Industrial Cybersecurity Landscape in 2020: Trends, Challenges, and Opportunities

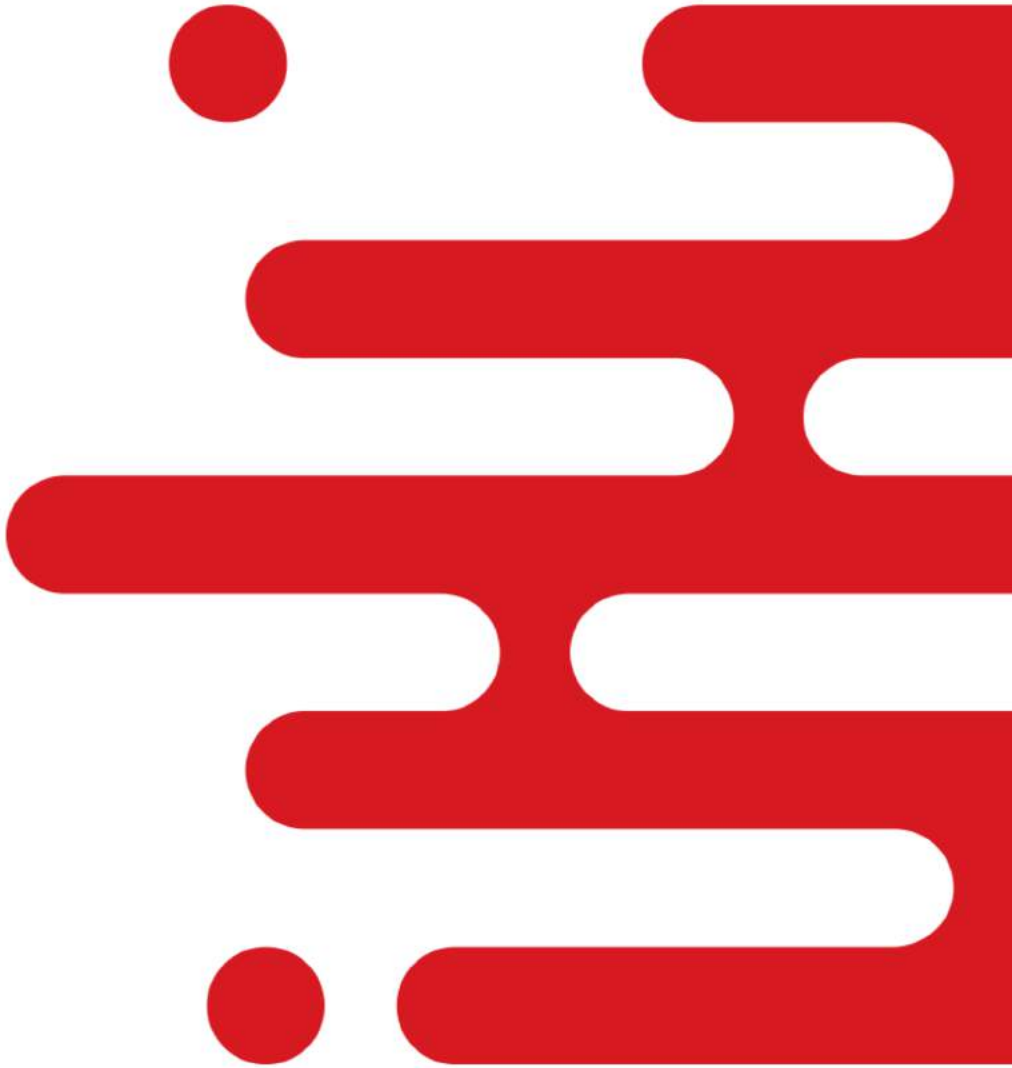
Dr. Terence Liu

VP-GM, Trend Micro and TXOne Networks

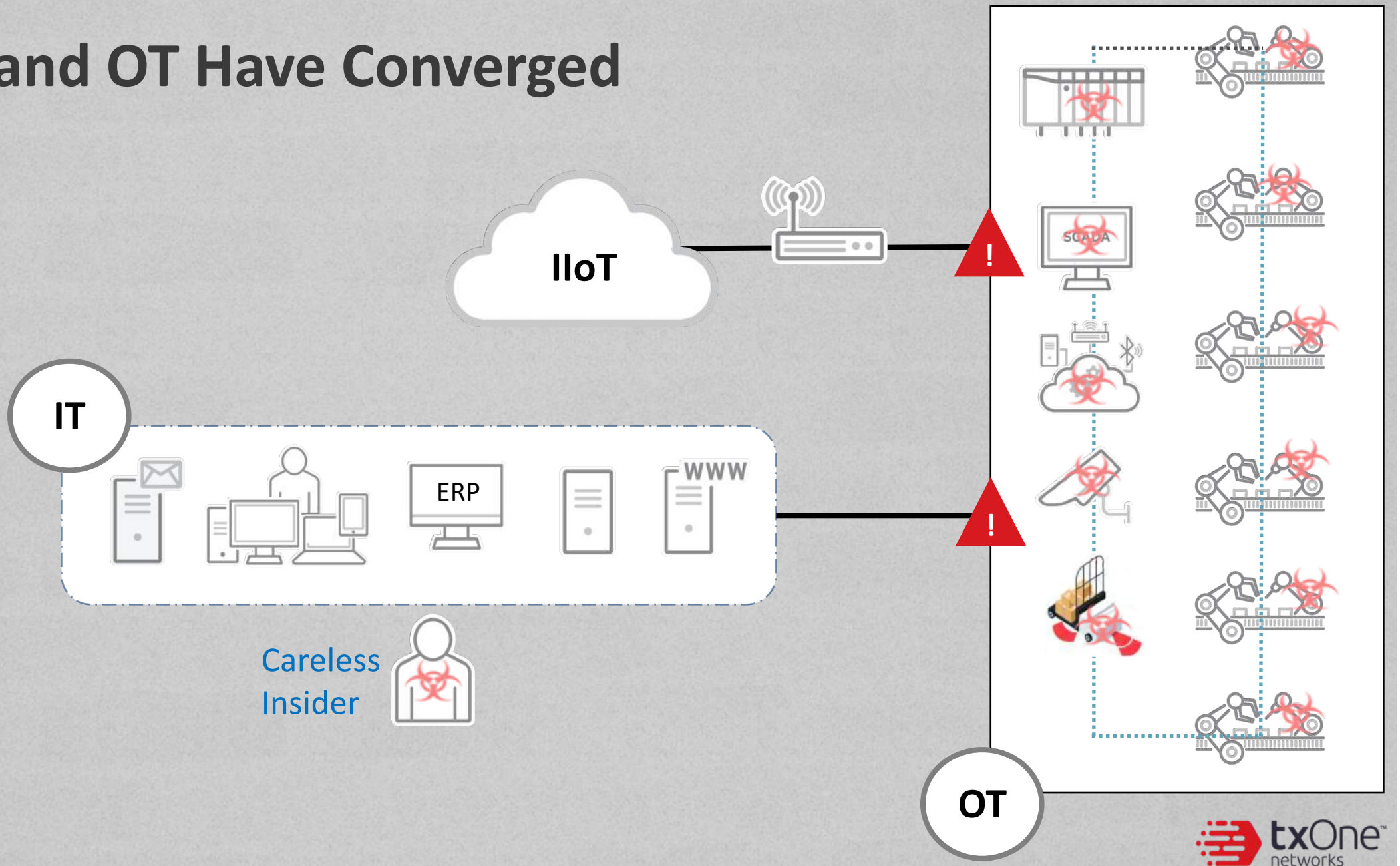
txOne networks

txOne networks

START POINT OF THE HEAT



IT and OT Have Converged



Foiled Conspiracy

1. Launch an DDoS attack against Tesla in order to preoccupy the company's security staff
2. Utilize malware to exfiltrate data for further ransom

txOne networks

Air-gapped OT is actually RARE for modern factories

- No wireless, no Bluetooth
- No connection (ethernet)
- Physical Isolation (six walls)
- All software/hardware tested BEFORE installing
- Data only passed by personal means, USB, CD, DVD

== Your business does not need to optimize production

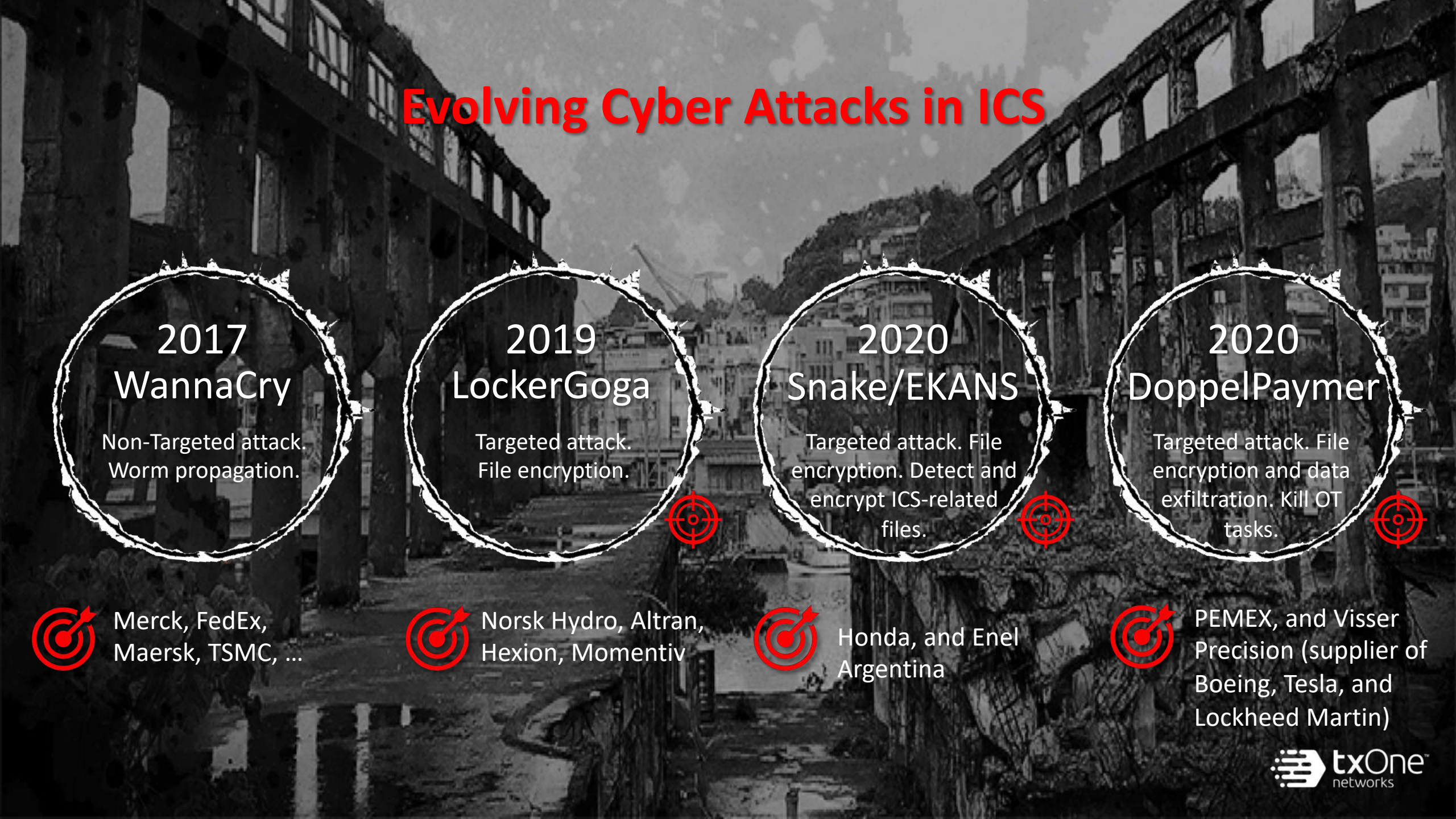
txOne networks

Threat's Paradigm Shift in ICS World

Manufacturers could be TARGETED

txOne networks

Evolving Cyber Attacks in ICS



2017 WannaCry

Non-Targeted attack. Worm propagation.

Merck, FedEx, Maersk, TSMC, …

2019 LockerGoga

Targeted attack. File encryption.

Norsk Hydro, Altran, Hexion, Momentiv

2020 Snake/EKANS

Targeted attack. File encryption. Detect and encrypt ICS-related files.

Honda, and Enel Argentina

2020 DoppelPaymer

Targeted attack. File encryption and data exfiltration. Kill OT tasks.

PEMEX, and Visser Precision (supplier of Boeing, Tesla, and Lockheed Martin)

txOne networks

Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024

Financial Impact of Cyber-Physical System Attacks Resulting in Fatalities Expected to Grow

Liability for cyber-physical security incidents will pierce the corporate veil to personal liability for 75% of CEOs by 2024, according to Gartner, Inc.

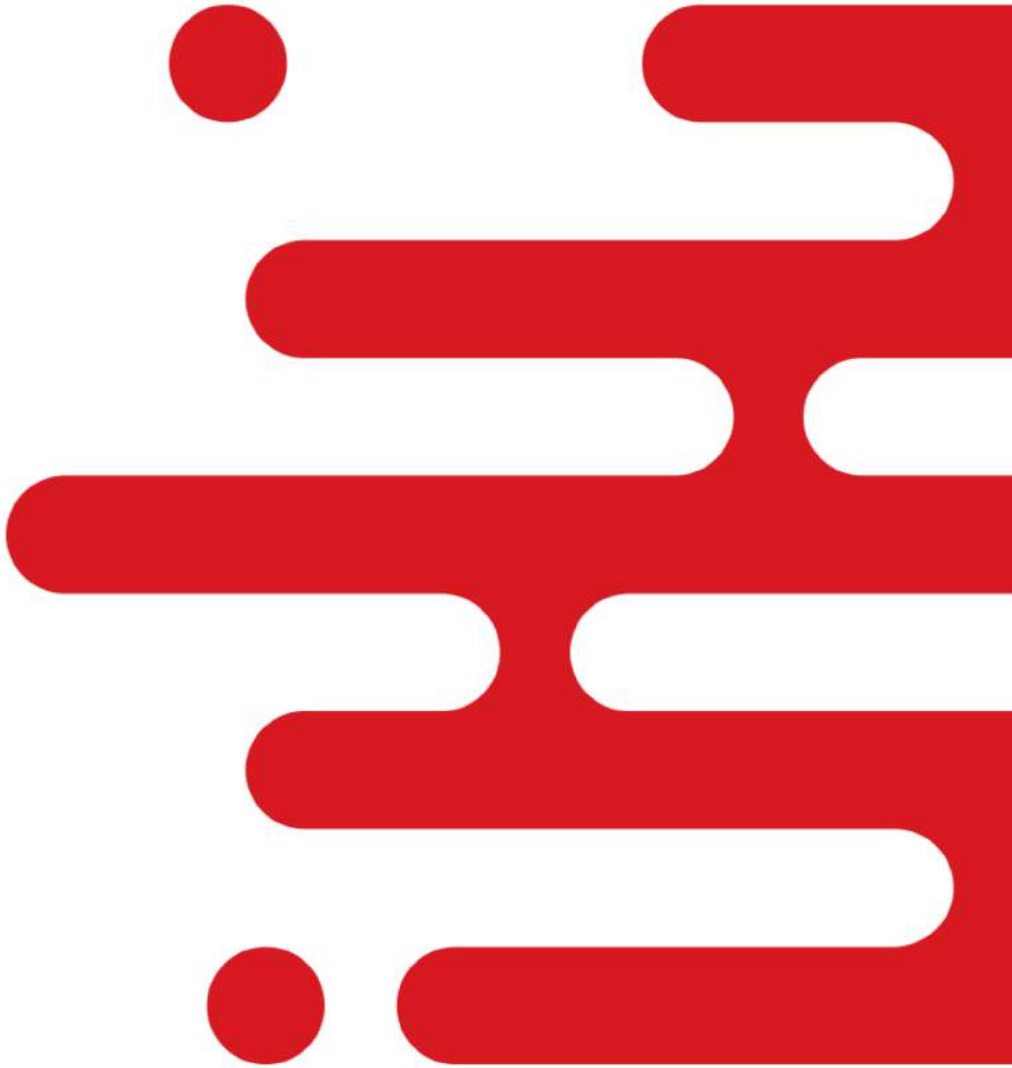
Due to the nature of cyber-physical systems (CPSs), incidents can quickly lead to physical harm to people, destruction of property or environmental disasters. Gartner analysts predict that incidents will rapidly increase in the coming years due to a lack of security focus and spending currently aligning to these assets.

““A focus on ORM – or operational resilience management - beyond information-centric cybersecurity is sorely needed,” - Gartner

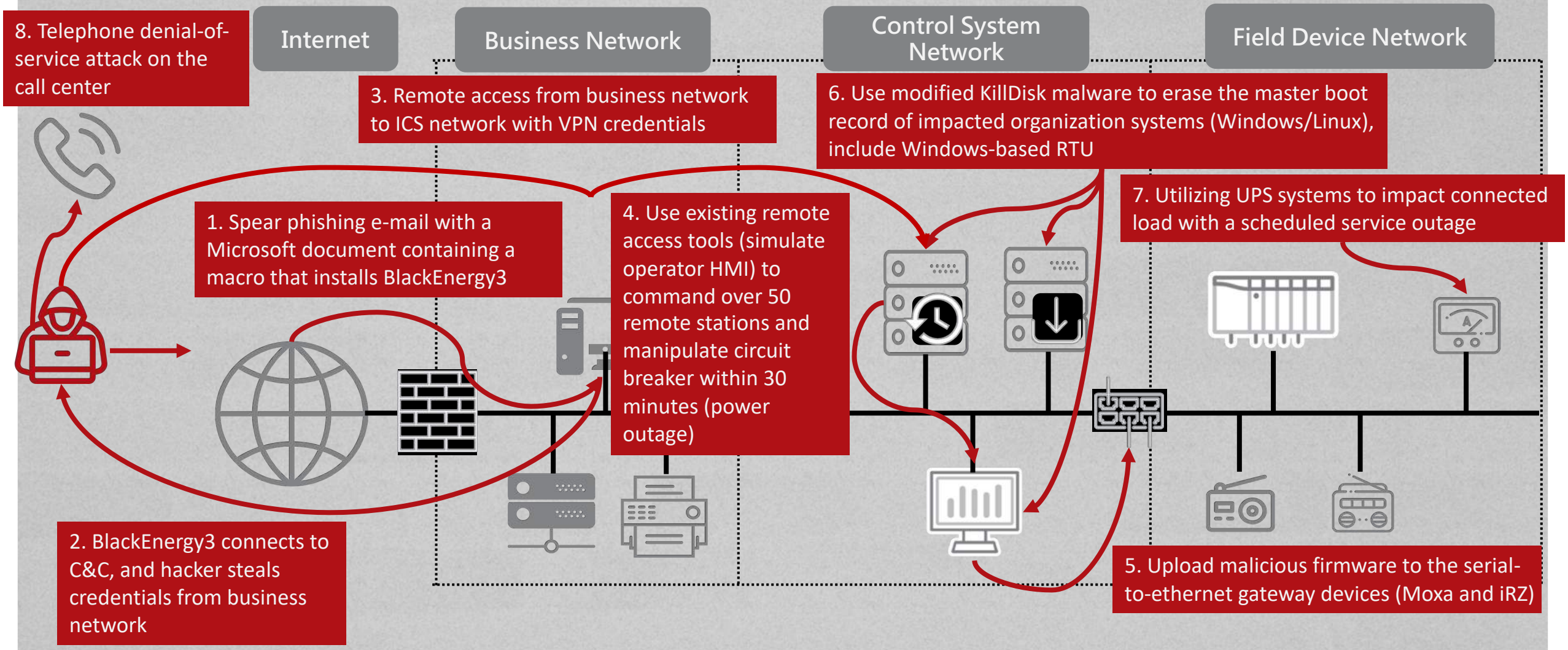
txOne networks

txOne networks

A LEAGUE OF THEIR OWN

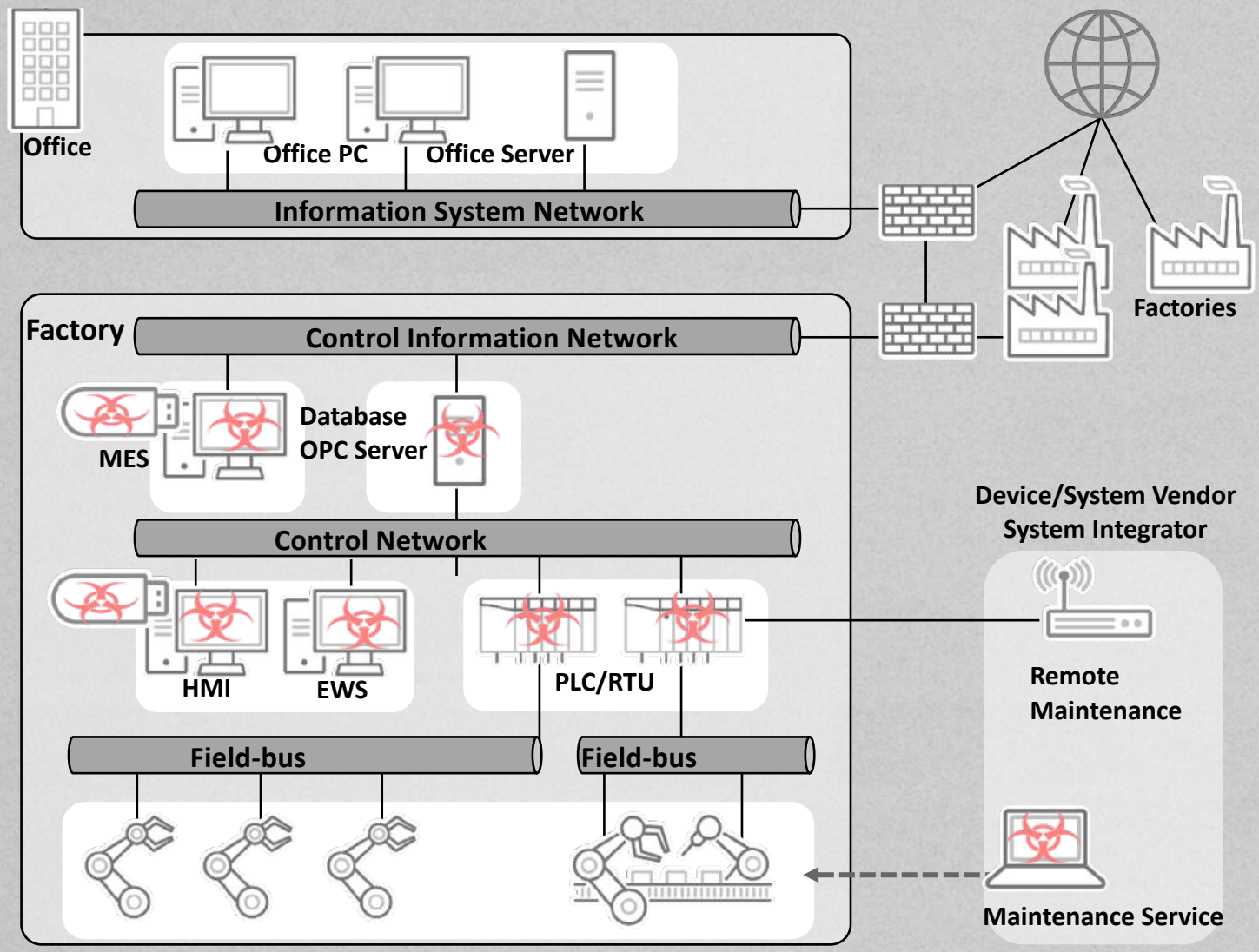


2015 Ukraine Power Grid Cyber Attack



txOne networks

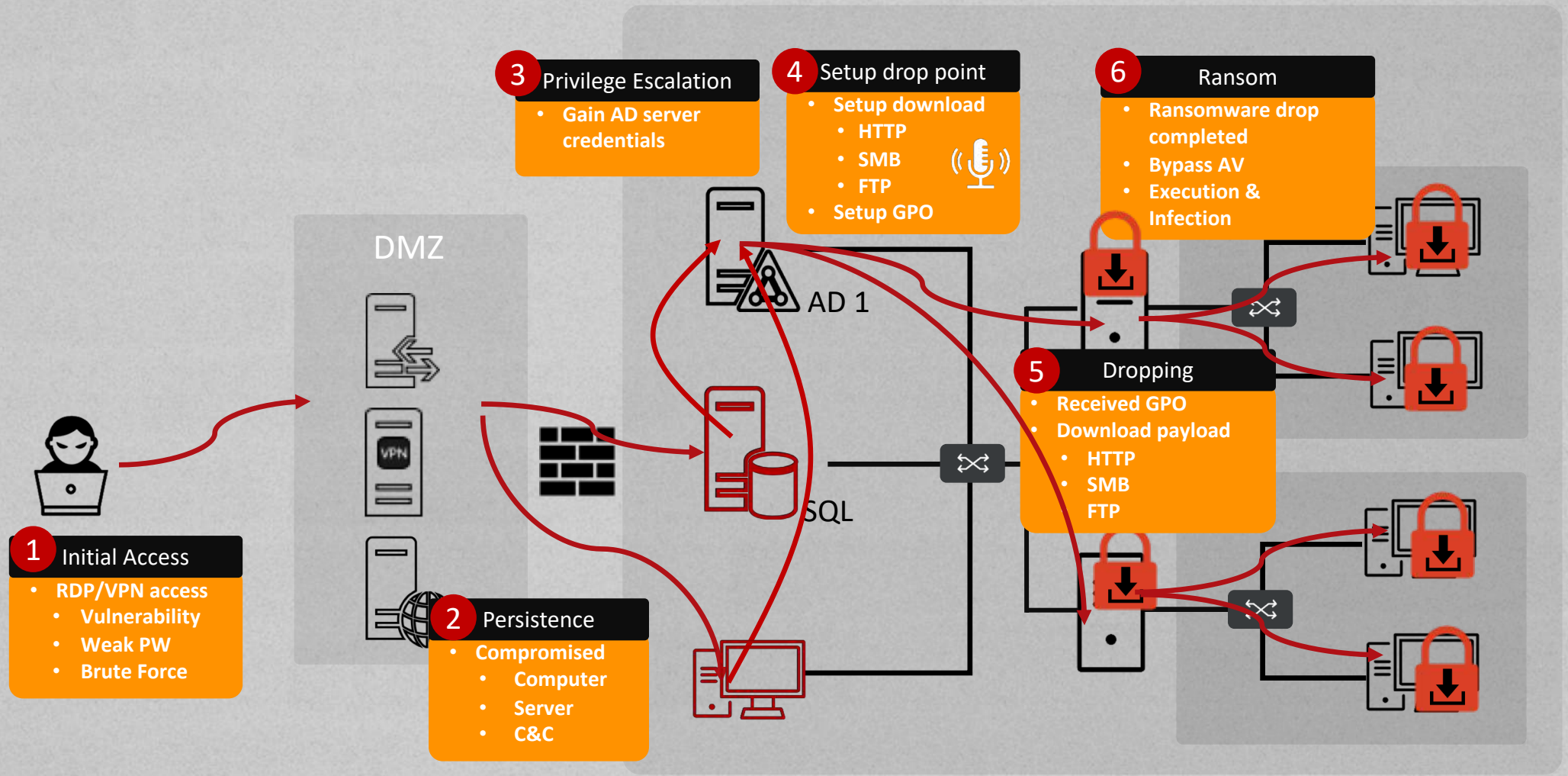
Worm Propagation in 2017-2018



Victim Companies	Impact
Pharmaceutical, Chemical (German)	$310,000,000+
Multinational Delivery Services	$300,000,000+
Construction Materials	$380,000,000+
Maritime	$300,000,000+
Semiconductor Manufacturing	$83,000,000+

txOne networks

Targeted Ransomware Attack in 2019 and 2020



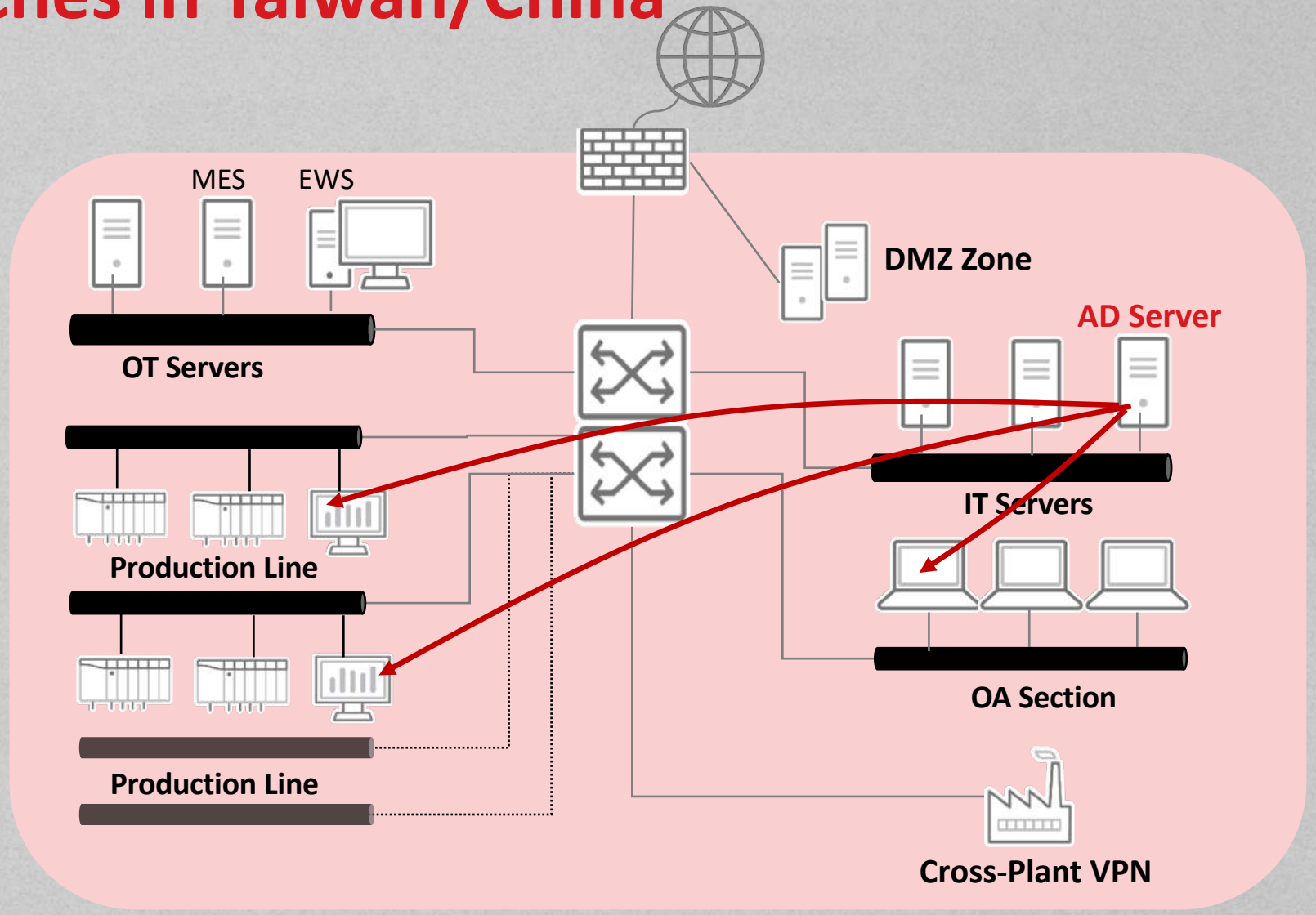
txOne networks

Recent Cyber breaches in Taiwan/China

- Suffer from both Non-Targeted and Targeted Attacks
  - No boundaries between IT and OT
  - No boundaries between factories
  - Abuse the high-credential accounts

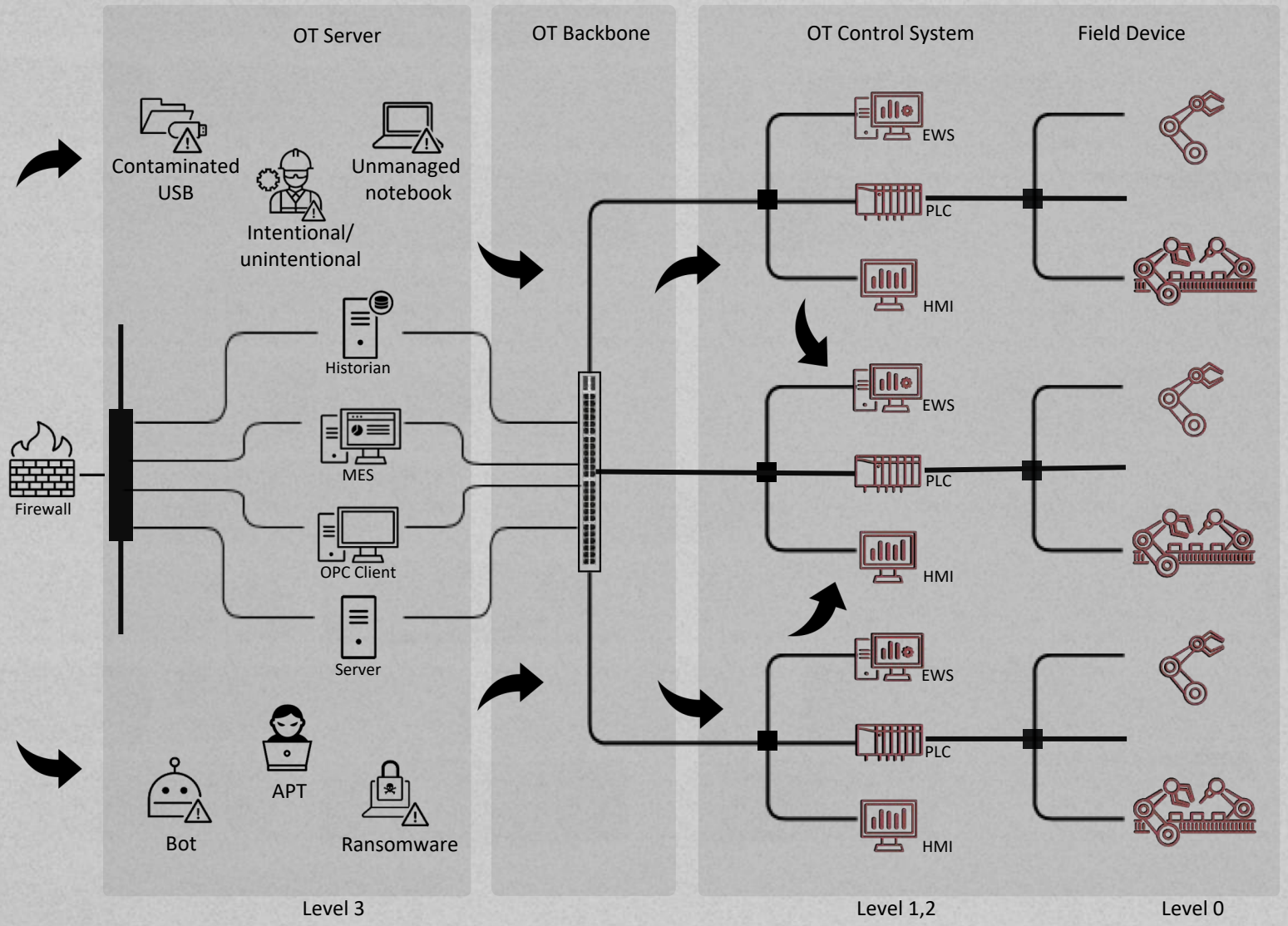
~~Zero Trust~~

Full Trust…



txOne networks

Threats and Attack Vectors



Ransomware

Targeted attack
Production Outage

Worm

Non-Targeted attack
Production Outage

PLC Misuse

Targeted attack
Production Outage

txOne networks

ICS Cyber Security Challenges

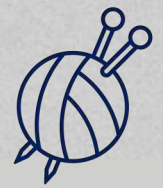
Equipment and Technology

Legacy Liability

Due to legacy liability, which is preventing cybersecurity countermeasure deployment

No Visibility

Lack of visibility and connected device management in quantity and quality control



No Tailored Solutions

People need to use IT-centric products to deal with OT-specific issues

Resource and Priority

Lack of Ability

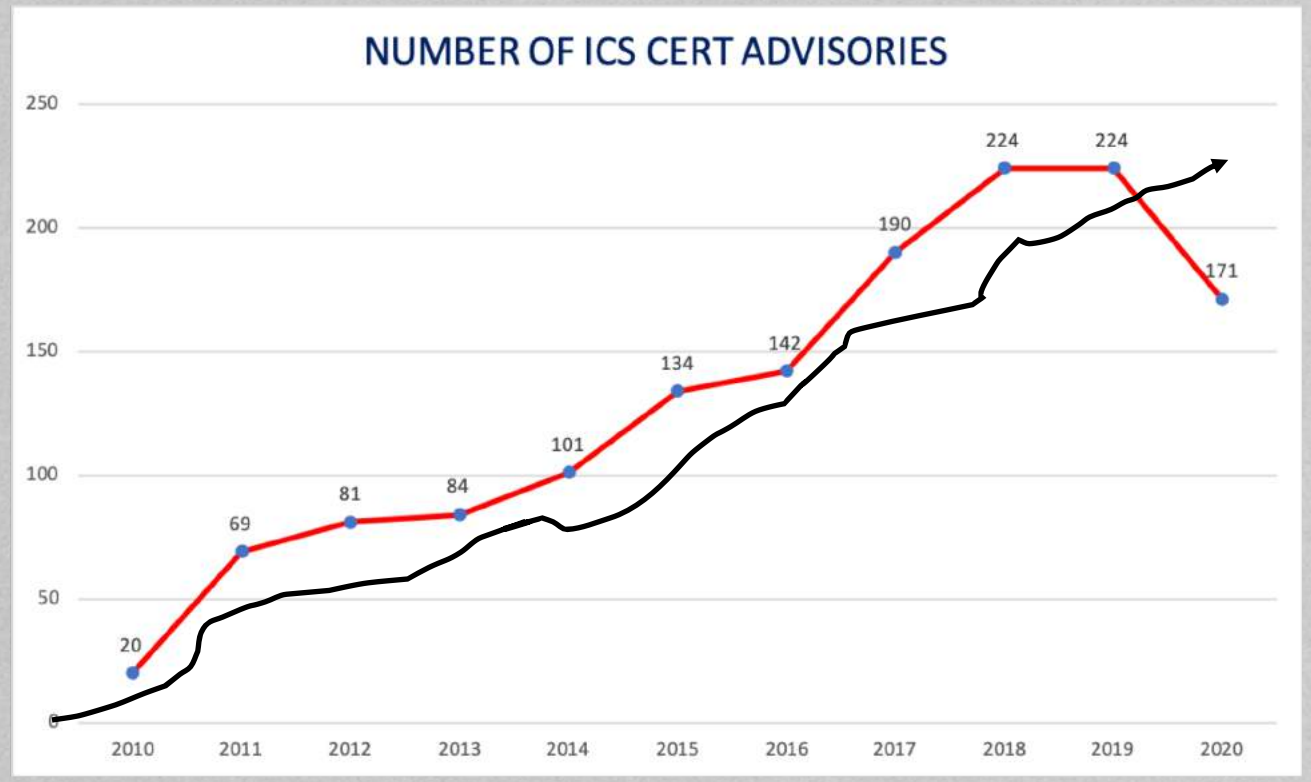
Insufficient knowledge of cybersecurity and countermeasures in OT

Pursuit of Productivity

The principle of manufacture productivity will override every cybersecurity practice and SOP

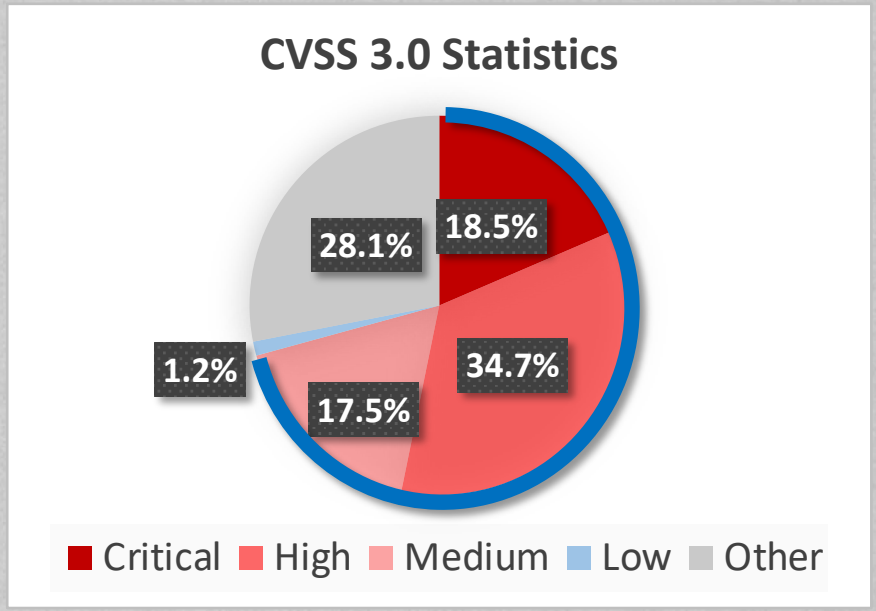
txOne networks

Majority of ICS Vulnerabilities are easily exploited

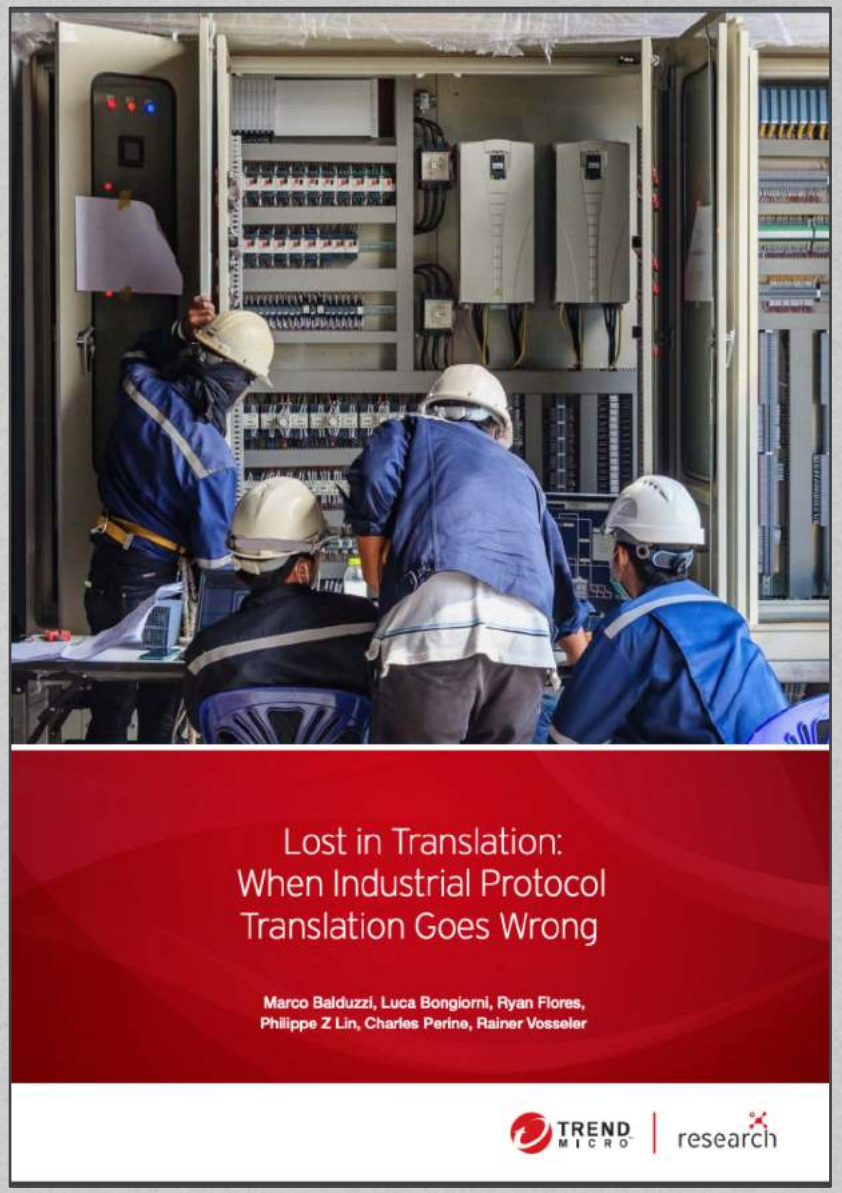


Source: ICS-CERT https://ics-cert.us-cert.gov/

1. Non-Authenticated **control command**
2. Unsecured **web service**
3. Native device **backdoor**
4. Easily conducted **Buffer Overflow**



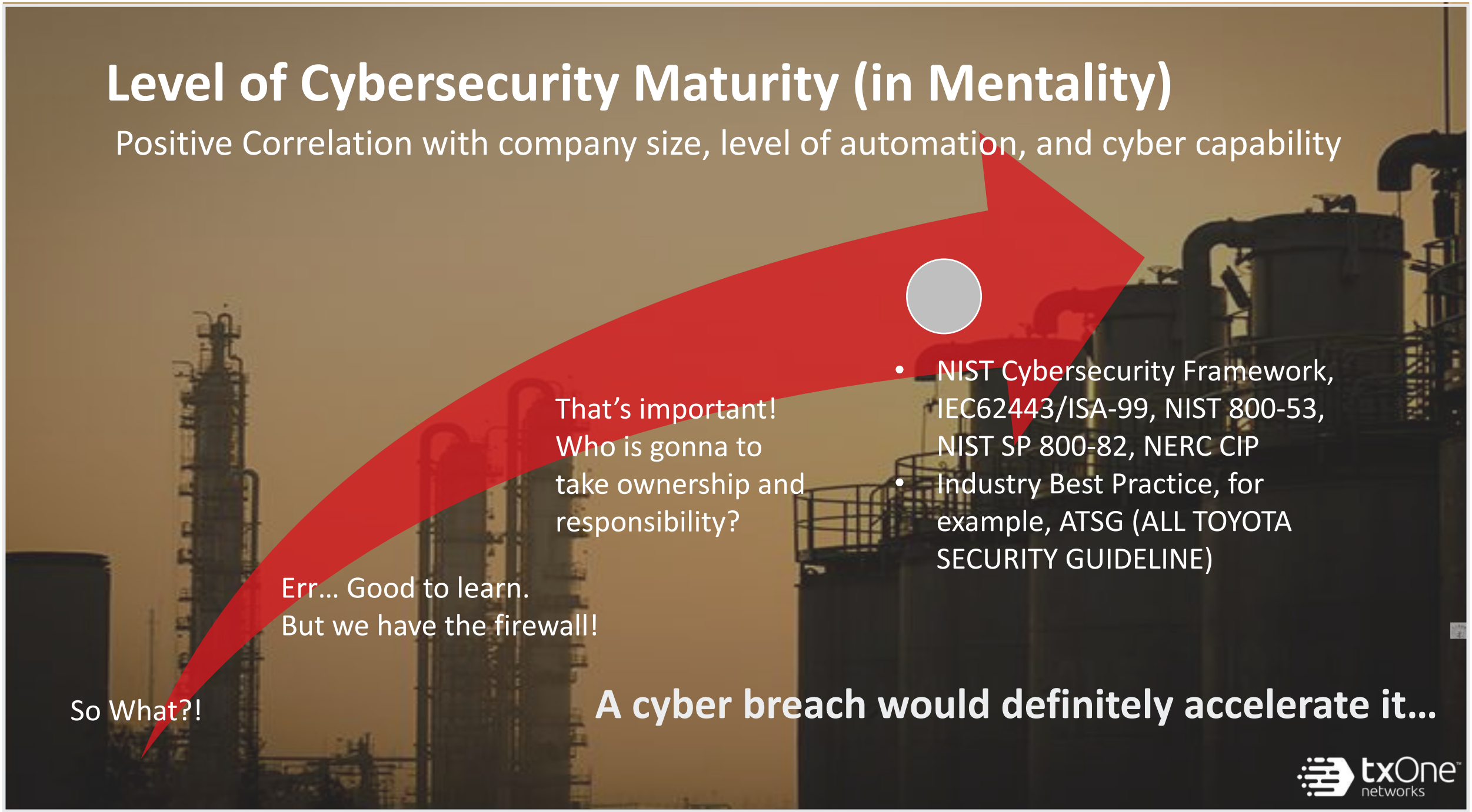
txOne networks



txOne networks

Level of Cybersecurity Maturity (in Mentality)

Positive Correlation with company size, level of automation, and cyber capability



txOne networks

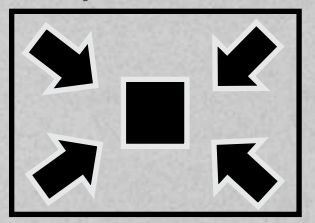
Demands to Supply Chain

- Customers' requests in real-time data visibility would uplift the OT infrastructure
- Cybersecurity is becoming a highlighted issue in supply chain management. i.e, NIST CSF
- Certificate of Origin

Defense Readiness

- OT is pretty much a black box
- IT Defense:

  Semiconductor > LCD Panel > EMS = PCB > Others
- IT runs OT security >>> OT runs OT security



Adversary

- State-Sponsored > Profit-Driven
- AD server compromising + Ransomware
- Intention? Pay or Not?

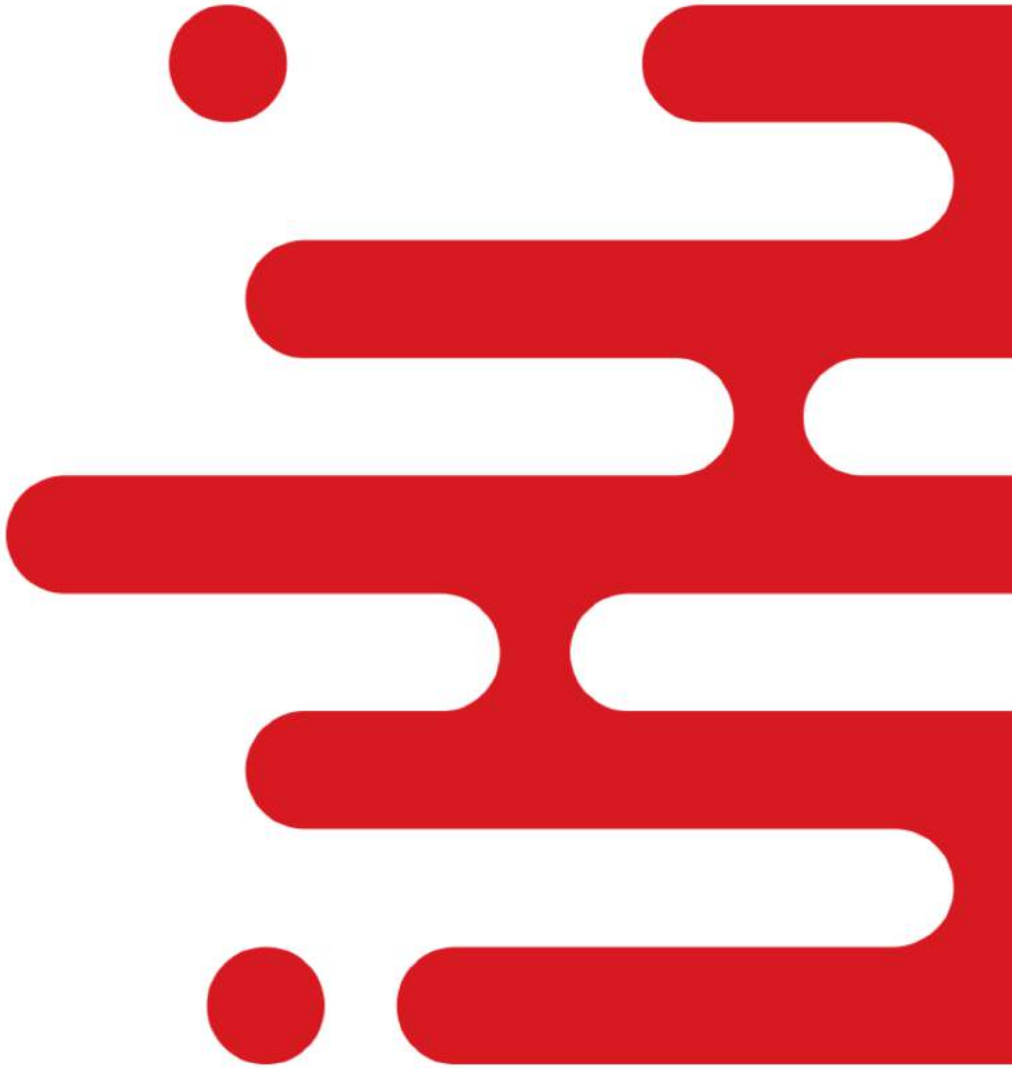
Gov's works

- 經濟部工業局資安旗艦計畫
  - ITRI: SecPaas (cybersecurity as a platform) coaches ICS users, provides pentest and evaluation services, and bridges cybersecurity vendors to the users to lower the barrier.
  - III-CSTI: ICS Testbed, Private LTE and 5G, Certification, and MITRE

txOne networks

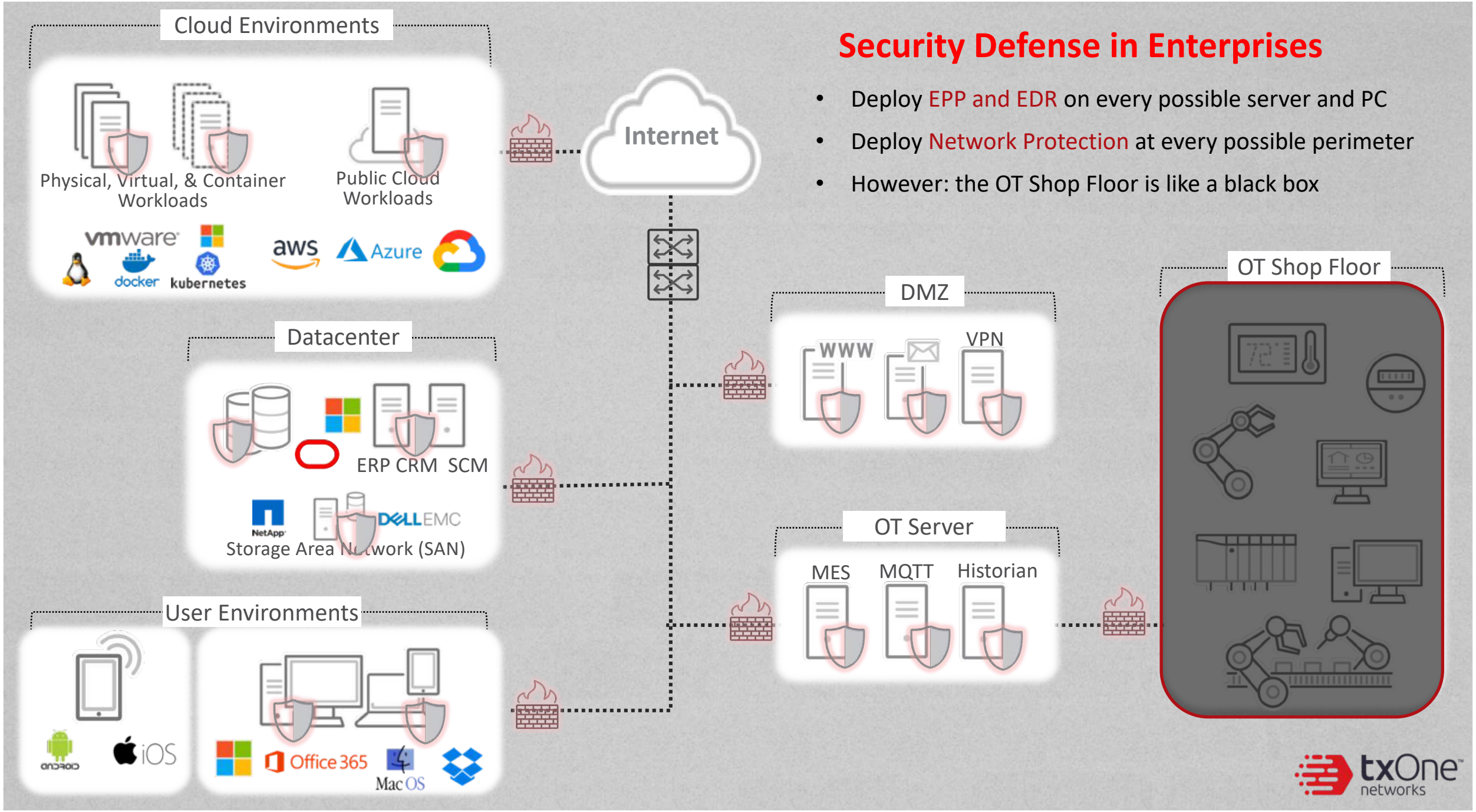
txOne networks

THE GOOD GUYS

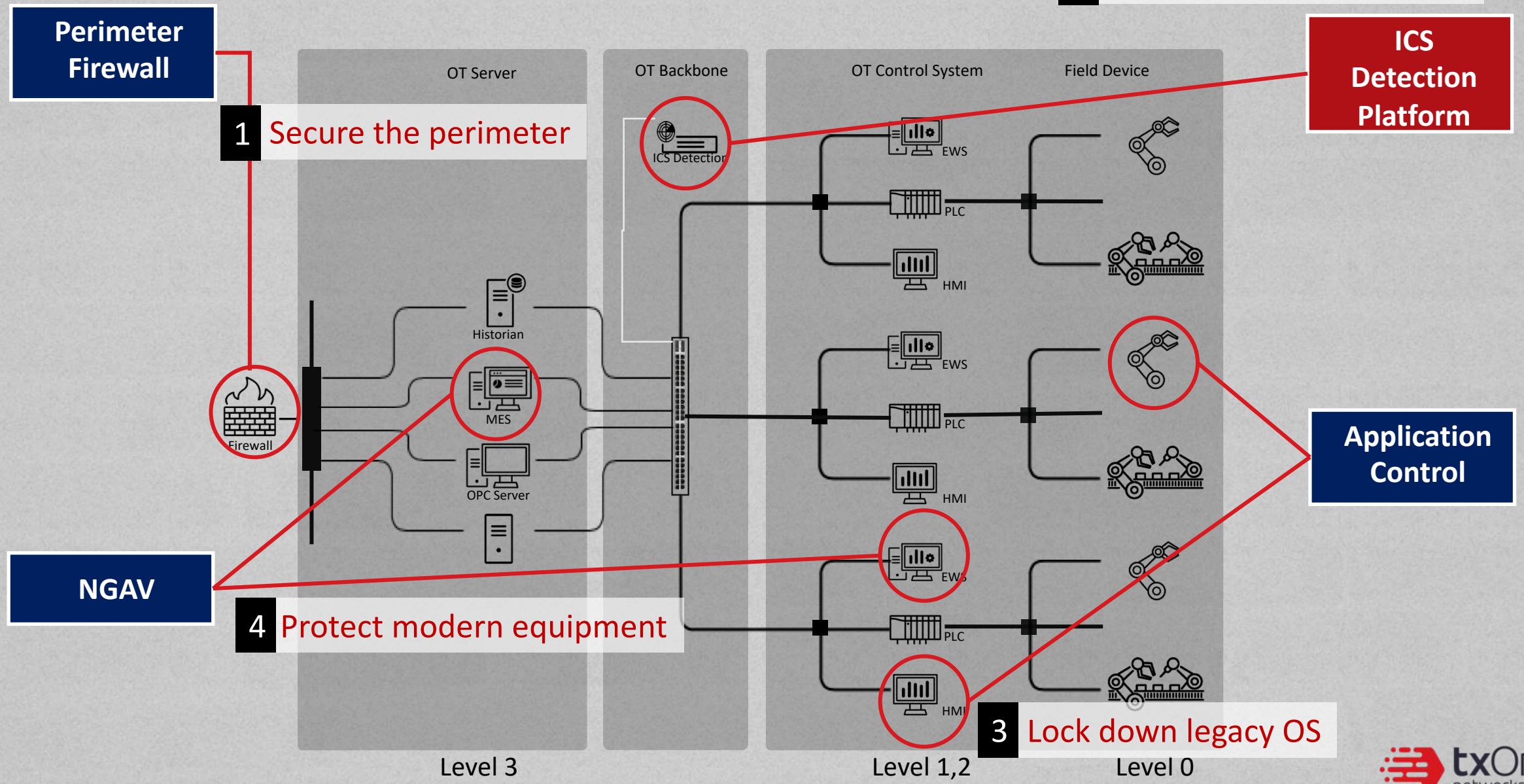


Security Defense in Enterprises

- Deploy EPP and EDR on every possible server and PC
- Deploy Network Protection at every possible perimeter
- However: the OT Shop Floor is like a black box



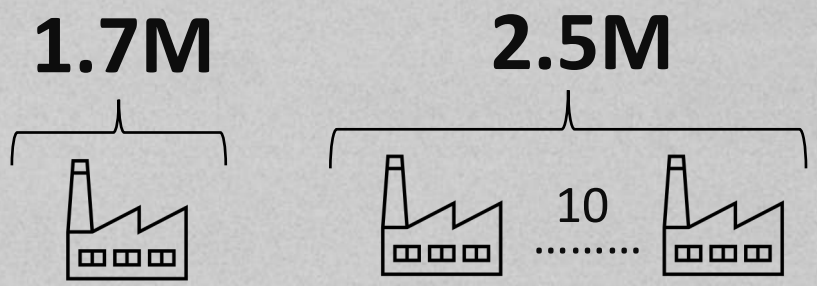
Defense in OT Shop Floo



txOne networks

ICS Detection Platform

- For startups founded 5 years ago, the target use case was an ICS Intrusion Detection System
- But OT was not quite ready then and therefore many firms pivoted to Asset Visibility and Management
- Firms MUST have dedicated resources for monitoring
  - Accenture (at S4x20) estimated the annual cost of ICS Detection at



txOne networks

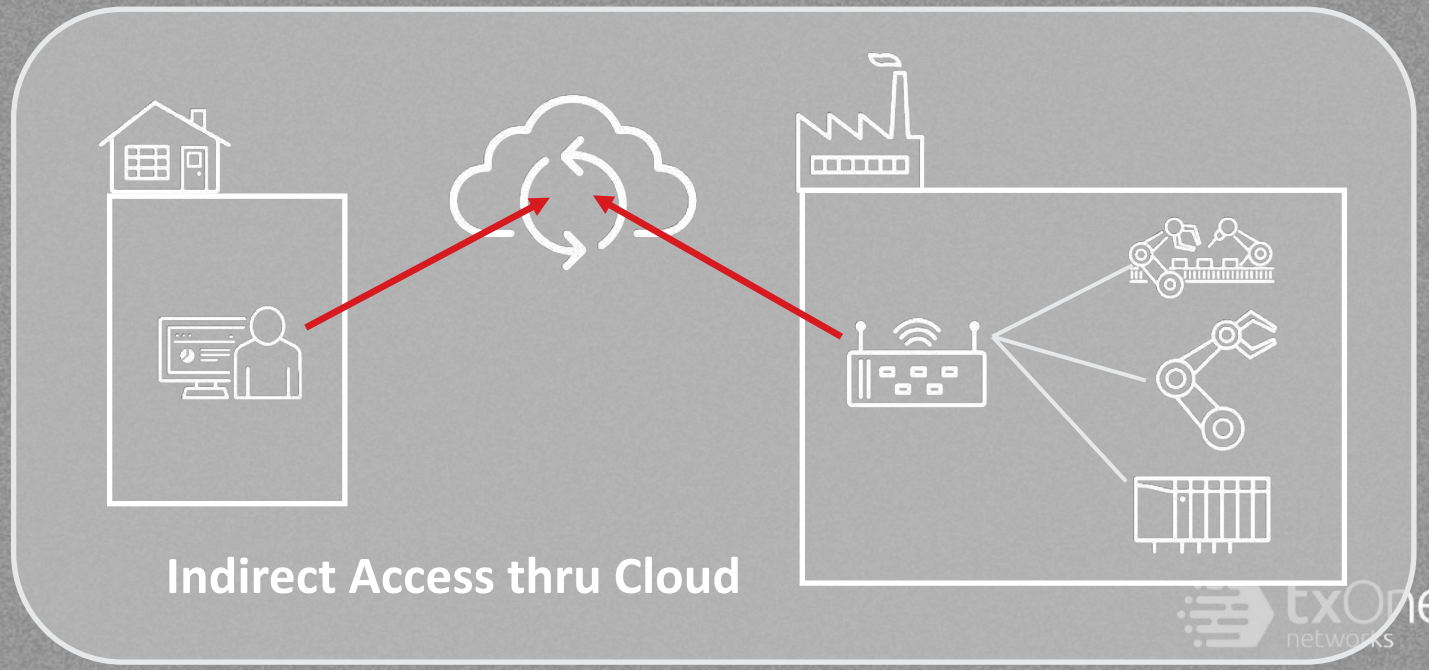
Remote Access – COVID makes it worse

Use Cases

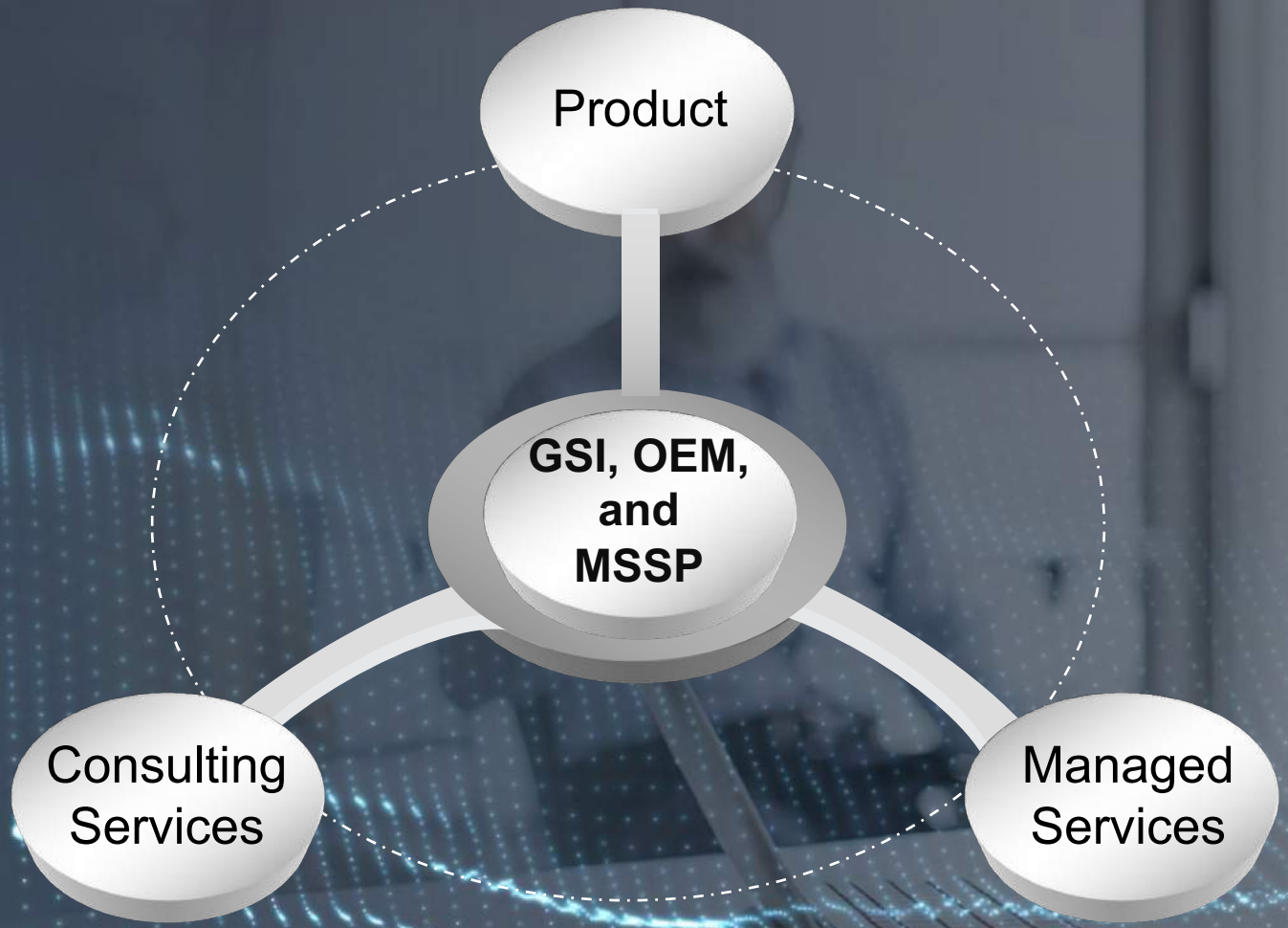
- For Customer (and Boss):
  Wants to know the utilization, progress, and even recipes and parameters in real-time
- For Equipment vendor:
  Cannot send technician to do on-site support and need remote access and control

”Direct Remote Access” is risky

- Vulnerability of VPN and RDP gateways
- Weak Authentication of VPN and RDP
- Loss of visibility through VPN
- Loss of control through RDP



Service-Oriented Value Proposition



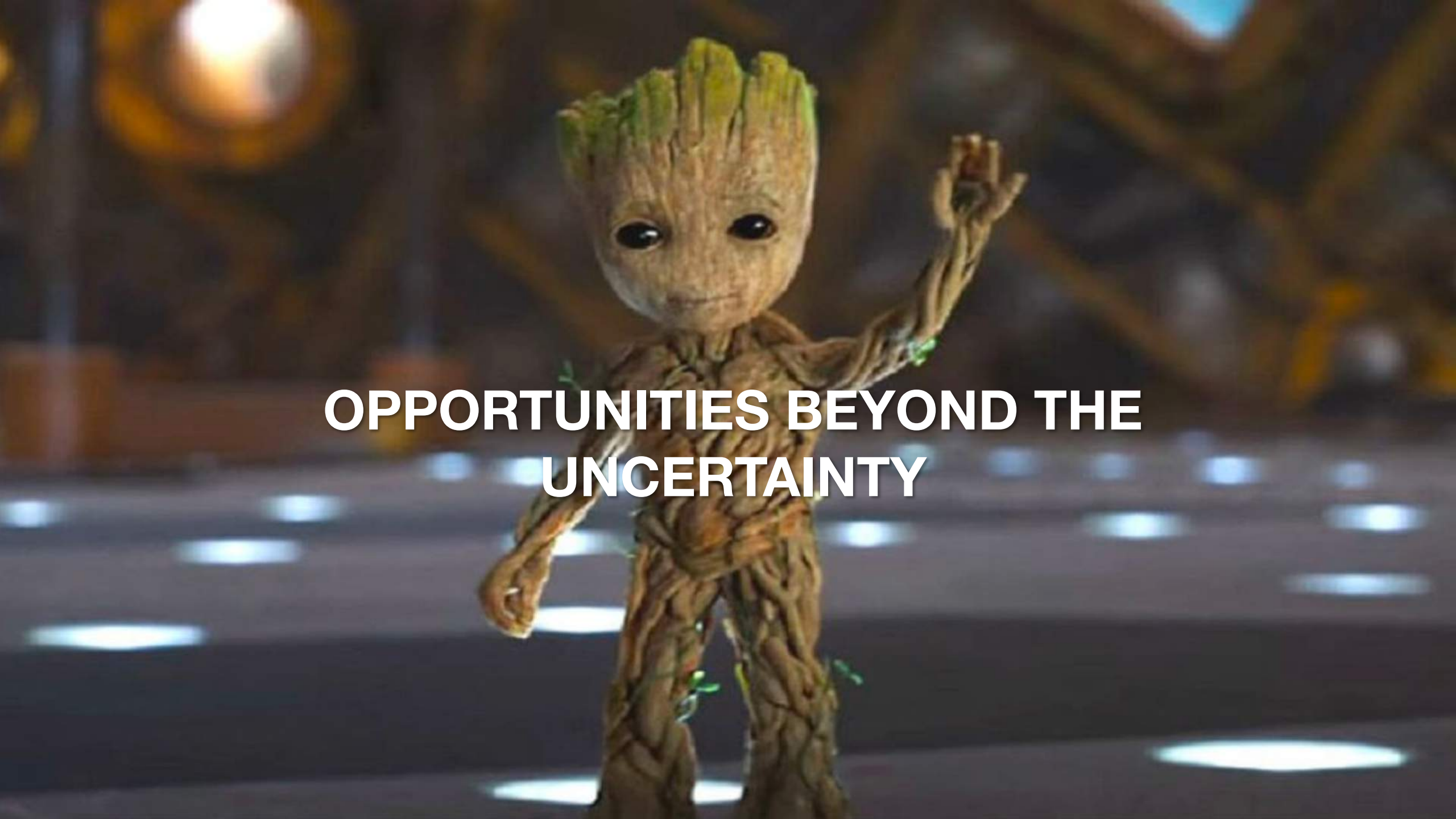
Product
- 20% Margin

Service
- 3x+ Margin

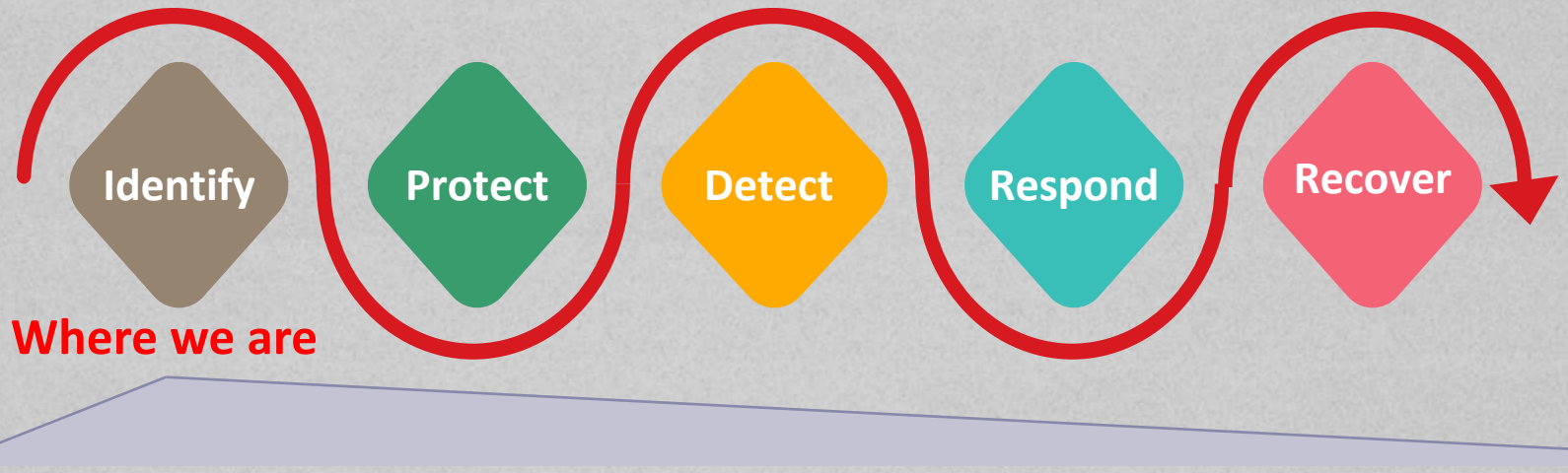
Consulting Services
- Cybersecurity Architecture & Design Services

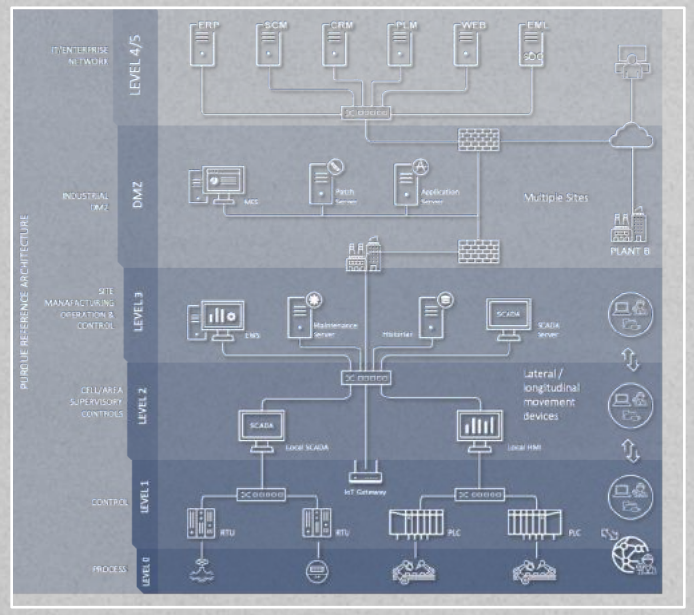
Managed Services
- Ongoing Maintenance
- IR & Forensics

txOne networks


OPPORTUNITIES BEYOND THE
UNCERTAINTY

NIST Cybersecurity Framework





Asset Discovery & Network Visualization

Discover assets & visualize the ICS network with passive & active monitoring

Vulnerability Assessment

Know where vulnerabilities are and how assets may be compromised

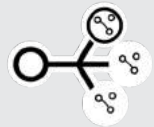
txOne networks


This is our priority:
Availability
Confidentiality
Integrity
Keep the Operation Running
Last Line of Defense
• Protect Operations
• OT-specific Knowledge
• Quickest Recovery
txOne networks

Endpoint and Network Protection

ICS Endpoint Protection

- Lightweight and doesn't impact the operation
- Identify and secure critical processes
- Cannot require frequent updates
- Very low rate of false positives



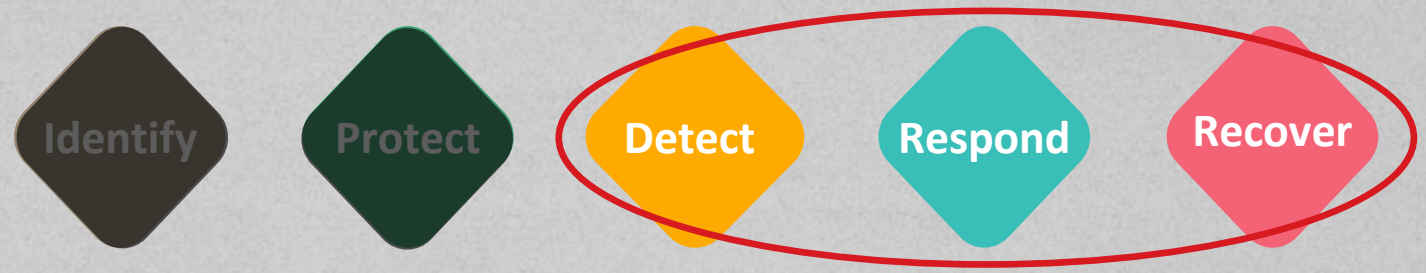
ICS Network Segmentation

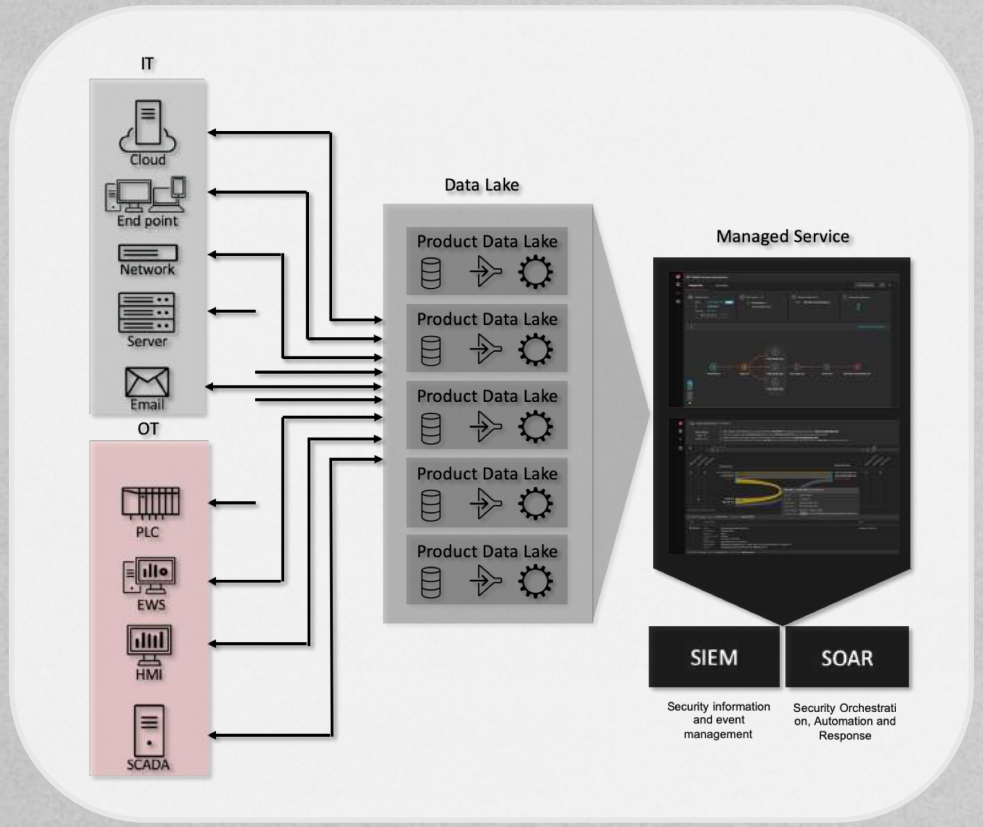
- Lightweight and doesn't impact the operation
- Meet a bunch of hardware requirements
- Shield not only system vulnerabilities but also ICS protocols and control commands in order to secure critical processes

Keep the Operation Running

txOne networks

Detection, Response, and Recover





Before

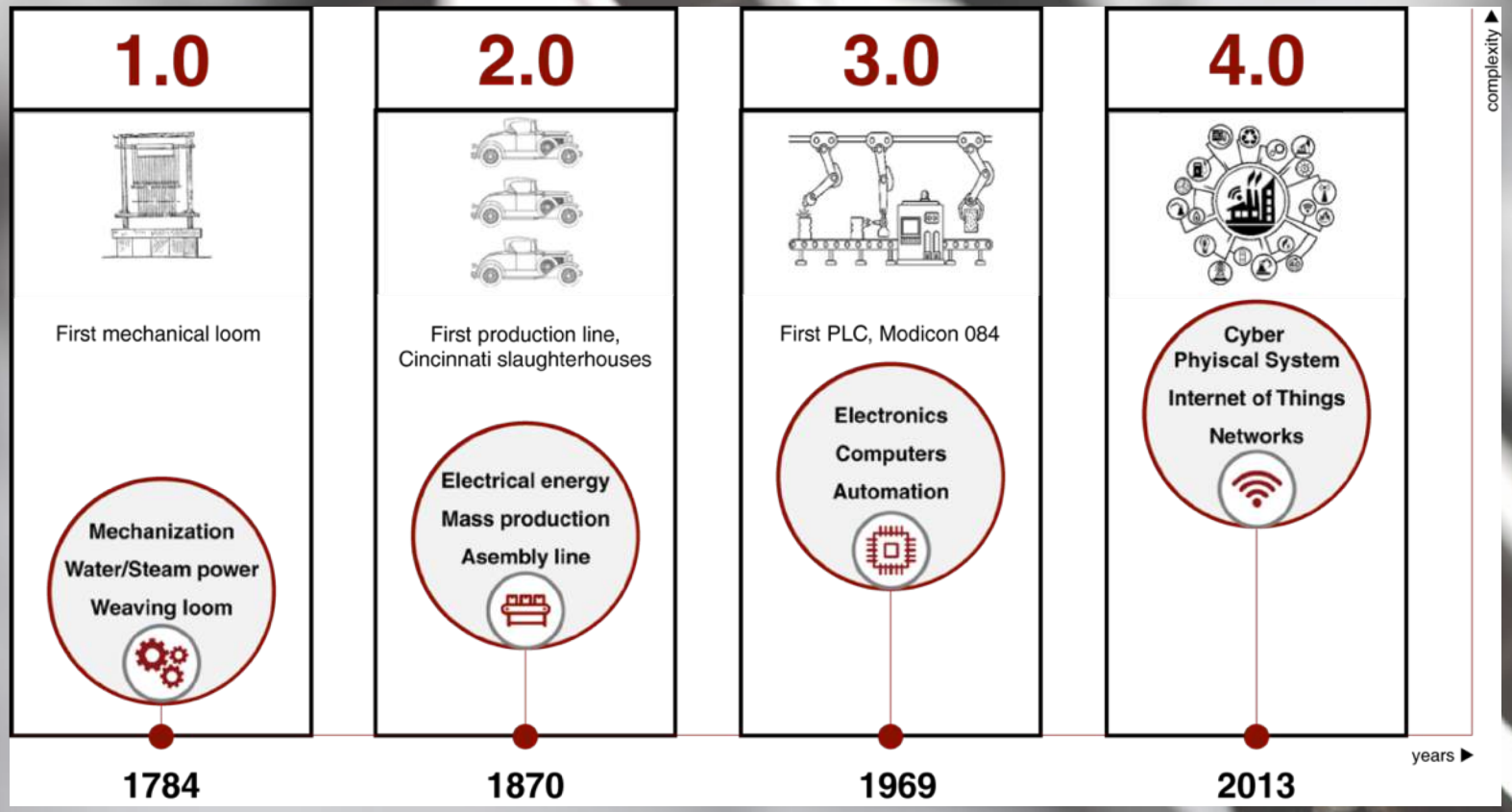
- OT anomalies and telemetry
- Full visibility across the Enterprise

During and After

- Analysis and Investigation
- Remediation and mitigation
- Back up and restore

txOne networks

We are still in the very Beginning



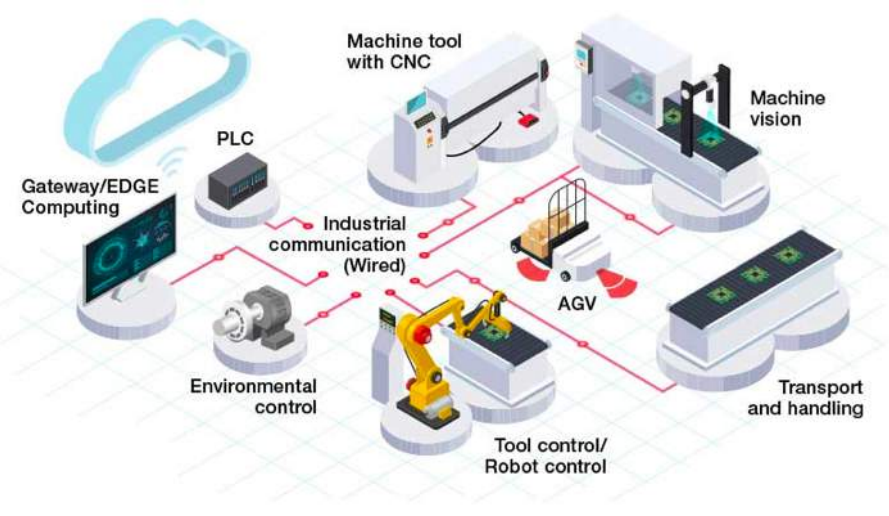
- OT is being weaponized with IT technologies
- But they have different capability, capacity, and maturity of IT technology
- The journey of OT Cyber just starts

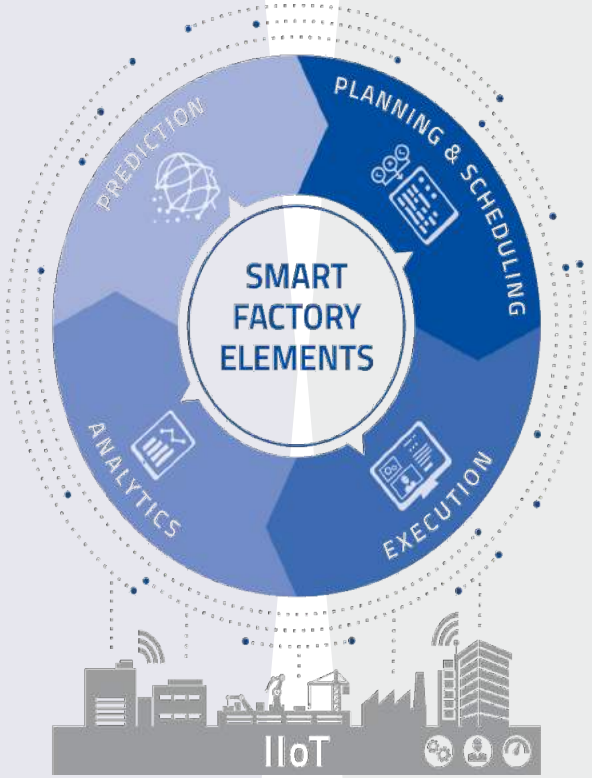
txOne networks

COMPUTING

Virtualization, Private Cloud, and Edge Computing

- Imagine in addition to OT servers, all workstations and PLCs will be virtualized and running on COTS hardware
- Edge Cloud





CONNECTIVITY

Time-Sensitive Network (TSN), 5G, Wifi6

Remotely controlling
- High Bandwidth (5G eMBB)
- Low Latency (5G URLLC)

Communication inside the digital factory
- Wifi6

Time-critical, reliable process optimization
- Low Latency - TSN

Cost-saving for outdoor connectivity
- High Coverage – 5G mMTC

Perfect Storm for OT Cybersecurity

- OT is NOT air-gapped anymore as enterprises are collecting data for cloud analysis (IIoT)
- Industry 4.0, 5G, AI/ML, Edge Computing, Digital Twin

- From 2017, OT has suffered from both non-targeted and targeted attacks
- Hackers are aware of OT weaknesses and target accordingly
- Technology of the dark side is also evolving and more impactful

- Limited number of experts who understand both OT and cybersecurity
- Lack of OT-specific products and playbooks

txOne networks

If you are in charge of OT cybersecurity:

- Focus on Operational Resilience Management
- Identify your assets and network
- Shield vulnerable and critical assets, and implement network segmentation to avoid production outage
- Adding OT visibility into the SIEM/SOC
- Hire experts (internal or external)

txOne networks