ENTIRE TEC

PLS

# IT/ OT SOLUTION DAY

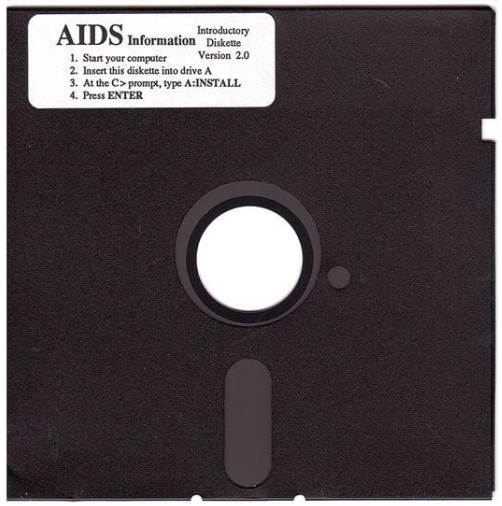
## *Netzwerk- & Security-Architektur für die Anforderungen moderner Industrie- und Produktionsumgebungen*

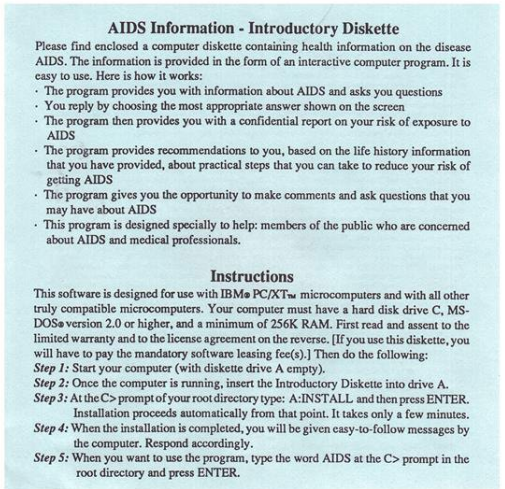
Thomas Herrmann, Patrick Christ

07.03.2023

# 1. Ransomware

## AIDS - 1989

**AIDS Information - Introductory Diskette**

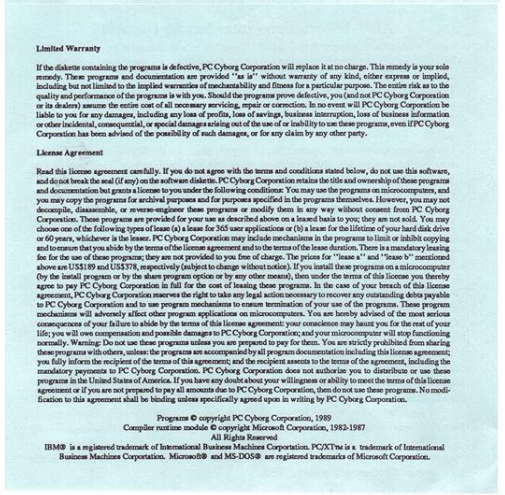
Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

**Instructions**

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

*Step 1:* Start your computer (with diskette drive A empty).
*Step 2:* Once the computer is running, insert the Introductory Diskette into drive A.
*Step 3:* At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
*Step 4:* When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
*Step 5:* When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.



**Limited Warranty**

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

**License Agreement**

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corporation. PC/XT™ is a trademark of International Business Machines Corporation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

If you install [this] on a microcomputer…
then under terms of this license you agree to pay PC Cyborg Corporation in full for the cost of leasing these programs…
In the case of your breach of this license agreement, PC Cyborg reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use…
These program mechanisms will adversely affect other program applications…
You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life…
and your [PC] will stop functioning normally…
You are strictly prohibited from sharing [this product] with others…

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                    Press ENTER to continue
```

# Cyberkriminalität

## Facts & Stats

**83%**
der Angriffe sind finanziell motiviert

2023 Verizon - Data Breach Investigations Report

**$4.45M**
Ø Kosten eines Angriffs mit Datendiebstahl

2023 Ponemon Institute - Cost of a Data Breach Report

**320 Tage**
Ø Dauer zur Erkennung eines Angriffs

2023 Ponemon Institute - Cost of a Data Breach Report

**Der präventive Ansatz hat seine Grenzen erreicht**

Komplexe und mehrstufige Ransomware Angriffe

**Supply Chain Risiken**
Solarwinds, Microsoft, Citrix, Medizingeräte, IoT, OT

Bedrohungen durch Innentäter und menschliche Fehler

**Zeit für Detection and Response**

Erkennung von Angriffen, die nicht durch Präventivmaßnahmen verhindert wurden

Erkennungszeit von 200+ Tagen auf Stunden und Minuten reduzieren

Angriffserkennungs-Systeme **verpflichtend** für betroffene Unternehmen von NIS2 ab dem 17.Oktober 2024

**75%**

der mit Ransomware infizierten Organisationen, hatten aktualisierte Endpoint Protection Systeme installiert

2022 Sophos

# Compliance und Haftung

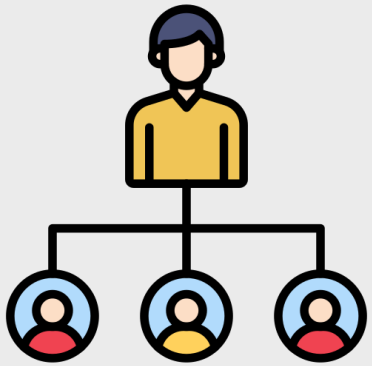
## Kontrolle und Einhaltung liegt beim Management

### IT-Compliance-Pflicht für Leitungspersonen

Unter Compliance versteht man die Pflicht von Leitungspersonen in Unternehmen, sich selbst rechtskonform zu verhalten und zu verhindern, dass aus dem Unternehmen heraus, also von Mitarbeitenden, Rechtsverstöße begangen werden. Hergeleitet wird die Pflicht zur Compliance aus der allgemeinen Sorgfalt der Leitungspersonen, § 43 GmbHG, §§ 93, 76 AktG.

### Treiber

- Änderungen aus dem IT Sicherheitsgesetz 2.0 mit der Notwendigkeit der Einführung eines Security Operations Center (SOC)
- NIS 2 Richtlinie in Umsetzung
- Seit dem 1.5.2023 sind zwingend „Systeme zur Angriffserkennung“ gefordert



# NIS2

## Wer ist betroffen von der NIS2-Richtilinie?

Es gelten grundsätzlich zwei Kriterien: erstens, die Unternehmensgröße und, zweitens, die Zugehörigkeit zu bestimmten Sektoren.

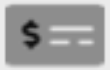
**1. Kriterium**

Unternehmen mit
- mindestens 50 Mitarbeiterinnen und Mitarbeitern und
- einem Umsatz/einer Bilanzsumme von über 10 Mio. Euro pro Jahr

fallen unter die NIS2-Richtlinie, wenn Kriterium 2 erfüllt ist.

Auch kleinere Unternehmen, die eine kritische Tätigkeit ausüben, fallen unter die NIS2-Richtlinie, wenn Auswirkungen auf die öffentliche Ordnung oder grenzüberschreitende Risiken bestehen.

**2. Kriterium**

| Wesentliche Sektoren | | | Wichtige Sektoren | | | |
|---|---|---|---|---|---|---|
|  Transport |  Banken |  Finanzmärkte |  Postdienste |  Spezialprodukte |  Entsorgung |  Verwaltung |
|  Wasser |  Digitale Infrastruktur |  Energie |  Raumfahrt |  Forschung |  IT-Dienste |  Lebensmittel |
|  Gesundheit | | |  Telekommunikation |  Chemie |  Internetdienste | |

Für betroffene Unternehmen aus „wichtigen Sektoren“ sind geringere Geldstrafen vorgesehen und sie unterliegen einer reaktiven Aufsicht durch die Behörden, wo hingegen betroffene Unternehmen der „wesentlichen Sektoren“ höhere Geldstrafen und einer proaktiven Aufsicht der Behörden unterliegen.

# NIS2

## Vorgehensweise

### Betroffenheit ermitteln

- Ist das Unternehmen im Sinne der NIS2-Richtlinie betroffen?
  - Direkt betroffen nach Größe und Sektor
  - Indirekt betroffen Kundenstruktur
- Selbstmeldung an die Behörden!
- Aufmerksamkeit herstellen für mögliche Haftung und Sanktionen durch den Gesetzgeber bei Nichterfüllung.

### Analyse der vorhandenen Maßnahmen

- Vorhandene Struktur (Technisch / Organisatorisch)
- Besondere Rahmenbedingungen / Anforderungen des Unternehmens bzw. deren Kunden
- Identifizierung der Lücken in Bezug auf o.g. Anforderungen
- Planung der erforderlichen Aktionen zur Erfüllung der Anforderungen

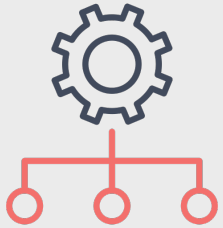
### Umsetzung der Maßnahmen

1. Risikoanalyse für IT-Systeme
2. Vorfall-Management
3. Business Continuity Management
4. Sicherstellung der Lieferantenkette
5. Schwachstellen-Management
6. Sicherheitsvalidierung
7. Cybersecurity Training
8. Kryptographie
9. Identity & Access Management
10. MFA & Notfallkommunikation

**Security Operation Center**

# Cyber Security

## Herausforderungen?



### Prozesse

- Prozesse nicht dokumentiert oder gelebt
- Keine zentralen Verantwortlichkeiten
- Vorgaben matchen nicht mit dem gelebten Prozess
- Notfallprozeduren unbekannt

### Daten und Sichtbarkeit

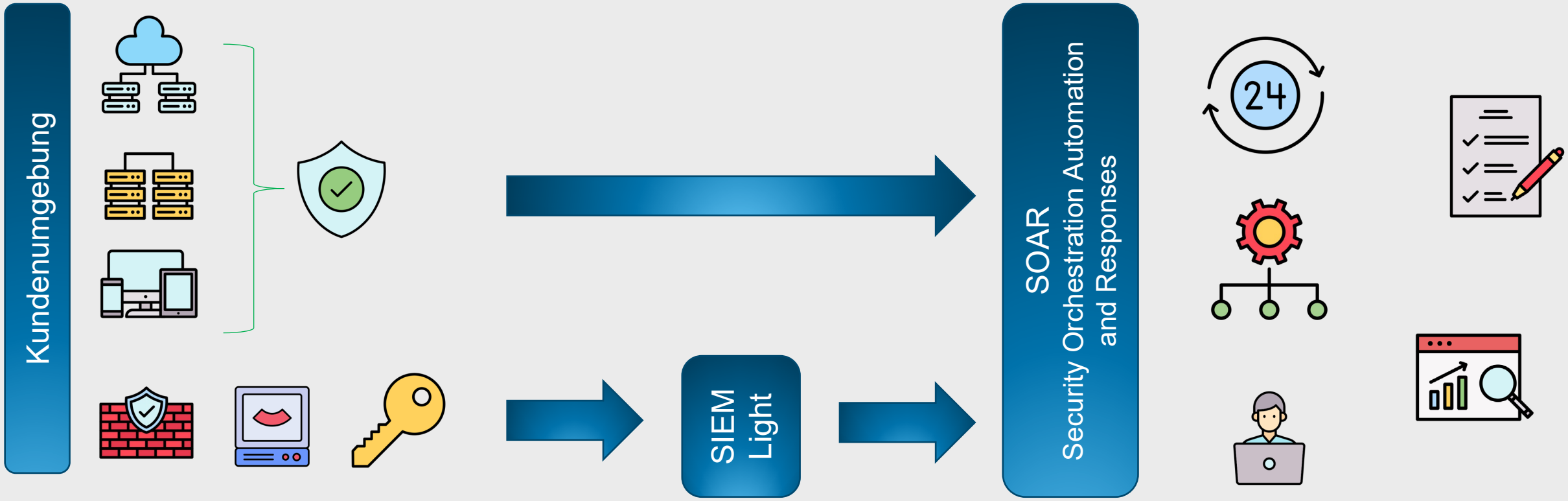
- Kein komplettes Inventar vorhanden
- Unsichtbare Devices
- Unerwünschte Kommunikation der Geräte untereinander und nach aussen
- Keine Echtzeitdaten und keine Korrelation möglich

### Grundlegende Security

- IT Grundschutz nicht etabliert
- Kein ISMS
- Lückenhafte Netzwerksegmentierung
- Lange Nutzungsdauer (Patches, Veraltete OS und SW)

# Moderne Ansätze

## Hybrider MDR Ansatz mit SIEM Light

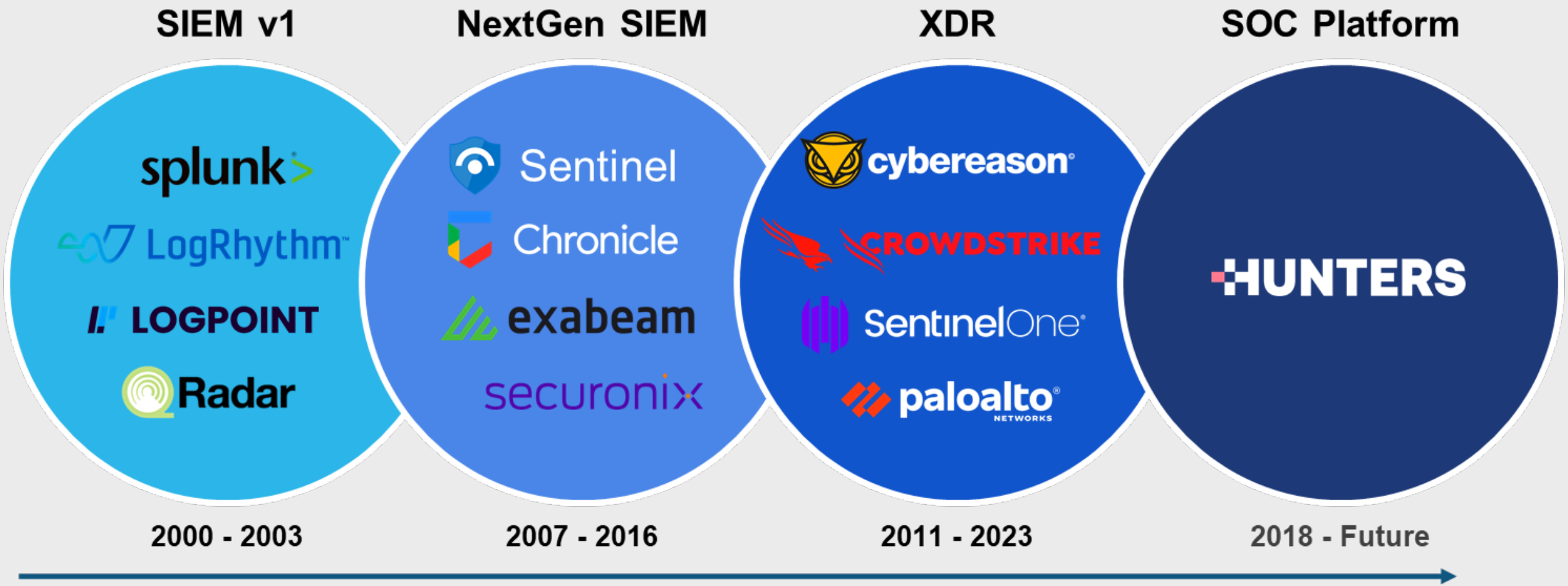



- EDR für Prävention und Erkennung
- Ergänzung mit XDR oder SIEM

- Ideal für Managed SOC
- Wirtschaftlicherer Ansatz

# Zukunft von SOC

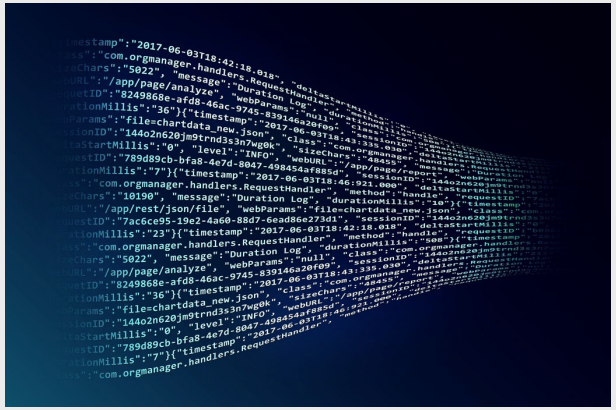
## SOC Platform



# SOC - Security Operations Center

## Eigenbetrieb oder Managed Service?

### SOC als interner Service



**Pro**

- Detail Kenntnisse des Unternehmens
- Intern gespeicherte Daten
- Abteilungsübergreifende Korrelation
- Bedarfsgerechte Anforderungen

**Con**

- Kosten
- Mitarbeiter (Einstellen/Halten)
- Möglicher Interessenskonflikt
- ROI Bedenken

### SOC als externer Service


**Pro**

- OPEX-Kosten, die verteilt werden können
- Kein Interessenskonflikt
- Skalierbarkeit und Flexibilität
- Profitieren von anderen Kundensituationen

**Con**

- Mangelnde Detail Kenntnisse des Unternehmens
- Externe Tools und Datenverkehr
- Mögliche Kommunikationsprobleme
- Normalerweise unbekannte Personen
- Begrenztes Customizing
- Dienstleistungen aus Kostengründen begrenzt

# Industrial Cyber Security

## Herausforderungen

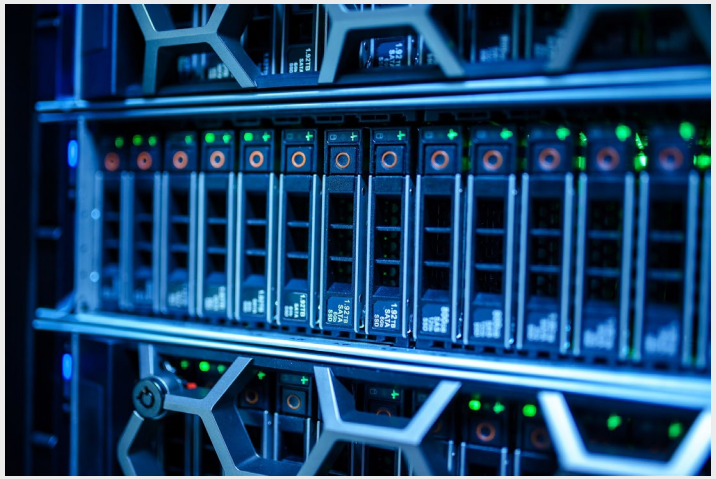
### OT

Unterschiedliche Nutzungsweise von Computersystemen

Lange System-Nutzungszyklen

Unbedingte Verfügbarkeit der Produktionsmittel

Fragmentierte nationale Regelwerke



### IT

Interaktive Nutzung von Computersystemen

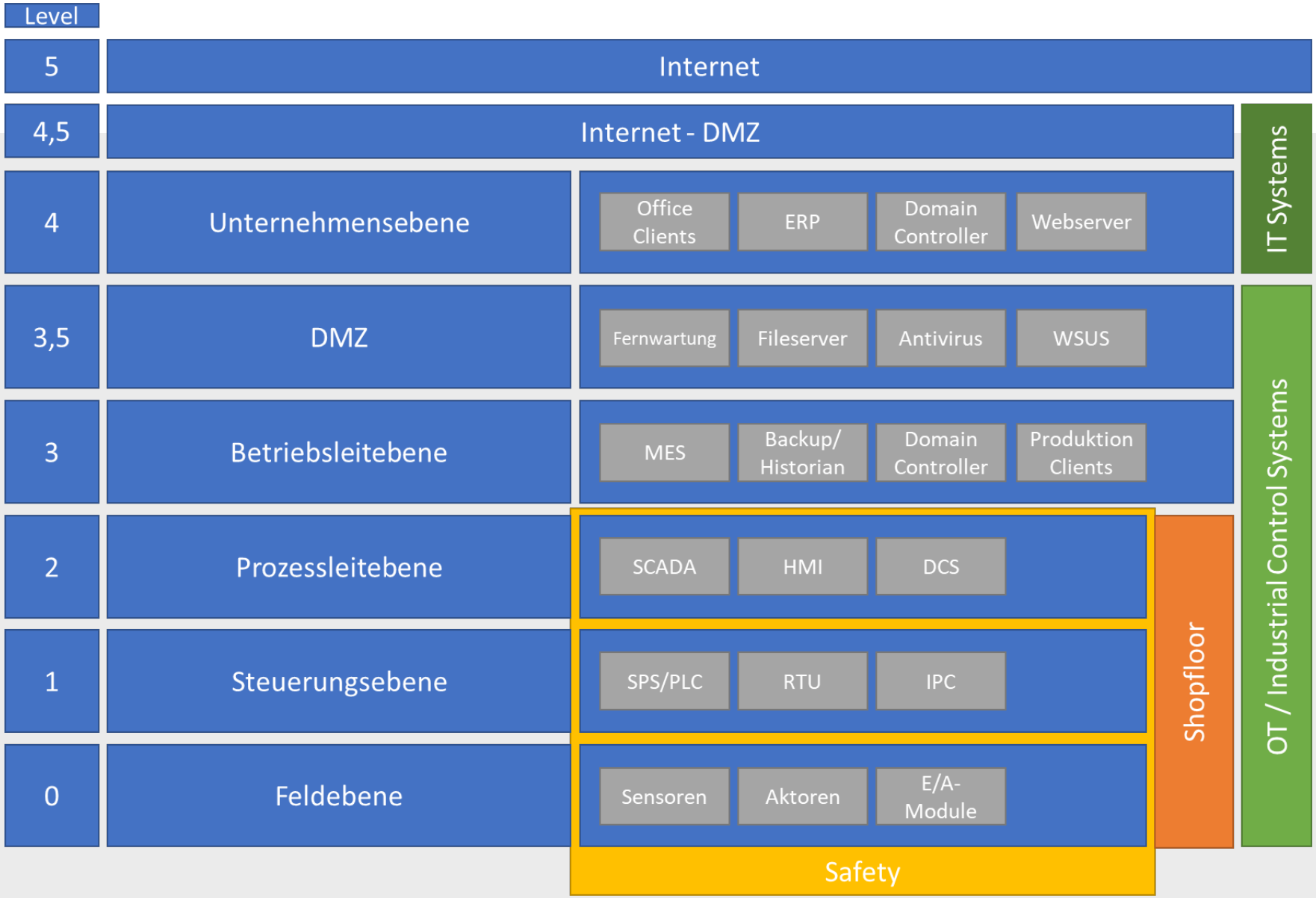
Kurze System-Nutzungszyklen

Daten- Verfügbarkeit und Integrität

Zentrale Regelwerke (Prozesse, defacto-Standards)

# Industrial Cyber Security

PURDUE Model



# Industrial Cyber Security

## OT Malware

**STUXNET**

Schadsoftware explizit für Siemens Simatic S7

Ziel: Sabotage des iranischen Atomprogramms

**HAVEX**

Remote-Access-Trojaner mit Fokus auf ICS/SCADA-Komponenten

Ziel: Spionage via Fernsteuerung von Systemen, Mitlesen von Netzwerkverkehr, Nachladen weiterer Schadsoftware

**BLACKENERGY 2**

Toolkit um DDoS Attacken auszuführen

Ziel: Störung/Sabotage kritischer Infrastruktur

**INDUSTROYER/ CRASHOVERRRIDE**

Modulare Malware mit ICS Fokus

Ziel: Störung/Sabotage kritischer Infrastrukturen

**TRITON/TRISIS**

Malware zum Fernzugriff und Umprogrammierung der Firmware

Ziel: Manipulation der Safety Steuerungen Triconex von Schneider Electric

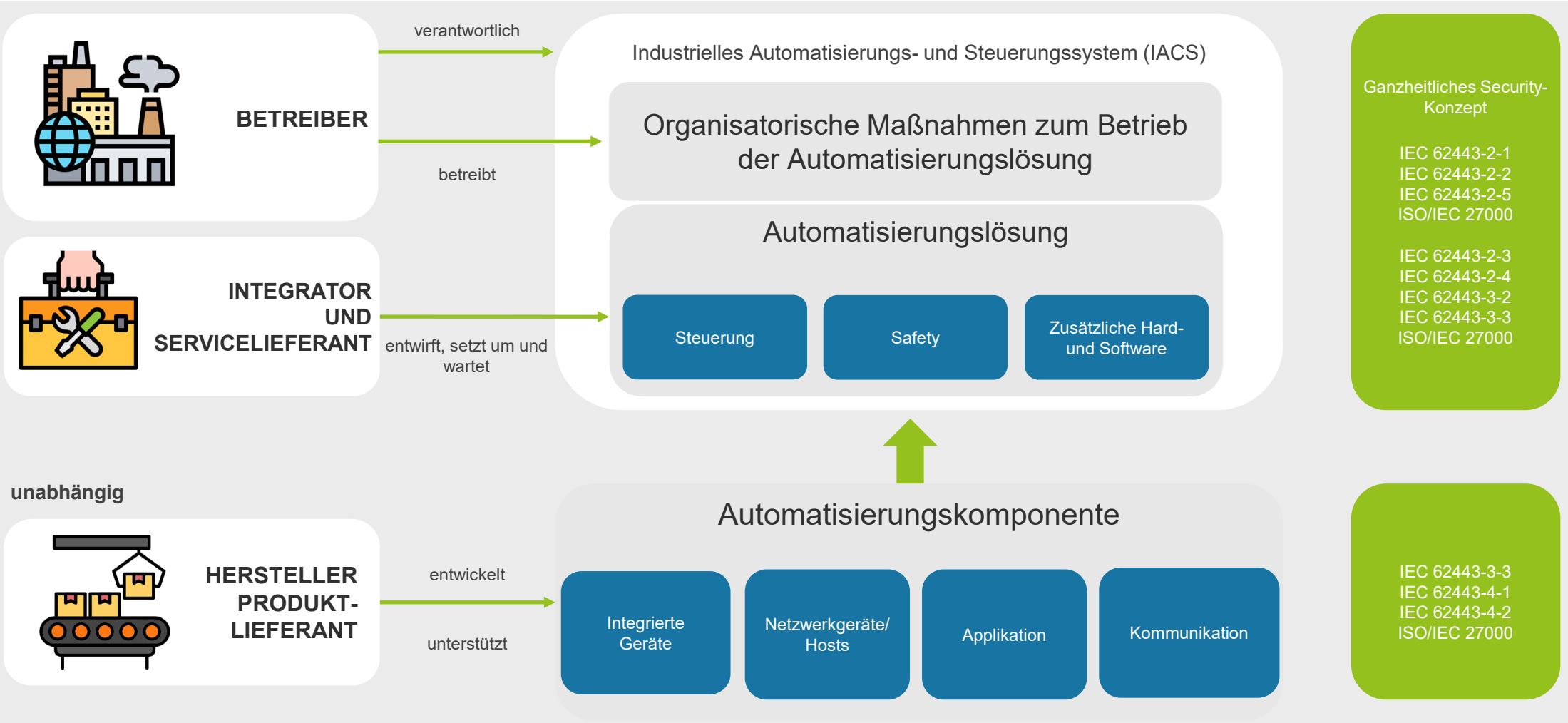
**PIPEDREAM**

Malware Toolkit

Ziel: OPC UA Server, Schneider und Omron PLCs

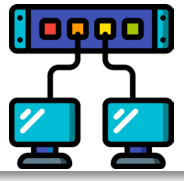
# Industrial Cyber Security

## IEC 62443 - Industrielle Kommunikationsnetzwerke - Netzwerke und Systemsicherheit



# Industrial Cyber Security

## Fokus

| | INVENTAR | SEGMENTIERUNG | ALT-SYSTEME | RICHTLINIEN | STANDARDISIERUNG |
|---|---|---|---|---|---|
| |  |  |  |  |  |
| **IST** | ○ Eingeschränkte Sicht auf Betriebskomponenten<br>○ Komplexe und heterogene Umgebung<br>○ Mangelnde betriebliche Effizienz | ○ Flache Netzwerkstruktur<br>○ OT ist abhängig von IT<br>○ Klumpenrisiken, operative Lähmung, mangelnde Eindämmung | ○ Out of support Betriebssysteme<br>○ Nicht patchfähig aufgrund von Herstellervorgaben | ○ Richtlinien und Vorgaben sind unvollständig<br>○ Abweichungen von den geforderten Standards und Regularien<br>○ fehlende Prozesse | ○ Begrenzte Zukunftsfähigkeit, funktionale Einschränkungen, fehlende Standardisierung und Referenzarchitekturen |
| **SOLL** | ○ Vollständige Übersicht über alle Geräte und Infrastrukturkomponenten<br>○ Beherrschbarkeit komplexer Umgebungen | ○ Sinnvolle Segmentierung der Netzwerke<br>○ Wartung der IT Komponenten wirkt sich nicht auf OT Prozesse aus | ○ Betrieb abgesicherter Altsysteme<br>○ Migration/Modernisierung | ○ Unternehmensrichtlinien und regulatorische Vorgaben werden gleichermaßen umgesetzt und eingehalten | ○ Standardisierung unter Beachtung der OT und IT Nutzungsparadigmen |

# Sicht der Kunden – Aktuelle Projekte

## Wie stellen sich Kunden der Herausforderung?

IT Grundschutz Parallel oder als separates Projekt. Aber losgelöst!

### Verlängerte Werkbank

- 24x7 Hotline
- Sicherstellung der Hilfe im Notfall
- Experten als Ansprechpartner
- Koordination des Vorgehens im Ernstfall
- Absicherung

### Bedarfsanalyse

- Was habe ich?
- Was brauche ich?
- Definition der Anforderungen
- Vertragliche Eckpunkte
- Zeitplan mit Meilensteinen

### Auswahl SOC Service

- Markt Analyse
- Passender Partner
- Art des Service
  - Hybrid
  - Full Managed
- Zusatzleistungen
- Ausschreibung

Transition

Laufender Betrieb

# WIR NEHMEN UNS GERNE ZEIT FÜR SIE!


**PLS Management GmbH**

Nikolaus-Otto-Straße 13
70771 Leinfelden-Echterdingen

+49 711 933 033-0
+49 711 933 033-914
info@pls.ag
www.pls.ag

# Quellennachweise

## Links

**AIDS Ransomware**

- https://de.wikipedia.org/wiki/AIDS_(Trojanisches_Pferd)
  - Creative Commons

**Icons**

- https://www.flaticon.com/free-icons/
  - icons created by Muhammad Ali – Flaticon

**Bilder**

- https://pixabay.com/de/