ACP IT Solutions AG

Hauzenberg • Regensburg • Nürnberg

www.acp.de

IT for innovators.

ACP

Cyber Security Forum 2023

IT for innovators.

ACP

Grundlagen der OT Security

IT for innovators.

ACP

Vier Schritte zur gemeinsamen Strategie

1) Beidseitiges Verständnis

2) Planung der Netzwerkinfrastruktur

3) Definierter IT-/OT-Netzwerkübergang

4) Übergreifende IT-/OT-Security-Konzepte

IT for innovators.

Die vier Säulen der Informationssicherheit

Verfügbarkeit

Integrität

Vertraulichkeit

Authentizität (Stichpunkt M2M Kommunikation via Zertifikat)

Die vier Säulen der Informationssicherheit

☑Verfügbarkeit

? Integrität

? Vertraulichkeit

? Authentizität

In Produktionsumgebungen kommt auch „Safety“ noch hinzu

Unsere Testumgebung ist nach wenigen Minuten installiert und erfordert keine Unterstützung der IT-Abteilung. Sie benötigen lediglich eine Mobilfunk Netzabdeckung. **Buchen Sie deshalb noch heute eine kostenlose Testumgebung und analysieren Sie bereits morgen Ihre Daten!**

Die Herausforderungen

- ✓ Produktionsnetzwerke die mittlerweile stark in die Jahre gekommen sind
- ✓ Heterogene Maschinenparks mit unterschiedlichen, auch älteren Steuerungen und Betriebssystemen zuverlässig abzusichern
- ✓ Safety-Bestimmungen
- ✓ Echtzeit-Ansprüchen von Industrie 4.0 und Digitalisierung
- ✓ Anbindung bisher isolierter Maschinen an das Netzwerk
- ✓ Fernzugriff auf Maschinen in der Anlage
- ✓ Verarbeitung von Betriebsdaten über Edge- und Cloud Computing
- ✓ Bereitstellung eines sicheren Netzwerkkonzepts von der Zellen- bis zur Industrial Backbone-Ebene

Zusammenspiel Physischer & Digitaler Komponenten

Messwerte aus der physischen Welt können durch Sensoren digitalerfasst, in der digitalen Welt gespeichert und analysiert werden, und mittels Aktoren zur Steuerung physischer Vorgänge genutzt werden

- *… entfalten großes Potenzial in der „Operational Technologie“*
- *… ermöglichen Digitalisierung in ursprünglich „analogen“ Bereichen*
- *… eröffnen neue Geschäftsfelder und Produktinnovation*
- *… bedürfen neuer Programmierparadigmen*
- … erfordern aber auch neue Sicherheitskonzepte und Risikoanalysen

Alarm Hackerangriffe auf Produktionen…

Top 10 Bedrohungen der OT 2022

Top 10 Bedrohungen	Trend seit 2019
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	
Infektion mit Schadsoftware über Internet und Intranet	
Menschliches Fehlverhalten und Sabotage	
Kompromittierung von Extranet und Cloud-Komponenten	
Social Engineering und Phishing	
(D)DoS Angriffe	
Internet-verbundene Steuerungskomponenten	
Einbruch über Fernwartungszugänge	
Technisches Fehlverhalten und höhere Gewalt	
Soft- und Hardwareschwachstellen in der Lieferkette	

Quelle: Allianz-für-Cybersicherheit

Die
EU – NIS2 Direktive

Autor: Ricardo Graf, ACP HAL

IT for innovators.

Was ist die NIS2 – Direktive?

- NIS = Network and Information Security
  - Rahmenwerk für Betreiber kritischer Infrastrukturen
  - Legt EU – weite Mindeststandards für Cyber Security fest
  - Gestaltungsspielraum nur für höheres Cybersicherheitsniveau

- Wesentlich größerer Geltungsbereich als Kritis
  - Bedeutet mehr betroffene Unternehmen
  - Strikte Überwachung & Aufsicht durch Behörden

Sanktionen:
bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Vorjahresumsatzes

IT for innovators.

Gesetzliche Rahmen

Geltungs-bereich	Bezeichnung	Status	Betroffen-heit	IT Security	OT Security	Product Security
Deutschland	**IT-Sicherheitsgesetz 2.0**	Aktiv 28.05.2021		x		(x)
Deutschland	**NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz (NIS2UmsuCG)**	Referenten-entwurf 03.07.2023		x	x	(x)
EU	**Funkanlagenrichtlinie – Delegierter Rechtsakt** Umsetzungsfrist 01.08.2024	Inkraft seit 01.02.2022 hEN in Arbeit				x
EU	**NIS2 Richtlinie** (Umsetzung in Deutschland durch das NIS2UmsuCG)	Inkraft seit 16.01.2023 Umsetzungsfrist 10/2024		x	x	(x)
EU	**Cyber Resilience Act**	Abstimmung EP, Start Tilog 10/ 2023		(x)		x

Quelle:https://www.vdma.org/documents

NIS2 - Sektoren

- Essential
  - Energie
  - Transport
  - Bankwesen
  - Finanzmärkte
  - Gesundheit
  - Trinkwasser
  - Abwasser
  - Digitale Infrastruktur
  - ICT Service Management
  - Öffentliche Verwaltung
  - Weltraum
- Important
  - Post und Kurier
  - Abfall
  - Chemikalien
  - Lebensmittel
  - Industrie (Herstellung)
  - Digitale Dienste
  - Forschung

Die meisten Sektoren mit diversen Untersektoren

IT for innovators.

Wer ist betroffen?

- Große Betreiber
  - >250 Beschäftigte, >50 Mio € Umsatz, >43 Mio € Bilanzsumme
- Mittlere Betreiber
  - 50 – 250 Beschäftigte, 10 – 50 Mio € Umsatz, <43 Mio € Bilanzsumme

Diverse Sonderfälle unabhängig von Unternehmensgröße

IT for innovators.

NIS2 – Sektoren - Wer ist betroffen

- Energie
- Transport
- Bankwesen
- Finanzmärkte
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- ICT Service Management
- Öffentliche Verwaltung
- Weltraum

- Post und Kurier
- Abfall
- Chemikalien
- Lebensmittel
- Industrie (Herstellung)
- Digitale Dienste
- Forschung

Beispiele

Großer Energieversorger, 50 Tsd MA, 10 Mrd. Umsatz *teilw. kritis*

IT-Systemhaus, 300 MA, 60 Mio. Umsatz

Kommunales Stadtwerk, 50 MA, 11 Mio Umsatz

Hersteller Autositze, 65 MA, 15 Mio. Umsatz

IT for innovators.

Quelle https://www.openkritis.de/r/Briefing_IT-Sicherheitsgesetz_2_0_DE.pdf)

Mindestanforderungen – Cyber Security Maßnahmen

- **Policies**: Richlinien für Risikomgmt. und Informationssicherheit
- **Incident Management**: Prävention, Detektion und Bewältigung von Cyber Incidents
- **Business Continuity**: BCM mit Backup Management, DR, Krisenmanagement
- **Supply Chain**: Sicherheit in der Lieferkette — Lieferantenaudits
- **Einkauf**: Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
- **Effektivität**: Vorgaben zur Messung von Maßnahmen
- **Training:** Awareness- und Sicherheitsschulungen
- **Kryptographie**: Vorgaben für Kryptographie – Einsatz Verschlüsselung wo möglich
- **Personal**: Human Resources Security
- **Zugangskontrolle**
- **Asset Management**
- **Authentication**: Einsatz von Multi Factor Authentisierung und SSO
- **Kommunikation**: Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- **Notfall-Kommunikation**: Einsatz gesicherter Notfall-Kommunikations-Systeme

Das impliziert die Einführung eines ISMS

IT for innovators.

Fristen & Vorgehen

- Derzeit keine Festlegungen, fundierte Vermutung für „important Entities“
  - Basis: Festlegungen für Unternehmen im besonderen öffentlichen Interesse im IT-SiG 2.0
  - „Kritis-light“

- Registrierung
  - Frist: zwei Jahre
  - Registrierung bei BSI unter Abgabe „Selbsterklärung zur IT-Sicherheit“
  - Danach alle zwei Jahre Selbsterklärung neu vorlegen

- Inhalt Selbsterklärung zur IT-Sicherheit
  - Nachweise:
    - Zertifizierungen der IT-Sicherheit der letzten zwei Jahre
    - Sonstige Sicherheitsaudits und Prüfungen der IT-Sicherheit der letzten zwei Jahre
    - Beides jeweils mit Prüfgrundlage und Geltungsbereich
  - Sicherheitsmaßnahmen
    - Für besonders schützenswerte IT-Systeme, Komponenten & Prozesse
    - Nach aktuellem Stand der Technik

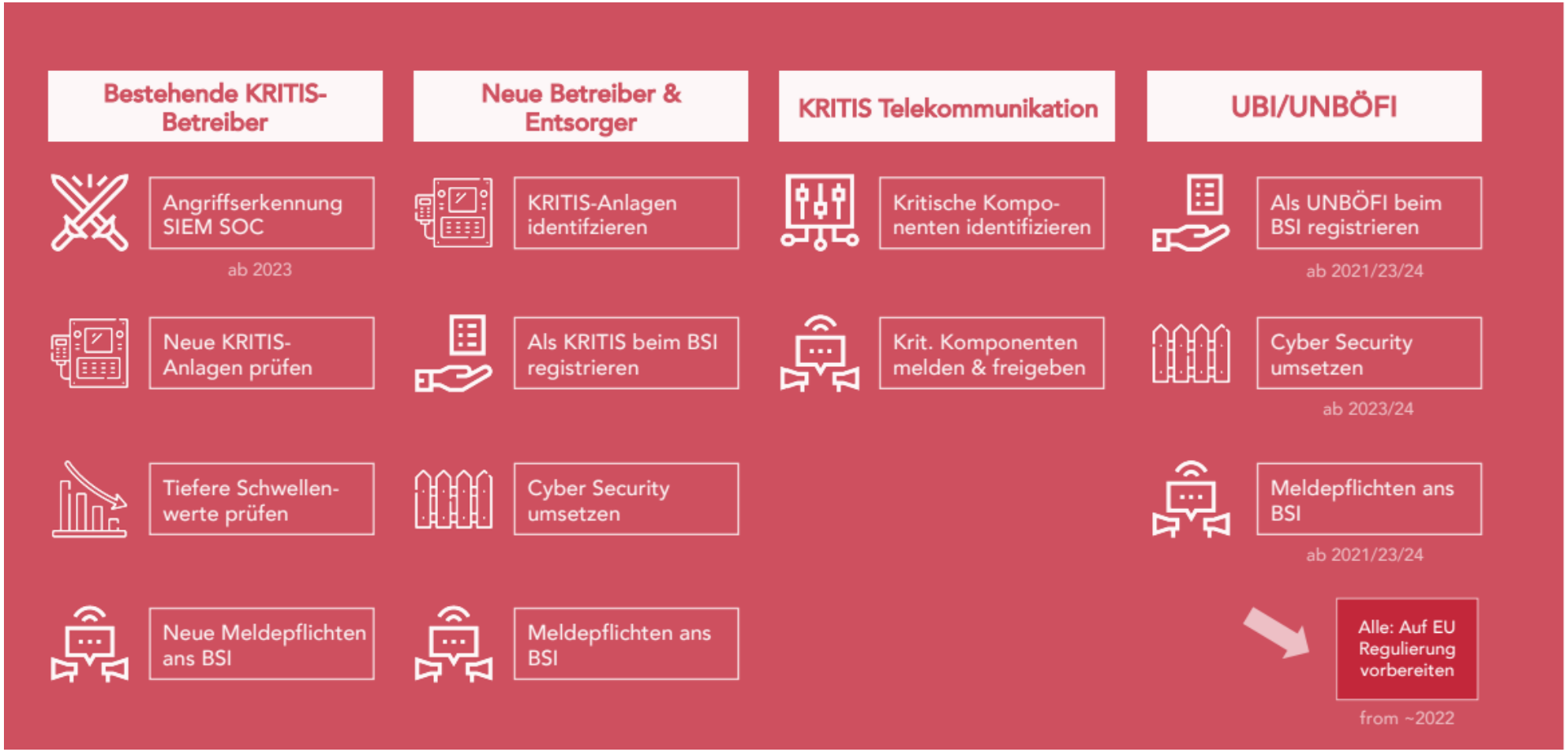
- Für „essential Entities“ wird das eher härter => Kritis

IT for innovators.

Übersicht Gesetze

Gesetz	Kurzform	KRITIS-Relevanz
BSI-Gesetz		•Rechte und Pflichten des BSI gegenüber KRITIS-Betreibern •Definitionen zu KRITIS wie Sektoren, Mindeststandards •Anforderungen und Pflichten von KRITIS-Betreibern
Energiewirtschaftsgesetz	EnWG	•Meldewesen an das BSI •Mindeststandards und Sicherheitsanforderungen Betreiber
Telekommunikationsgesetz	TKG	•Meldewesen an das BSI •Mindeststandards und Sicherheitsanforderungen Anbieter
Atomgesetz	AtG	•Meldewesen an das BSI
Telemediengesetz	TMG	•Anforderungen und Pflichten von Diensteanbietern
BKA-Gesetz	BKAG	•Befugnisse in der Strafverfolgung
Weitere	BBesG BGebGEG	•diverses

Wer muss nun was machen?



Quelle https://www.openkritis.de/r/Briefing_IT-Sicherheitsgesetz_2_0_DE.pdf)

Zurück zur OT

IT for innovators.

OT als „kritische“ Infrastruktur

Security Maßnahme	IT	OT
Antivirus/Malware	Standard und Stand der Technik	Kompliziert und oft nicht implementierbar
Life Cycle	3-5 Jahre	5-20 Jahre
Awareness	hoch	nicht so hoch
Patch Management	regelmäßig	selten in Abhängigkeit der Produktion
Change Management	regelmäßig	in Abhängigkeit der Komponenten, eher weniger
Logdaten Auswertung	etabliert bzw. zunehmend etabliert	meist nur im Bereich der Maschinendaten
Zeitkritisch	Verzögerungen aktzeptiert	Echtzeit
Verfügbarkeit	wichtig aber gaps möglich	24/7
IT Security Awareness	steigend bis hoch	nicht sehr ausgeprägt
Security Tests	üblich	aufwändig
Test Umgebungen (labs)	gängig	aufwändig

ROI für Ransomware

Kosten Entwicklung Ransomware
- 160 h, 200 €/Stunde

Kosten gemietete Infrastruktur
- 10 Server (50 € / Server)

Kosten Ransomeware Attacke
- Startknopf drücken
- Monitoring für 10 Tage (240 h / 150 €)

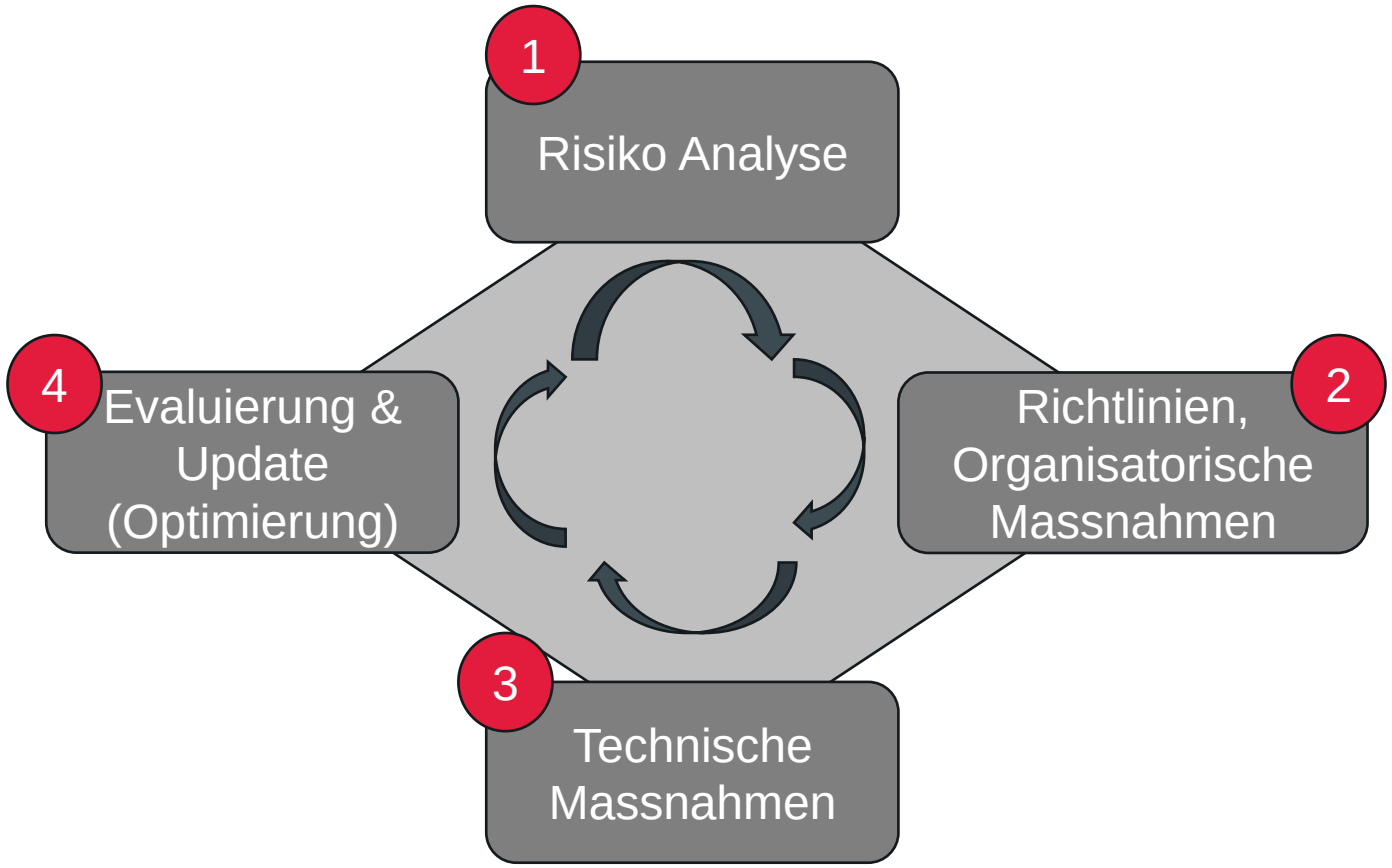
Angriff auf 1 Mio Ziele
- 1% bezahlt € 300 / System

	Kosten
Entwickler	€ 32.000
Infrastruktur	€ 500
Launch der Attacke	€ 50
Help Desk	€ 36.000
Gesamt	€ 68.550
1% erzielter Anteil	€ 3000.000
Gewinn ROI	€ 2.931.450

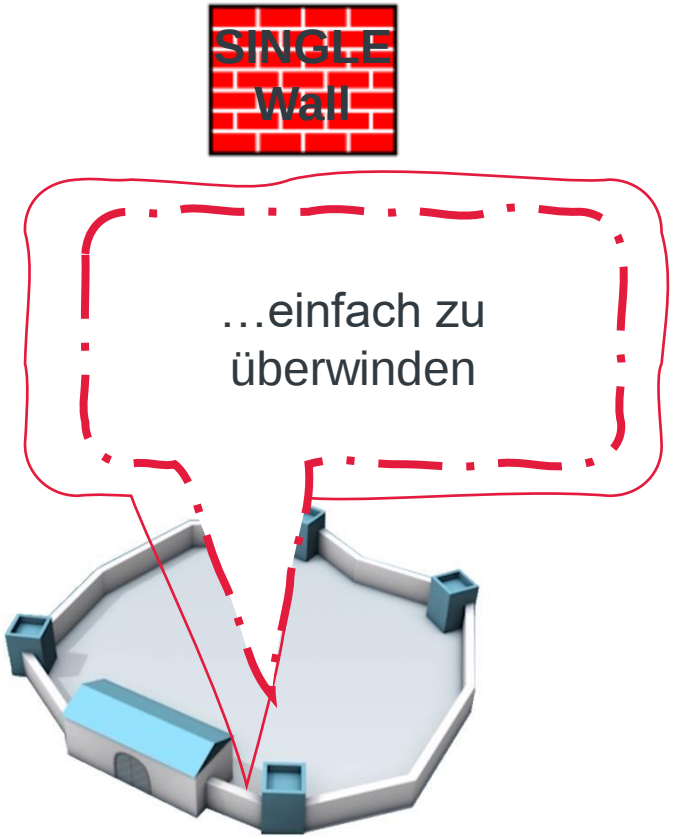
Abwehrstrategien

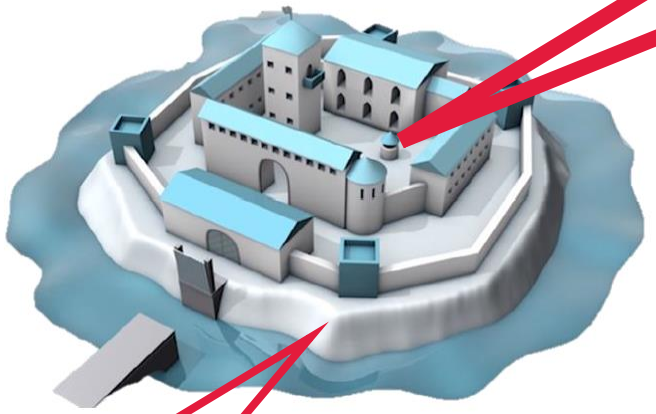
1. Die Gefahr verstehen
2. Ein Zielbild für die OT-Security entwickeln
3. Integration in eine Cyber-Sicherheitsstrategie
4. IT- & OT-Strategie budgetieren und umsetzen

OT Security als Prozess

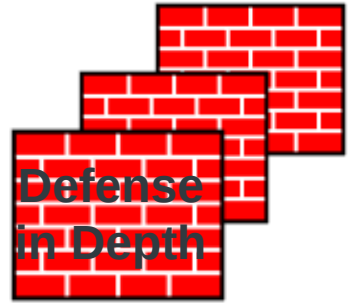


Verteidigungsstrategien auf Basis des ISA/IEC 62443



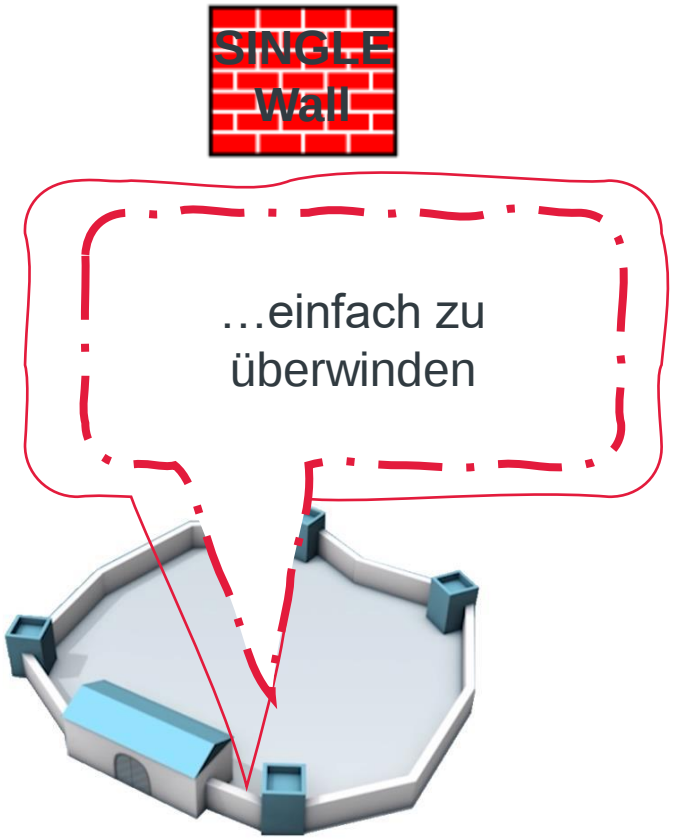


…und erschweren es den Angreifern sich (unbemerk) auszubreiten

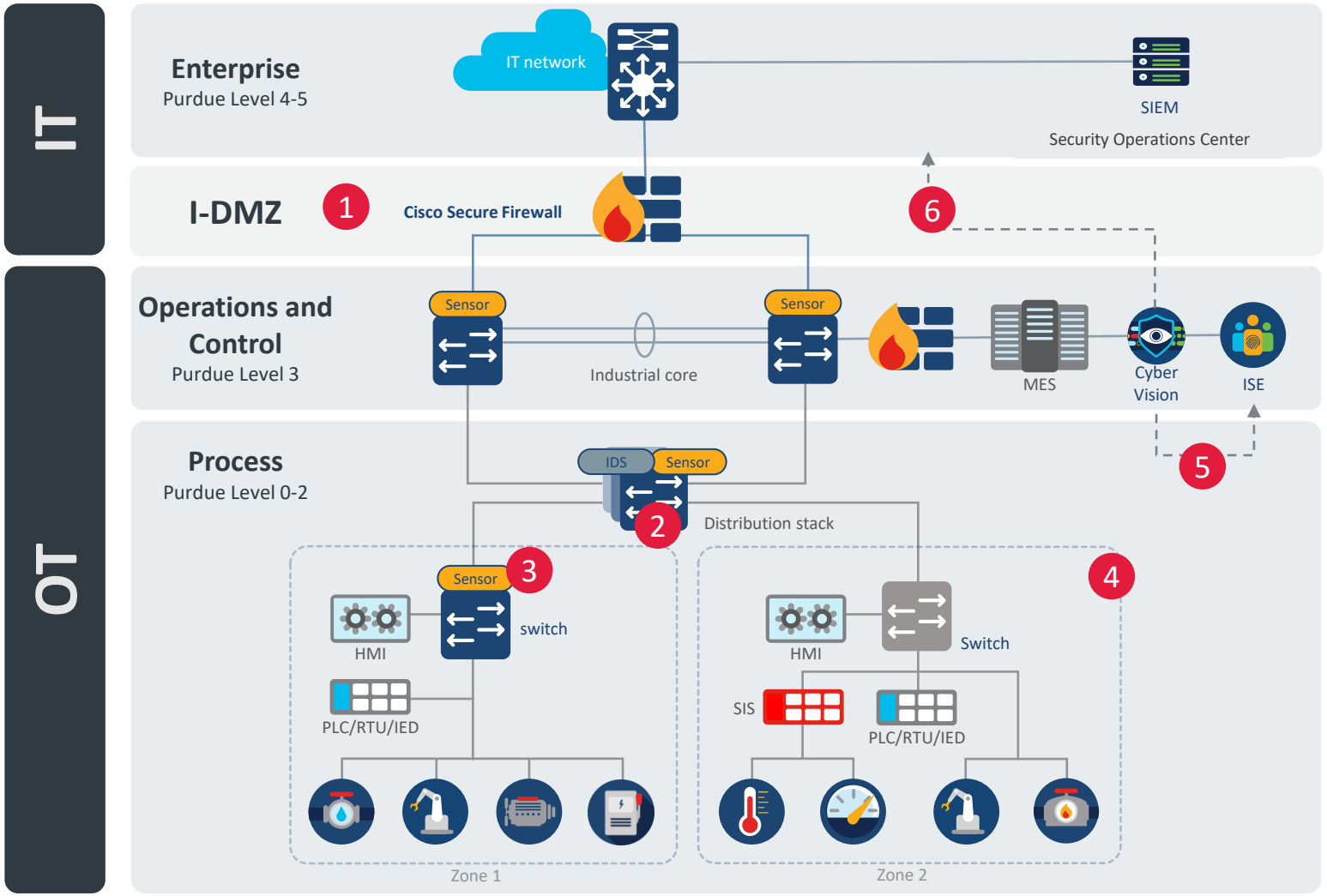


Mehrere voneinander unabhängige Layer verringern die Angriffsfläche…

Verteidigungsstrategien auf Basis des IEC 62443



OT Security Maßnahmen



1. Isolieren Sie IT und OT durch die Installation einer industriellen DMZ mit Cisco Secure FW
2. Erstellen Sie Makrosegmentierungszonen in den Catalyst Switches der Serie 9300 und stellen Sie Cyber Vision-Sensoren mit Snort IDS bereit.
3. Cyber Vision-Sensoren, die in Segmenten von IE3400-Switches eingesetzt werden
4. Cyber Vision-Hardwaresensoren, die über One-Hop-SPAN bereitgestellt werden, um Transparenz auf Switches anderer Hersteller zu
5. erzielen
6. Erstellen Sie Zonen und Conduits in Cyber Vision und teilen Sie sie mit der ISE für die Mikrosegmentierung

   Cyber Vision teilt Details zu OT-Geräten und -Ereignissen mit dem SOC, um fundierte Sicherheitsrichtlinien zu erstellen und Bedrohungen domänenübergreifend zu untersuchen

Roadmap

Bestandsaufnahme / Risiko Analyse (Healthcheck)

Begehung, Befragung, Netzwerkpläne, Abhängigkeiten

Netzwerkanalyse (Tools) Transparenz Sichtbarkeit

- Monitoring
- System Integrität (Konfigurationen etc.)
- Kommunikationsbeziehungen

Netzwerk Security

Handlungsempfehlungen

Nächste Schritte, Grobkonzept

Überprüfung und Verbesserungen

Unsere Leistungen

erbracht vom SOC Team

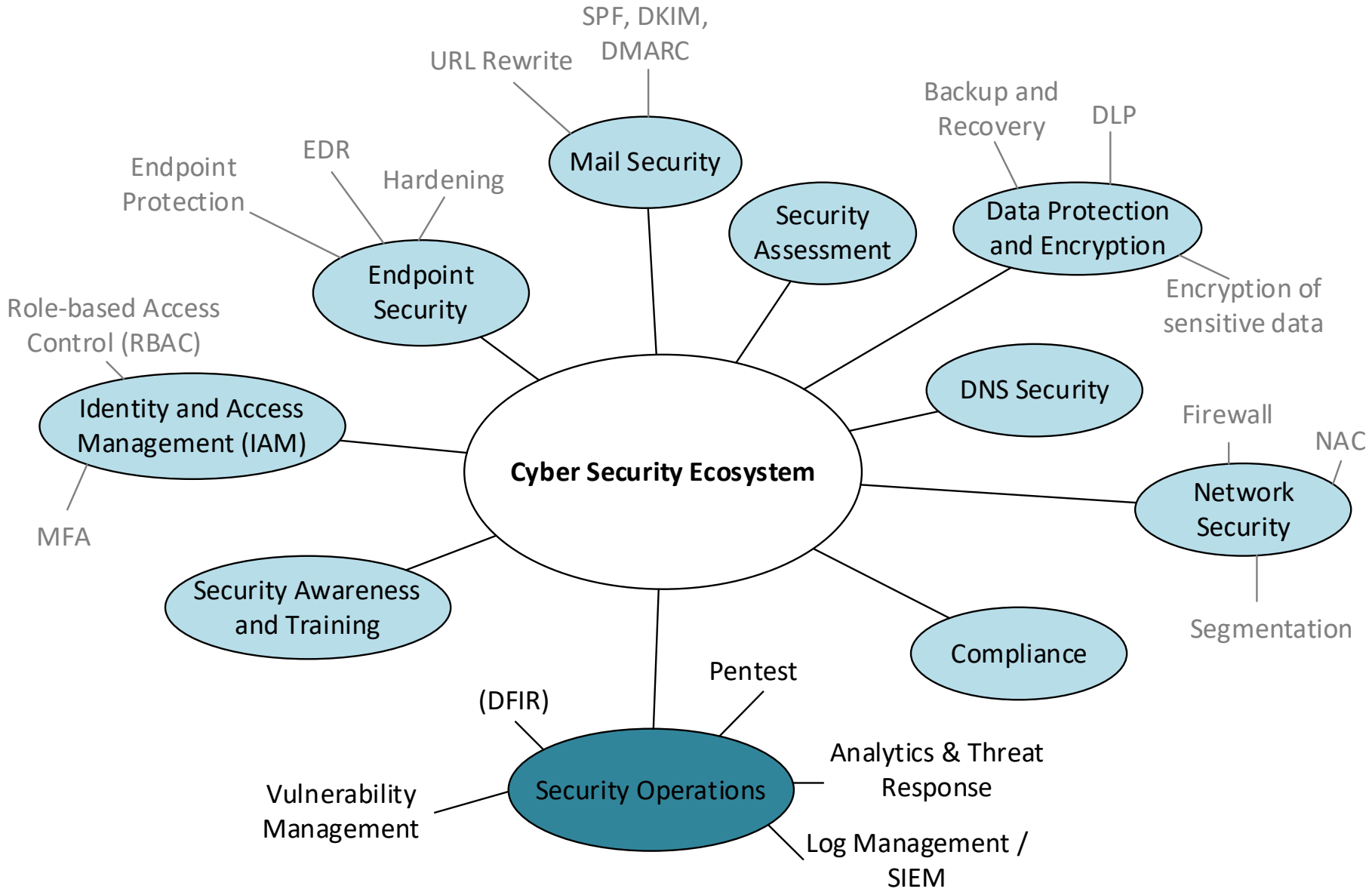
IT for innovators.

ACP

Cybersecurity Ecosystem

IT for innovators.

Cybersecurity Ecosystem



Fragen?
Antworten.

IT for innovators.