Cybersecurity – Eine Herausforderung

Ronny Globisch

Senior Sales Engineer

SOPHOS

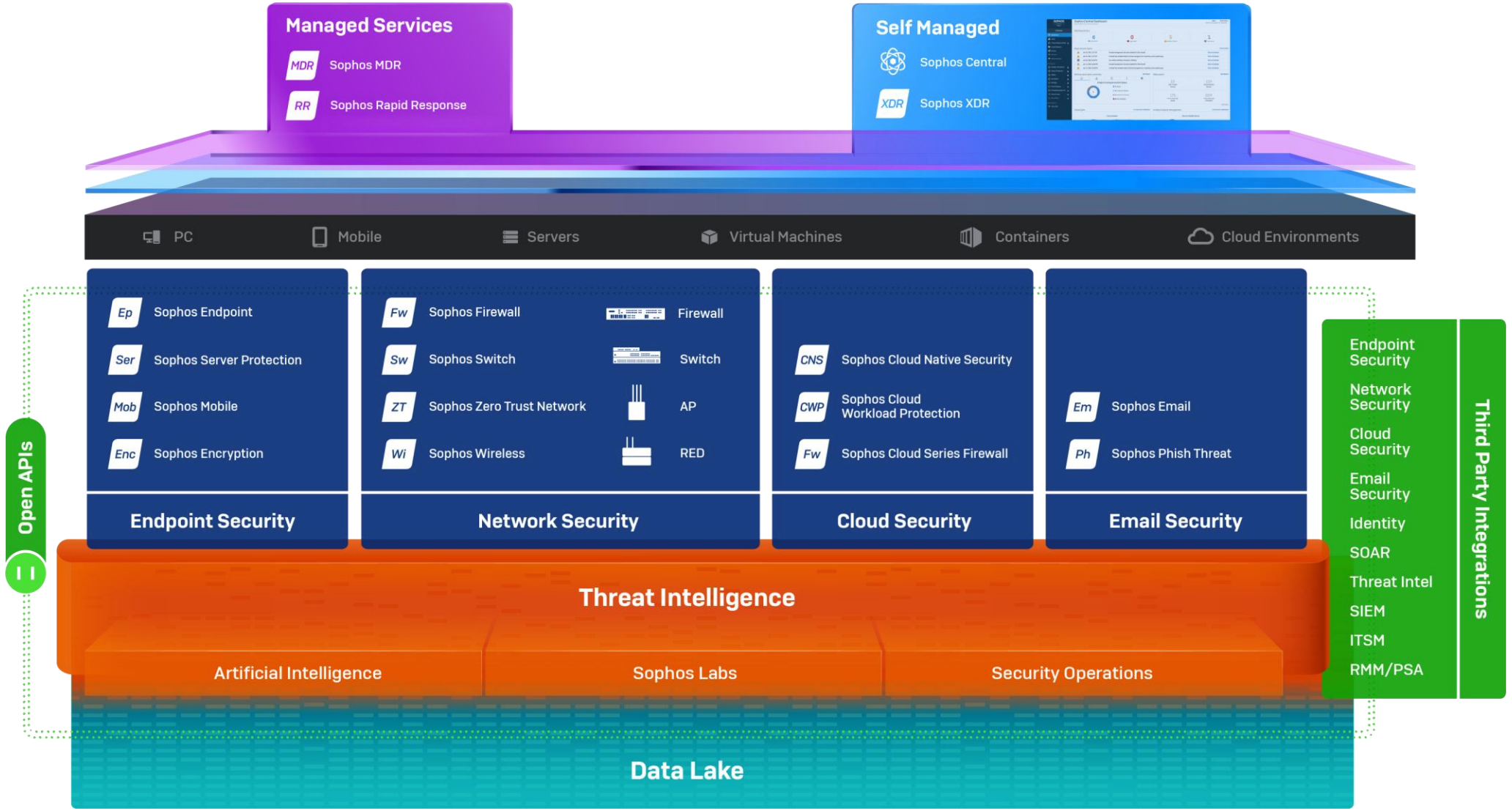
Welche Ziele verfolgen Cyberkriminelle?

- Wirtschaftsspionage
- Politik
- Datenmissbrauch
- Erpressung
- usw…

Cybersecurity – heute !

- komplex
- reaktiv
- Unübersichtlich
- inkompatibel
- usw…

Adaptive Cybersecurity Ecosystem - ACE



SOPHOS

Wer sagt, dass ich das wirklich brauche?

- Cyberrisikenversicherer
- DSGVO
- Regulierungsbehörden
- Während eines Vorfalls: **Jeder** wünscht, es wäre schon da gewesen

Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2021

3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

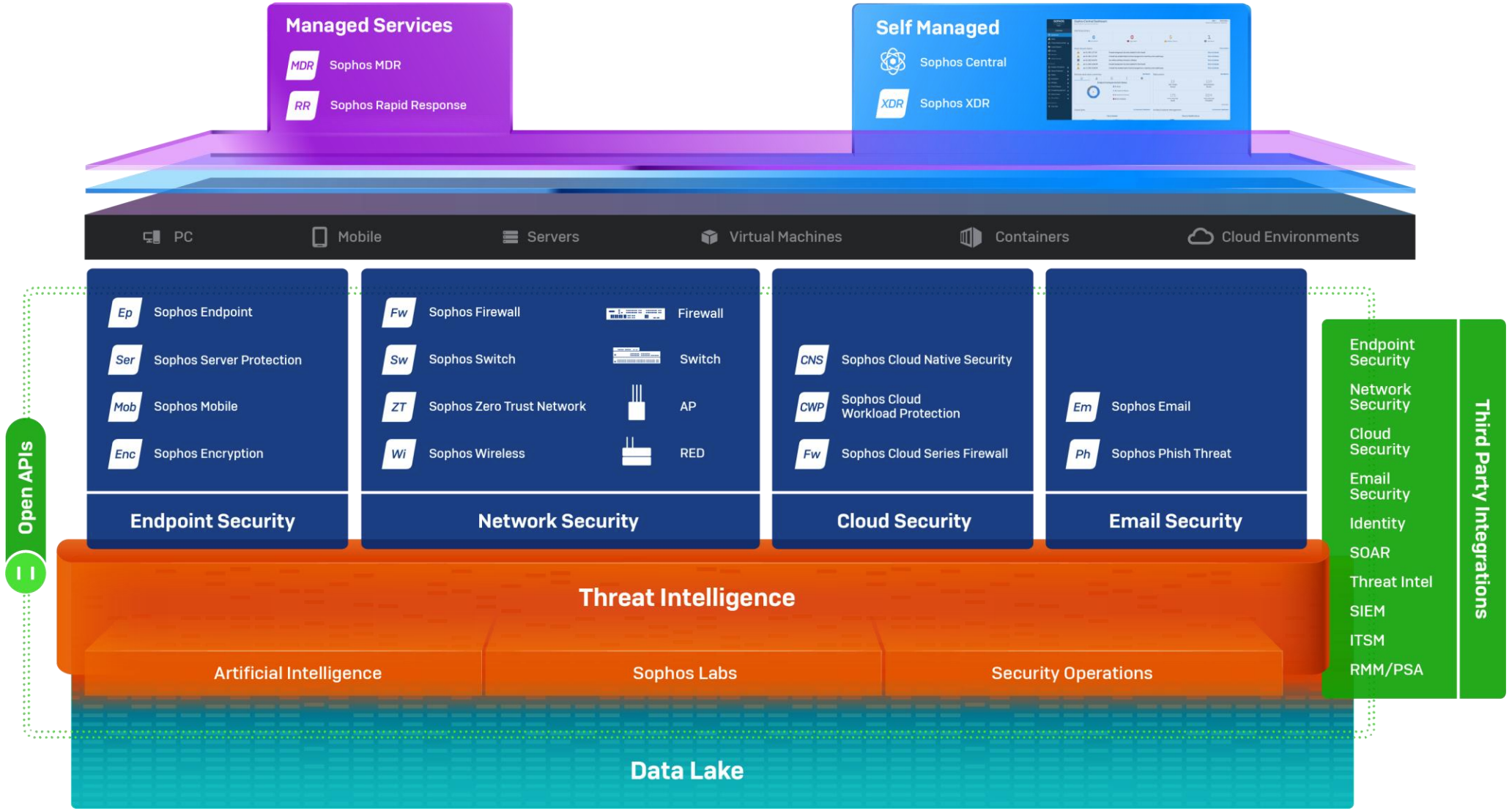
Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

EDR-Plattformen kombinieren wirksame Detektions- und Präventionstechniken, um die Kompromittierung von Clients und Servern, auch über Computer und Betriebsystemgrenzen hinweg, zu verhindern und sogar aktive Angreifer in Computernetzen zu enttarnen.

https://www.stand-der-technik-security.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

SOPHOS

Adaptive Cybersecurity Ecosystem - ACE



SOPHOS

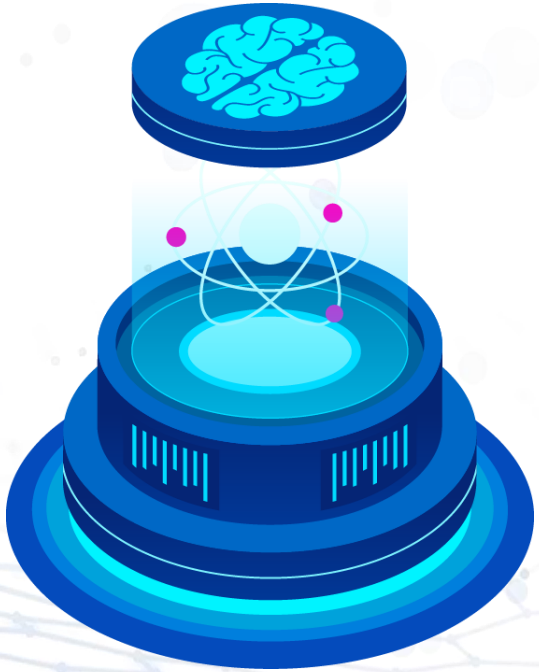
Endpoint Detection & Response

SOPHOS

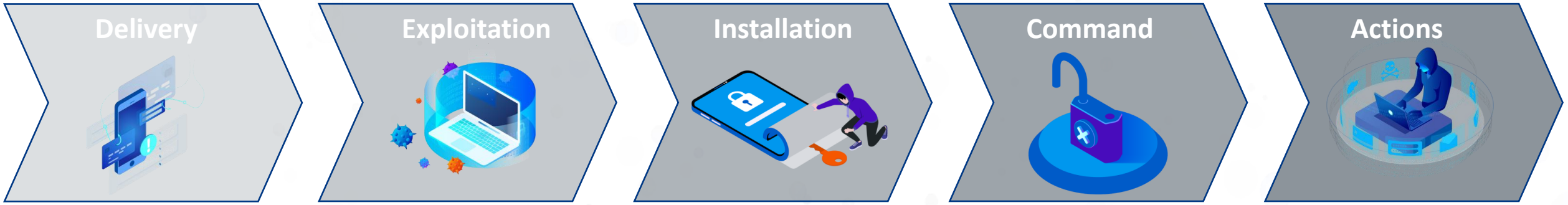
Prävention optimieren

Angriffsfläche reduzieren

Verhindern, dass Angriffe ausgeführt werden



Optimize Prevention



Pre

- Web Control
- Web Protection
- Intrusion Prevention System
- Peripheral Control
- Download Reputation

- Local Privilege Mitigation
- Application Lockdown
- Side Loading
- CTF Protocol
- Code Mitigations
- Memory Mitigations
- APC Mitigations

Post

- Pre-execution Behavior
- Machine Learning
- Live Protection
- Anti-Malware
- Clean and Block
- Server Lockdown
- Process Protections
- PUA
- Application Control

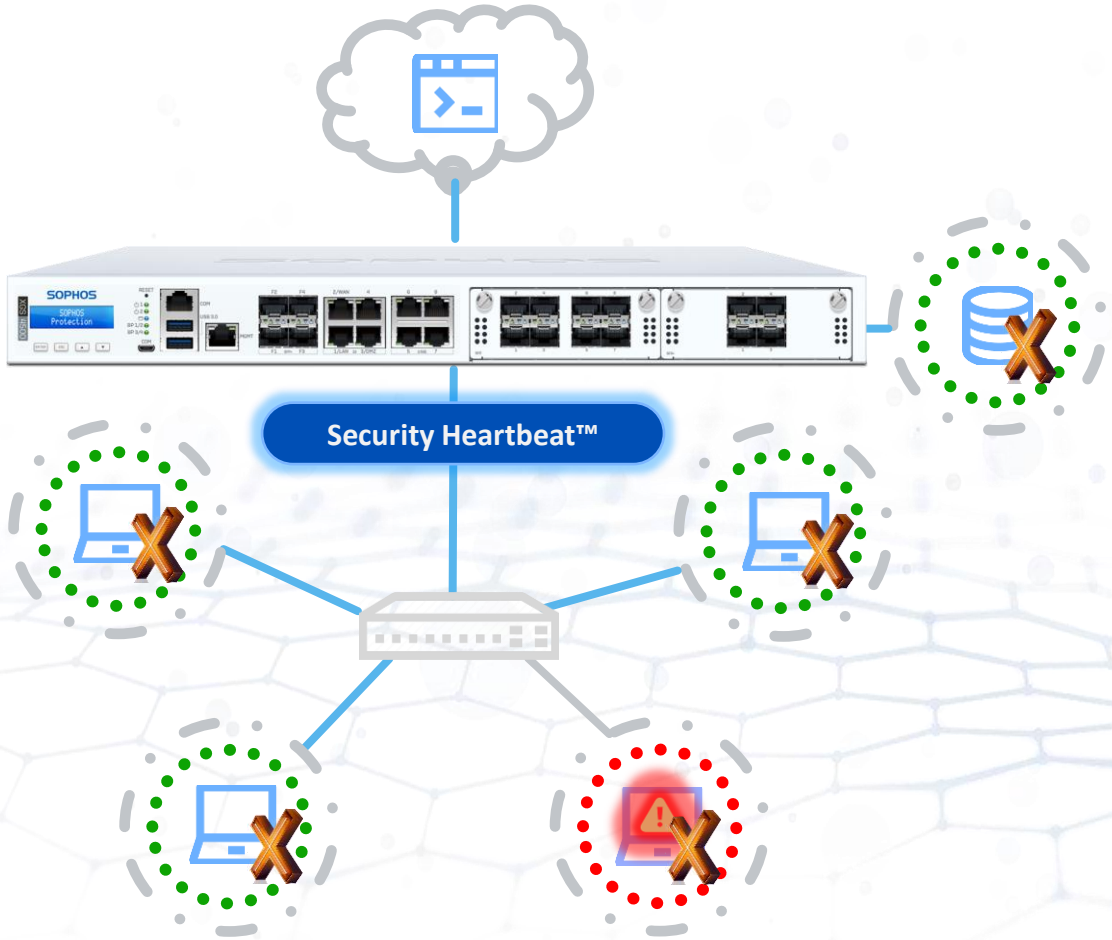
- Credential Theft Protection
- Dynamic Shellcode
- Safe Browsing
- Malicious Traffic Detection

- Runtime Behavior Analysis
- Data Loss Prevention
- MFA Cookie
- Server FIM
- Anti-Ransomware
- Automatic + Manual client isolation

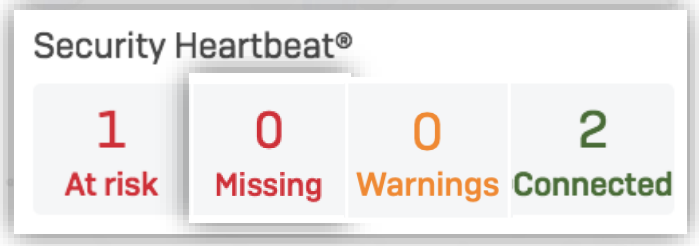
Synchronized Security

1# Schritt

Automatische Reaktion auf Bedrohungen und Sicherheitsverstöße

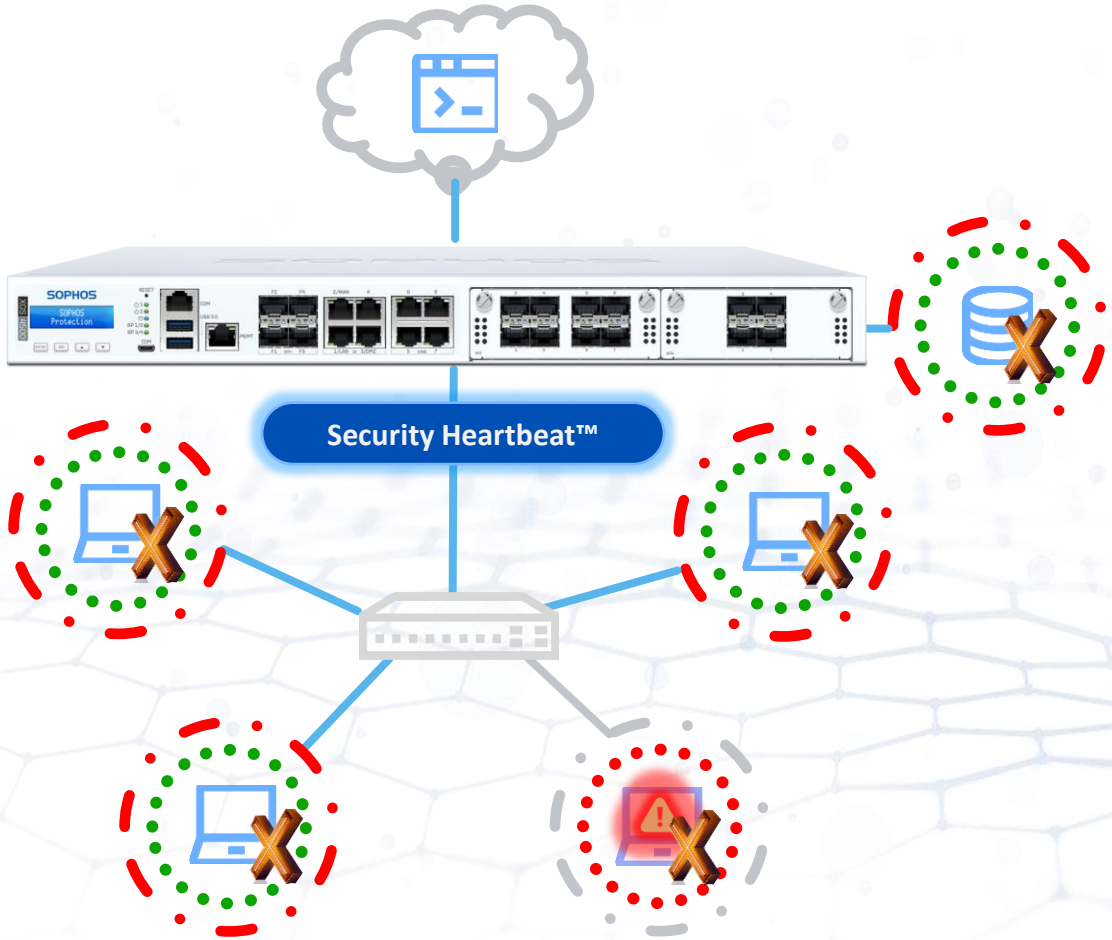


1 **Bedrohung identifiziert**

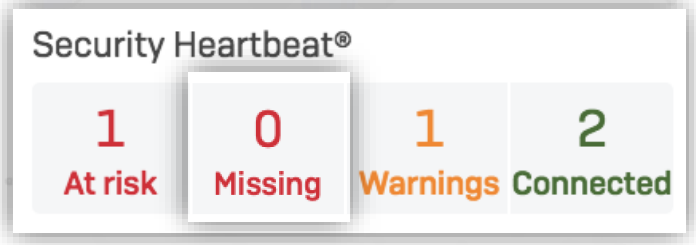


SOPHOS

Automatische Reaktion auf Bedrohungen und Sicherheitsverstöße

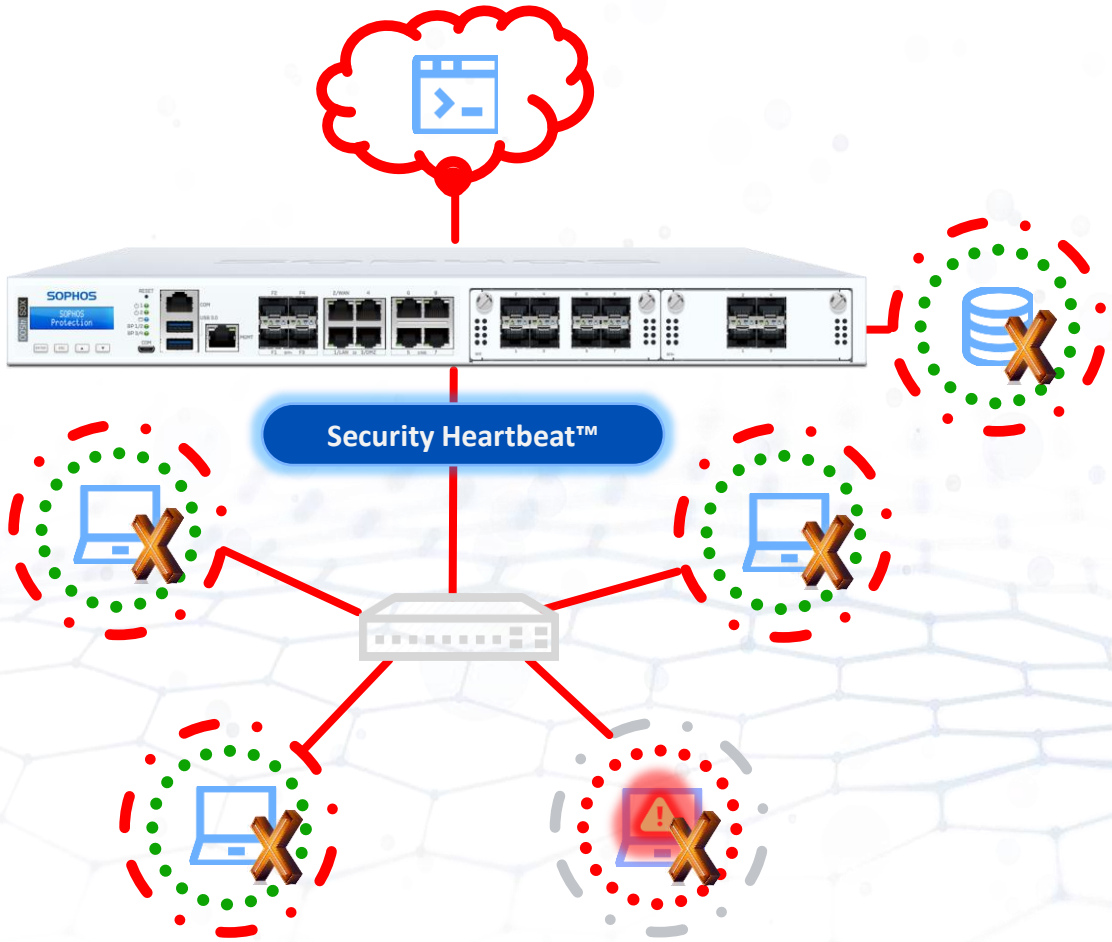


1 **Bedrohung identifiziert**

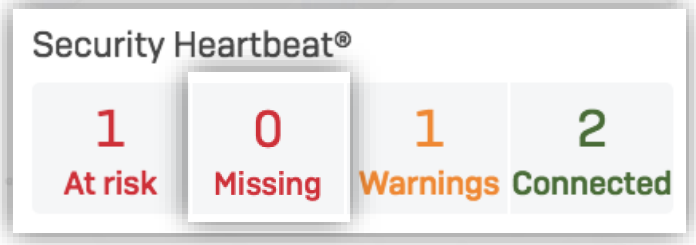


2 **Lateral Movement Protection**

Automatische Reaktion auf Bedrohungen und Sicherheitsverstöße



1 **Bedrohung identifiziert**



2 **Lateral Movement Protection**

3 **Kompromitierte Endgeräte isolieren**

SOPHOS

eXtended Detection & Response

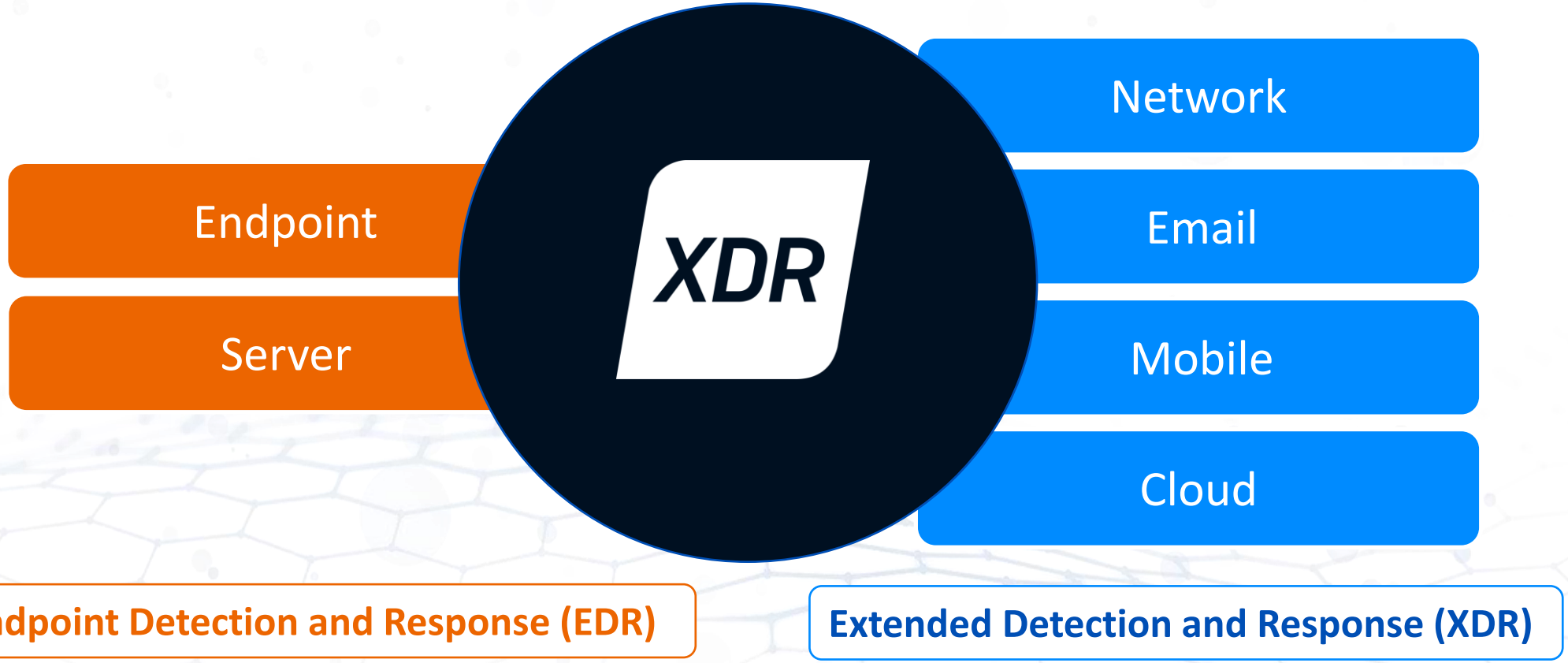
SOPHOS

Stoppen Sie mehr Bedrohungen schneller

PRÄVENTION OPTIMIEREN

MINIMIEREN SIE DIE ZEIT ZUM ERKENNEN UND REAGIEREN

Sensoren in jedem Bereich


Endpoint
Server
XDR
Network
Email
Mobile
Cloud
Endpoint Detection and Response (EDR)
Extended Detection and Response (XDR)

XDR – Endpoints/Server + Firewall + Email +..

Intercept X with XDR

Data Lake 7 Tage frei

Central XDR

+30 Tage Daten im Data Lake

+ Zugriff auf Central Firewall Reporting Daten und weitere Produkte

Ereignisse, Status

Abfragen live/geplant
LiveResponse

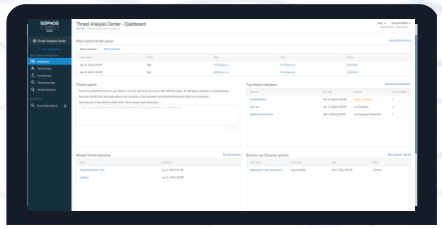
Logdaten

Logdaten

Logdaten, Status

Central Admin
Zugriff

Programm-
gesteuerter
Zugriff



Ep **Sophos Endpoint**
Intercept X

Fw **Sophos Firewall**

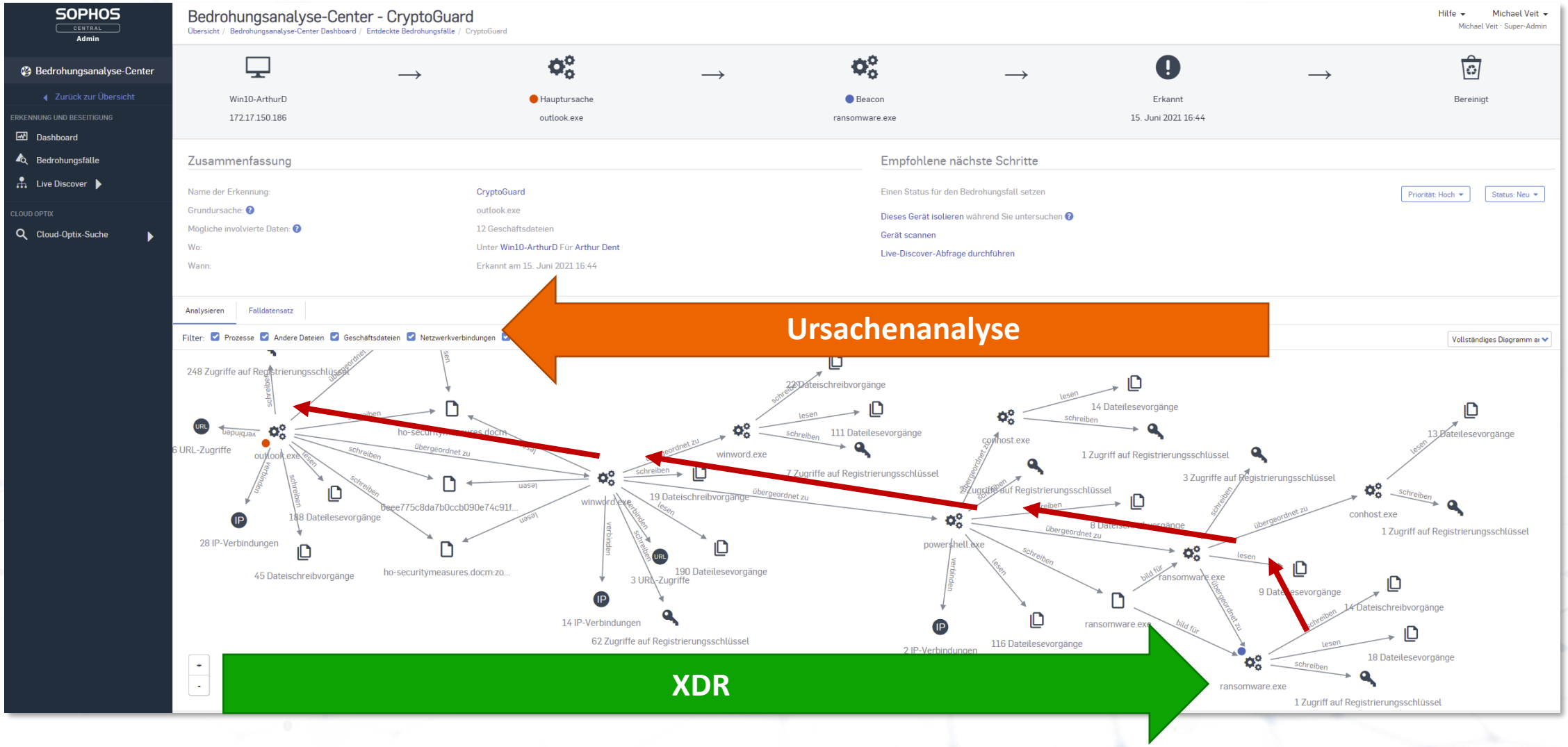
Em **Sophos Email**

Mb **Sophos Mobile**

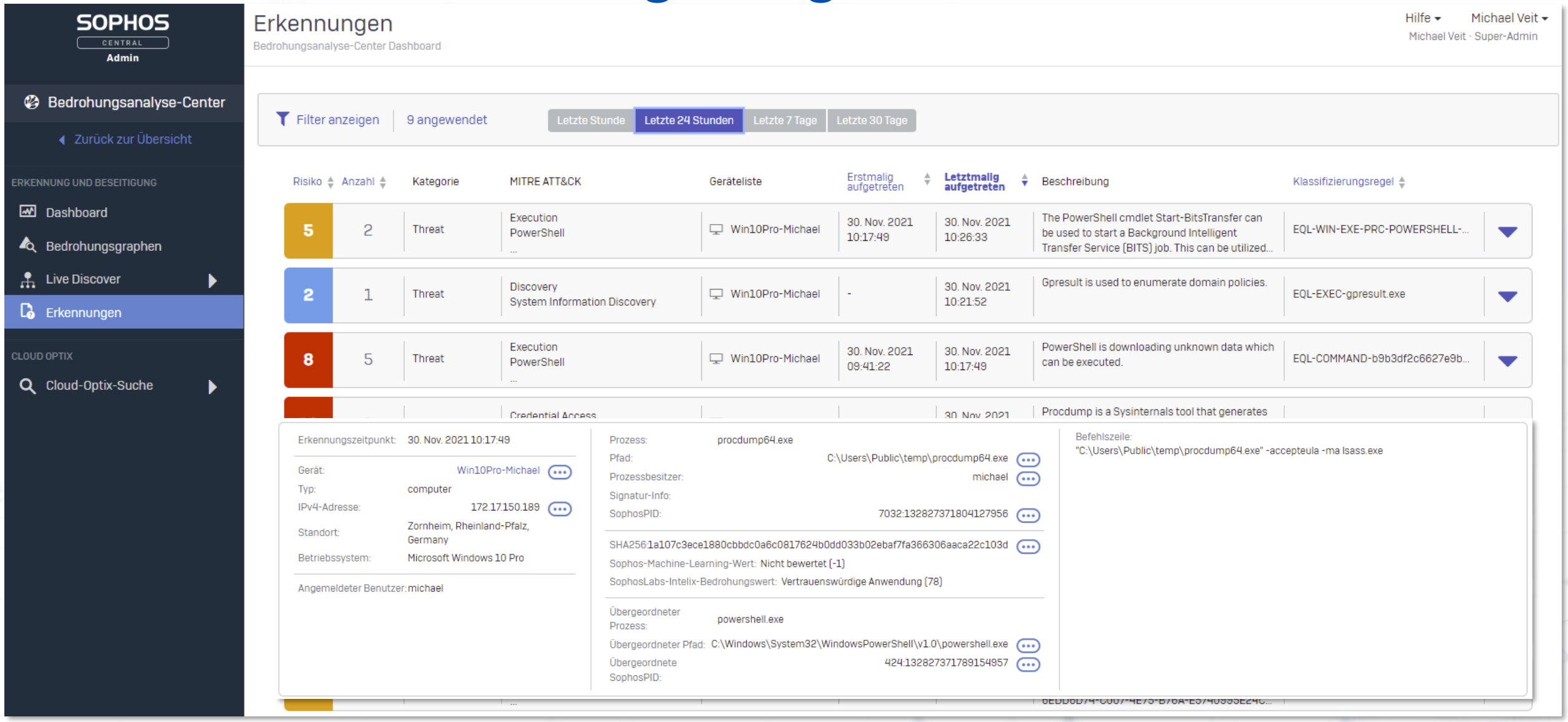
Cld **Sophos Cloud**
Cloud Optix

SOPHOS

Sophos XDR


SOPHOS
CENTRAL
Admin
Bedrohungsanalyse-Center
Zurück zur Übersicht
ERKENNUNG UND BESEITIGUNG
Dashboard
Bedrohungsfälle
Live Discover
CLOUD OPTIX
Cloud-Optix-Suche
Bedrohungsanalyse-Center - CryptoGuard
Übersicht / Bedrohungsanalyse-Center Dashboard / Entdeckte Bedrohungsfälle / CryptoGuard
Hilfe
Michael Veit
Michael Veit · Super-Admin
Win10-ArthurD
172.17.150.186
Hauptursache
outlook.exe
Beacon
ransomware.exe
Erkannt
15. Juni 2021 16:44
Bereinigt
Zusammenfassung
Name der Erkennung:
CryptoGuard
Grundursache:
outlook.exe
Mögliche involvierte Daten:
12 Geschäftsdateien
Wo:
Unter Win10-ArthurD Für Arthur Dent
Wann:
Erkannt am 15. Juni 2021 16:44
Empfohlene nächste Schritte
Einen Status für den Bedrohungsfall setzen
Priorität: Hoch
Status: Neu
Dieses Gerät isolieren während Sie untersuchen
Gerät scannen
Live-Discover-Abfrage durchführen
Analysieren
Falldatensatz
Filter:
Prozesse
Andere Dateien
Geschäftsdateien
Netzwerkverbindungen
Vollständiges Diagramm a
Ursachenanalyse
XDR
248 Zugriffe auf Registrierungsschlüssel
6 URL-Zugriffe
outlook.exe
28 IP-Verbindungen
188 Dateilesevorgänge
45 Dateischreibvorgänge
ho-securitymeasures.docm:zo...
22 Dateischreibvorgänge
111 Dateilesevorgänge
winword.exe
7 Zugriffe auf Registrierungsschlüssel
19 Dateischreibvorgänge
190 Dateilesevorgänge
3 URL-Zugriffe
14 IP-Verbindungen
62 Zugriffe auf Registrierungsschlüssel
14 Dateilesevorgänge
conhost.exe
1 Zugriff auf Registrierungsschlüssel
2 Zugriffe auf Registrierungsschlüssel
powershell.exe
2 IP-Verbindungen
116 Dateilesevorgänge
ransomware.exe
3 Zugriffe auf Registrierungsschlüssel
13 Dateilesevorgänge
conhost.exe
1 Zugriff auf Registrierungsschlüssel
9 Dateilesevorgänge
14 Dateischreibvorgänge
18 Dateilesevorgänge
ransomware.exe
1 Zugriff auf Registrierungsschlüssel

KI identifiziert verdächtige Ereignisse



Überprüfung auf verdächtige Nutzung von Systemtools mit EDR

IoC Hunt new (Datalake) Ergebnisse der Abfrage

Mitre_ID	Tactic	Technique	SubTechnique	Instances	Process_Name	Cmd_Line	User_List
T1033	Discovery	System Owner/User Discov...	GetActiveUser	3	whoami.exe	whoami /groups	arthur
T1033	Discovery	System Owner/User Discov...	GetActiveUser	3	cmd.exe	cmd.exe /c whoami /groups	arthur
T1049	Discovery	System Network Connectio...		2	powershell.exe	powershell.exe -ExecutionPolicy Restricted -Command $res = 0; if(ge...	SYSTEM
T1063	discovery	Security Software Discovery	Discover antivirus programs	2	WMIC.exe	WMIC.exe /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProdu...	arthur
T1003	Credential-access	Credential Dumping		2	reg.exe	reg query HKLM /f password /t REG_SZ /s	arthur
T1069	discovery	Permission Groups Discovery	Permission Groups Discovery	2	gpresult.exe	gpresult /r	arthur
T1063	discovery	Security Software Discovery	Discover antivirus programs	2	WMIC.exe	WMIC.exe /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProdu...	arthur
T1077	lateral-movement	Windows Admin Shares	Net use	1	net.exe	net use \\172.17.150.189\c$ /user:administrator@sophos SpaceInva...	SYSTEM
T1003	Credential-access	Credential Dumping		1	reg.exe	reg query HKLM\sam /f password /t REG_SZ /s	arthur
T1531	Impact	net	Account creation	1	net.exe	net user /add backupadmin Passw0rd!	SYSTEM
T1047	lateral-movement	Windows Management Instr...	Start remote process (WMI)	1	WMIC.exe	wmic /node:172.17.150.189 /user:sophos\administrator /password:...	SYSTEM
T1003	Credential-access	Credential Dumping		1	reg.exe	reg save HKLM\sam C:\Users\Arthur\AppData\Local\Temp\sam	arthur
T1047	execution	Windows Management Instr...	Remote Execution	1	WMIC.exe	wmic /node:172.17.150.189 /user:sophos\administrator /password:...	SYSTEM
T1003	Credential-access	Credential Dumping		1	reg.exe	reg query HKLM%/f password% /t REG_SZ\x1B	arthur

Erkennung verwundbarer Applikation durch Live-Abfrage der CVE-Datenbank

Anfrage : Vulnerability Scanner in a query

‹ Zurück zu Kategorien / Alle Abfragen

Vulnerability Scanner in a query

Bearbeiten | Speichern | Löschen

Alle Abfragen: Vulnerability Scanner in a query

Erstellt von Admin - MFA

Quellen

Windows

Erwartete Leistung

Schlecht — Hervorragend

0 Übertragene Daten (Kb)

Klein — Gro

SQL

```
SELECT
   publisher,
   CAST(name AS TEXT) || ' ' || version Application,
   url 'Identified CVE List'
FROM program_list
   JOIN curl ON
      url = 'ht
         || re
         || '%
         || re
         || '%
         || pr
```

CVE Vulnerability Scanner in a query Ergebnisse der Abfrage

epName	publisher	Applica	
Idefix	Irfan Skiljan	IrfanView 4 50 (64-bit) 4.50	https://www.cvedetails.com/v...

CVE Details

The ultimate security vulnerability datasource

Log In Register

Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ

Irfanview » Irfanview » 4.50 ~~~x64~~ : Vulnerability Statistics

Vulnerabilities (33) Related Metasploit Modules (Cpe Name:*cpe:/a:irfanview:irfanview:*

Vulnerability Feeds & Widgets

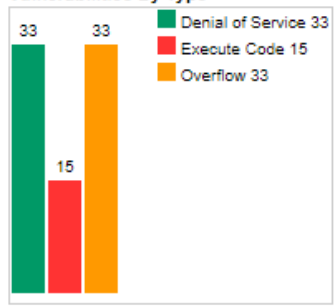
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS
2017	33	33	15	33			
Total	33	33	15	33			
% Of All		100.0	45.5	100.0	0.0	0.0	0.0

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and ch
years.)

Vulnerabilities By Year

Vulnerabilities By Type



SOPHOS

Sophos Lösungen und Services

Schutz + Detection & Response

Do it yourself?

Werkzeug

EDR Endpoint Detection and Response) ist ein ganzheitlicher Ansatz der Endpoint/Server Sicherheit

XDR (eXtended Detection and Response) ermöglicht produktübergreifende Korrelation von Ereignissen

Denken Sie, was ich denke?

- Wow, das ist echt ein mächtiges Werkzeug
- Ich wusste gar nicht, was alles möglich ist
- ……

Wer, Wie und Wann ???

Sophos MDR

Das Ergebnis zählt - rundum sicher durch Cybersecurity als Service

SOPHOS

Was ist Managed Detection and Response (MDR)?

Ein vollständig verwalteter Rund-um-die-Uhr-Service der von Experten bereitgestellt wird, die darauf spezialisiert sind, Cyberangriffe zu erkennen und darauf zu reagieren, die Technologielösungen allein nicht verhindern können

SOPHOS MDR: Offen und flexibel

Sophos MDR

Kompatibel mit Ihrer Umgebung
Wir nutzen Sophos Werkzeuge, die Werkzeuge anderer Anbieter – oder eine Kombination aus beiden

Kompatibel mit Ihren Anforderungen
Wir bieten komplettes Incident Response - oder Unterstützung für Ihr Team

Kompatibel mit Ihrem Unternehmen
Unser Team hat umfangreiche Erfahrung mit Angriffen auf Unternehmen aller Branchen

SOPHOS

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint

Microsoft, CROWDSTRIKE, McAfee, SentinelOne, CHECK POINT, TREND MICRO, Malwarebytes, BlackBerry CYLANCE

Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO

Network

DARKTRACE, Forcepoint

Erweiterte Telemetrie ermöglicht Sophos tiefe Einblicke

Sensoren

- Identity
- Cloud SaaS
- Firewall
- Network
- Email
- Endpoint

Data Lake

Geräte- und technologieübergreifende Aktionen
Ereigniskorrelation

Public Cloud
Ereignisse an unterschiedlichen Orten

Ungeschützte Geräte
Kommunikation von Geräten ohne XDR-Schutz

Mehrstufige Angriffe
Phishing -> Übernahme von Accounts -> Ausbreitung

Verschlüsselter Netzwerkverkehr
Network Detection and Response (NDR)

Analyse

Aktive Bedrohungen

Sophos MDR nutzt Daten folgender Integrationen kostenfrei

Sophos XDR

Die einzige XDR-Plattform, die native Endpunkt-, Server-, Firewall-, Cloud-, E-Mail-, Mobil- und Microsoft-Integrationen vereint.

Sophos Firewall

Überwachung und Filterung des ein- und ausgehenden Netzwerkverkehrs, um aktuelle Bedrohungen zu stoppen, bevor sie Schaden anrichten.

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint Protection

Blockieren Sie aktuelle Bedrohungen und erkennen Sie böswillige Verhaltensweisen - einschließlich Angreifern, die sich als legitime Benutzer ausgeben.

Sophos Network Detection and Response

Überwachen Sie kontinuierlich die Aktivitäten innerhalb Ihres Netzwerks, um verdächtige Aktionen zwischen Geräten zu erkennen, die sonst unbemerkt bleiben.

Third-Party Endpoint Protection

Kompatibel mit...

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Sophos Cloud

Sichern Sie Ihre Cloud Ressourcen und gewinnen Sie Transparenz über Ihre wichtigen Cloud-Dienste, einschließlich AWS, Azure und Google Cloud Platform.

Sophos Email

Schützen Sie Ihren Posteingang vor Malware und profitieren Sie von der fortschrittlichen KI, die gezielte Imitations- und Phishing-Angriffe.

90-Tage Datenhaltung

SOPHOS

Sophos MDR Add-On Integrationen für schnellste Reaktion

Firewall

Kompatibel mit...

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

Public Cloud

Kompatibel mit...

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

Identity

Kompatibel mit...

- Okta
- Duo

Network Security

Kompatibel mit...

- Darktrace
- Forcepoint
- McAfee (web gateway)

Email

Kompatibel mit...

- Proofpoint
- Mimecast

1-Jahr Datenhaltung

Alle Integration Packs sind für Sophos MDR, Sophos MDR Complete und Sophos Threat Advisor verfügbar.
Die Datenhaltung ist für Sophos MDR und Sophos XDR erhältlich.
Alle Integration Packs müssen entsprechend der Anzahl der Sophos MDR-Lizenzen des Kunden erworben werden.

Zusammenarbeit mit dem MDR - Team

Benachrichtigung

Sophos: *„Auf diesen 10 Rechnern haben wir einen Angriff mit folgenden Aktivitäten festgestellt.“*

Kunde: *„Danke, wir übernehmen."*

Zusammenarbeit

Sophos: *„Sollen wir in diesem Fall den Angriff stoppen?“*

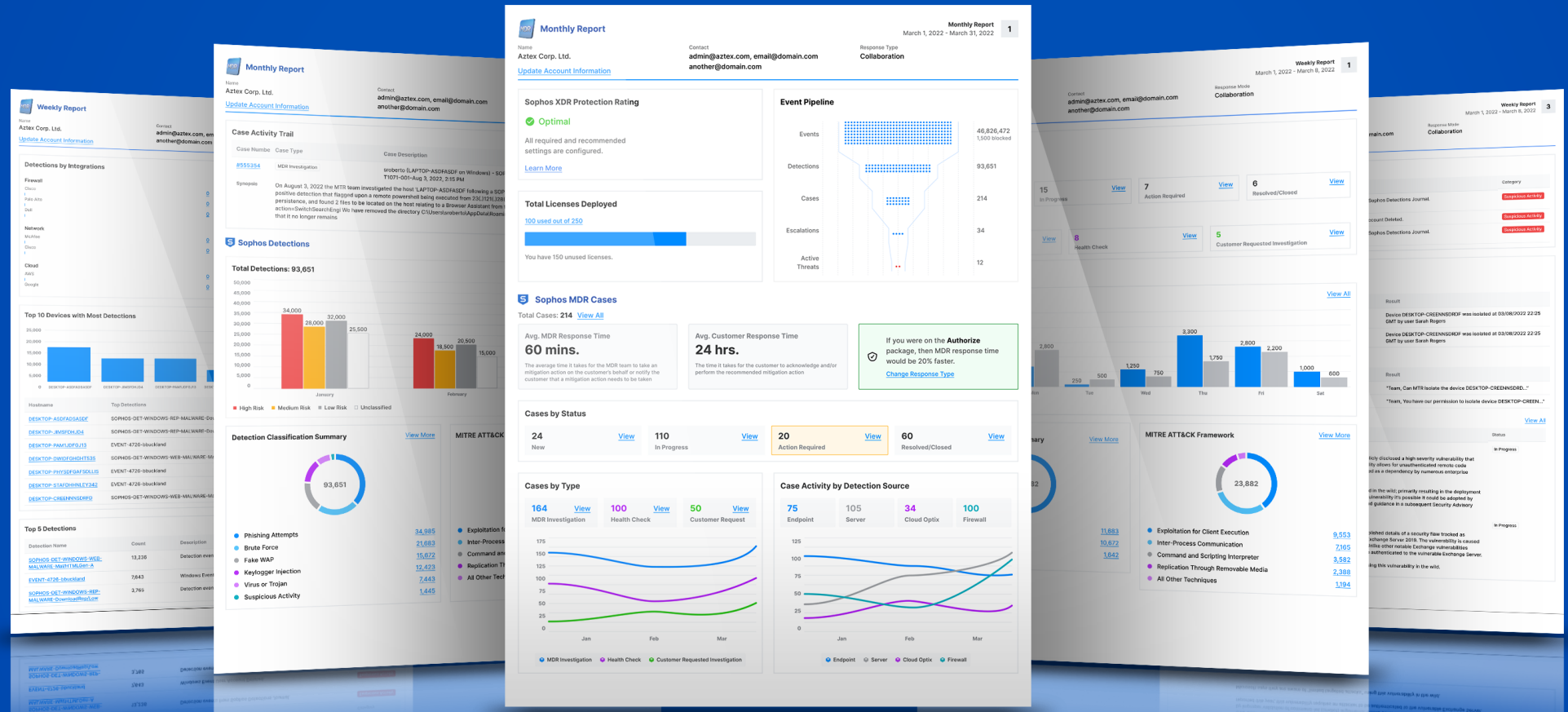
Kunde: *„Ja bitte, aber während der Geschäftszeiten immer nachfragen, dafür nachts und am Wochenende bitte sofort loslegen!"*

Autorisierung

Kunde: *„Sophos, bitte stoppt jeden eindeutigen Angriff!“*

Sophos: *„Wird gemacht."*

Managementtaugliche Cybersecurity Reports



SOPHOS

Sophos Lösungen und Services

Schutz + Detection & Response

EDR (Endpoint Detection and Response) ist ein ganzheitlicher Ansatz der Endpoint/Server Sicherheit

Do it yourself?

Werkzeug

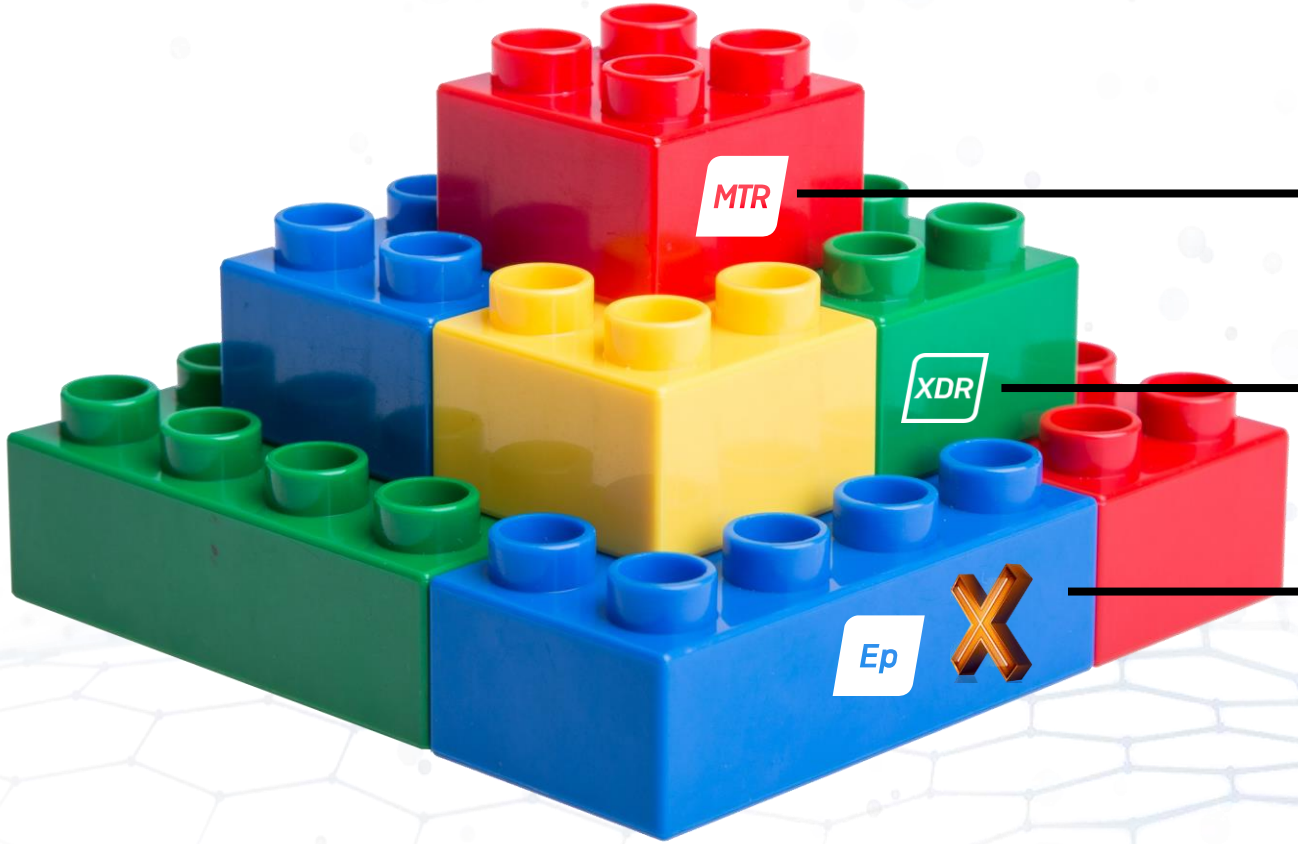
Outsourcing?

+ Service

Managed Detection & Response

SOPHOS

Sophos ACE - Funktionspyramide



- Managed SOC
  (Intercept X Advanced mit MTR)
- Sichtbarkeit und Reaktion
  (Intercept X Advanced mit XDR)
- Bester Endpoint-Schutz
  (Intercept X Advanced)

Sophos Central

Sophos Rapid Response

Blitzschnelle Unterstützung bei aktiven Bedrohungen durch ein weltweites Expertenteam von Spezialisten

rapidresponse@sophos.com
+49 611 711 86766

SOPHOS Produkte Lösungen Partner Support

BSI stuft Sophos als qualifizierten APT-Response-Dienstleister ein

SOPHOS PRESS RELEASE

Nach intensiver Prüfung hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Sophos in seine Liste qualifizierter Dienstleister im Bereich APT aufgenommen.

Nach einem umfangreichen Prüfverfahren gehört Sophos nun der Liste qualifizierter APT-Response-Dienstleister (**A**dvanced **P**ersistent **T**hreat, kurz APT) für KRITIS-Unternehmen an. Diese Übersicht unterstützt Betreiber kritischer Infrastrukturen dabei, ohne großen Rechercheaufwand geeignete Service-Unternehmen zu identifizieren, die in der Lage sind, getarnte Cyberattacken, die über einen längeren Zeitraum ein Netz oder System angreifen, aufzudecken und zu stoppen.

Neben der von den geprüften Unternehmen zur Verfügung gestellten Dokumentation über ihre Services steht vor allem der Praxisbezug beim Auswahlverfahren im Fokus. In einem mehrstündigen Termin beim BSI müssen zertifizierte Dienstleister anhand fiktiver Szenarien wie zum Beispiel einer Ransomware-Attacke oder einer Phishing-Kampagne zeigen, dass sie in der Lage sind, die angesprochenen Problemstellungen fach- und zielgerichtet zu lösen. Dabei achten die Experten sowohl auf das allgemeine Vorgehen des Dienstleisters als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen.

Über Sophos

Sophos ist ein weltweit führender Next-Gen-Cybersecurity-Anbieter und schützt über 500.000 Organisationen und Millionen von Kunden in mehr als 150 Ländern vor komplexen Cyberbedrohungen. Mit Threat Intelligence, KI und Machine Learning aus den SophosLabs und SophosAI bietet Sophos ein breites Portfolio modernster Produkte und Services. Diese schützen Benutzer, Netzwerke und Endpoints zuverlässig vor Malware, Exploits, Phishing und anderen Cyberangriffen. Mit Sophos Central hat Sophos eine zentrale, cloudbasierte Management-Konsole im Angebot. Sie bildet das Herzstück unseres adaptiven Cybersecurity-Ökosystems. Teil dieses Systems ist ein zentralisierter Data Lake. Er nutzt eine Vielzahl offener APIs, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung

SOPHOS