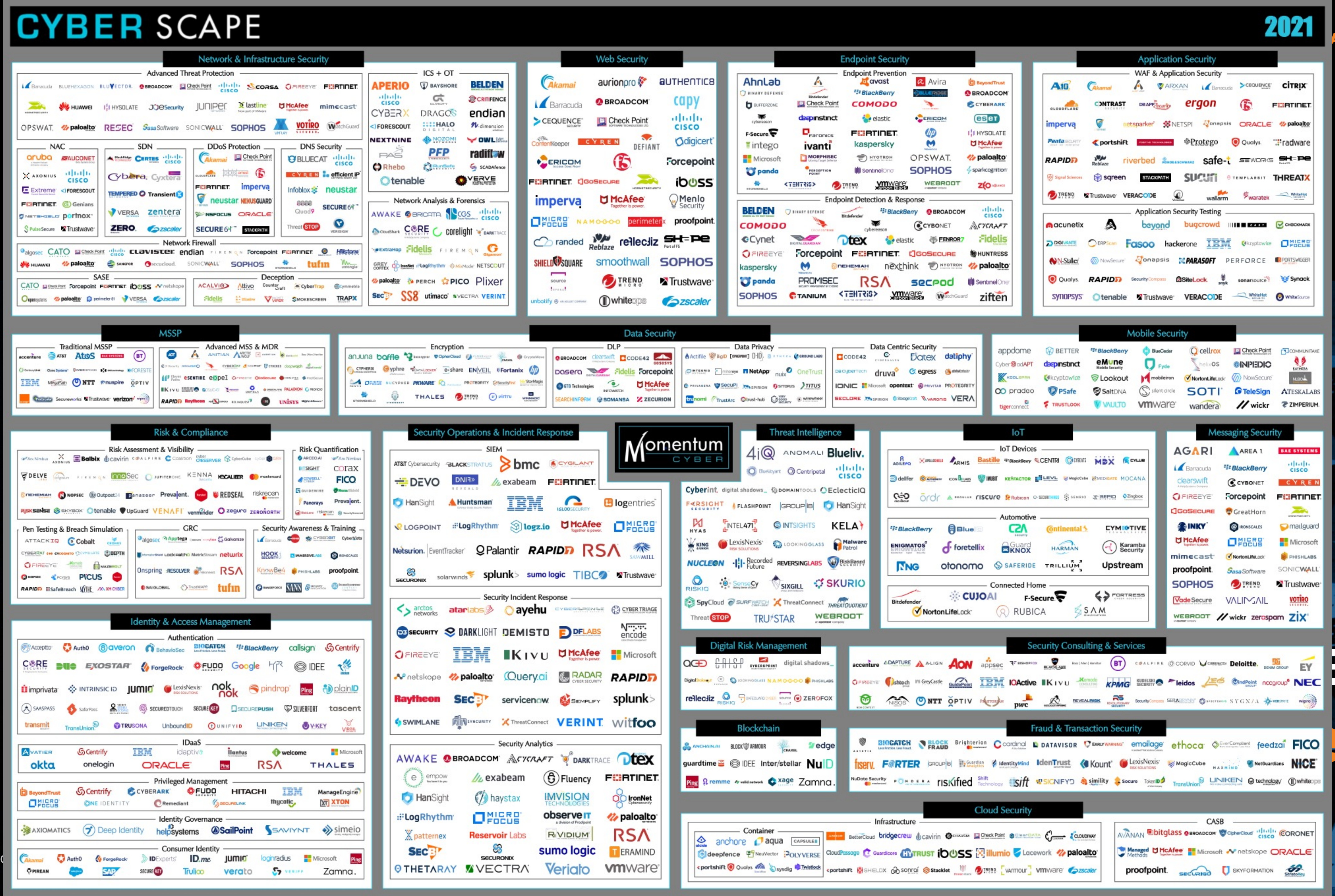
Arctic Wolf erkennt Angriffe frühzeitig und unterbricht die Kette bevor es zu schweren Verläufen kommt.

Tag 0

Max Mustermann fällt auf eine Phishing Mail herein und gibt sein Passwort unwissentlich weiter.

Eine “tatsächliche” Ransomware Attacke

ATIONS



ein

em

©2021 Ar

Was wir häufig vorfinden…

Ending Cyber Risk

Security Operations

THE LEADER IN SECURITY OPERATIONS

Angestrebtes Sicherheitslevel

Arctic Wolf Security Operations

GAP

Die meisten Firmen sind hier

BASIS

Passwörter / AD

Patch Management

Backups

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

ERWEITERTE VERTEIDIGUNG

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

WIDERSTANDS-FÄHIGKEIT

Proaktiv

Konform (ISO etc)

Versicherbar

ARCTIC WOLF

IDENTIFIZIEREN

SCHÜTZEN

ERKENNEN

REAGIEREN

WIEDERHERSTELLEN

Arctic Wolf Security Operations

Security ganz einfach – Weil einfach einfach einfach ist

5.300+
Kunden

24x7
in deutsch

570+
Security Engineers

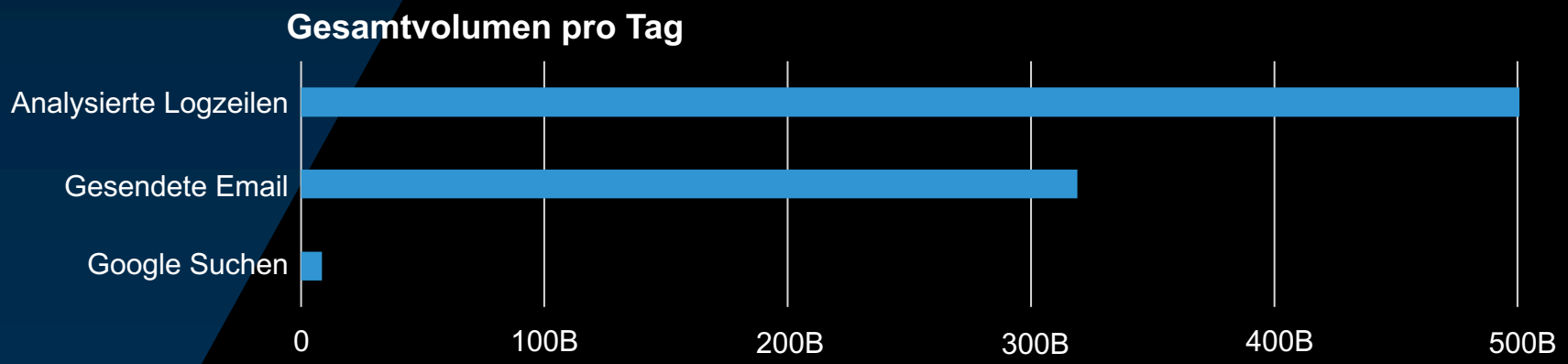
5
DC weltweit

500+
Milliarden Logzeilen pro Tag

3M+
aktive Agenten and 25,000+ sensors

12M+
Schwachstellen werden pro Woche identifiziert

600+
Incident Response Fälle pro Jahr



AI&ML kann den Mensch nicht ersetzten

Wir lösen Probleme

Angriffserkennung

Fachkräftemangel

Cyber-Versicherungsfähigkeit

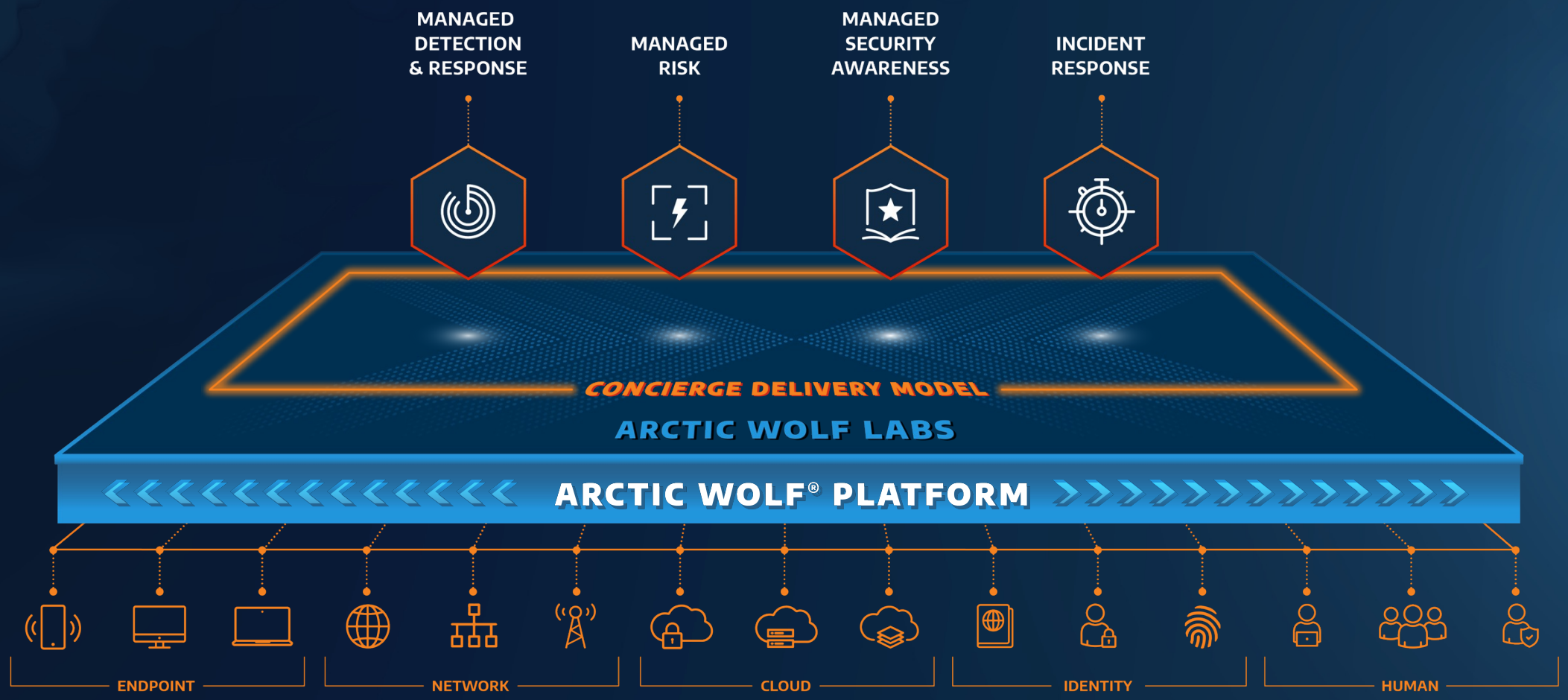
Unzufriedenheit mit Security-Tools & Produkten

Ineffiziente Ausgaben für Security

Nachweise zur Einhaltung von Regularien

ARCTIC WOLF

Security Operations Cloud



Die Denkweise muss sich ändern.

Weg von Tools und hin zu effektivem Betrieb.

Investments schützen

Bestehende Technologien nutzen und optimieren

Breitere Visibilität

Breite Abdeckung gegenüber allen Angriffstypen und Punkten

Widerstandsfähiger werden

Hinzufügen von Experten, 24x7 Überwachung & Schutz, sowie Einführung von taktischen und strategischen Security Aktionen.

Concierge Modell

Technologie und Teams liefern echte sicherheitsrelevante Ergebnisse

TECHNOLOGIE

Security Journey

Strukturierte Assessments Ihres Sicherheitszustands zur Härtung Ihrer Umgebung

Daten-Explorer

Schnelle Ad-Hoc Untersuchungen und Self-Service-Berichte

Starthilfe Portal

Proaktive Planung für Security Incidents um die Auswirkungen eines Vorfalls zu minimieren

Maßgeschneidertes Reporting

Concierge Reporting gibt Ihnen genau die Einblicke die Sie brauchen

CONCIERGE Modell

TEAMS

Bereitstellung

Stellen sicher das Ihre Umgebung eingerichtet und einsatzbereit ist

Concierge Team

Strategische Beratung Erhöhung Ihres Sicherheitsniveaus durch Workshops

SOC

24x7 Ereignis Triage

Security Assessments

Angeleitete Wiederherstellung

Incident Response

Wiederherstellung des Geschäftsbetriebs nach einem Vorfall

Digitale Forensik

Arctic Wolf: Das Beste im Thema Cyber Security

Zu einem Bruchteil der Kosten, die bei einem Alleingang anfallen würden, bietet Arctic Wolf einen umfassenden Schutz und einen ganzheitlichen Ansatz zur Vermeidung von Cyberrisiken.

Schnelle Wertschöpfung

Nutzen Sie bestehende Investitionen, erweitern Sie Ihr Team um Fachkräfte und -wissen, und reduzieren Sie den Aufwand mit einer schlüsselfertigen Lösung.

Zweckgebundene Plattform

Schlüsselfertige, skalierbare SOC Leistungen auf der Grundlage von Open-XDR für eine breite Abdeckung und 24x7-Schutz

Cyber Risk Management

Minderung von Cyberrisiken mit unserer Security Operations Cloud und Reduzierung des Restrisikos über unsere Garantie- und Versicherungspartnerschaften

Concierge Delivery

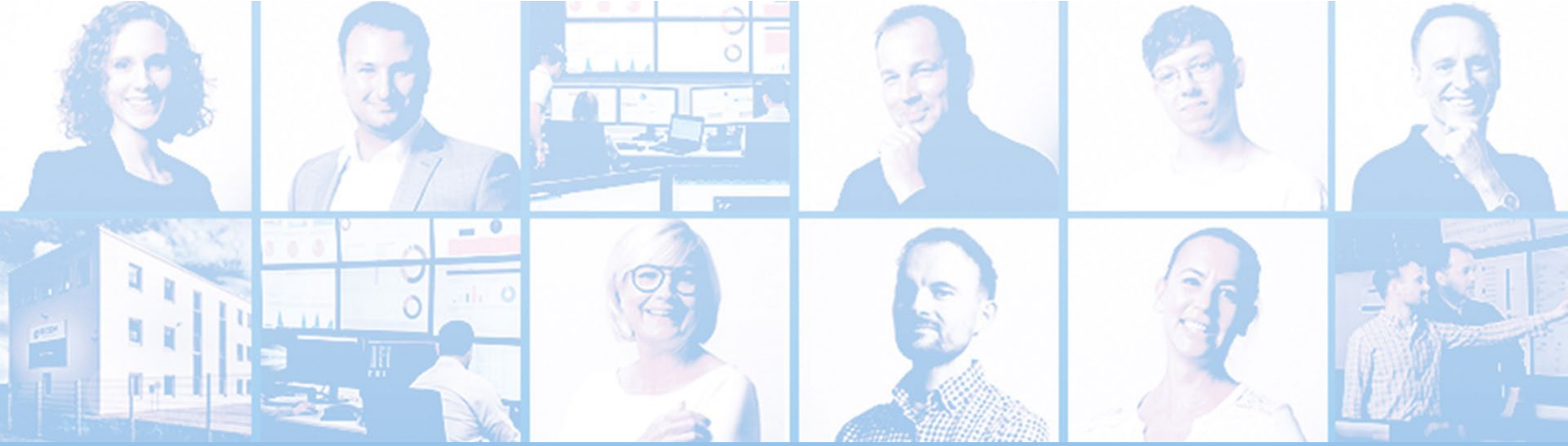
Sicherheit, die auf Ihre spezifischen Bedürfnisse zugeschnitten ist, mit Flexibilität bei den eingesetzten Tools, Mitarbeitern und Prozessen, um diese auf die für Sie am besten geeignete Weise zu gewährleisten

Vielen Dank

8 COM
CYBER SECURITY

„Der unverzichtbare Einsatz von SOAR im SOC“

Dienstag, 21. November 2023



1 8com-Vorstellung

Wir l(i)eben Sicherheit

8 COM
CYBER SECURITY

92

Mitarbeiter*innen

seit 2004

Cyber Security

97

Security Operations Center Kunden

> 600

IT-Forensik, Incident Response, Penetration Testing und Awareness-Kunden

8COM CYBER SECURITY

8com Security Operations Center

Orchestrierung Security Technologien

- SIEM (OnPrem/Cloud)
- UEBA
- EDR/xDR
- NDR
- Cloud Security Tools
- OT-Security
- . . .

Wird durch das 8com-SOAR orchestriert.

24/7/365 aus Deutschland

- Leistungserbringung aus Deutschland
- Leistung wird aus dem 8com SOC heraus erbracht, nicht aus Home Office
- Das 8com SOC ist ein eigenständiger Hoch-sicherheitsbereich
- SOC-Betrieb ist vollständig vom 8com Betrieb getrennt

Kontinuität und Kompetenz

- seit 2004 aus-schließlich Cyber Security Services im Angebot
- seit über 10 Jahren Betrieb des 8com SOC
- SOC ist die 8com Kernkompetenz
- Stabilität der Mitarbeiterstruktur

alle Level aus einer Hand

Das 8com SOC erbringt alle notwendigen Leistungen professionell aus einer Hand. Angefangen bei der Integration / Konfiguration von Security Technologien für das 8com-SOC, über die Alarmbearbeitung, Threat Analysis und Threat Hunting bis hin zu IT-Forensik, Malware Analysis, Incident Response Management, Vulnerability Management etc..

In **über 40 Ländern**
aktiv

Bundesamt
für Sicherheit in der
Informationstechnik

ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz

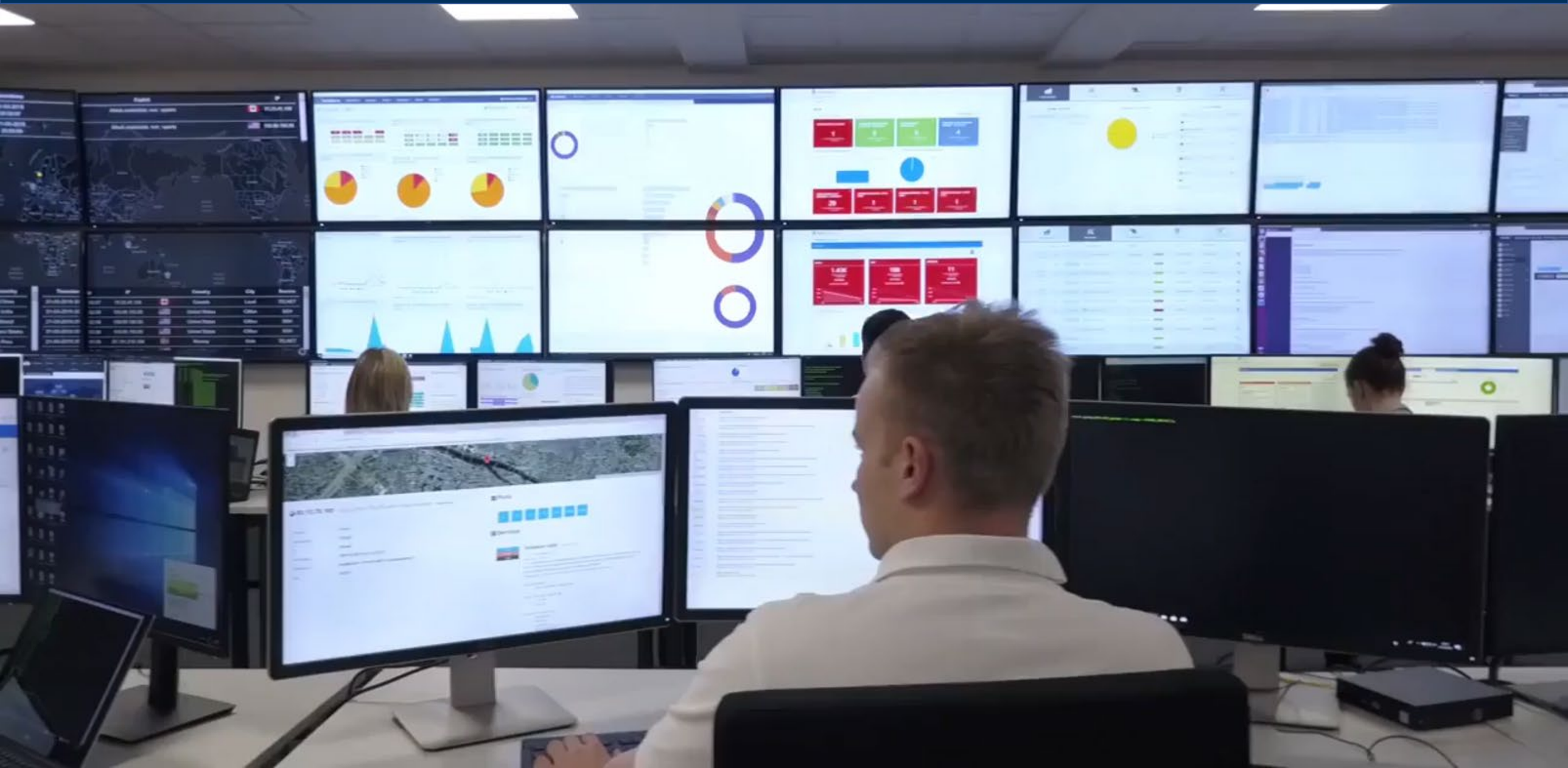
Zertifikat Nummer:
BSI-IGZ-0505-2022
Gültig bis 14.06.2025

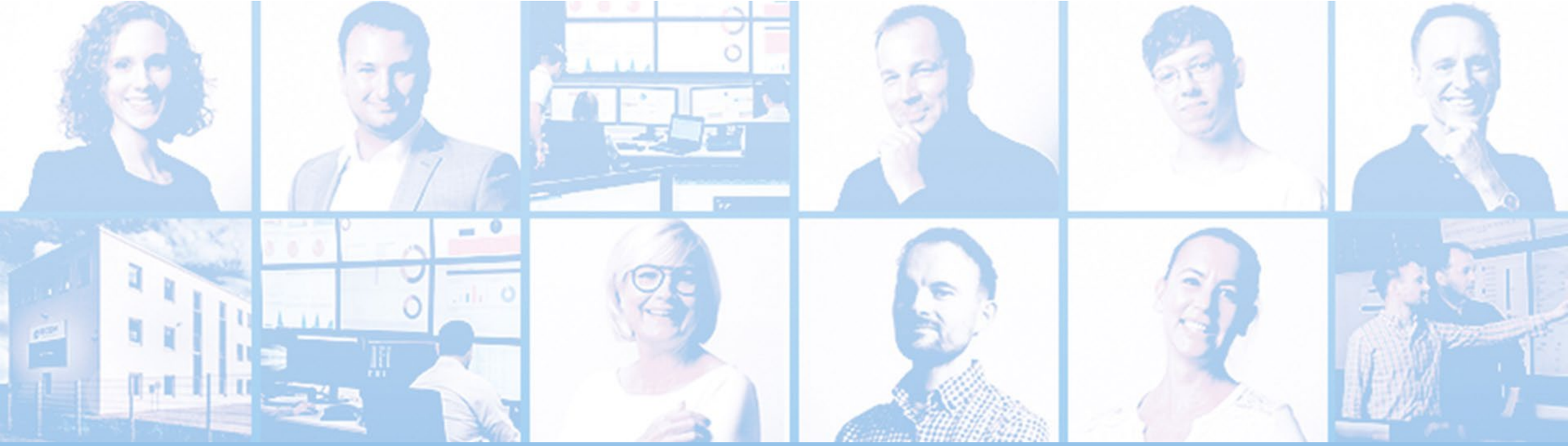
24/7/365 (3-Schicht-Modell)
nur aus Deutschland
Hochsicherheitsbereich
kein Homeoffice für SOC-Mitarbeiter

WIR L(I)EBEN SICHERHEIT.

8COM
CYBER SECURITY

8com Security Operations Center





2 Warum ist eine SOAR-Lösung wichtig für Sie als SOC-Kunde?

8COM CYBER SECURITY

SOC ohne SOAR = Ineffizienz

- Automatisierung repetitiver Aufgaben
- Orchestrierung verschiedenster Sicherheitstools (SIEM, EDR/xDR, NDR, Mail Security, OT-Security . . .)
- schnelle und präzise Reaktion auf Sicherheitsvorfälle

8COM CYBER SECURITY

1.

8COM
CYBER SECURITY

Beispiel

(… langweilige & repetitive Tasks)

8COM
CYBER SECURITY

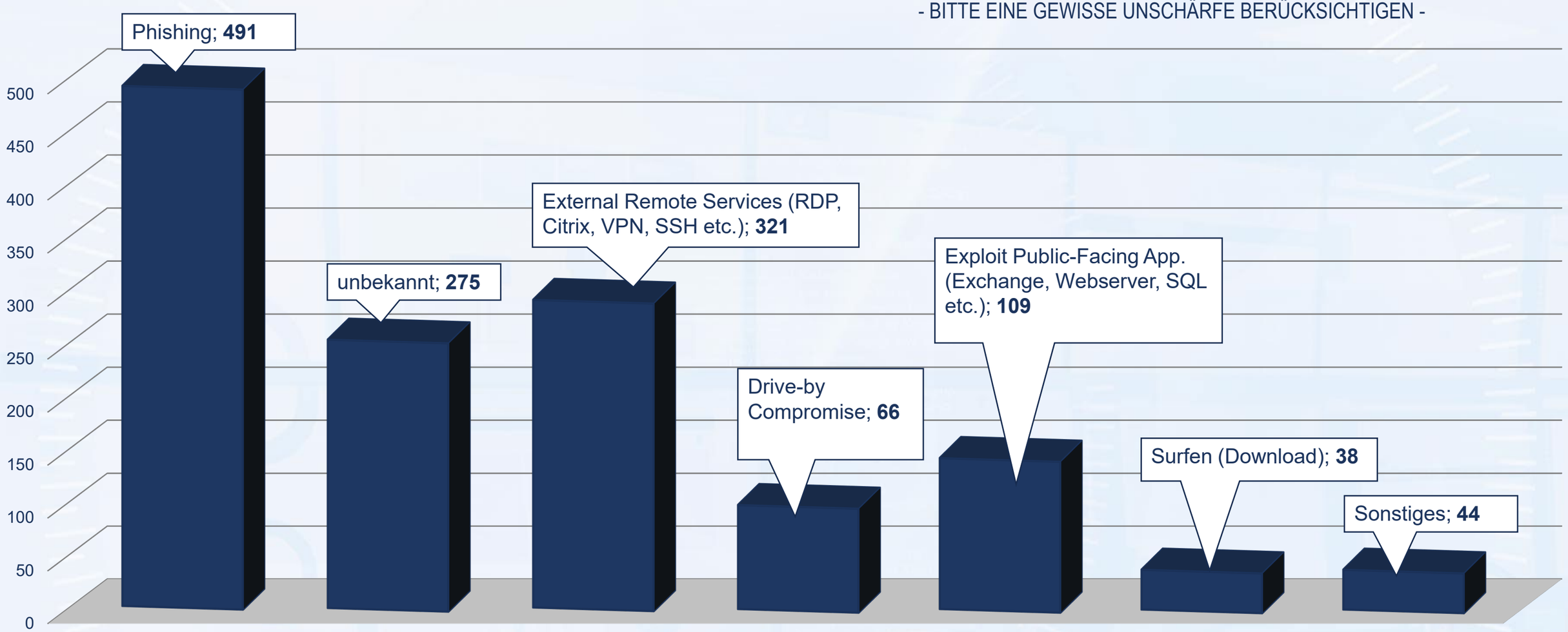
Phishing

8COM
CYBER SECURITY

Verteilung Initial Access Cyber Angriffe

01.01.2020 bis 30.06.2023 (1.344)

- BITTE EINE GEWISSE UNSCHÄRFE BERÜCKSICHTIGEN -



8COM CYBER SECURITY

PHISHING

FRÜHER

1. Alarm (AV, SIEM, User, Mail Security etc.) an SOC
2. Analyst erstellt „Case“
3. Analyst kontaktiert User / zuständigen Administrator
4. User / Admin leitet potentielle Phishing-Mail weiter
5. Analyst prüft Mail: Indikatoren, Header, SMTP-Verbindungsdaten, IoCs, öffnet Anlagen oder Links über eine Sandbox etc.
6. Bewertung: Phishing Mail?

FRÜHER

7. Meldung an User + Admin
8. User / Admin muss Mail löschen
9. Manuelle Suche nach weiteren Phishing Mails mit gleichen / ähnlichen Indikatoren
10. Prüfung ob User Anlage geöffnet / Link geklickt hat …
11. Bericht erstellen, Case schließen

DAUER: Ø 45 MIN

HEUTE

1. Alarm → SOAR
2. SOAR startet Playbook „Phishing“
3. SOAR: verschiebt Mail in „Analyse-Postfach“
4. SOAR: erstellt Case, informiert ggf. User
5. SOAR: reichert den Case um relevante Daten an (SIEM, EDR, Mail, Mail-Security, IoCs und Threat Intelligence, Analysiert Header, SMTP-Verbindungsdaten Mail-Appliance etc. Anlagen und Links werden in Sandbox ausgeführt. File Reputation Check . . .

HEUTE

7. SOAR: schadhaft – Malicious Indicators werden geblockt und unternehmensweit aus weiteren Mailboxes entfernt.
8. SOAR: prüft ob Malicious Indicators ausgeführt worden sind (. . . auch der Analyst).
9. SOAR: Gibt Case an Analysten. Analyst prüft, gibt ggf. Mail etc. wieder frei.
10. SOAR: Bericht erstellt, Case und Playbook wird beendet, User informiert.

DAUER: Ø 3 MIN

PHISHING

FRÜHER

1. Analyst muss Data Enrichment / Triage selbst durchführen, teils Daten manuell zusammentragen.
2. Langwierige Analyse Phase, da immer wieder auf unterschiedliche Konsolen zurückgegriffen werden muss.
3. Aufwendige Kommunikationsprozesse (Mail, Ticket etc.)
4. Aufwendige Dokumentation und Berichtspflichten . . .

HEUTE

1. ML-Unterstützung: lernt – unterstützt – bereitet Bewertung vor
2. Analyst bekommt (fast) IMMER alle zur vollständigen Analyse benötigten Daten aufbereitet.
3. SOAR-Lösung stellt dazu historische Daten identischer oder vergleichbarer Fälle zur Verfügung.
4. Kommunikation fast vollständig automatisiert über SOAR-Lösung
5. Dokumentation und Berichtswesen fast vollständig automatisiert.

2.

8COM
CYBER SECURITY

Orchestrierung

- Detektion
- Analyse
- Response

8COM CYBER SECURITY

Die Gartner „SOC Visibility Triad“

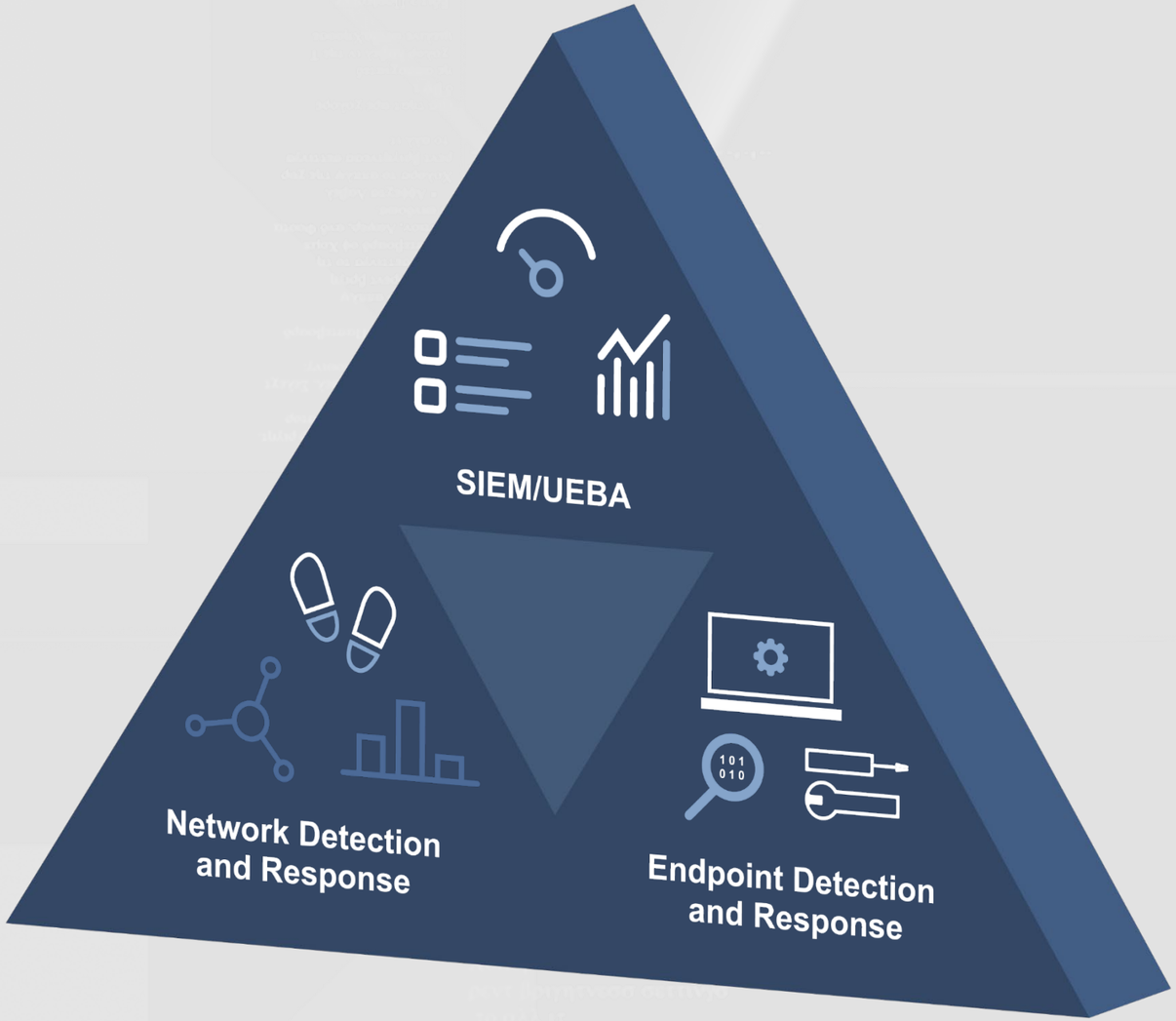
Gartner
2019

Die Sichtbarkeit von Cyber-Angriffen basiert bei 8com auf einer Kombination von drei unterschiedlichen Datenquellen-Arten:

1. Logfiles (SIEM) inkl. einer ML/KI basierten Anomalie-Erkennung (UEBA)

2. Endpoint Detection and Response Technologien

3. Netzwerkbasierte Erkennungen (Darktrace, Rhebo, IDS/IPS, NetFlow, HoneyPots etc.)



8COM CYBER SECURITY

ORCHESTRIERUNG | SECURITY TOOLS

DETEKTION

1. SIEM
2. EDR / xDR
3. NDR
4. OT-Security Monitoring
5. Cloud Security
6. Schwachstellenscans
7. . . .

ANALYSE

Aufbereitung der Daten für den Analysten

1. SIEM
2. EDR / xDR
3. NDR
4. Sandbox
5. Mail-Security
6. HR-Systeme
7. . . .

REAKTION

Containment:

1. EDR
2. Netzsegmentierung über Router, Switches, Firewalls etc.
3. AD – User sperren (OnPrem / Azure)
4. VPN-Zugang sperren
5. IP-Filter (Firewalls)
6. Cloud-Zugänge
7. . . .

3.

8COM
CYBER SECURITY

Enrichment

- Reduktion der Mitwirkungspflichten des SOC-Kunden
- Extreme Performance Steigerung der Analyse

8COM CYBER SECURITY

Typische Alarmmeldung

„suspicious M365 login“

- M365 User-Anmeldung von einer IP-Adresse aus Barcelona – 23:30 Uhr
- Früher am Tag: M365 User-Anmeldung von einer bekannten IP aus Deutschland – 12:00 Uhr

8COM CYBER SECURITY

SUSPICIOUS M365 LOGIN

8COM CYBER SECURITY

FRÜHER

1. UEBA-Alarm: suspicious M365 login
2. UEBA erstellt Timeline für auslösenden User + Entität
3. Alarmanreicherung durch TIF
4. Analyst prüft Alarm und weitere Aktivitäten und fügt diese ggf. zu einem Case zusammen.
5. Analyst fragt beim SOC-Kunden nach, ob User Anmeldung aus Barcelona legitim ist.

FRÜHER

6. Wartet auf Rückmeldung (kann Tage dauern)
7. Kunde meldet sich (positiv oder negativ)
8. Positiv: weitere Analysen, Aktivitäten des Users . . .
9. User wird gesperrt (manuell)
10. . . .
11. Case geschlossen, ggf. Bericht erstellt.

DAUER: Ø 60MIN
(MEAN TIME TO RESOLVE: 18 STUNDEN)

HEUTE

1. UEBA-Alarm: “suspicious M365 Login“ - SOAR
2. SOAR erstellt Case und startet Playbook „suspicious M365 login“
3. SOAR: Abfrage „HR-Reisemanagement (User auf Geschäftsreise in Barcelona)
4. Bestätigt: User = Barcelona
5. Case wird geschlossen
6. User ist nicht in Barcelona
7. SOAR: Triage EDR von verwendetem Endpunkt,

HEUTE

Logs M365, Historische Daten etc. – werden für Analyst aufbereitet.

7. SOAR/Analyst: prüfen ob Malicious Indicators vorhanden sind
8. SOAR/Analyst: sperrt User in Azure, informiert Vorgesetzten und Admin
9. SOAR: Bericht erstellt, Case und Playbook wird beendet, relevante Personen informiert.

DAUER: Ø 6 MIN
(MEAN TIME TO RESOLVE: 15 MIN)

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

Götz Schartner

goetz.schartner@8com.de

www.8com.de

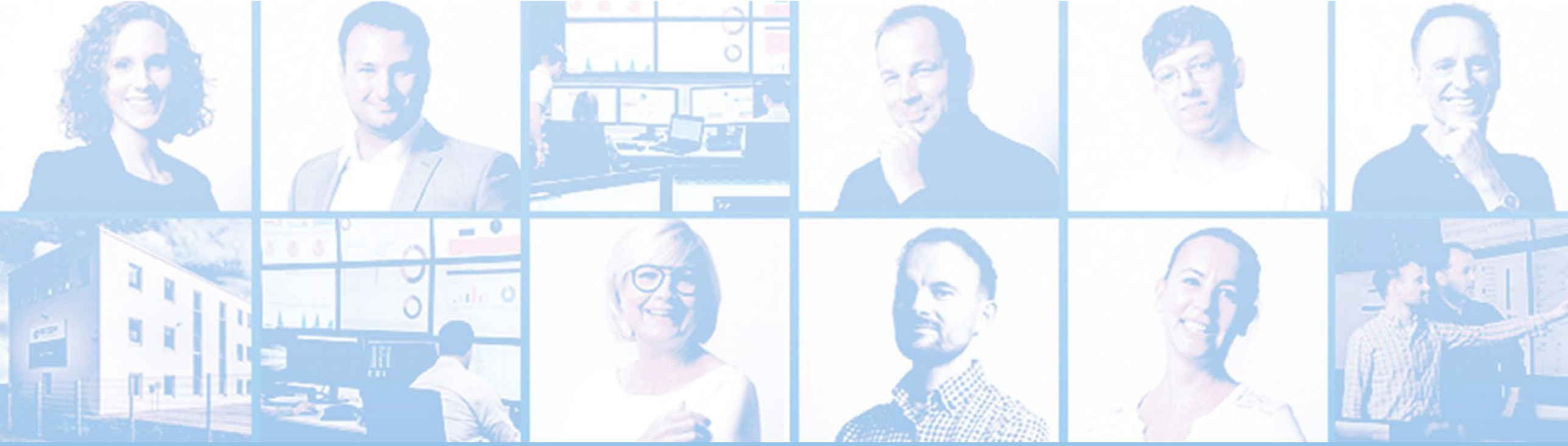
DANKE FÜR IHRE
AUFMERKSAMKEIT!

8COM CYBER SECURITY

8COM
CYBER SECURITY

„Überwachung in Echtzeit - SIEM“

Dienstag, 21. November 2023



1 8com-Vorstellung

Wir l(i)eben Sicherheit

8 COM
CYBER SECURITY

92

Mitarbeiter*innen

seit 2004

Cyber Security

97

Security Operations Center Kunden

> 600

IT-Forensik, Incident Response und Penetration Testing

8COM CYBER SECURITY

8com Security Operations Center

Orchestrierung Security Technologien

- SIEM (OnPrem/Cloud)
- UEBA
- EDR/xDR
- NDR
- Cloud Security Tools
- OT-Security
- . . .

Wird durch das 8com-SOAR orchestriert.

24/7/365 aus Deutschland

- Leistungserbringung aus Deutschland
- Leistung wird aus dem 8com SOC heraus erbracht, nicht aus Home Office
- Das 8com SOC ist ein eigenständiger Hoch-sicherheitsbereich
- SOC-Betrieb ist vollständig vom 8com Betrieb getrennt

Kontinuität und Kompetenz

- seit 2004 aus-schließlich Cyber Security Services im Angebot
- seit über 10 Jahren Betrieb des 8com SOC
- SOC ist die 8com Kernkompetenz
- Stabilität der Mitarbeiterstruktur

alle Level aus einer Hand

Das 8com SOC erbringt alle notwendigen Leistungen professionell aus einer Hand. Angefangen bei der Integration / Konfiguration von Security Technologien für das 8com-SOC, über die Alarmbearbeitung, Threat Analysis und Threat Hunting bis hin zu IT-Forensik, Malware Analysis, Incident Response Management, Vulnerability Management etc..

In **über 40 Ländern**
aktiv

Bundesamt
für Sicherheit in der
Informationstechnik

ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz

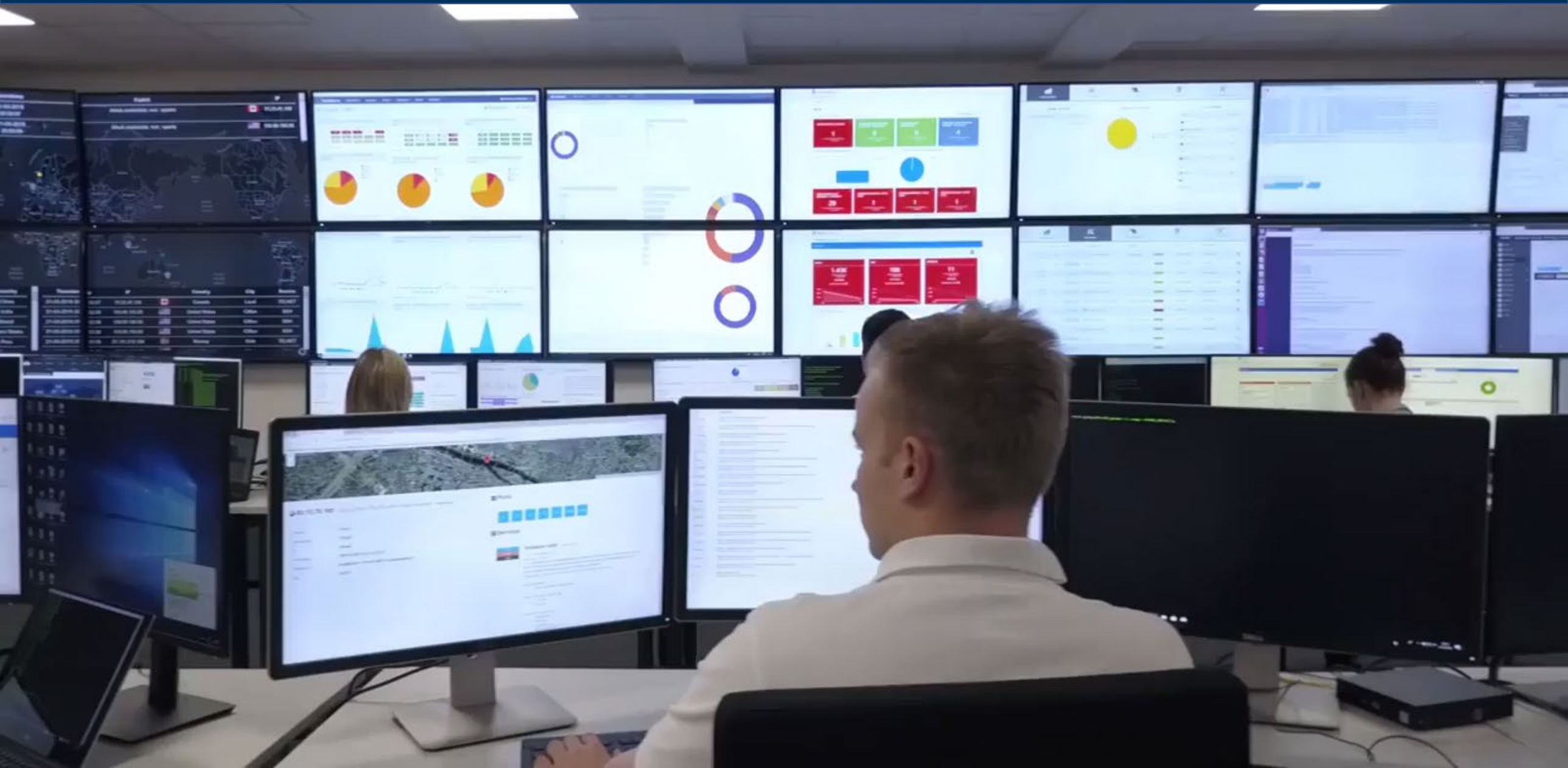
Zertifikat Nummer:
BSI-IGZ-0505-2022
Gültig bis 14.06.2025

24/7/365 (3-Schicht-Modell)
nur aus Deutschland
Hochsicherheitsbereich
kein Homeoffice für SOC-Mitarbeiter

WIR L(I)EBEN SICHERHEIT.

8COM
CYBER SECURITY

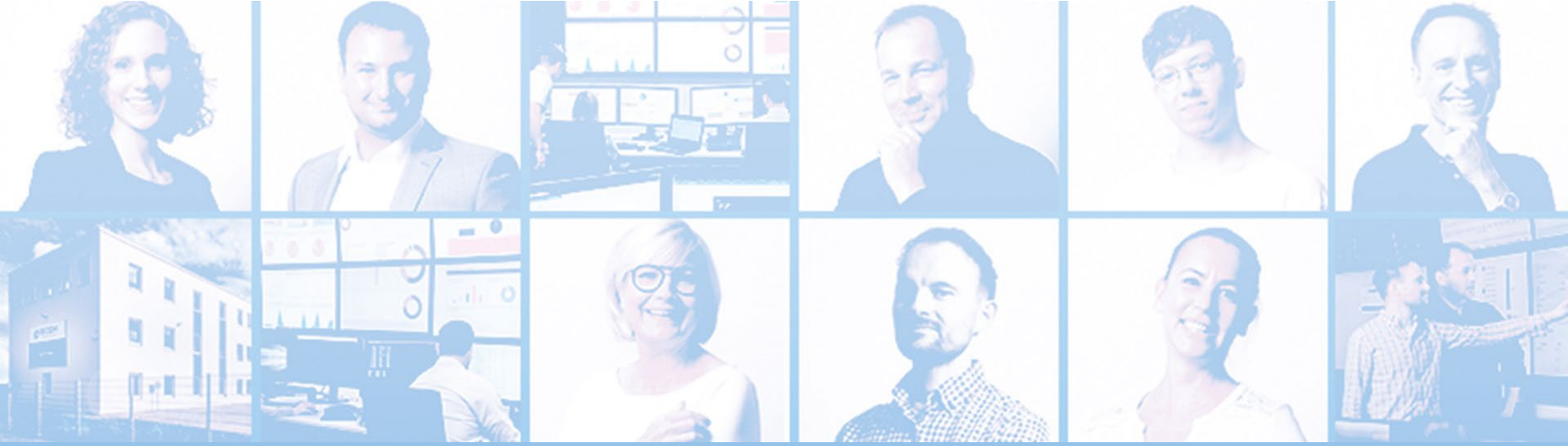
8com Security Operations Center



SIEM, EDR/xDR, NDR . . .
OnPrem IT/OT, Cloud, Mobile . . .

Was sollte zur Überwachung verwendet werden?

8COM CYBER SECURITY



2 Statistik „Inital Access“

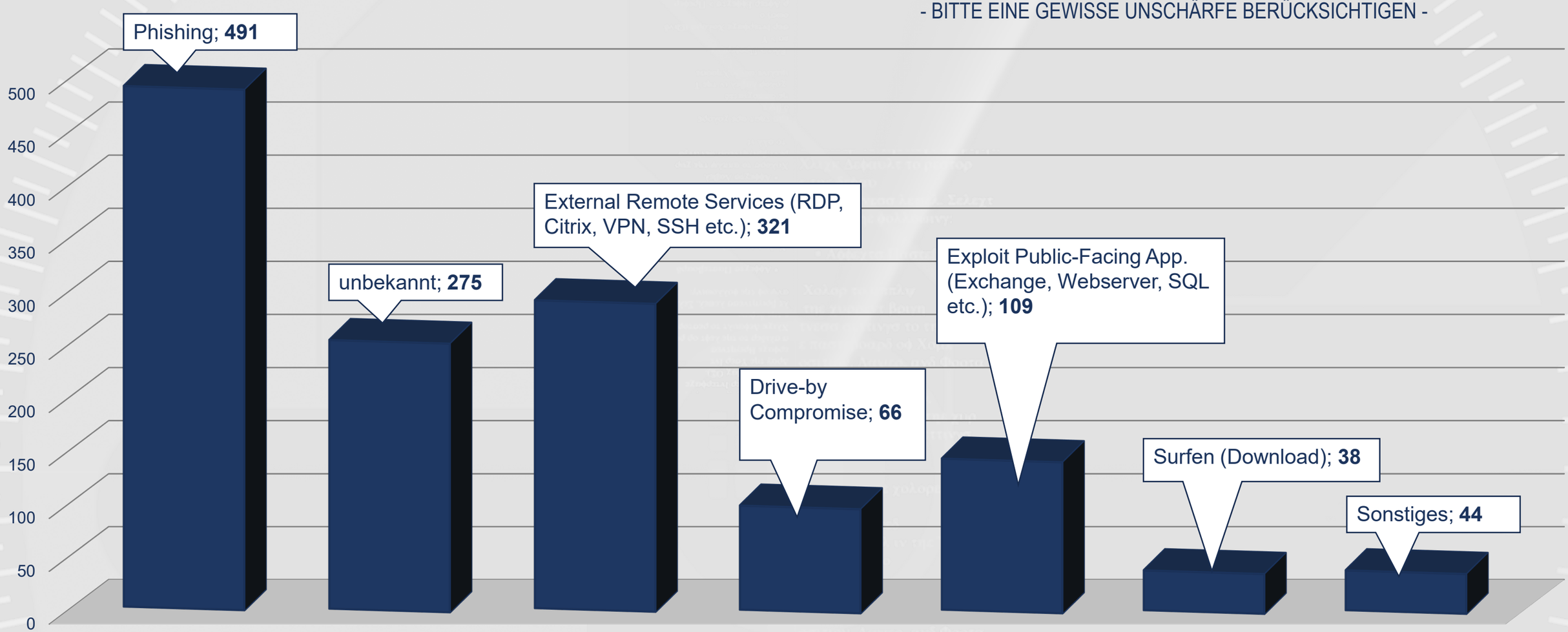
. . . aus 1.344 Cyber Angriffe

8COM CYBER SECURITY

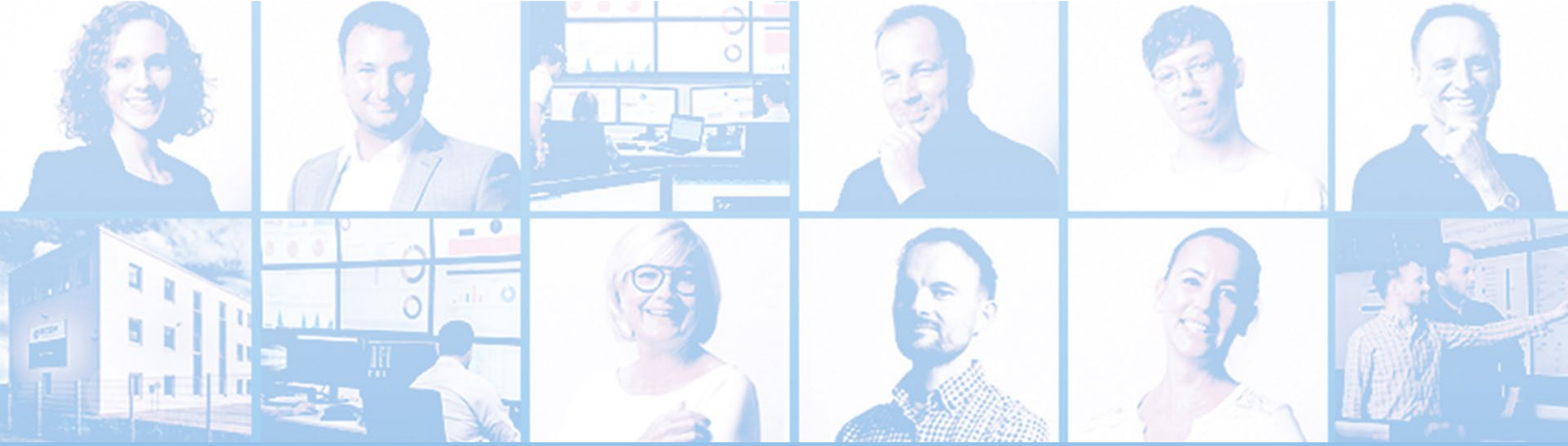
Verteilung Initial Access Cyber Angriffe

01.01.2020 bis 30.06.2023 (1.344)

- BITTE EINE GEWISSE UNSCHÄRFE BERÜCKSICHTIGEN -



8COM CYBER SECURITY



3 Cyber Attacke
2023

8COM CYBER SECURITY

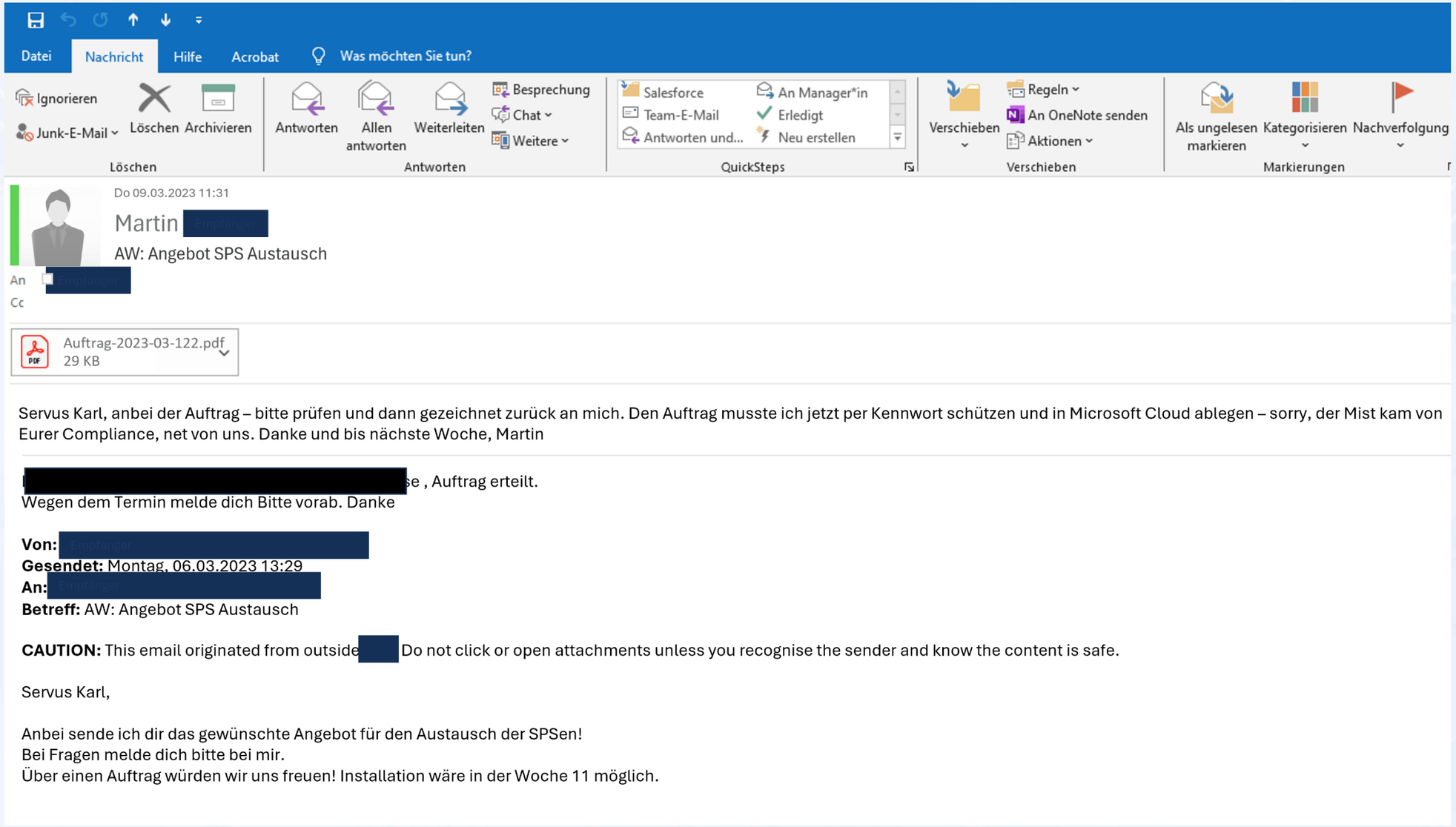
1.

8COM
CYBER SECURITY

1.

Qakbot Kampagne
37 verschiedene Empfänger / 30 verschiedene Absender

Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 11:29:00	▪ Mail mit PDF wird versendet ▪ Mail inkl. PDF wurde untersucht (Sandbox etc.)	Keine Auffälligkeit	Keine Auffälligkeit


Datei
Nachricht
Hilfe
Acrobat
Was möchten Sie tun?
Ignorieren
Junk-E-Mail
Löschen
Archivieren
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Antworten
Salesforce
Team-E-Mail
Antworten und...
An Manager*in
Erledigt
Neu erstellen
QuickSteps
Verschieben
Regeln
An OneNote senden
Aktionen
Verschieben
Als ungelesen markieren
Kategorisieren
Nachverfolgung
Markierungen
Do 09.03.2023 11:31
Martin [redacted]
AW: Angebot SPS Austausch
An [redacted]
Cc
Auftrag-2023-03-122.pdf
29 KB
Servus Karl, anbei der Auftrag – bitte prüfen und dann gezeichnet zurück an mich. Den Auftrag musste ich jetzt per Kennwort schützen und in Microsoft Cloud ablegen – sorry, der Mist kam von Eurer Compliance, net von uns. Danke und bis nächste Woche, Martin
[redacted]se , Auftrag erteilt.
Wegen dem Termin melde dich Bitte vorab. Danke
Von: [redacted]
Gesendet: Montag, 06.03.2023 13:29
An: [redacted]
Betreff: AW: Angebot SPS Austausch
CAUTION: This email originated from outside [redacted] Do not click or open attachments unless you recognise the sender and know the content is safe.
Servus Karl,
Anbei sende ich dir das gewünschte Angebot für den Austausch der SPSen!
Bei Fragen melde dich bitte bei mir.
Über einen Auftrag würden wir uns freuen! Installation wäre in der Woche 11 möglich.

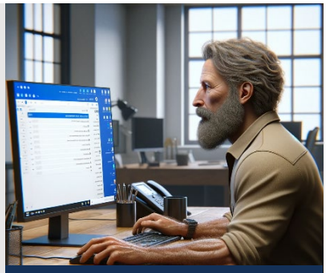
2.

8COM
CYBER SECURITY

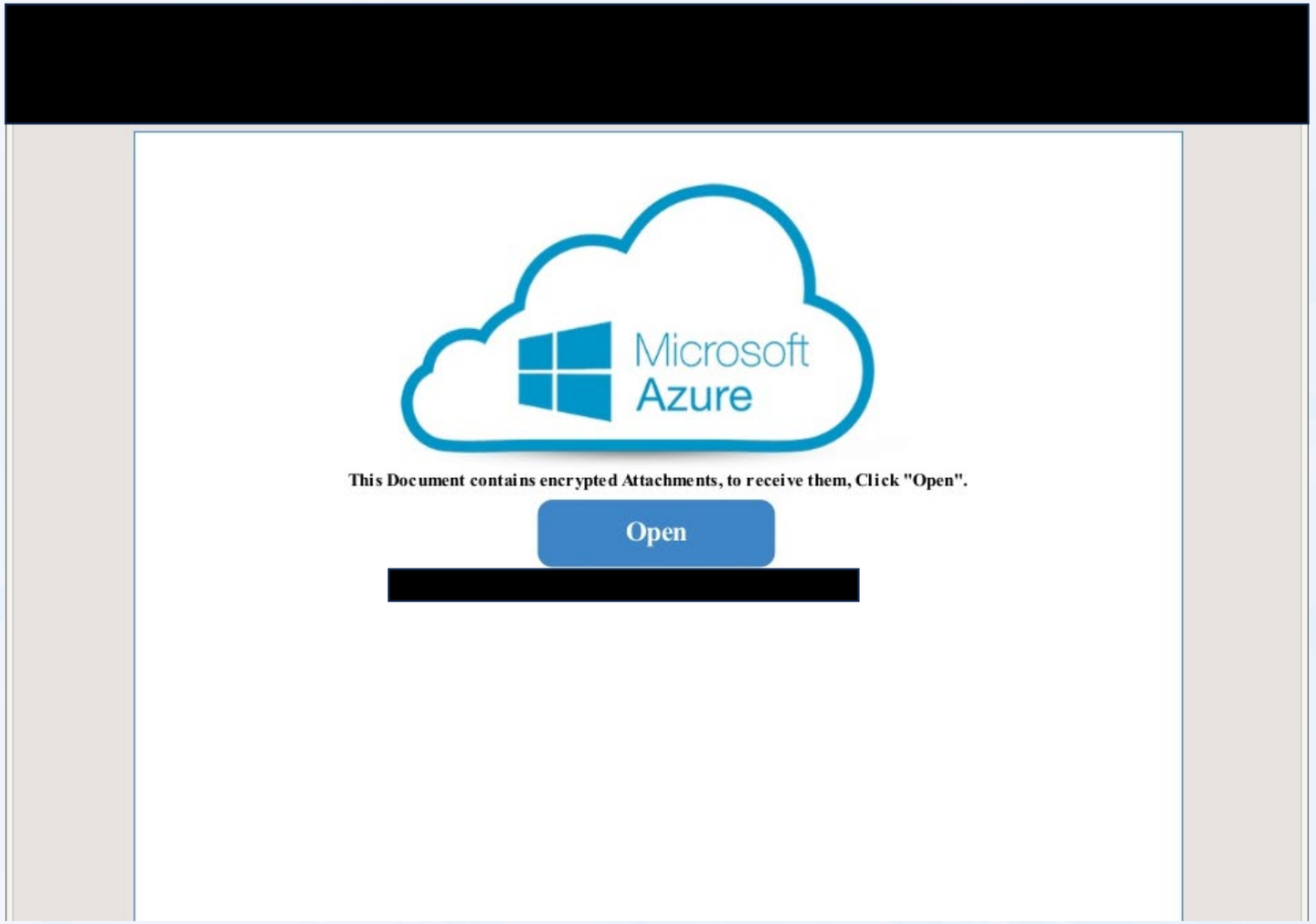
2.

Qakbot Kampagne
37 verschiedene Empfänger / 30 verschiedene Absender


Checkpoint Firewall


Karl

Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 11:53:00	▪ Empfänger öffnet die PDF	./.	./.


Microsoft
Azure
This Document contains encrypted Attachments, to receive them, Click "Open".
Open

3.

8COM
CYBER SECURITY

3.

Qakbot Kampagne
37 verschiedene Empfänger / 30 verschiedene Absender

Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 11:53:00	▪ lädt Zip-Datei herunter ▪ Windows Scripting Host führt Javascript aus ▪ Javascript ist hochgradig obfuskiert ▪ eine Reihe von Funktionen baut einen PowerShell-Befehl zusammen	Sysmon Event auf dem Client hätte wscript.exe Ausführung alarmiert (Event ID 1)	Entpacken des JavaScript hätte die Detektion triggern müssen (File Write Event), leider nicht passiert.

4.

8COM
CYBER SECURITY

4.

Qakbot Kampagne
37 verschiedene Empfänger / 30 verschiedene Absender

Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 11:53:00	▪ PowerShell-Befehl führt ein Base64-codiertes PowerShell-Script aus ▪ mittels wget wird eine DLL aus dem Netz geladen ▪ mit rundll32 ausgeführt ▪ DLL ist Qakbot Schadsoftware	Windows PowerShell Event Logs im SIEM wäre die Base64-codierte PowerShell-Skript Ausführung erkannt worden (Event ID 800).	▪ Herunterladen der DLL hätte File-Write Event + Detektion triggern müssen.

local privilege escalation fehlt

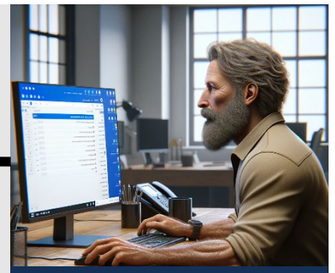
8COM CYBER SECURITY

5.

8COM
CYBER SECURITY

5.

Qakbot Team übergibt anscheinend an Black Basta



Karl

Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 13:55:00	▪ getmac.exe (Qakbot DLL-Injected) führt diverse Gruppenmitgliedschaften und Authentifizierungsversuche aus. ▪ Möglicherweise wurde mimikatz BOF (Beacon Object File) injiziert und gestartet	Sysmon Event Logs im SIEM wäre die getmac.exe Ausführung protokolliert worden (Event ID 1).	▪ Prozess Injection wurde erkannt und alarmiert, aber erst nach Bekanntwerden des Incidents analysiert.

6.

8COM
CYBER SECURITY

6.

Black Basta

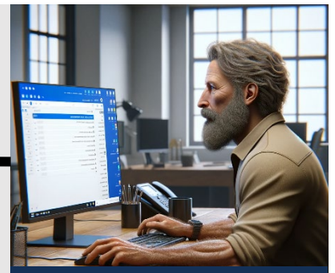
Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 14:12:00	▪ Base64-codiertes PowerShell-Skript lädt PowerSploit Komponente herunter ▪ startet Get-NetDomainController um Domain Controller im Netzwerk zu enumerieren.	Windows PowerShell Event Log im SIEM wäre die Base64-codierte PowerShell-Skript Ausführung (Event ID 800) erkannt worden.	▪ PowerSploit Komponente wurde durch File Write Event detektiert und als Alarm abgesetzt. ▪ Analyse erst nach Bekanntwerden des Incidents

7.

8COM
CYBER SECURITY

7.

Black Basta



Karl

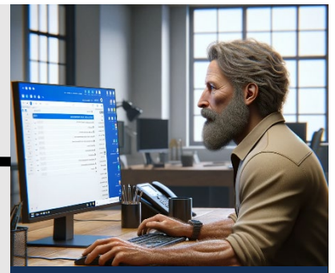
Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 14:18:00	▪ Explorer.exe führt Anmeldevorgänge mit Logon-Type 9 mit Dienstbenutzer durch, die auf Cobalt Strike Access Token Erzeugung (make_token) hindeuten.	Windows Security Event Logs im SIEM wäre die ungewöhnliche Anmeldung erkannt worden (Event ID 4624, Logon-Type 9, Logon-Process advapi).	./.

8.

8COM
CYBER SECURITY

8.

Black Basta



Karl

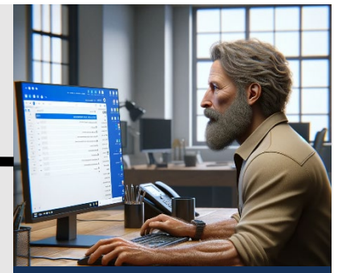
Datum | Uhrzeit	Beschreibung	**SIEM** (nicht vorhanden)	**xDR** (vorhanden)
09.03.2023 | 14:19:00	▪ Explorer.exe wird ein weiterer Anmeldevorgang mit Logon-Type 9 mit demselben Dienstbenutzer durchgeführt, diesmal mit Pass-The-Hash (runas) Charakteristik.	Windows Security Event Logs im SIEM wäre die ungewöhnliche Anmeldung erkannt worden (Event ID 4624, Logon-Type 9, Logon-Process seclogon).	./.

9.

8COM
CYBER SECURITY

9.

Black Basta



Karl

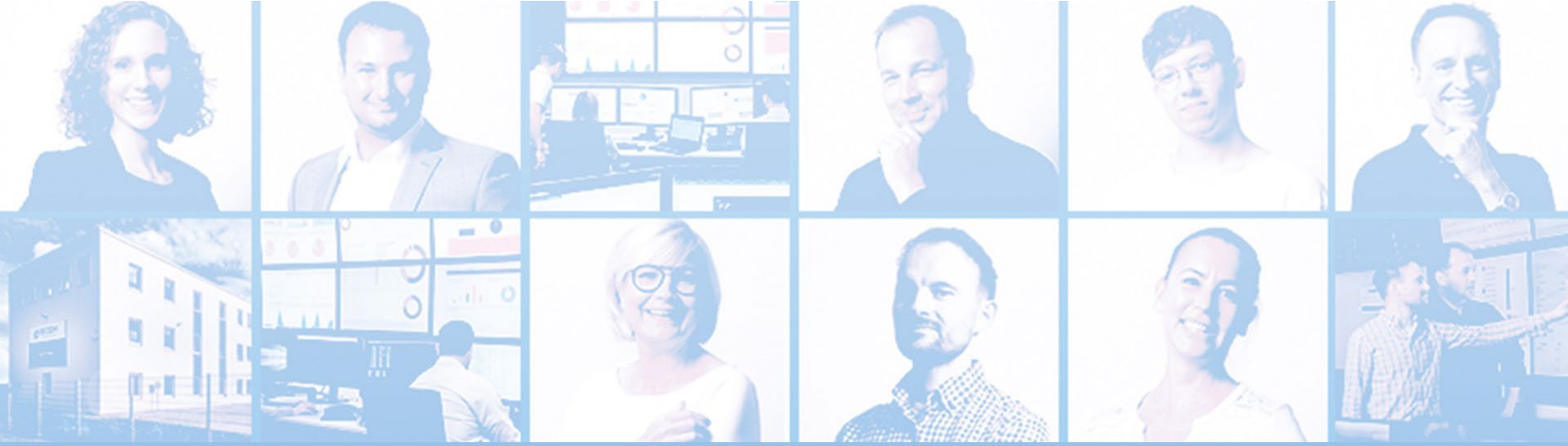
Datum | Uhrzeit	Beschreibung	SIEM (nicht vorhanden)
09.03.2023 | 14:19:00	▪ Mit dem Dienstbenutzer ist lateral movement zu zwei Domain Controllern möglich. ▪ Threat Actor nutzen „Jump To“ (psexec, psexec_psh) von Cobalt Strike, um mit Dienstregistrierung weiteres Cobalt Strike Beacon auf dem DC auszuführen. ▪ Der Dienstbenutzer hat Administrator Rechte auf diesen Systemen. Credential Dumping ist damit möglich -> Domäne kompromittiert.	Server Windows System Event Logs im SIEM wäre die Cobalt Strike Beacon installation erkannt worden (Event ID 7045, Dienstname *\ADMIN$* oder %COMSPEC% * powershell * JAB…).

. . . 32 Tage später

8COM
CYBER SECURITY

. . . 80% der relevanten Daten sind verschlüsselt

8COM CYBER SECURITY



3 Schäden

8COM CYBER SECURITY

Business Impact in Euro

(Achtung: teilweise geschätzt)

I. Reputations-schaden	II. Schadensbe-seitigungs-kosten	III. Datenschutz	IV. Haftungsfragen Organe	V. Haftungsfragen aufgrund gestohlener Daten	VI. Betriebsunter-brechungs-schäden + Unterbrechung der Geschäfts-entwicklung
tbd	ca. 17,3 Mio. €	ca. 4 Mio.	tbd	tbd	ca. 90 Mio Euro
Vertrauensverlust bei Kunden und Partnern	• Forensik • Incident Response • Krisenkom-munikation • Rechtsberatung • Dekontaminierung der IT-Systeme und teils neue IT-Infrastruktur	▪ Bußgelder (1% - 2% Jahresumsatz) ▪ Reorganisation Datenschutz-organisation	Haftung ggf. aufgrund von Obliegenheits-verletzungen von Organen (DSB, ISB, GF, Vorstand) **Achtung:** Änderungen durch NIS 2.0 in 2024 möglich (max. 30.000 Unternehmen in D)		

8COM CYBER SECURITY

4 SIEM oder EDR/xDR?

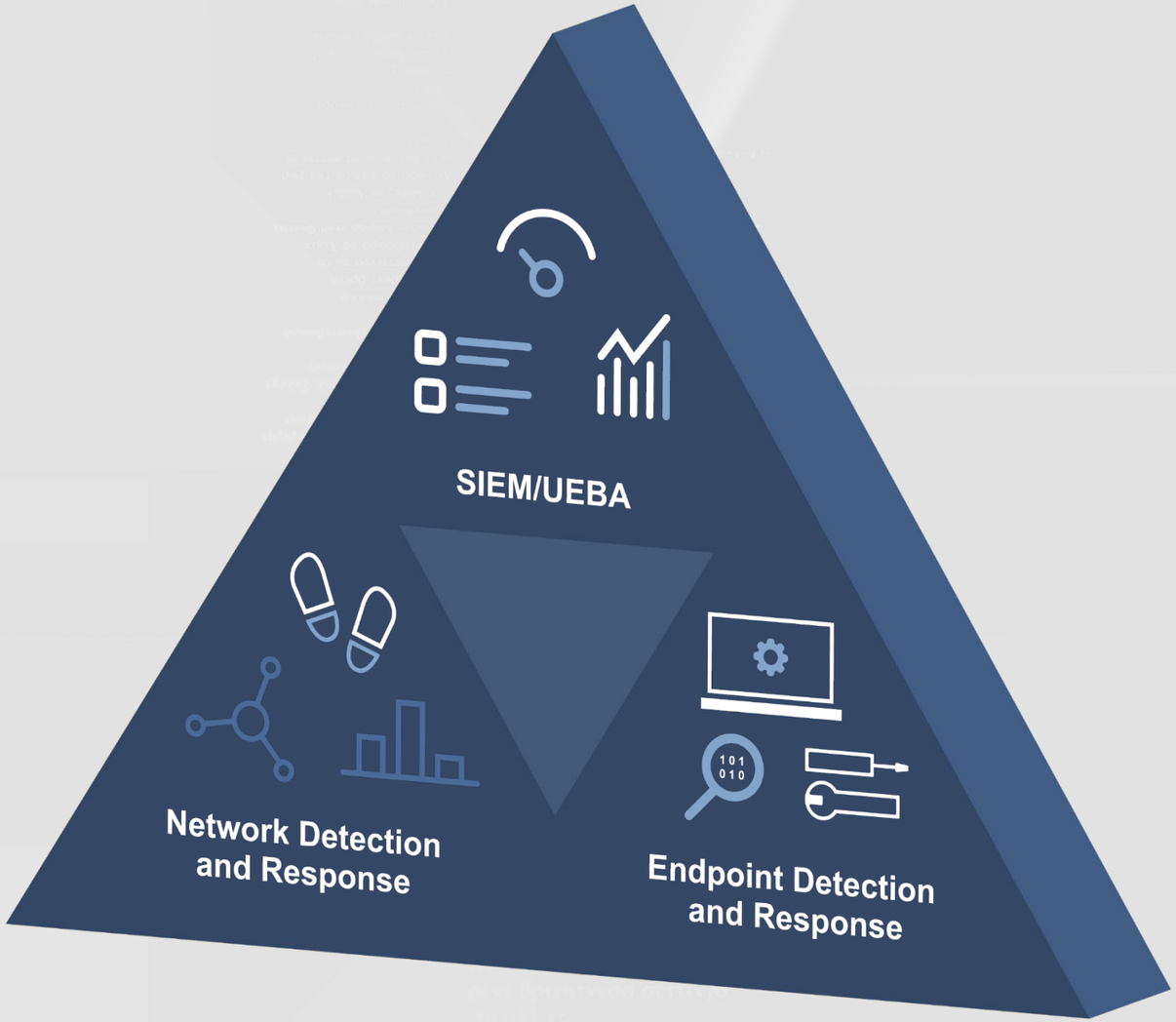
8COM CYBER SECURITY

Gartner „SOC Visibility Triad“

Gartner
2019

Die Sichtbarkeit von Cyber-Angriffen basiert bei 8com auf einer Kombination von drei unterschiedlichen Datenquellen-Arten:

1. Logfiles (SIEM) inkl. einer ML/KI basierten Anomalie-Erkennung (UEBA)
2. Endpoint Detection and Response Technologien
3. Netzwerkbasierte Erkennungen (Darktrace, Rhebo, IDS/IPS, NetFlow, HoneyPots etc.)
4. Cloud, OT etc. nicht vergessen



8COM CYBER SECURITY

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

Götz Schartner

goetz.schartner@8com.de

www.8com.de

DANKE FÜR IHRE
AUFMERKSAMKEIT!

8COM CYBER SECURITY

LOGPOINT

MARKTAUSBLICK

DEUTSCHLAND VOR NIS2

550 Large Enterprise

SAP-BCS

MSSP – SIEM Services

https://disfold.com/germany/companies/

6.500 Mittelstandskunden

(500 – 5.000 Mitarbeiter)

OnPrem

MSSP-Services

SOC –Services

DEUTSCHLAND AB 17.10.2024 (NIS 2)

22.500 Mittelstandskunden

(100 – 500 Mitarbeiter)

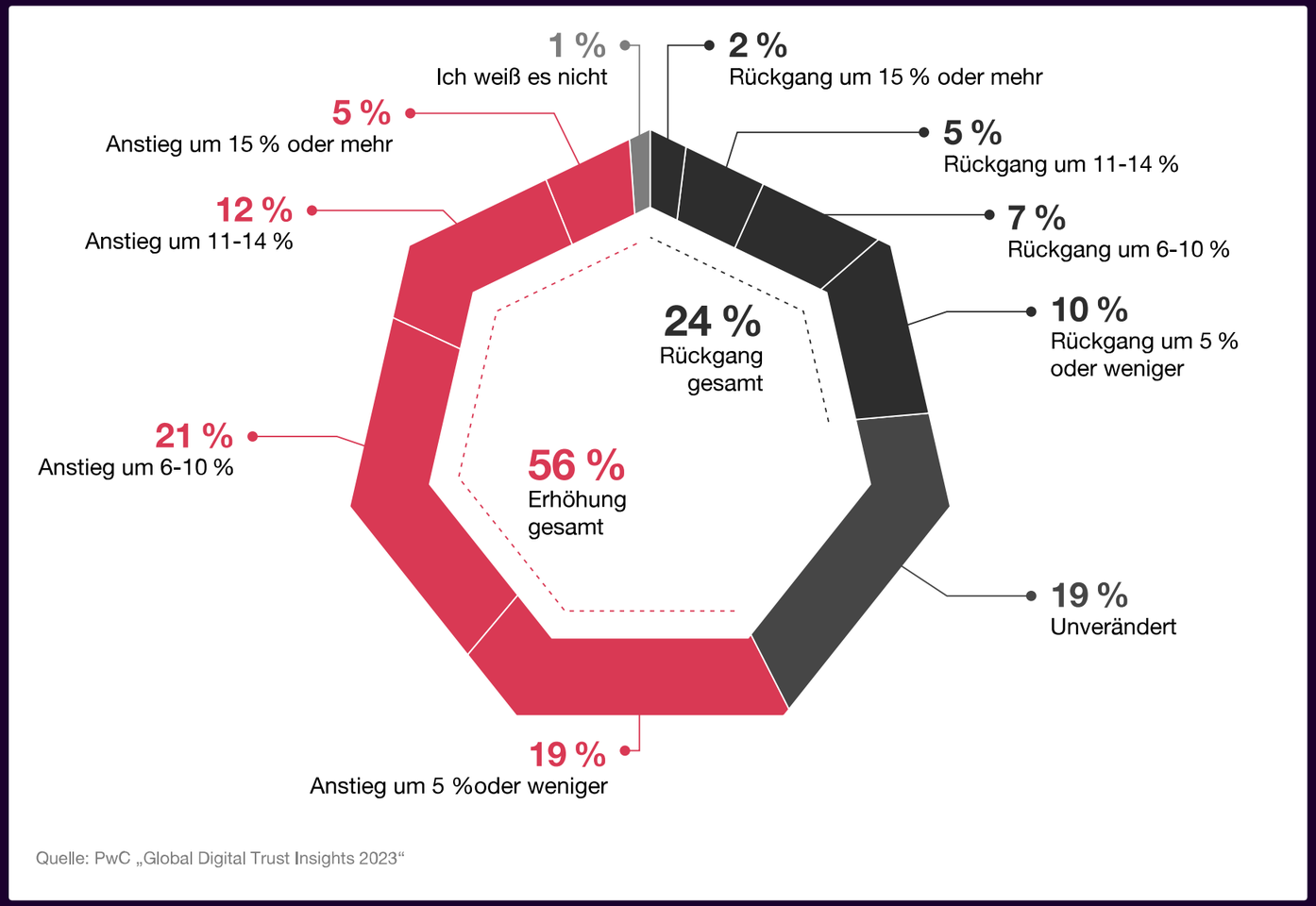
SOC –Services

360° Cyberservices

ECOSYSTEM VERSUS PLATTFORM

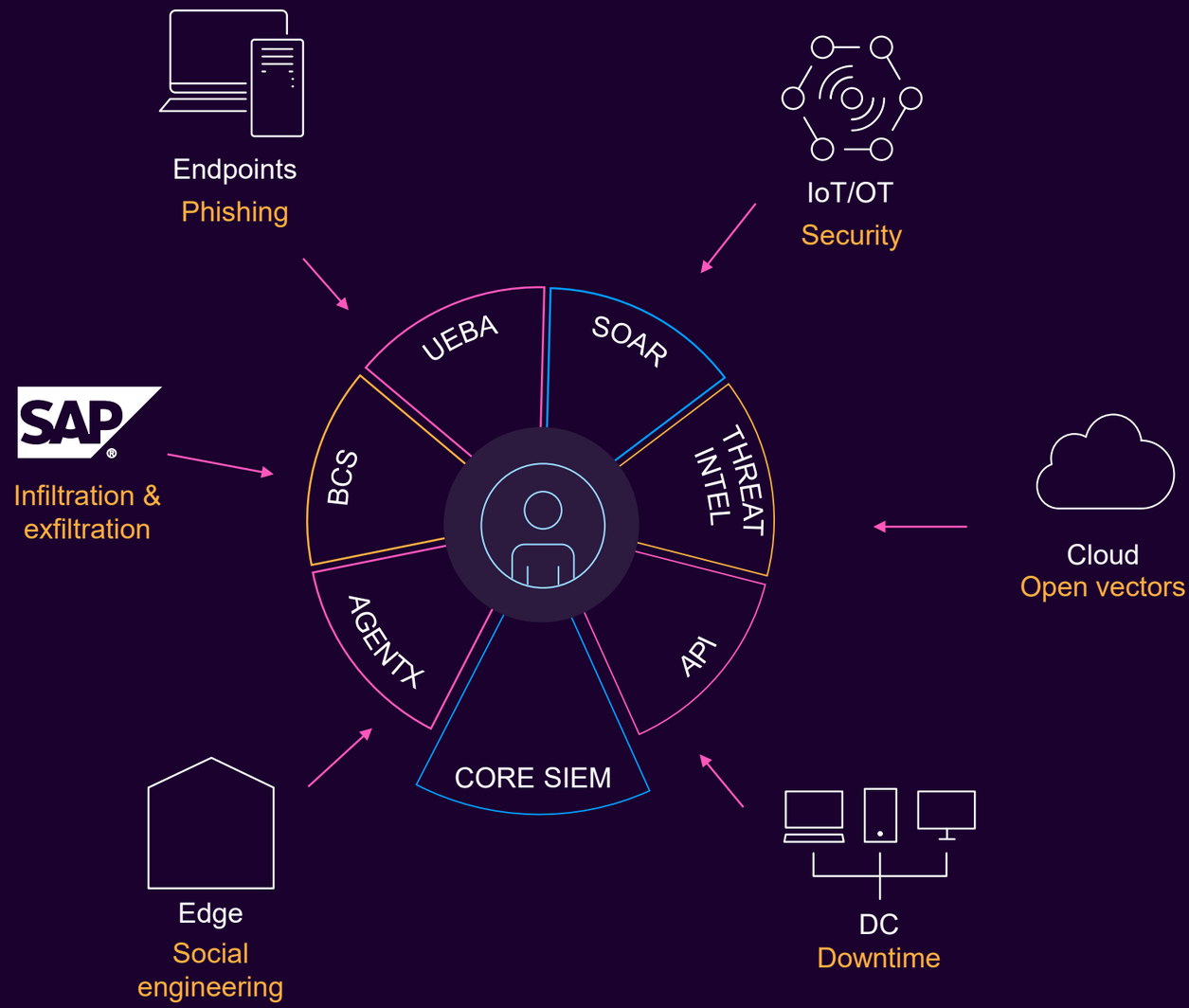
- **Bei 56 Prozent der deutschen Unternehmen steigt das Budget für Cyber Security 2024**
- **Investition in Cybersicherheit ein Muß**
- **2,7 Millionen offene Jobs benötigen hohe Automatisierung (SOAR) und treiben Services**
- **Total cost of ownership wird zum Kaufkriterium**
- **Kunden kaufen ein “outcome”**

Erwartete Entwicklung des Cyber Security-Budgets bei deutschen Unternehmen



Quelle: PwC „Global Digital Trust Insights 2023“

ECOSYSTEME INTEGRIEREN JEDEN UND ALLES



INTEGRATION* ERFORDERT SYSTEMOFFENHEIT

*ergänzen, vervollständigen, sich zusammenschließen, in ein größeres Ganzes eingliedern' (18. Jh.)

Integration

Erweiterte Möglichkeiten

Werkzeugeinsatz vereinfachen

Erhöhung der Skalenerträge

Bedrohungen aufspüren und jagen

Verbesserung der Sicherheitslage

Sicherheitsanalytik

Leichte Bereitstellung von Inhalten

Validierung

Konsistenz & Reproduzierbarkeit

VIELEN DANK