ACTEMIUM axians

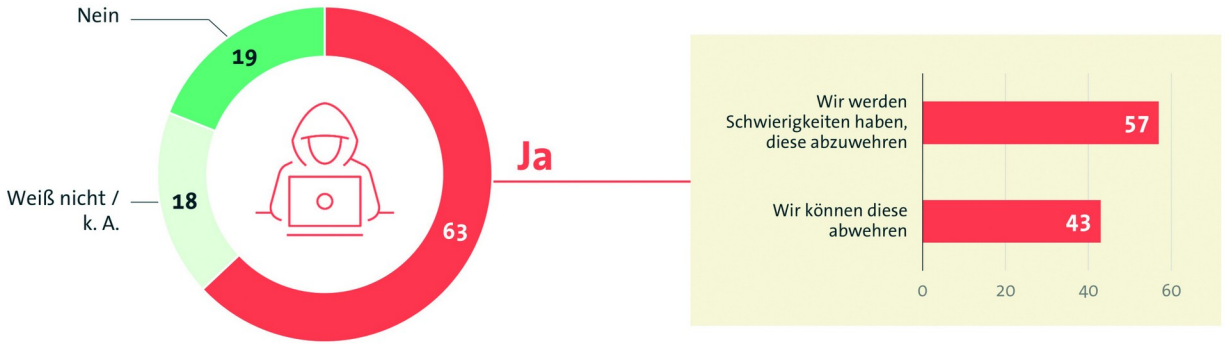
DATA DRIVEN INDUSTRY

VINCI ENERGIES

Was man nicht sehen kann, kann man auch nicht schützen!

Zwei Drittel der Unternehmen erwarten Cyberangriffe

Glauben Sie, dass Ihr Unternehmen in den kommenden 12 Monaten Ziel von Cyberangriffen wird?



in Prozent

Basis (links): Alle Unternehmen (n=603) | Basis (rechts): Unternehmen, die Cyberangriffe erwarten (n=380) | Quelle: Bitkom Research 2023

bitkom

Quelle Branchenverband bitkom e.V.

Erhöhtes Risikoprofil

Angriffe können physische Auswirkungen haben.

Konvergierende IT/OT-Umgebungen

Zunehmende Vernetzung schafft neue Angriffsvektoren.

Spezialisierte Protokolle

Industrieprotokolle erfordern spezielle Überwachungslösungen.

Alternde Infrastruktur

Legacy-Systeme ohne integrierte Sicherheitsfunktionen dominieren.

- **Sabotage:**

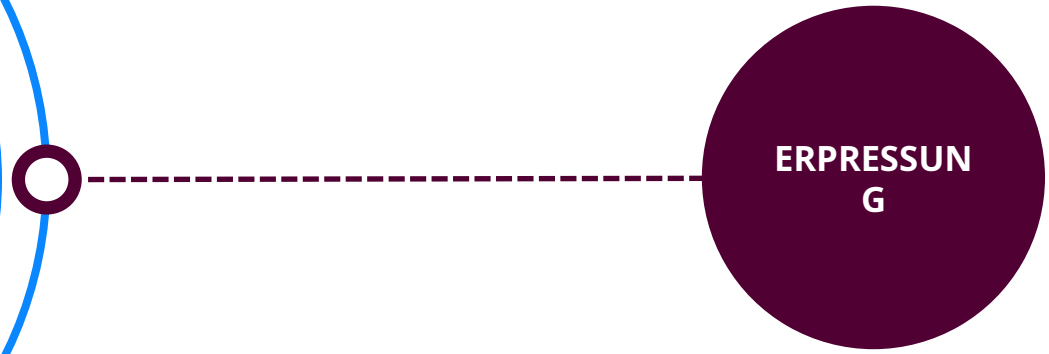
Steuerungssysteme z.B. werden gezielt manipuliert.

- **Erpressung:**

Das Unternehmen wird zum Ziel von Erpressungen.

- **Spionage:**

Industriespionage ist der Klassiker für Angriffe auf OT-Systeme.



- **Sabotage:**

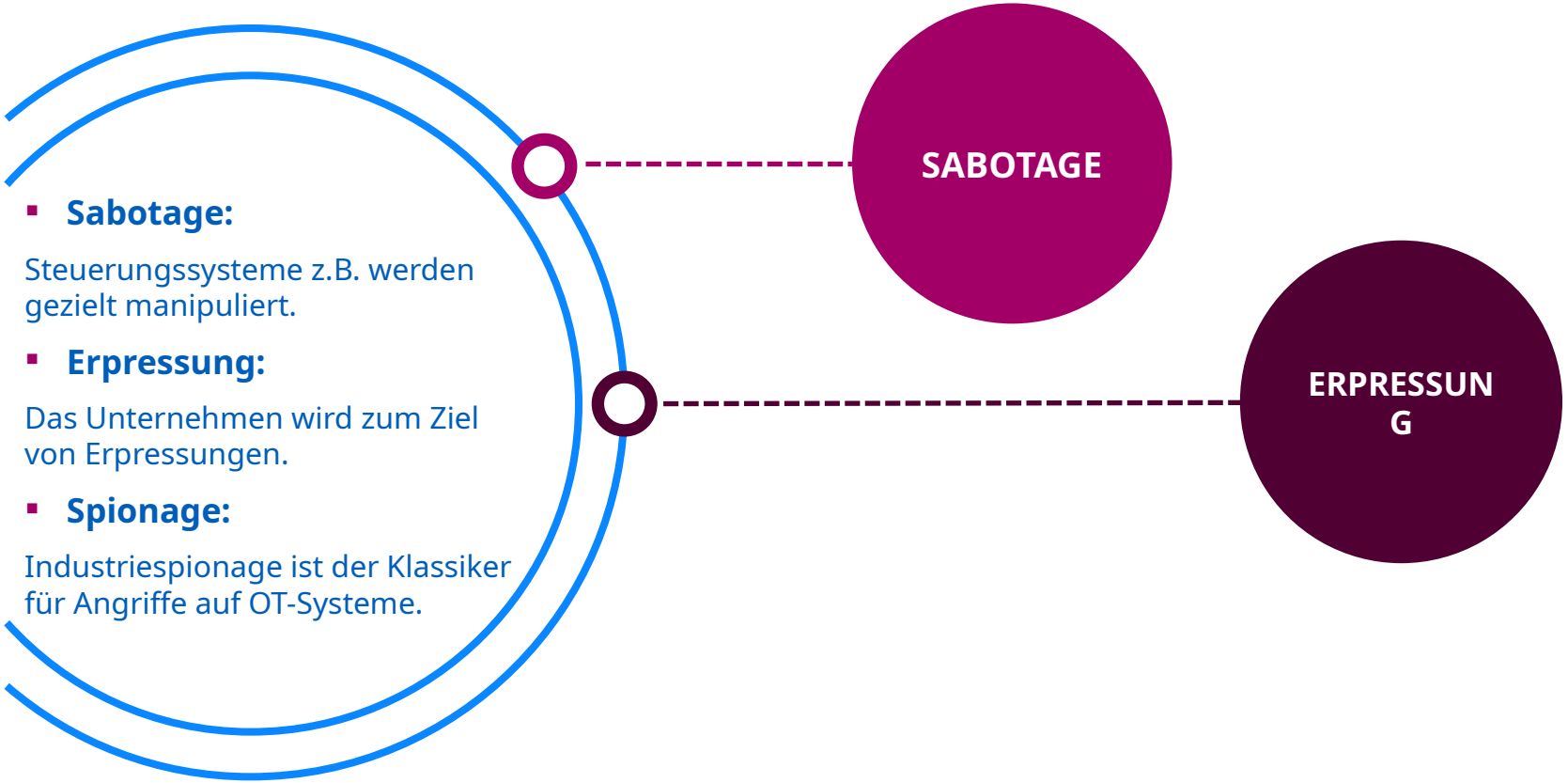
Steuerungssysteme z.B. werden gezielt manipuliert.

- **Erpressung:**

Das Unternehmen wird zum Ziel von Erpressungen.

- **Spionage:**

Industriespionage ist der Klassiker für Angriffe auf OT-Systeme.



- **Sabotage:**

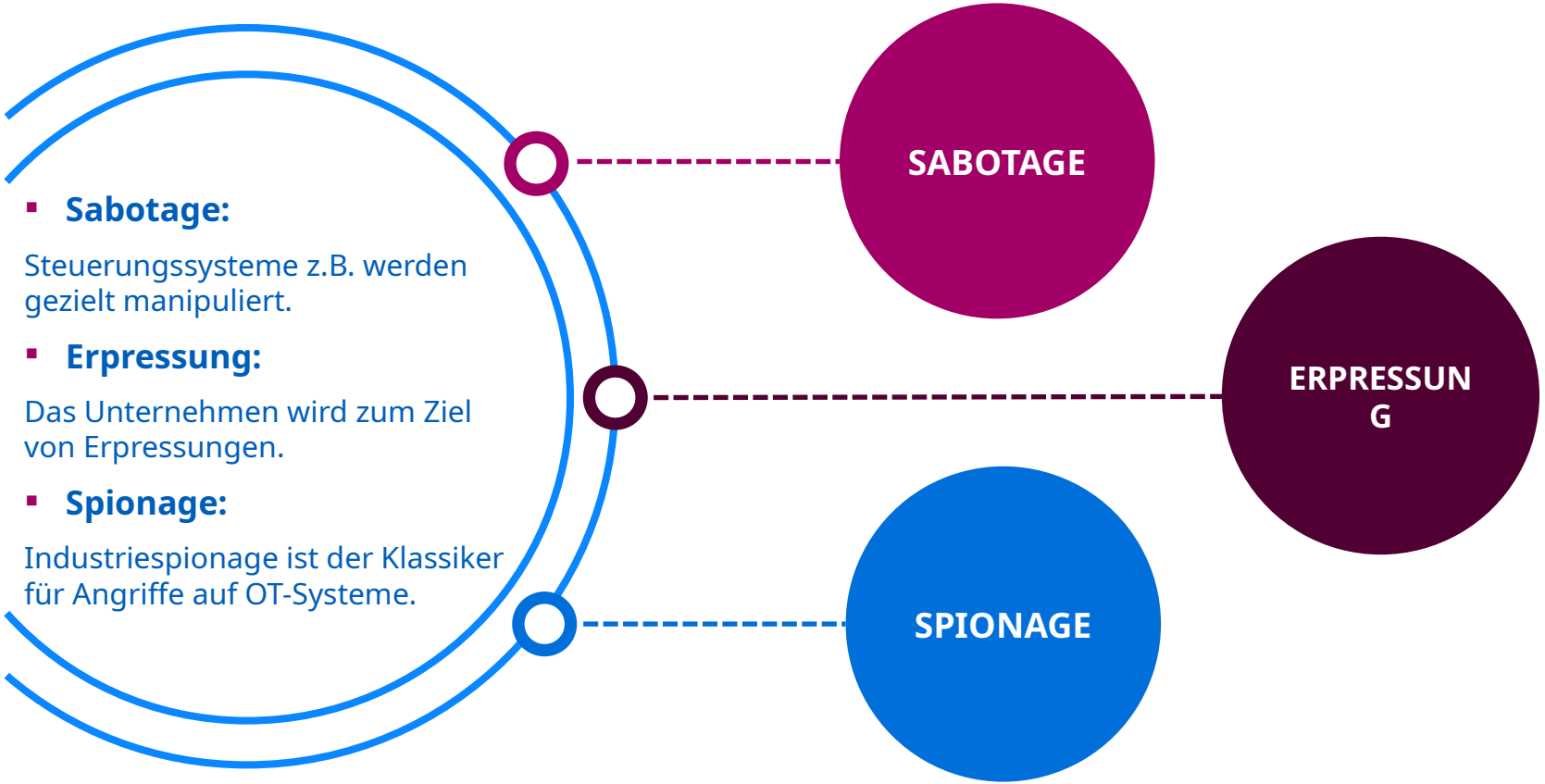
Steuerungssysteme z.B. werden gezielt manipuliert.

- **Erpressung:**

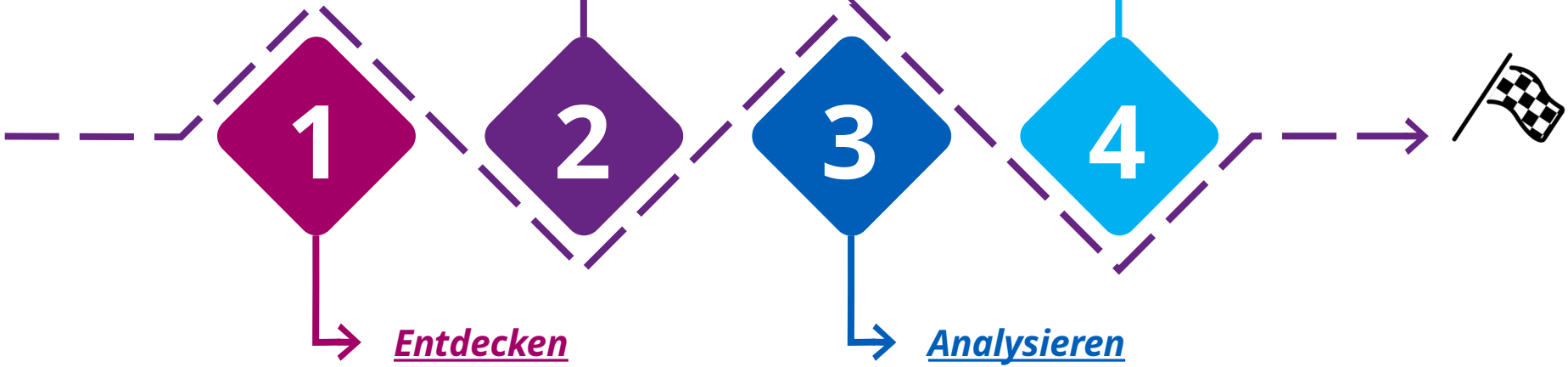
Das Unternehmen wird zum Ziel von Erpressungen.

- **Spionage:**

Industriespionage ist der Klassiker für Angriffe auf OT-Systeme.



axians



Entdecken

Asset Erfassung und -Klassifizierung

Bewerten

umfassende und kontinuierliche Schwachstellenbewertung

Analysieren

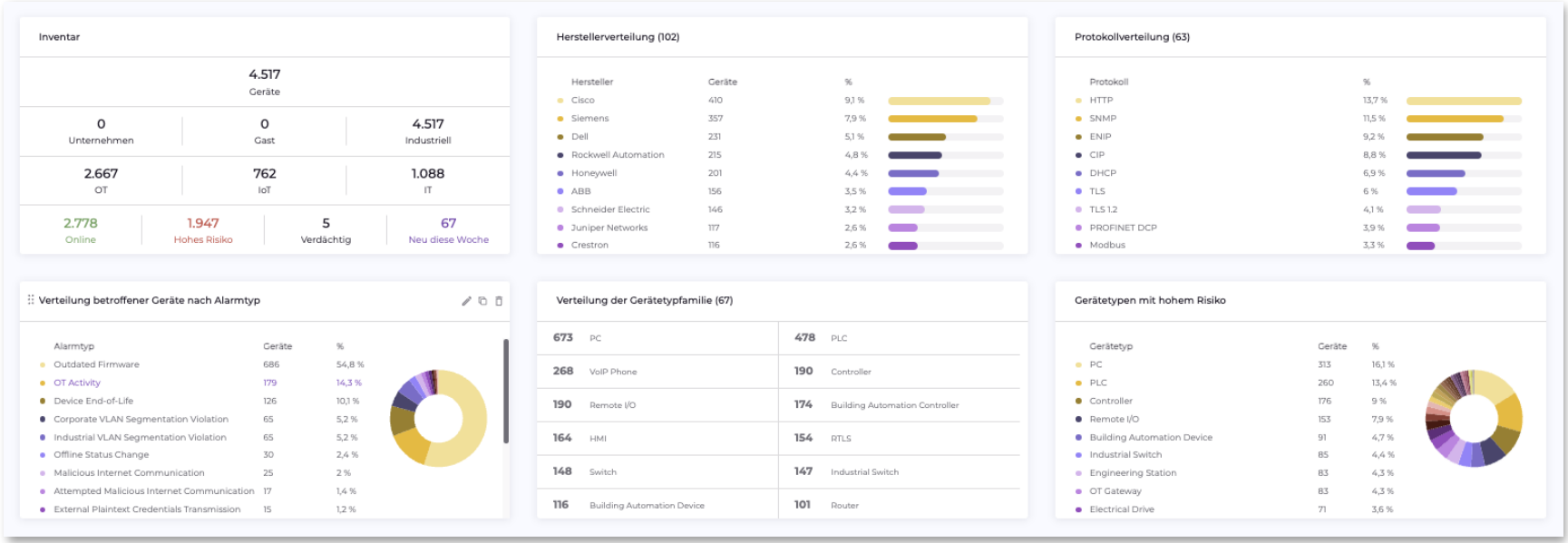
Schwachstellenanalyse und -priorisierung

Beheben

Schwachstellenbehebung und -validierung

GRUNDLEGENDE ANALYSE DER OT-LANDSCHAFT

- SICHTBARKEIT ERSTELLEN -



Inventar

4.517
Geräte

0	0	4.517
Unternehmen	Gast	Industriell
2.667	762	1.088
OT	IoT	IT

2.778	1.947	5	67
Online	Hohes Risiko	Verdächtig	Neu diese Woche

Herstellerverteilung (102)

Hersteller	Geräte	%
Cisco	410	9,1 %
Siemens	357	7,9 %
Dell	231	5,1 %
Rockwell Automation	215	4,8 %
Honeywell	201	4,4 %
ABB	156	3,5 %
Schneider Electric	146	3,2 %
Juniper Networks	117	2,6 %
Crestron	116	2,6 %

Protokollverteilung (63)

Protokoll	%
HTTP	13,7 %
SNMP	11,5 %
ENIP	9,2 %
CIP	8,8 %
DHCP	6,9 %
TLS	6 %
TLS 1.2	4,1 %
PROFINET DCP	3,9 %
Modbus	3,3 %

Verteilung betroffener Geräte nach Alarmtyp

Alarmtyp	Geräte	%
Outdated Firmware	686	54,8 %
OT Activity	179	14,3 %
Device End-of-Life	126	10,1 %
Corporate VLAN Segmentation Violation	65	5,2 %
Industrial VLAN Segmentation Violation	65	5,2 %
Offline Status Change	30	2,4 %
Malicious Internet Communication	25	2 %
Attempted Malicious Internet Communication	17	1,4 %
External Plaintext Credentials Transmission	15	1,2 %

Verteilung der Gerätetypfamilie (67)

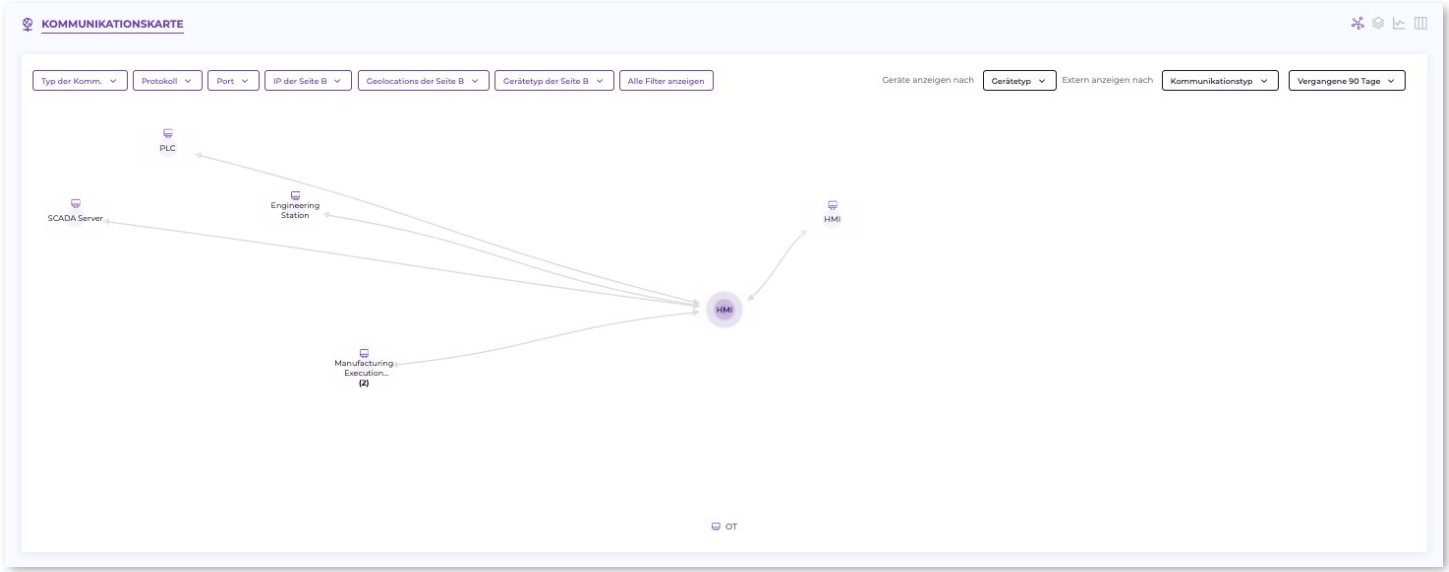
673	PC	478	PLC
268	VoIP Phone	190	Controller
190	Remote I/O	174	Building Automation Controller
164	HMI	154	RTLS
148	Switch	147	Industrial Switch
116	Building Automation Device	101	Router

Gerätetypen mit hohem Risiko

Gerätetyp	Geräte	%
PC	313	16,1 %
PLC	260	13,4 %
Controller	176	9 %
Remote I/O	153	7,9 %
Building Automation Device	91	4,7 %
Industrial Switch	85	4,4 %
Engineering Station	83	4,3 %
OT Gateway	83	4,3 %
Electrical Drive	71	3,6 %

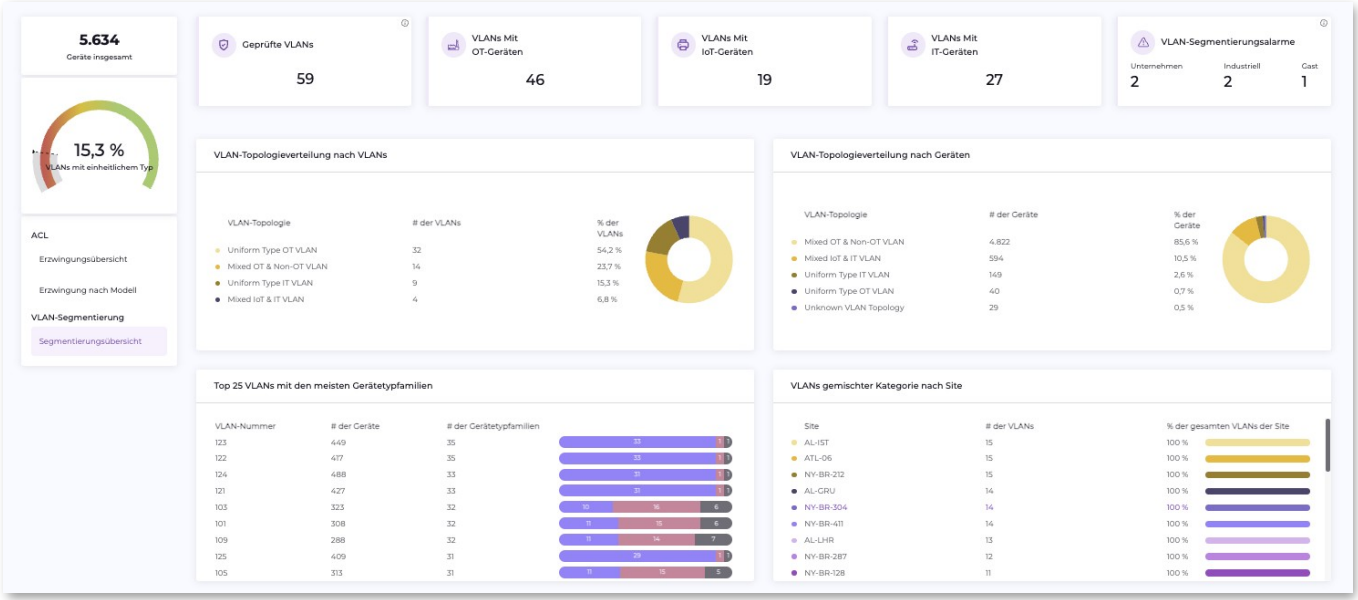
ANALYSE DER KOMMUNIKATIONSWEGE

- NETWORK COMMUNICATION VISIBILITY -



ANALYSE DER KOMMUNIKATIONSWEGE

- NETWORK COMMUNICATION VISIBILITY -



ASSET MANAGEMENT AUFBAUEN

- INVENTORY / OVERALL DEVICE VIEW -

Herstellerverteilung (8)

Hersteller	Geräte	%
Siemens	357	31,3 %
Rockwell Automation	215	18,9 %
Honeywell	190	16,7 %
ABB	156	13,7 %
Schneider Electric	146	12,8 %
Bosch	50	4,4 %
Hirschmann	20	1,8 %
Beckhoff	5	0,4 %

Protokollverteilung (33)

Protokoll	%
ENIP	11,8 %
CIP	11,6 %
SNMP	7,6 %
TLS	7,2 %
HTTP	7,1 %
PROFINET DCP	6,3 %
ARP	5,2 %
Modbus	5 %
S7comm	4 %

Inventar

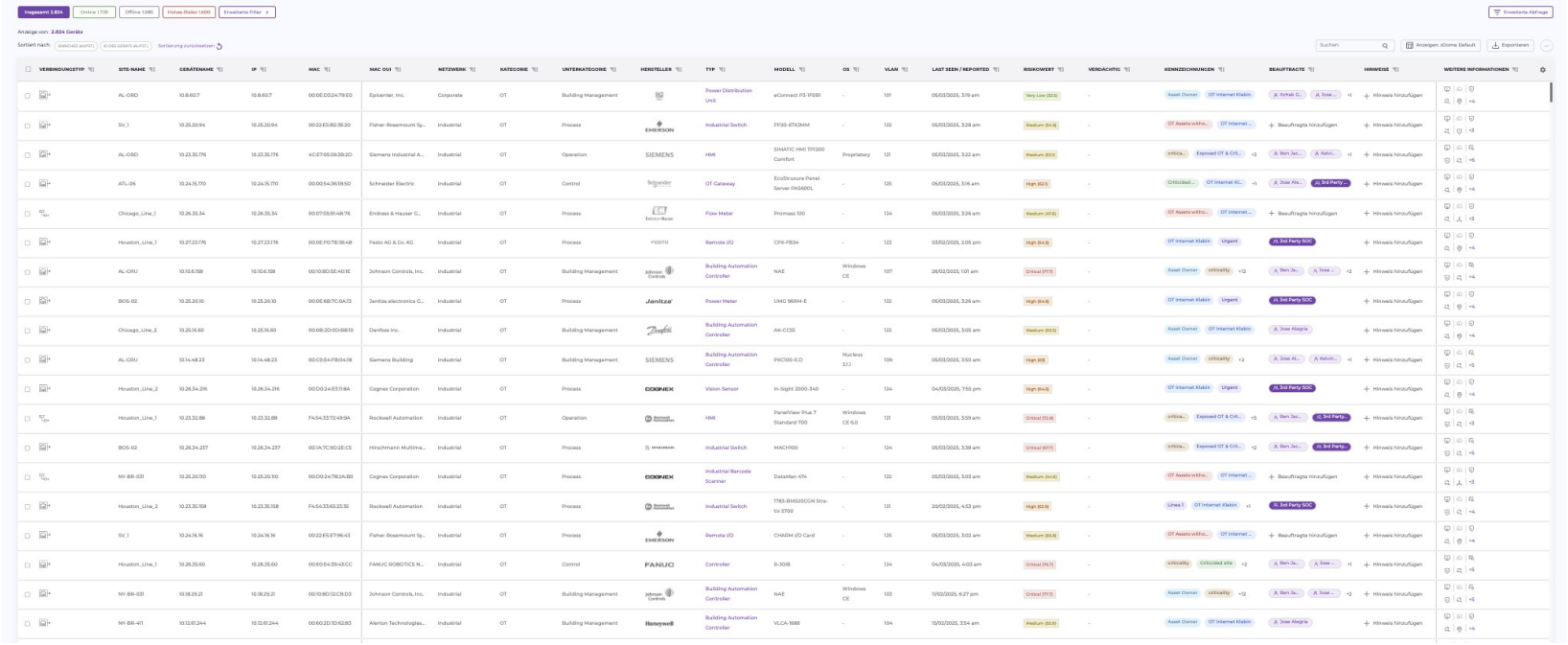
1.139 Geräte			
0 Unternehmen	0 Gast	1.139 Industriell	
1.139 OT	0 IoT	0 IT	
726 Online	739 Hohes Risiko	0 Verdächtig	14 Neu diese Woche

Verteilung der Gerätetypfamilie (21)

326	PLC	116	HMI
104	Controller	89	Industrial Switch
71	Building Automation Controller	63	SCADA Server
57	Engineering Station	43	Electrical Drive
40	Remote I/O	40	Building Management System
36	Inspection System	35	Industrial Printer

ASSET MANAGEMENT AUFBAUEN

- INVENTORY / OVERALL DEVICE VIEW -

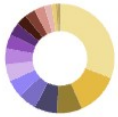


SCHWACHSTELLENANALYSE AUFGRUND DER DATEN

- VULNERABILITY IDENTIFICATION -

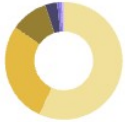
Gerätetypen mit hohem Risiko

Gerätetyp	Geräte	%
PLC	228	30,9 %
Controller	93	12,6 %
Industrial Switch	55	7,4 %
Engineering Station	49	6,6 %
Electrical Drive	41	5,5 %
SCADA Server	38	5,1 %
Remote I/O	37	5 %
Industrial Printer	35	4,7 %
HMI	31	4,2 %



Verteilung betroffener Geräte nach Alarmtyp

Alarmtyp	Geräte	%
Outdated Firmware	277	56,8 %
OT Activity	136	27,9 %
Device End-of-Life	50	10,2 %
Offline Status Change	16	3,3 %
Out-of-Policy Communication	4	0,8 %
Network Threat Signature	3	0,6 %
Malicious Internet Communication	2	0,4 %



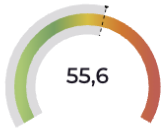
SCHWACHSTELLENANALYSE AUFGRUND DER DATEN

- VULNERABILITY IDENTIFICATION -

RISIKO INSGESAMT

Geräte Insgesamt		Kritisches Und Hohes Risiko		Neu Kritisches Und Hohes Risiko		Kürzlich Gestiegen		Kürzlich Gesunken	
Geräte	Modelle								
5.634	505	2.388	42,4 %	2.388	42,4 %	0	0 %	0	0 %

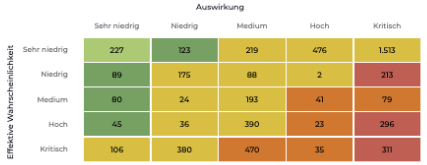
Risikowert insgesamt



Risikowert-Verteilung

Risikowert	Geräte	%
Critical	1.032	18,3 %
High	1.356	24,1 %
Medium	2.536	45 %
Low	524	9,3 %
Very Low	186	3,3 %

Effective Likelihood und Impact Heat Map im Vergleich



WAHRSCHEINLICHKEIT UND AUSWIRKUNG

Verteilung der Wahrscheinlichkeitsrisikofaktoren – Auswirkungen auf Gesamtrisiko

Verteilung der Auswirkungsrisikofaktoren – Auswirkungen auf Gesamtrisiko

Hilfe

- OT-SECURITY STRATEGIE -

Beheben

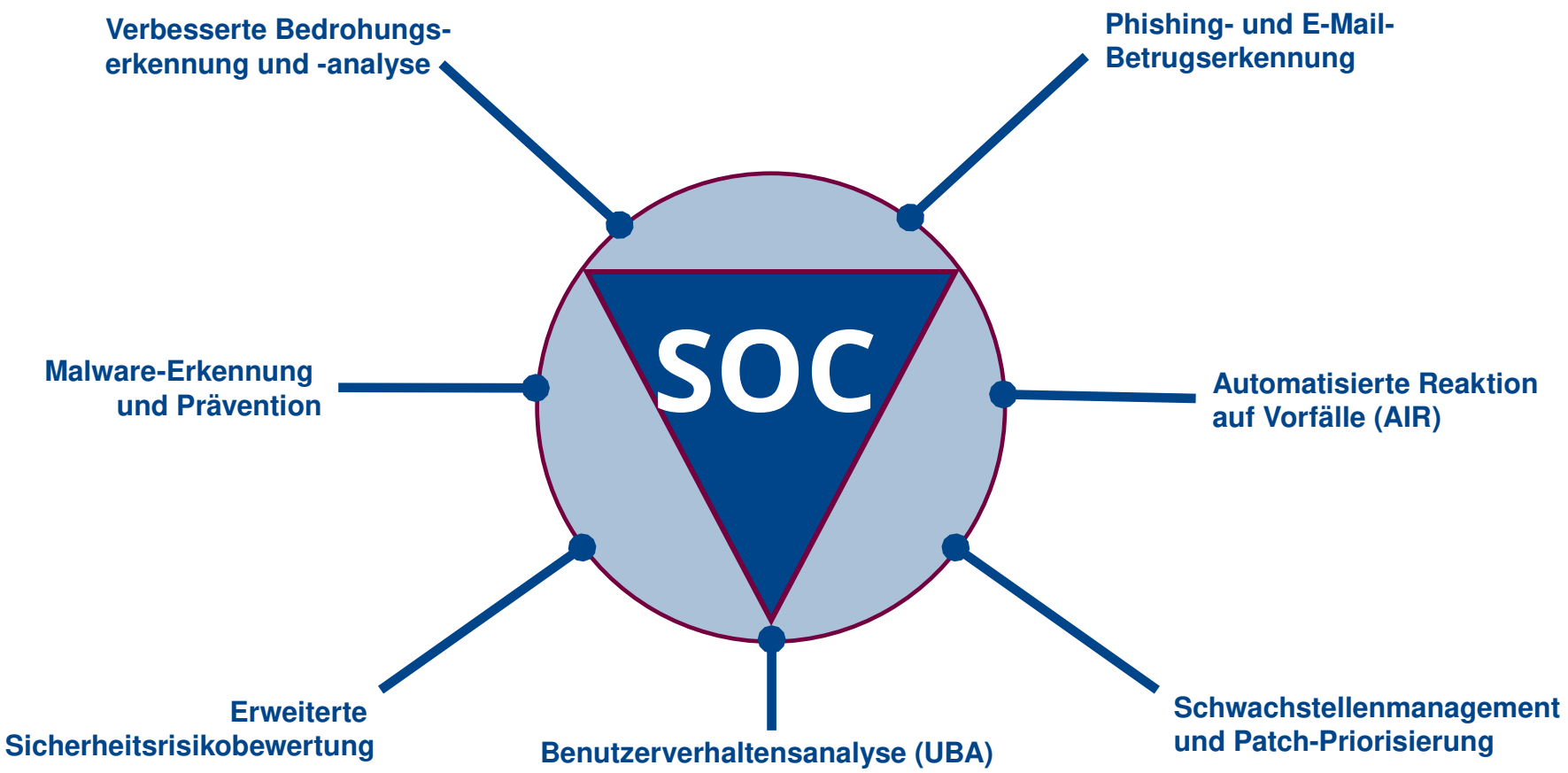
Eine solide OT-Security-Strategie ist der Fahrplan für den Schutz Ihrer industriellen Steuerungssysteme (ICS) vor Cyberbedrohungen.

CLAROTY

exeon

ARMIS®

tenable®


Verbesserte Bedrohungs-
erkennung und -analyse
Phishing- und E-Mail-
Betrugserkennung
Malware-Erkennung
und Prävention
SOC
Automatisierte Reaktion
auf Vorfälle (AIR)
Erweiterte
Sicherheitsrisikobewertung
Benutzerverhaltensanalyse (UBA)
Schwachstellenmanagement
und Patch-Priorisierung

Eine moderne OT-SOC-Architektur bietet:

- **Erhöhte Transparenz:** OT-Bedrohungen in Echtzeit erkennen
- **Skalierbarkeit:** Flexible Anpassung an neue OT-Assets
- **Reduzierung von False Positives:** Smarte Anomalie Erkennung
- **Compliance-Sicherheit:** Unterstützung von NIS2, ISO 27001, IEC 62443
- **Einsatz von AI:** Hilft dabei ein SOC effizienter & professioneller auszurichten

Integration von OT-Security in ein Managed-SOC:

- **Protokollierung und Erfassen industrieller Protokolle**
  Datenquellen: Syslog, OPC UA, Modbus, NetFlow

Integration von OT-Security in ein Managed-SOC:

Protokollierung und Erfassen industrieller Protokolle
Datenquellen: Syslog, OPC UA, Modbus, MQTT, NetFlow

- **Datenaggregation: Taps, Paketbroker, Edge-Gateways, SIEM-Connectoren**

Integration von OT-Security in ein Managed-SOC:

Protokollierung und Erfassen industrieller Protokolle
Datenquellen: Syslog, OPC UA, Modbus, MQTT, NetFlow

Datenaggregation: Taps, Paketbroker, Edge-Gateways, SIEM-Connectoren
Korrelieren von OT- und IT-Daten zur ganzheitlichen Bedrohungserkennung
Datenanalyse: OT-Security-Tool, Assetmanagement-Tool, SZA

Integration von OT-Security in ein Managed-SOC:

Protokollierung und Erfassen industrieller Protokolle
Datenquellen: Syslog, OPC UA, Modbus, MQTT, NetFlow

Datenaggregation: Taps, Paketbroker, Edge-Gateways, SIEM-Connectoren
Korrelieren von OT- und IT-Daten zur ganzheitlichen Bedrohungserkennung
Datenanalyse: OT-Security-Tool, Assetmanagement-Tool, SZA
Reaktionsmechanismen: Automatische Alarme, Playbooks, Incident Response

Integration von OT-Security in ein Managed-SOC:

- **Protokollierung und Erfassen industrieller Protokolle**
  Datenquellen: Syslog, OPC UA, Modbus, MQTT, NetFlow

- **Datenaggregation:** Taps, Paketbroker, Edge-Gateways, SIEM-Connectoren
- **Korrelieren von OT- und IT-Daten zur ganzheitlichen Bedrohungserkennung**
  Datenanalyse: OT-Security-Tool, Assetmanagement-Tool, SZA
- **Reaktionsmechanismen:** Automatische Alarme, Playbooks, Incident Response

Das integrierte OT-SOC im Einsatz.

OT im SOC

Der Erfolg von OT im SOC hängt sehr stark von den spezifischen Anforderungen und Zielen des Unternehmens ab.

Die Integration von OT-Sicherheit erfordert angepasste Prozesse. Die Zusammenarbeit zwischen SOC und OT-Teams ist entscheidend.

Konvergenz IT/OT

Konvergenz IT/OT

axians

« Vielen Dank »

Gibt es noch Fragen?

Frank Sommerhoff

frank.sommerhoff@magellan-net.de

+49 160.982.523.83

fernaomagellan

VINCI ENERGIES