



TXOne Networks

OT Cybersecurity Approach for Digital Transformation Era

Business Development Director | Carl-Johan Dahlgren



TXOne Introduction

Founded in 2019



Purpose built



Vertical leader



OT/ICS threat research



Solution integration



+500



Worldwide offices

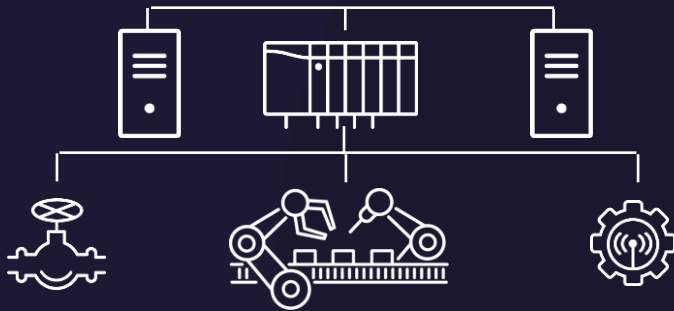




Digital Transformation

OT is in the spotlight

Air-gapped Isolation



Interconnection



More attack surfaces

The rapid change in OT

Staying Competitive

Friend become enemy. Avoid extinction

Technology Adoption

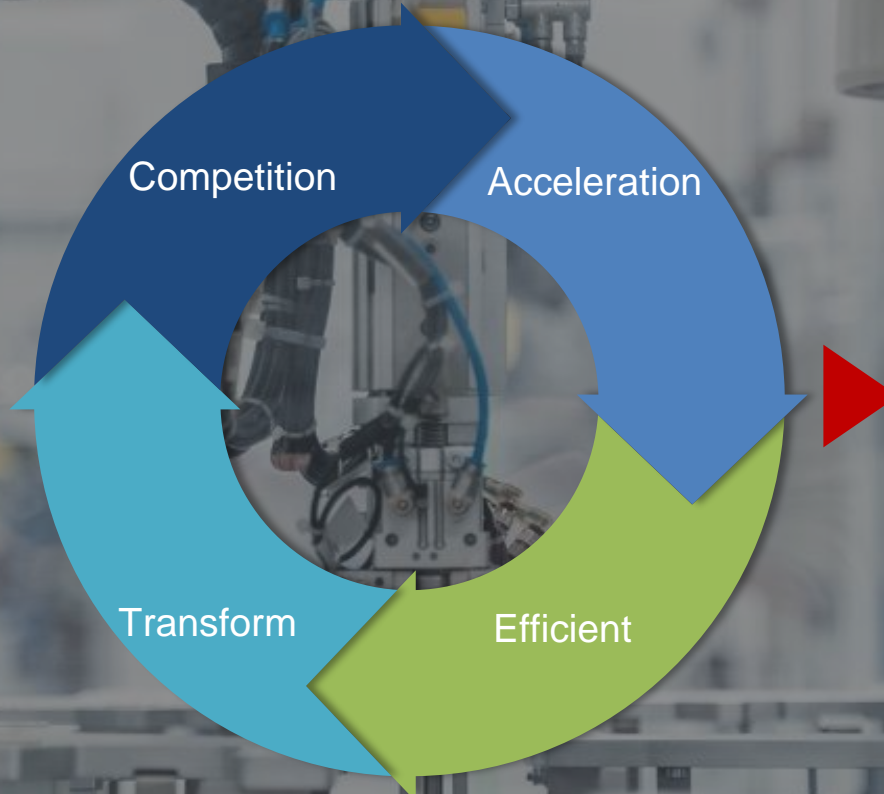
Highly adopt IT technologies for data, connectivity and computation

Digital Experience

Data flow change. Contexture data presentation

Exploring new business model

Based on data, MTO (Make to Order), ATO (Assemble-to-order)



Threat landscape change in OT

Data Flow Change

IT and OT convergence

Global Turbulence

Covid -19 accelerate the DX

Data Value

Double Extortion



OT Threat Landscape

TECHNOLOGY | Company News | News Wire

OCTOBER 31, 2022

Boeing Subsidiary Jeppesen Hit By Cyberattack

Danny Lee, Bloomberg News



The Boeing Co. logo hangs from an entrance to its factory in Sheffield, U.K., on Thursday, Oct. 25, 2018. The U.S. planemaker opened its first European factory, a 40 million-pound (\$52 million) facility that will make system-control components used for 737 and 737 Max narrowbody and 767 widebody jets. Photographer: Matthew Lloyd/Bloomberg, Bloomberg



Committees
European Parliament

Search...

Choose your committee

IMCO

Home

Meetings

Documents

Events

Supporting analyses

About

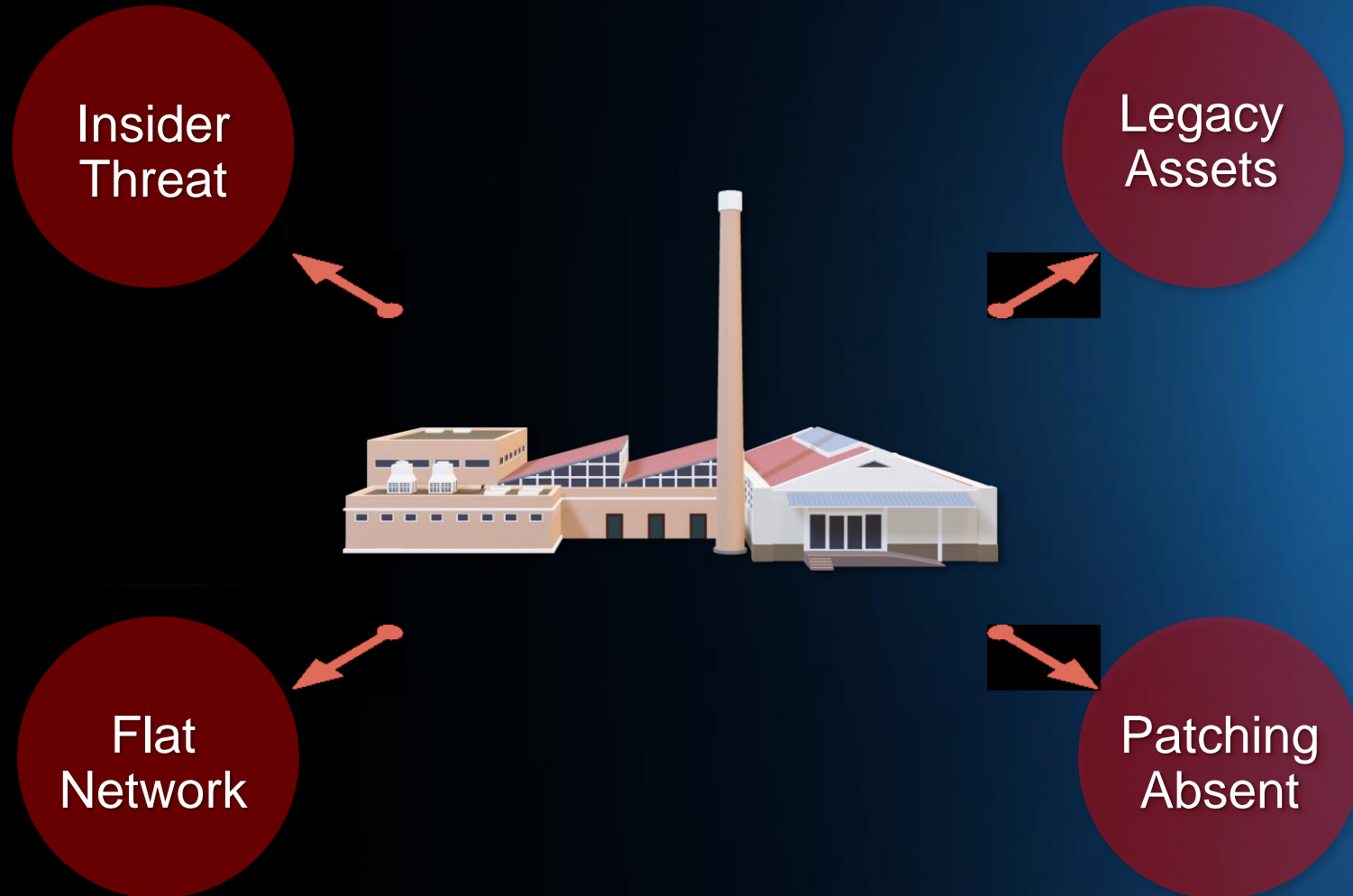
IMCO / Home / Subject files / Regulation on Machinery Products

Regulation on Machinery Products

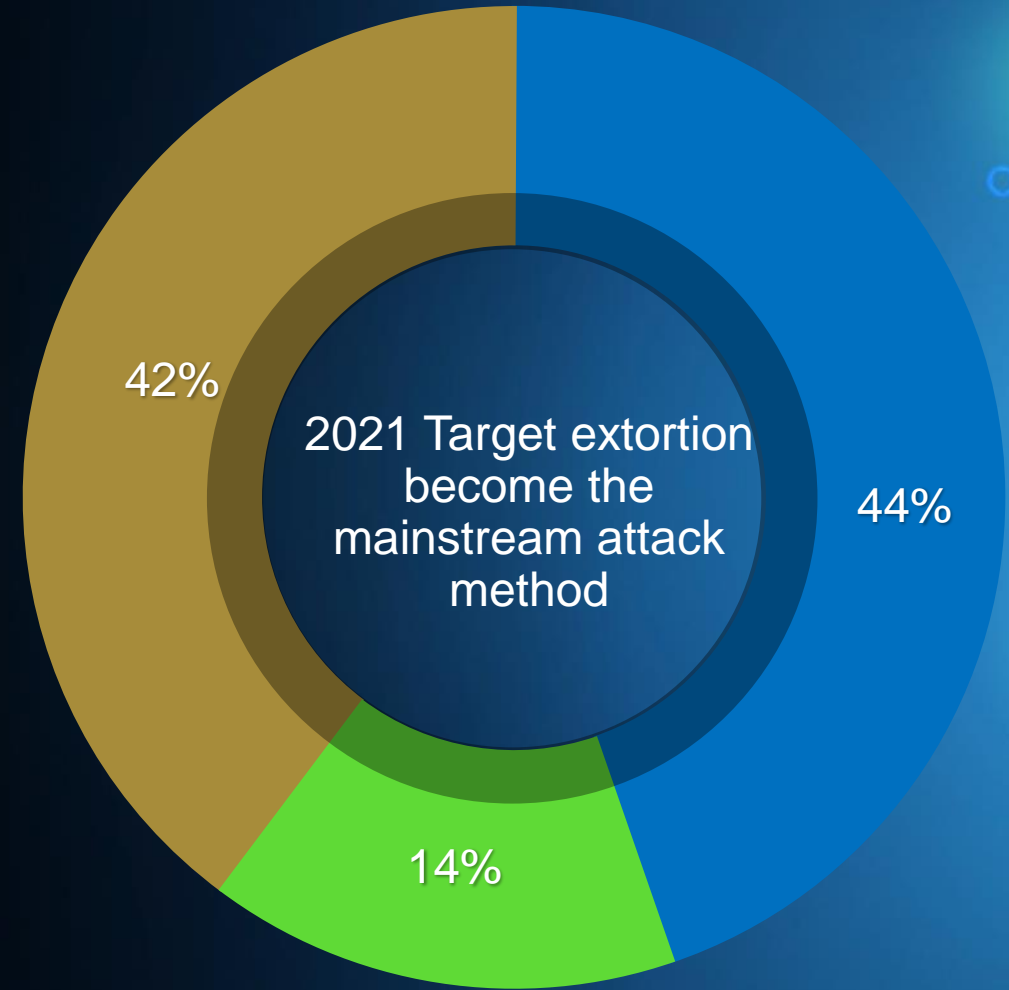
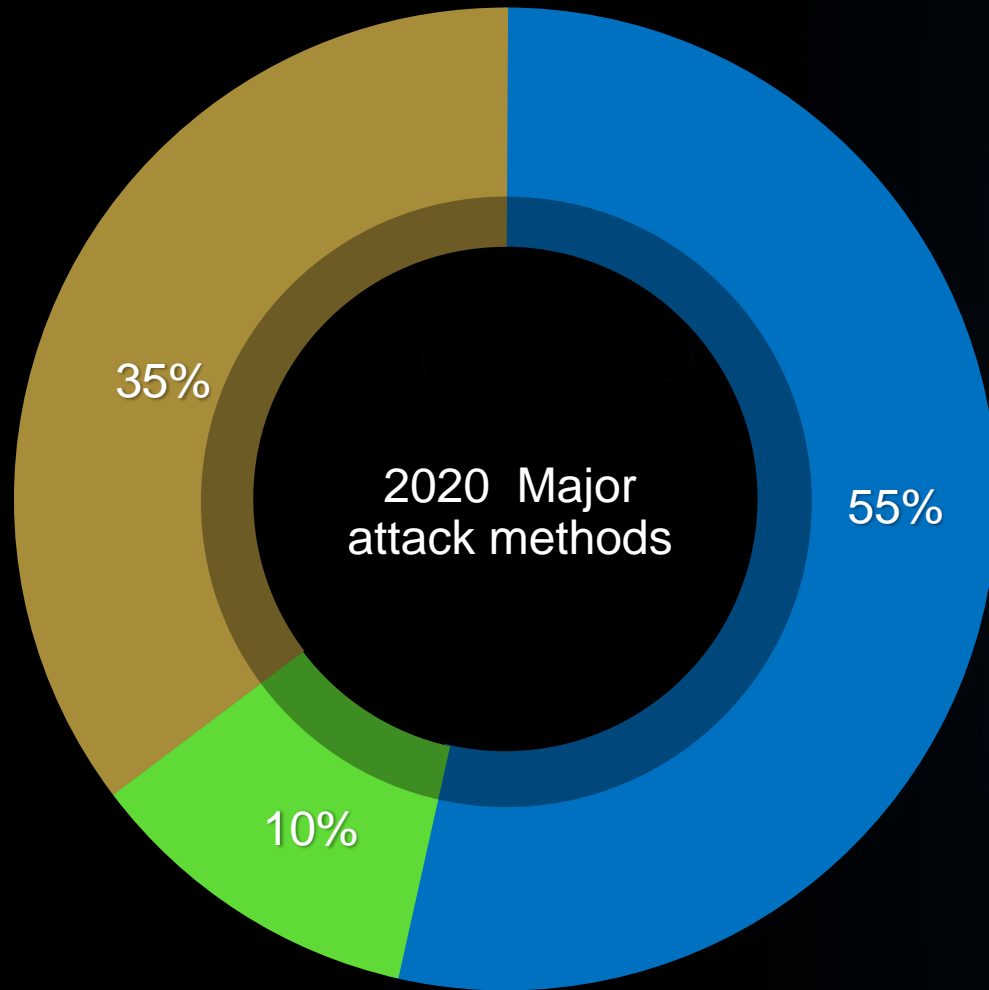
IMCO



Why OT/ICS is so vulnerable



Attack method change - Extortion becoming mainstream



● Target attack ● Target extortion ● Typical attack

Source: Trend Micro Taiwan CSIRT

This is my priority

Availability

Confidentiality

Integrity

This is my priority

Confidentiality

Integrity

Availability

But IT and OT have different priority

IT-based solutions can't help

No support
for legacy
assets

Require
constant update

Lack of OT
network
protocols
support

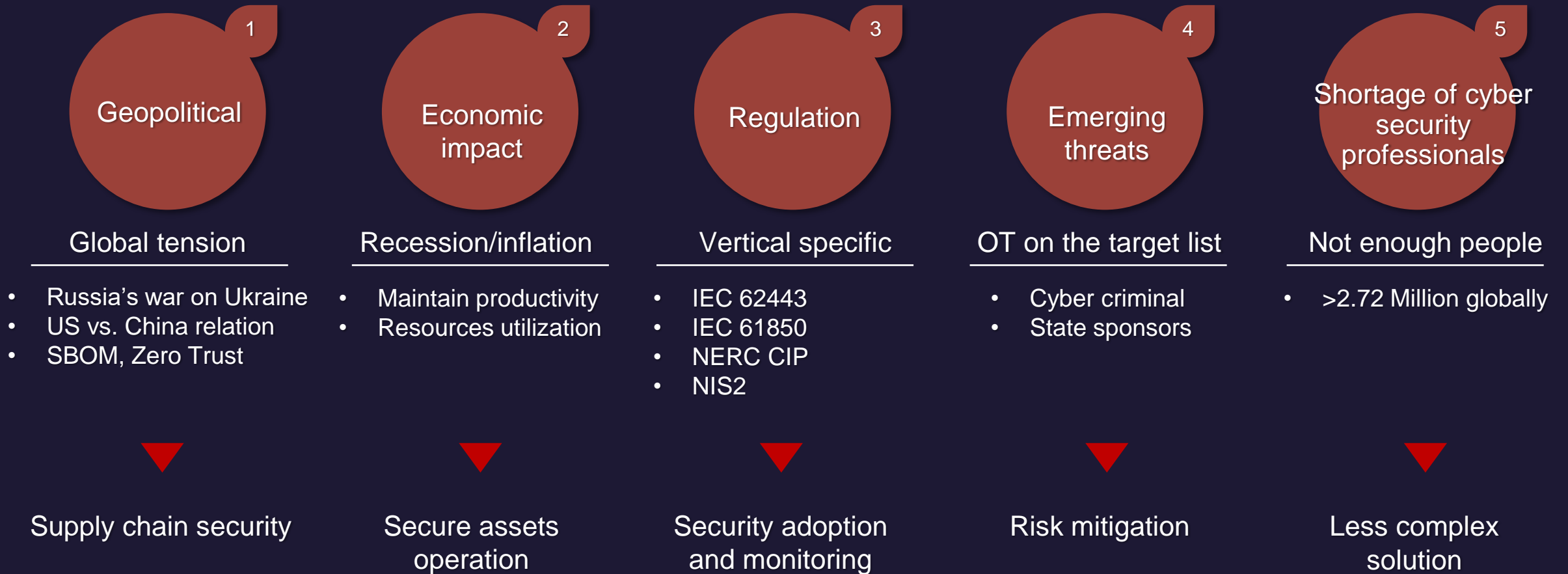
Not helping but
killing



IT cybersecurity never needs to
understand the actual operations
they're protecting

But it's essential and critical in OT

The clear and present dangers in OT cybersecurity





How TXOne can help

Asset Lifecycle Protection

Assets from Suppliers



Workforce Protection

Workload Protection

Workplace Protection

Onboarding



Staging



Production



Maintenance

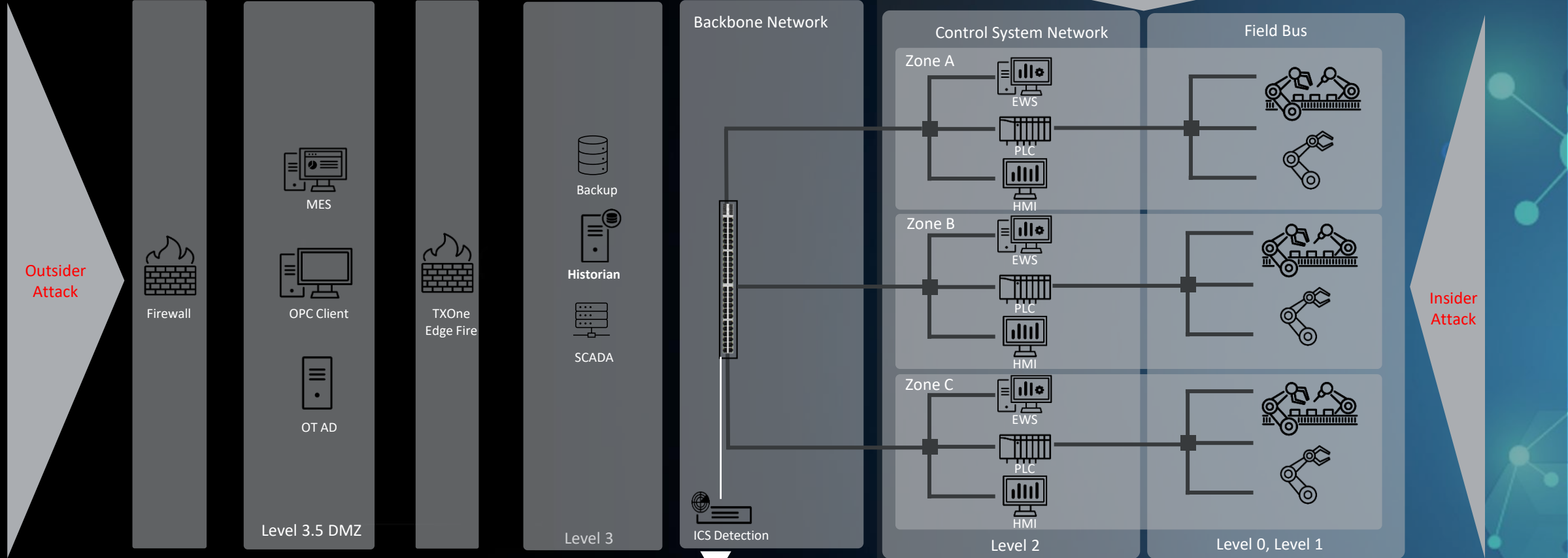


Security Inspection

Endpoint Protection

Network Defense

Security Inspection

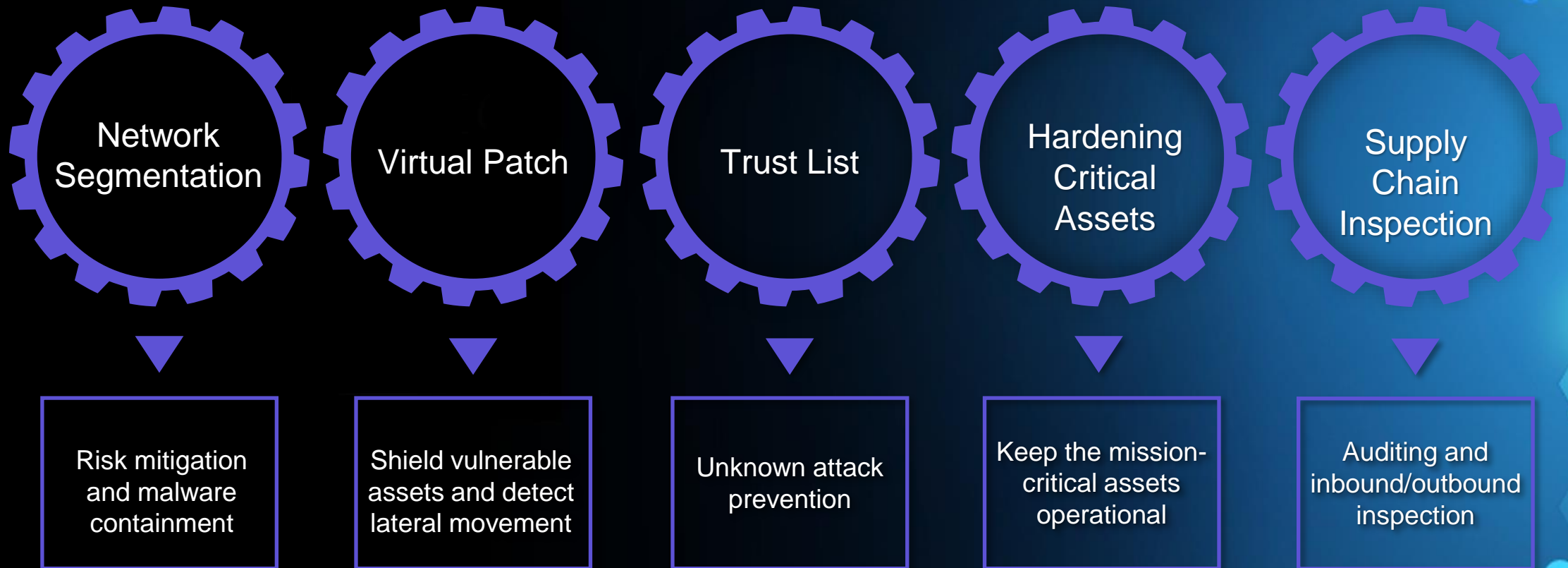


“ICS Detection” solution monitor the traffic between shop floor and control center for

- Asset visibility (in most cases)
- Can't detect cross zone attack (Blind)
- Can't prevent/protect insider attack

1. Secure shop floor deeply into the OT by effective segmentation and segregation (when perimeter defence fails)
2. Provide asset, protocol, and control command visibility on the shop floor (which could be blind to ICS Detection)
3. Provide Protection and Enforcement (while ICS Detection only detect)

Best practices ICS/OT Cybersecurity – OT Zero Trust



Thank you for your attention

Keep the operation running!

cj@txone.com