Hoe breng je je cybersecurity naar het volgende niveau door ‘visibility’ toe te voegen aan OT-netwerken?

Ruud Sauren & John Adams

Keysight Network Apps. & Security

2020.10.28

Poll 1

Wie is er bekend wat een SPAN-poort / Mirror-poort of Reflector-port is?

- **Wel bekend**
- **Niet bekend**

Poll 2

Wie gebruikt SPAN-poorten (of welke benaming dan) voor monitoring of security?

- **Wel in gebruik**
- **Niet in gebruik**
- **Niet van toepassing / Geen idee**

The High Cost of a Cybersecurity Incident

MORE THAN JUST A BLACK EYE

Average estimated cost of cyberattack

$1.7M

“Cyberattacks on critical infrastructure and strategic industrial assets are now one of the top five global risks.”

World Economic Forum
Global Risk Report, 2018

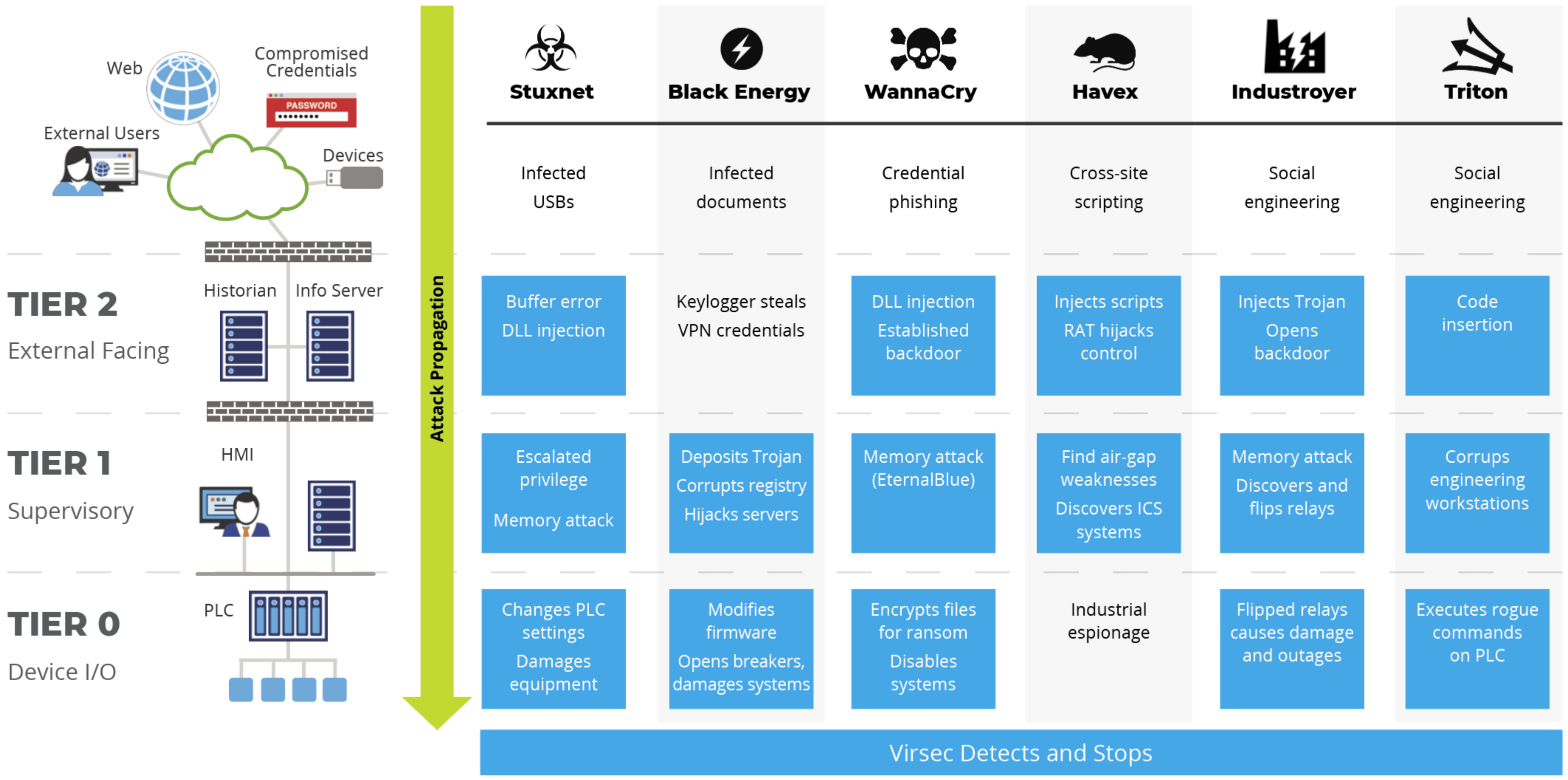
	Organization	Issue/Attack	Cost
2019	Norsk Hydro	LockerGoga Ransomware	$70m
	Duke Energy	Compliance Violation	$10m
2018	Saudi Petrochem	Triton	Unknown
	UK NHS	WannaCry	92m GBP
2017	Merck	NotPetya	$870m
	FedEx (TNT Express)	NotPetya	$400m
	Maersk	NotPetya	$300m
	Mondelēz	NotPetya	$188m
2016	Ukrenergo	Industroyer/Crashoverride	Outage
2012	Saudi Aramco	Shamoon	$1 Billion

Sources: Wired, Wall Street Journal, UK Telegraph, Threatpost

The Threat

EXAMPLES OF IIOT CYBERSECURITY ATTACKS

How Major Attacks Have Spread Through Industrial Systems

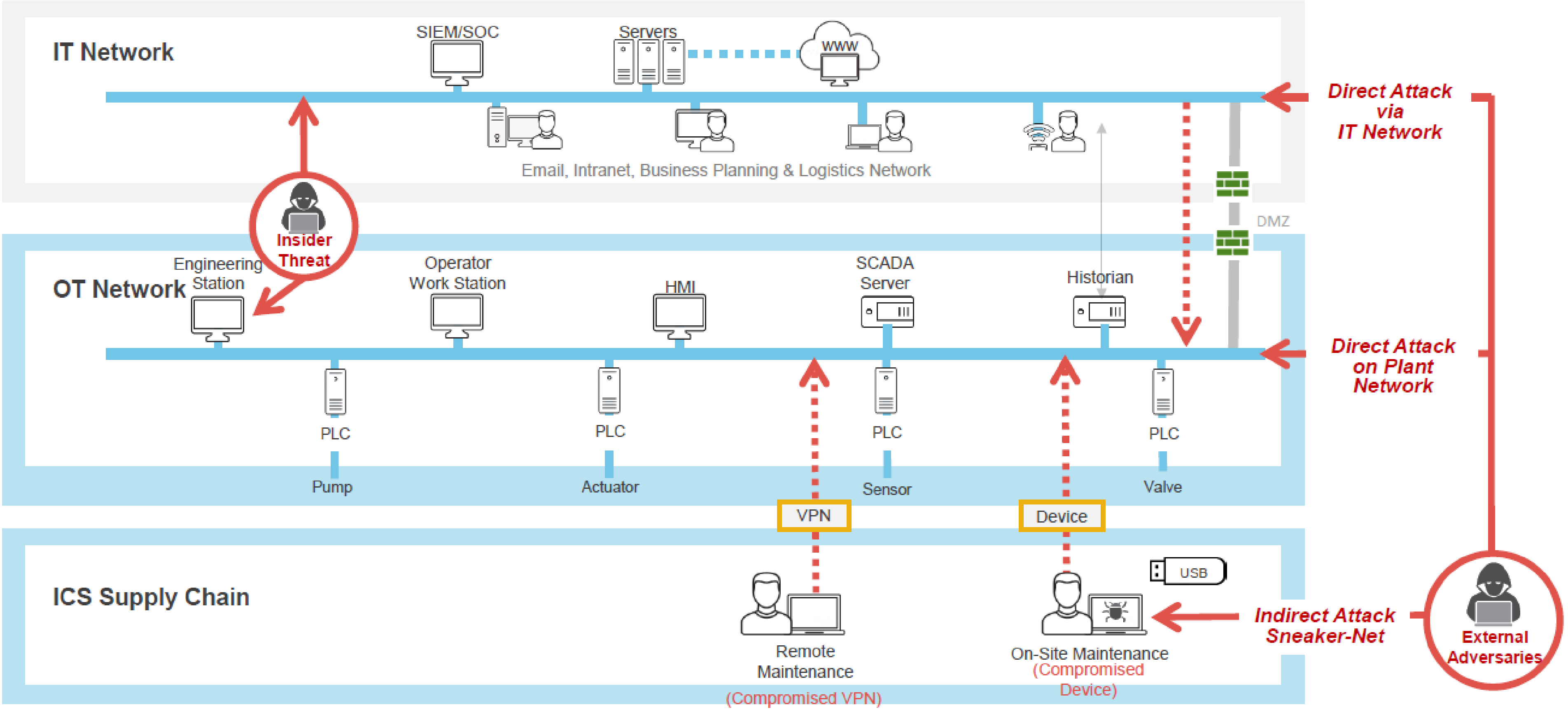


	Stuxnet	Black Energy	WannaCry	Havex	Industroyer	Triton
	Infected USBs	Infected documents	Credential phishing	Cross-site scripting	Social engineering	Social engineering
TIER 2 External Facing	Buffer error DLL injection	Keylogger steals VPN credentials	DLL injection Established backdoor	Injects scripts RAT hijacks control	Injects Trojan Opens backdoor	Code insertion
TIER 1 Supervisory	Escalated privilege Memory attack	Deposits Trojan Corrupts registry Hijacks servers	Memory attack (EternalBlue)	Find air-gap weaknesses Discovers ICS systems	Memory attack Discovers and flips relays	Corrups engineering workstations
TIER 0 Device I/O	Changes PLC settings Damages equipment	Modifies firmware Opens breakers, damages systems	Encrypts files for ransom Disables systems	Industrial espionage	Flipped relays causes damage and outages	Executes rogue commands on PLC

Virsec Detects and Stops

Source: Virsec company website

ICS THREAT VECTORS



IT Network

SIEM/SOC

Servers

WWW

Email, Intranet, Business Planning & Logistics Network

Direct Attack via IT Network

Insider Threat

DMZ

OT Network

Engineering Station

Operator Work Station

HMI

SCADA Server

Historian

Direct Attack on Plant Network

PLC

PLC

PLC

PLC

Pump

Actuator

Sensor

Valve

VPN

Device

ICS Supply Chain

USB

Remote Maintenance (Compromised VPN)

On-Site Maintenance (Compromised Device)

Indirect Attack Sneaker-Net

External Adversaries

Rockwell Automation

Source: Rockwell Automation

Keysight Threat Simulator

FAST, EASY-TO-USE, AND EFFECTIVE

Attack Yourself Quickly, Safely, & Securely

- Deploy and run in a matter of minutes.
- Simulate the kill chain with real-world malware & techniques
- Agents hosted in Dark Cloud ensure safety

Remediate and Optimize Rapidly

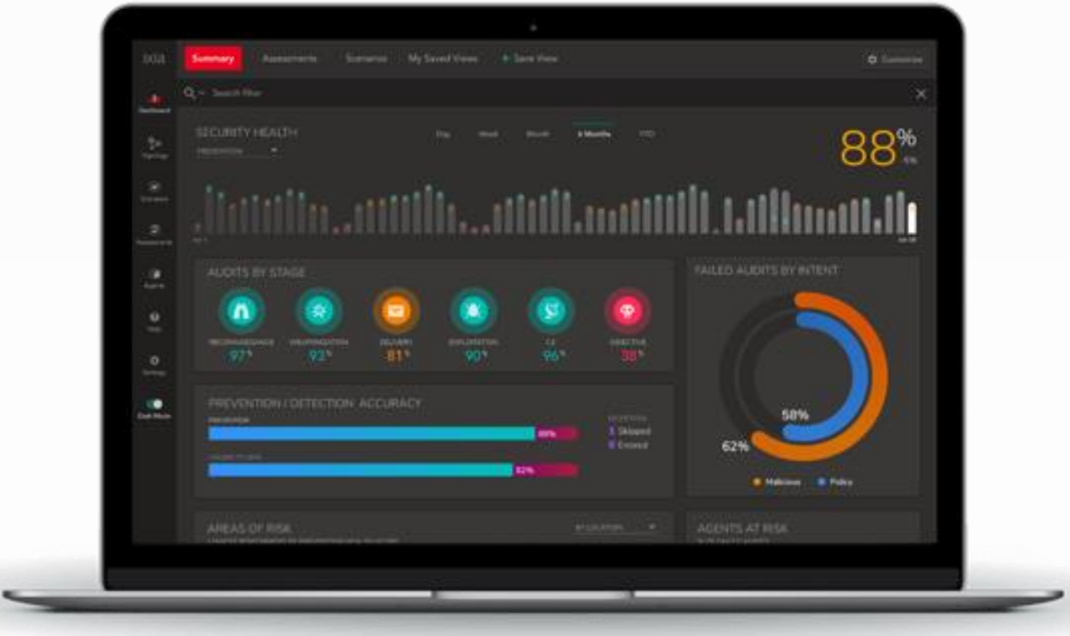
- Best-in-class step-by-step recommendations close gaps
- Maximize existing products without extra cost

Analyze Detection and Blocking Capabilities

- Be confident in detection and blocking rules, even after changes

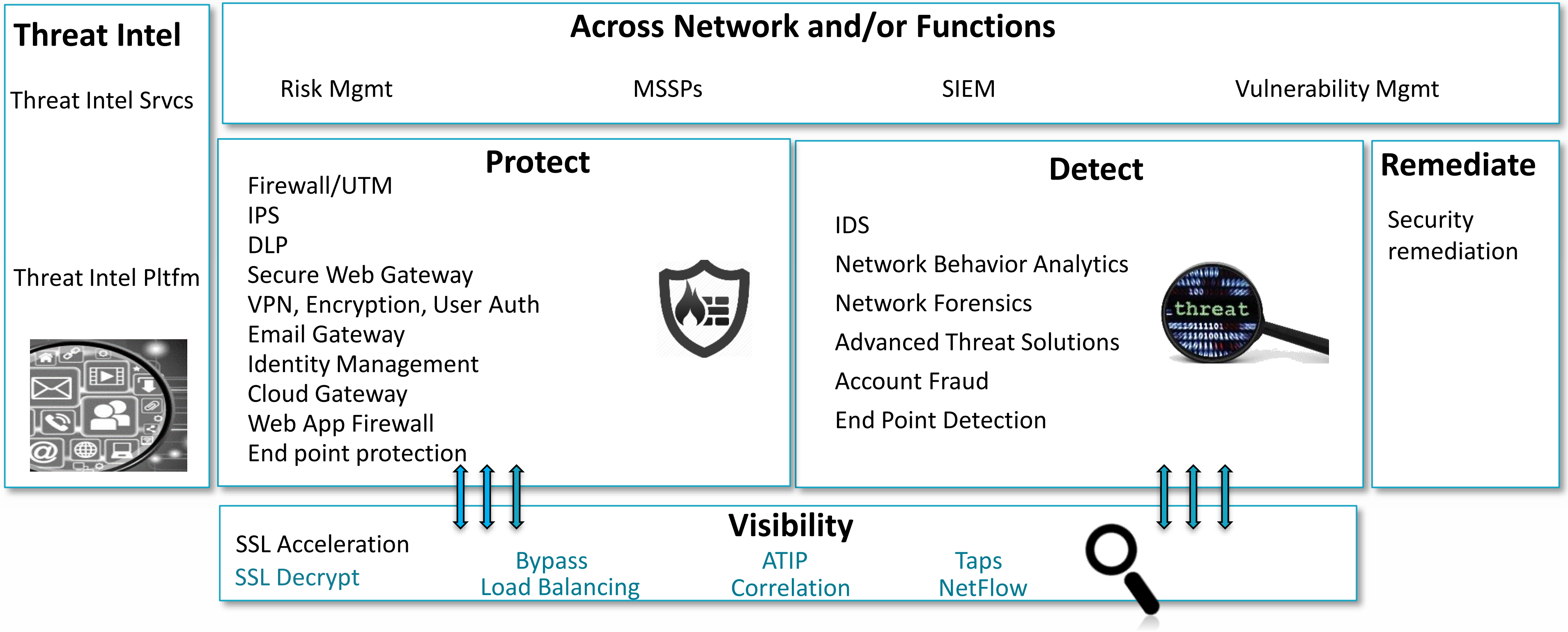
Get In Front of New Attacks with Continuous Audits

- Minimize risk from config. changes, new threats, etc.



OT Network Security Framework

MAJOR CATEGORIES & SOLUTIONS



Threat Intel

Threat Intel Srvcs

Threat Intel Pltfm

Across Network and/or Functions

Risk Mgmt

MSSPs

SIEM

Vulnerability Mgmt

Protect

Firewall/UTM
IPS
DLP
Secure Web Gateway
VPN, Encryption, User Auth
Email Gateway
Identity Management
Cloud Gateway
Web App Firewall
End point protection

Detect

IDS
Network Behavior Analytics
Network Forensics
Advanced Threat Solutions
Account Fraud
End Point Detection

Remediate

Security remediation

Visibility

SSL Acceleration
SSL Decrypt

Bypass
Load Balancing

ATIP
Correlation

Taps
NetFlow

Application Security Testing

OT Security Visibility Vendors

EMERGING KEYSIGHT TECHNOLOGY PARTNERS

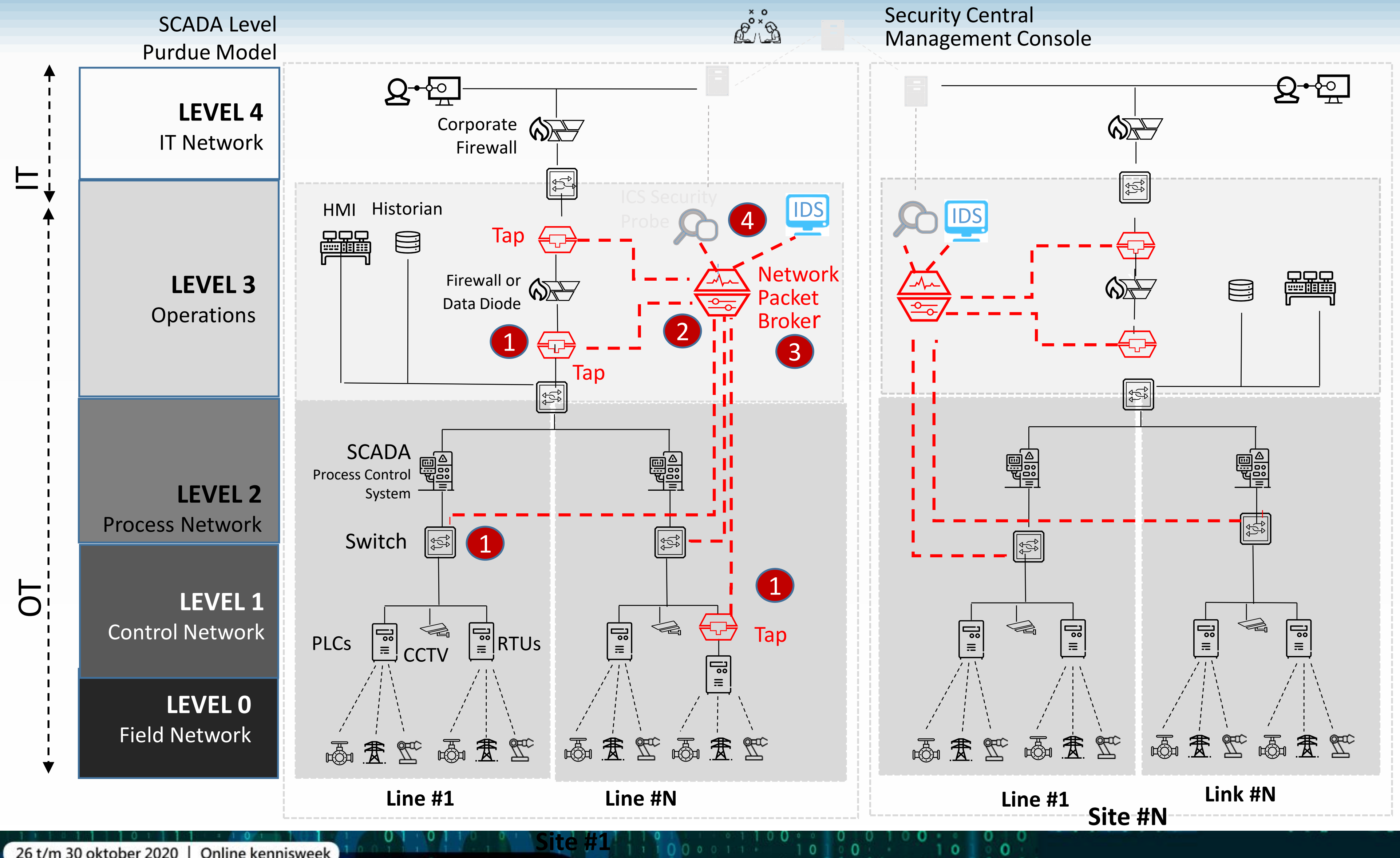
- Nozomi
  - Industrial Focus
  - ICS Security & Visibility
  - Close partnership with ICS SIs (e.g. Siemens)
- Armis
  - Broad IoT Focus
  - Startup with strong funding and backing
  - Agentless Device Security
  - Integrated with Palo Alto Cortex
- Forescout (Security Matters acquisition)
  - Broad Focus
  - $300M+ revenue
  - Industrial Cyber Resilience – Silent Defense
  - VMWare Integration for IoT

IXIA XCEED PARTNERS

Tenable
- Cyber Exposure specialist
- Powered by Indegy
- Unified risk-based platform

- Dragos
  - Purely Industrial focused
  - Offers Services with products
  - Discover, Secure, Optimize
- Darktrace (Industrial Immune System)
  - OT / IT/ IoT
  - Large late stage startup
  - Cyber AI for OT Environments

ICS/OT Security Visibility Reference Architecture



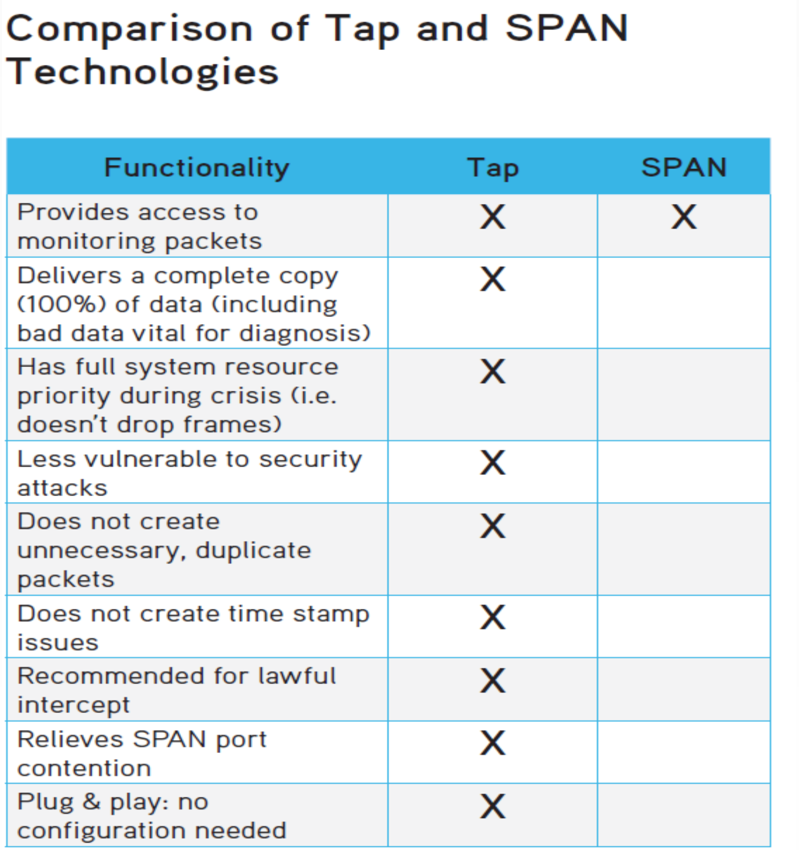
1 Tap or SPAN traffic in Level 1/2/3 for full visibility

2 Aggregate traffic to NPB in Level 3 to simplify security tool deployment

3 Filter out unneeded traffic (ex. CCTV) to maximize tools

4 Share traffic with multiple tools

TAP vs SPAN

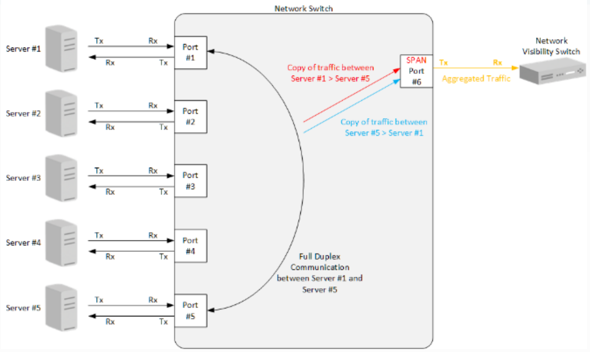


Comparison of Tap and SPAN Technologies

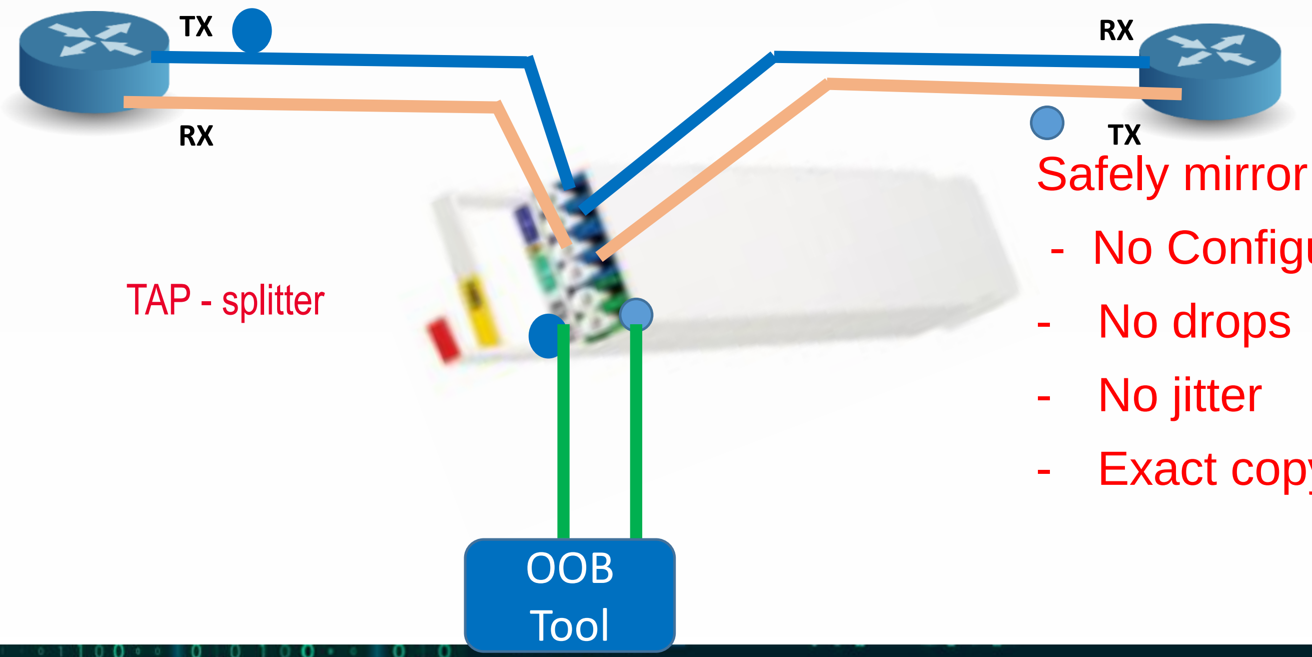
Functionality	Tap	SPAN
Provides access to monitoring packets	X	X
Delivers a complete copy (100%) of data (including bad data vital for diagnosis)	X	
Has full system resource priority during crisis (i.e. doesn't drop frames)	X	
Less vulnerable to security attacks	X	
Does not create unnecessary, duplicate packets	X	
Does not create time stamp issues	X	
Recommended for lawful intercept	X	
Relieves SPAN port contention	X	
Plug & play: no configuration needed	X	

SPAN

- Low number of SPAN ports per switch; easy to run into SPAN contention
- Susceptible to packet drops when link utilization is high (especially during aggregation)


Network Switch
Server #1
Server #2
Server #3
Server #4
Server #5
Tx
Rx
Port #1
Port #2
Port #3
Port #4
Port #5
SPAN Port #6
Copy of traffic between Server #1 > Server #5
Copy of traffic between Server #5 > Server #1
Full Duplex Communication between Server #1 and Server #5
Aggregated Traffic
Network Visibility Switch

TAPs protect, deliver all traffic, minimize downtime – max reliability



Safely mirror all frames

- No Configuration
- No drops
- No jitter
- Exact copy of frame

Industrial ICS Visibility

PRIMARY KEYSIGHT VISIBILITY USE CASES

Challenge	Solution	Benefit	Notes
Multiple links to monitor	NPB Aggregation	Visibility into all links, rationalize tool spend	Low cost and form factor are important
SPAN limitations	Tap	See all ports, avoid affecting production	Avoid Traffic Loops, OT switches limited SPAN
SPANs drop packets	Tap	Avoid Dropped Packets on both **Production** and Visibility environments	Taps easier to deploy at ‘Level 3’ and ‘Level 4’. **No load on production switches**
CCTV traffic overwhelms ICS Security tools	NPB Filtering	Reduce up to 80% of traffic to hit tools	RTP/RTSP packets not needed by ICS Tools
Different tools need data	NPB Traffic Sharing	All tools that need the data can get it	Number of tools less than in IT

Use Case: Electric Utilities in United States

Business Objective:

- North American Energy Corporation (NERC) Compliance

Technical Solution:

- Monitoring at SCADA Level 2 of Transmission Substations

Keysight Role:

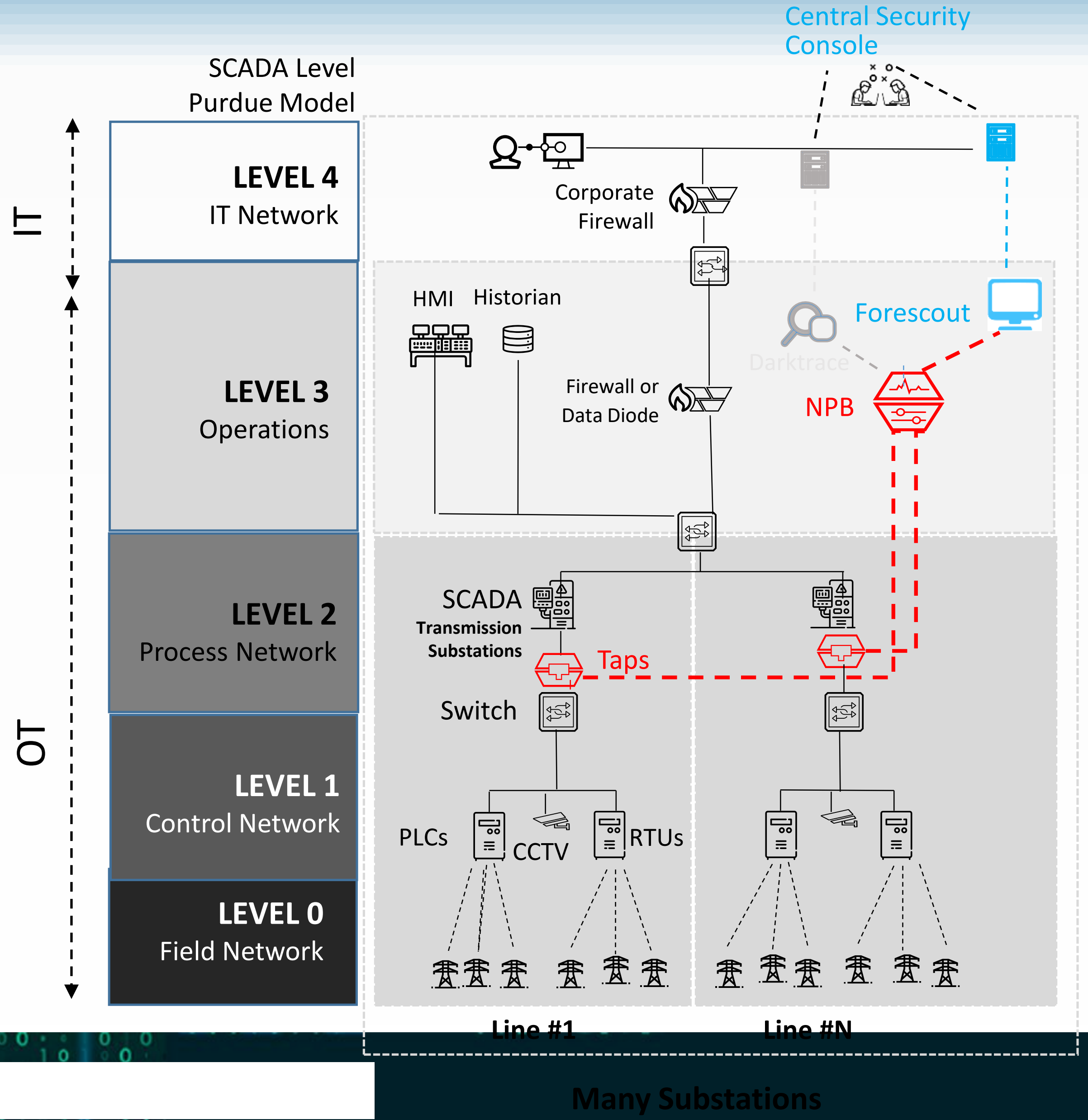
- Taps, Aggregation, avoid traffic drops, specialized rails and power supplies: Copper and Fiber Taps, E10 NPB

Technology Providers/Partners:

- Ernst & Young, Forescout, Darktrace

Benefits:

- Knowing what is in their sites (some not seen 20+ years)
- Avoid fines of 10s of Millions, restore public confidence



Use Case: Manufacturer

KEYSIGHT, NOZOMI, AND INCIDENT RESPONSE

Business Objective:

- Ensure cybersecurity in wake of industrial threats

Technical Solution:

- Monitoring at SCADA Level 2 of OT network

Keysight Role:

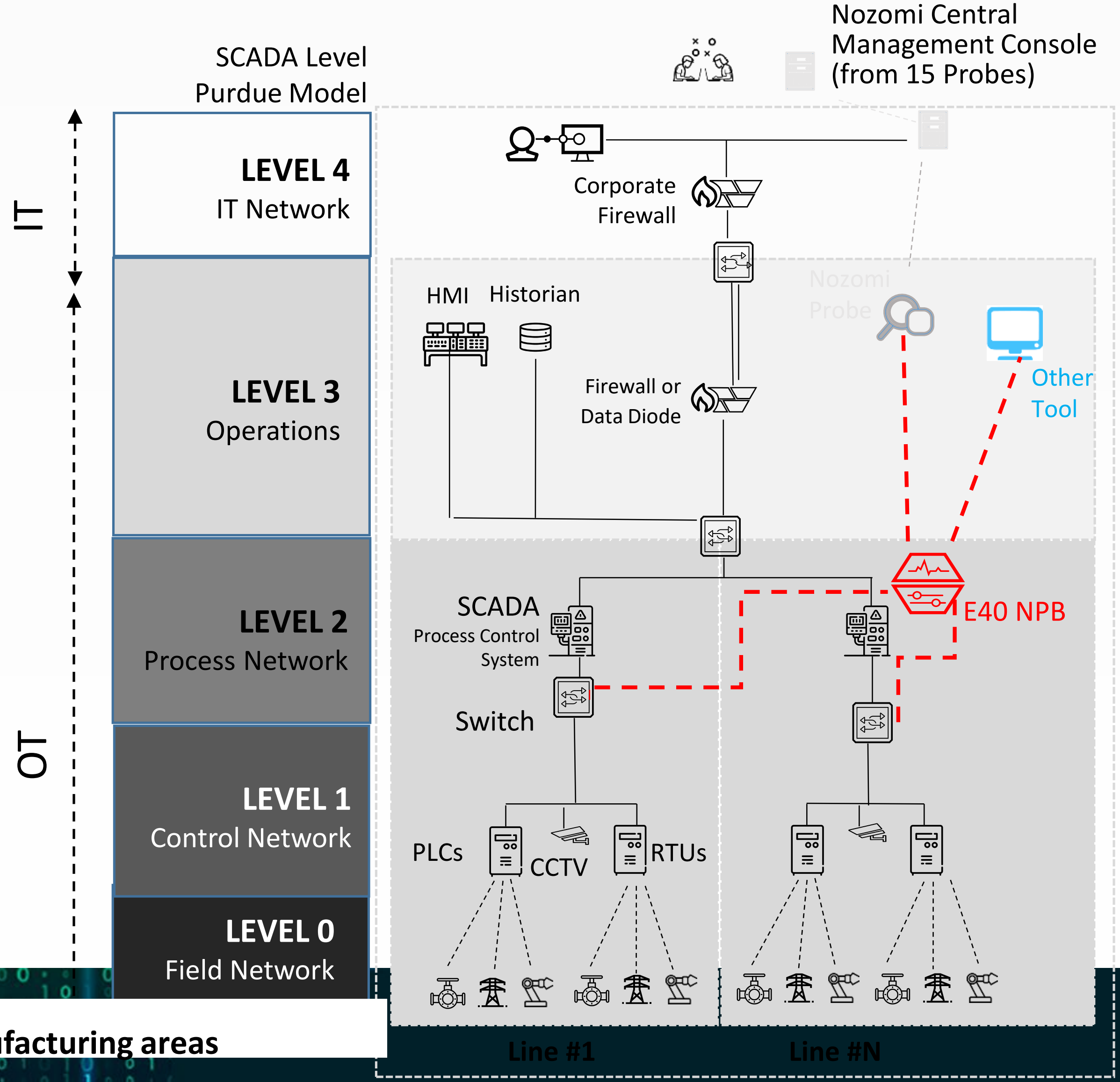
- SPAN Aggregation, Tool Sharing, Avoiding risks of faulty RSPAN configuration (e.g. Spanning Tree loops)

Technology Providers/Partners:

- Nozomi Networks

Benefits:

- Clean view of all OT Traffic for complete security
- Avoid risks of misconfigured production switches (RSPAN)
- Customer saves money by consolidating monitoring



1 of 15 Manufacturing areas

Use Case: Mass Transport Agency in Asia

Business Objective:

- Critical Infrastructure Protection Compliance

Technical Solution:

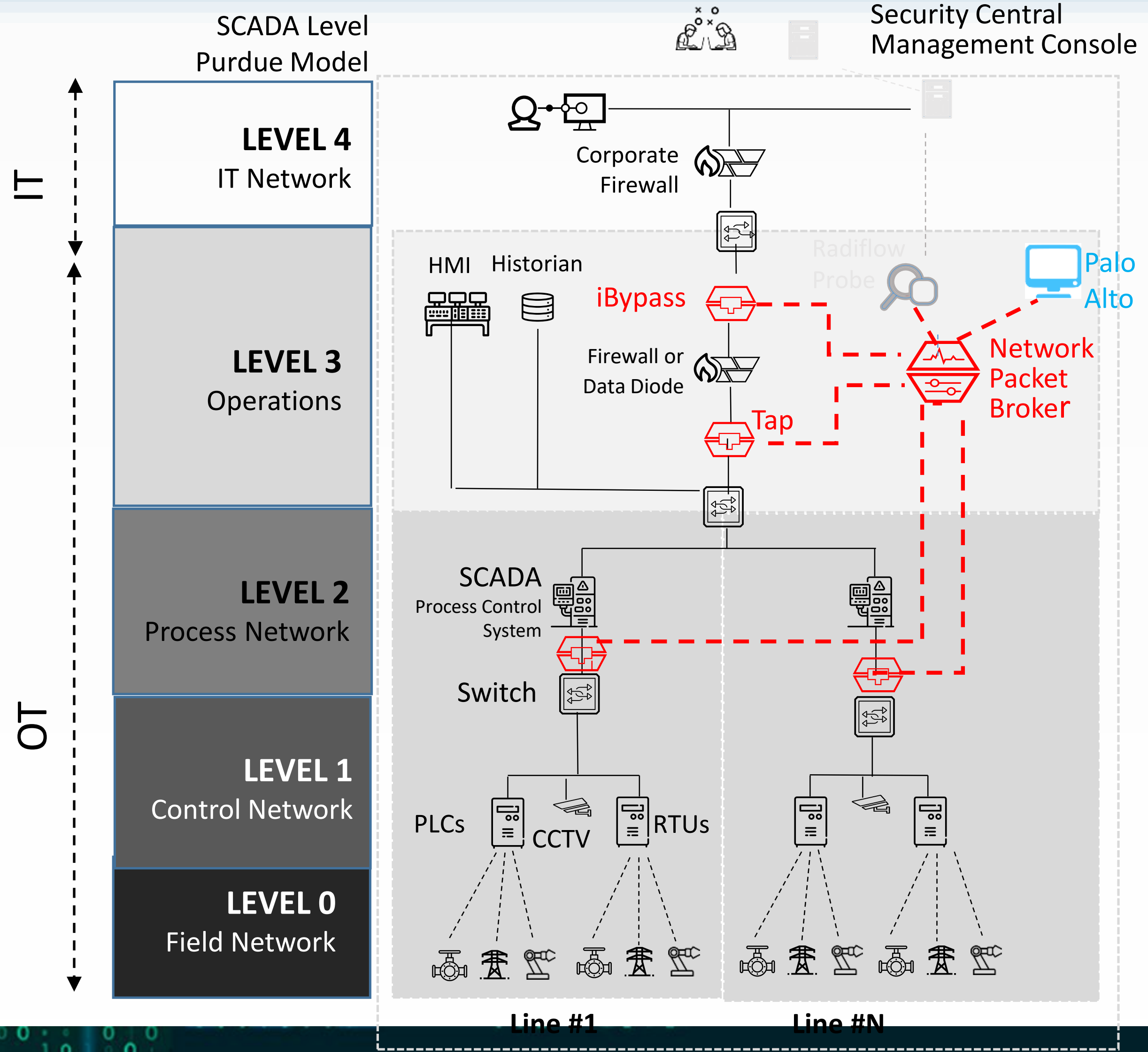
- Monitoring of operational network with multiple tools

Keysight Role:

- Aggregation, Bypass, Tool Sharing: NPB, Taps, iBypass

Technology Providers/Partners:

- Palo Alto Networks, Radiflow



Vragen

Bedankt voor uw aandacht, stel u vragen gerust in de chat!

Mocht u contact met ons op willen nemen stuur ons dan een email:

John Adams
John.Adams@Keysight.com

Ruud Sauren
Ruud.Sauren@Keysight.com

KEYSIGHT
TECHNOLOGIES