# Bedrohungen, Anforderungen und Beispiele zur gesetzeskonformen Umsetzung der vorgeschriebenen Monitoring-Lösung

René Odermann
Account Director CyberSecurity


telent
service • commitment • value

# Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

## Top 3-Bedrohungen je Zielgruppe:

**Gesellschaft**

Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

**Wirtschaft**

Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

**Staat und Verwaltung**

Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

## Erster digitaler Katastrophenfall in Deutschland

**207 Tage Katastrophenfall**

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

## Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

**116,6 Millionen** zugenommen.

## Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

## Kollateralschaden

nach Angriff auf Satelliten-kommunikation

**20.174**

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

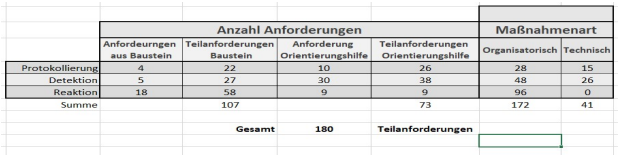
# IT SIG 2.0 Anforderungen

| | Anzahl Anforderungen | | | | Maßnahmenart | |
|---|---|---|---|---|---|---|
| | Anfordeurngen aus Baustein | Teilanforderungen Baustein | Anforderung Orientierungshilfe | Teilanforderungen Orientierungshilfe | Organisatorisch | Technisch |
| Protokollierung | 4 | 22 | 10 | 26 | 28 | 15 |
| Detektion | 5 | 27 | 30 | 38 | 48 | 26 |
| Reaktion | 18 | 58 | 9 | 9 | 96 | 0 |
| Summe | | 107 | | 73 | 172 | 41 |
| | | **Gesamt** | **180** | **Teilanforderungen** | | |

- Betrachtung der gesamten Anforderungen
- Aufgliederung in Anforderungen und Teilanforderungen
- Trennung in organisatorisch und technische Anforderungen

telent
service • commitment • value

# Konkrete Beispiele bei der Aufteilung der Anforderungen



| | Anzahl Anforderungen | | | | Maßnahmenart | |
|---|---|---|---|---|---|---|
| | Anfordeurngen aus Baustein | Teilanforderungen Baustein | Anforderung Orientierungshilfe | Teilanforderungen Orientierungshilfe | Organisatorisch | Technisch |
| Protokollierung | 4 | 22 | 10 | 26 | 28 | 15 |
| Detektion | 5 | 27 | 30 | 38 | 48 | 26 |
| Reaktion | 18 | 58 | 9 | 9 | 96 | 0 |
| Summe | | 107 | | 73 | 172 | 41 |
| | | Gesamt | 180 | Teilanforderungen | | |

## Aufgabe des Betreibers

## Betreiber & Dienstleister

## Dienstleister

### Beispiele Protokollierung:

Die spezifische Sicherheitsrichtlinie MUSS vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden.

Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.

Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.

### Beispiele Detektion:

Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden.

Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden.

Jeder Benutzer MUSS die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 Behandlung von Sicherheitsvorfällen)..

### Beispiele Reaktion:

In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist.

Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MUSS der Zuständige zunächst das Problem eingrenzen und die Ursache finden.

Zudem MÜSSEN alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des Problems geben könnten.

telent
service • commitment • value

## Kommende weitere Anforderungen – NIS 2

- Zusätzlich zu den bereits bestehen Betreiber kritischer Anlagen (KRITIS-Betreiber) werden wichtige und besonders wichtige Einrichtungen innerhalb der Sektoren dazu verpflichtet höhere Security Anforderungen umzusetzen

- NIS 2 Umsetzung in DEU: Entwurf liegt seit April 23 vor

- Etwa 30.000 Unternehmen werden betroffen sein

- Soll im Oktober 2023 in Kraft treten

- Besonders wichtige §28 (6) und wichtige **Einrichtunge**n §28 (7) werden nach Größe des Unternehmens identifiziert, es gibt dabei mittlere und große Unternehmen:

  a. Mittlere Unternehmen, zwei Möglichkeiten:

  50 bis 249 Mitarbeiter und Umsatz weniger 50 Mio EUR oder Bilanz weniger 43 Mio EUR

  **oder**

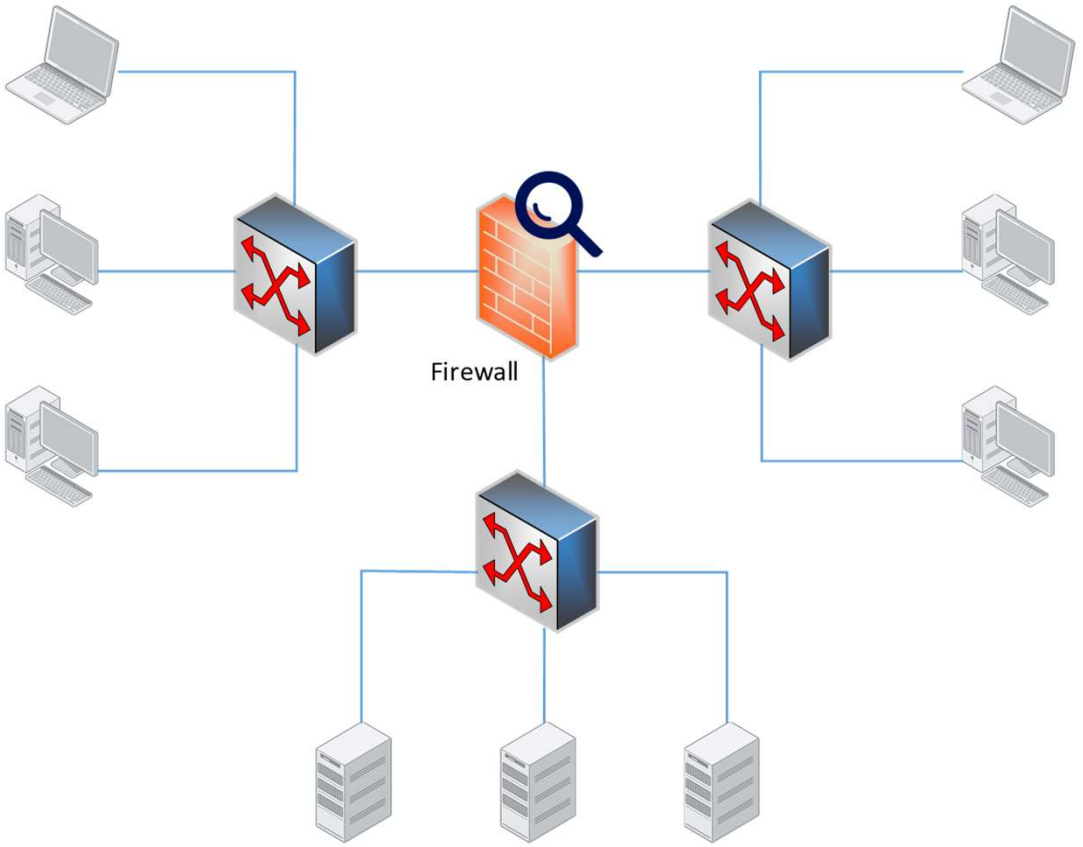
  Weniger 50 Mitarbeiter und Umsatz 10-50 Mio EUR und Bilanz 10-43 Mio EUR

  b. Großunternehmen, zwei Möglichkeiten:

  Mindestens 250 Mitarbeiter **oder** ab 50 Mio. EUR Umsatz und Bilanz ab 43 Mio EUR

# Ausbauvariante A
# Firewall + NGFW Features

- Umsetzung mit bestehender Infrastruktur
- IDS / IPS (Blacklisting)
- Auswertung Firewall Logs
- Analyse aller Edge-Daten




PLANUNGSPHASE

- Basismaßnahmen umgesetzt?
- Relevante Angriffsvektoren definiert?
- Netzpläne und Assets sauber dokumentiert?

UMSETZUNG

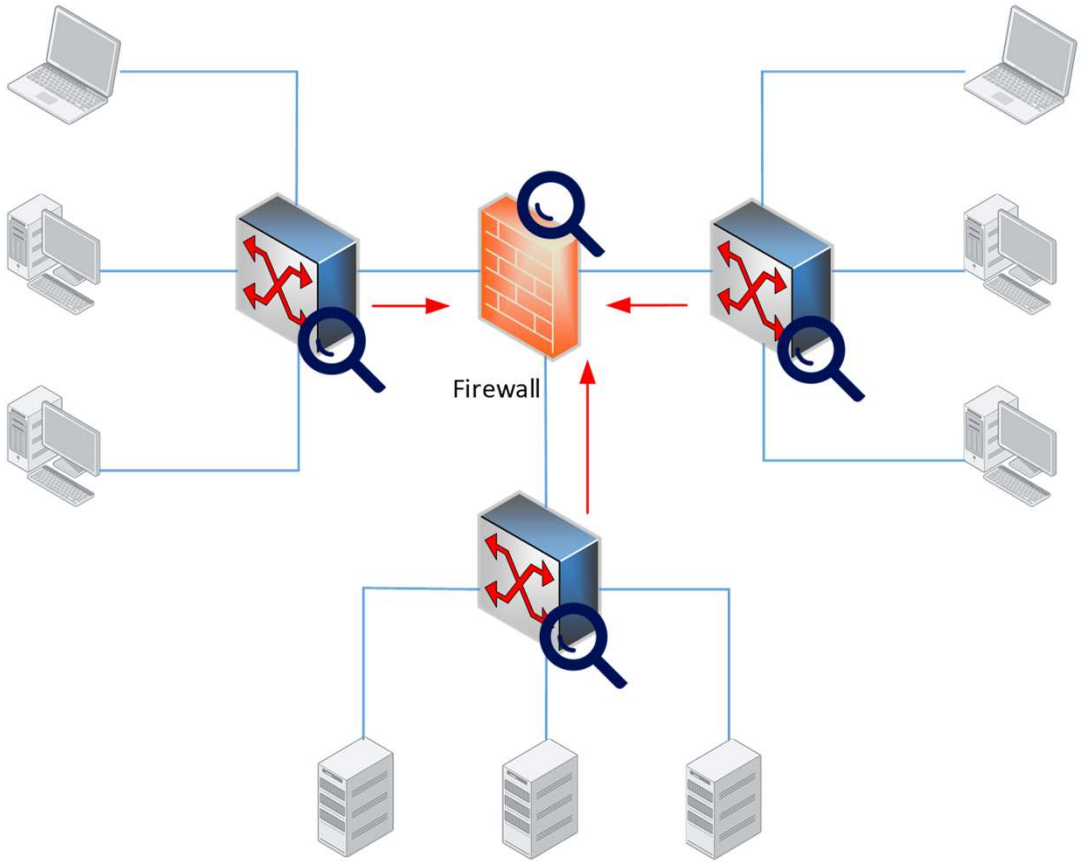
- Sind die Netzwerke-Switche SPAN-fähig? Ports frei?
- Platzierung der Mirroring/SPAN-Ports
- System in einen „sauberen“ Zustand zu bekommen



telent
service • commitment • value

# Ausbauvariante A*
# Firewall + NGFW Features

- Umsetzung mit bestehender Infrastruktur
- IDS / IPS (Blacklisting)
- Auswertung Firewall Logs
- Analyse aller Netzwerkdaten

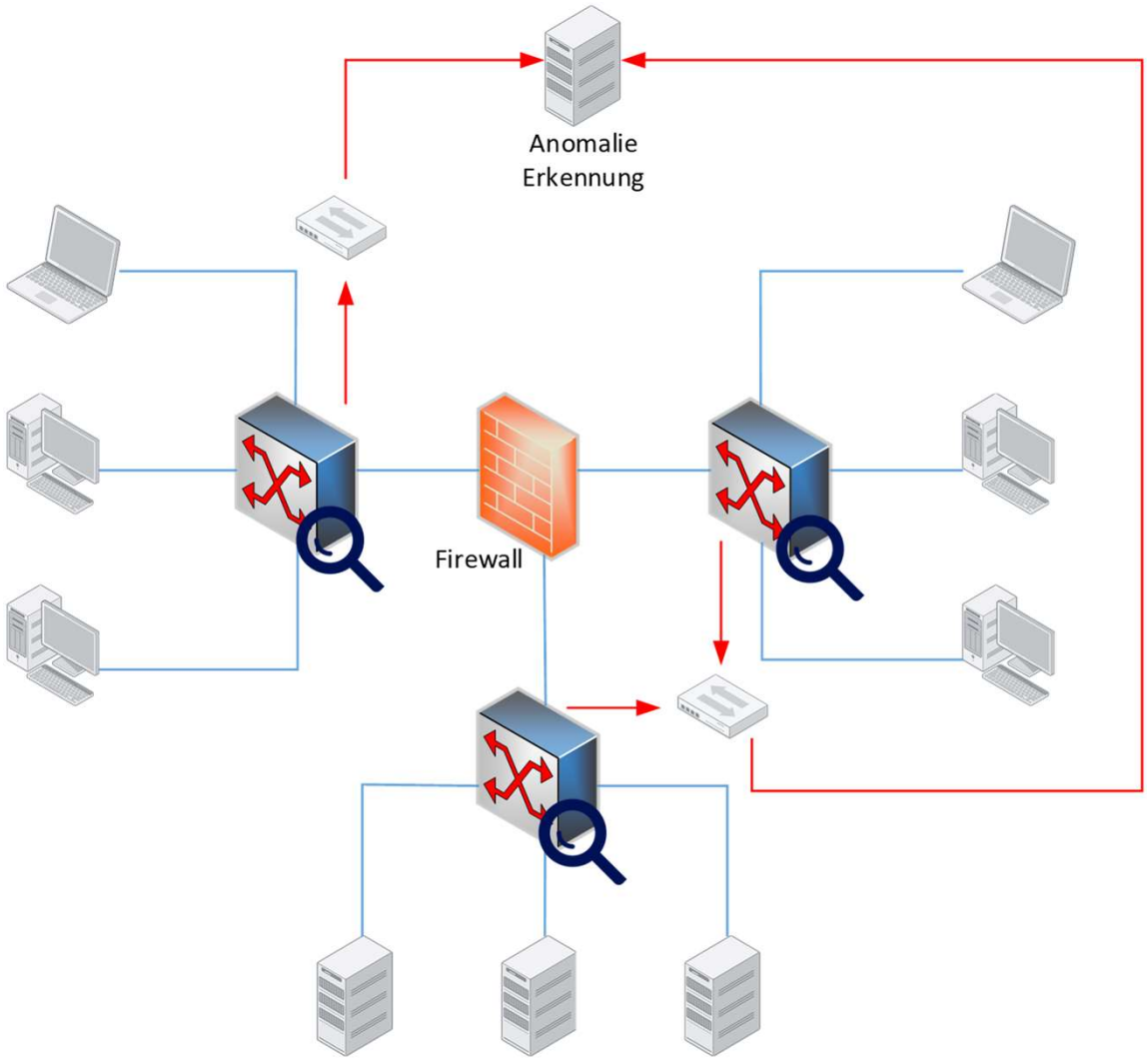





telent
service • commitment • value

# Ausbauvariante B
# Anomaly-Detection

- Zusätzliches Anomalie-Erkennungs-Produkt
- Anomalie-Erkennung (Whitelisting)
- Anbindung  Log/SIEM- Server
- Analyse aller Netzwerkdaten
- Asset-DB / Netzwerkkarte
- Schwachstellenerkennung

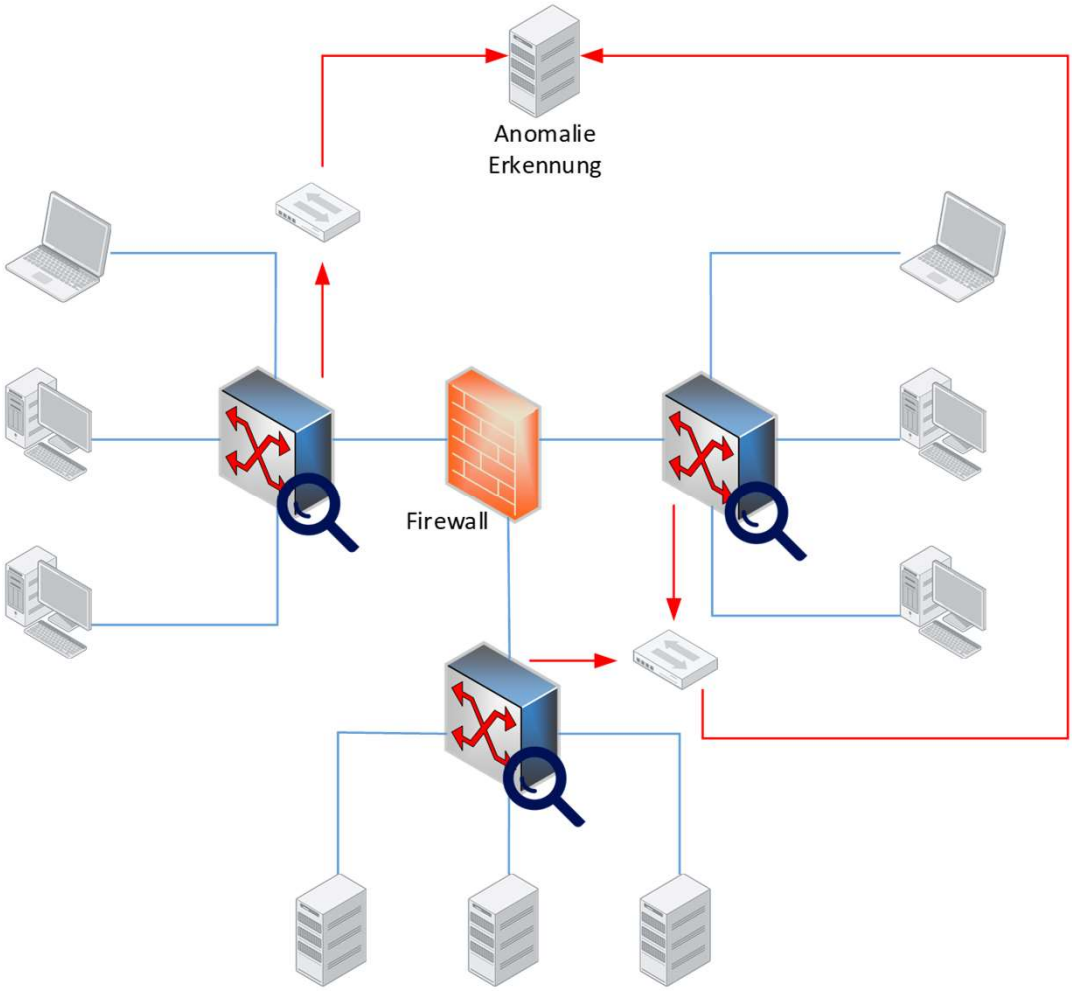





telent
service • commitment • value

# Ausbauvariante C
# Anomaly-Detection + Scanner

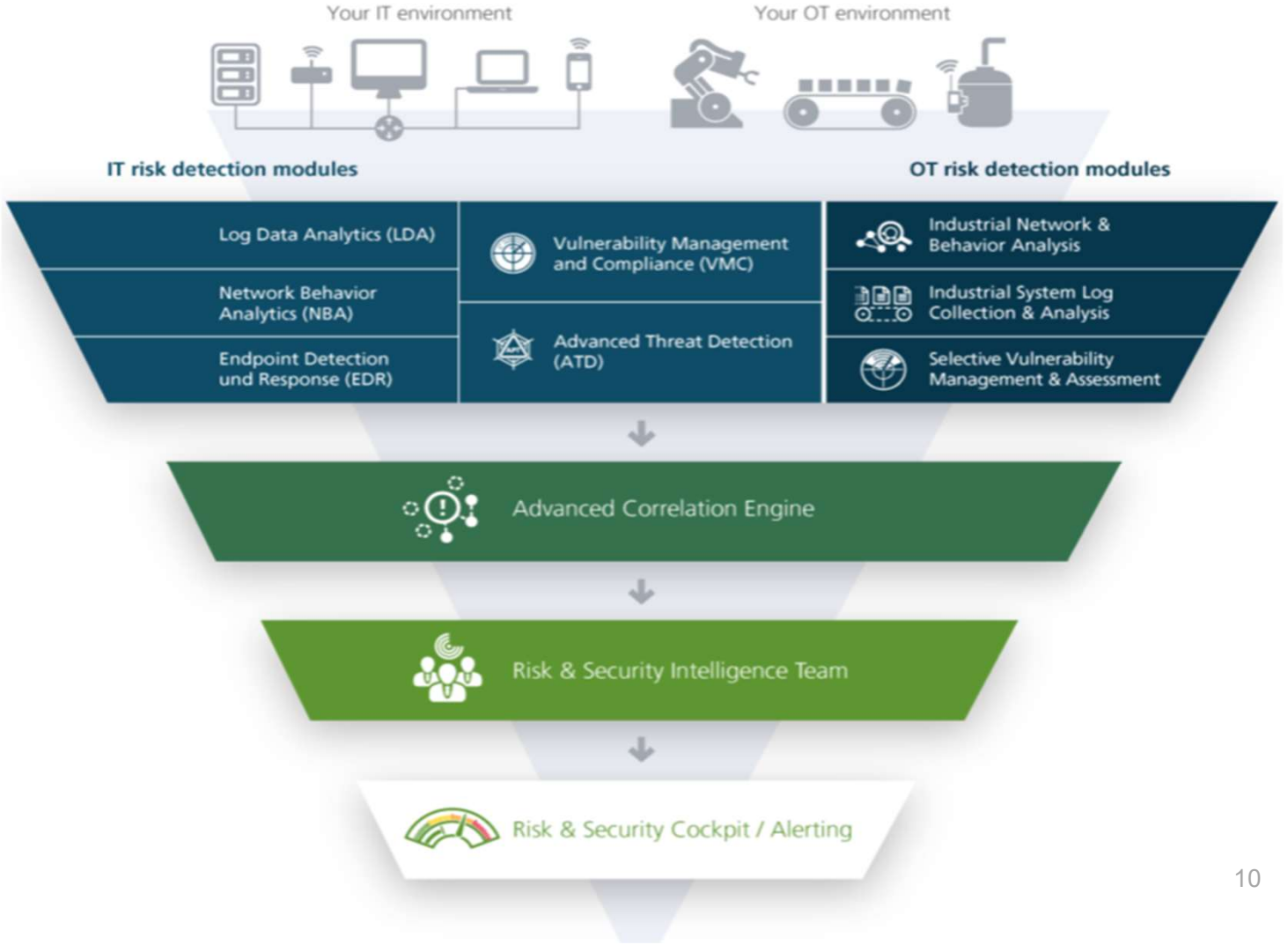
- Zusätzlicher automatisierter Schwachstellen-Scan
  - Automatisierter Prozess
  - Aktive Schwachstellensuche
  - **Vorsichtige Implementierung sehr wichtig**






telent
service • commitment • value

# Ausbauvariante D
# Security Operation Center






telent
service • commitment • value

## Best Practice Ansätze

- K.I.S.S (Keep it simple and safe)
- wachsende Umsetzung anstreben
- auf Unterstützung der eingesetzen Industrie Protokolle achten
- Vorbereitung/Verwendung SIEM/SOC

# VIELEN DANK



telent
service • commitment • value