NOZOMI NETWORKS

IKARUS security software

Herbert Dirnberger

Industrielle Cyber Sicherheit verstehen und anwenden

Praxiserprobtes Know-how für die sichere Produktion und kritische Infrastruktur

IKARUS Security in a Nutshell

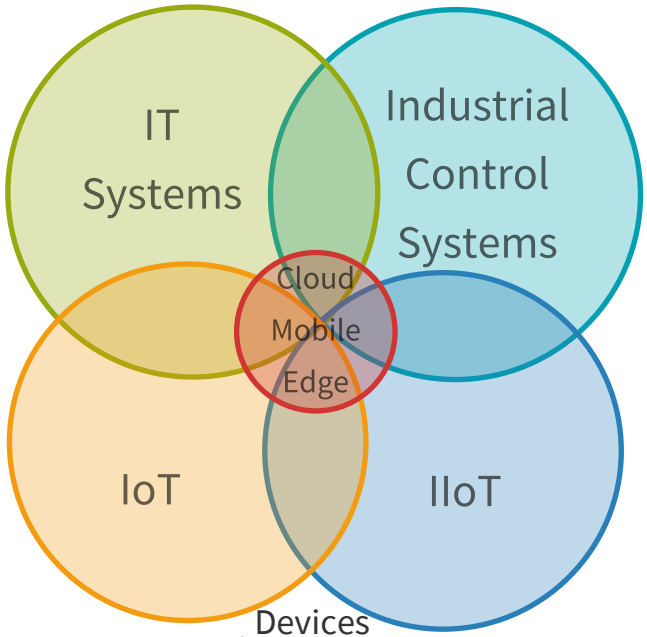

Automation
Industrial IT
Operational Technology
Industrial IoT
BAD BOY
IODINE
FREEMAN-RUSSELL
DR JAKE DAWSON'S
LINIMENT TONIC
SNAKE OIL
50¢
A wonderful pain destroying compound
NEURALGIA, SCIATICA, LAME BACK, LUMBAGO
FROSTBITES, CHILL BLAINS, BRUISES SORE THROAT & BITES OF ANIMALS, INSECTS AND REPTILES.
HAIR GROWING TONIC
IMMEDIATE RELIEF
COUGH NOSTRUM
New

Bleeding Edge meets Legacy

Manage Information

IT

Systems



Devices

Manage Physical Processes

OT

Next Generation IIoT

"Industrial Edge Computing"

with Industrial IoT Controller

"The Industrial Internet of Things and service is not an upgrade, it is a new world of technology."

https://smartbuildingsmagazine.com/news/creating-value-iot-and-data-analytics-from-beckhoff

NOZOMI NETWORKS

IKARUS security software

Die Herausforderung

Digitale Transformation inklusive (Business Kontinuität und Cyber Resilienz)

Stillstände, Legacy

Cyber Risk

NOZOMI NETWORKS

IKARUS security software

Motivatoren für Industrielle Cyber Sicherheit

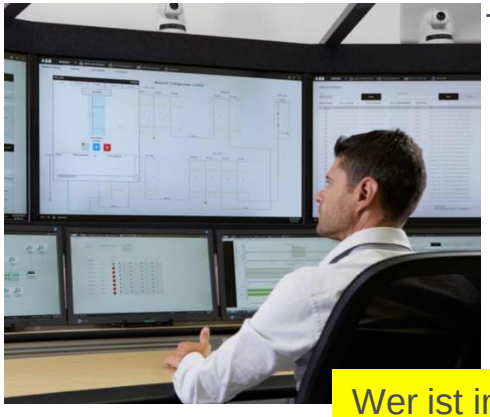
Business Kontinuität und Cyber Resilienz

Compliance

Bedrohung durch Cyberangriffe

https://www.forbes.com/sites/daveywinder/2019/02/19/how-the-speed-of-russian-bears-can-help-your-business-understand-the-1-10-60-rule/

Digitalisierungs-strategie



Transformation

Wer ist im Unternehmen für Industrielle Cyber Sicherheit verantwortlich?

Industrial Cyber Security Program / Journey

Asset discovery is one of the critical aspects of managing and securing OT/IoT

“Our common journey get started with a proof of value (PoV)“

“We want to enable your OT Security capabilities“

60% of orgs are here

30% of orgs are here

10% of orgs are here

OT/IoT Asset Disovery and Inventory

Asset Discovery

- Geräte suchen und entdecken
- Örtliche Position – Location
- Meist ohne Feldbus-Geräte
- Ansprechpartner und Owner
- Manuelle Erfassung
- Import von Projektinformationen
- Active Scanner und Agents (IT) oder Passives Sniffing (OT)

+ Metadata

Asset Inventory

- Überblick über Komponenten und Systeme **(aggregiert** und immer aktuell)
- Hardware, Software, Betriebssystem, Firmwarestände, Seriennummern, User/shares Netzwerkkonfiguration etc.
- (Schwachstellen und Patches)
- Kopplung an ERP und CMDB

Single Source of Truth

of reachable IP Addresses in OT

Asset Metadata I

- Physical Location - Ortskennzeichen
  - AM-H31a Amstetten, Halle 31, Produktionszelle
  - ZS-H12a-S1 Zell am See, Halle 12, Zelle A, Schaltschrank 1
- Types
  - PLC, HMI, IED, IFW (Industrie Firewall), ISW (managed Industrial Switch), CNC, ROB, etc.
- Unique Hostnamen (Labels)
  - AM-H31A-IFW-1 Amstetten, Halle 31, Produktionszelle 1, Industriefirewall, Index 1
  - AM-H31A-IPC -1 Amstetten, Halle 31, Produktionszelle 1, Industrie PC, Index 1
  - AM-H31A-HMI-2 Amstetten, Halle 31, Produktionszelle 1, Human Machine Interface, Index 2

Asset Metadata II

- Purdue Model für Asset Typen! (Produktion)
  - L5 Enterprise and Cloud Services
  - L4 Site Business Operations (ERP)
  - L3.5 DMZ IT/OT
  - L3 Operations Control (Historian, MES) (hosted by IT in Datacenter)
  - L2.5 Industrial DMZ

  ----- CELL -----
  - L2 Control (HMI, SCADA)
  - L1 Process (PLC, RTU, IED, ...)
  - L0 Physical (Sensor, Aktor)

Asset Metadata III

- Kritikalität
  - None, Low, Medium, High
- Security Level
  - SL0 … SL4 nach IÉC 62443
- Owner (Rollen)
  - OP-AUT-ENG
  - IT-SRVMGT
- Beschreibung, Repositories, Inbetriebnahmedatum, …

OT Security Sensor – „automatisiertes“ Asset Inventory

Virtual

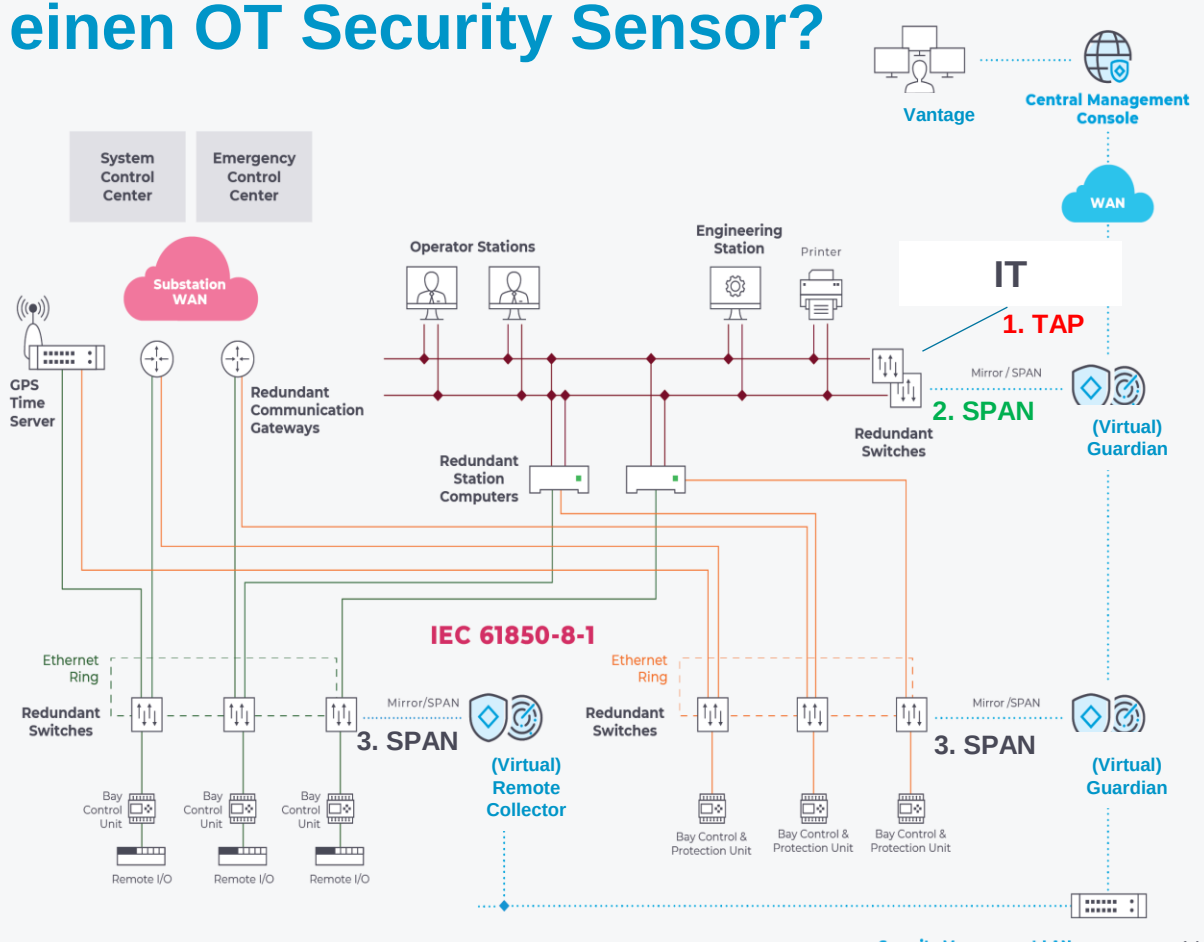
vmware ESXi

NOZOMI NETWORKS

Wie integriert man einen OT Security Sensor?

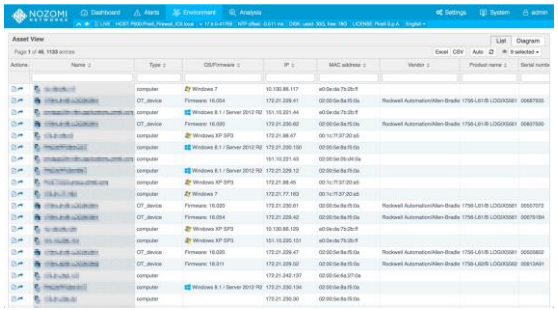
- **Passive Erfassung**
- **SPAN**/Mirror Port von Switchen
- **TAP** Test Access Points
- Network Packet Broker

1. **TAP** Nord Süd (IT/OT)
2. **SPAN** Ost West (zw. OT Zellen)
3. **SPAN** Industrial Ethernet in OT Zelle (Real Time Traffic etc)

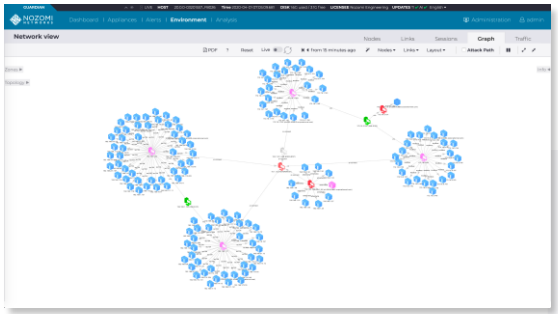


Was ist der Nutzen eines OT Security Sensors?

Automatisiertes Asset Inventory

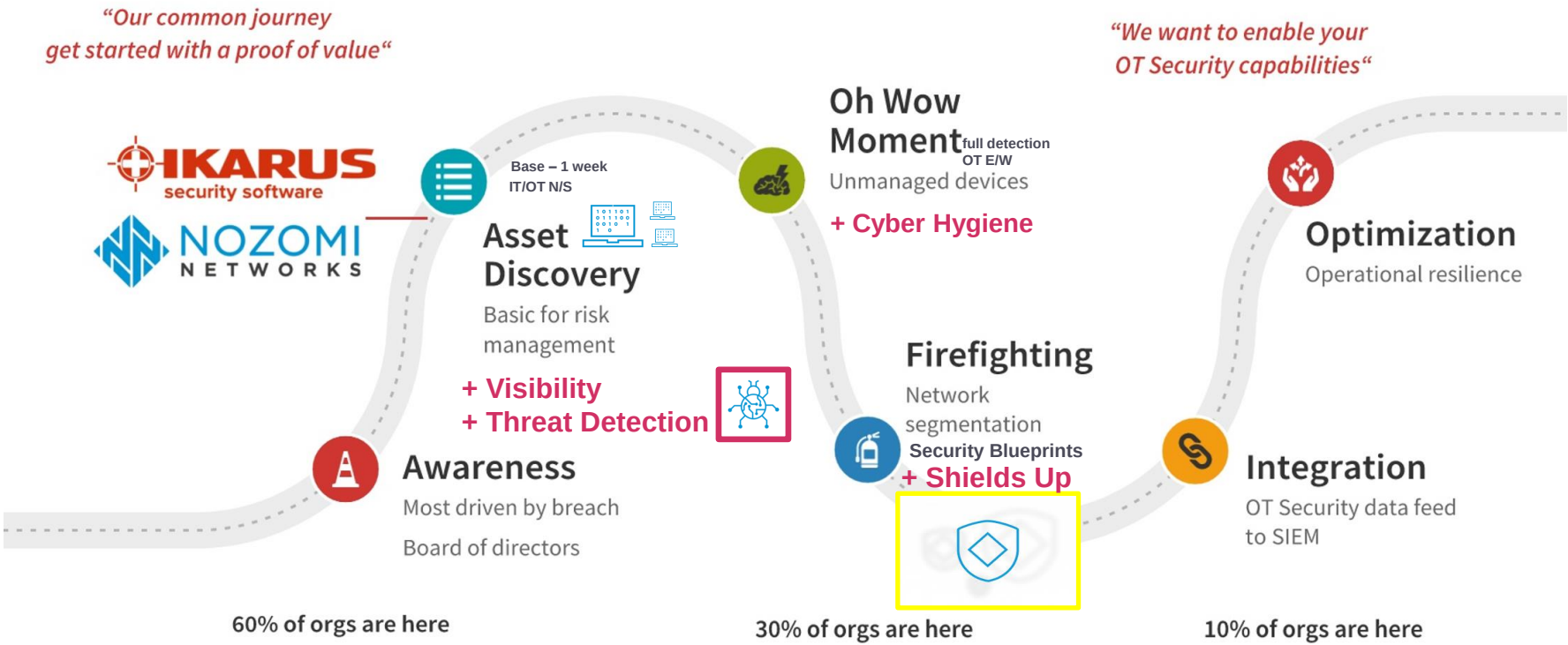


Visualisierung und Monitoring



Advanced Threat Detection und Abwehr

Industrial Cyber Security Program / Journey



Herbert Dirnberger
Industrial Cyber Security Expert

IKARUS security software

NOZOMI NETWORKS Industrial Cyber Security

You've heard from us.

We want to hear from **you.**

+43 1 58995-500

sales@IKARUS.at

https://www.IKARUSsecurity.com