Mehr Transparenz im Risikomanagement und Realtime-Monitoring in der Automatisierungsebene

Markus Wolf
Division Kritische Infrastrukturen

Daten & Fakten

secunet Security Networks AG

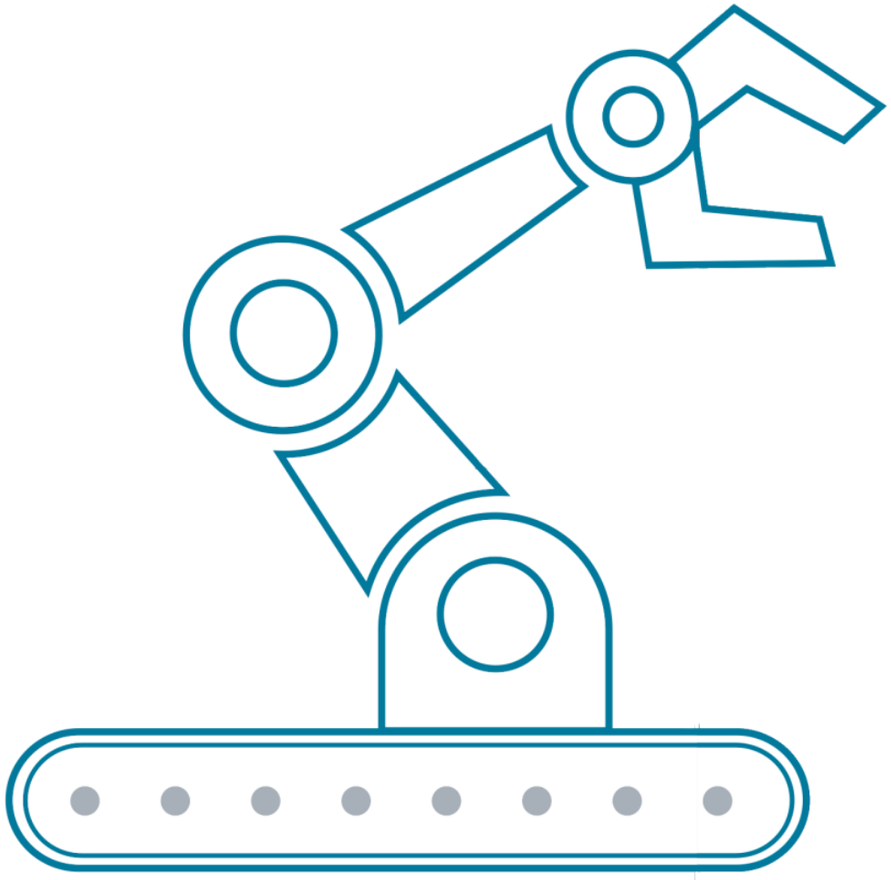
- Kundenorientierte Unternehmensstruktur
- Mehr als 500 Mitarbeiter an elf deutschen Standorten
- Gegründet 1997
- Im Prime Standard der Deutschen Börse gelistet
- Größter Anteilseigner (79%): Giesecke & Devrient GmbH
- Umsatz 2018: € 163,3 Mio.
  EBIT 2018: € 26,9 Mio.

Warum dieser Vortragstitel?

Warum dieser Vortragstitel?

Unser letzter Kunde hat mich darauf gebracht.

Unser letzter Kunde - Steckbrief



- produzierendes Unternehmen
- Informationssicherheits-managementsystem (ISMS) eingeführt und zertifiziert
- Diverse IT-Sicherheitsmaßnahmen umgesetzt

Was sollten wir tun?

Was sollten wir tun?

Bestätigen, dass nun alles sicher ist.

Was sollten wir tun?

Vertrauenswürdigkeit
des Produktionsdatennetzes

Widerstandsfähigkeit
des Netzwerkperimeters

Was Sie wissen müssen!

Vertrauenswürdigkeit
des Produktionsdatennetzes

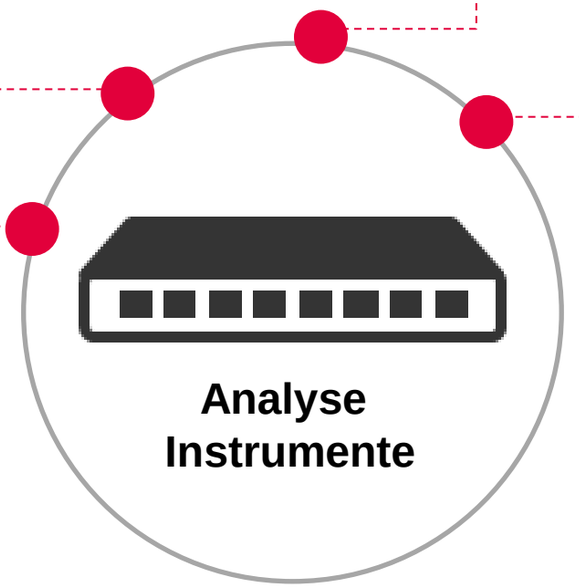
Widerstandsfähigkeit
des Netzwerkperimeters

Sämtliche
Kommunikation

Relevante
Schwachstellen

Alle
IT-Assets

Anomales
Kommunikationsverhalten



secunet

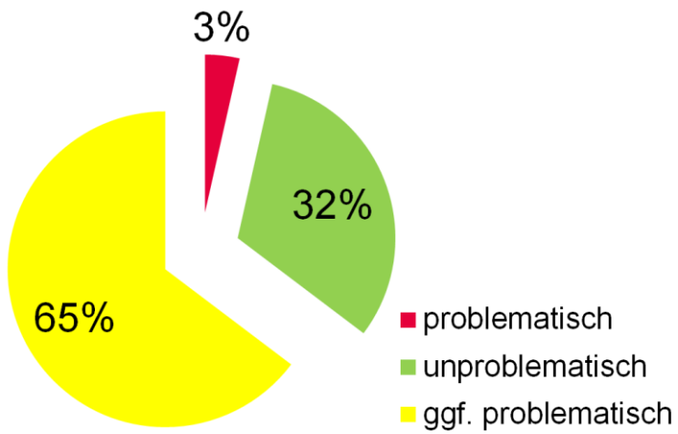
Was kam heraus?

Interessantes!

Was kam heraus - Überblick

Vertrauenswürdigkeit des Produktionsdatennetzes

- Unbekannte IT-Assets und Kommunikation



  - 1x Switch eines weltweit bekannten Herstellers kommuniziert mit IP eines sicheren Drittstaats
  - 3 x unbekannte Fernwartungsschnittstellen zum Hersteller
  - 2x Datenaustausch mit Büro-IT-Netzwerk

Widerstandsfähigkeit des Netzwerkperimeters

- Löchrige Firewall
  - IPsec-Verbindungsanfragen aus dem Internet kamen an, obwohl Firewall das unterbinden sollte
  - Fehlkonfiguration innerhalb des Untersuchungszeitraums - versehentliche Öffnung des 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)

secunet

Darum dieser Vortragstitel!

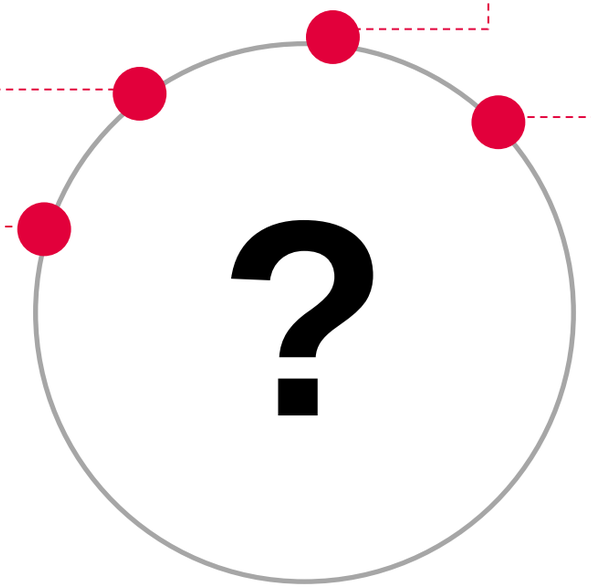
Und nun?

1. **Prüfen Sie den Grad der Transparenz und führen Sie eine derartige Analyse durch.**

Und nun? – Prüfen Sie den Grad der Transparenz

Sämtliche
Kommunikation

Relevante
Schwachstellen



Alle
IT-Assets

Anomales
Kommunikationsverhalten

secunet

Und nun?

2. **Ermitteln Sie wesentliche IT-Sicherheits-Risiken anhand typischer UseCases und handeln Sie.**

Und nun? – Ermitteln typischer UseCases

Sichere Anbindung an int. Netzwerke

Cloud-Dienste und Fernwartung

Realtime-Monitoring

Sicherer Datenaustausch

secunet

Und nun? – Handeln Sie

HARDWARE FÜR DEN INDUSTRIELLEN EINSATZ

- Industrielle Langzeitverfügbarkeit
- Betriebstemperatur: -40°C bis +85°C
- passiv gekühlt
- schock- und vibrationsresistent (IP 40)
- VESA-Mount (75x75, 70x70)
- Befestigung für DIN-Rail und 19” Racks
- CE, FCC, EN50155 zertifiziert

INDIVIDUALISIERUNG DURCH DOCKER-UMGEBUNG

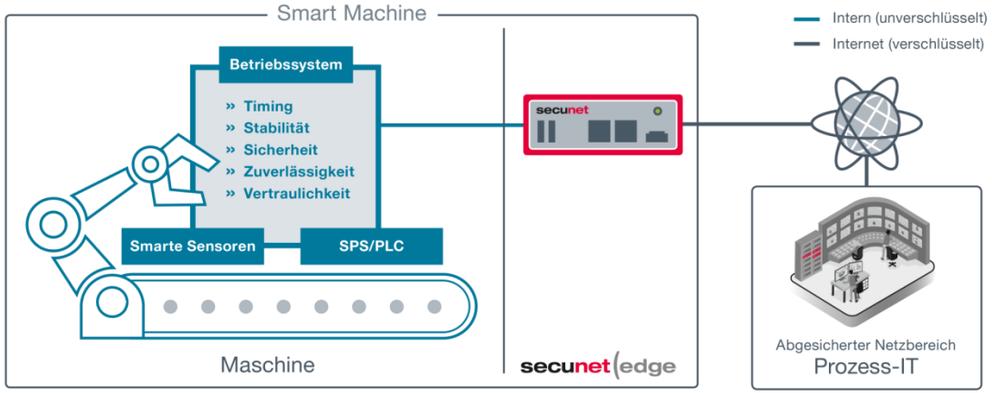
- Zukunfts- und investitionssicher: modular erweiterbar um weitere Anwendungen
- Flexible Umsetzung eigener Geschäftsmodelle
- Eigenständiges Entwickeln und Betreiben von Docker-Anwendungen
- Sicherheitsanwendungen für Industrie 4.0-Anwendungsfälle verfügbar

IT-INTEGRATION

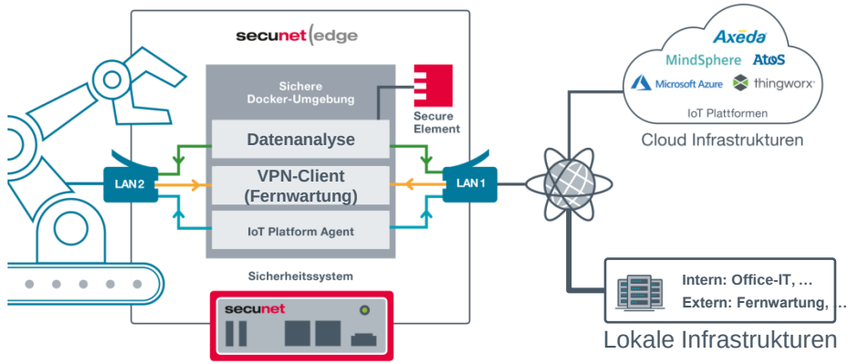
- Einfache und schnelle Integration in bestehende OT-Infrastrukturen
- LAN, Bluetooth, Wi-Fi, 4G, serieller COM-Port

Und nun? – Handeln Sie

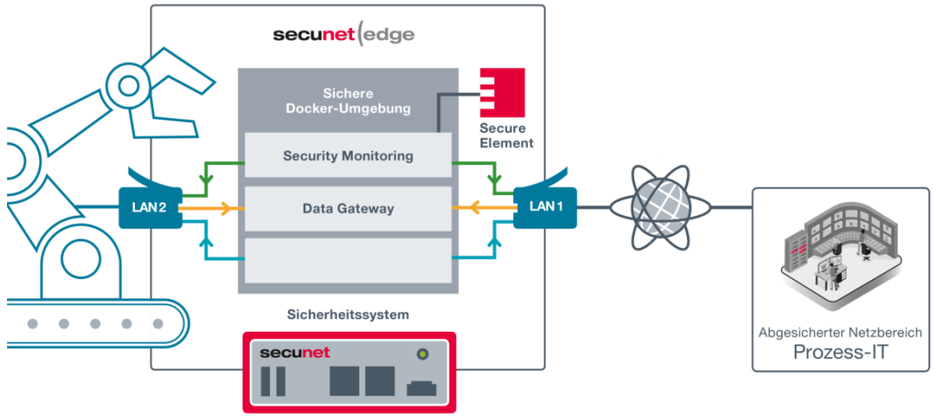
Sichere Anbindung an int. Netzwerke



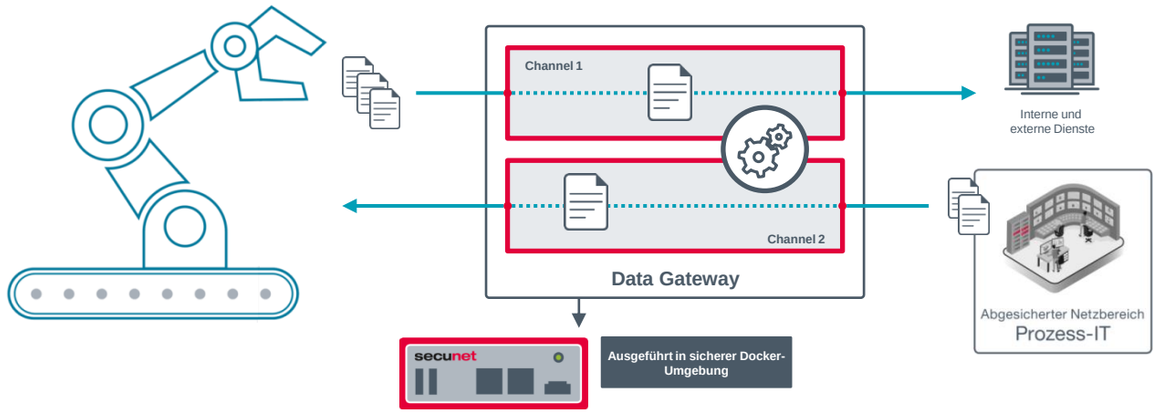
Cloud-Dienste und Fernwartung



Realtime-Monitoring



Sicherer Datenaustausch

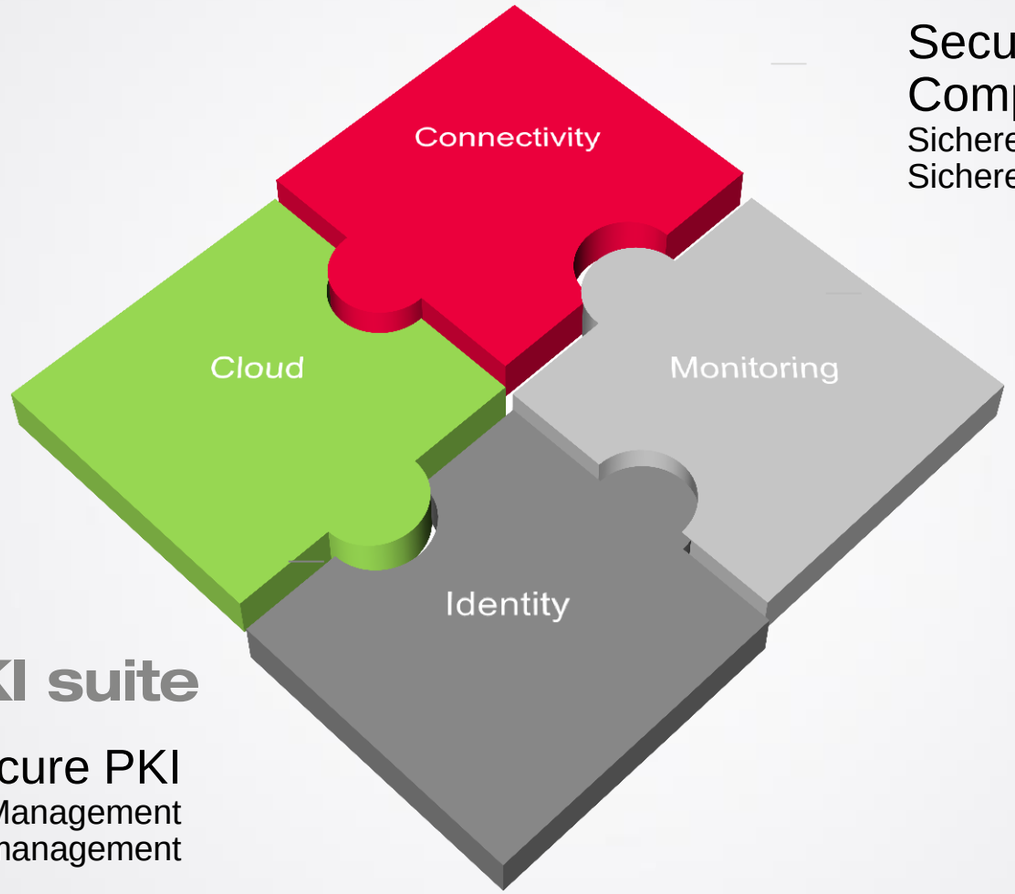


secunet

Und nun? – Handeln Sie

secustack

Secure Cloud Solution
Sichere Mandantenfähigkeit
Sicheres Key Management
Sichere Datenspeicherung
Sichere Anbindung



secunet edge

Secure Edge Computing
Sichere Netzwerk-Separierung
Sichere Anbindung

finally safe

Security Monitoring
Netzwerkanalyse
Anomalieerkennung
Schwachstellenanalyse
IDS/IPS

secunet eID PKI suite

Secure PKI
Sicheres Key-Management
Sicheres Zertifikatsmanagement

Markus Wolf
Leiter, Security Infrastructure - Industrial Security

secunet Security Networks AG
Alt-Moabit 96,
10559 Berlin
Telefon +49 201 5454-3756
Telefax +49 201 5454-1321
markus.wolf@secunet.com