SPIE

X-SPIErience Day 2020

DIGITALE SOUVERÄNITÄT

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
DIGITALE SOUVERÄNITÄT

SPIE

OT-Sicherheit ohne Betriebsunterbruch: Cybervisibilität gewinnen und Risiken minimieren

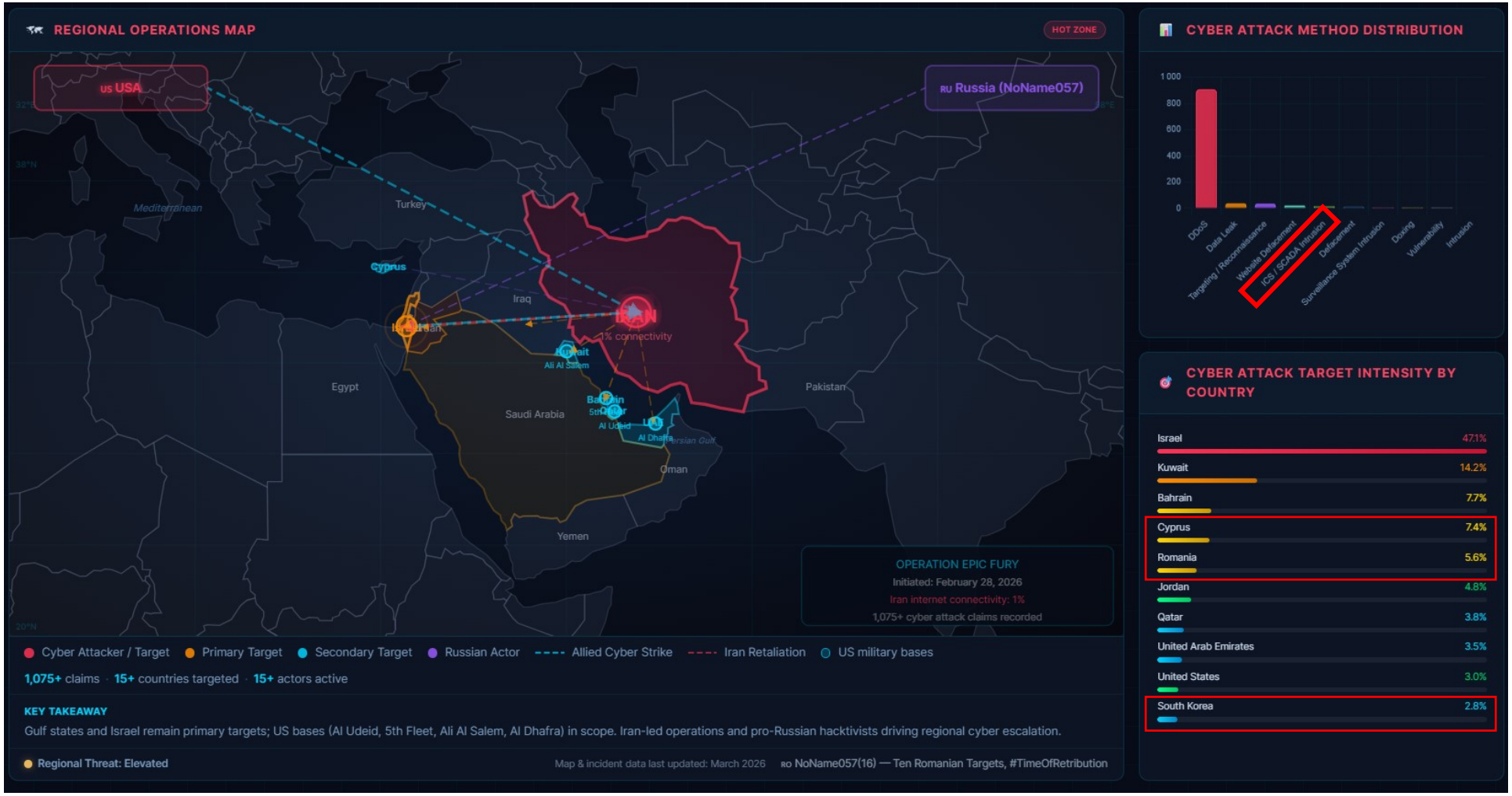
MARTIN FISCHER

Network Engineer
SPIE ICS

HUBERT RÉMOND

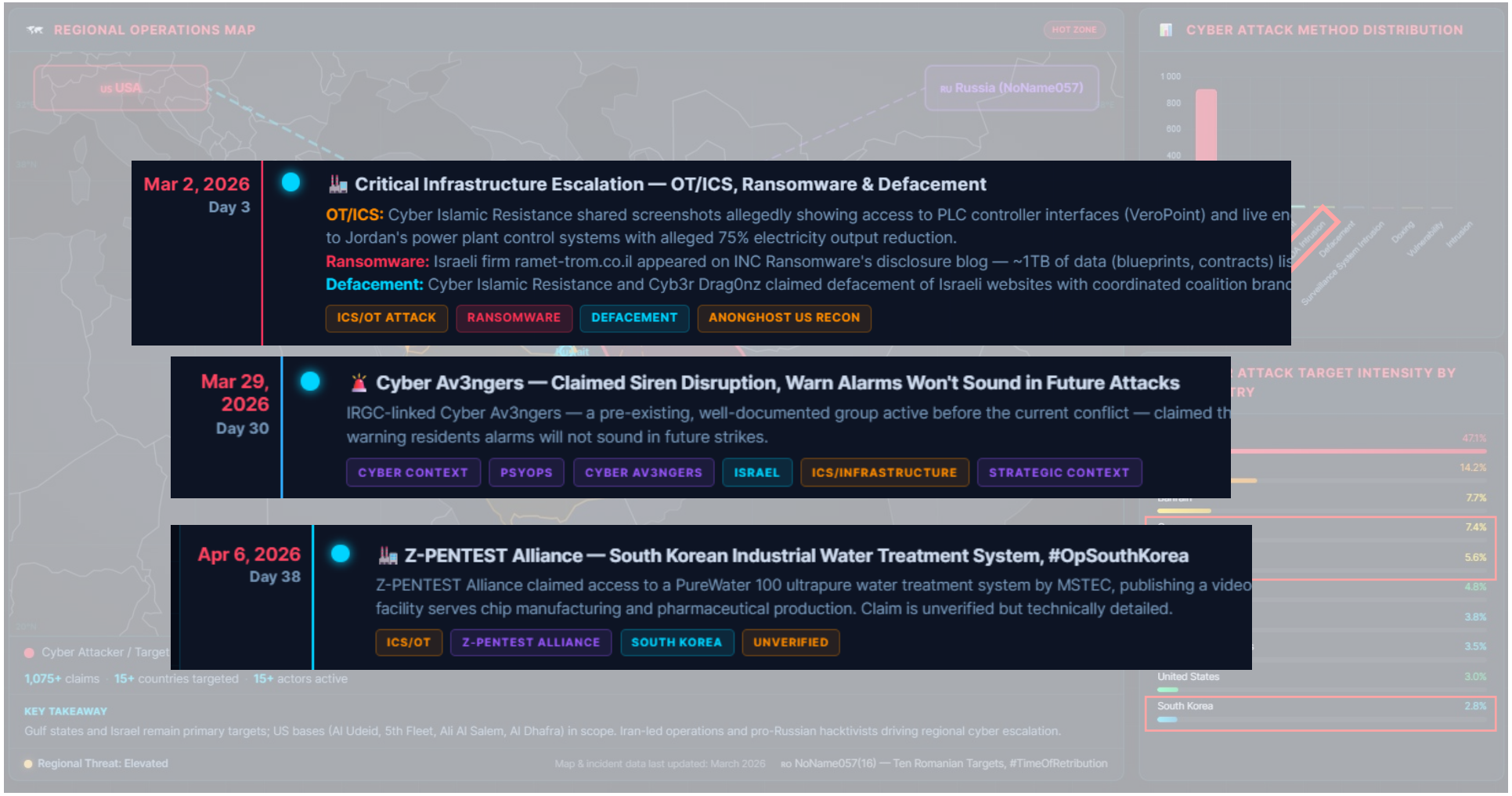
Team Leader Solution
Network Security
SPIE ICS

Aktuelle ICS/OT-Bedrohungslage



Source: Iran–Israel/US Cyber War 2026

Aktuelle ICS/OT-Bedrohungslage



Source: Iran–Israel/US Cyber War 2026

Bedrohungslage in der Schweiz

SWI swissinfo.ch The Swiss voice in the world since 1935

GEOPOLITIK DEMOKRATIE WISSENSCHAFT GESELLSCHAFT WIRTSCHAFT SWISS ABROAD

325 Angriffe aus dem Netz auf kritische Infrastrukturen gemeldet

325 Meldungen zu Angriffen auf kritische Infrastrukturen hat der Bund im vergangenen Jahr erhalten. Seit 1. April 2025 müssen Betreiberinnen und Betreiber von kritischen Infrastrukturen Cyberangriffe von Gesetzes wegen melden, innerhalb von 24 Stunden.

30. März 2026 - 10:40 1 Minute

Bundesverwaltung › Departement: VBS › BACS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Cybersicherheit BACS

Besserer Schutz der kritischen Infrastrukturen in der Schweiz

18.02.2026 - Der Bundesrat will kritische Infrastrukturen, die für Bevölkerung und Wirtschaft der Schweiz essenziell sind, besser gegen Ausfälle aller Art schützen. Auch die wichtigsten elektronischen Daten von Bund, Kantonen und kritischen Infrastrukturen sollen einen besseren Schutz gegen Cyberangriffe und Manipulation erhalten. Deshalb hat der Bundesrat an seiner Sitzung vom 18. Februar 2026 entschieden, in Umsetzung zweier überwiesener Motionen die Arbeiten für entsprechende Gesetzesentwürfe voranzutreiben, um die Resilienz und die Datensicherheit kritischer Infrastrukturen zu verbessern.

Die Motion 23.3001 «Zeitgemässe Rechtsgrundlagen für den Schutz kritischer Infrastrukturen» der Sicherheitspolitischen Kommission des Ständerates (SiK-S) fordert eine Anpassung von Rechtsgrundlagen, damit es dem Bund möglich wird, verbindliche Vorgaben für die Ausfallsicherheit und Störungsbehebung kritischer Infrastrukturen zu erlassen und so die Resilienz (Widerstandsfähigkeit) zu verbessern. In einigen Bereichen, etwa bei der Stromversorgung, sind solche bereits heute vorhanden, in vielen anderen Bereichen hingegen kaum.

Eine zweite Motion der SiK-S (23.3002), «Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz», verlangt eine Rechtsgrundlage für den Erlass von Vorgaben an Bund und Kantone sowie die Betreiberinnen kritischer Infrastrukturen, wie sicherheitsrelevante Daten besser geschützt werden können.

Sicherung der OT-Infrastruktur | Lab Overview

Vorstellung
Setup

SCENARIO 1

ohne
Security

SCENARIO 2

Segmentation
PAM & OT
Advanced
Threat
Protection

SCENARIO 3

Honeypot,
Advanced
Detection &
Response

Sicherung der OT-Infrastruktur | Lab Overview

The Setup

- Ein produktives Datacenter wird mit einer Klimaanlage betrieben
- Die Temperatur des Datacenter wird mit einer Siemens PLC überwacht
- Grünes Licht =  **Temperatur ok**
- Wenn die Temperatur über 30°C steigt wird ein Alarm generiert  **Alarm !**
- Die Siemens PLC verwendet das BACnet Protocol
  - weit verbreitet in der Gebäudeautomation
  - Klartext-Kommunikation
  - keine Access Control on BacNet
  - keine Kontrolle der Passwortstärke

Scenario 1 | Wie sollte man OT nicht betreiben

Die Plattform:

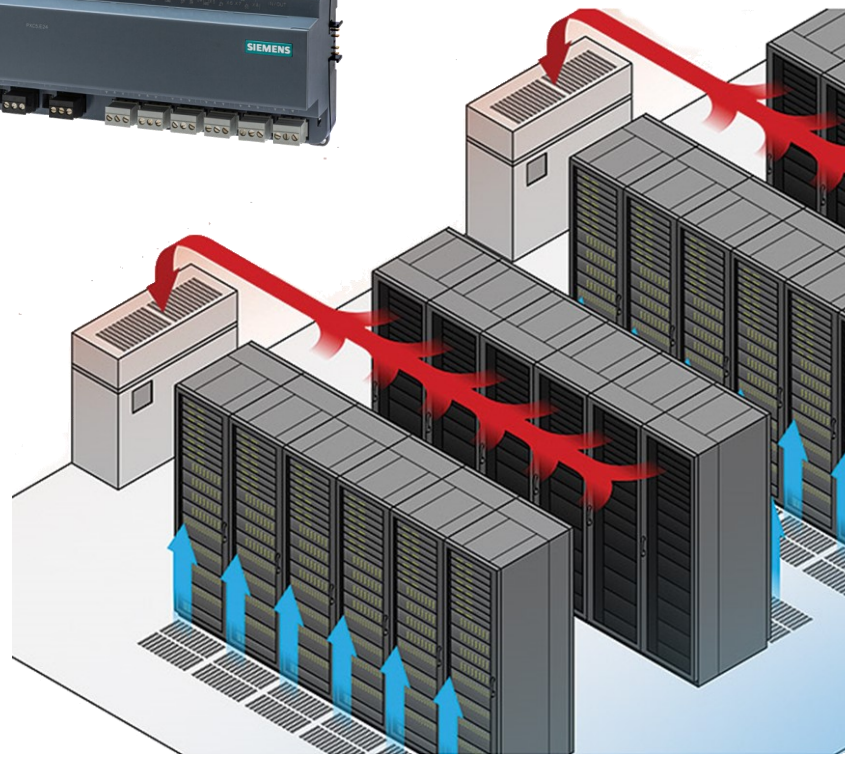
Appliances:

- Siemens PXC5.E24 PLC
- Moxa unmanaged switch
- No firewall = 1 flat network für IT und OT

Software:

- Inneasoft BACnet Explorer keine Access Control und keine Kontrolle über die Passwortkomplexität (Password enforcement)

Scenario 1 | Wie sollte man OT nicht betreiben



Scenario:

- Standard-Intervention an einem Steuergerät (PLC)
- Techniker verwendet BACnet Software um den Temperatur-Alarm von 30°C auf 35°C zu ändern
- Der Techniker macht danach einen Systemtest

Setup:

- PLC & PC des Technikers werden durch einen unmanaged Moxa Switch verbunden
- Es wird nur ein Subnetz verwendet – keine Segmentation, keine Security, keine Access Control im gleichen Layer 2-Netzwerk

Scenario 1 | Wie sollte man OT nicht betreiben

INNEA BACnet EXPLORER

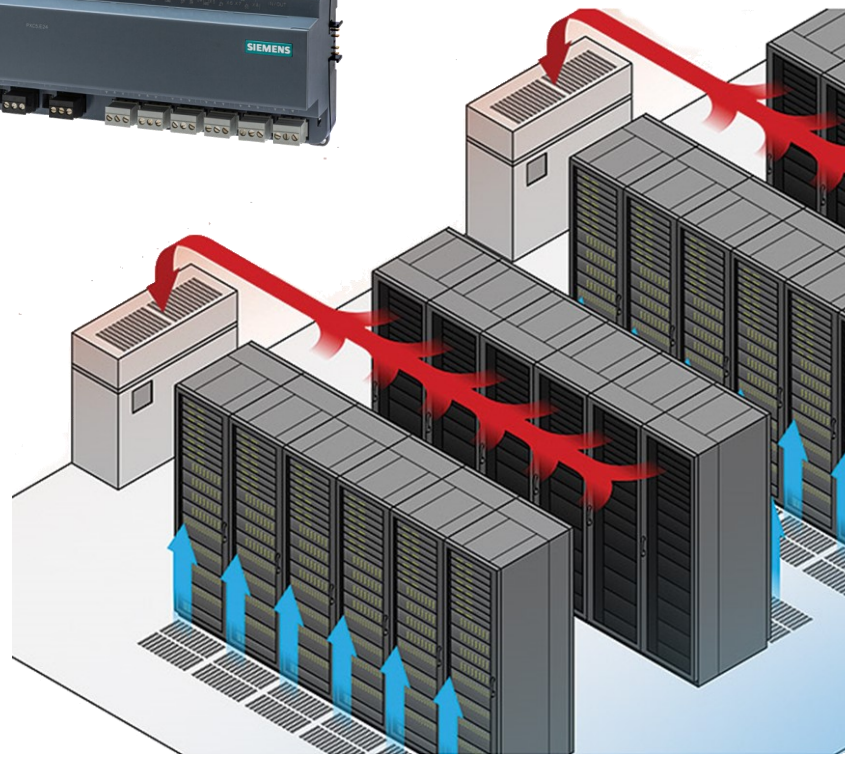
BACnet

Scenario:

- Das Ziel des Angreifers ist es, einen Ausfall des ganzen Datencenters zu erwirken
- Dem Angreifer ist es vorgängig gelungen über einen kompromitieren Hosts ins Netz zu kommen
- Der Angreifer verwendet die gleiche BACnet Software um den Temperatur-Alarm und den Trigger für die Klimaanlage auf 999°C zu stellen

Setup:

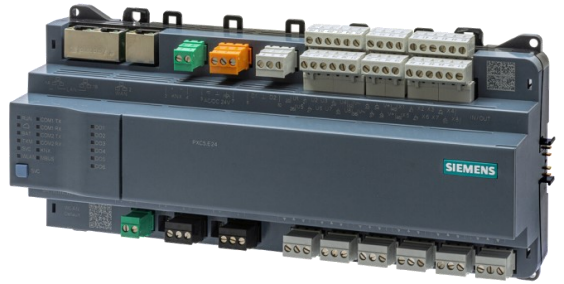
- gleiches, flaches Network



Scenario 2
Segmentation, PAM & Advanced OT Security

Appliances:

- Siemens PXC5.E24 PLC



- FortiGate 50G (Rugged) Next-Gen Firewall
- FortiPAM

NEW

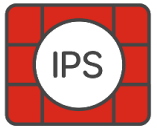
NEW

FortiPAM

Software:

- Inneasoft BACnet Explorer
- Fortinet OT IPS/App Ctrl Signatures package

Scenario 2 | Segmentation & Advanced OT Security



FortiPAM

PAM:
Privileged Access
Mgmt

BACnet

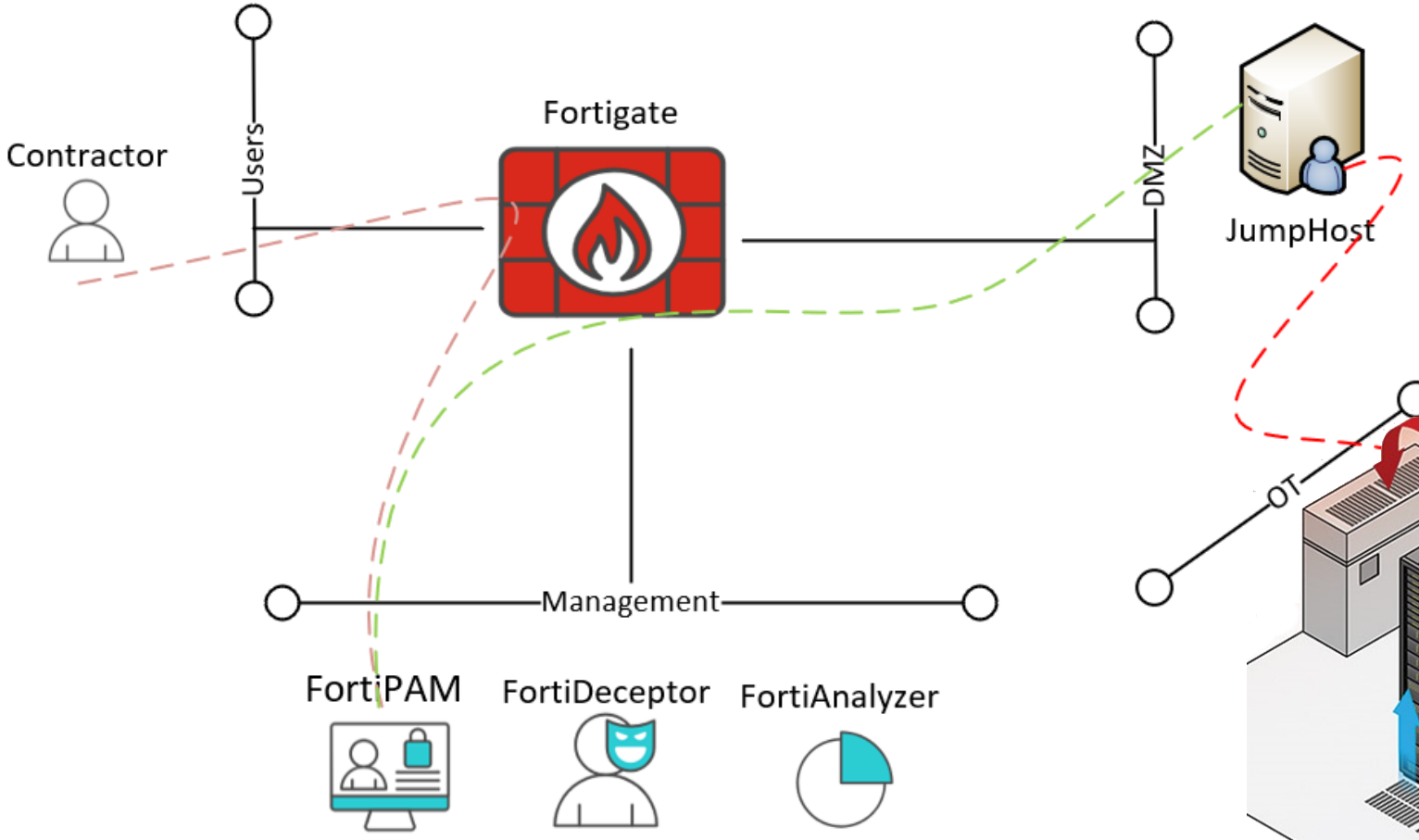
Scenario:

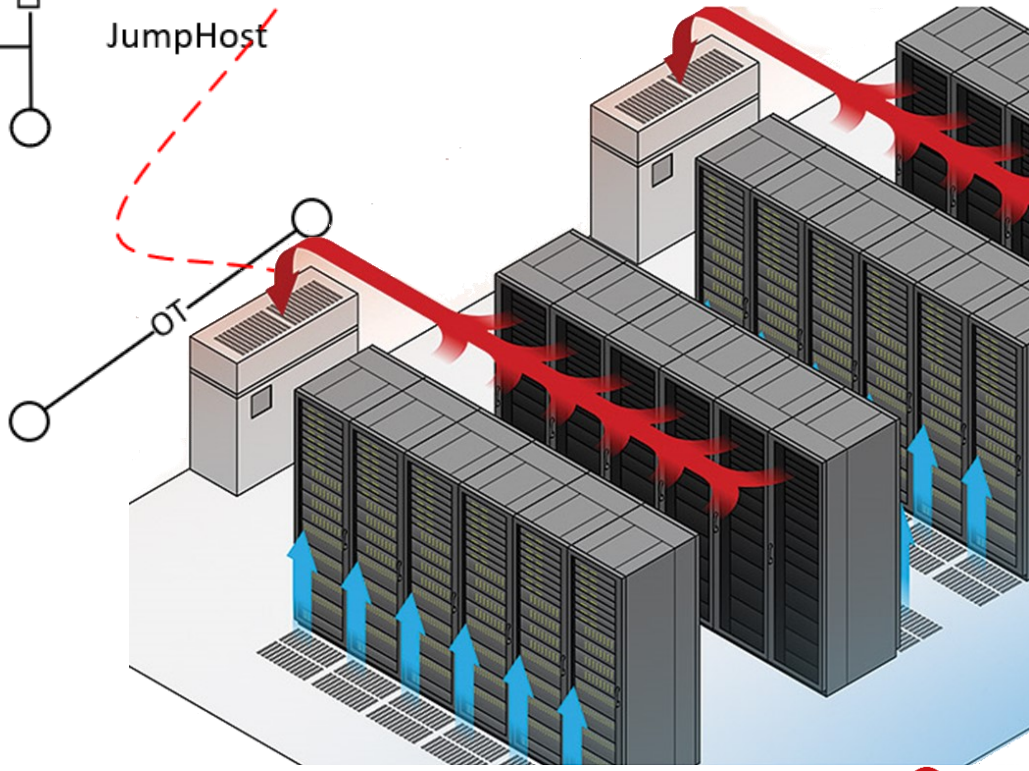
- gleiches, flaches Network

Setup:

- Die Segmentierung ist nun mit einem dedizierten VLAN für die PLC umgesetzt
- Advanced security mit den Fortinet OT IPS Signatures
- Die Attacke wird durch die Firewall verhindert, Werte über 60° für den Alarm werden durch die Firewall verhindert!
- Contractor Access kann durch FortiPAM kontrolliert werden

Scenario 2 | Segmentation & Advanced OT Security





Scenario 3 | Advanced Detection & Response

Appliances:

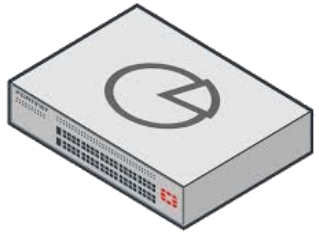
- Siemens PXC5.E24 PLC
- Decoy PLC
- FortiGate 50G (rugged) Next-Gen Firewall
- FortiPAM
- FortiAnalyzer (automated SOC) NEW
- FortiDeceptor (honeypot)

Software:

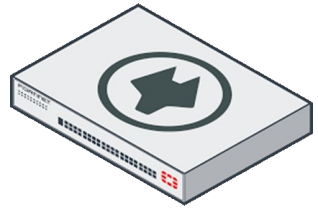
- Inneasoft BACnet Explorer
- Fortinet Security Fabric NEW

FortiPAM

NEW

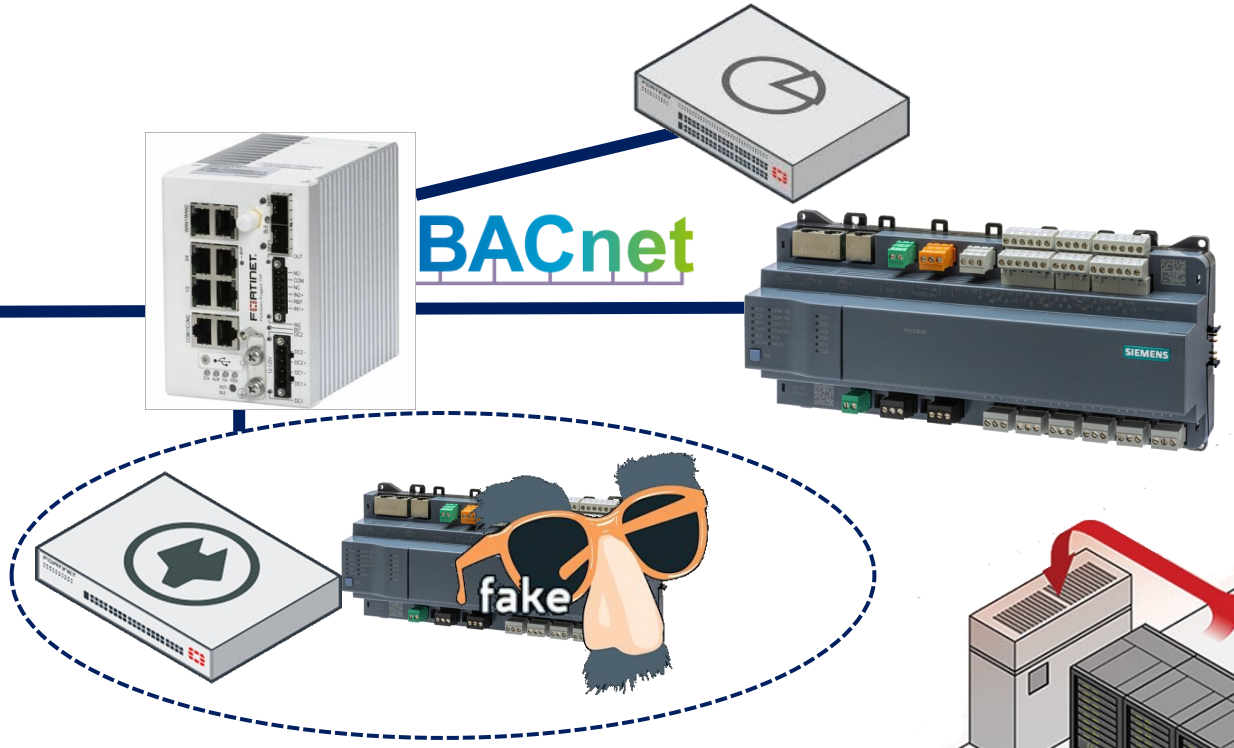


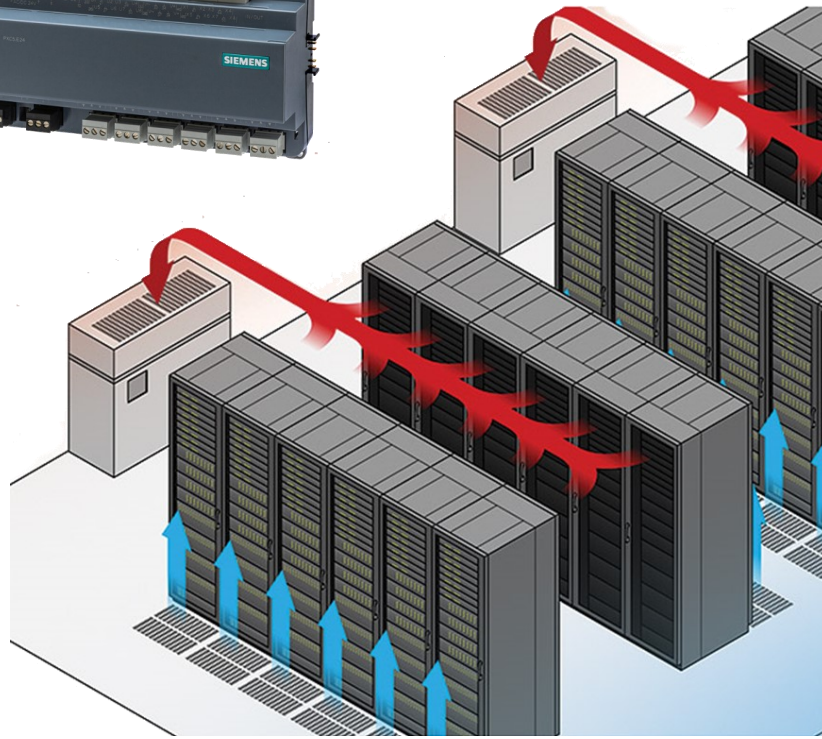
FortiAnalyzer VM



FortiDeceptor VM

Scenario 3 | Advanced Detection & Response





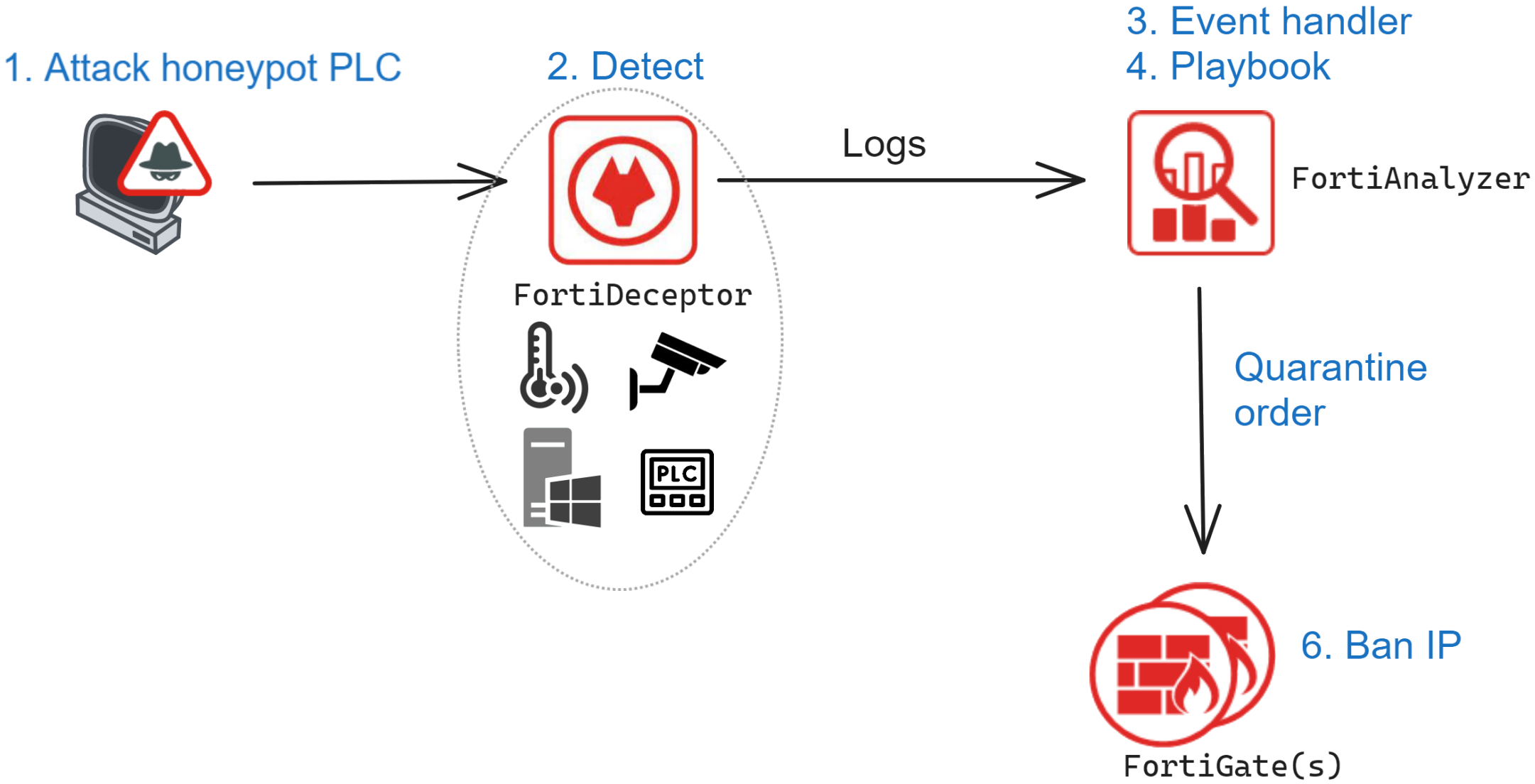
Scenario:

- Der Bösewicht kommt zurück
- ... er weiss die IP der PLC nicht
- ... er scannt das Netz und findet eine PLC zum angreifen ...
- ... er versucht sich mit der PLC zu verbinden

Setup:

- Auf einem FortiDeceptor findet der Angreifer eine Fake-/Decoy-PLC, diese ist im selben Netz wie die echte PLC
- Können wir den Angreifer sehen und was können wir etwas dagegen unternehmen?

Scenario 3 | Advanced Detection & Response



Aspekte zur Sicherung der OT-Infrastruktur

Lab Conclusion

Segmentierung (Makro und Mikro) und **Zugangskontrolle** sind Schlüssel!

Verwenden Sie Standards wie das **Purdue-Modell**, um Ihre OT-Architektur zu erstellen

Das dedizierte **OT-Signaturpaket** bietet fortschrittlichen Bedrohungsschutz

Firewall und **Managed Switch** sind der Kern einer sicheren Implementation

Der **Logs Collector** bietet fortschrittliche Echtzeit-Alarmierung und Forensik

Honeypots schützt gegen seitliche Bewegungen und kann Angreifer erkennen und verlangsamen

Automated Security Fabric bietet Full-Stack-Transparenz und Automatisierung, um die OT-Umgebung zu sichern

Wie startet man ein OT-Cybersecurity-Projekt?

SCHRITT 1 Finden Sie die richtigen Ansprechpartner (IT & OT)

SCHRITT 2 Kennen Sie Ihre Umgebung

SCHRITT 3 Verwenden Sie anerkannte Sicherheitsarchitektur-Standards

SCHRITT 4 Einführung relevanter Sicherheitslösungen

Ihre Ansprechpartner bei SPIE ICS

Martin Fischer

Network Engineer

Tel. +41 79 475 80 08

Mail martin.fischer@spie.com

Hubert Rémond

Team Leader Solution Network Security

Mail info.ch@spie.com

spie.ch/secure