Cybersicherheit in industriellen Umgebungen

- ist doch wie IT? Eben nicht!

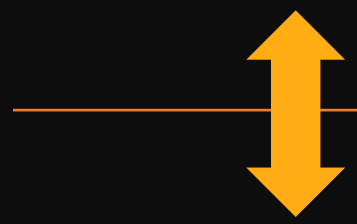
Mirco Kloss – Business Development Director DACH , TXOne Networks Europe

Agenda

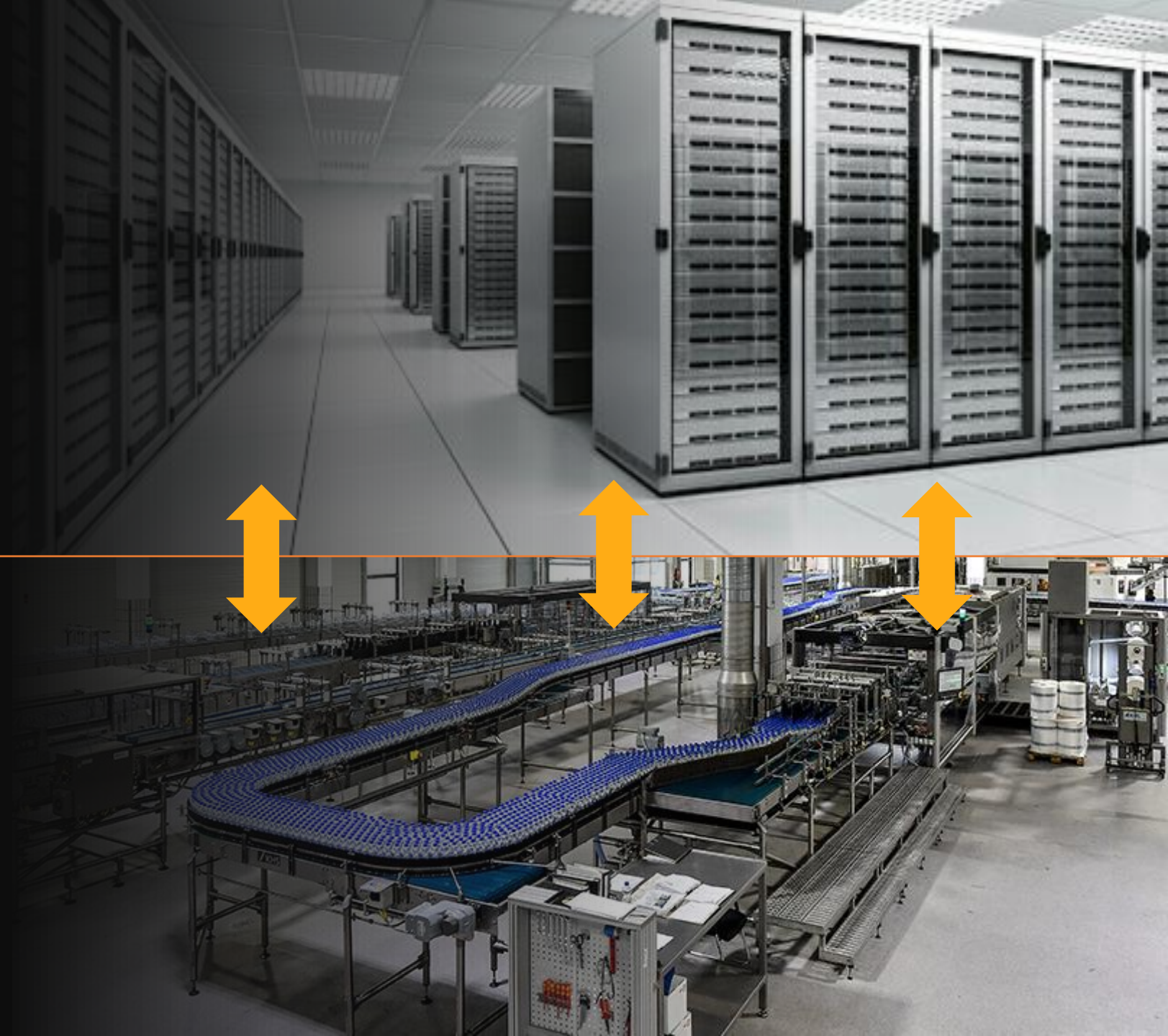
- Introduction
- Regulation
- Protection
- Q&A

Introduction

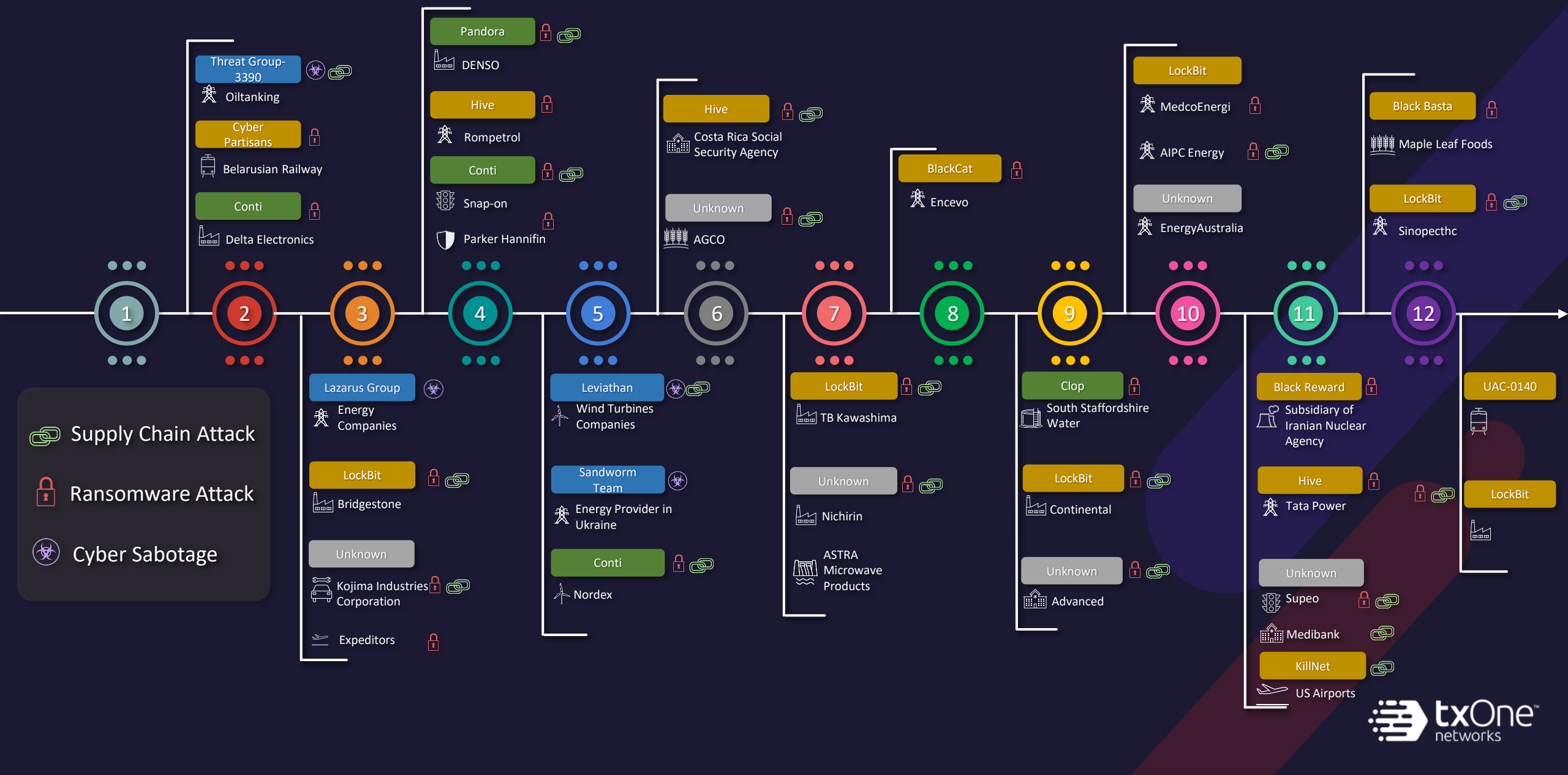
IT



OT



Diversified OT Attack Techniques in 2022



TXOne OT/ICS Cybersecurity Report 2023

https://www.txone.com/security-reports/ot-ics-cybersecurity-2023/


safety. Historically, ...
infrastructure, leveraging specialized expertise the...
of OT testbeds and protocols has aided malicious actors in the develop...
opening the floodgates for cyber criminals who no longer need specialized training to conduct deadly attacks. Now, ransomware is the most common threat in Operational Technology and Industrial Control Systems (OT/ICS) environments. In 2023, 47% of organizations reported incidents of ransomware cyberattacks. Challenges also arise from unpatched systems, a concern for 38% of organizations, while 76% fear nation-state attacks.

47% of organizations reported encountering ransomware attacks in OT/ICS security incidents in 2023.

38% of organizations faced challenges with unpatched system vulnerabilities.

76% of organizations expressed significant concerns over nation-state attacks.

The convergence of Information Technology (IT) and Operational Technology (OT) changes the terrain of the organization's entire ecosystem, necessitating a holistic defense system that can fortify this expanded attack surface. The increased interplay between Internet of Things (IoT)/OT networks and critical infrastructure, combined with inadequate safety measures in OT networks and device security, also amplifies risks. Legacy systems within OT networks add burdensome complexity to cybersecurity efforts. Globally, 97% of organizations have reported IT incidents that impact OT; 59% of organizations are at risk of OT cyber threats, with 46% having already suffered OT security incidents. Additionally, 59% of organizations continue to grapple with cybersecurity complexity.

97% of organizations reported IT security incidents also affected OT environments.

76% of organizations reported moving toward IT-OT converged networks.

59% of organizations were at risk of OT threats.

59% faced challenges due to cybersecurity complexity.

4


Ransomware Threats in OT/ICS

The inherent focus of the OT sector on automation, compared to IT, makes it more vulnerable to significant operational and financial losses, even from brief downtimes. This vulnerability has made OT industries particularly attractive to cybercriminals, as the high cost of operational disruption increases the likelihood of ransom payment.

Figure 2 from the 2023 survey reveals that the OT sector has faced a variety of security incidents, predominantly ransomware. In 2023, 47% of organizations reported experiencing ransomware cyberattacks. The United Arab Emirates (UAE) has the highest incidence rate of ransomware attacks in the OT sector at 52%, followed by significant rates in USA (51%) and other countries.

Which of the following OT security incidents have you encountered in your organization in the past 12 months?

OT Security Incidents Encountered in the Past 12 Months		OT Security Incidents			
Total (n=186)		USA (n=49)	Germany (n=48)	UAE (n=52)	Japan (n=37)
Ransomware attack	47%	51%	37%	52%	49%
Vulnerability of unpatched systems	38%	31%	59%	33%	34%
Virus or malware infiltration	37%	47%	26%	48%	27%
Advanced Persistent Threat (APT) attack	35%	31%	41%	31%	37%
Employee Actions - Human Error (unintentional)	35%	35%	31%	33%	41%
Distributed Denial of Service (DDoS) attack	30%	20%	31%	29%	39%
Phishing emails aimed to penetrate systems	27%	31%	30%	21%	27%
Identity theft, fake login credentials	22%	22%	28%	24%	12%
Employee Actions - Malicious Motives	20%	18%	31%	10%	20%
Third-party vendor or supplier compromise	13%	18%	7%	17%	10%

Source: 401 CIO respondents, Sep 2023, Frost & Sullivan

Figure 2 : OT Security Incident Types Encountered in the Past 12 Months

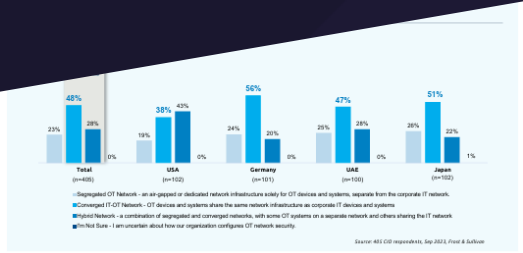


Figure 8 : Movement Toward IT And OT Converged Networks

Risks Engendered by IT/OT Convergence

Number of IT Security Incidents for Organizations Worldwide

Globally, 68% of organizations acknowledge potential IT security risks, with 56% having experienced cybersecurity incidents. A smaller portion (12%) neither encountered incidents nor conducted any assessment. In contrast, 32% reported no incidents but regularly conduct forensics and assessments, indicating a more proactive cybersecurity stance.

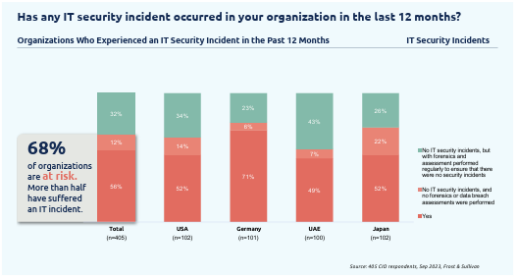
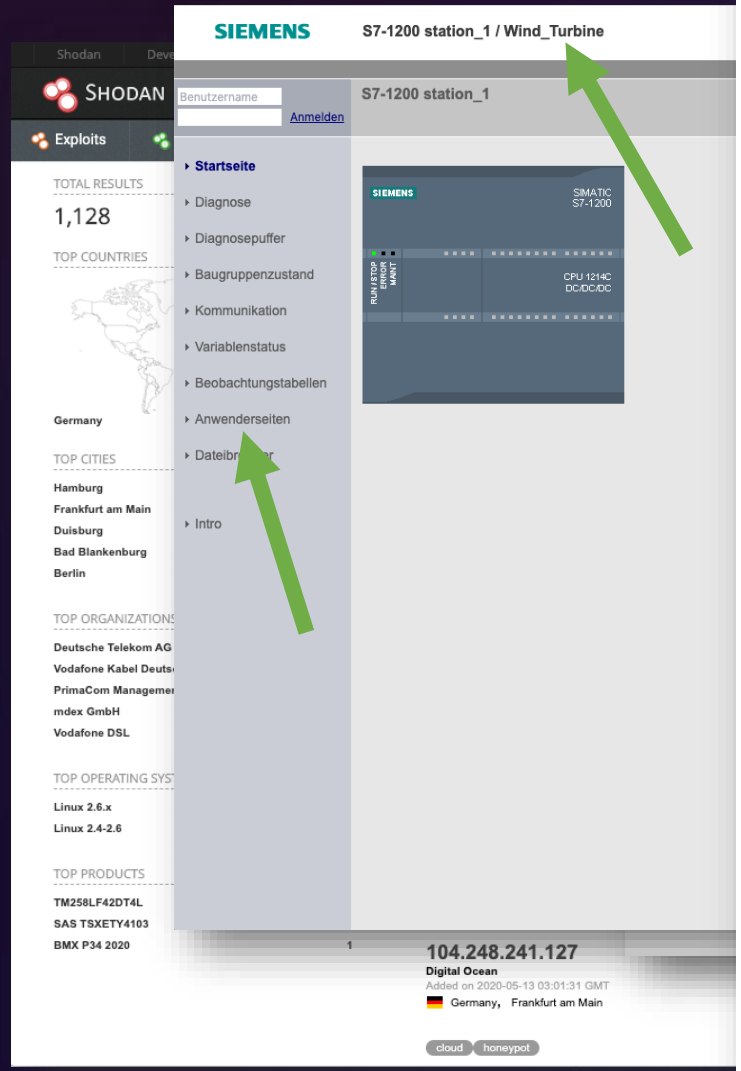


Figure 9 : IT Security Incidents Reported in 2023

16

Shodan



WIND TURBINE STATUS AND CONTROL

Power Meter		
Ua = 239.9 V	**Ub** = 239.6 V	**Uc** = 238.7 V
Ia = 58.9 A	**Ib** = 54.3 A	**Ic** = 60.5 A
P = 39.8947 kW		
S = 40.4147 kVA		
Q = -6.4619 kVAr		
PF = 0.99		
ImpWh = 41907.41 kWh		
ExpWh = 633.256 kWh		
ImpVArh = 647.736 kVArh		
ExpVArh = 40804.05 kVArh		

Turbine Parameters	
Wind Speed = 8.19	**Wind Direction** = 176
Motor RPM = 1001.77	**Main Shaft** = 45.22
Motor Temp = 13	
Bearing Temp = 37.7	
Brake Temp = 30.2	
Ambient Temp = 8	
Multiplicator Temp = 31.2	

Faults

Step = 5

Fault Code = 0

RESET

Turbine

START

STOP

START

MAN START

Rotation

CCW

STOP

CW

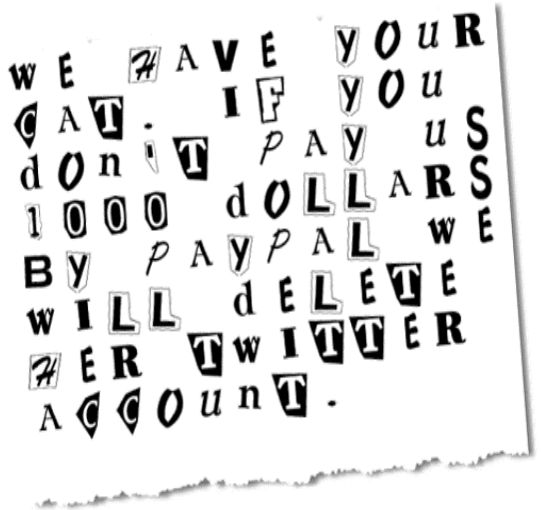
Sayano-Shushenskaya power station accident

Losses (deaths):	75 people
Property damage:	$425M
Reconstruction costs:	$1.5Bn
Reconstruction period:	2 years

https://en.wikipedia.org/wiki/Sayano-Shushenskaya_power_station_accident

Cybercrime

THIEVES

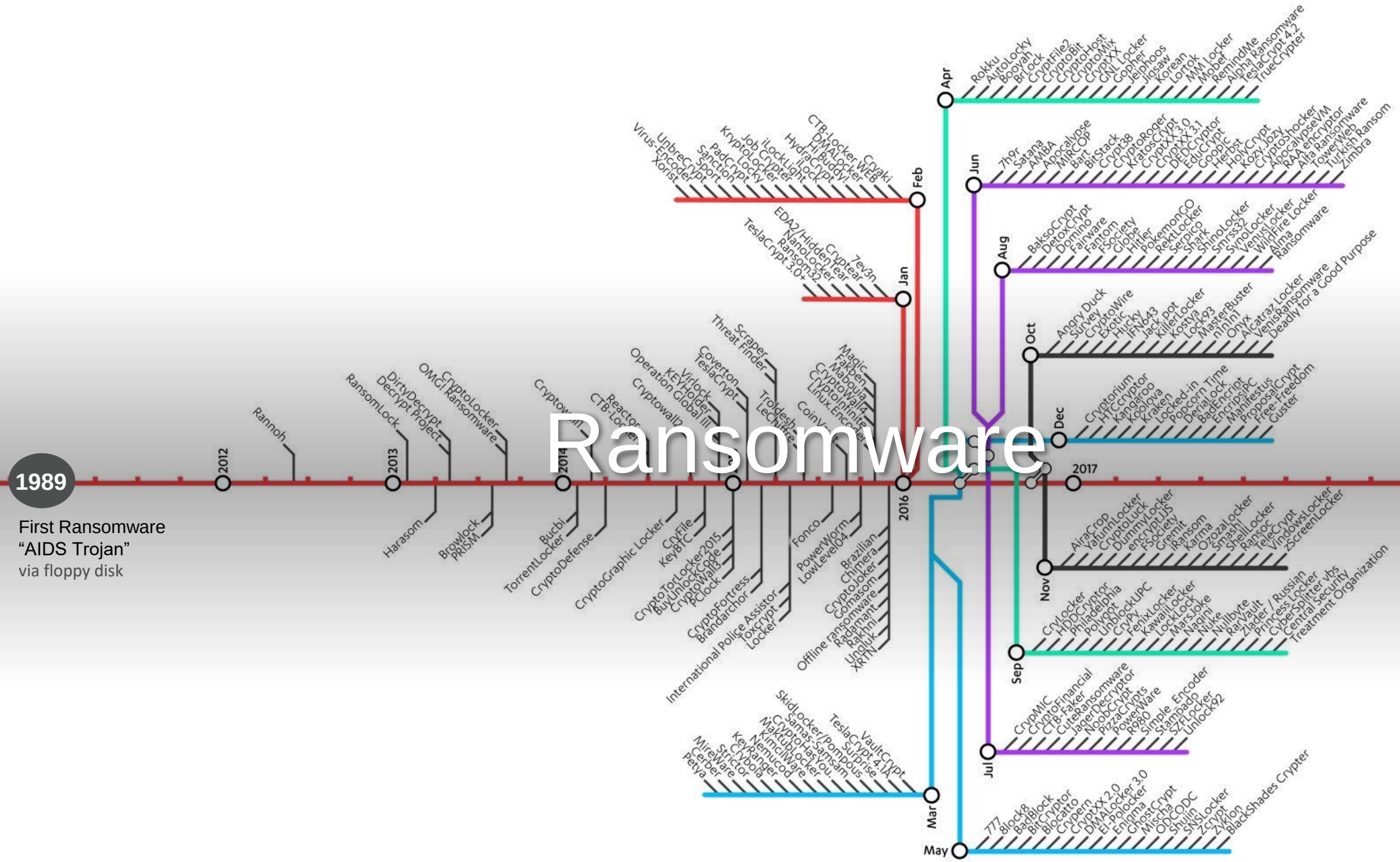


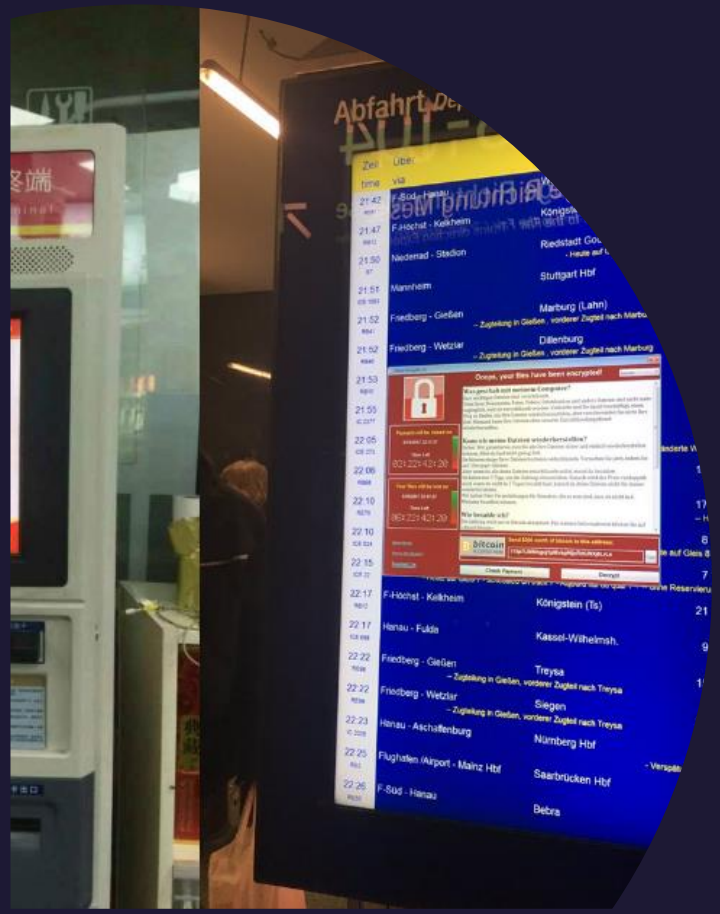
KIDNAPPER

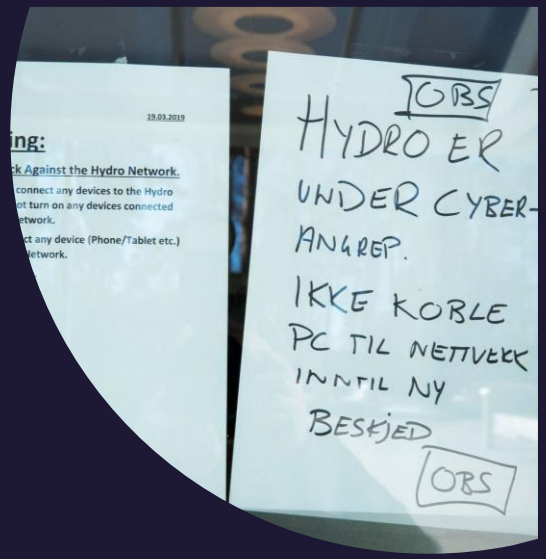
DATA BREACH

RANSOMWARE

Ransomware


1989
First Ransomware
“AIDS Trojan”
via floppy disk
2012
2013
2014
2016
2017
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Rannoh
RansomLock
DirtyDecrypt
DecrypT Project
CryptoLocker
OMG! Ransomware
Harasom
Browlock
PRISM
Bucbi
TorrentLocker
CryptoDefense
CryptoGraphic Locker
CryFile
KeyBTC
CryptoTorLocker2015
BuyUnlockCode
CryptoWall3
PClock
CryptoFortress
Brandarchor
International Police Assistor
Toxcrypt
Locker
Fonco
PowerWorm
LowLevel04
Brazilian
Chimera
CryptoJoker
Comasom
Offline ransomware
Radamant
Rakhni
Ungluk
XRTN
Scraper
Threat Finder
Coverton
TeslaCrypt
Virlock
KEYHolder
Operation Global III
Cryptowall2
Magic
FakBen
Mabouia
CryptoWall4
CryptoInfinite
Linux.Encoder1
CoinVault
Troldesh
LeChiffre
Reactor
CTB-Locker
Cryptowall
EDA2/HiddenTear
NanoLocker
Ransom32
TeslaCrypt 3.0+
7ev3n
Cryptear
CTB-Locker WEB
DMALocker
Cryaki
Hi Buddy!
HydraCrypt
iLock
iLockLight
Job Crypter
KryptoLocker
Locky
PadCrypt
Sanction
Sport
UnbreCrypt
Virus-Encoder
Xorist
SkidLocker/Pompous
TeslaCrypt 4.1A
VaultCrypt
Surprise
Samas-Samsam
CryptoHasYou
MakTubLocker
KimcilWare
Nemucod
KeyRanger
Scrypton
Strictor
MireWare
Cerber
Petya
Rokku
AutoLocky
Booyah
BrLock
CryptFile2
CryptoBit
CryptoHost
CryptoMix
CryptXX
GNL Locker
Gopher
Jeiphoos
Jigsaw
Korean
Lortok
MM Locker
Mobef
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
7h9r
Satana
AMBA
Apocalypse
MIRCOP
Bart
BitStack
Crypt38
CryptoRoger
KratosCrypt
CryptXX 3.0
CryptXX 3.1
DEDCryptor
EduCrypt
Goopic
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
ApocalypseVM
RAA encryptor
Alfa Ransomware
TowerWeb
Turkish Ransom
Zimbra
BaksoCrypt
DetoxCrypt
Domino
Fairware
Fantom
FSociety
Globe
Hitler
PokemonCO
RektLocker
Serpico
Shark
ShinoLocker
Smrss32
SynoLocker
VenusLocker
WildFire Locker
Alma
Ransomware
Angry Duck
Survey
CryptoWire
Exotic
Hucky
IFN643
Jack.pot
KillerLocker
Kostya
Lock93
MasterBuster
nnnnn
Onyx
Alcatraz Locker
VenisRansomware
Deadly for a Good Purpose
Cryptorium
HTCcryptor
Kangaroo
Koolova
Kraken
Locked-in
Popcorn Time
Derial.lock
BadEncript
EncriptsPC
Manifestus
ProposalCrypt
Free-Freedom
Guster
AiraCrop
YaLumiLocker
CryptoLuck
DummyLocker
encryptJJS
FSociety
Gremit
iRansom
Karma
OzozaLocker
Smash!
ShellLocker
Ransoc
TeleCrypt
VindowsLocker
zScreenLocker
CryLocker
HDDCryptor
Philadelphia
Polyvot
UnblockUPC
CryPy
FenixLocker
KawaiiLocker
LockLock
MarsJoke
Naqni
Nuke
NullByte
RaVault
Zlader / Russian
PrincessLocker
CyberSplitter vbs
Central Security
Treatment Organization
CrypMIC
CryptoFinancial
CTB-Faker
CuteRansomware
JagerDecryptor
NoobCrypt
PizzaCrypts
PowerWare
R980
Simple_Encoder
Stampado
SZFLocker
Unlock92
777
8Block8
BadBlock
BitCryptor
Blocatto
Crypern
CryptXX 2.0
DMALocker 3.0
El-Polocker
Enigma
GhostCrypt
Mischa
ODCODC
Shujin
SNSLocker
Zcrypt
Zyklon
BlackShades Crypter





Ransomware is hitting the Economy

Regulation

Regulation and Standardization

European examples

- NIS Directive 2.0 (EU 2016/1148)
- Cybersecurity Act (EU 2019/881)
- *Cyber Resilience Act*
- *Machinery Regulation (EU 2023/1230)*

→ ENISA

National examples

- IT-Sicherheitsgesetz (IT-SiG 2.0)
- Kritische Infrastruktur (BSI-KritisV)
- Kritische Infrastruktur (APCIP)
- Informationssicherheitsgesetz (ISG)

Standardization examples

- ISO/IEC 27001 (Info Sec.)
- IEC 62443 (OT Security)
- ISO/IEC 27019 (Energy)
- ISO/SAE 21434 (Cars)

→ ISO, IEC

enisa THE EU CYBERSECURITY AGENCY

European Union Agency for Cybersecurity

NIS - Network and Information Security
BSI - Bundesamt für Sicherheit in der Informationstechnik
APCIP - Österreichisches Programm zum Schutz kritischer Infrastrukturen

ISO International Organization for Standardization (ISO)

IEC International Electrotechnical Commission (IEC)

Requirements For Critical Entities Under NIS2 As Outlined In Articles 20 & 21 & 24

Critical Security Control	EU Regulations	International Security Standards and Guidelines	
	NIS2	ISO 27001/2	IEC 62443
Governance	NIS 2 Article 7 & 20	ISO 27001:2022 Information security management systems (ISMS) A5.	IEC 62443-2-1 Establishing an IACS security program
ISMS/CSMS Scope	NIS 2 Article 7 & 21	ISO 27001:2022 Clause 4.3	IEC 62443-2-1 Element 4.3.2.2
Supply Chain Security	NIS 2 Article 12 & 21	ISO 27001:2022 Annex A.15	IEC 62443-2-4 Security program requirements for IACS service provider
Product Security	NIS 2 Articles 24 (Related to CRA)	ISO 27001:2022 A.8.28 Secure coding	IEC 62443-4-1: Product Security Development Lifecycle Requirements IEC 62443-4-2: Technical Security Requirements for IACs Components
Technology & Security capabilities	NIS 2 Article 21	ISO 27002:2022 Information security controls	IEC 62443-3-3 System security requirements and security levels

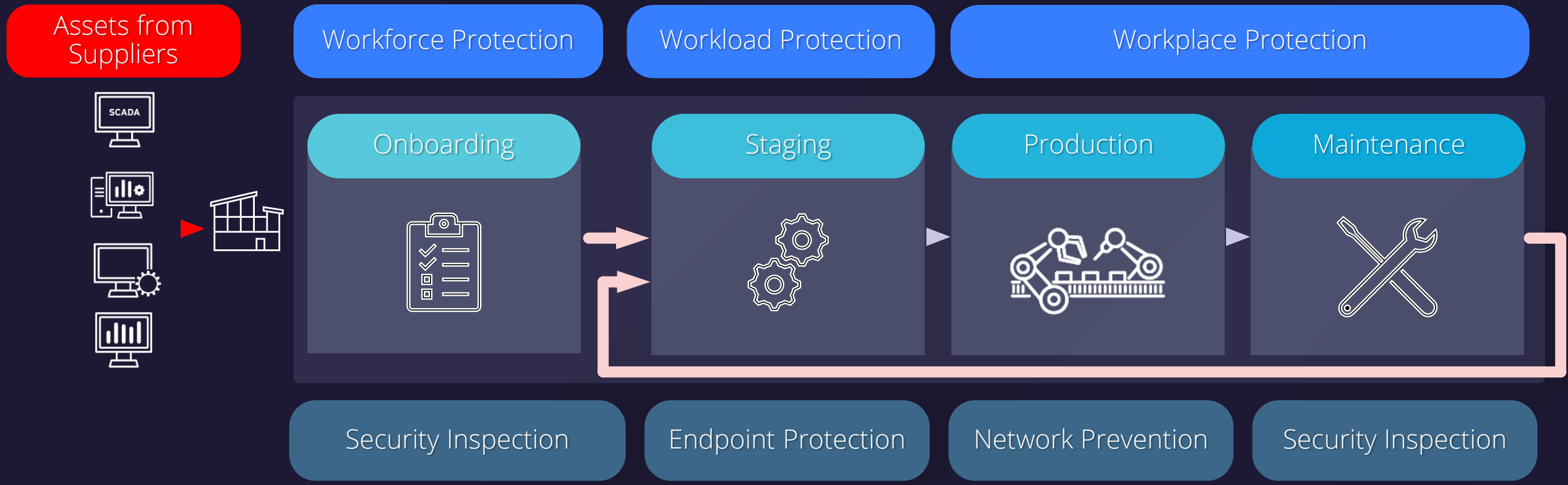
OT Lifecycle Introduced By IEC 62443

Concept of Lifecycle	Product Development Lifecycle (Build it Secure)	Automation Solution Lifecycle (Keep it Secure)
Scope	Focuses on the development of a single product from **concept to production to end-of-life**.	Encompasses the complete lifecycle of an automated solution, which may include multiple products, software, and systems integrated to solve a specific operational need.
Phases	Generally, includes stages like concept, design, prototyping, testing, production, and maintenance.	Besides the product-specific phases, it also involves an **Integration Phase** and an **Operation** and **Maintenance Phase** for the entire automation system.
Risk Management	Addresses risks related to the product such as functionality, safety, and manufacturability.	Addresses broader risks such as system compatibility, scalability, and operational downtime.
Standards	• Part 4-1: Product Security Development Lifecycle Requirements • Part 4-2: Technical Security Requirements for IACs Components	• Part 2-1: Establishing an IACS Security Program • Part 2-2: IACS Security Program Rating • Part 2-3: Patch Management in the IACS Environment • Part 2-4: Security Program Requirements for IACS Service Providers • Part 3-2: Security Risk Assessment for System Design • Part 3-3: System Security Requirements and Security Levels
Stakeholders	Primarily involves product manufacturers.	Involves a broader range of stakeholders, including system integrators, operation teams, and end-users.
Outcome	Aims for a finished product that can be manufactured and sold.	Focuses on a fully-integrated automation solution that solves specific operational problems, which may involve the integration of multiple products.

Protection

Asset Lifecycle Protection

Never trust, always verify assets on every stages



Secure the entire assets lifecycle by Zero Trust methodology

Never trust, and always verify assets at every stages

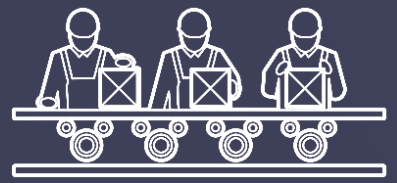
CPS Platform

Security Inspection | Endpoint Protection | Network Defense | Security Inspection

Assets from Suppliers

Onboarding

Staging



Production

Maintenance

Element

The Element portfolio

Designed for enterprise

Agentless Inspection Tool

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

Portable Inspector

Centralized Dashboard

ElementOne

Removable Media Sanitizer

Safe Port

txOne networks

TXOne Stellar – OT Endpoint Security

Multi-method threat prevention

ICS root of trust and advanced threat scan secure the OT assets with no interruption to operations

ICS Application Safeguard

Intelligently locate and secure the integrity of ICS from ICS targeted attacks
processes by device

Operations Behavior Anomaly Detection (CPSDR)

Detect abnormal operations with least privilege control to prevent malware-free attacks

Operation Lockdown

Lock down the operations efficiently reducing the chance of downtime and cost of resilience

USB Vector Control

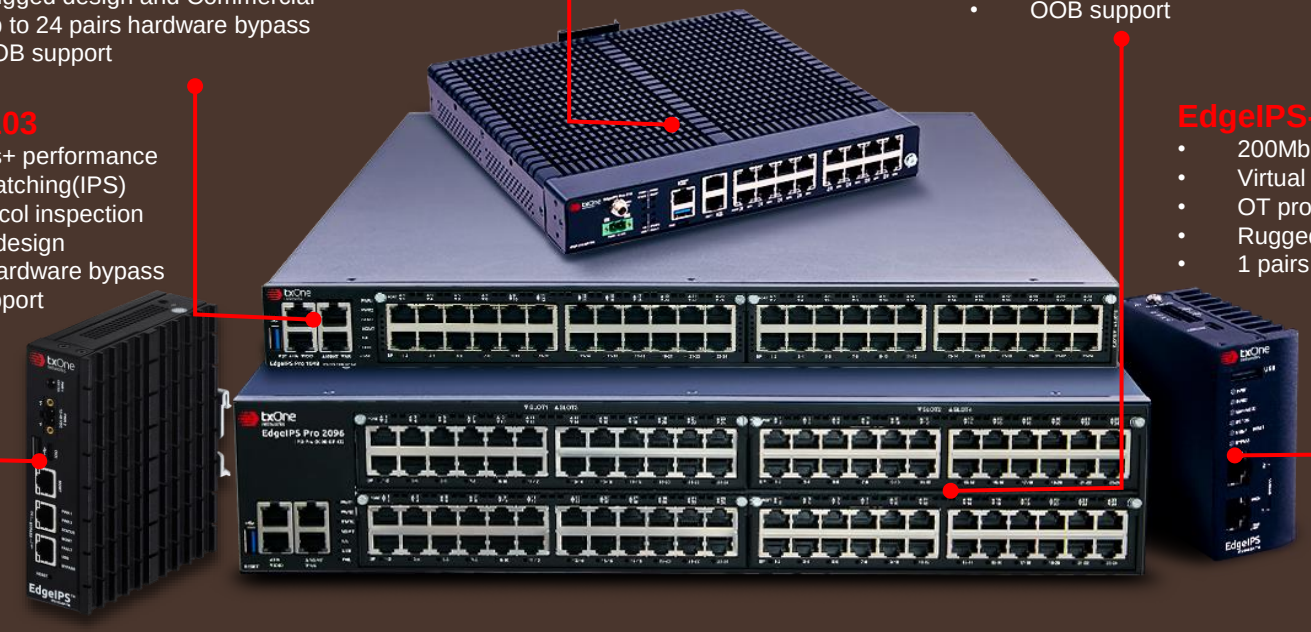
Prevent insider threats and malicious activities

TXOne Networking Solution Models

EdgeIPS Pro-1048 Gen2
- 10Gbps+ performance
- Virtual Patching(IPS) / Anvti-virus
- OT protocol inspection
- Rugged design and Commercial
- Up to 24 pairs hardware bypass
- OOB support

EdgeIPS Pro-216 R&C
- 1.8Gbps+ performance
- Virtual Patching(IPS) / Anti-virus
- OT protocol inspection
- Rugged design and Commercial
- 8 pairs hardware bypass
- OOB support

EdgeIPS Pro-2096 Gen2
- 10Gbps+ performance
- Virtual Patching(IPS) / Anvti-virus
- OT protocol inspection
- Rugged design and Commercial
- Up to 48 pairs hardware bypass
- OOB support



EdgeIPS-103
- 850Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- 1 pairs hardware bypass
- OOB support

EdgeIPS-102 Gen2
- 200Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- 1 pairs Hardware bypass

EdgeIPS LE-102
- 150Mbps+ performance
- Virtual Patching(IPS)
- 1 pairs Hardware bypass

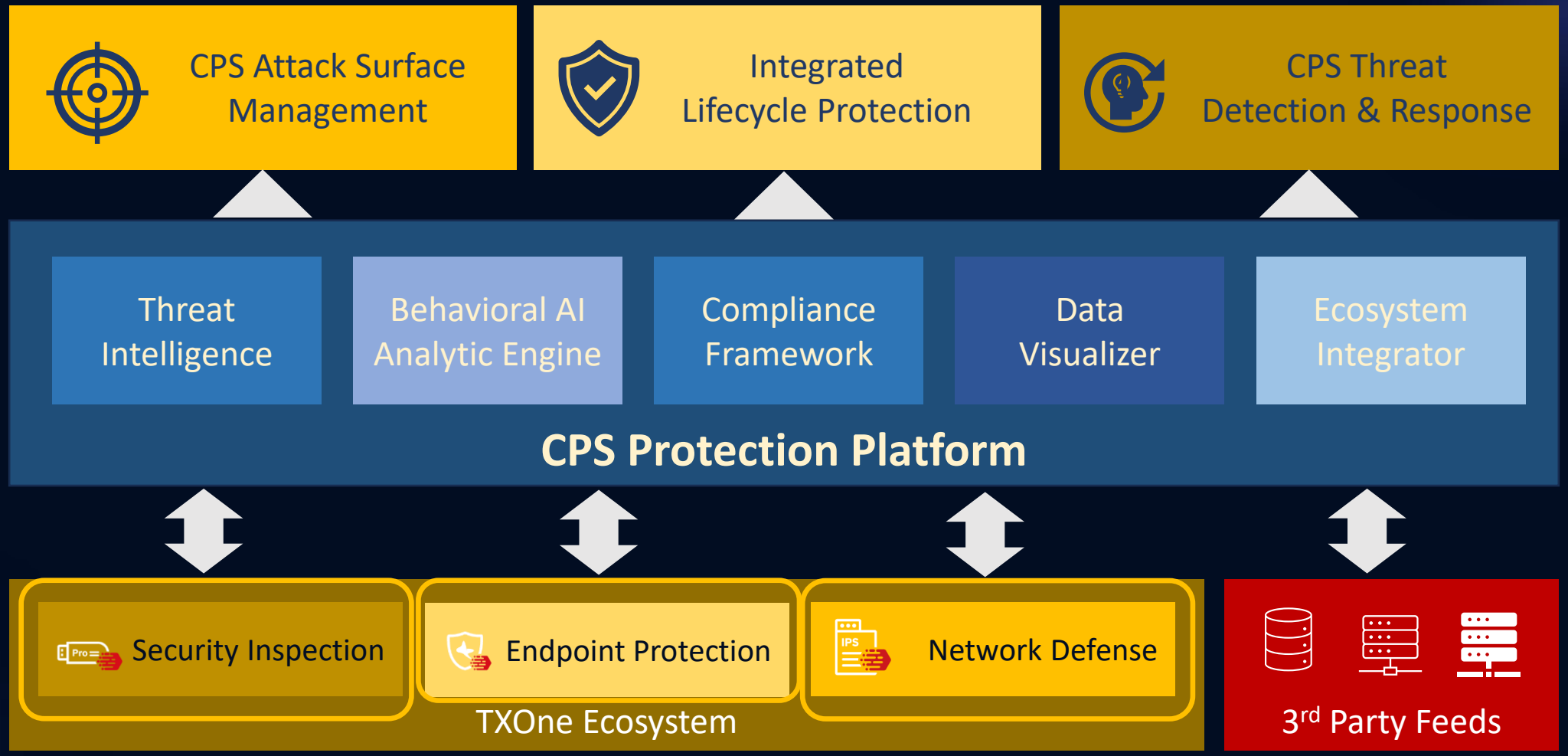
EdgeOne
- Available management all Edge product in one console
- Network visibility
- Centralized policy management
- SIEM and XDR integration
- Security posture and report
- Multi-hypervisor support (Vmware /KVM/Hyper-V)

EdgeFire-1012
- 200Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- NAT and
- Remote access protection(VPN)
- OOB support

EdgeIPS Pro-2008
- 20Gbps+ performance
- Virtual Patching(IPS) /Anti-Virus
- 4 pairs 10G copper with Hardware bypass

EdgeIPS Pro-2016F
- 20Gbps+
- Virtual Patching(IPS) /Anti-Virus
- 8-Pairs 10G Fiber Bypass (Gen3)

SageOne – CPS Protection Platform



TXOne OT native Solutions Portfolio

https://www.txone.com/data-sheets/ics-cybersecurity-suite/

Security Inspection

Element Series

A malware scanner, equipped with world-leading AV engine in a USB stick form factor

No software installation on the target ICS

Easy operation for Risk Assessment, Regulation & Compliance tool

Security Inspection & Asset Management

Support for air-gapped environments

Endpoint Protection

Stellar

ICS endpoint protection for both modernized and legacy assets (Windows XP & 2000)

No Reboot needed Minimal downtime for mass deployment

4-in-1 lockdown for legacy and un-patchable devices

ICS-NGAV for modernized and patchable devices

Finger-Printing of Assets

CPSDR

Network Defense

Edge Series

Security appliances IDS/IPS, Next-Gen FW to segment, Virtually patch and granular C&C OT protocol control

Easier deployment plug-n-play on the rack or cabinet

Robust hardware to support wide temperature range and long MTBF

Fail-safe Hardware bypass without interrupting production even on hardware failure

CPS Platform

SageOne

Comprehensive SOC security platform for monitoring and managing OT infrastructure

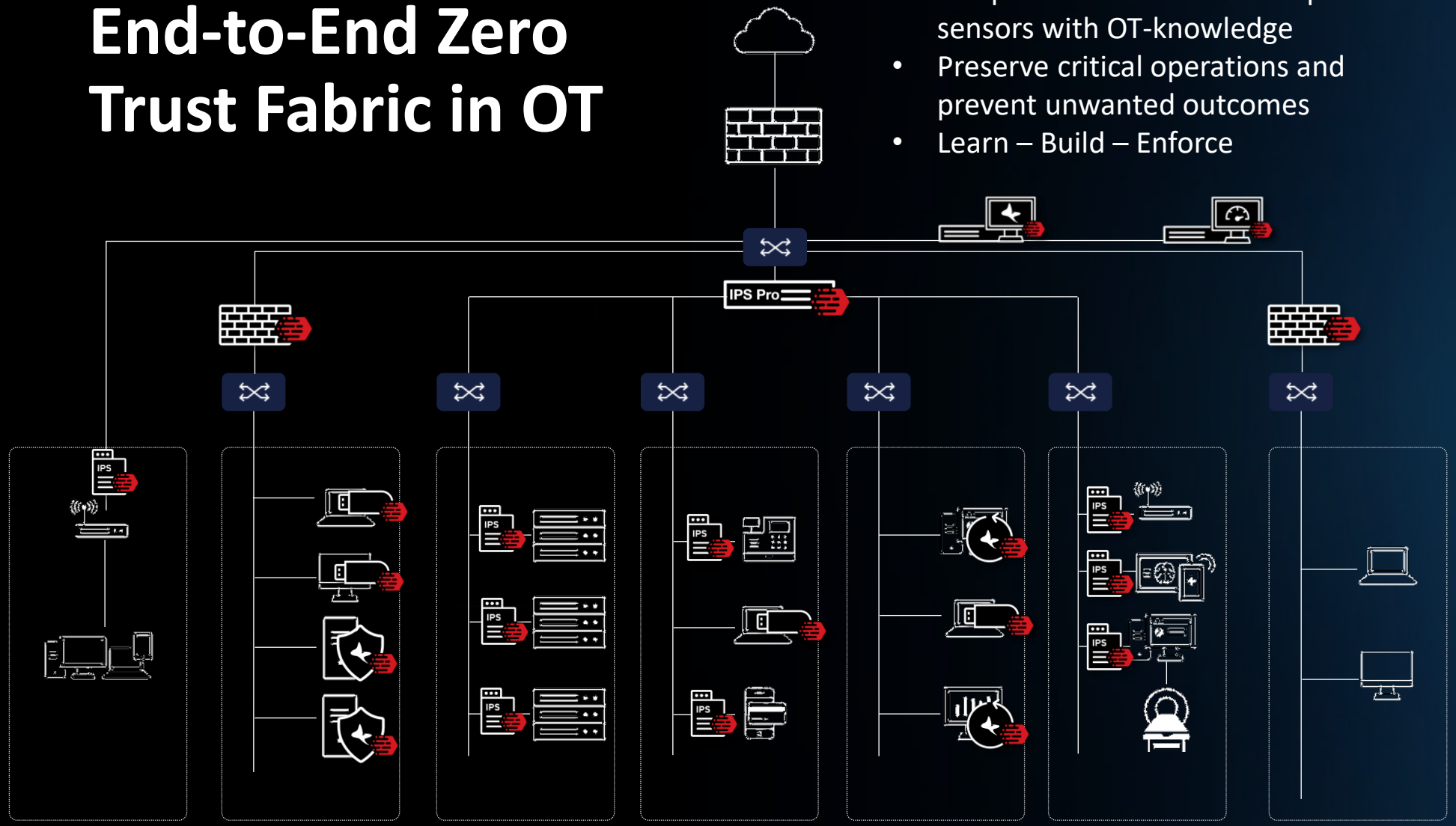
Asset lifecycle management across TXOne security solutions

Vulnerability management and monitoring of critical assets

CPSDR detects and response to potential OT threats

End-to-End Zero Trust Fabric in OT

- Ubiquitous network and endpoint sensors with OT-knowledge
- Preserve critical operations and prevent unwanted outcomes
- Learn – Build – Enforce



Security Inspection

- Portable Security

Endpoint Protection

- StellarOne
- StellarProtect
- StellarEnforce

Network Prevention

- EdgeIPS Pro
- EdgeIPS
- EdgeFire
- ODC

txOne networks

TXOne OT native Solutions

Cooperate IT Security and Network Solution/Vendors

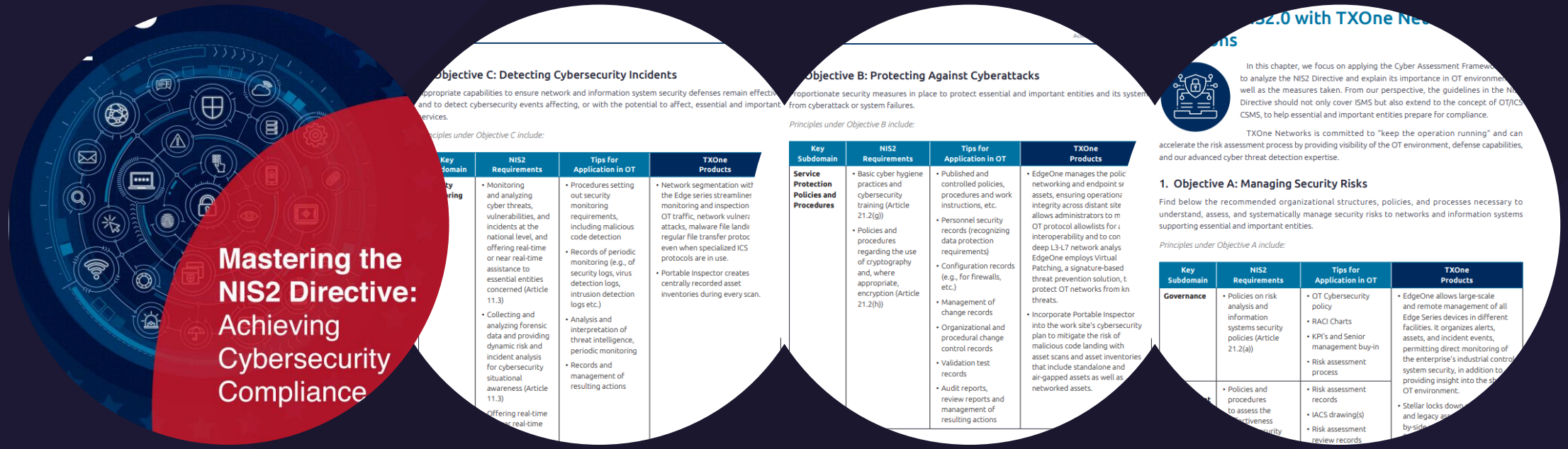
txOne networks

All-terrain Cybersecurity Solution for OT/ICS Shop Floor Environment

TXOne Solution Position Mapping with NIS2 Article 21

Risk analysis and information system security policies	Incident handling	Business continuity and crisis management	Supply chain security	Vulnerability handling and disclosure
SageOne	SageOne	EdgeOne StellarOne ElementOne	Portable Inspector	Edge series- virtual patching
Policies and procedures to evaluate cybersecurity risk management efficacy	Basic cyber hygiene practices and cybersecurity training	Policies and procedures for cryptography and encryption	Human resources security, access control policies and asset management	Use of multi-factor authentication and secure communication systems
EdgeOne StellarOne ElementOne	OT zero-trust solutions enhance cybersecurity efficiency, saving manpower and simplifying oversight.	Portable Inspector includes secure storage equipped with AES-256 encryption	Edge series- Network Trust listing Stellar- Endpoint Trust listing	EdgeIPS series support the principle of least privilege, allowing businesses to minimize the OT attack surface

TXOne NIS2 Whitepaper – Solution Mapping



https://www.txone.com/white-papers/mastering-nis2-directive/

Mirco Kloss
Business Development Director
TXOne Networks Europe B.V.
☎+49 173 41 31 705
✉Mirco_Kloss@txone.com
LinkedIn
www.txone.com