SHD.
WIR BEWEGEN IT.

# Guardians of the SOC

## Security Operations by SHD


14.09.2023


# 01 Szene #1 Cyber Resilienz

# Ihr Drehbuch für sichere, resiliente und verfügbare IT

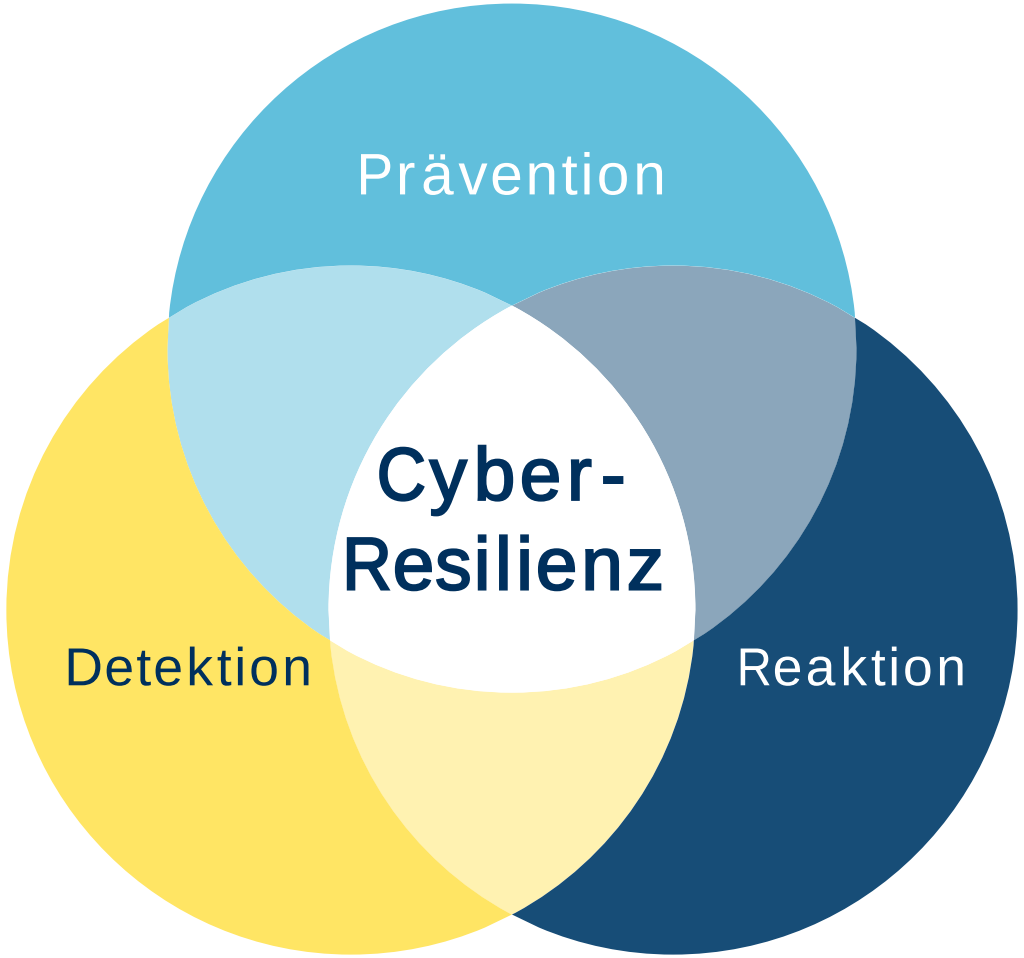
1 Von IT-Sicherheit zu Cyberresilienz - so gelingt der Change

2 Lagezentrum Security Operations Center

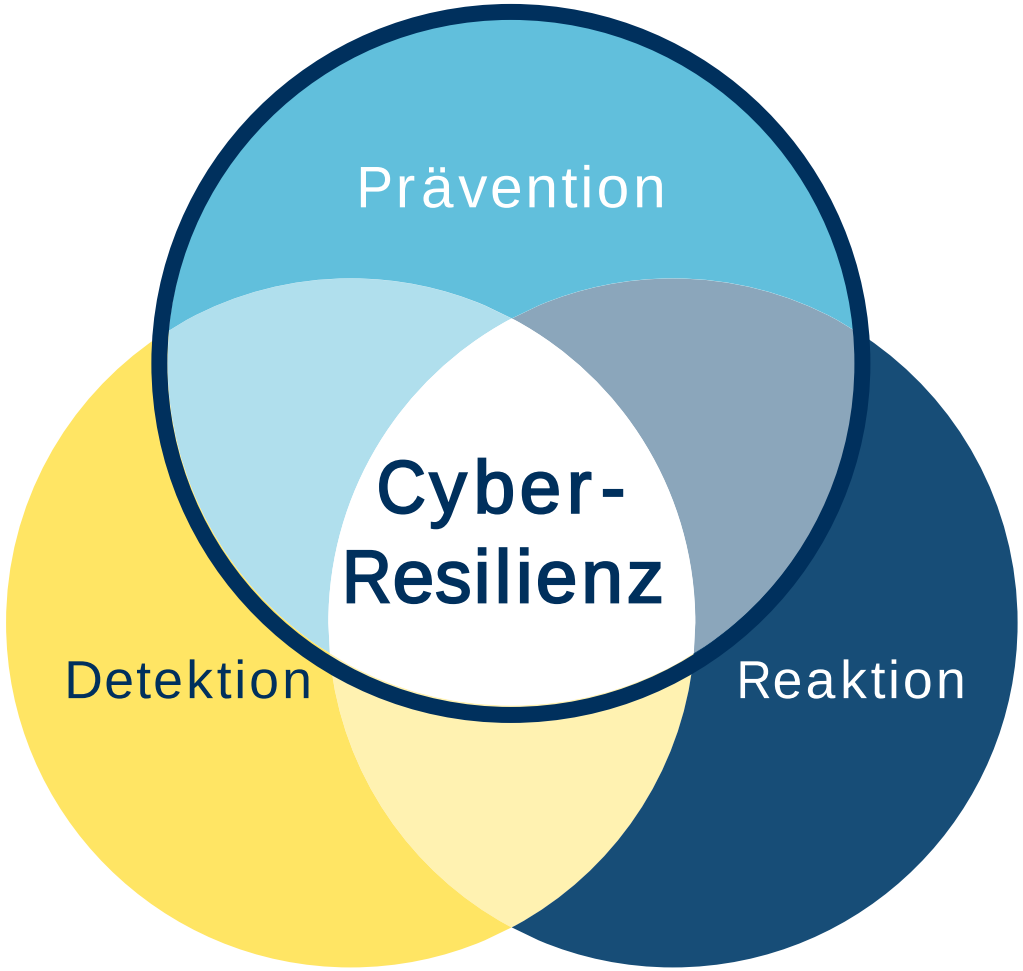
- Einsatzzweck und Nutzen
- SIEM, Schwachstellen und Zero-Day-Exploits

3 Tatortreiniger: Incident Response Team (IRT)

# Ihr Drehbuch für sichere, resiliente und verfügbare IT



# Cyber Resilienz

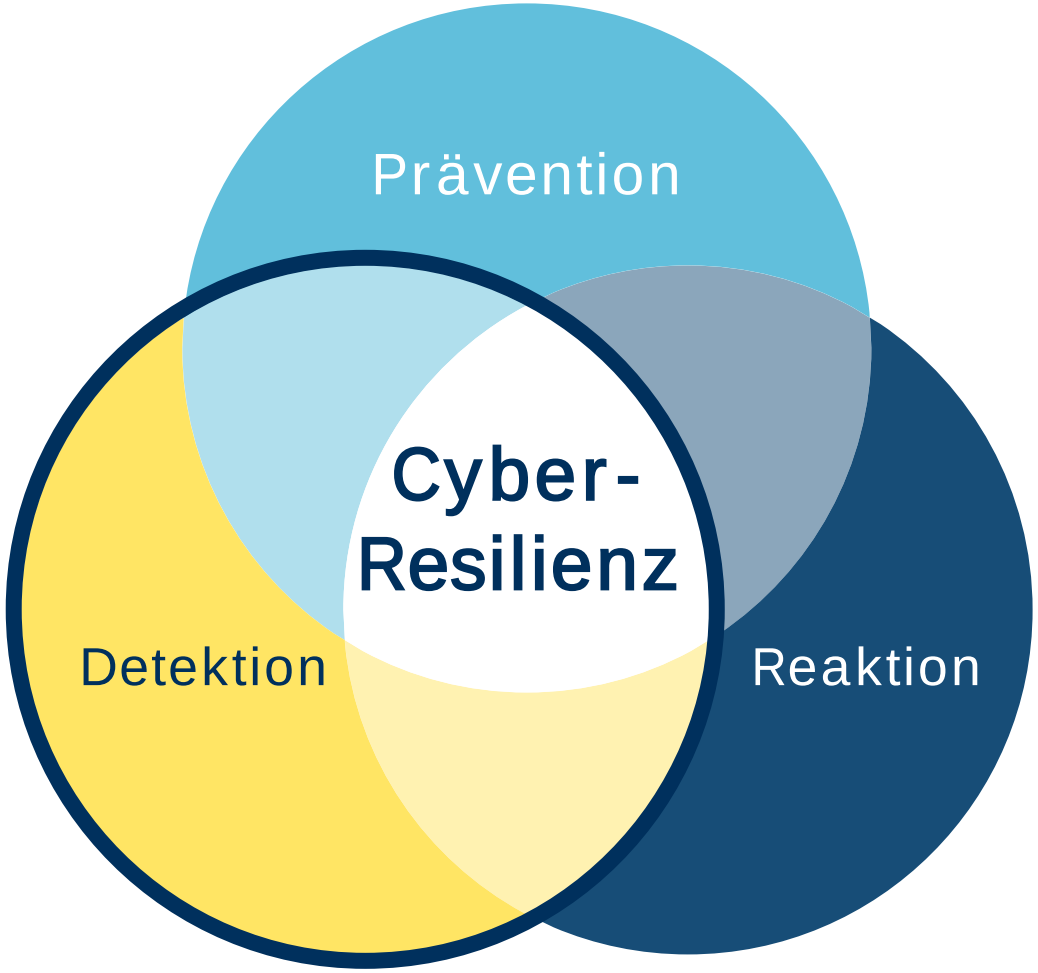



## Prävention

**vorbeugen, verhüten, „schützen“, verhindern**

proaktiv

# Cyber Resilienz

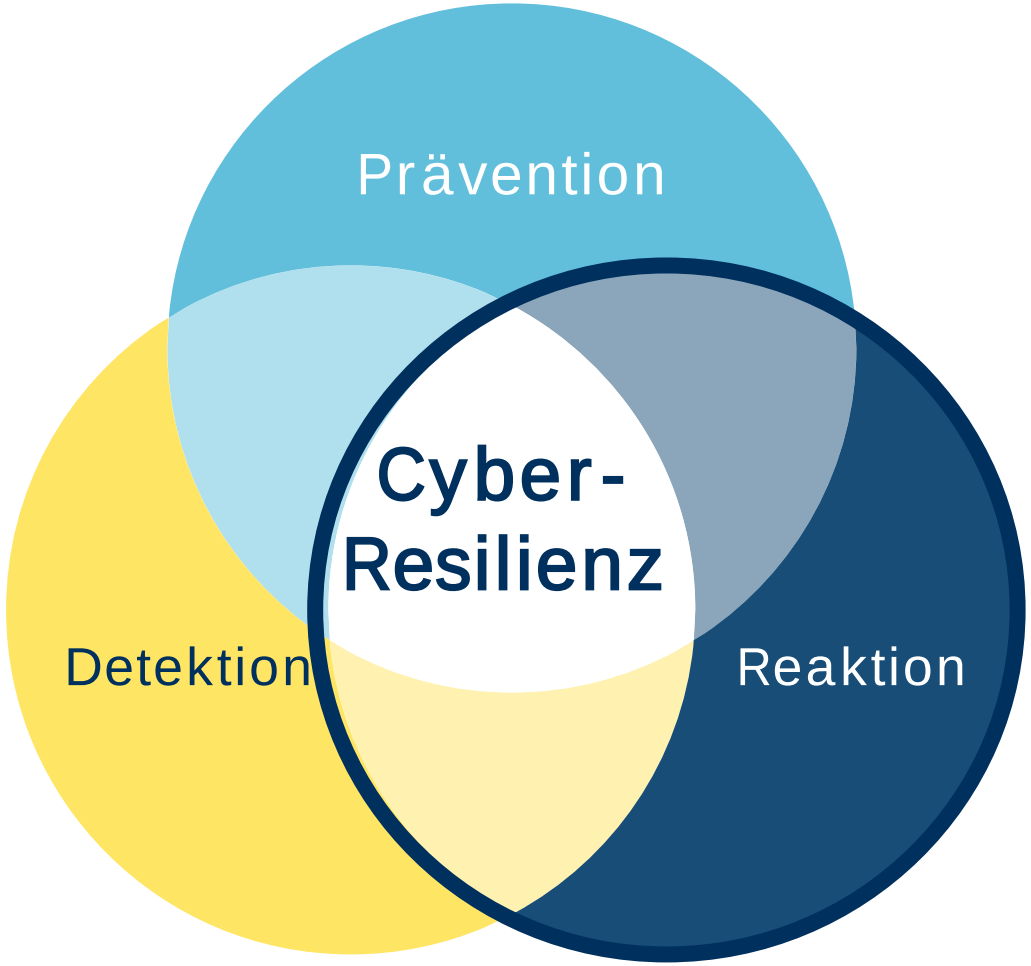



## Detektion

(Erkennung, Feststellen)

Entdecken, Erfassen, Isolieren, Feststellen, Sichtbarmachen.

# Cyber Resilienz




## Reaktion / Response

Schnell und effektiv auf Erkennungen reagieren, Angriffe eindämmen, Schadsoftware stoppen

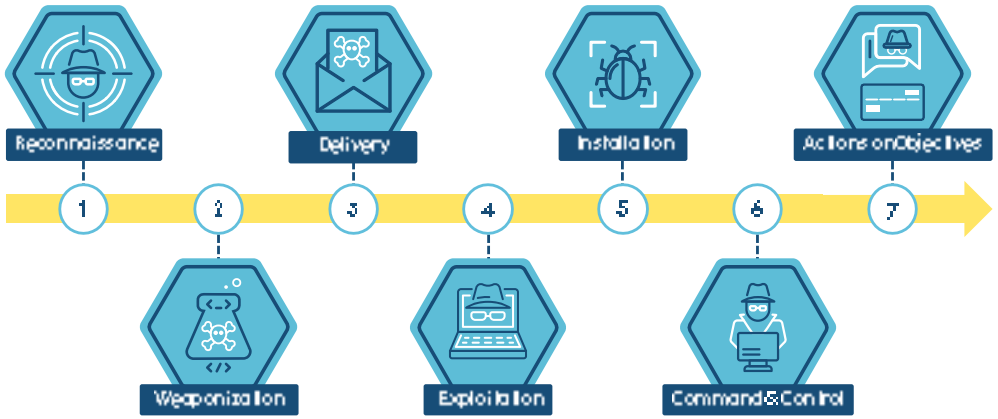
reaktiv

# Stationen eines Angriffs - Cyber Kill Chain

alles läuft

Cyber **Kill Chain*...**


Game over




*Lockheed Martin

# Stationen eines Angriffs - Cyber Kill Chain

alles läuft


Game over

mittlere Verweildauer der Angreifer

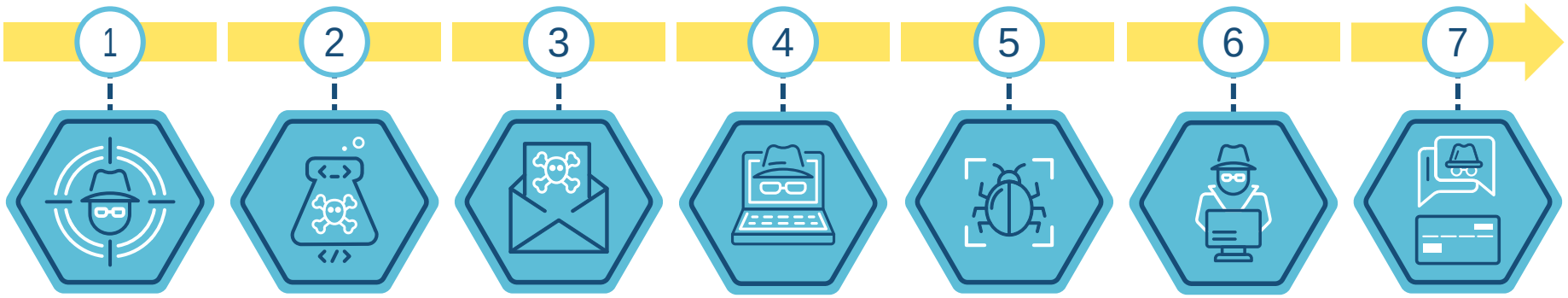
Wochen bis Monate!

*BSI 2022: >200 Tage !*

**Lockheed Martin*

# Cyber Kill Chain vs. etablierte Lösungsansätze

## Prävention



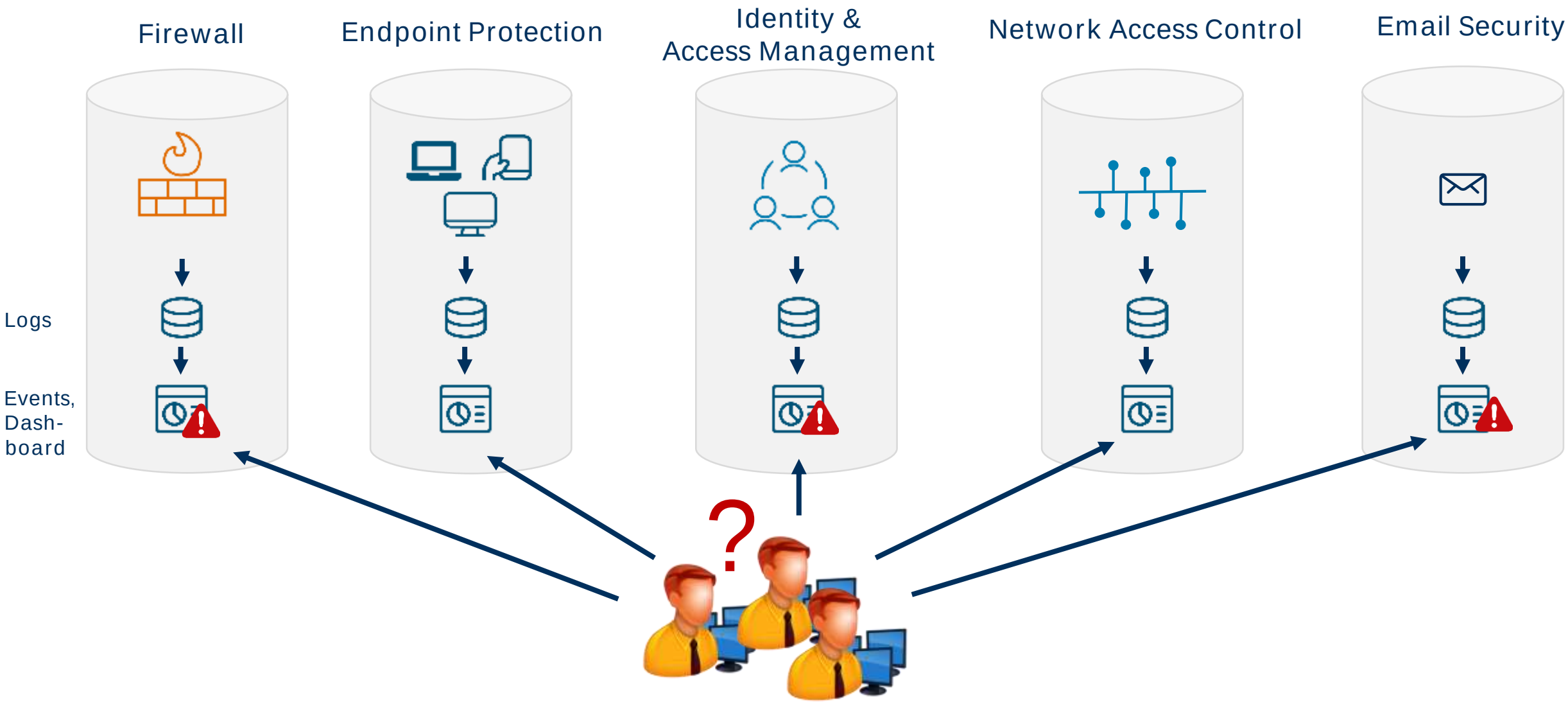

| Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command & Control | Actions on Objectives |
|---|---|---|---|---|---|---|
| Footprinting<br>User Training | User Training<br>Awareness | FW<br>Proxy<br>Mail<br>IPS<br>NAC<br>IAM<br>EDR | EDR<br>IPS<br>PatchMgmt | EDR<br>IPS<br>IAM<br>Threatfeeds | FW<br>Proxy<br>EDR<br>IPS<br>IAM<br>Threatfeeds | FW<br>Proxy<br>IAM<br>!Ransomware<br>IRT<br>BCM |

SECURITY MANAGEMENT

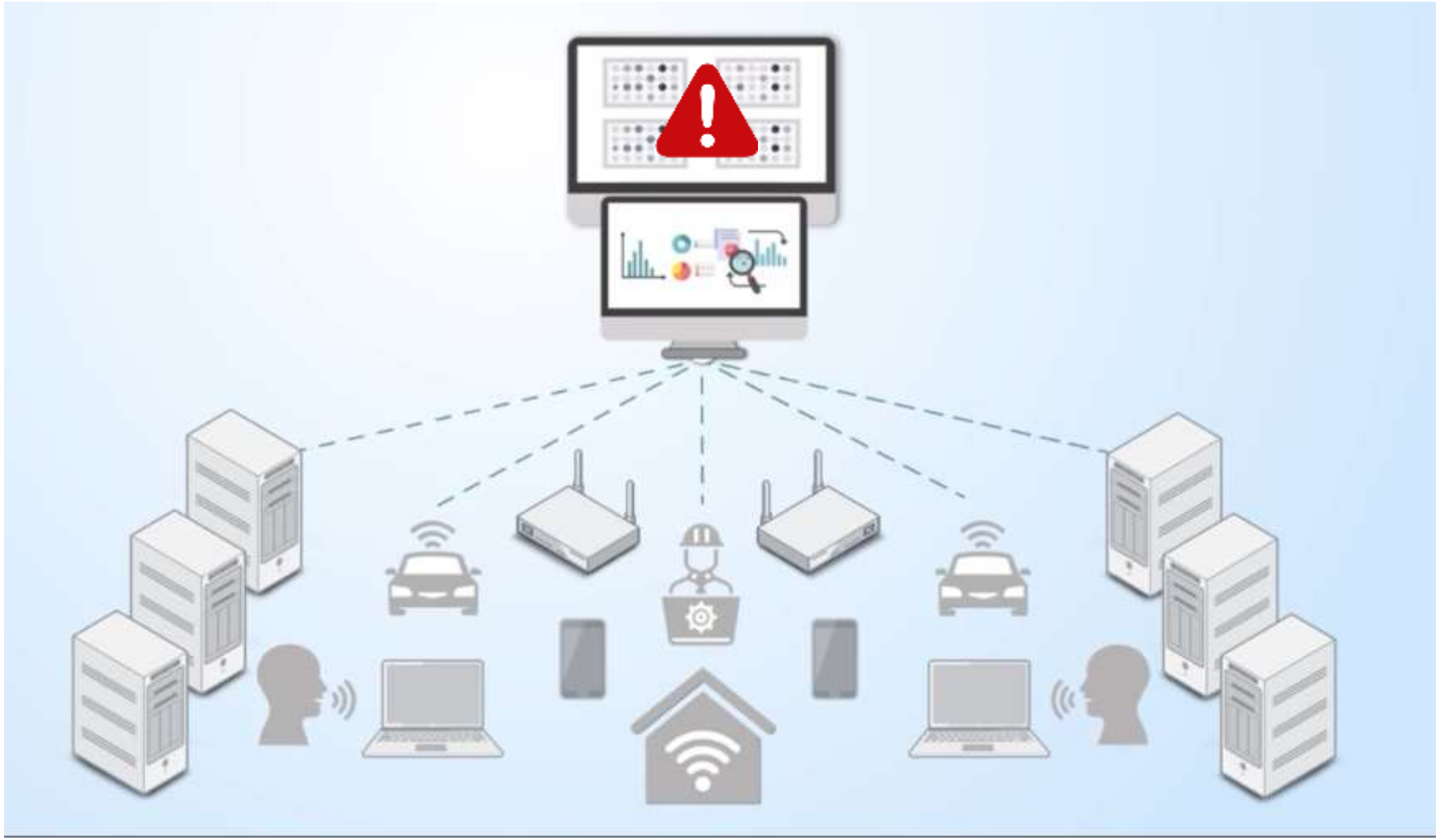
**ISMS**
(organisatorisch – Informations-sicherheitsmanagementsystem)

- BCM (Notfallplanung)
- Log Management & SIEM
- Monitoring
- Penetration Tests
- Incident Management
- User Awareness
- Endpoint Management

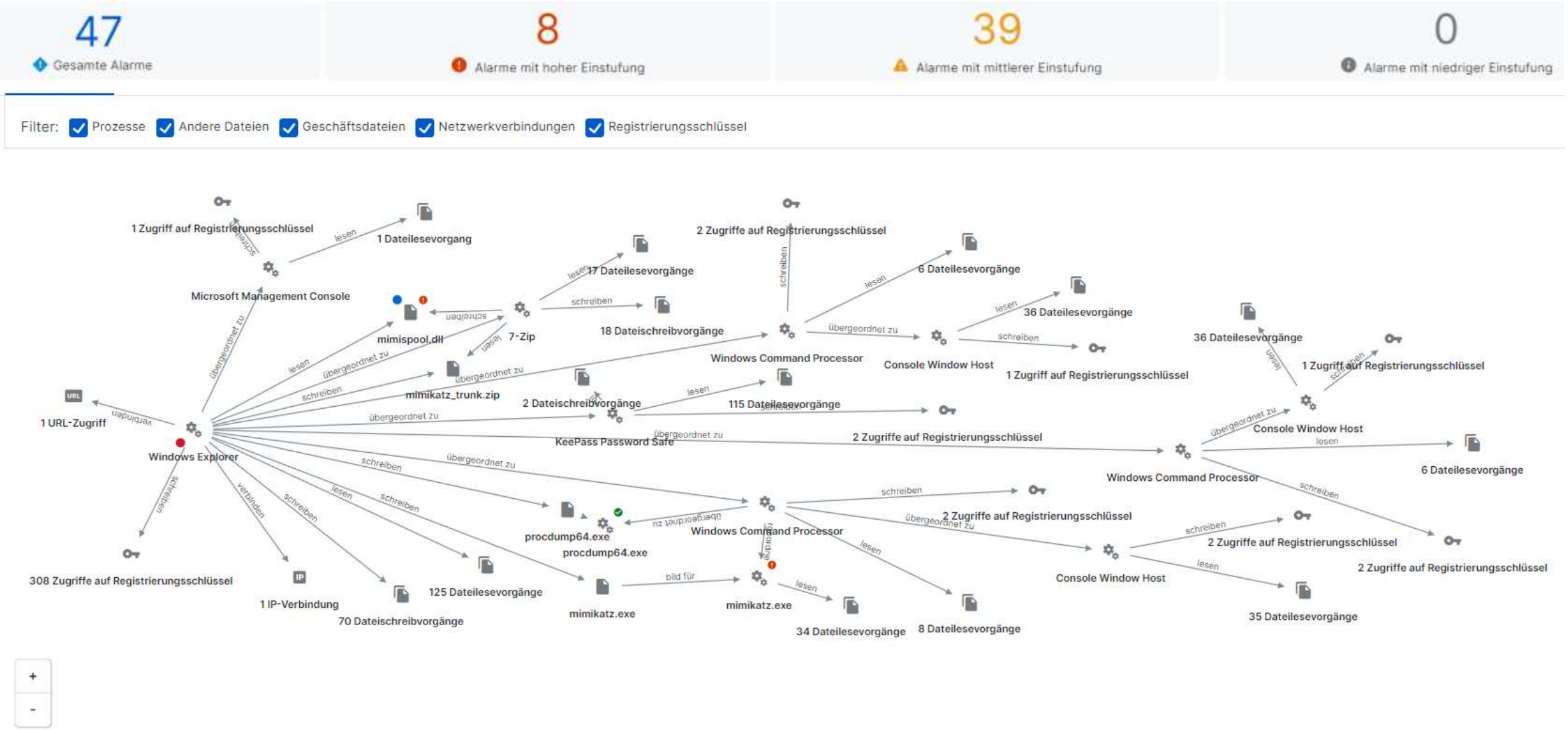
# Bisherige Herangehensweise: Security Silos



# Herausforderung #1: Ein Blick auf Alles / single pane of glass



# Herausforderung #2: Know How zur Bedrohungsanalyse

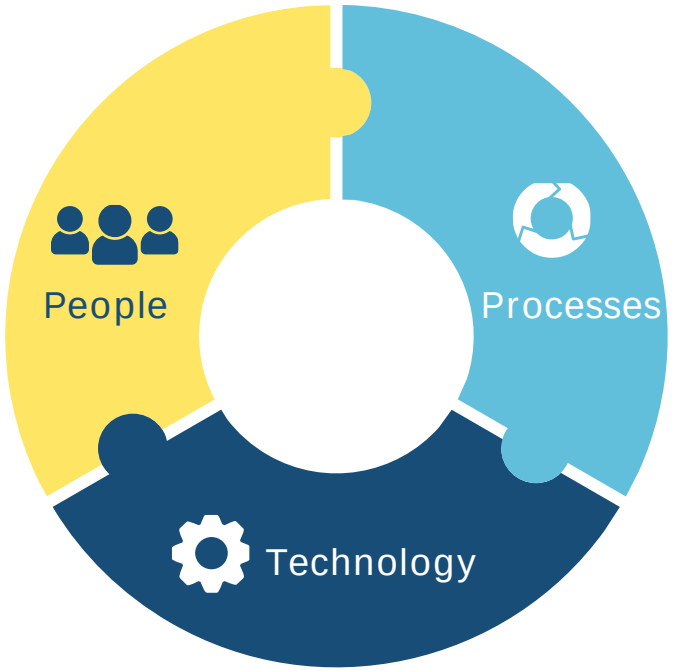


# #2 Security Operations Center – System zur Angriffserkennung

## Protokollierung, Detektion und Reaktion

# Security Operation Center - Servicemodell

24/7 Security Operations
- Plattform Operators
- 1. Level (Observation)
- 2. Level (SOC Analyst)
- 3. Level (Forensiker)



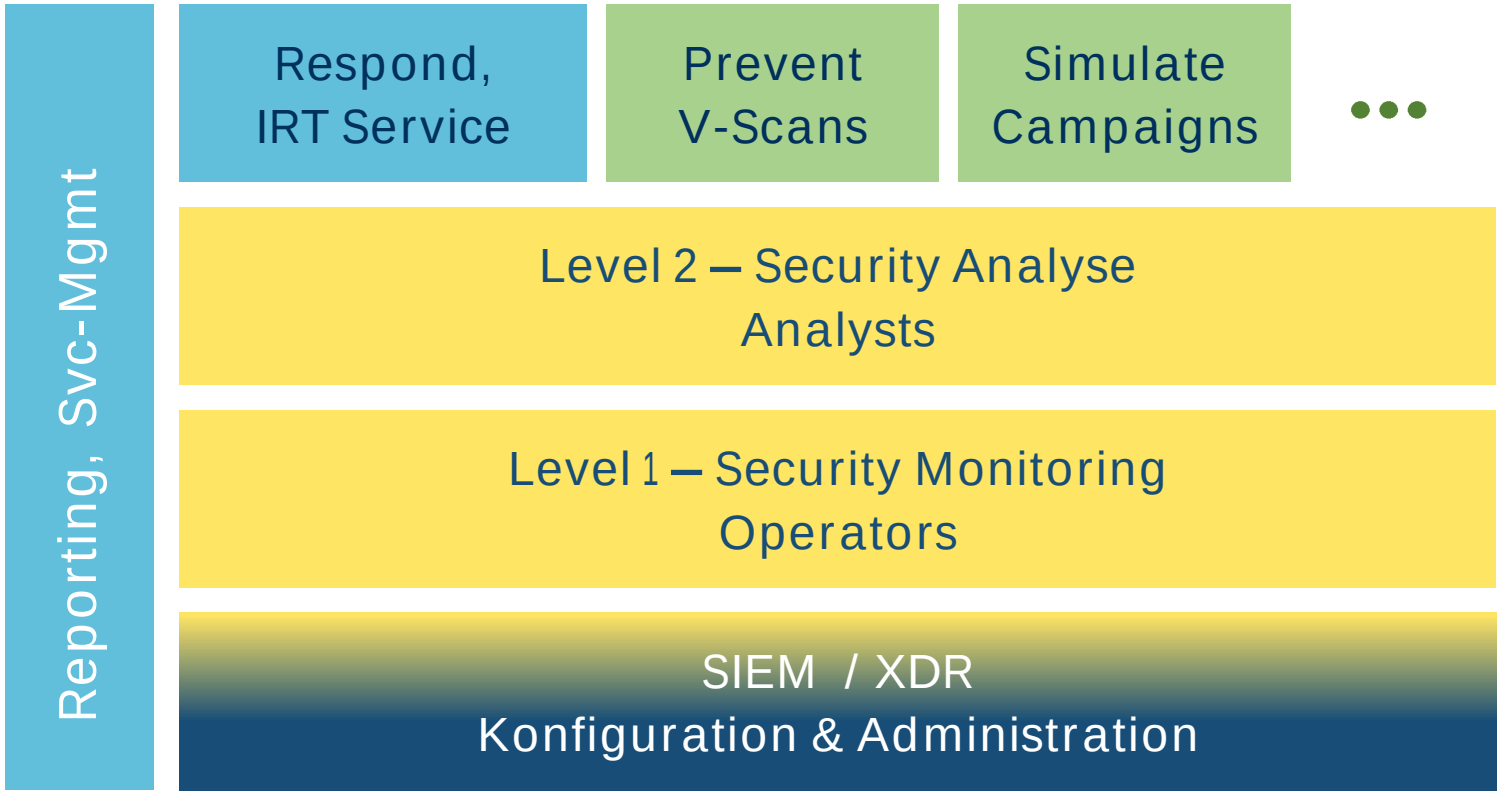

SIEM/XDR Ökosystem
- NextGen Schutz
- Telemetrie
- Erkennung & Korrelation
- Reaktion & Automation

Vorgehen bei Incidents
- Meldeketten, Dashboard
- Incident Bewertung
- Incident Response
- Playbooks

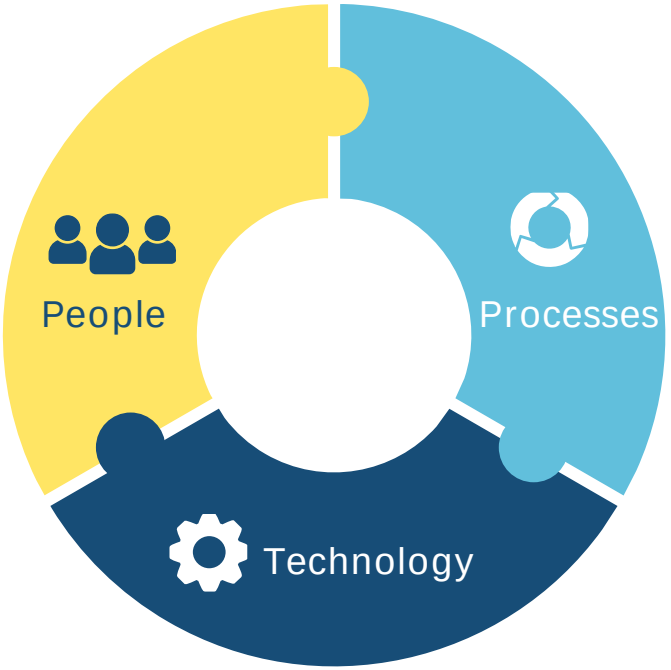
Service Management
- Joure Fixes
- Reports

# Security Operation Center

## SOC - Organisation




## Service Modell



# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

## Security Event Monitoring

### SOC Start

- (Co-) Managed Security-Event Monitoring
- (Co-) Managed DER

### SOC complete

- Paket S
- Paket M
- Paket L

## Additional Services

- V-SCAN (Schwachstellenscan)
- Zero Day Exploit Alarming
- Incident Response Service

## Additional Solutions

- PenTesting
- Workshops
- Awareness Training
- Security Assessments

# Security Operation Center – Services & Solutions


## SOC – Start/Advanced

- Security Event Observation an **kundeneigener EDR Lösung**
- 5/9, 24/7* Service
- Monitoring & Reporting
- Reaktion auf Incidents
- 1 - 4 Themenfeld-Überwachung


## SOC complete - S

- Security Event Observation in **Managed SIEM Lösung**
- 5x9 Service
- Monitoring & Reporting
- Reaktion auf Incidents
- zzgl. Devices-Lizenzierung und Ticketbearbeitung
- inkl. 1 TB mtl. Datenvolumen (bis zu 4 Themenfelder)


## SOC complete - M

- Leistungen aus S-Paket
- 24/7 Service
- monatlicher Jourfix (1 Stunde per Web)
- bis 2 TB monatliches Datenvolumen (bis zu 8 Themenfelder)


## SOC complete - L

- Leistungen aus M-Paket
- direkter Ansprechpartner SM
- Premium Reporting
- wöchentlicher Jour Fix Termin (Web)
- bis zu 5 TB monatliches Datenvolumen (bis 12 Themenfelder)

# Leistungspakete SOC Start & Advanced *(kundeneigenes XDR)*

## SOC Services powered by SHD
## START

- ✓ 24 x 7 Support inkl. Admin-Hotline
- ✓ Automatisierte Alarmierung
- ✓ Unverzügliche Bearbeitung relevanter Alarme
- ✓ Fester SHD-Ansprechpartner
- ✓ Monitoring und Reporting
- ✓ auf Basis des eigenen M365 Defenders

Microsoft Lizenzen und Ticket-Bearbeitung werden separat angeboten

inklusive Themenfelder

- Endpoint Detection and Response

OPTIONAL: Vulnerability Management



## SOC Services powered by SHD
## ADVANCED

- ✓ 24 x 7 Support inkl. Admin-Hotline
- ✓ Automatisierte Alarmierung
- ✓ Unverzügliche Bearbeitung relevanter Alarme
- ✓ Fester SHD-Ansprechpartner
- ✓ Monitoring und Reporting
- ✓ auf Basis des eigenen M365 Defenders

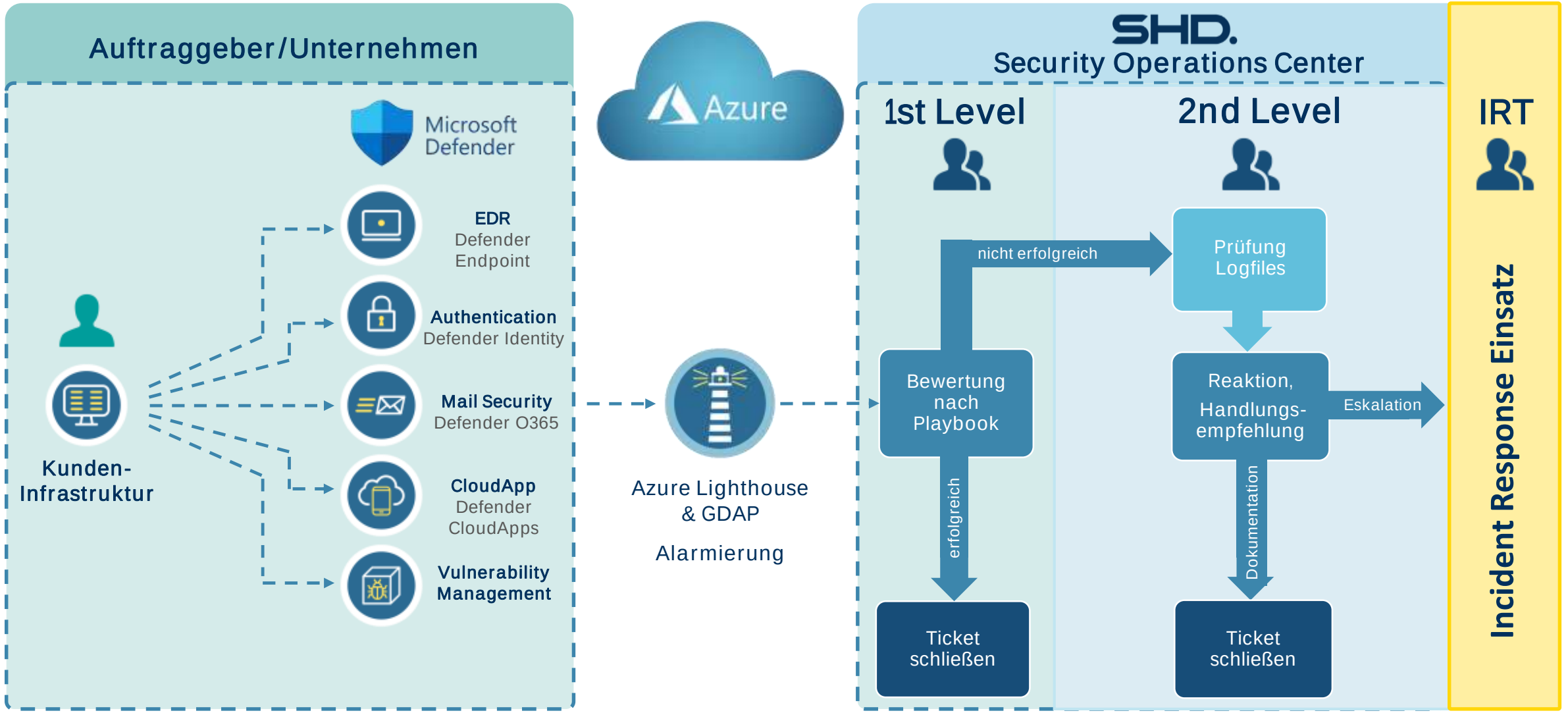
Microsoft Lizenzen und Ticket-Bearbeitung werden separat angeboten

inklusive Themenfelder

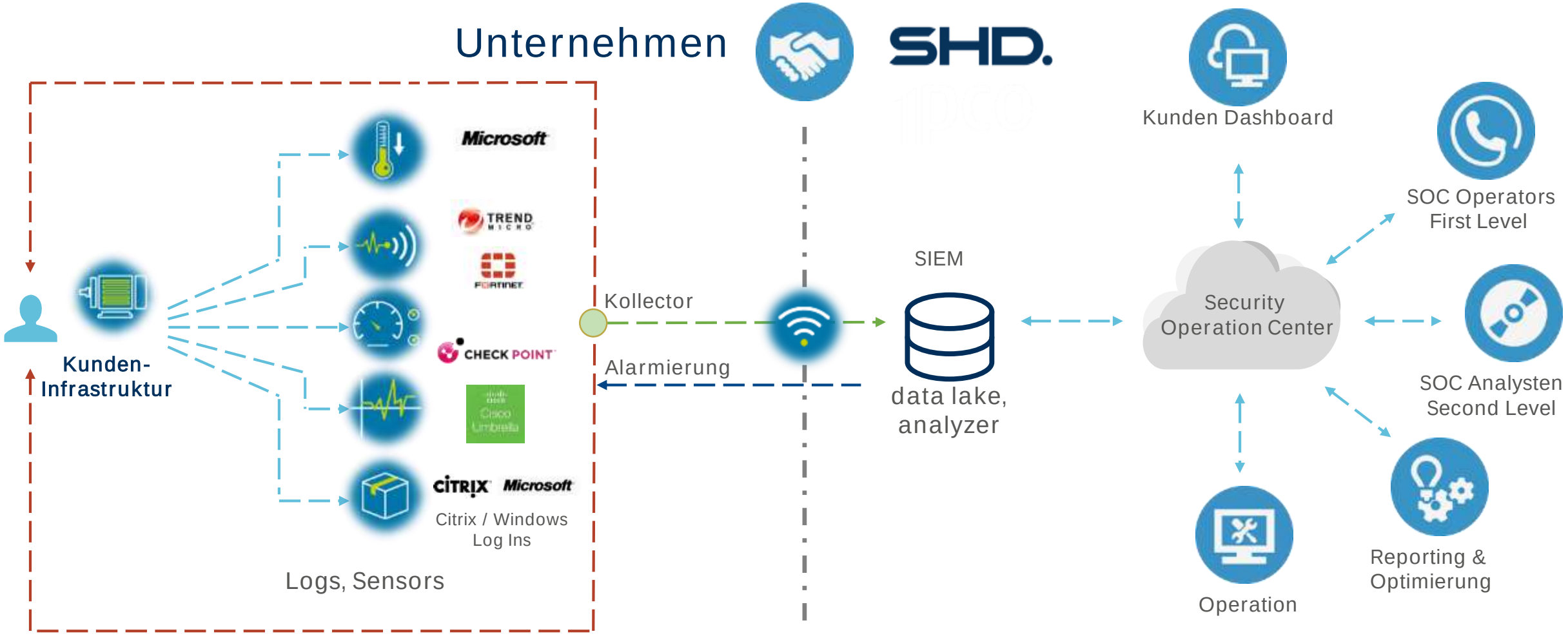
- Endpoint Detection and Response
- Mail Security
- Authentication
- Cloud App Security

OPTIONAL: Vulnerability Management

# Service Aufbau (Bsp. M365)



# Security Operation Center as a Service (complete)



# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

## Security Event Monitoring

### SOC Start

- (Co-) Managed Security-Event Monitoring
- (Co-) Managed DER

### SOC complete

- Paket S
- Paket M
- Paket L

## Additional Services

- V-SCAN (Schwachstellenscan)
- Zero Day Exploit Alarming
- Incident Response Service

## Additional Solutions

- PenTesting
- Workshops
- Awareness Training
- Security Assessments

# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

**Vulnerability Scan**
- Interner Scanner
- Schwachstellenanalyse
- Ports & Software

**Zero Day Exploit Alerts**
- zielgruppenangepasst
- zeitnahe Alarmierungen
- Behandlungshinweise

**SOC complete**

Paket M

Paket L

**Additional Services**

V-SCAN (Schwachstellenscan)

Zero Day Exploit Alarming

Incident Response Service

**Additional Solutions**

PenTesting

Workshops

Awareness Training

Security Assessments

# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

**Incident Response Service**

- Abrufbereitschaft des Einsatzteams

**SOC complete**

Paket M

Paket L

**Additional Services**

V-SCAN (Schwachstellenscan)

Zero Day Exploit Alarming

Incident Response Service

**Additional Solutions**

PenTesting

Workshops

Awareness Training

Security Assessments

# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

## Security Event Monitoring

**SOC Start**

- (Co-) Managed Security-Event Monitoring
- (Co-) Managed DER

Paket S

**PenTesting**

- Active Directory
- DMZ & Webseiten
- WiFi

**Workshops**

- Windows AD Security
- Notfall Management
- IT Service Portfolio

## Additional Services

- V-SCAN (Schwachstellenscan)
- Zero Day Exploit Alarming
- Incident Response Service

## Additional Solutions

- PenTesting
- Workshops
- Awareness Training
- Security Assessments

# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

## Security Event Monitoring

**SOC Start**

- (Co-) Managed Security-Event Monitoring
- (Co-) Managed DER

Paket S

**Awareness Training**

- User Awareness
- Phishing Simulation
- (Admin Awareness)

**Security Assessments**

- O365 Security Checkup
- Vor-Ort Begehung
- ISMS Gab-Analyse

## Additional Services

- V-SCAN (Schwachstellenscan)
- Zero Day Exploit Alarming
- Incident Response Service

## Additional Solutions

- PenTesting
- Workshops
- Awareness Training
- Security Assessments

# Security Operation Center – Services & Solutions

1. Level - Operator
2. Level - Analyst
3. Level - Forensiker

Operations Manger
SOC Consultants
Fach Consultants

## Security Event Monitoring

### SOC Start

- (Co-) Managed Security-Event Monitoring
- (Co-) Managed DER

### SOC complete

- Paket S
- Paket M
- Paket L

## Additional Services

- V-SCAN (Schwachstellenscan)
- Zero Day Exploit Alarming
- Incident Response Service

## Additional Solutions

- PenTesting
- Workshops
- Awareness Training
- Security Assessments

# Nutzen eines SOC

## PREVENTION

- Planung von Vorsorgemaßnahmen
- Vordefinierte Handlungsanweisungen auf Sicherheitsvorfälle (Runbooks)
- Erkennung und Eliminierung von Schwachstellen
- Erfahrungsaustausch und Nutzung von Security Best Practices

## DETECTION

- Professionelle Unterstützung im Angriffsfall durch Cyber-Security-Experten
- Registrierung und zentrale Protokollierung sicherheitsrelevanter Vorgänge
- Minimierung bzw. kein Reputationsverlust durch rechtzeitige Schadenserkennung
- Forensische Analyse von Vorfällen, um den Angriff zu verstehen und geeignete Schutzmaßnahmen abzuleiten

## COMPLIANCE

- Einhaltung gesetzlicher Vorgaben, zum Beispiel NIS-2 und IT-SiG 2.0
- Erhöhung der Betriebssicherheit durch Risikominimierung von Geschäftsausfällen

## ECONOMICS

- Investitions- und Personalkosten für Etablierung u. Betrieb eines eigenen SIEM / SOC einsparen, denn Managed Services sind oft günstiger als Eigenerbringung
- Mögliche Einsparungen bei Cyber-Versicherungsprämien durch Reifegradermittlung der Unternehmens-IT
- Hohe Skalierbarkeit durch vorhandene und automatisierbare Security-Plattformen

# #3 SOS! Gehackt – und nun?

## Tatortreiniger Incident Response Team (IRT)

# Cyberangriff? – SHD hilft!

Incident Responder /
Security Consultant

Krisenmanager /
Ermittlungsleiter

Forensiker


XDR Lösung

Verbrauchsmaterial

Analyse Hardware

# Incident Response - Notfall Bewältigung - Desaster Recovery


Notfallplan ?

Notfallstab / Krisenstab

Lage-bewertung → RCA/ Forensik → Cleaning → Recovery Restore → Normal-betrieb

IRT Einsatzleitung

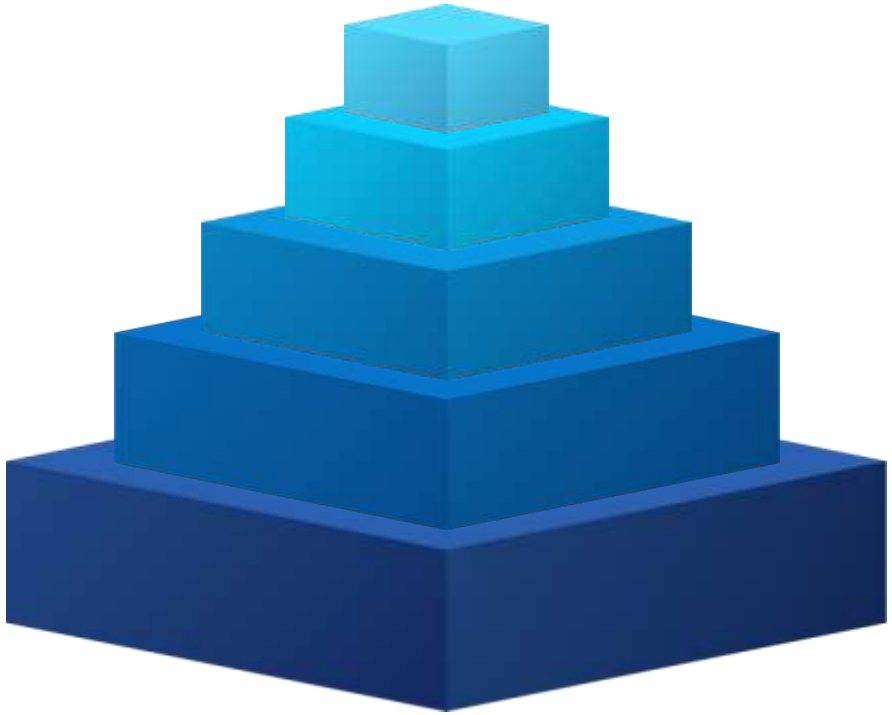
Security Consulting, Forensik

Incident Responder

Infrastruktur Expert

Administration, Operation

# Incident Response Team – Notfall Bewältigung



Notfallübungen

Incident Response DL

Log-Management (forensic readyness)

Wiederanlaufpläne (BIA)

Notfallplanung

**Das sichere Fundament → Cyber Resilienz**

# Deutsches Incident Response Team (DIRT)

Sie benötigen schnelle Hilfe bei einem CyberVorfall? Wir sind für Sie da.
Mit deutschen Unternehmen - bundesweit.


DIRT.
Deutsches Incident Response Team.

Compass Gruppe
IT-Quality at work.

Cyber-Sicherheitsnetzwerk

Bundesamt für Sicherheit in der Informationstechnik

SHD.

WIR BEWEGEN IT.

## Ihr Ansprechpartner

Thomas Beckert
Cyber Security Consultant

thomas.beckert@shd-online.de

- IT-Infrastruktur Services
- IT-Sicherheit
- Managed und Cloud Services
- Professioneller IT-Service
- Digitale Transformation

SHD System-Haus-Dresden GmbH
Drescherhäuser 5b · 01159 Dresden

# Zeit für Diskussion.


SHD.
WIR BEWEGEN IT.