Zukunftssichere IT-Security

Michael Veit
Technology Evangelist, Sophos

SOPHOS

Fürchten Sie sich davor?

Hacker vor 5 Jahren

Hacker heute

State of Ransomware 2022

VansonBourne

66%

der SMB wurden im letzten Jahr mit Ransomware angegriffen

65%

der angegriffenen Unternehmen hatten danach verschlüsselte Daten

30 Tage

hatten die Opfer keine voll funktionsfähige IT

90%

der Opfer hatten Einschränkungen der Produktion

$1.7M

Schaden pro Vorfall, vor allem durch Betriebsausfall

Quelle: The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos

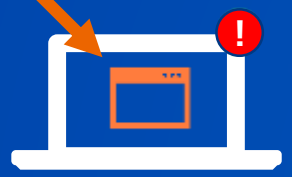
SOPHOS

Sieht Ihr Netzwerk so aus?

= verwaltet, EPP, gepatcht, aktuelles OS

..oder so?

"Tolles Tool" vom User selbst installiert

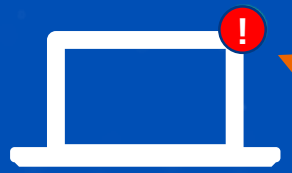


WLAN-Webcam, noch nie upgedatet

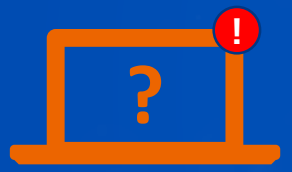
Privates älteres Android ohne Updates, ohne AV

Mitarbeiter, der auf jeden Link und Anhang klickt

Win7-Notebook "im Schrank"



"später neu starten" geklickt



Privates Notebook

Reboot erst im nächsten Wartungsfenster

Server2003/2008 mit alter Software

Drucker/Scanner/Kopierer mit Windows Embedded ohne AV und Updates

Entwickler-Workstation mit vielen Scan-Ausnahmen

Maschinensteuerung mit NT 4.0/Win2000

= unsicher

= verwaltet, EPP, gepatcht, aktuelles OS


..oder so?
WLAN-Webcam,
noch nie upgedatet
Privates älteres Android
ohne Updates, ohne AV
"Tolles Tool" vom
User selbst installiert
Mitarbeiter, der auf
jeden Link und Anhang klickt
Win7-Notebook
"im Schrank"
..dann brauchen Sie
XDR
Privates Notebook
Server2003/2008
mit alter Software
Wartungsfenster
Drucker/Scanner/Kopierer
mit Windows Embedded
ohne AV und Updates
Maschinensteuerung
mit NT 4.0/Win2000
Entwickler-Workstation
mit vielen Scan-Ausnahmen
= unsicher
= verwaltet, EPP, gepatcht, aktuelles OS

Was ist Sophos XDR (eXtended Detection and Response)?

- Beste proaktive Schutztechnologien
- Erfassung, Analyse und Korrelation aller Technologien: Endpoint, Firewall, Cloud, Email, Netzwerk, Identität..
- Aussagefähigkeit
  - Cyberangriff?
  - Datenabfluss / Compliance-Verstoß?
  - Zustand der IT?
- Bei einem Vorfall: Fähigkeit zur Reaktion
- Automation - z.B. automatische Isolation unsicherer Systeme

EDR / XDR = „Stand der Technik“

Wer sagt, dass ich das brauche?

- Cyberrisiken-Versicherer
- Geschäftspartner, Zulieferer
- Compliance (DSGVO, SOX, PCI)

- Während eines Vorfalls… - jeder!

„Wäre es schon dagewesen!“

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

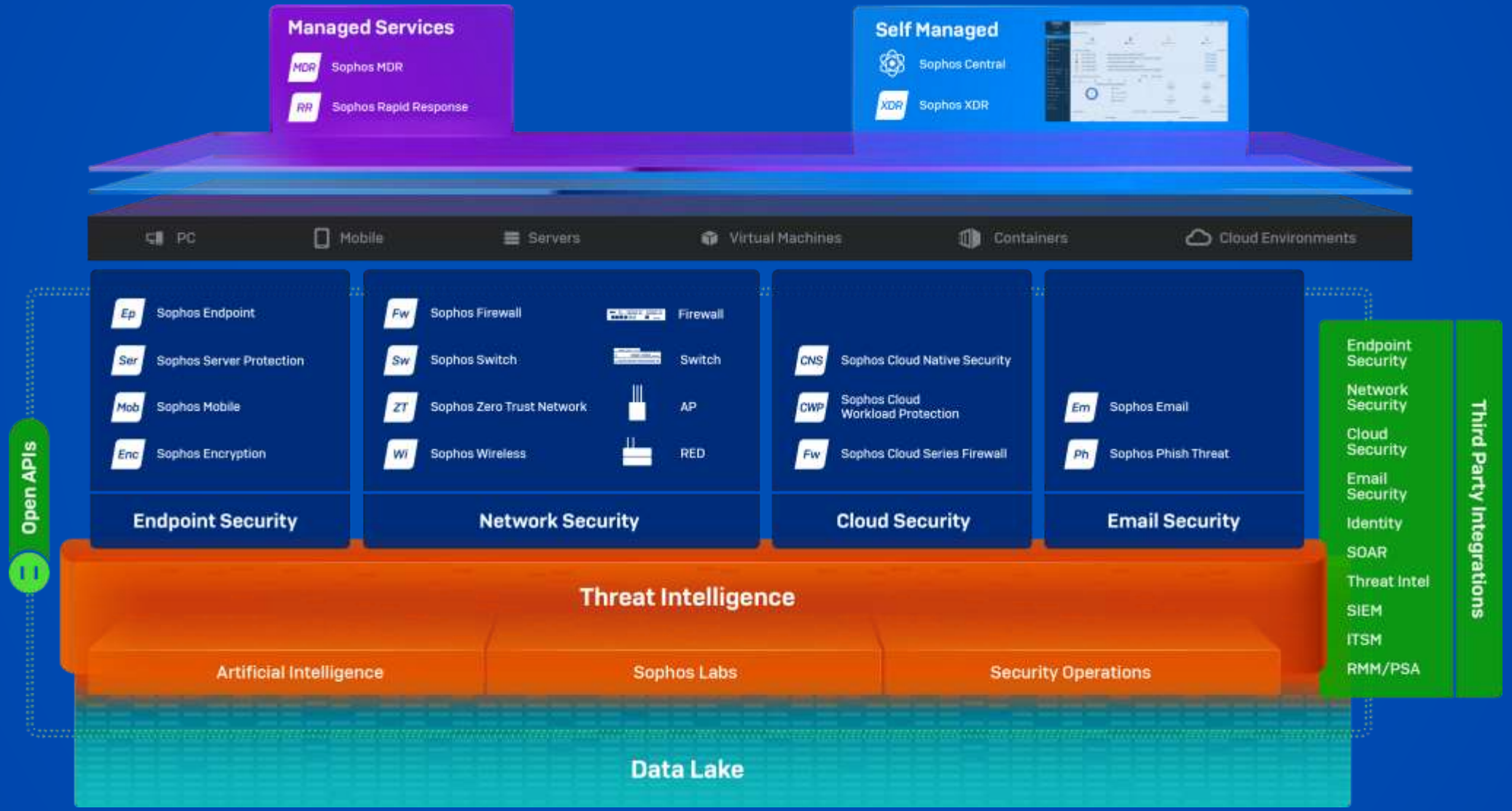
Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

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/2021-09_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

SOPHOS

SOPHOS Adaptive Cybersecurity Ecosystem - XDR



SOPHOS

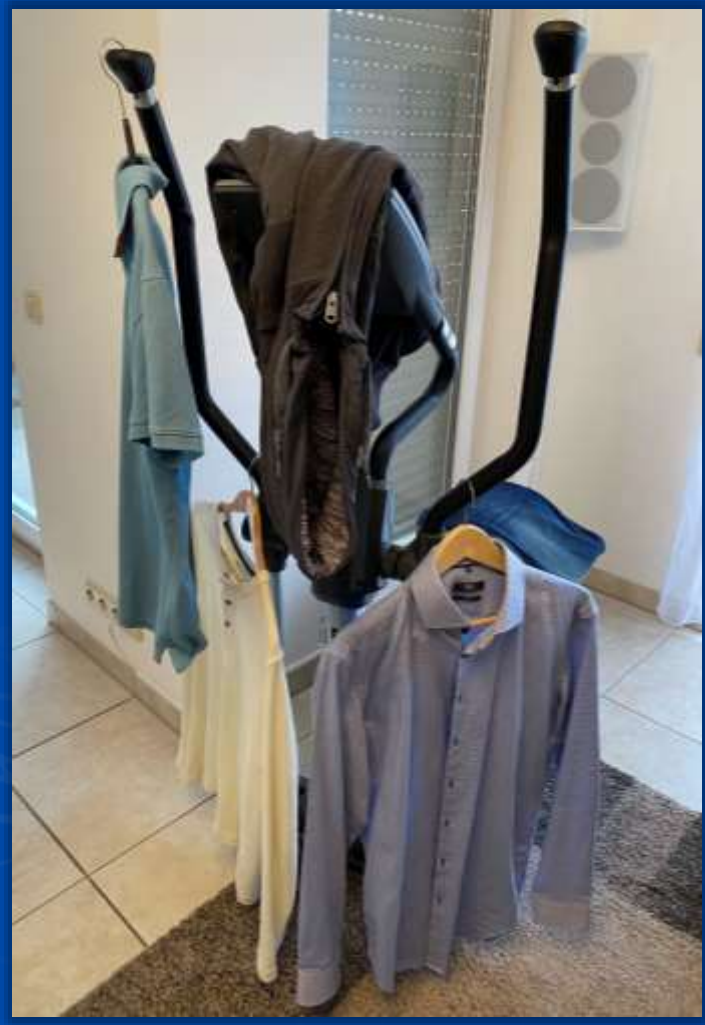
Technologie

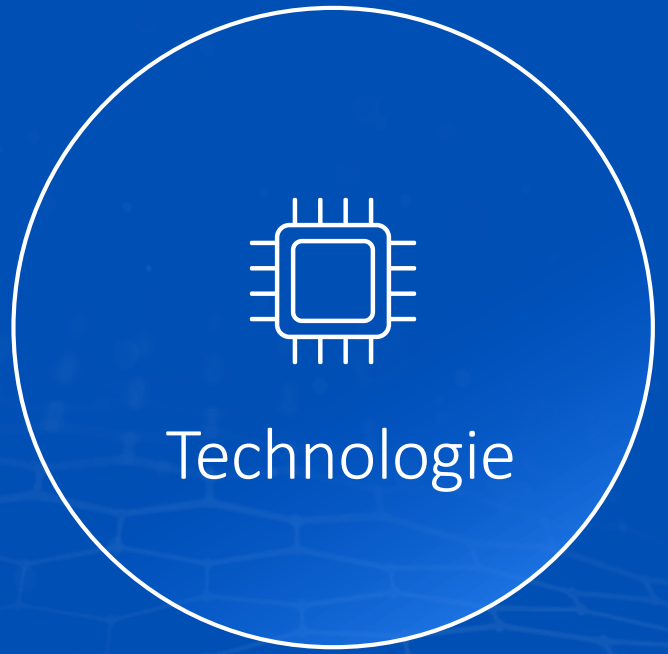
SOPHOS

Alle Jahre wieder Ende Dezember…

SOPHOS

Eine Lösung kaufen reicht nicht mehr

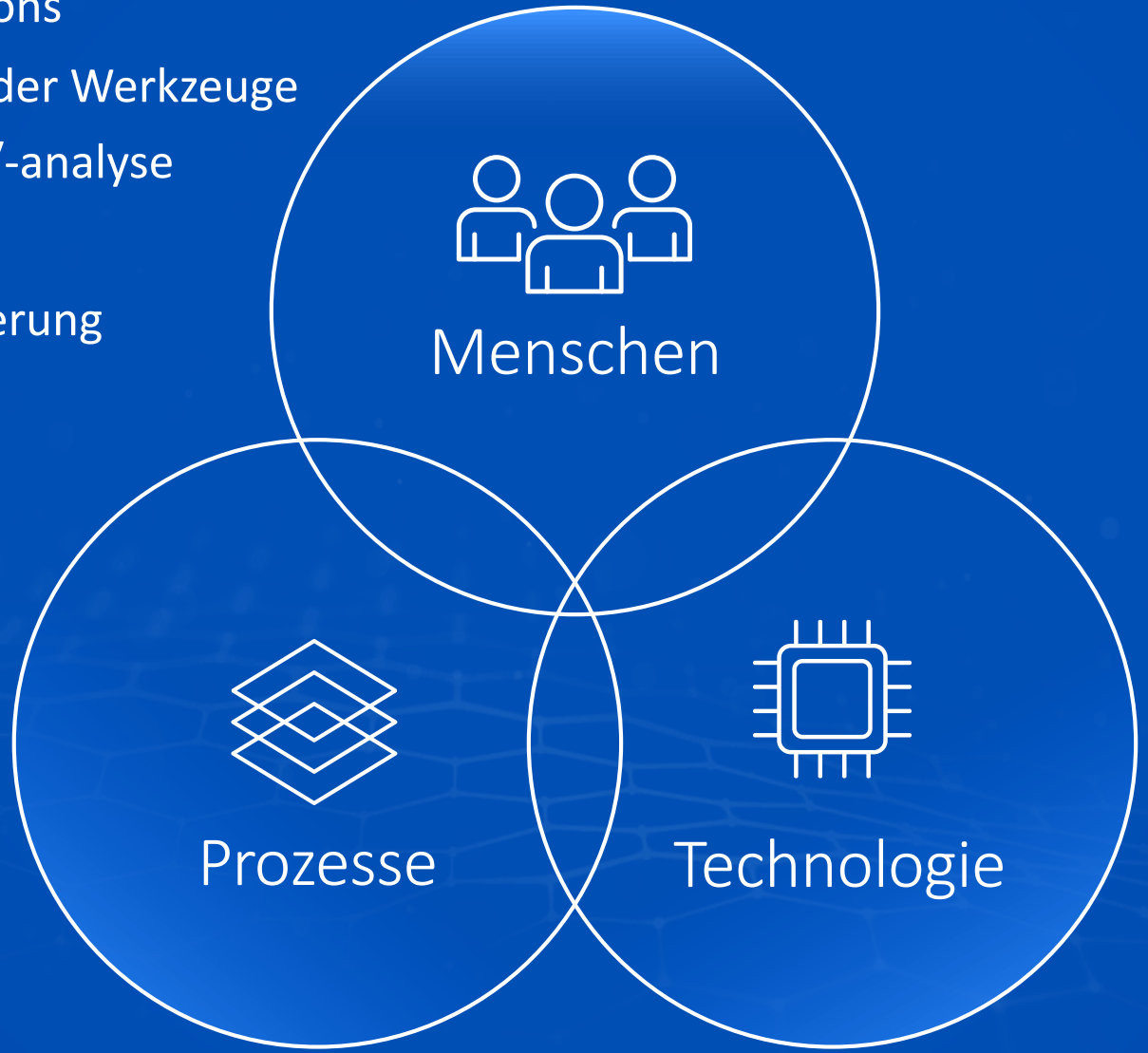




SOPHOS

24/7 Security Operations

- Aktive Bedienung der Werkzeuge
- Bedrohungssuche/-analyse
- Threat Intelligence
- Proaktive Verbesserung der Sicherheit



Vorgehen bei Vorfall

- Incident/Response
- Eindämmung
- Neutralisierung

Stand der Technik = XDR Ökosystem

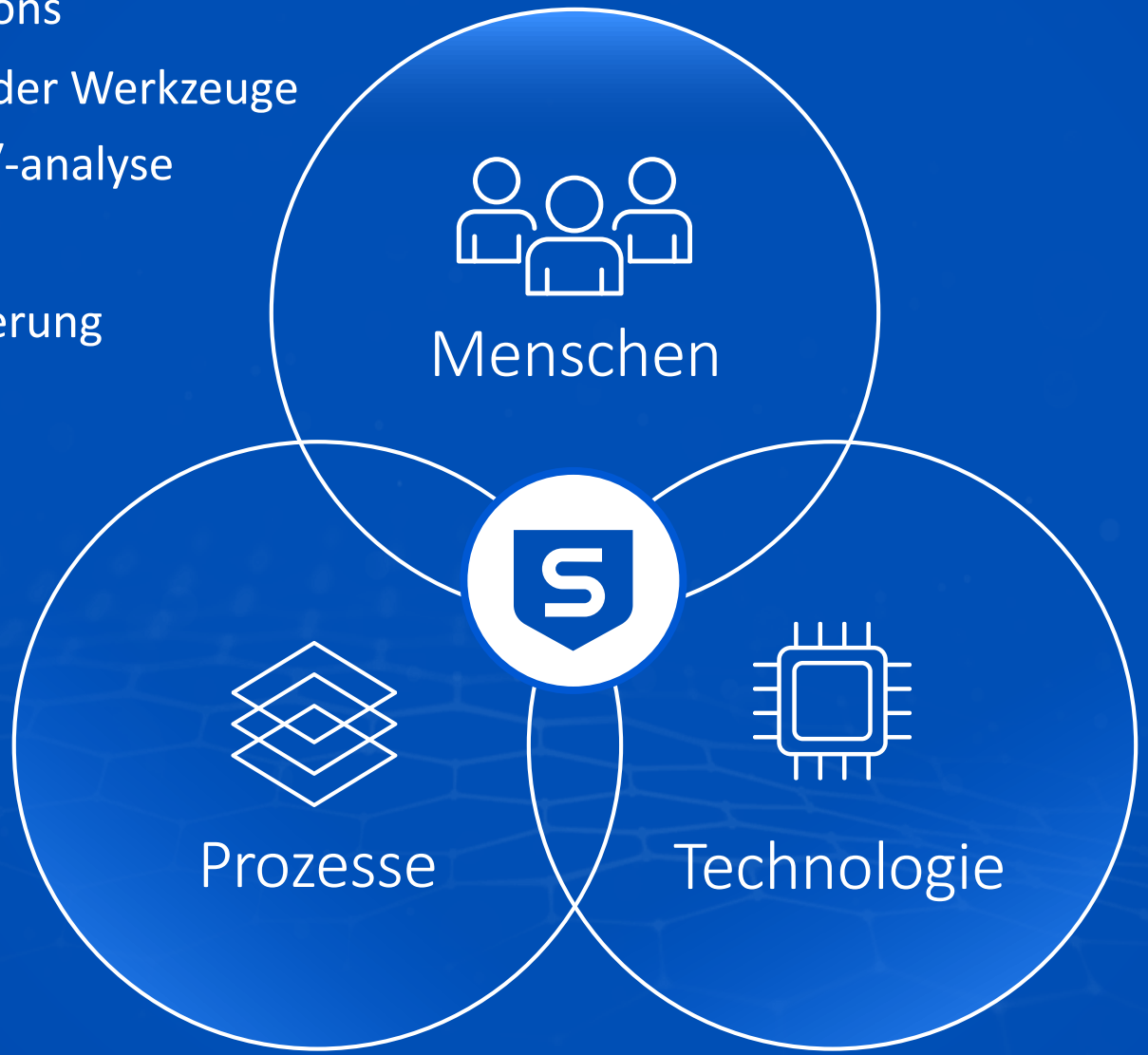
- NextGen Schutz überall
- Telemetrie aller Quellen
- Erkennung + Korrelation
- Reaktion
- Automation

= Werkzeuge

Sophos MDR

24/7 Security Operations

- Aktive Bedienung der Werkzeuge
- Bedrohungssuche/-analyse
- Threat Intelligence
- Proaktive Verbesserung der Sicherheit



Vorgehen bei Vorfall

- Incident/Response
- Eindämmung
- Neutralisierung

Stand der Technik = XDR Ökosystem

- NextGen Schutz überall
- Telemetrie aller Quellen
- Erkennung + Korrelation
- Reaktion
- Automation

= Werkzeuge

Nächste Schritte:

Halle 7, Stand 328

Sophos Adaptive Ecosystem (ACE)

Mit einer Kombination von Automatisierung und menschlichen Experten bietet das Sophos Adaptive Cybersecurity Ecosystem (ACE) leistungsstarken Schutz, der kontinuierlich dazulernt und sich verbessert.

- https://www.sophos.com/de-de/content/adaptive-cybersecurity-ecosystem

Sophos XDR - eXtended Detection and Response

Erkennen und analysieren Sie Bedrohungen lückenlos – mit Endpoint-, Server-, Firewall-, Email und weiteren Datenquellen.

- https://www.sophos.com/de-de/products/endpoint-antivirus/xdr.aspx

Sophos Managed Detection Response

24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service

- Mehr Infos: https://www.sophos.com/de-de/products/managed-threat-response.aspx

SOPHOS