March 18, 2021

IIoT World's Manufacturing Day

The largest Industrial IoT virtual event in the world

IIoT World

Send your questions using:

#IIoTWorldDay #IIoTWorldDays

Who is attacking Smart Factories?

2:45 PM – 3:15 PM ET

Udo Schneider

Trend Micro

Lucian Fogoros

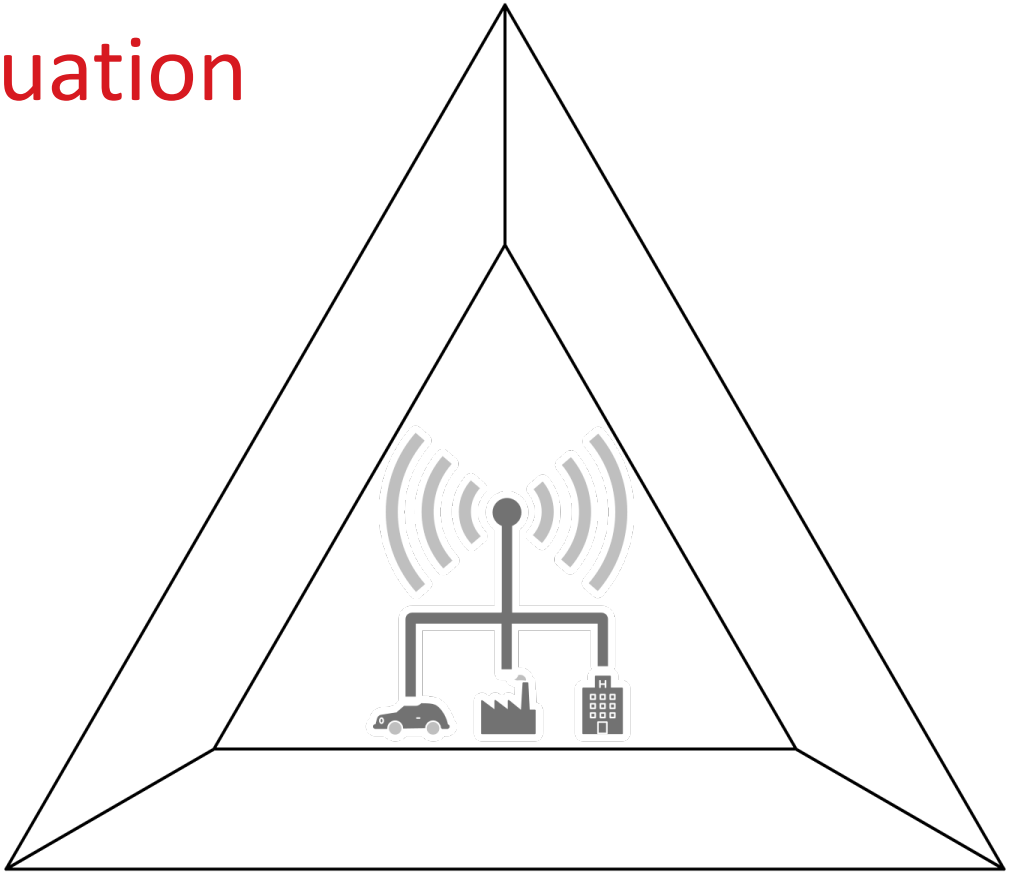
IIoT World

Chris Luecke

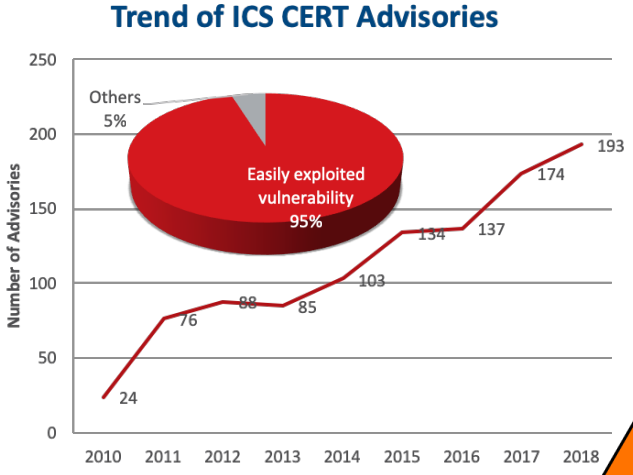
Manufacturing Happy Hour

DON’T PANIC!

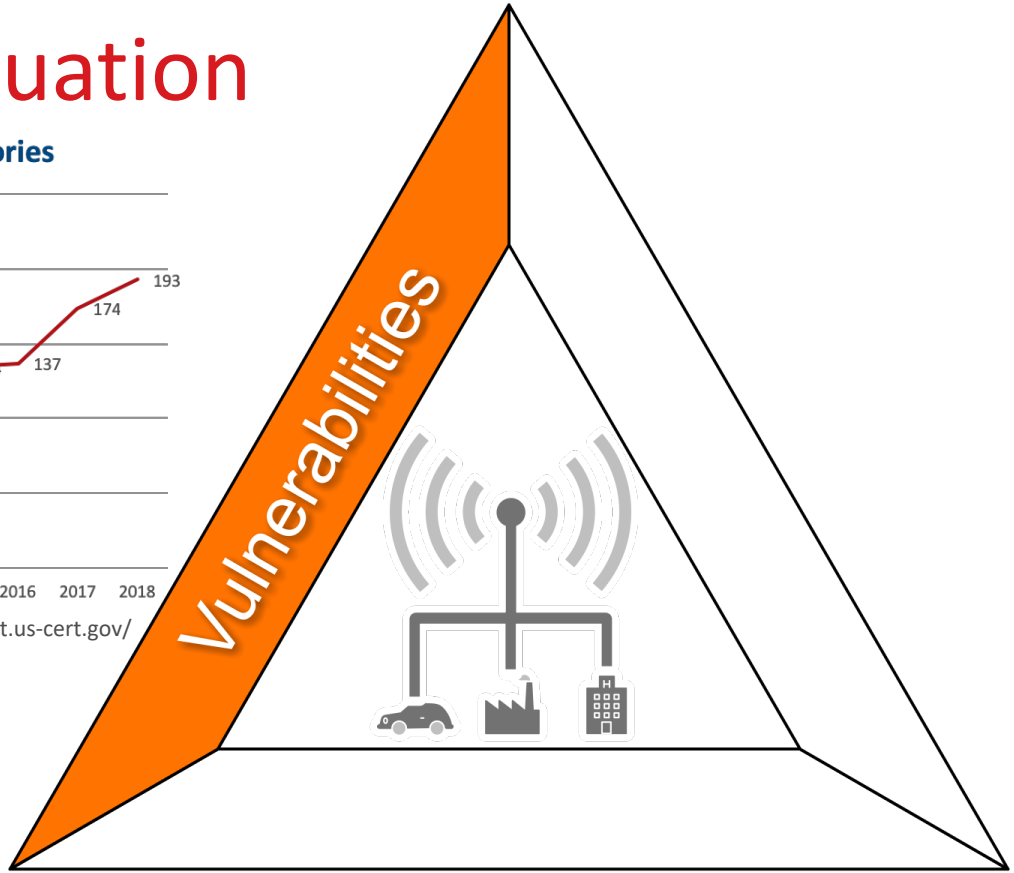
Risk Evaluation



Risk Evaluation

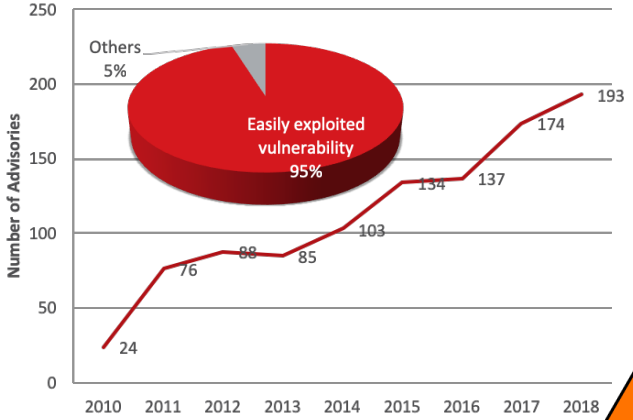


Source: (I)IoT-CERT https://ics-cert.us-cert.gov/

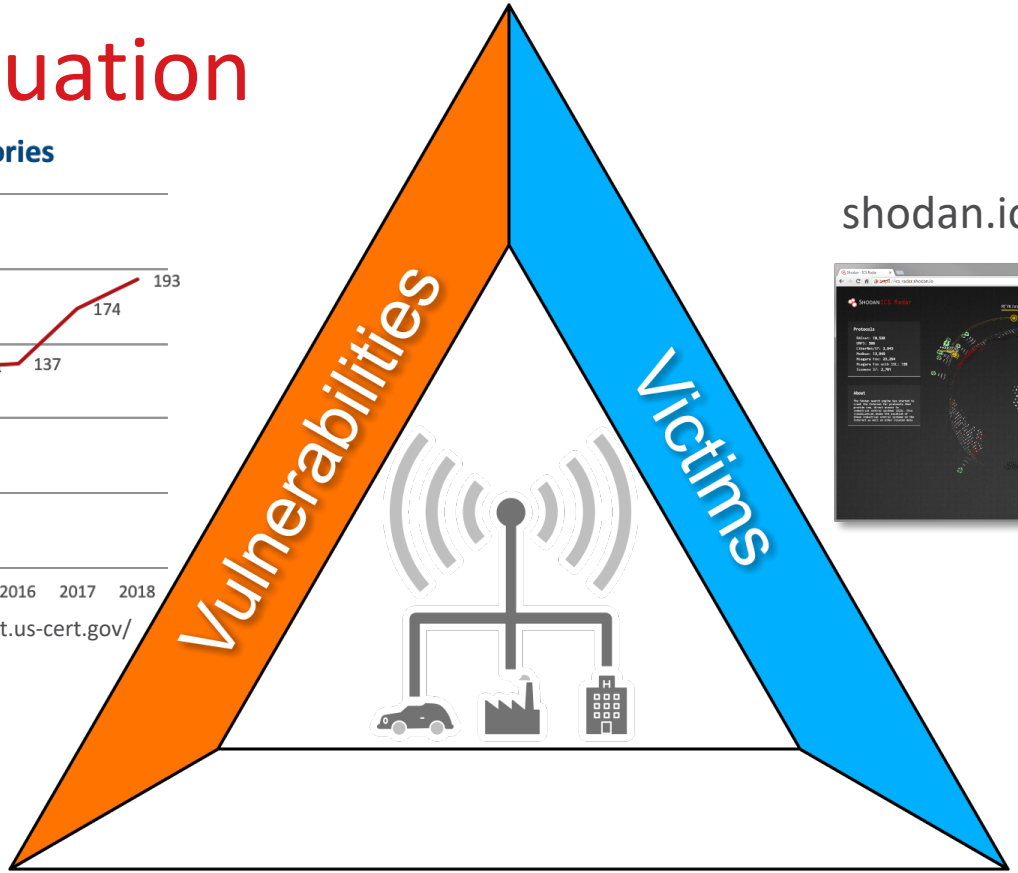


Risk Evaluation

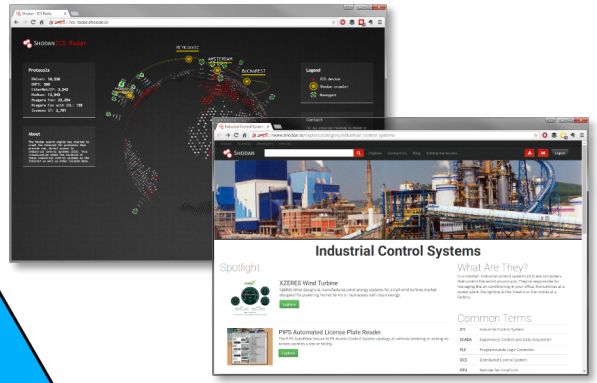
Trend of ICS CERT Advisories



Source: (I)IoT-CERT https://ics-cert.us-cert.gov/



shodan.io, Censys, ZoomEye



Threat Paradigm Shift in ICS Security

State-sponsored targeted attack

Cyber Espionage

- 2010 Stuxnet
- 2011 DUQU
- 2012 Shamoon, Flamer, Gauss
- 2013 Havex/Dragonfly
- 2014 BlackEnergy 3
- 2015 Industroyer
- 2016 Shamoon 2
- 2017 Triton/Trisis

2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

Threat Paradigm Shift in ICS Security

State-sponsored target attack

Cyber Espionage

- 2010 Stuxnet
- 2011 DUQU
- 2012 Shamoon, Flamer, Gauss
- 2013 Havex/Dragonfly
- 2014 BlackEnergy 3
- 2015 Industroyer
- 2016 Shamoon 2
- 2017 Triton/Trisis

2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020

Non-Targeted Attack

Cybercriminals

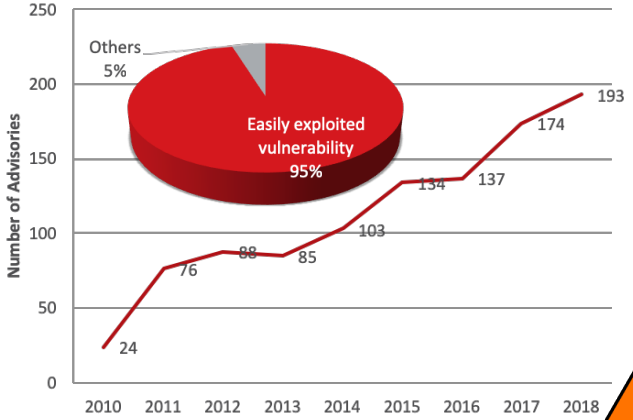
2017
WannaCry
NotPetya
Bad Rabbit

Targeted Attack

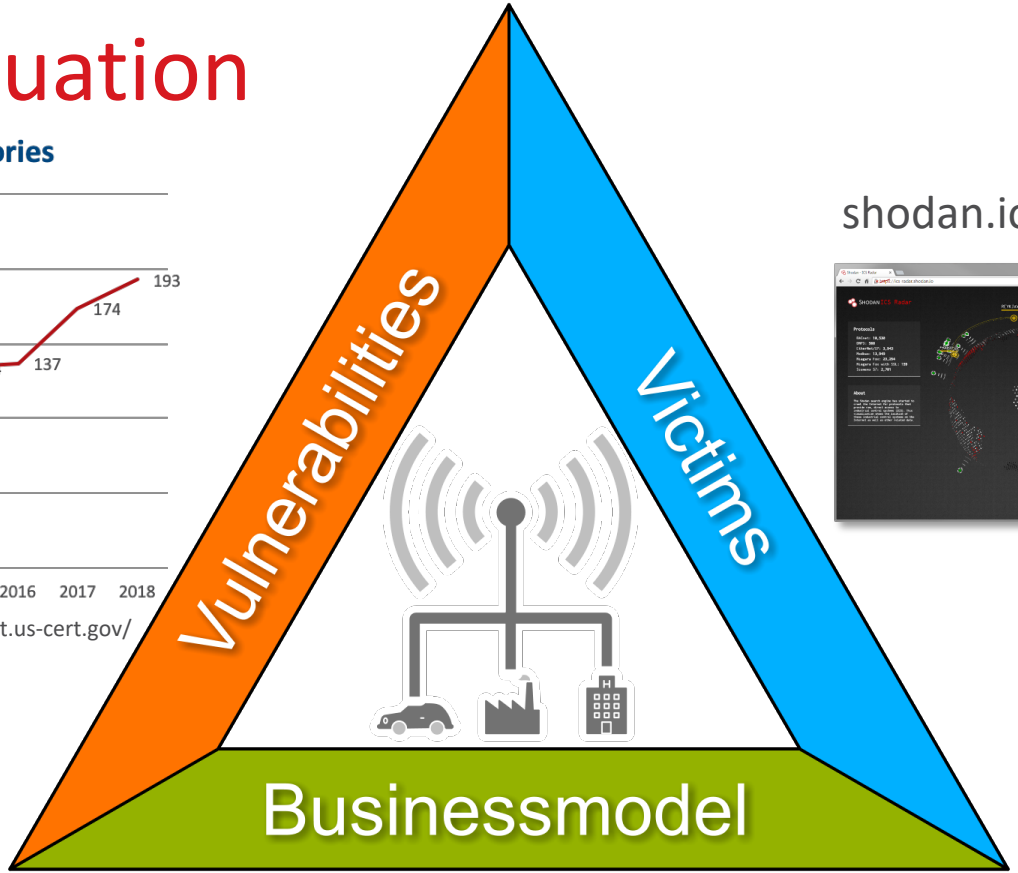
2019 - 2020
LockerGoga,
Snake/Ekans
DoppelPaymer

Risk Evaluation

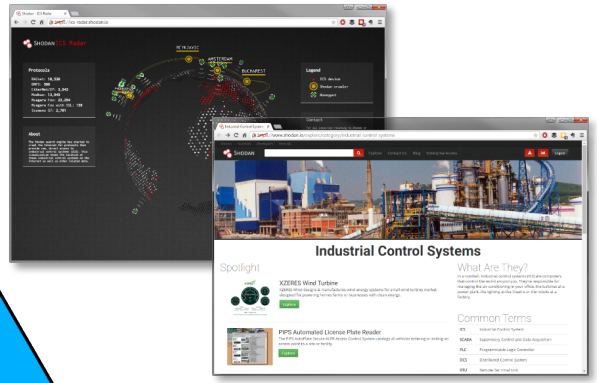
Trend of ICS CERT Advisories



Source: (I)IoT-CERT https://ics-cert.us-cert.gov/



shodan.io, Censys, ZoomEye

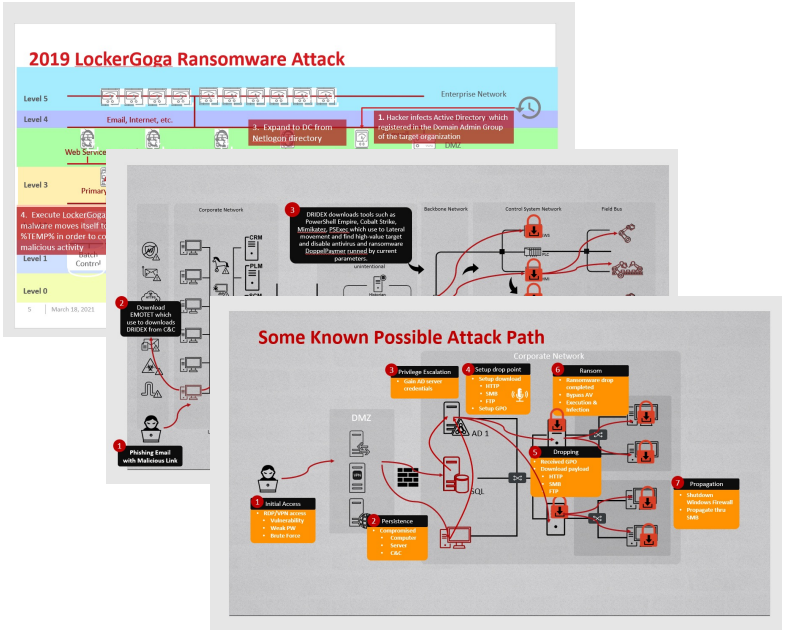


How to monetize an ICS attack

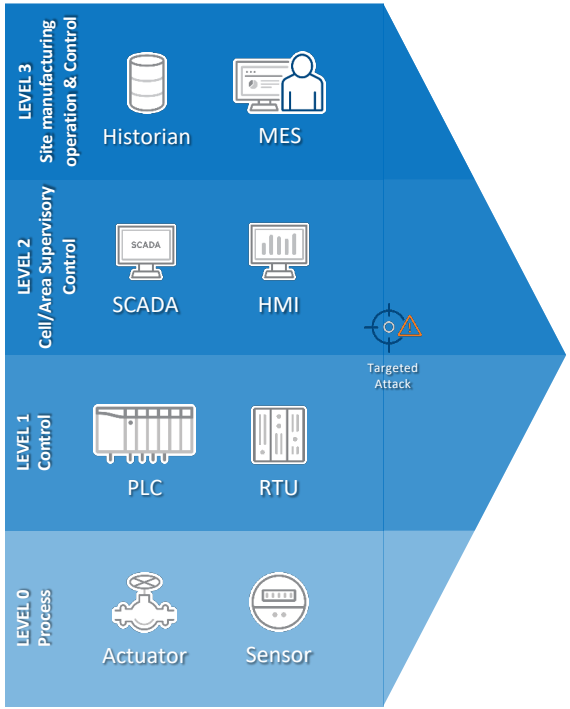
Businessmodel	Cyberthreat	ROI
„Political“ actors	DoS, Destruction	?
Industrial Espionage	Stealing interlectual property	$
Extortion	Ransomware („Lucky shot“, Office IT)	$$$
Extortion	Ransomware (Targeted Attack)	$$$$$

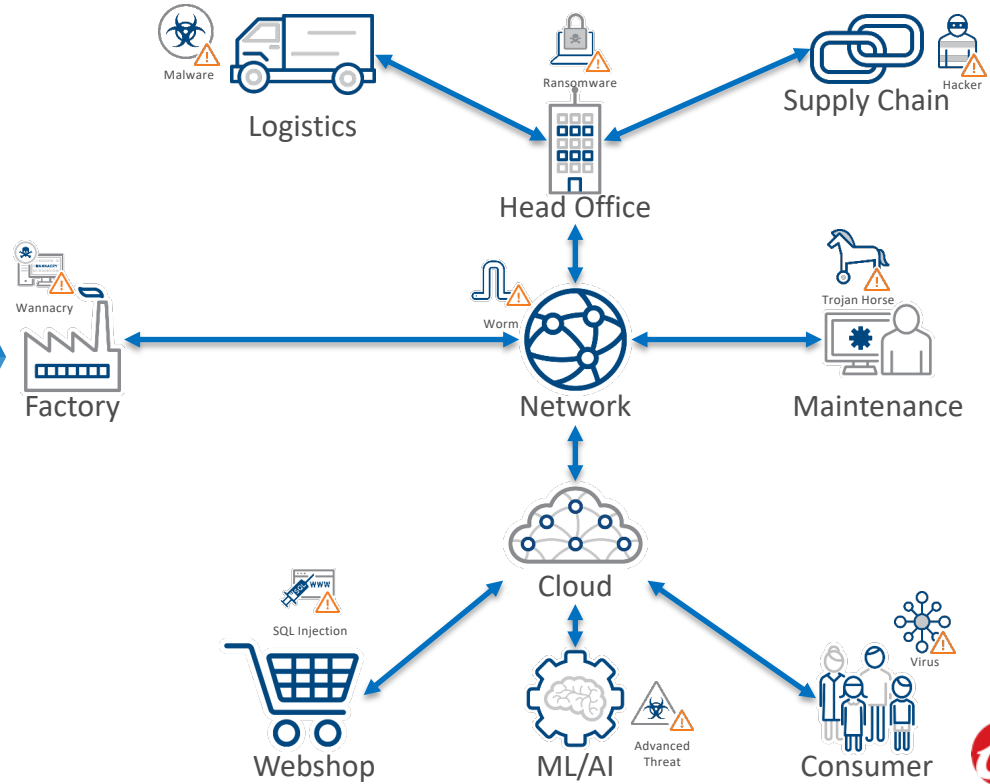
Attack vectors

- ICS specific? Nope …
- Social Engineering
  - Phishing
- Office-IT Vulnerability “du jour” (N-days)
  - EternalBlue
  - EternalKeep
  - …



Value chain threats





Cybersecurity Guidelines

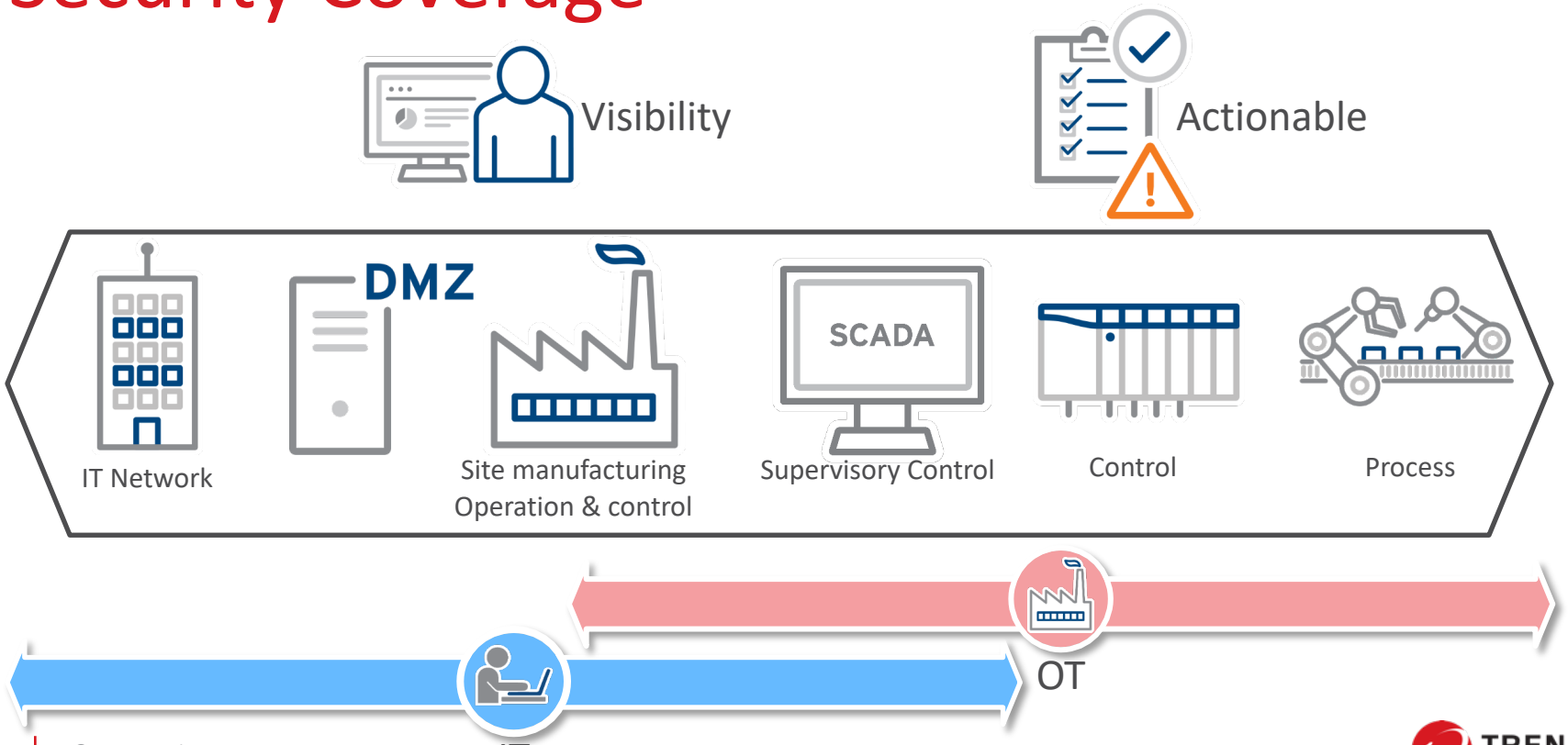
IT

OT

Compliance

Information security	
ISO/IEC 27001	Information security management system
NIST CSF, SP 800-53	Cyber security framework & SP800
ICS Security	
IEC 62443 / ISA 99	Security for industrial automation and control systems
NIST SP800-82	Guide to Industrial Control Systems Security
Board of Directors	
NACD / ISA	Director‘s Handbook on Cyber-Risk Oversight
ISA / ecoda	Cyber-Risk Oversight Handbook (for Europe)

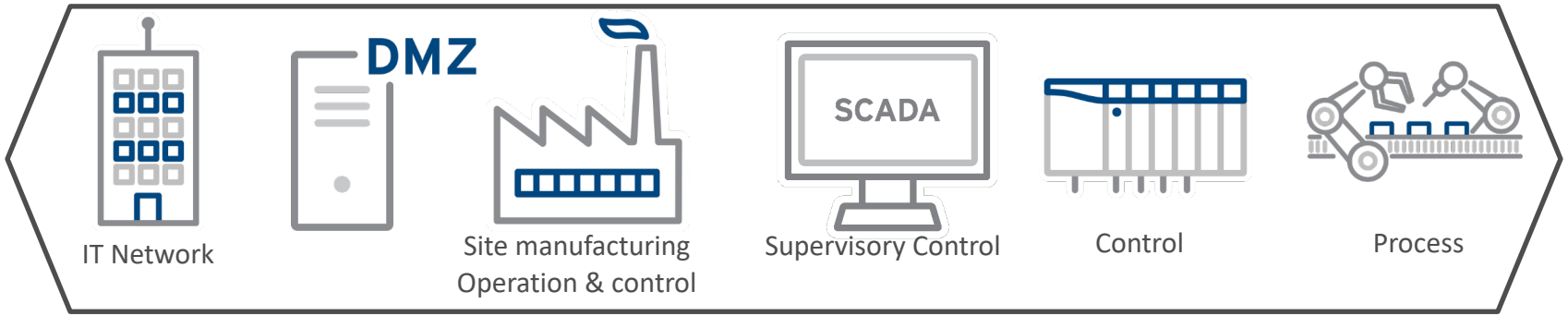
Security Coverage



Trend Micro Solutions

Trend Micro Vision One
Platform for detection & response of SOC

Cloud One
Cloud security for workload, container, file storage, conformity and network



Network One
Intrusion prevention & advanced threat protection

Apex One
Endpoint security

TX One
Network security and asset protection specialized for ICS environment

Summary

- ICS extortion is here to stay
- Technical shopfloor countermeasures are not enough!
- Security along the value/supply chain

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro deployment shifts over time—from on-premises to SaaS-based solutions. **Created with real data by artist Stefanie Posavec.**