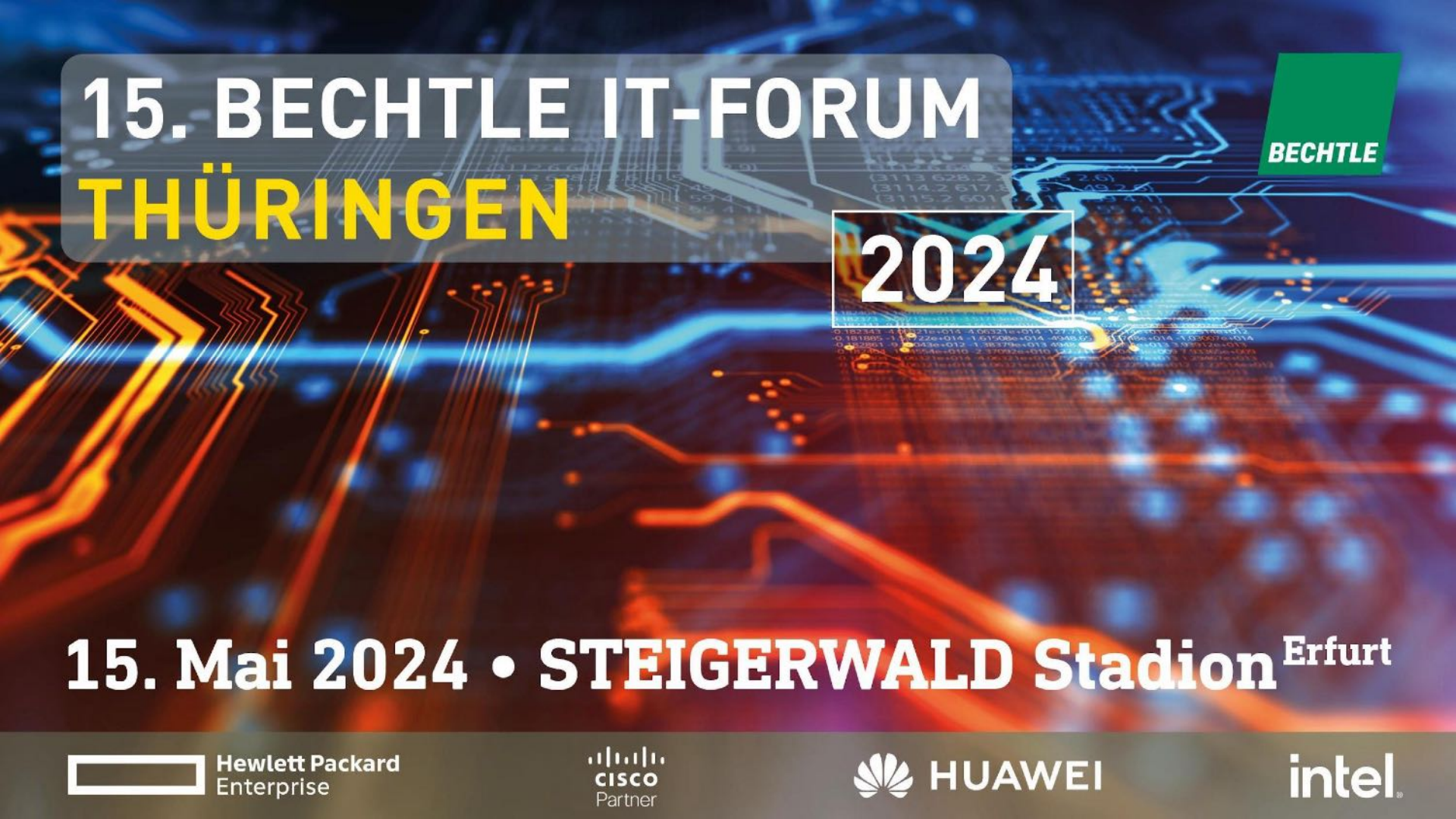

15. BECHTLE IT-FORUM
THÜRINGEN
2024
BECHTLE
15. Mai 2024 • STEIGERWALD Stadion Erfurt
Hewlett Packard Enterprise
cisco Partner
HUAWEI
intel

Vom Endgerät bis überall – Wie Rundumschutz wirklich funktioniert.

Jens Gehring

Enterprise Account Director

Mobile | +49 177 52700 73

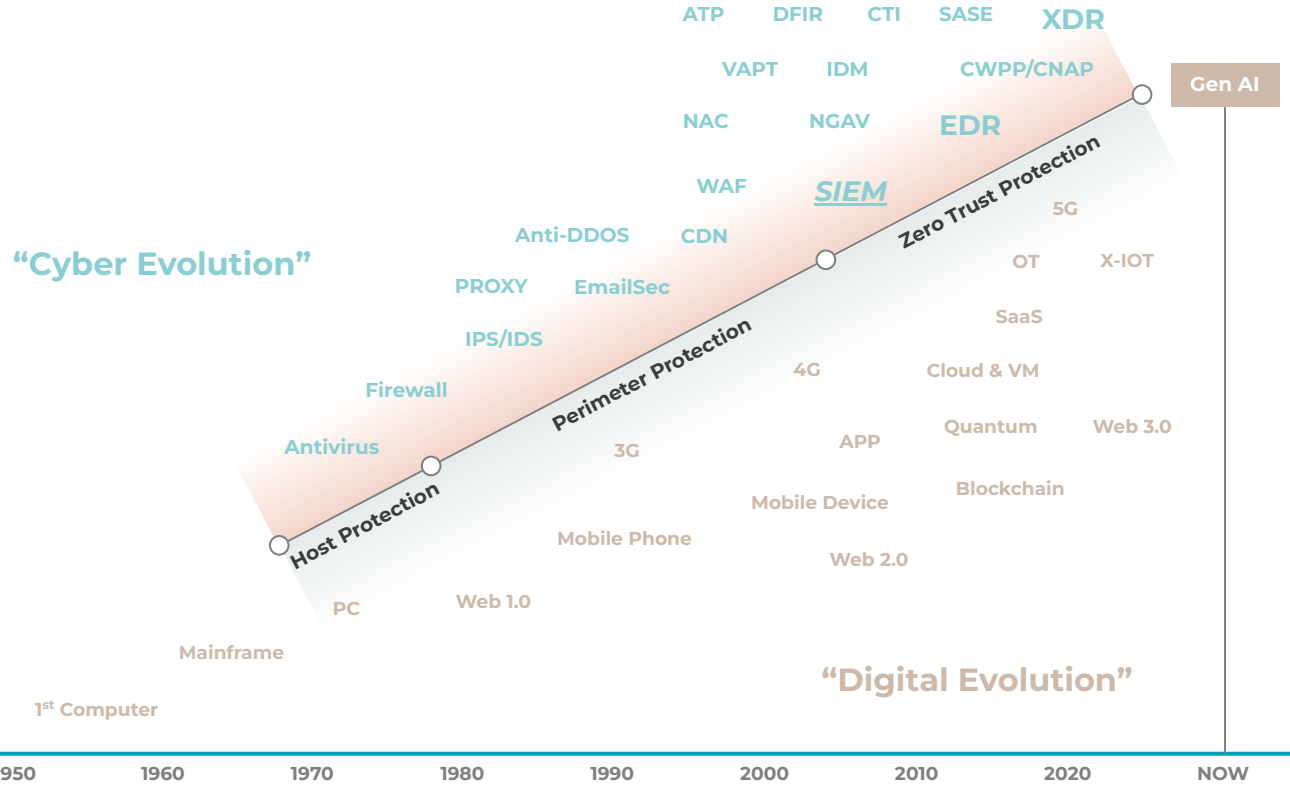
LinkedIn |

https://www.linkedin.com/in/jensgehring/

Umfrage

- Wer kennt den Begriff EDR?
- Wer kennt XDR?
- Wer kann den Begriff XDR präzise und *marktgerecht* erklären?
- Und wer kann EDR oder XDR nicht mehr hören?

Die digitale Evolution in Bezug auf CyberSec



MEHR Rechenressourcen
MEHR Daten
MEHR Security Tools
MEHR Bedrohung
MEHR Security Warnungen

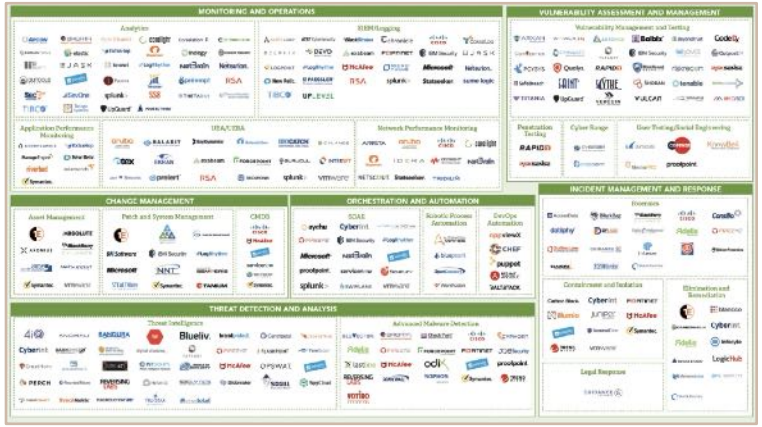
WENIGER Budget Steigerung
WENIGER Betriebs-zentrisch
WENIGER CyberSec Talente
WENIGER Fähigkeiten

60% YoY
Wachstum in Ransomware Attacken

Eine Vielzahl an Möglichkeiten

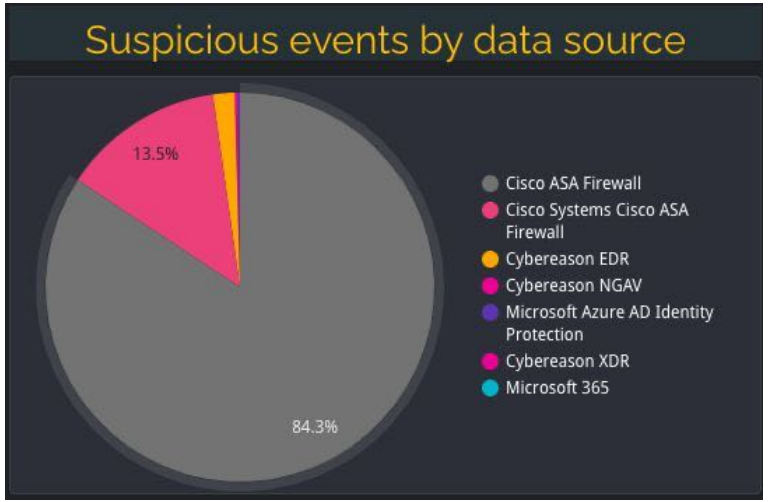
Cyber Software Tools

Cyber Service Tools

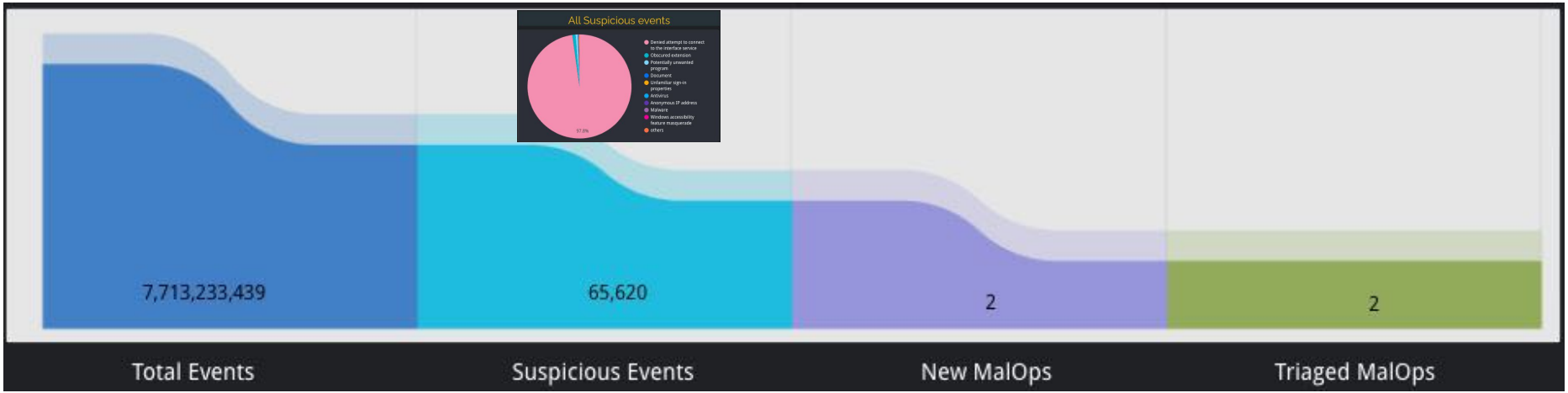


Warum also der Endpunkt?

Woher kommen die Daten bei XDR?
- ein Fallbeispiel

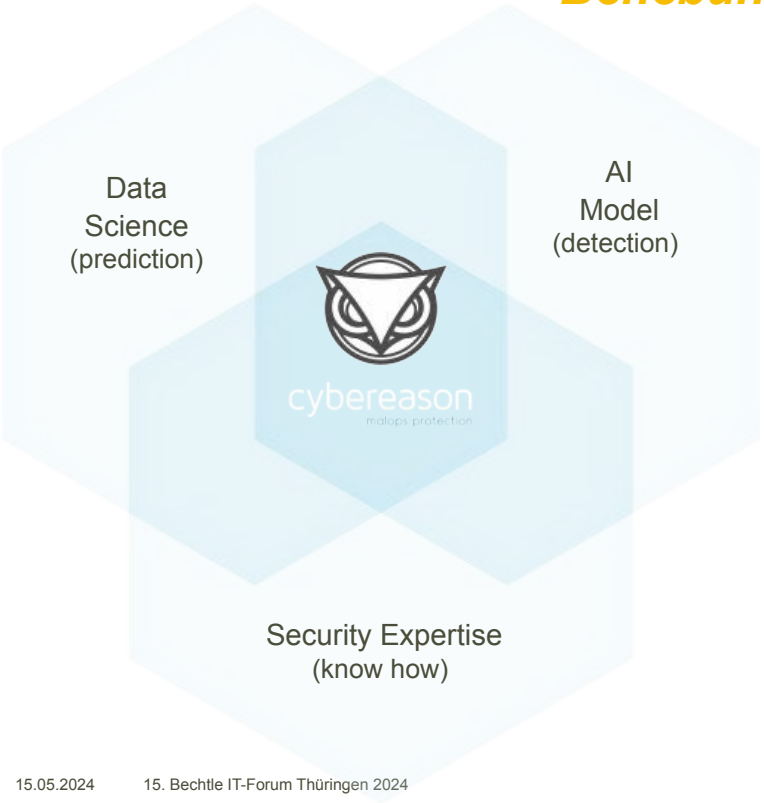


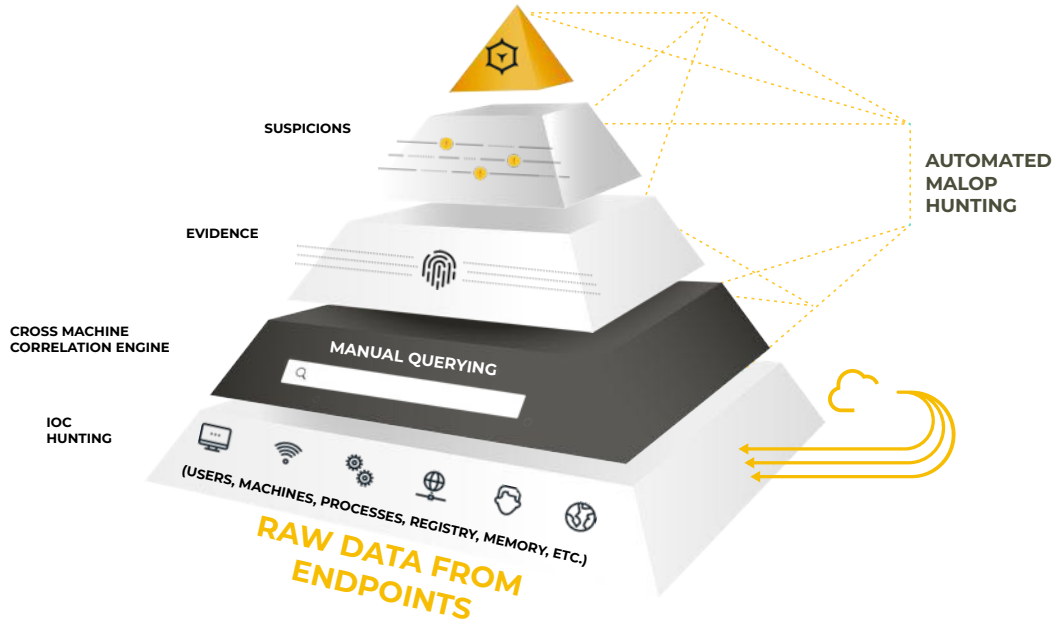
Was wurde aus den Daten?
- ein Fallbeispiel



Was ist dieser ominöse “MalOp”?

Reduzierung der menschlichen Interaktion für die Erkennung und Behebung von Bedrohungen





The MalOp™ (Malicious Operation)

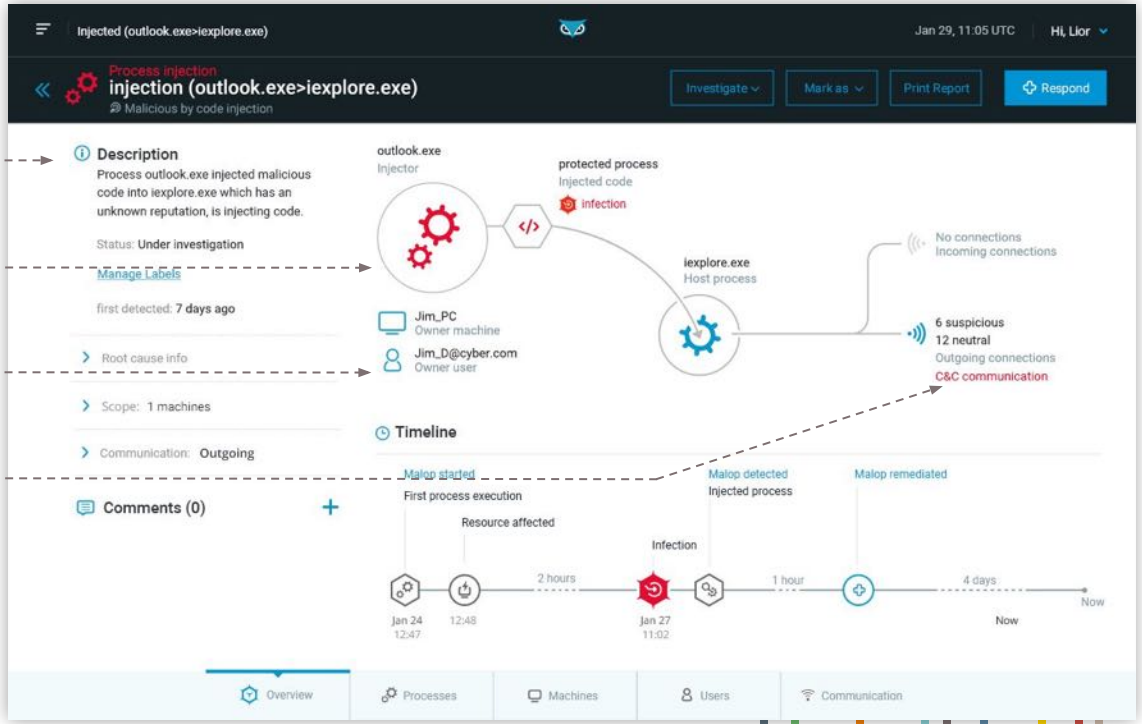
Effizient & Wirksam - Sichtbarkeit der kompletten Angriffskette

Ursache

Programme

Betroffene User & Geräte

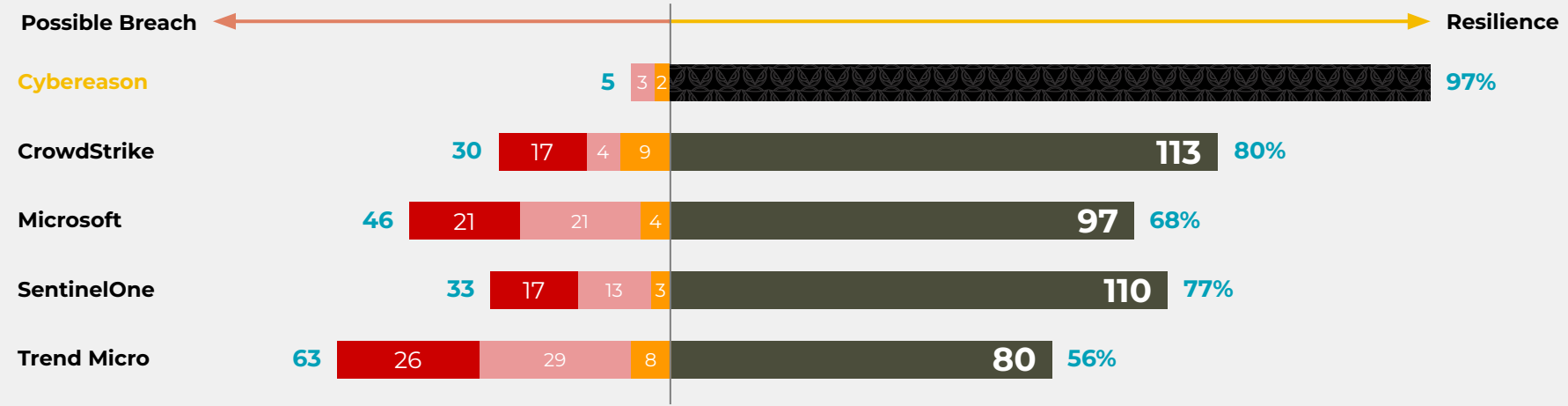
Kommunikationen der Attacke



WIRKSAMKEIT! - attestiert durch MITRE

Denn jede Detection zählt

Cybereason @ MITRE ATT&CK 2023 Detection Coverage (143 Steps*)



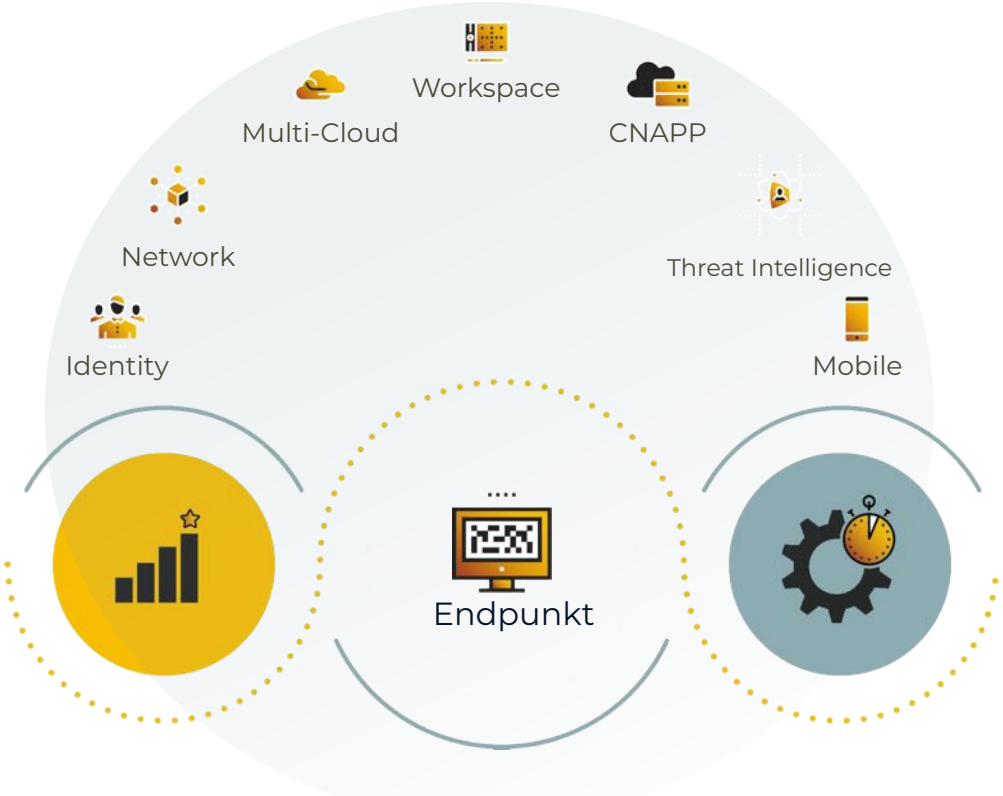
Effizienz & Wirksamkeit

MalOp

Weniger

ist

MEHR



Datenquellen

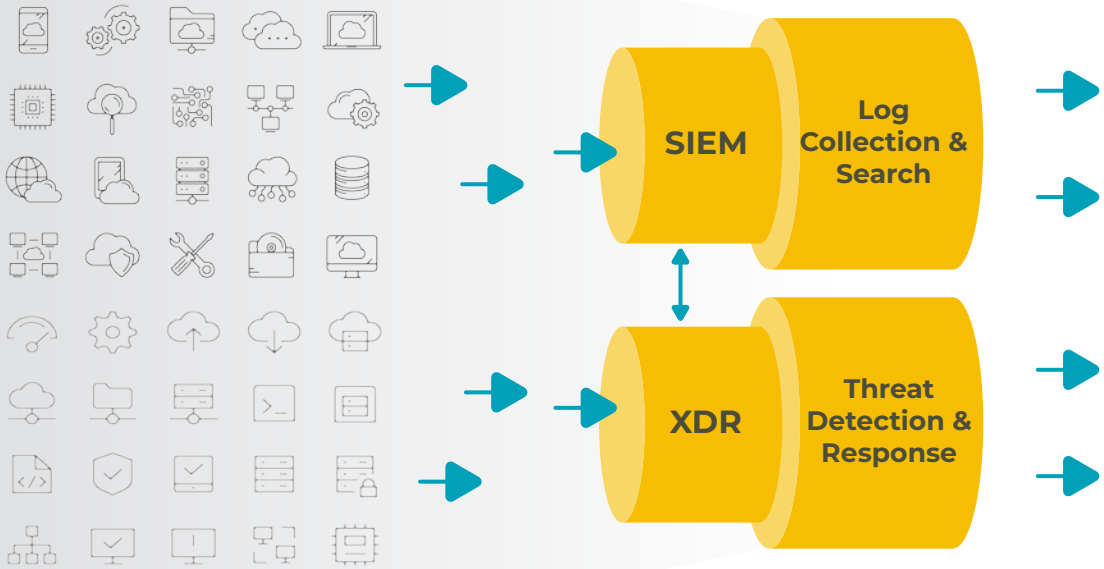
MEHR

ist

MEHR

Das Problem von “Mehr ist Mehr”

Exponentielles Datenwachstum und Kostenexplosion

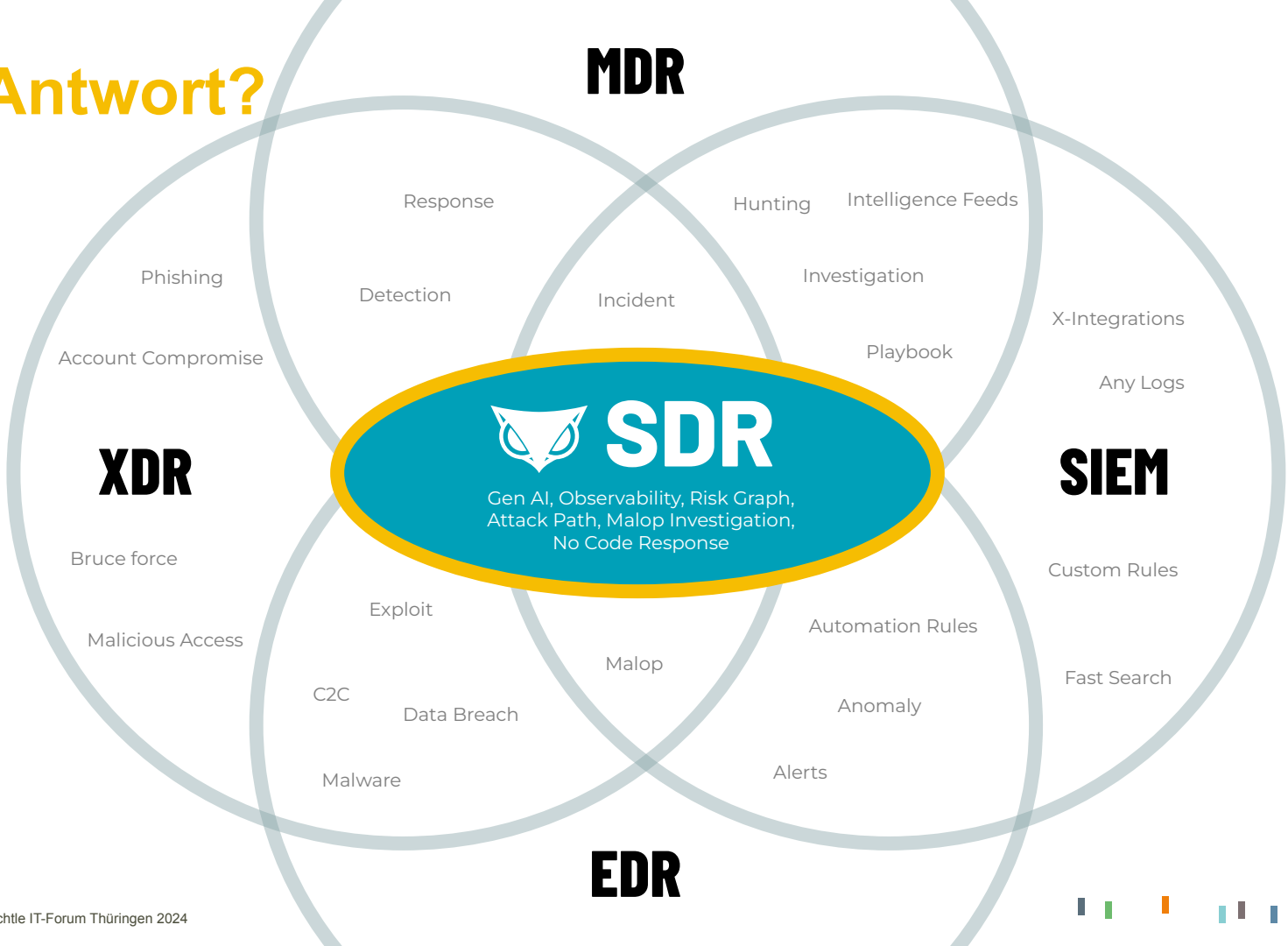


Daten Komplexität

- **Separate “Data Lakes”**
- **Unvollständige Data Sets**
- **AI-basierte Analysen sind schwierig**
- **Exponentielle Datenkosten**
- **Keine ganzheitliche Security strategisch**

IT & Security Data | **Security Data Lake Strategy** | **Security Outcome**

Die Antwort?


MDR
Response
Hunting
Intelligence Feeds
Phishing
Detection
Incident
Investigation
X-Integrations
Account Compromise
Playbook
Any Logs
SDR
Gen AI, Observability, Risk Graph,
Attack Path, Malop Investigation,
No Code Response
XDR
SIEM
Bruce force
Custom Rules
Exploit
Automation Rules
Malicious Access
Malop
Fast Search
C2C
Anomaly
Data Breach
Alerts
Malware
EDR

Wie geht “überall” und “Rundumschutz” nun wirklich?

Ganz simpel → Effizienz & Wirksamkeit

Unified Portal

SDR | MDR | TI | DFIR | Search & Reporting

Public API

</>

Detection

Malop Inbox | Threat Models | Malop Engine

Investigation

Graph Explorer | Action Planner

Data

Data Ingest | Data Lake | Data Graph | Vector DB

Collection

Sensor

Network, Cloud & Workspace

cybereason

Let´s DEFEND!