secunet

Sichere Vernetzung von IIoT-Geräten und Anlagen

secunet Security Networks AG

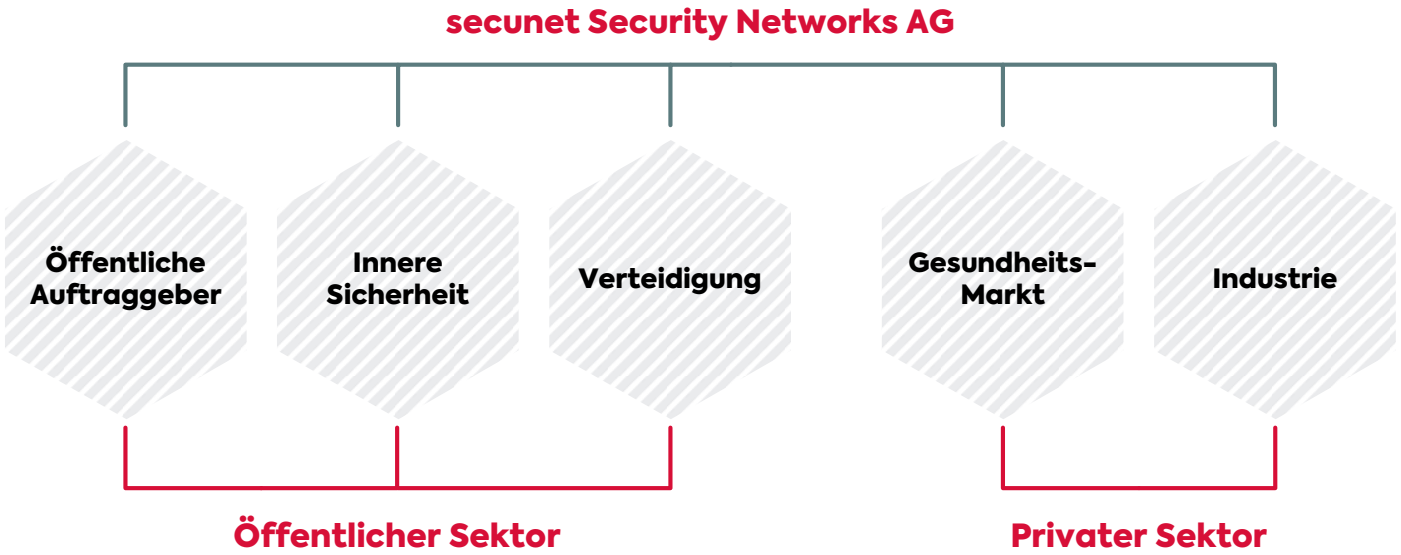
Steffen Heyde

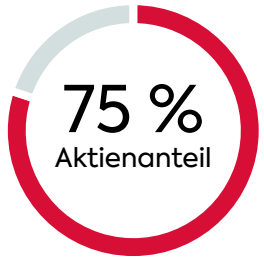
Division Industry

Leiter Marktsegmente

- mehr als 25 Jahre im Bereich IT-/OT-/Cybersicherheit
- Beratung bei Bundesbehörden, im Finanzsektor, bei herstellender Industrie, im Handel, bei Versorgungsunternehmen, in der IKT-Branche, in der Automobilbranche, in der Transportbranche, …
- Vertreter der secunet bei Bitkom, TeleTrusT, …

secunet auf einen Blick





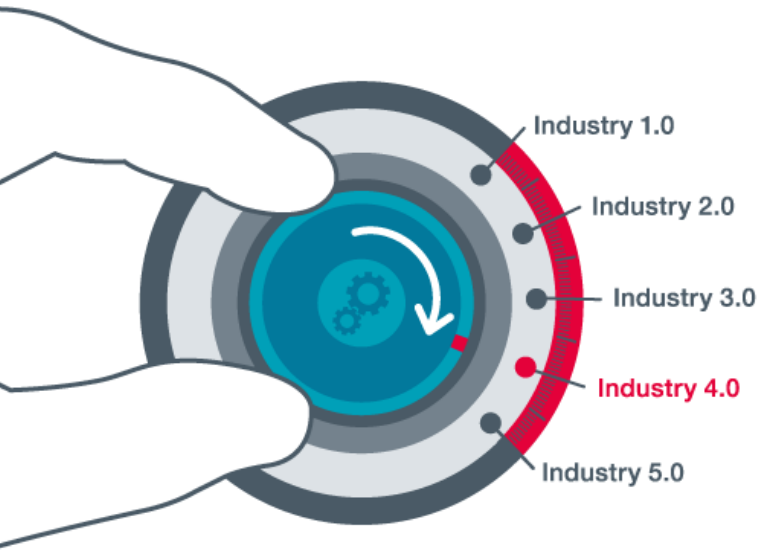
Hauptaktionär:
Giesecke + Devrient

Joint-
Venture

226,9 Mio.
Euro Umsatz

Über 700 MA
11 Standorte

IT-Sicherheit als Fundament der Industrie 4.0



SCHUTZ VOR KOSTEN INFOLGE VON SICHERHEITSVORFÄLLEN

Korrektiv: Mikro-Segmentierung, Isolation, sichere Fernwartung, ...

SENKUNG VON BETRIEBSKOSTEN

Präventiv: Zustandsbasierte Wartung, Wartungsplanung, Prädiktive Wartung

PROZESSEFFIZIENZ DURCH AUTOMATISIERUNG SCHAFFT KOSTENEINSPARPOTENTIALE

Software- Management: Rollout von Software und Konfigurationen

NEUE GESCHÄFTSMODELLE UND UMSATZTREIBER

Mehrwerte: Daten kontrolliert verfügbar machen, Drittanbieter sicher einbinden

Jede digitale Transformation ist eine individuelle Reise

Verzahnung zuvor getrennter Welten

Möglichkeiten und Herausforderungen

Neue Möglichkeiten

durch Vernetzung von Sensoren, Maschinen & Anlagen

Effiziente, flexible und intelligente Produktionsprozesse steigern die Produktivität.

Neue Möglichkeiten der Datenanalyse schaffen **Transparenz**, **Einsparpotenziale** und neue **Geschäftsmodelle**.

Kollaboratives Arbeiten statt Silodenken: Neue Schnittstellen zwischen Maschinen und zu internen / externen Diensten.

Neue Herausforderungen

durch Vernetzung von Office-IT und Prozess-IT (OT)

Systeme werden durch die Verwendung von Diensten im Internet **weltweit verfügbar – auch für Angreifer!**

Schwachstellen von zuvor nicht erreichbaren Systemen sind plötzlich **ausnutzbar**.

Isolierte Betrachtung einzelner Systeme ist nicht mehr ausreichend!

Herausforderung: Schutz sensibler Bereiche bei gleichzeitiger Öffnung zur Erhöhung der Konnektivität.

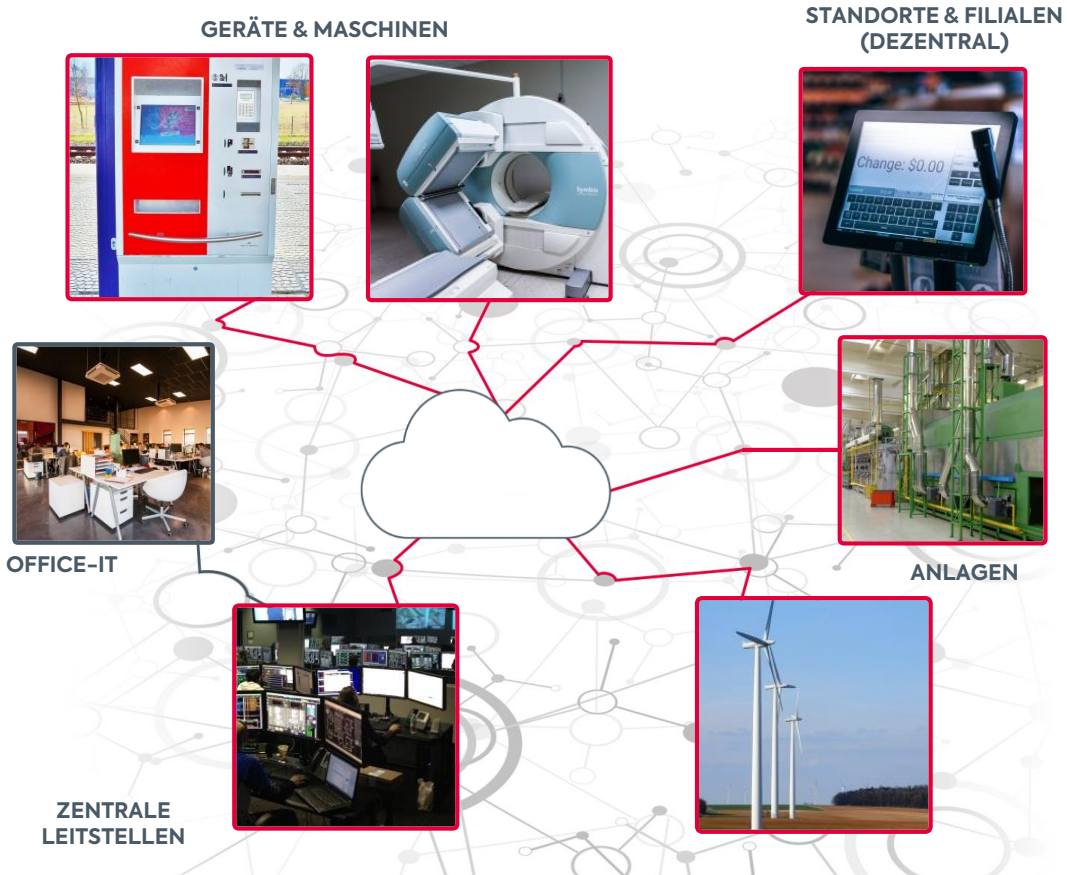
Herausforderungen und Sicherheitsstrategien in der Digitalisierung

COMPLIANCE

INTERNATIONAL
ISO 270xx
IEC 62443
NIST Framework

NATIONAL
BSI-Kritisverordnung, B3S
IT-Sicherheitsgesetz (BSI)
Standards & Best Practices

INTERN
Leitlinien
Richtlinien
Konzepte



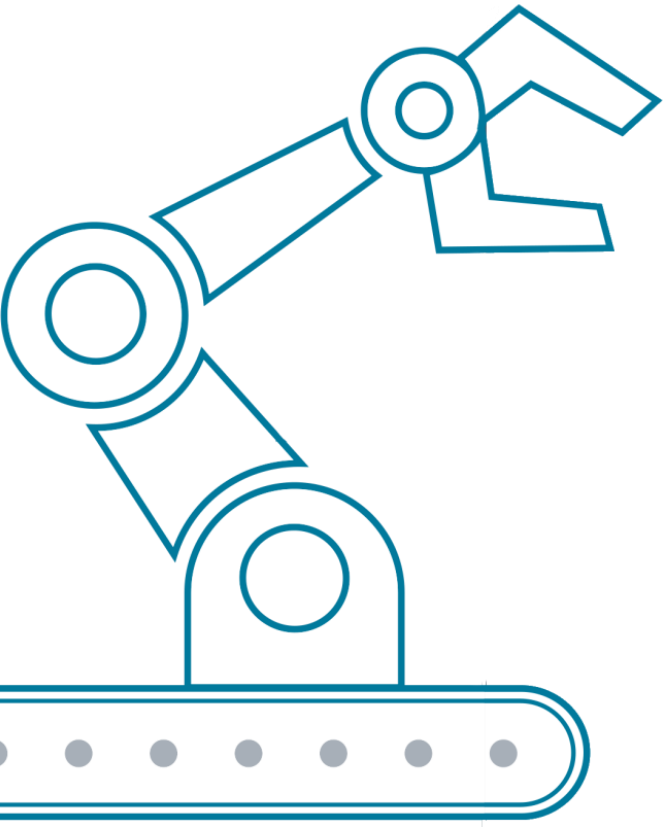
BEDROHUNGEN

- Fehlende starke Authentifizierung
- Unverschlüsselte Kommunikation
- Ausnutzen von Schwachstellen
- Befall von Schadsoftware
- Unkontrollierte Internetnutzung
- Unzureichender Zugriffschutz

Herausforderung: Starke Vernetzung
Office-IT und Prozess-IT sind gleichermaßen von Regulierungen und Bedrohungen betroffen!

Maschinen- bzw. Anlagensicherheit im Fokus

Protect. Connect. Detect.



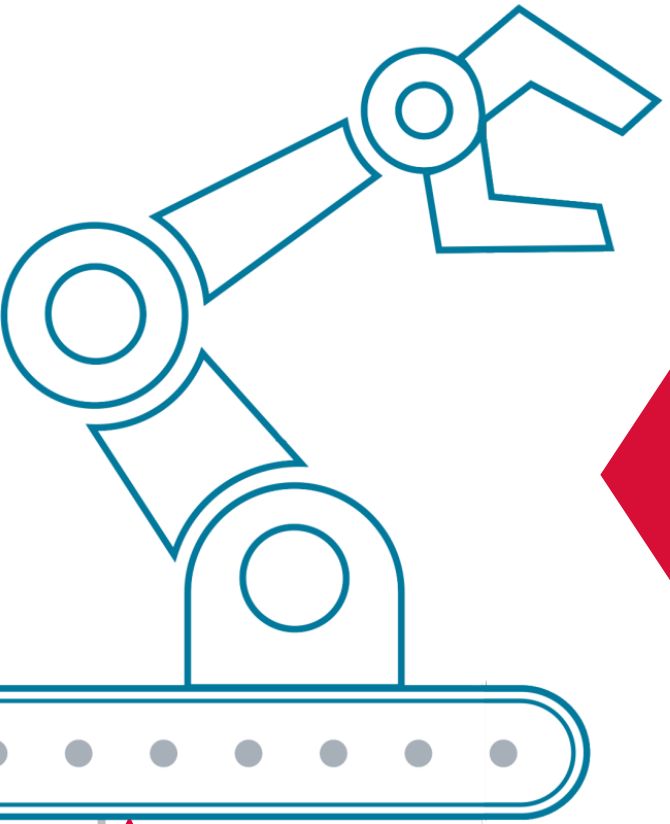
Aktuelle Bedrohungslage und Schutzbedarf

Sicherheit im Einklang mit Anforderungen der Industrie 4.0

Der Weg zur Etablierung eines angemessenen Sicherheitssystems

Überwachung von Geräten, Maschinen und Anlagen

Anlagen und Maschinen vor Netzwerken schützen



Systeme verfügen über bekannte und ausnutzbare Schwachstellen

Externe Mitarbeiter, Remote-Zugänge und Kopplung von Fremdnetzen

Zahlreiche unterschiedliche Systeme und Kommunikationen

Menschliches Fehlverhalten, Social Engineering und Sabotage

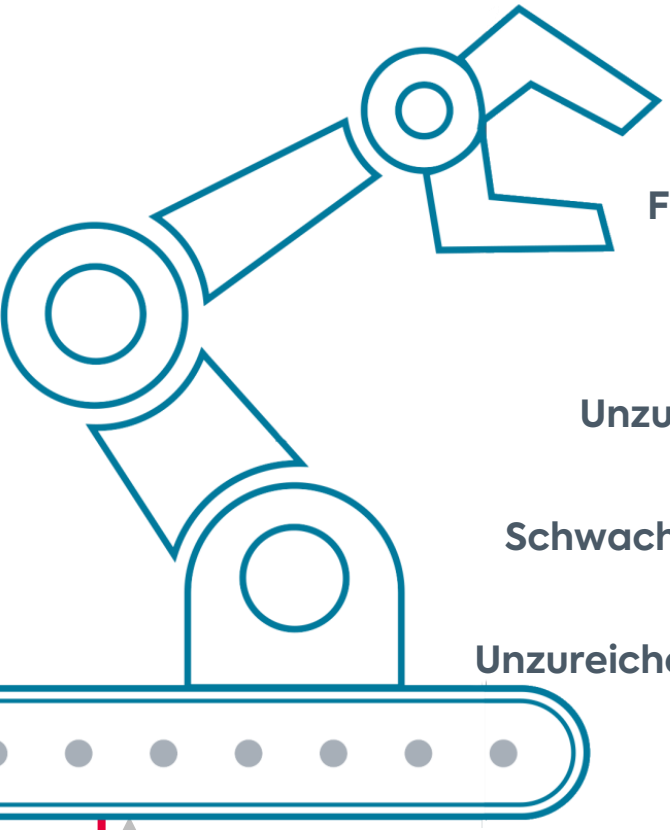
(D)Dos-Angriffe, Ausfall zentraler Gegenstellen und Technikausfall

Unzureichende Nachvollziehbarkeit von Benutzeraktivitäten

(#2 ICS-CERT / NCCIC 2017)

Überwachung von Geräten, Maschinen und Anlagen

Zentrale Automatisierungssysteme vor Maschinen und Anlagen schützen



Maschinen verfügen über bekannte und ausnutzbare Schwachstellen

Fehlender bzw. unzureichender Netzzugangsschutz

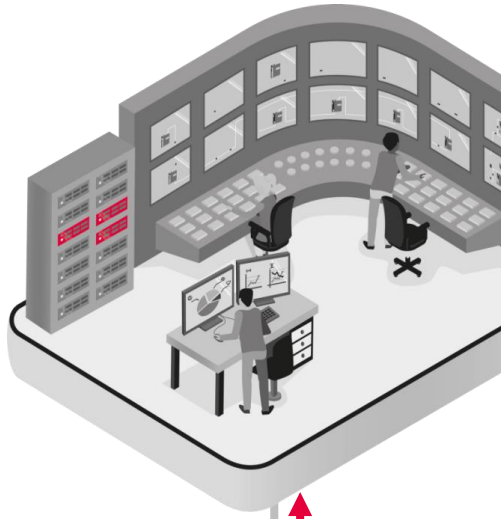
Ungesichert an das Internet angebunden
(#6 BSI ICS Top 10 Bedrohungen)

Unzureichende Absicherung der Fernwartungszugänge
(#4 BSI ICS Top 10 Bedrohungen)

Schwache Absicherung der Übergänge zwischen IT und ICS
(#1 ICS-CERT / NCCIC 2017)

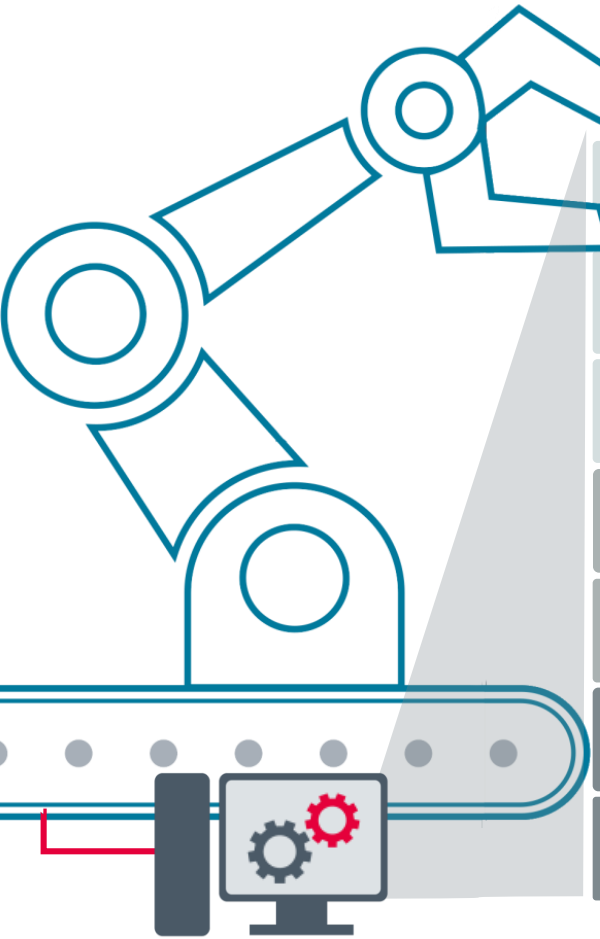
Unzureichende Nachvollziehbarkeit von Benutzeraktivitäten
(#2 ICS-CERT / NCCIC 2017)

Mangelnder Zutritts- Und Zugangsschutz
(#4 ICS-CERT / NCCIC 2017)



Warum IT-Sicherheit nicht in die Anlage integrieren?

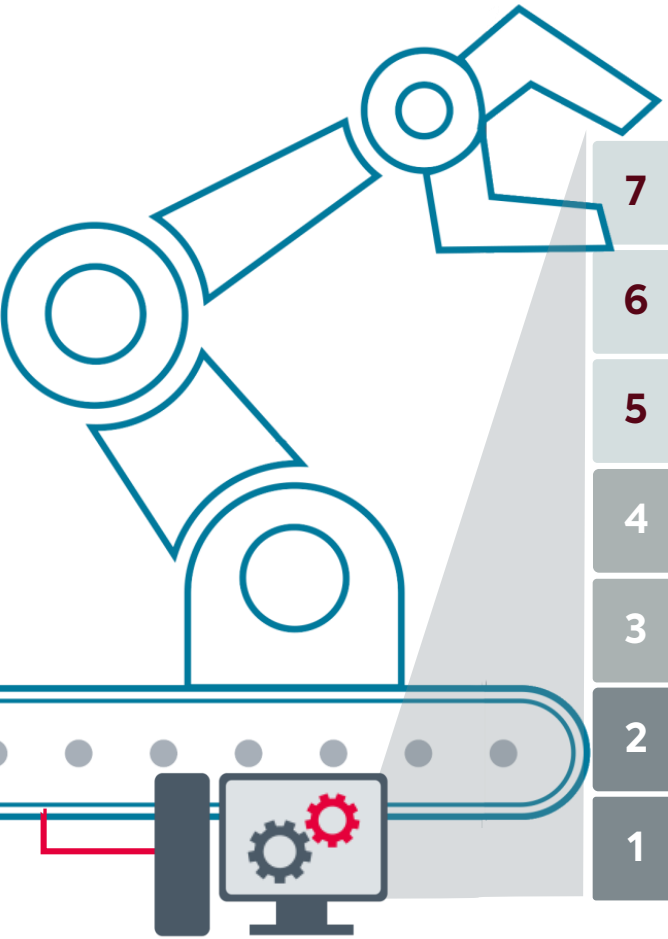
Der Lebenszyklus als Problem: Maschinen laufen > 20 Jahre



		BENUTZERVERHALTEN
7	ANWENDUNGSSCHICHT	**SCHWACHSTELLEN** in Anwendungen
6	PRÄSENTATIONSSCHICHT	**SCHWACHSTELLEN** in Laufzeitumgebungen (Java, .NET, ...)
5	SITZUNGSSCHICHT	**VERALTETE BETRIEBSSYSTEME** Windows NT / XP, ...
4	TRANSPORTSCHICHT	
3	VERMITTLUNGSSCHICHT	**FEHLER** in Treiber
2	SICHERUNGSSCHICHT	**FEHLER** in Firmware
1	BITÜBERTRAGUNGSSCHICHT	**NEUE STANDARDS**

SICHERHEITS-ANWENDUNGEN
Virenschutz, Firewall, ...

Entlastung und Sicherheit auf Basis von secunet edge



		BENUTZERVERHALTEN
7	ANWENDUNGSSCHICHT	**SCHWACHSTELLEN** in Anwendungen
6	PRÄSENTATIONSSCHICHT	**SCHWACHSTELLEN** in Laufzeitumgebungen (Java, .NET, ...)
5	SITZUNGSSCHICHT	**VERALTETE BETRIEBSSYSTEME** Windows NT / XP, ...
4	TRANSPORTSCHICHT	
3	VERMITTLUNGSSCHICHT	**FEHLER** in Treiber
2	SICHERUNGSSCHICHT	**FEHLER** in Firmware
1	BITÜBERTRAGUNGSSCHICHT	**NEUE STANDARDS**

KONTROLLIERTER ZUGANG

VPN-CLIENT | IOT AGENT | PARTNER-CONTAINER

SICHERE DOCKER-UMGEBUNG
Container-Management
Datenflusskontrolle

UP TO DATE BETRIEBSSYSTEM
(gehärtet), Langzeitsupport durch secunet

INTEGRIERTE SICHERHEIT
Protokollübersetzer
Firewall
IT-Management
Anomalieerkennung

SICHERHEITSMANAGEMENT
der Firmware

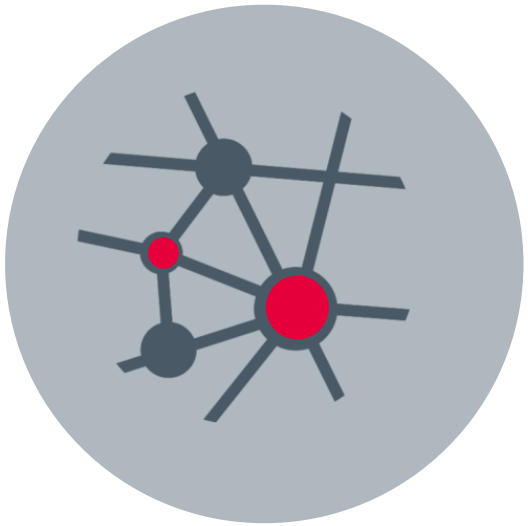
SECURE ELEMENT
(zertifiziert)

Modulares Schutzsystem zur Umsetzung individueller Use Cases

PROTECT.

Sicherheit für Systeme und Netzwerke durch Mikrosegmentierung und Isolation von Maschinen

CONNECT.

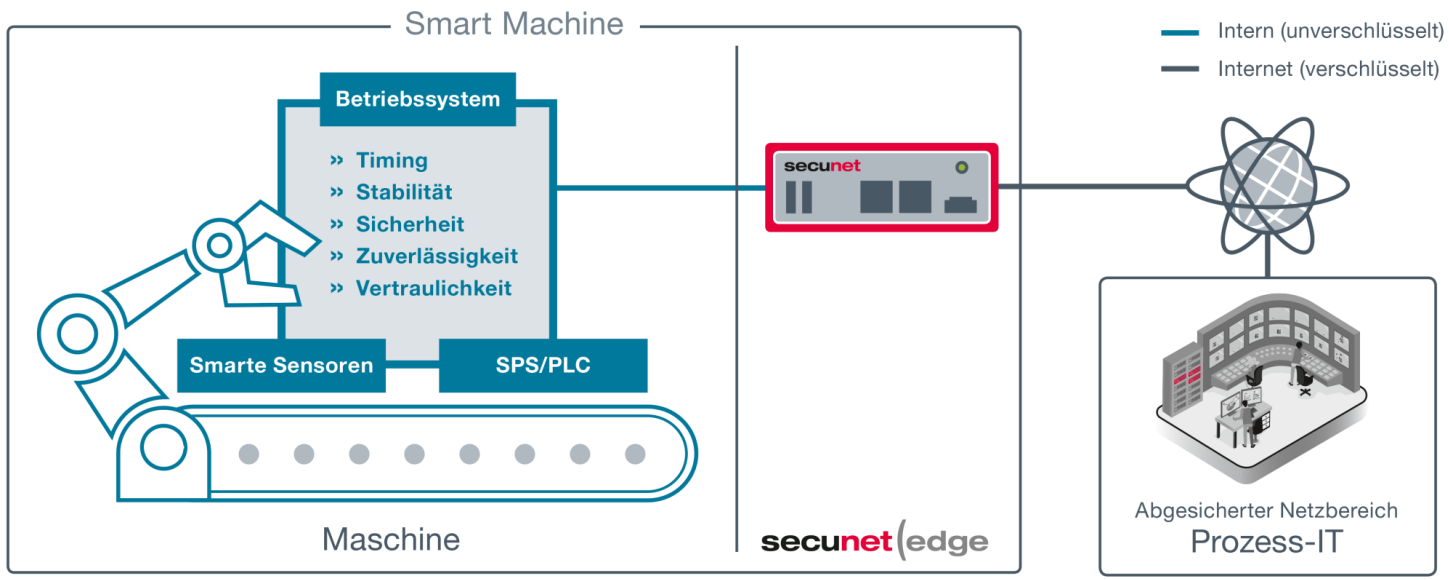


Sichere Konnektivität: Anbindung an interne und externe Dienste

DETECT.

Hohes Sicherheitsniveau durch Sicherheitsanwendungen von secunet

Protect.
Sicherheit für Anlagen und Netzwerke



Maschinen einfach sicher integrieren

- Sichere, kontrollierte und flexible Integration der Maschine in das Netzwerk
- Regulierbarer Zugriff auf Maschine und Netzwerk

Stealth Factory-Ansatz oder Mikro-Segmentierung

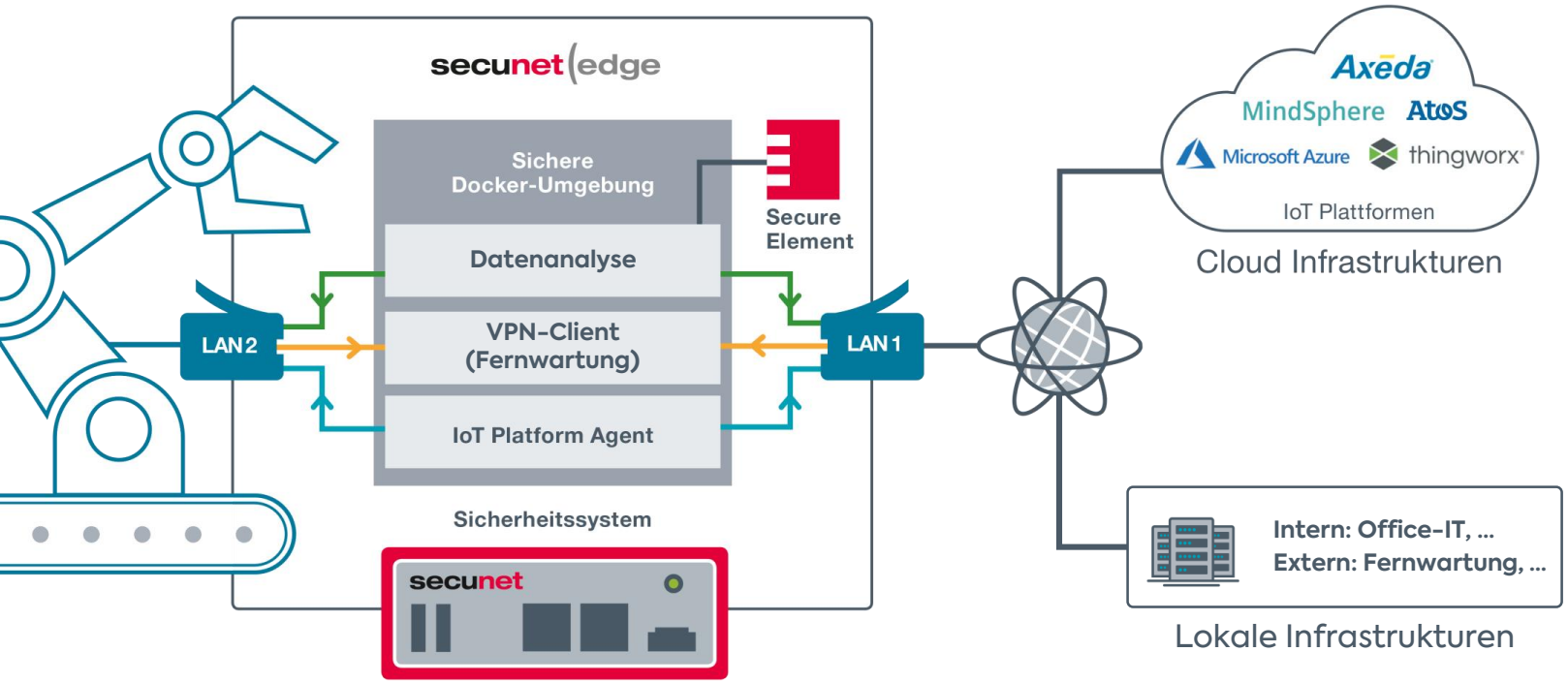
- **Stealth Mode Firewall:** Zu schützende Maschinen sind für das Internet unsichtbar
- **IP Firewall Mode:** Isolation der Maschine durch feingranulare Netzsegmentierung
- **Application Layer Gateway Mode:** Datenflusskontrolle durch intelligente und sicher betriebene Applikationen

Beispiel: Sicherer Fernzugriff

- Regelbare Zugriffssteuerung auf Geräteklassen
- Anlassbezogene Freischaltung

Connect.

Flexible Plattform mit sicherer Ausführungsumgebung für Applikationen



Die Ausführungsumgebung

Sicher und modular

- Ausführung von Applikationen in sicherer Docker-Umgebung auf gehärtetem System
- Flexibles Hinzufügen weiterer Applikationen zur Umsetzung neuer Anwendungsfälle

Eigene Geschäftsideen und Anwendungsfälle

- Schnittstellen zur Docker-Umgebung ermöglichen Entwicklung und Betrieb eigener Anwendungen

Typische Anwendungsszenarien

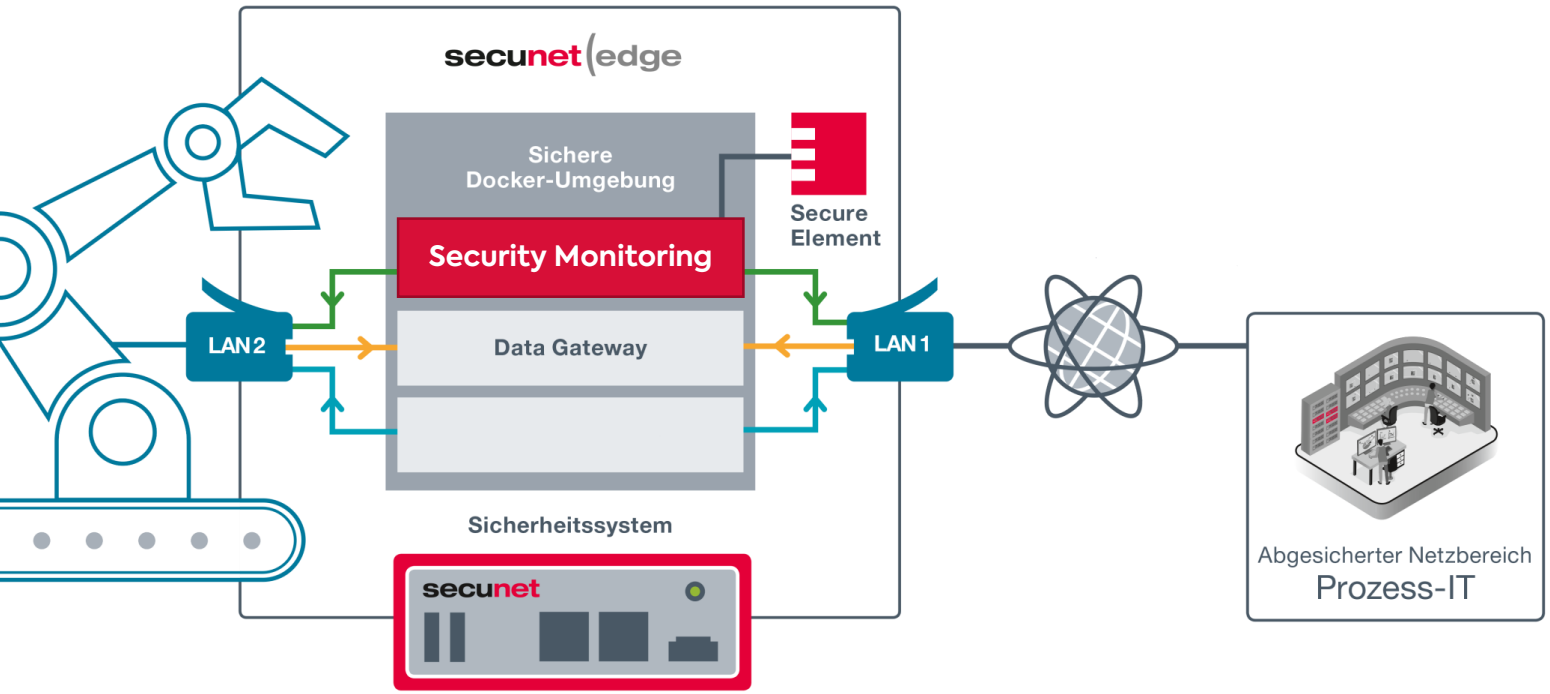
Konnektivität zwischen Maschine und Diensten

- Kontrollierte und sichere Anbindung an lokale und Cloud Infrastrukturen sowie IoT Plattformen

Edge Computing

- Lokale Analyse und Vorverarbeitung maschinenerzeugter Daten

Detect.
secunet Sicherheitsanwendungen für System- und Datensicherheit



Hardware-basierte Informationssicherheit

- Secure Element als Vertrauensanker für Informationssicherheit und Docker-Anwendungen
- Fest verbauter und manipulationssicherer Chip (vergleichbar mit Smartcard)

secunet Sicherheitsanwendungen

Data Gateway – Sichere Übertragung von Daten

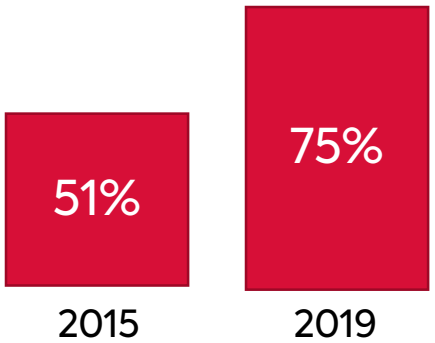
- Gerichteter Transfer von Nutzdaten der Maschine zu Backend- oder externen Diensten
- Protokollübersetzung: von sicher zu unsicher

Security Monitoring – Echtzeitüberwachung von Informationsflüssen

- Erkennen und Kontrollieren von Datenströmen
- Erkennen von Anomalien in Datenverbindungen

IT-Sicherheitslage in Deutschland

Qualität und Umfang der Cyberangriffe nehmen weiter zu



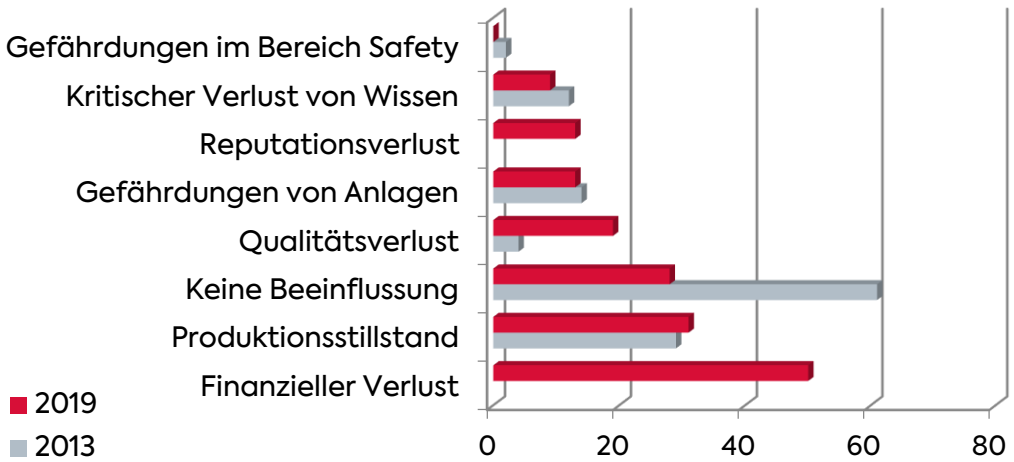
75 Prozent der deutschen Unternehmen hatten 2019 IT-Sicherheitsprobleme
(Quelle: Studie PreciseSecurity)

102,9 Mrd. Euro Schaden

pro Jahr in Deutschland
durch Datendiebstahl, Industriespionage oder Sabotage
(Quelle: Studie Bitkom 2019)

Ergebnisse erfolgter Angriffe

(Quelle: Studie VDMA 2019)



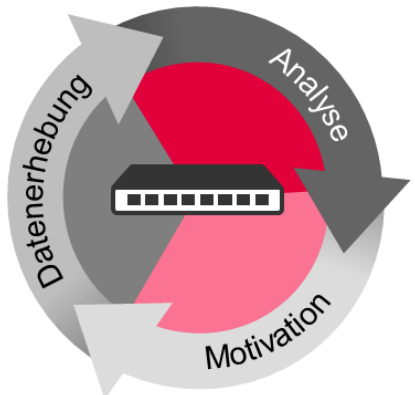
Könnte Ihr IT-Leiter diese Fragen beantworten?

secunet monitor

unsere Antwort zur Sicherheitsmonitoring in IT und OT

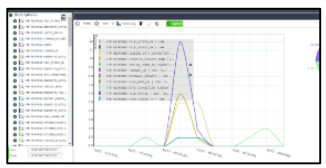
VERHALTENSANALYSE (DETEKTION)
Aufdeckung von Verhaltensauffälligkeiten (Anomalien) und Hinweisen auf zielgerichtete Angriffe (APT)

SCHWACHSTELLENANALYSE (COMPLIANCE)
Aufdecken von unbekannten Kommunikationsverbindungen und Schwachstellen

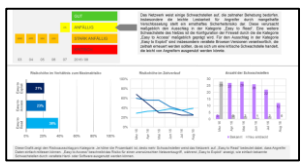


NETZWERKANALYSE
Asset Discovery, Analyse gängiger Protokolle in IT- und OT-Netzwerke

IDS/IPS (PRÄVENTION)
Bekannte Attacken aufs Netzwerk automatisiert erkennen und abwehren

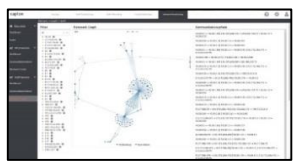


EXPERTENSYSTEM /-ANALYSE



LAGEBILD-AUSWERTUNG

ECHTZEIT-MONITORING

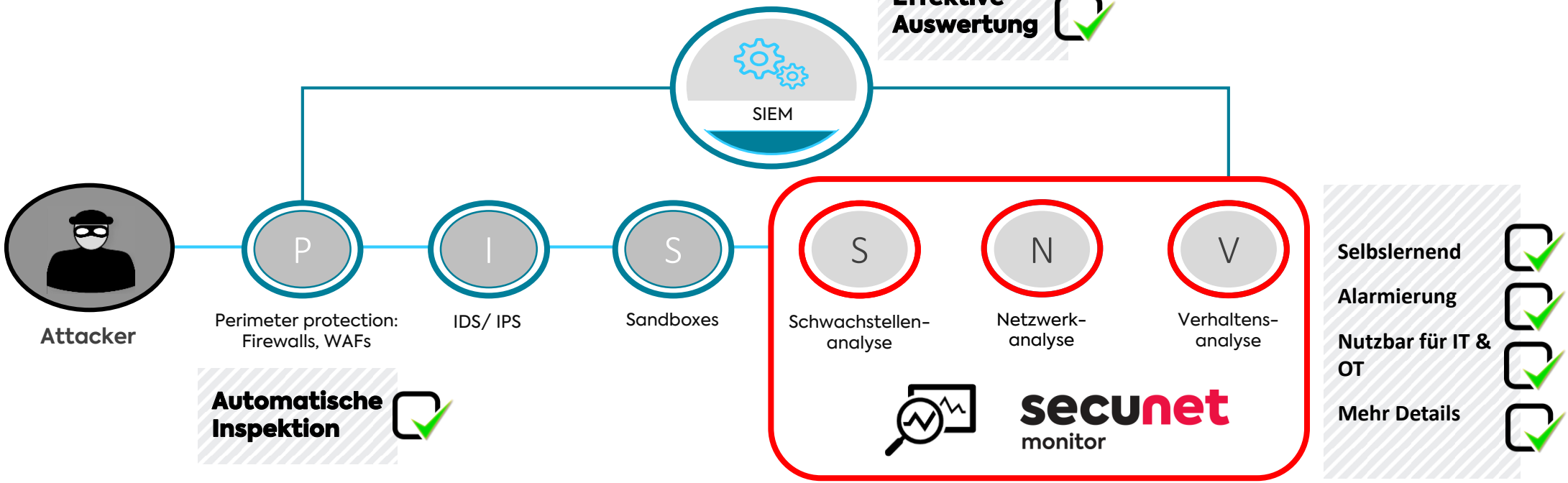


SERVICE-MONITORING

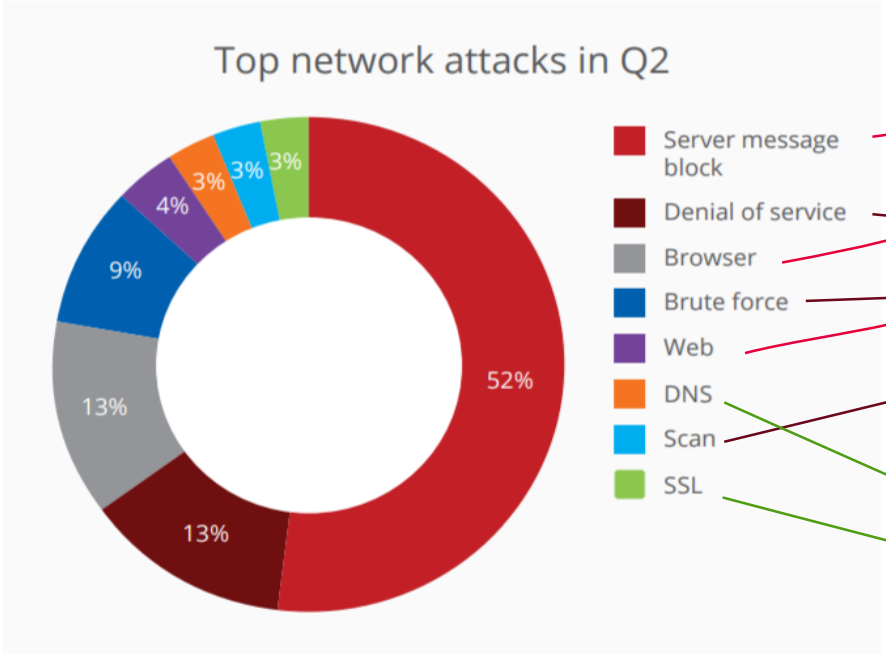
ADVANCED THREAT DETECTION

Ergänzung der klassischen Sicherheitstools

Komplementierung existierender Sicherheitskomponenten
Prüfung der umgesetzten Sicherheitsanforderungen



secunet monitor Angriffsvektoren & Verteidigungsstrategien

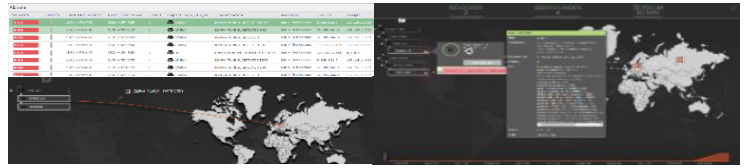


Source: McAfee Labs, 2018.

Network Compliance & Vulnerabilities

Network Anomaly Detection

Network Threat Detection



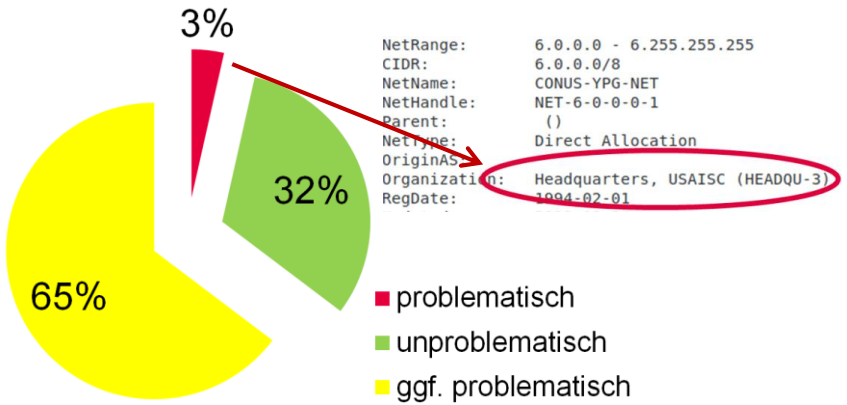
Findings bei einem letzten Kunden – Beispiele (1/3)

Vertrauenswürdigkeit des Prozessdatennetzes

- Unbekannte IT-Assets und Kommunikation
  - » 3x unbekannte Fernwartungsschnittstellen zum Hersteller
  - » 2x Datenaustausch mit Büro-IT-Netzwerk
  - » 1x Switch kommuniziert mit IP der „United States Army Intelligence and Security Command"

Widerstandsfähigkeit des Netzwerkperimeters

- Unerlaubte ICS-Kommunikation
  - » In Protokollen Modbus und PSI Ketel wurden nicht dokumentierte Funktionen verwendet



Findings bei einem letzten Kunden – Beispiele (2/3)

Vertrauenswürdigkeit des Prozessdatennetzes

- Löchrige Firewall
  - » IPsec-Verbindungsanfragen aus dem Internet kamen trotz Firewall an
  - » Fehlkonfiguration innerhalb des Untersuchungszeitraums – versehentliche Öffnung des TCP Port 23 (Telnet)
- Bekannte Schwachstellen
  - » IT-Systeme der DMZ hatten diverse Schwachstellen (z.B. alte Java Versionen und alte Betriebssystemversionen)
  - » In der DMZ wurden anfällige Protokolle verwendet (z.B. SMBv1)

Widerstandsfähigkeit des Netzwerkperimeters

- Malware
  - » Malwareinfektion auf einem ICS-Steuerungssystem mit DGA und C2

```
Standard query response 0x83f4 A fqsdyirlwpk.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0xe4b9 A qinxzzyfeqv.cn A 157.122.62.194
Standard query response 0x4722 A hfimsktquo.cn A 157.122.62.194
Standard query response 0x2e6d A hlpambj.ws A 38.102.150.27 A 104.244.14.252
Standard query 0x2ef3 A crwyxnogjv.ws
Standard query 0x726f A avllfjzb.ws
Standard query 0x6018 A hnhjh.ws
Standard query response 0xc2b4 A jjueiowzz.cn A 157.122.62.194
Standard query response 0x2ef3 A crwyxnogjv.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0x726f A avllfjzb.ws A 104.244.14.252 A 38.102.150.27
Standard query response 0x6018 A hnhjh.ws A 38.102.150.27 A 104.244.14.252
Standard query 0xc3f6 A zhtthraz.ws
Standard query 0x9f73 A loksmepbq.ws
Standard query response 0xc3f6 A zhtthraz.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0x9f73 A loksmepbq.ws A 104.244.14.252 A 38.102.150.27
Standard query 0xc234 A jvcelukrlp.ws
Standard query 0xc33c A ydqxko.ws
Standard query response 0xc33c A ydqxko.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0xc234 A jvcelukrlp.ws A 104.244.14.252 A 38.102.150.27
Standard query 0x81c6 A kgzvnwcnsgt.ws
Standard query response 0x81c6 A kgzvnwcnsgt.ws A 38.102.150.27 A 104.244.14.252
```

secunet monitor

Beispiele (3/3)

- Sichere Verschlüsselungen wurden etabliert und nachhaltig gestärkt

TLS 1.2	67.604.266	87,62
TLS 1.1	61.858	< 0,1
TLS 1.0	9.433.327	12,23
SSL 3.0	60.177	< 0,1
SSL 2.0	0	0,0
Other	0	0,0
Gesamt	**77.159.628**	**100**

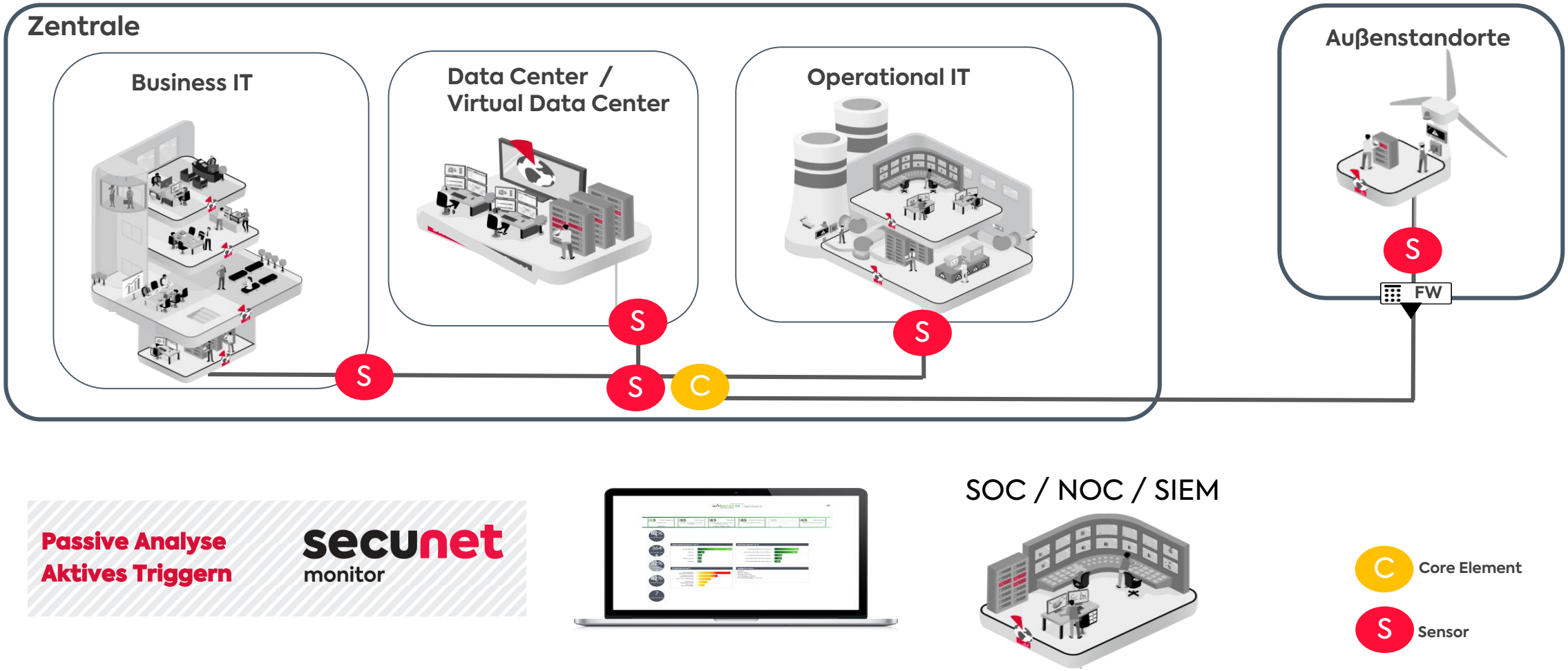
Beispiel vor der Behandlung

TLS 1.3	20.314.161	8,09
TLS 1.2	230.796.954	91,9
TLS 1.1	19.901	< 0,1
TLS 1.0	17.611	< 0,1
SSL 3.0	0	0,0
SSL 2.0	0	0,0
Other	0	0,0
Gesamt	**251.148.627**	**100**

Beispiel nach der Behandlung

secunet monitor

Beispielumsetzung: IT- und OT-Netzwerk-Infrastrukturen bei Versorgern



Passive Analyse
Aktives Triggern

secunet monitor

SOC / NOC / SIEM

C Core Element

S Sensor

On Premises oder as a Service

On Premises

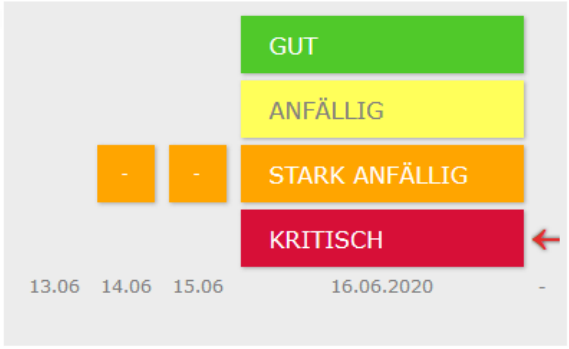
- Vollständige **Installation und Betrieb** der Sensoren und des Core-Systems **auf Seite des Kunden**
- **Auswertung** der Monitoring-Ergebnisse **durch den Betreiber**
- ggf. zusätzliche Unterstützung durch secunet bei weiterführenden Fragestellungen

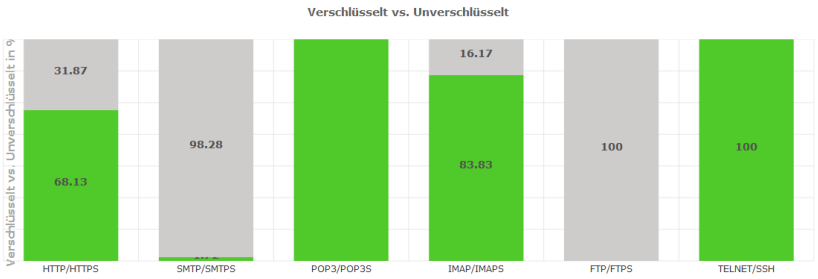
As a Service

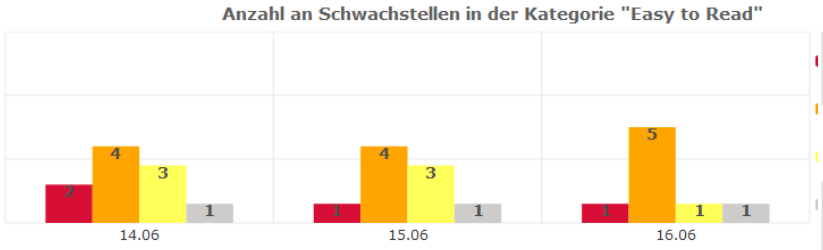
- **Installation der Sensoren beim Kunden**
- **Installation des Core-Systems bei secunet** (dedizierte sichere IT-Umgebung oder auf SecuStack – sichere Cloud)
- **Sichere Kommunikation** zw. Core-System und Sensoren
- **Auswertung** der Monitoring-Ergebnisse **durch Kunde und secunet möglich**

secunet monitor — Berichte – für Manager und Techniker

Standards leicht auf Kunden-wünsche anpassbar







Schwachstelle	Bewertung	Art	Beschreibung	Mengeninformation	Gegenmaßnahmen	Herkunft
1. DHCP IPv4	kritisch	Ausgehender Verkehr	DHCP ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.	93 Pakete	Entsprechende Ports auf Firewall schließen.	
2. Null Cipher HTTPS	kritisch	Ein- und ausgehender Verkehr	Cipher-Suite ohne Verschlüsselung. Dies täuscht Sicherheit nur vor.	4 Pakete	Cipher-Suite auf starke Cipher beschränken.	
3. Datenbank Oracle	alarmierend	Zugriff auf int. Server	Datenbanken sollten nicht von außen verfügbar sein.	2 Pakete	Datenbanken sollten nicht von außen verfügbar sein.	
4. DHCP IPv4	alarmierend	Ausgehender Verkehr	DHCP ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.	91 Pakete	Entsprechende Ports auf Firewall schließen.	
5. GE-SRTP	alarmierend	Zugriff auf ext. Server	ICS Protokolle beinhalten unter anderem Steuerbefehle für Industrieanlagen.	2 Pakete	Entsprechende Protokolle sollten im IT-Netz nicht auftauchen.	
6. OPCUA	alarmierend	Zugriff auf ext. Server	ICS Protokolle beinhalten unter anderem Steuerbefehle für Industrieanlagen.	92 Pakete	Entsprechende Protokolle sollten im IT-Netz nicht auftauchen.	
7. NetBIOS	alarmierend	Eingehender Verkehr	API zur Kommunikation zwischen zwei Programmen über ein lokales Netzwerk.	2 Pakete	Entsprechende Ports auf Firewall schließen.	
8. Firefox Version 3.x or lower (User-Agent)	hinweisend	Antwort von ext. Server	Durch einen veralteten Browser können Angreifer gezielt bekannte Schwachstellen ausnutzen und so Kontrolle über das System erlangen oder Einsicht in sensible Daten erhalten.	261 Pakete	Auf aktuelle Version von Firefox updaten.	

Schwachstelle	Bewertung	Art	Beschreibung	Mengeninformation	Gegenmaßnahmen	Herkunft
4. Windows XP (User-Agent)	alarmierend	Zugriff auf ext. Server	Der User-Agent ist ein Hinweis auf ein Betriebssystem. Windows XP sollte nicht mehr genutzt werden, da es keine Updates mehr erhält. Durch ein veraltetes Betriebssystem können Angreifer gezielt bekannte Schwachstellen ausnutzen und so Kontrolle über das System erlangen oder Einsicht in sensible Daten erhalten.	37 Pakete	Aktuelles Betriebssystem aufspielen oder Host vom Internet trennen.	
5. Internet Explorer 9 (User-Agent)	alarmierend	Zugriff auf ext. Server	Durch einen veralteten Browser können Angreifer gezielt bekannte Schwachstellen ausnutzen und so Kontrolle über das System erlangen oder Einsicht in sensible Daten erhalten.	97 Pakete	Überprüfen, ob Installation eines neuen Browsers möglich ist und Umstieg auf Firefox oder Host vom Internet trennen.	
6. Internet Explorer 10 (User-Agent)	alarmierend	Zugriff auf ext. Server	Durch einen veralteten Browser können Angreifer gezielt bekannte Schwachstellen ausnutzen und so Kontrolle über das System erlangen oder Einsicht in sensible Daten erhalten.	106 Pakete	Überprüfen, ob Installation eines neuen Browsers möglich ist und Umstieg auf Firefox oder Host vom Internet trennen.	
7. Windows 2003 Server (User-Agent)	alarmierend	Zugriff auf ext. Server	Der User-Agent ist ein Hinweis auf ein Betriebssystem. Windows 2003 Server sollte nicht mehr genutzt werden, da es keine Updates mehr erhält. Durch ein veraltetes Betriebssystem können Angreifer gezielt bekannte Schwachstellen ausnutzen und so Kontrolle über das System erlangen oder Einsicht in sensible Daten erhalten.	62 Pakete	Aktuelles Betriebssystem aufspielen oder Host vom Internet trennen.	

secunet monitor

Network Flight Recorder für Spezialanalysen

Möglichkeit einer optionalen detaillierten Datenanalyse

Aktivierung eines Network Flight Recorders (Ringspeicher) auf dedizierten Sensoren

Protokollierung des gesamten Netzwerkverkehrs

Analyse der vollen Netzwerkdaten samt Inhalte möglich

secunet monitor

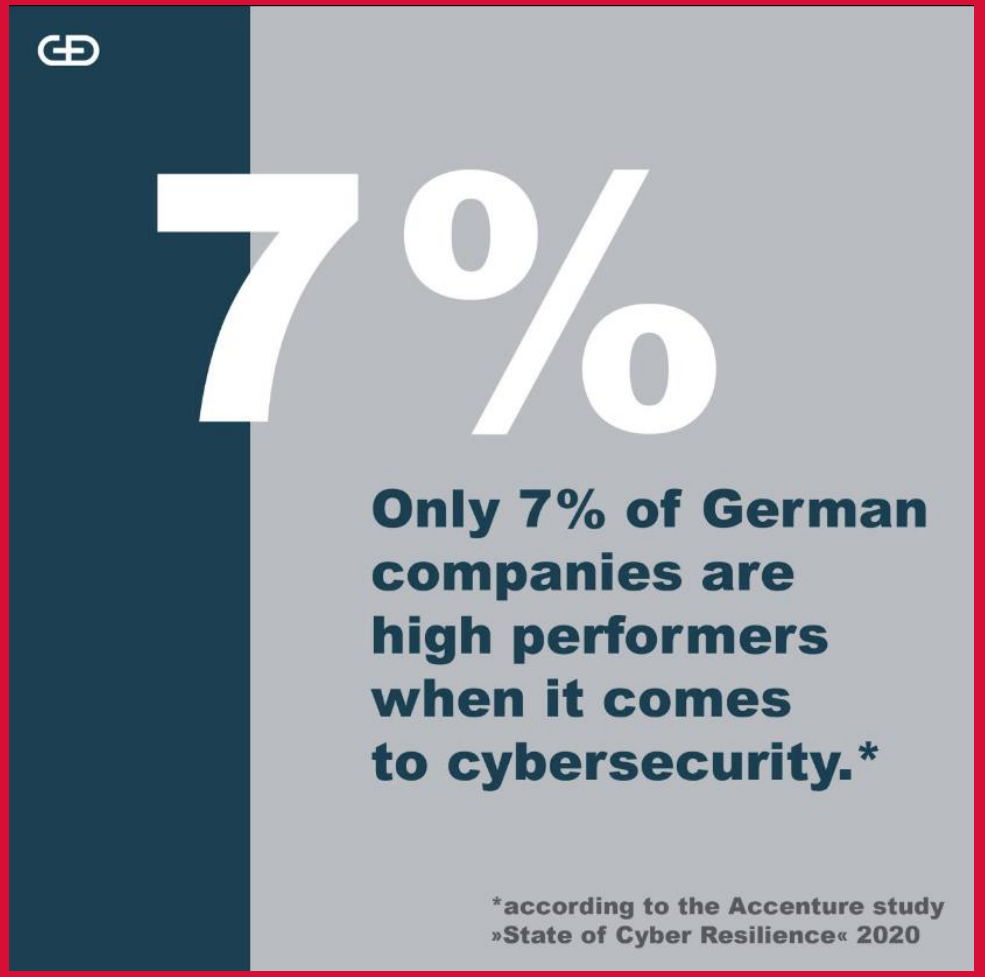
Vorteile der Lösung auf einen Blick

- Passive Analyse, aktive Trigger-Möglichkeit – **kein aktives Eingreifen in Prozessaktivitäten**
- **Maschinell-lernende Anomalieerkennung**
- **Tiefgehende Protokollanalye**
- Möglichkeit des Betriebes **on promises oder as a Service**
- Nutzbar auf **verschiedenen Hardware-Plattform**
- **Leicht erweiterbar** (Zugriffskontrolle auf vollständigen Quellcode durch secunet)
- integrierbar mit anderen Sicherheitssystemen (z.B. Log-Auswertungen)
- **Datenschutz-konform** zu GDPR / EU-DSGVO
- Made in Germany

secunet.com

Steffen Heyde

secunet Security Networks AG



secunet