

**Monti
Stampa
Furrer**

•

+

**OT cyber protection beyond the myth
of the impossible**

Reflecting OT protection concepts

Helsinki, June 2021

Franco.monti@msfpartners.com



MSFPartners was created in 2016 and has an international footprint

Office Zürich and Zug



Franco Monti
Senior Partner



Dante Stampa
Senior Partner



Hermann Ineichen
Senior Advisor

Office Lausanne



Jean-Pierre Therre
Managing Partner

Office Helsinki



Aapo Cederberg
Business Dev.
Scandinavia & Baltic



Office Tel Aviv



Rami Efrati
Managing Partner

Office Dubai



Thomas Pool
Director

Knowledge that matters

- We support organizations across infrastructure sectors to create the change in their OT security that really matters to them.
- From the C-suite to the Engineers, we partner with our clients to transform their OT environment into a secure environment by building enduring OT security capabilities.
- With exceptional people we combine OT security expertise and local industry insights to help you implement your OT security ambition into reality.










Our focus is problem solving in OT





We resolve specific OT challenges for our international clients

	Our services	Characteristics
	1 Cyber Security IT and OT strategies	<ul style="list-style-type: none">• Deriving necessary cyber security blueprint from business needs• Formulating cyber security roadmaps and programs• Providing financial cyber security investment planning
	2 Maturity assessment IT and OT	<ul style="list-style-type: none">• Assessment of cyber security maturity score and resilience against attacks in both, IT and OT
	3 OT Cyber Security technology evaluation	<ul style="list-style-type: none">• Scouting for new technologies and cyber security methodologies• Formulation of RFP specifications• Leading entire RFP processes• Preparing OT security proof-of-concepts with selected technologies and vendors
	4 Red Team and security assessments	<ul style="list-style-type: none">• Conducting complex penetration tests, assessing cyber security weaknesses and Incident Response capabilities• Verifying robustness of VPN access to corporate resources and home-office configurations
	5 Cyber Resilience	<ul style="list-style-type: none">• Establishing OT incident response plan and runbooks• Emergency cyber response organization• Linking to cyber contingency and recovery plans (BCM)• Cyber crisis exercise (C-Level, operational Level)
	6 OT Security Blueprint	<ul style="list-style-type: none">• Establishing specific OT security blueprints as the core element in plant protection• Deriving OT security roadmap and preparing an investment plan anticipating CAPEX/OPEX
	7 OT Security Projects	<ul style="list-style-type: none">• Leading complex OT security projects from the concept to operations• Taking over delivery responsibility for large OT security initiatives



1. Why shall we protect OT?

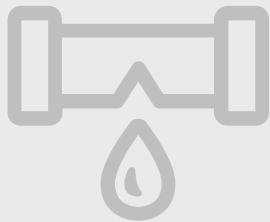


Three ways Ransomware **could** shut down a pipeline – Does this bother the Board?

1

LEAKING CREDENTIALS AND PANIC MOVES

- Even without evidence that the attack has migrated into operations, an organization might shut everything down in an abundance of caution



Colonial pipelines
(according to CISA)

2

TARGETING PHYSICAL OPERATIONS

- Attackers deliberately push the Remote Access Trojan into OT networks



Triton 2017

3

SHUT DOWN CRITICAL IT SYSTEMS IN OT

- In hindsight, these IT systems should probably have been protected as part of the OT network, not left on the Internet-exposed IT network



Manufacturing sites
shut down 2020



TECHNOLOGY AND IIOT

Cyberattack on Colonial Pipeline
Disrupts Normal Flow



Besides targeted OT attacks, operational issues could as well lead to an increased cyber security exposure

Raising internal and external issues in OT



Human Machine Interface (HMI) devices were infected with malware such as e.g. WannaCry



Vulnerable industrial control devices exposed to the internet



Third-party devices opened reserve tunnels, breaching network segmentation



Employee downloaded manufacturing plans data to their laptop



Connection of personal employee devices to the manufacturing network.



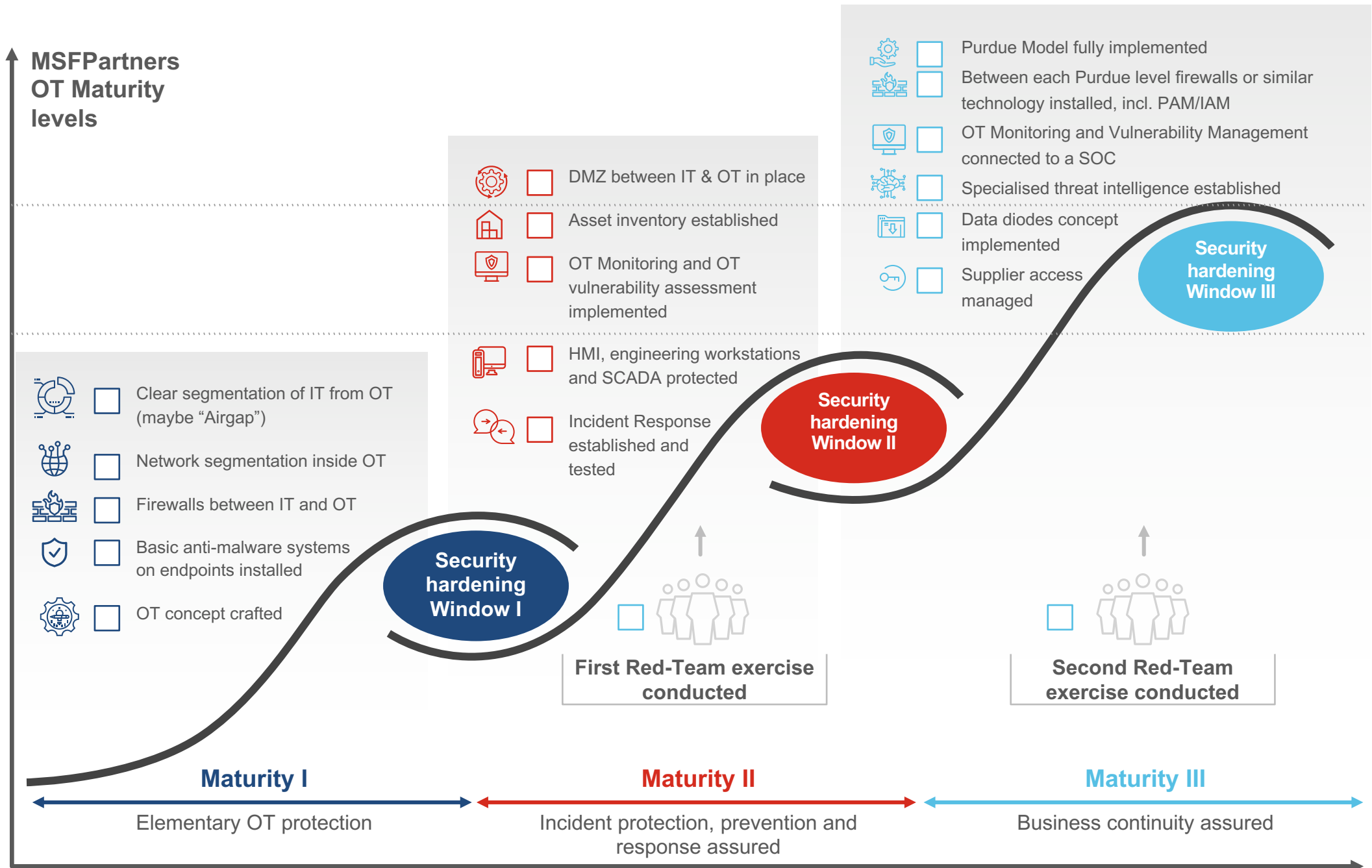
- Experience show a ratio of 1/3 internal malicious Cyber Security events vs. 2/3 internal misconfiguration based security issues
- Malicious activities are typically triggered by disgruntled employees, while misconfigurations have their origins in not following strict security rules and policies



2. How to protect OT?

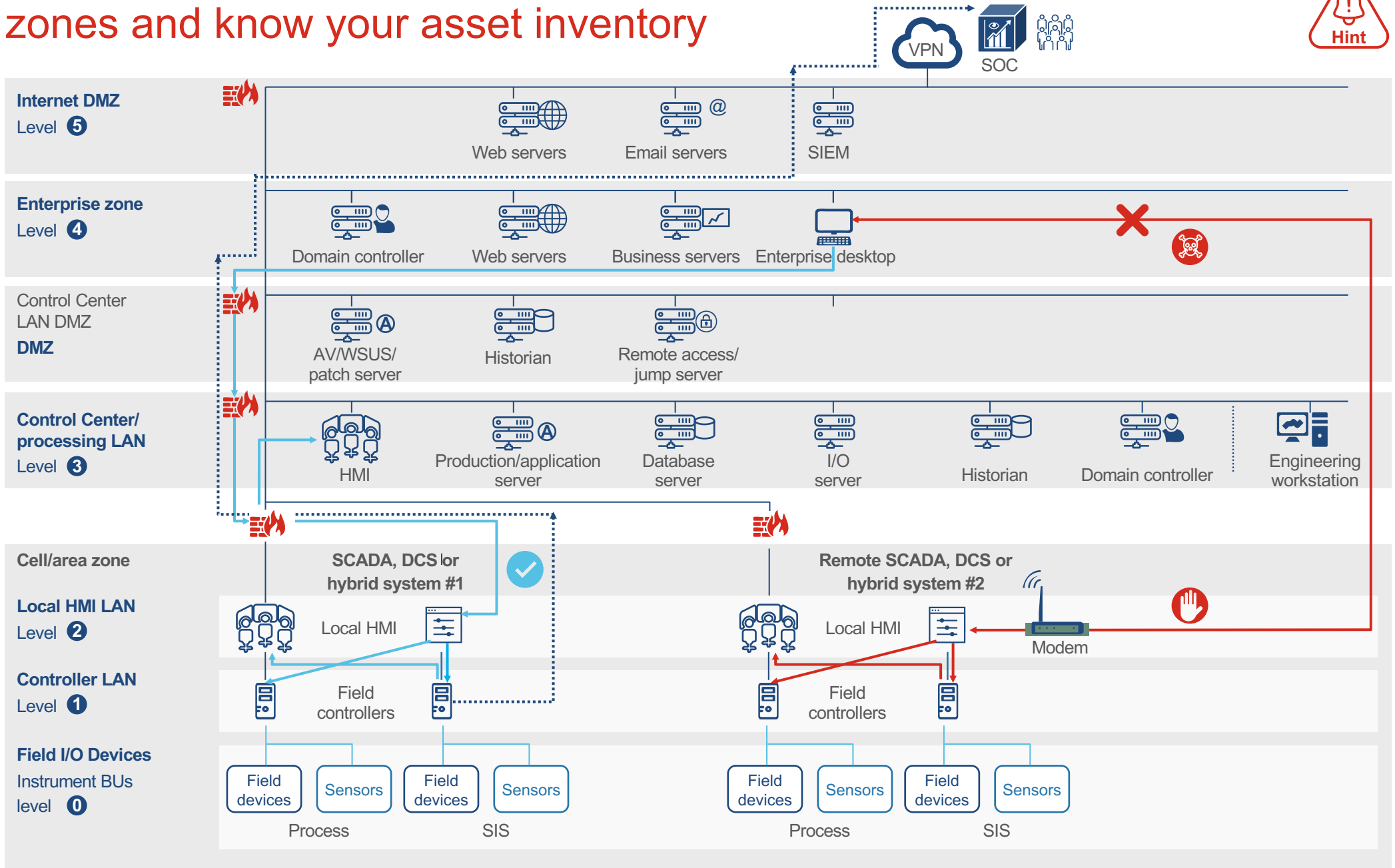


The OT maturity model helps to get transparency on the state of security





The Purdue Model prevents engineers from circumventing levels and zones and know your asset inventory

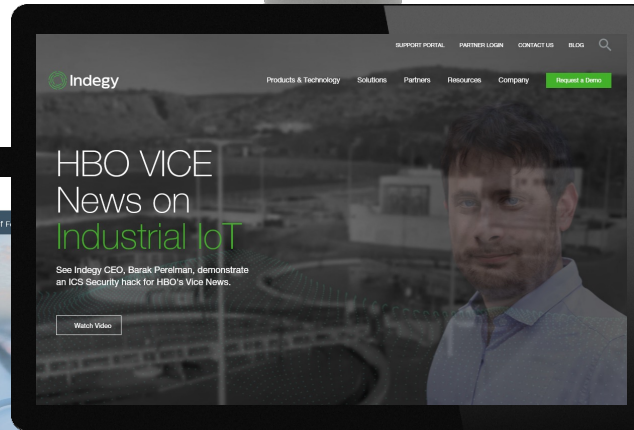
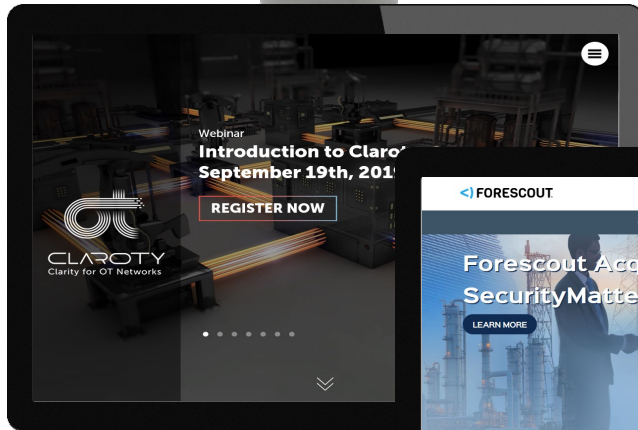


Legend: — Local Field BUs/hard wired — Vendor-specific BUs — Ethernet TCP/IP — SIS Status Only



OT Monitoring applications look all alike, but...realities are different

How you might perceive the market at the beginning



Important

- Identify the real experts – Some players position themselves as capable to monitor IT and OT seamlessly
- Identify the experience of an organisation with critical infrastructure projects
- Verify quality and experience of their OT experts



Hint

**Don't believe paper!
Run POCs**

In order to get away from marketing we invite vendors to a POC

Briefing Proof-of-Concept for Threat Monitoring and Vulnerability Management in the Grid (Operational Technology)

1. Goal of the POC

As part of the overall Cyber Program it has been decided to establish a SOC-as-a-Service protection scheme for the entire group. After having initiated to launch this service during phase 1 for IT, it has been decided to implement threat monitoring and vulnerabilities management as well in the area of Operational Technology (OT). In preparation of establishing the protection for OT, phase 2 will be launched conducting POC installations with selected suppliers of OT-protection applications and appliances. During the preparations of phase 2 and during a pre-screening of potential suppliers it has been noted, that most suppliers have a similar positioning. This lead the

- wants to observe the reliability of the offered solution in the OT environment considering following goals for the POC :
- I. Understanding the full scope and power of the solution in a real life OT environment during normal conditions
 - II. Testing the reliability of offered threat monitoring and vulnerability management
 - III. Understanding strength and weaknesses of the solution in comparison with its peer group
 - IV. Getting a first indication of the criticality of found vulnerabilities or anomalies in the OT test area at
 - V. Establishment of the OT infrastructure asset inventory to be compared with own inventory information for installed system components

to the decision testing key suppliers directly during POC installations in various areas of the OT environment.

2. Scope

The POC shall provide a silent listening, non-intrusive or passive mechanism for establishing a precise asset inventory and for conducting threat monitoring inclusively vulnerabilities assessment. It is assumed that the POC system is capable to analyze OT network traffic during listening and hence creates alerts in real-time case for pre-defined schemes of alerts will rely on the supplier's suggestion on definition of alert scheme (major, medium, minor alerts).

Alerts and other significant OT network information for malware, anomalies or dangerous configurations of certain devices shall be monitored and shown in the suppliers OT management system. All information collected from the OT network must be accessible for Logrhythm SIEM to be used in its SOC.

The POC shall run in two locations. These will be in the OT hub of the hydro plant at and in the control center of the hydro dam in . wants to run these two diverse locations to understand the impact of the solution to the grid monitoring.

1 Specific POC

- Write and share a vendor POC handbook

2 Simultaneously executed POC activities

- Install between 3-4 parallel vendor products in selected and diverse plant areas

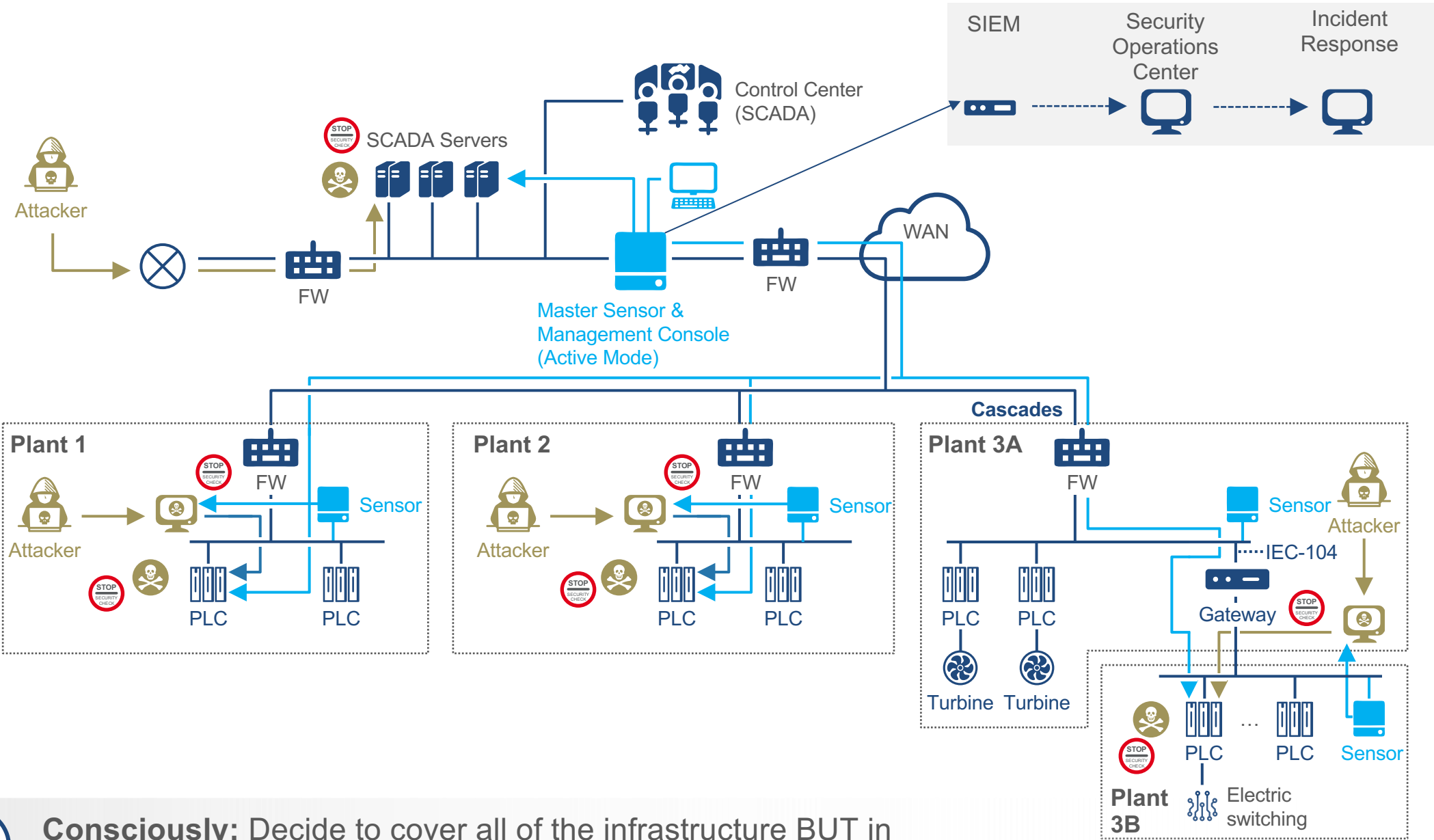
3 Debriefed POC in team

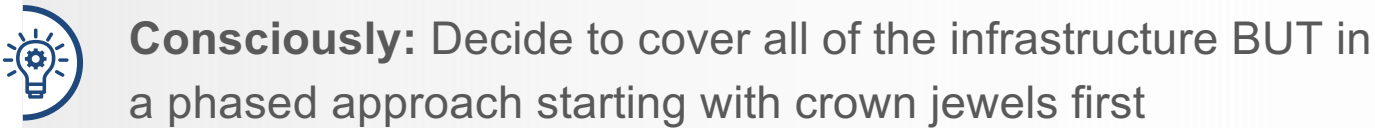
- Thoroughly discuss with each vendor effectiveness of his product in **your** environment
- Give particular emphasis on the details of the devices (PLC) detected



- We recommend to test an OT monitoring application BEFORE the RFP in the real life environment
- Observe how long the test preparation went and especially the ease of installation in YOUR own environment

Don't go for the "Emmental model" – Strive for full protection



 **Consciously:** Decide to cover all of the infrastructure BUT in a phased approach starting with crown jewels first

After the POC write a RFP integrating your Engineer's vision – The RFP document can be written in 3 weeks

3 DETAILS OF THE RFP

- 3.1 PLANNED DEPLOYMENT TIMELINE
- 3.2 TYPICAL RANGE OF POSSIBLE INCIDENTS IN THE [REDACTED]
- 3.3 TARGET APPLICATION TO BE OFFERED TO [REDACTED]
- 3.4 KEY QUESTIONS TO SUPPLIERS
 - 3.4.1 SUPPLIER COMPANY STRUCTURE
 - 3.4.2 ELIGIBILITY FOR THE PROJECT
 - 3.4.3 SECURITY, PRIVACY AND RESILIENCE
 - 3.4.4 FUNDAMENTALS OT PROTECTION
 - 3.4.5 FUNCTIONAL ASPECTS AND USER INTERFACE
 - 3.4.6 CONNECTIVITY WITH SOC AND SIEM
 - 3.4.7 INTEROPERABILITY WITH ECI MERCURY NFV SOLUTIONS
 - 3.4.8 THREAT INTELLIGENCE
 - 3.4.9 OT MONITORING AND VULNERABILITY MANAGEMENT REPORTING
 - 3.4.10 ESTABLISHMENT OF THE OT PROTECTION APPLICATION
 - 3.4.11 SUPPLIER PERSONNEL QUALIFICATIONS
 - 3.4.12 INTERNATIONAL EXCHANGE
 - 3.4.13 VARIOUS
- 3.5 ASSUMPTIONS AND EXPECTATIONS
- 3.6 PROJECT SCOPE AND SIZING

4 SUPPLIER QUALIFICATION CRITERIA

- 4.1 SUPPLIER PROPOSAL
- 4.2 REQUIREMENTS FOR THE PROPOSAL
 - 4.2.1 STRUCTURE OF THE PROPOSAL
 - 4.2.2 PROPOSAL ANALYSES
- 4.3 COST TRANSPARENCY
- 4.4 CURRENCY AND PAYMENT TERMS

5 ADMINISTRATIONAL RULES



Important

- Engineers in the OT departments should be integrated from the very beginning – no ivory tower exercises!
- Establish an OT workgroup which drives the entire process inclusively the RFP
- Don't forget to integrate future scenarios such as:
 - Integration into SIEM/SOC
 - Including endpoint detection & response for engineering workstations

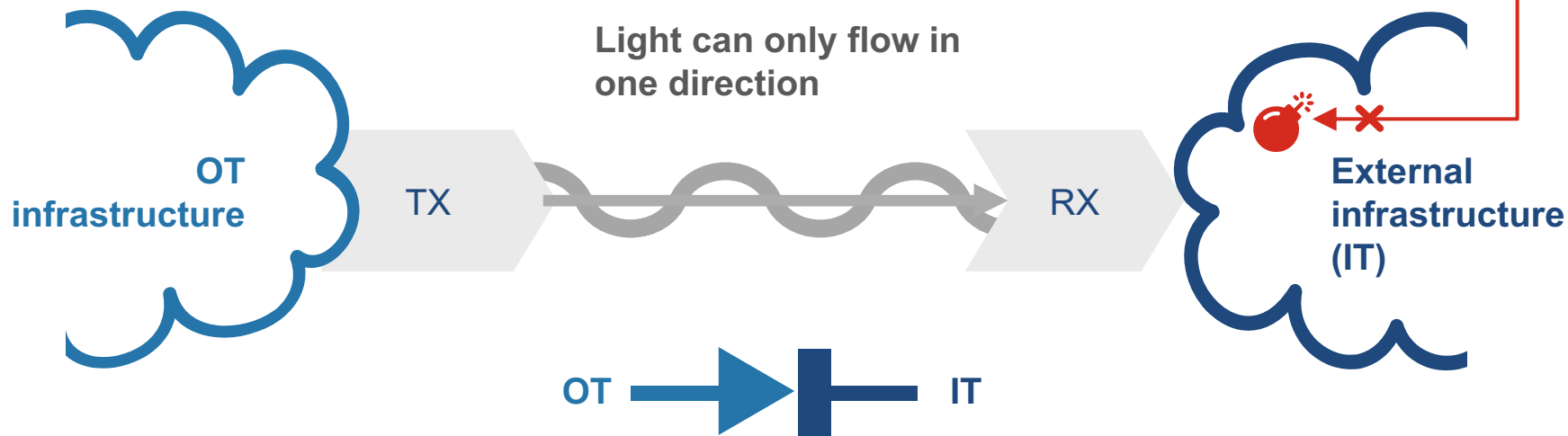


**3. One last thought on protecting OT
– Are there Quick-Wins?**



The physics of unidirectional gateways allows to transmit and to receive flows only in one direction using the optical nature of light

Unidirectional gateway fundamental idea



- No access to OT infra-structure by external actor
- Access to less critical IT infra-structure maybe authorized



Unidirectional gateways are useful technique to ensure safe encapsulation in OT

Monti
Stampa
Furrer
•

+ Key take-away:

1. Industrial infrastructure **must** be **protected**
2. **Involve** your plant engineers
3. Build your OT **security blueprint**
4. Stepwise refine and **focus** on quick-wins
5. Start building **your asset inventory** and **monitor OT**