Wie OT Security die Digitalisierung beschleunigt statt verlangsamt

Johannes Raff, CEO, Clue Security Services AG

IoT Security

Agenda

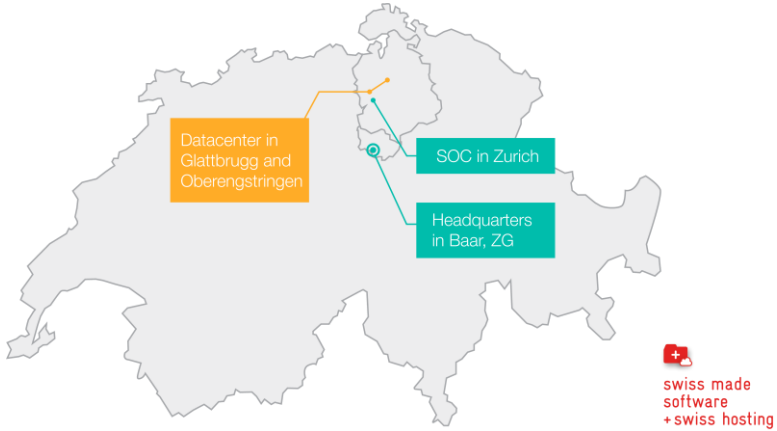
- Was ist OT
- OT Security – für wen relevant?
- Challenges
- Lösungen
- Massnahmen
- Vorgehen und Lösungsanätze
- Fazit

Clue in Kürze

- Gründung 2015
- Hauptsitz in Baar, ZG

- Schutz der IT-Infrastruktur für Unternehmen aller Art und Grösse
- Globales Kundennetzwerk
- Kunden profitieren von einem unkomplizierten, sicheren Betrieb ihrer Security-Architektur
- Security Operation und Defence Center in Baar

- Consulting zur Erhebung, Design und Umsetzung OT Security anhand von IEC62443
- SOC für IT und OT Infrastrukturen
- OT Managed Security Services
- Erfolgreiche Projekte in IT / OT Security weltweit



All the Things: OT-Security

Johannes Raff

CEO, GICSP

SECURITY SERVICES AG

CLUE

Neuhofstrasse 5a
6340 Baar

Tel. +41 44 667 77 66
info@clue.ch

clue.ch

Was sind für uns Operational Technologies

–

und was nicht?

- Umgebungen mit ICS
- Produktionsalagen (Einzeln oder übergreifend)
- Gebäudemanagement Systeme
- Kraftwerke
- Energiewirtschaft
- Manufacturing Management Systeme

- **IoT – Internet of Things**
  - Privatanwendung
  - Vernetze Geräte und Sensoren (Automaten, …)

Wikipedia: “From the very beginning security of operational technology has relied almost entirely on the **standalone** nature of OT installations, security by obscurity.”

Für wen Realität?

Cyberkriminelle veröffentlichen Daten von Läderach

Von Philipp Anz, 6. Oktober 2022 um 17:31

SECURITY CYBERANGRIFF RANSOMWARE SCHWEIZ LÄDERACH

Foto: Läderach

Einen Monat nach dem Cyberangriff auf den Schweizer Chocolatier sind mehrere Datenpakete im Darknet aufgetaucht. Läderach erklärt uns, die Situation genau zu beobachten.

Am 5. September hatte der Glarner Schokoladeproduzent Läderach einen Ransomware-Angriff festgestellt. Produktion, Logistik und Administration waren anfänglich beeinträchtigt, konnten aber im Verlauf von zwei Wochen ihre Arbeit nahezu im vollen Umfang wieder aufnehmen. Der Chocolatier bestätigte allerdings, dass bei dem Cyberangriff vermutlich Daten abgeflossen seien und warnte seine Mitarbeitenden entsprechend, private Daten könnten

Blick

Auch Angriffe in der Schweiz – die Trinkwasserproduzen investieren in die Sicherheit

Hacker vergiften Trinkwasser-Anlage in Florida

Mit ein paar Mausklicks haben Hacker in Florida die Mischung der Trinkwasser-Zutaten verändert und die Menge einer Chemikalie um über Hundertfache erhöht. Au Trinkwasser-Anlagen zu

Publiziert: 09.02.2021 um 21:43 Uhr

Industroyer2 Targets Ukraine's Electric Grid: How Companies Can Stay Protecte and Resilient

ICS/OT Security | 4 MIN READ NEWS

Ransomware Gangs Ramp Up Industrial Attacks in US

The manufacturing segment was especially hard hit by cyberattacks in the third quarter of 2022.

Tara Seals
Managing Editor, News, Dark Reading

October 26, 2022

Share Thi

ver grid using a new version of Industroyer mal
n created the following rapid update to help fa

rovides Industroyer2 Indicators of Compromis
own activity linked to the malware. There have
hich is an indication that the threat actors had
re deploying. Nozomi Networks will provide
mples are analyzed in-depth.

Blick

Schweiz | Zentralschweiz | Hacker-Attacke auf Wasserversorgung in Ebikon LU

Urheber in London und Korea

Hacker-Attacke auf Wasserversorgung in Ebikon LU

Die autonome Betriebssteueru
Ebikon LU hat im November Ta
bekommen.

Neue Zürcher Zeitung

Cyberangriff auf die Hirslanden-Gruppe: Die Spitäler sind wegen der Pandemie besonders anfällig für Erpressungen

Die Pandemie macht Gesundheitseinrichtungen zu einem lohnenden Ziel von Cyberkriminellen. Entsprechend bietet der Bund Unterstützung an – doch nicht alle nehmen sie an. Die Hirslanden-Gruppe wurde Opfer eines Angriffs.

Lukas Mäder
25.11.2020, 05.30 Uhr

Hören Merken Drucken Teilen

Die Angreifer sassen im Zentrum der IT-Infrastruktur: Die Hirslanden-Gruppe wurde im Sommer Opfer von Cyberkriminellen, kam jedoch mit einem verhältnismässig geringen Schaden davon.

Challenges auf verschiedenen Ebenen

Hersteller

- Individueller Einsatz der Komponenten bei Kunden
- Programme für die Erkennung von Schwachstellen
- Planung für die Beseitigung von Schwachstellen
- Kommunikation und Support mit Kunden
- Einsatzdauer der Komponenten

Betreiber

- Verlust des Betriebssupports
- Expertenwissen für Updates notwendig
- Keine geplanten Wartungsfenster
- Hohe Kosten für “kleine” Updates
- Risiko nicht tragbar

Lösungen

Hersteller

- Secure by Design
- Rechtliche Vorgaben
- “Grosse” Hersteller haben Produkt-Sicherheits-Strategien
- Allianzen bilden
- Zertifizieren

Betreiber

- Einkaufsprozesse
- Experten als Partner
- Asset Management
- Betriebssicherheit und Kontrolle

POLICY AND LEGISLATION | Publication 15 September 2022

Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

OT vs. IT

- Betriebszeiten 10-50 Jahre
- Kämpft mit Security Challenges, welche noch nicht existieren
- Es fehlt an Cyber Security Experten
- Es kann nicht gepatched werden
- Kommunikation mehrheitlich im Klartext
- Fokus auf funktionale Ziele
- IT bezogene Security Mechanismen können häufig nicht eingesetzt werden, wegen Trennung der Verantwortung und Designs sowie Mix aus Technologie

- Betriebszeit 1-5 Jahre
- Komponenten können schneller getauscht werden
- Es fehlt an Cyber Security Experten
- Unsichere Protokolle wurden weitestgehend eliminiert
- Hersteller nehmen Ihre Verantwortung grösstenteils wahr
- Anerkannte Hardening und Monitoring Techniken sind etabliert und verfügbar

AIC

- Verfügbarkeit, Vertraulichkeit, Integrität
- Das heisst: Dem Nutzer / Prozess Informationen präsentieren, wo immer dies möglich ist, und sich danach um die Korrektheit oder Vertraulichkeit zu kümmern

CIA

- Vertraulichkeit, Integrität, Verfügbarkeit
- Das heisst: Informationen müssen sicher und korrekt sein, bevor sie einem Benutzer zugänglich gemacht werden

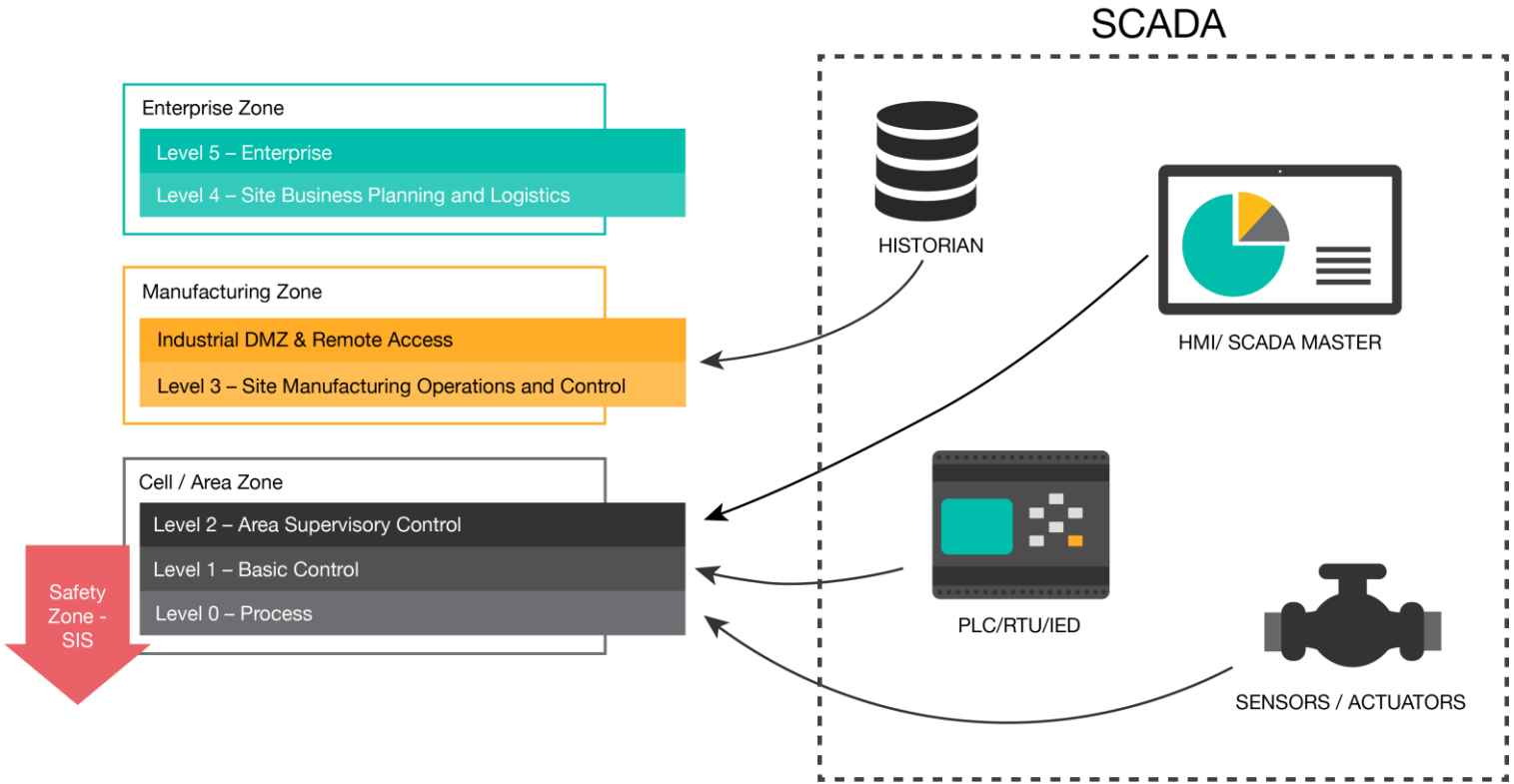
Massnahmen

- Asset Management !!!
  - Assets
  - Kommunikation
  - Protokolle
- Prozesse
  - Desaster Recovery and Planning
- Struktur
  - Mikrosegmentierung
  - Netzdesign
  - Standards (IEC62443 / Purdue)
- Remote Access
- Verschlüsselte Kommunikation
- Security Monitoring auf verdächtiges Verhalten in der Kommunikation
- Security Monitoring auf Betriebssystem Ebene

OT Asset Management

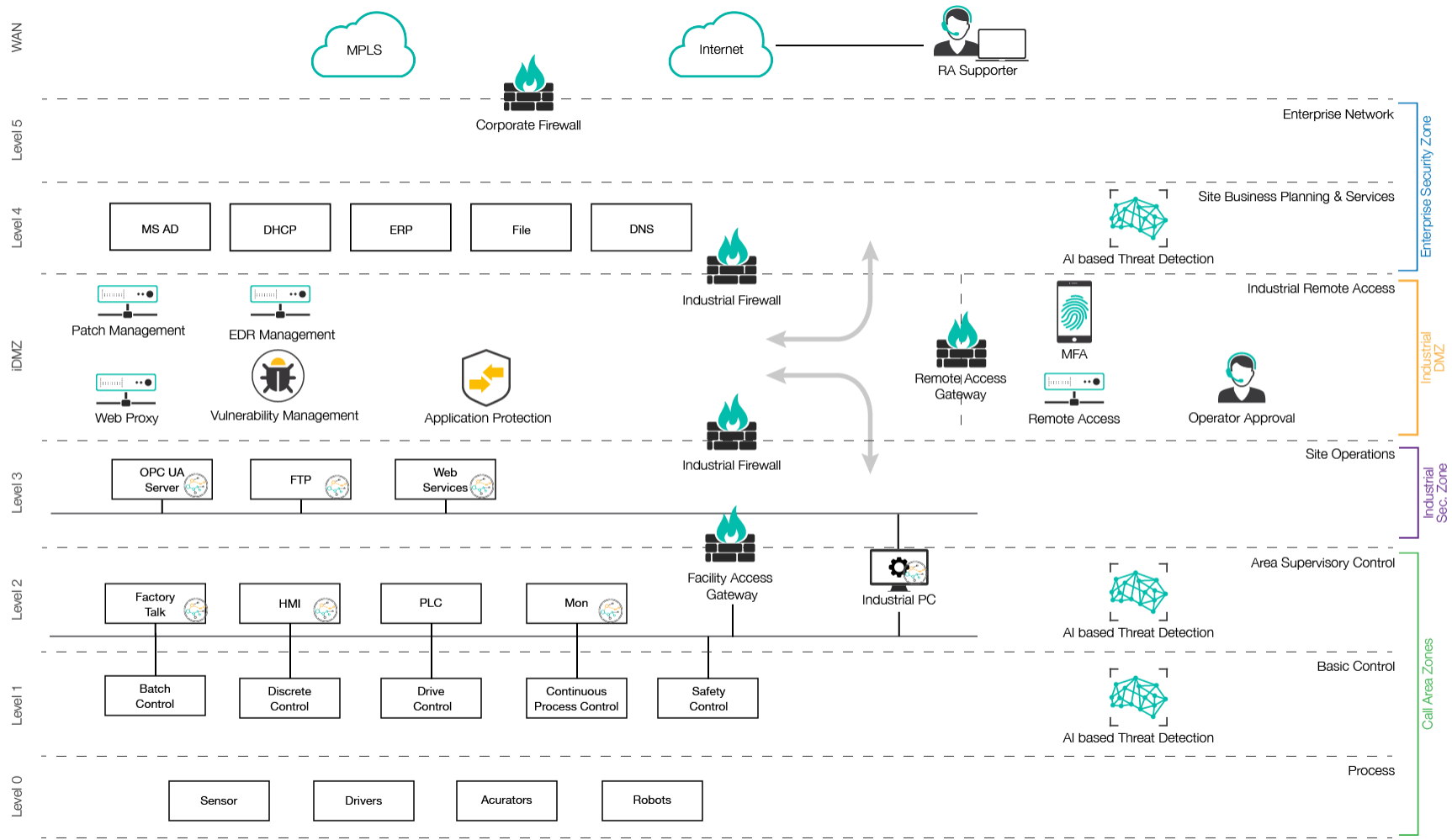
- Man muss kennen, was man schützen möchte > OT Asset Inventar
- Direkte OT Devices, Netzwerk, VMs und Serverkomponenten (Level 0-3)
- Organisation (Prozess Owner, Verantwortung über Asset über Lauzeit)
- Prozesse (Anschaffung, Inbetriebnahme, Changes, Decom)
- Inventar (Automatisierte Erfassung, keine Aktive Messung, Schutzbedarf analysieren)

OT Security Model

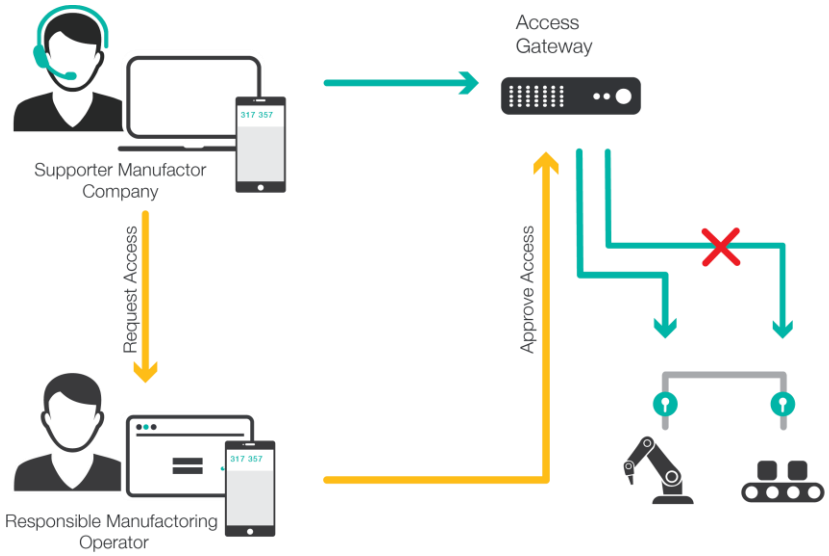


OT Security Framework (Purdue / IEC62443)

- PERA (Purdue Enterprise Reference Architecture) Model entwickelt von Rockwell und Cisco
- Entwicklung von Air-Gaped Produktionsanlagen zu verbundenen systems vom Sensor bis in die Cloud
- Security Model Architectur für verbundene und sichere Operational Technology Systeme
- Alle involvierten Komponenten werden in 5 Security Zonen unterteilt:
  - Enterprise Zone - Level 5: Enterprise
  - Enterprise Zone - Level 4: Site Business Planning and Logistics
  - Manufacturing Zone - Level 3: Site Manufacturing Operations and Control
  - Cell/Area Zone - Level 2: Area Supervisory Control
  - Cell/Area Zone - Level 1: Basic Control
  - Cell/Area Zone - Level 0: Process
- Das Model ist weltweit akzeptiert und wird von kleinen bis zu globalen Unternehmen angewendet

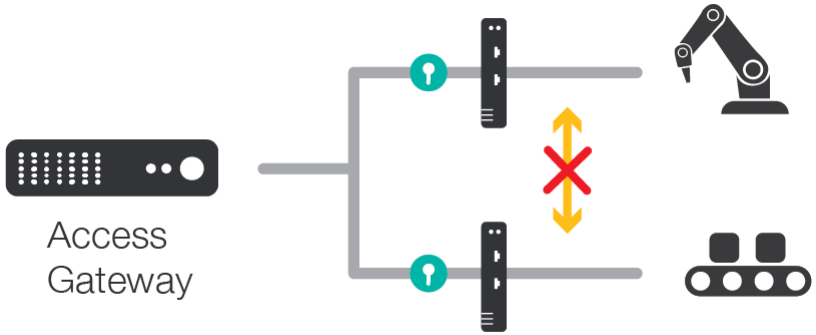

WAN
MPLS
Internet
RA Supporter
Corporate Firewall
Level 5
Enterprise Network
Enterprise Security Zone
Level 4
MS AD
DHCP
ERP
File
DNS
Site Business Planning & Services
AI based Threat Detection
Industrial Firewall
iDMZ
Patch Management
EDR Management
Industrial Remote Access
MFA
Remote Access Gateway
Vulnerability Management
Application Protection
Web Proxy
Remote Access
Operator Approval
Industrial DMZ
Industrial Firewall
Level 3
OPC UA Server
FTP
Web Services
Site Operations
Industrial Sec. Zone
Facility Access Gateway
Industrial PC
Level 2
Factory Talk
HMI
PLC
Mon
Area Supervisory Control
AI based Threat Detection
Level 1
Batch Control
Discrete Control
Drive Control
Continuous Process Control
Safety Control
Basic Control
AI based Threat Detection
Call Area Zones
Level 0
Sensor
Drivers
Acurators
Robots
Process

Secure Remote Access



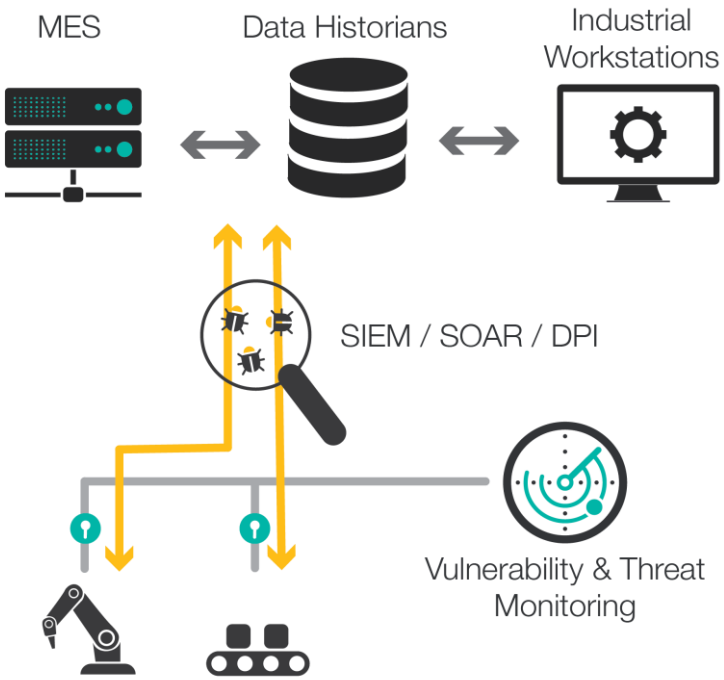
- Zeitlich limitierter Remote Access
- Einfach zu Nutzen für den Supporter und den Operator
- Direkter Zugang auf die Anlage mit den Entwicklungsumgebungen (z.B. Simatic)
- Freigabe des Zugang ohne IT Mitarbeiter
- Granularer Remote Acces nur auf die freigegebe Anlage
- Starke Authentifizierung für alle Teilnehmer
- Self Service Token Verwaltung

Protect from Cyber Threats



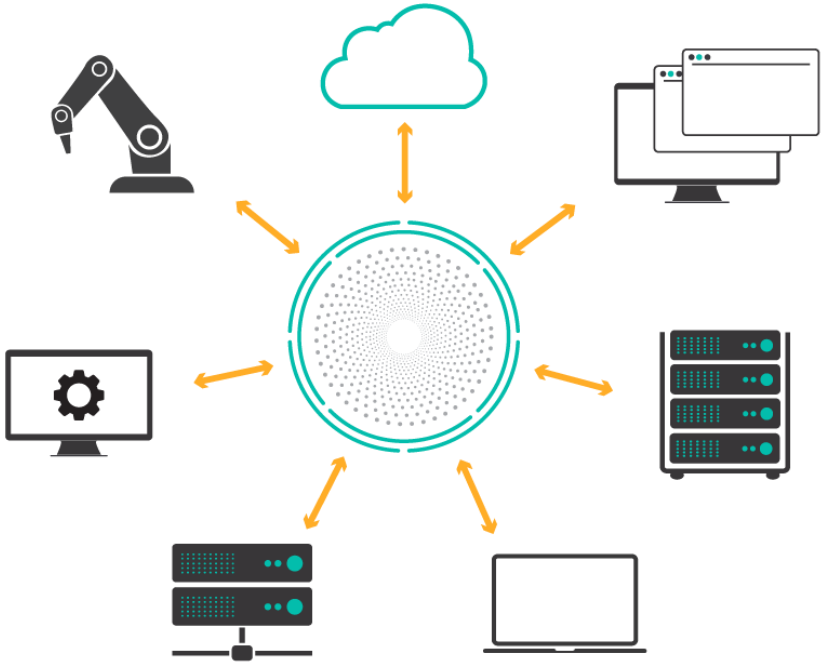
- Schützt vor Maschine zu Maschine Infektionen
- Limitiert die Exposure von Schwachstellen und ungeschützten Netzwerkprotokollen
- Eliminiert komplexe Netzwerk Designs
- Der Datenfluss und Sicherheits Policies werden rein Softwarebasiert gesteuert und zentral verwaltet
- Daten Verschlüsselung – Protokoll unabhängig
- Immer up-to-date und einfach auszurollen (ztd)
- Verbindet Produkttionsanlagen On-Campus und Off-Campus
- Autonome oder Manuelle Isolation von Zellen

Granulare Kommunikation und Inspektion



- Erlaubt nur erforderliche Kommunikation
- Granulare Kontrollen auf Protokoll und Befehlsebene
- Inspiziert Protokolle und Sub-Protokolle wie S7, S7+, IEC 60870, IEC 61850, DNP3 or Modbus
- Erkennt und raportiert Schwachstellen
- Aufzeichung und Visualisierung des Datenverkehr und Verhalten der Security-Kontrollen und Benutzer
- Simulierte Angriffspfad-Erkennung

Deep Visibility auf OS Ebene

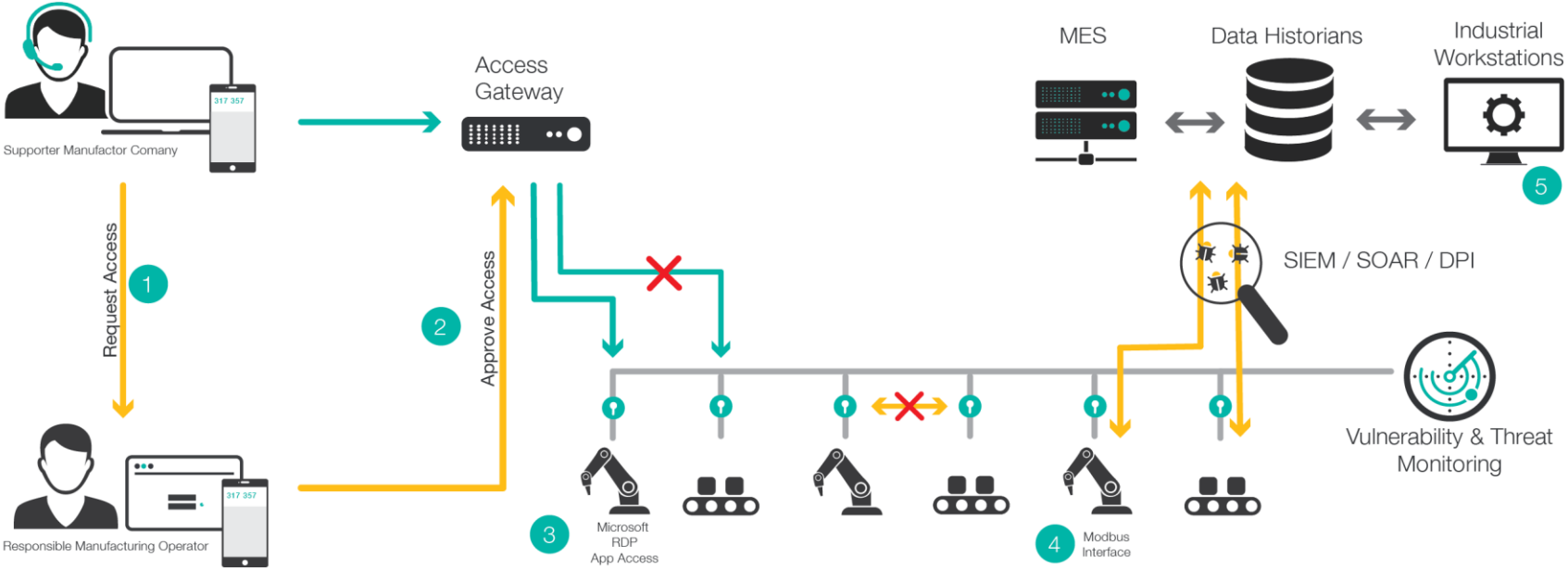


- Angriffe bleiben oft unentdeckt
- Zusätzlich zur traditionellen Erkennung
- Cyber-Attacken auf OT nehmen zu
- Die AI Agiert lokal und mit Unterstützung von Data-Lakes
- Verhaltensanalyse über Nodes hinweg
- 80% aller erfolgreichen Breaches basieren auf neuen oder unbekannten Zero-Day Exploits
- Manuelle Drehbücher verschlechtern die Reaktionszeit

Welche Anforderungen ergeben sich beim Einsatz in OT?

- Optionales Onpremise Management für Air-Gaped Umgebungen
- Unterstützung für eine grosse Anzahl von Legacy Betriessystemen wie Windows XP und Windows 7
- Granulare Möglichkeiten, zwischen Detect und Respond pro Funktion zu unterscheiden
- Trainings und Lernphasen für eine Nahtlose Integration
- Applikationen und Funktionen auf Endgeräten sind meist unbekannt und nicht verwaltet – Massgebliche Unterstützung beim Asset Management

Big Picture


Supporter Manufactor Comany
317 357
Request Access
1
Responsible Manufacturing Operator
317 357
Access Gateway
2
Approve Access
3
Microsoft RDP App Access
4
Modbus Interface
MES
Data Historians
Industrial Workstations
5
SIEM / SOAR / DPI
Vulnerability & Threat Monitoring

Summary

Welche Rückschlüsse können wir nun ziehen?

- Industrieanlagen sind ein lohnenswertes- und häuffig einfaches Ziel von Angreifern
- Das Risiko eines Cyber Security Vorfalls auf OT muss in der Gesammtrisiko-Bewertung zur Verfügbarkeit für die Produktion berücksichtigt werden
- Software Defined OT LAN, Mikrosegmenmtierung und Datenverschlüsselung erlauben schnelle (aber auch sichere) Integrationen von OT in die Unternehmensinfrastruktur
- Security Monitoring auf OS und Netzwerk Ebene unterstützen beim Troubleshooting und einer schnelleren Reaktion
- Sicherer Remote Access ermöglicht Wartung und Predictive Analysis auch zu Zeiten Pandemie

Danke

SECURITY SERVICES AG
CLUE

Neuhofstrasse 5A, 6340 Baar
+41 44 667 77 66
info@clue.ch