Secure OT

Realize the business benefits of IT and OT convergence while effectively managing risk

Contents

NTT

Why OT
needs to be secure

From industry 1.0 to industry 4.0
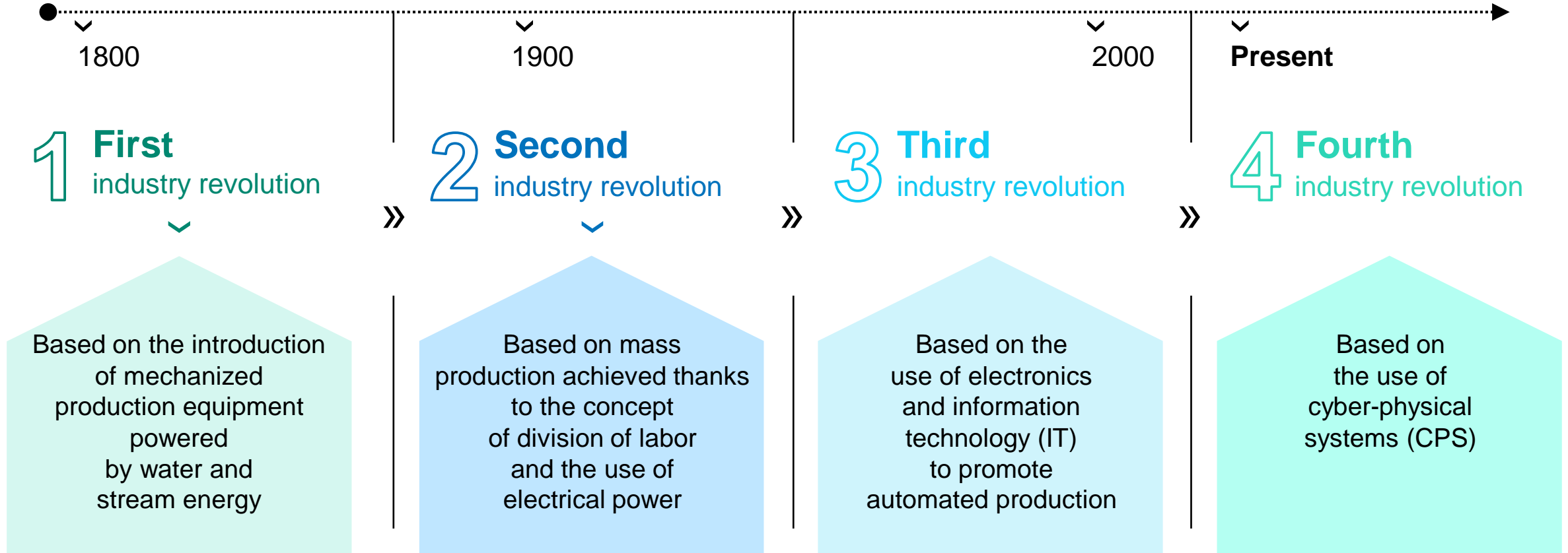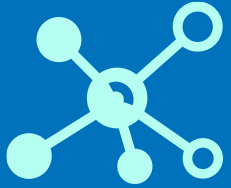
NTT

1800 — 1900 — 2000 — **Present**

1 First industry revolution

2 Second industry revolution

3 Third industry revolution

4 Fourth industry revolution

Based on the introduction of mechanized production equipment powered by water and stream energy

Based on mass production achieved thanks to the concept of division of labor and the use of electrical power

Based on the use of electronics and information technology (IT) to promote automated production
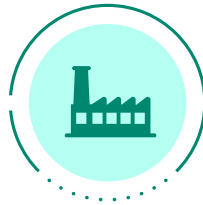
Based on the use of cyber-physical systems (CPS)

IT and OT Typical Environment

Information Technology (IT)
- Enterprise Network / Business Network (BN) / IT Network

Operational Technology (OT)
- Control Room + Industrial Data Center (IDC)

Industrial Zone
containing
"Industrial IT"

- Process Control Network (PCN)

Enterprise Zone
Purdue Level 4-5

IDMZ
"Level 3.5"

Control Zone
Purdue Level 3

Area Zone
Purdue Level 2

Cell Zone
Purdue Level 0-1

IT network

IT CORES

PERIMETER FIREWALL

IDMZ   IDMZ servers

INDUSTRIAL CORES   HISTORIAN   MES

HMI

OT-IDS   SCADA / DCS

Switch

Switch

PLC/RTU/IED

SIS   PLC/RTU/IED

Zone-1   Zone-2

IT and OT are converging

Cost	Performance	Productivity	Safety

Enabling business to reap the benefits of cyber-physical systems

Big data and data analytics	Cloud computing	IoT	Robotics and automation	3D printing	Augmented reality

IT
- ERP
- Internet Protocol
- CRM
- Data Accumulation & Storage
- Human to Machine
- SQL
- Business Applications

OT
- PLC
- HMIs
- SCADA
- BMS
- Direct monitoring and control
- Physical Equipment
- ICS

IT/OT Security
lead to real consequences

Who owns Cyber Risk in OT?

Boards are becoming aware and more engaged to the topic of cyber risk to industrial operations (with increased pressure from shareholders, local governments and regulation)

Board of Directors

CEO

Boards are instructing CEO's to ensure cyber risk to operations is being managed and has a clear owner in the organization

CEO's are asking CIO's and CISO's to owner cyber risk to OT systems just like they own cyber risk to business systems. Therefore, CIO/CISO need an OT security program that effective in the OT domain yet measurable and manageable in the business domain

CIO/CISO

COO

CFO

COOs and the teams supporting Operations are being asked to digitalize and leverage IT to bring additional business benefits but may be doing so in isolation of IT and cybersecurity Teams.

IT Manager

e.g. Operations/Plant/ Facilities/Site Managers

Technology Manager

Engineering Manager

Quality Manager
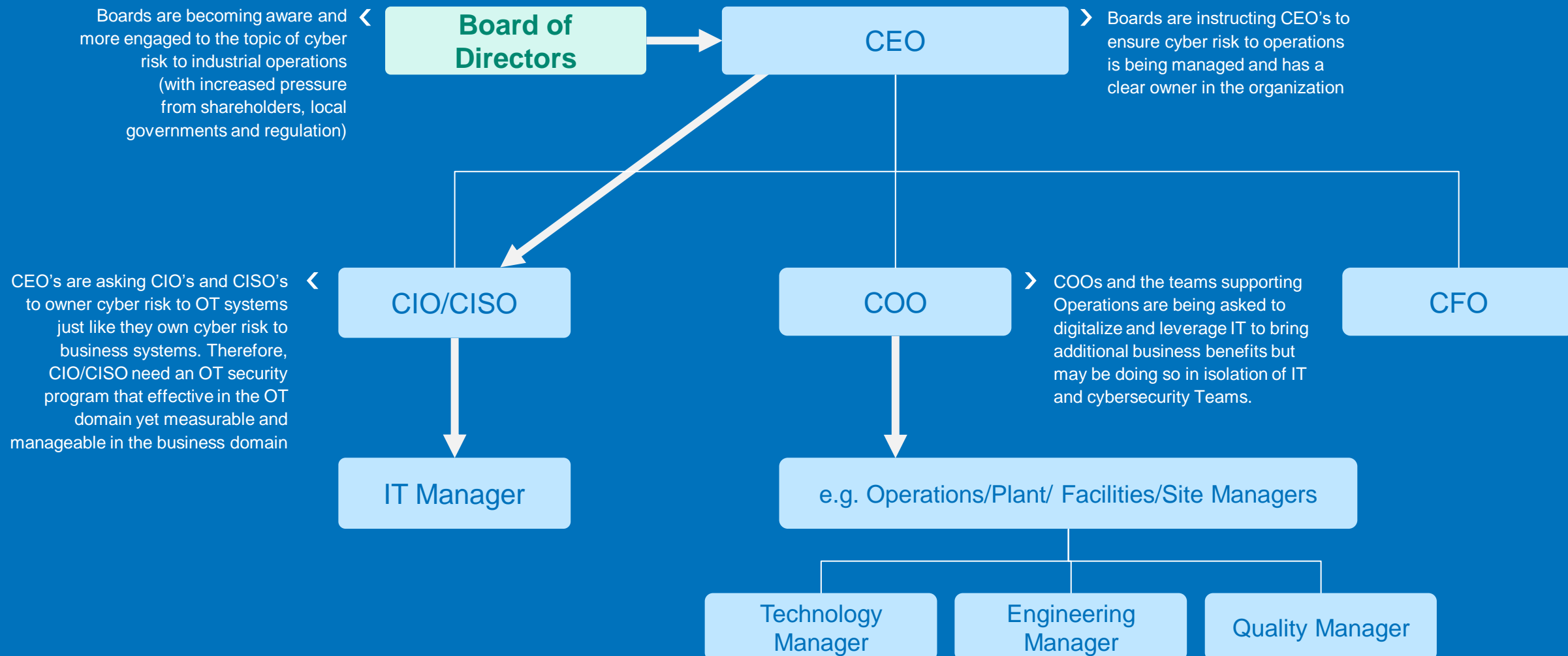
Assumptions that
leave organizations vulnerable

My business needs to move quickly. I can consider OT security later or 'as required'.

- Safety, productivity, operational efficiency and profitability are all compromised if you do not build cybersecurity in from the start and you'll be on the back against cyberthreats.

OT devices have been working well for years, it's not a priority to patch them and could lead to business disruption if I do.

- Basic security hygiene across new and old OT devices, like patching and firmware updates, is a must to reduce risk.

My OT network does not need to be segmented from my IT network.

- Segmentation is critical to minimizing the spread of threats across your IT network, for efficient monitoring for unusual behavior, and controlling and preventing unnecessary access.
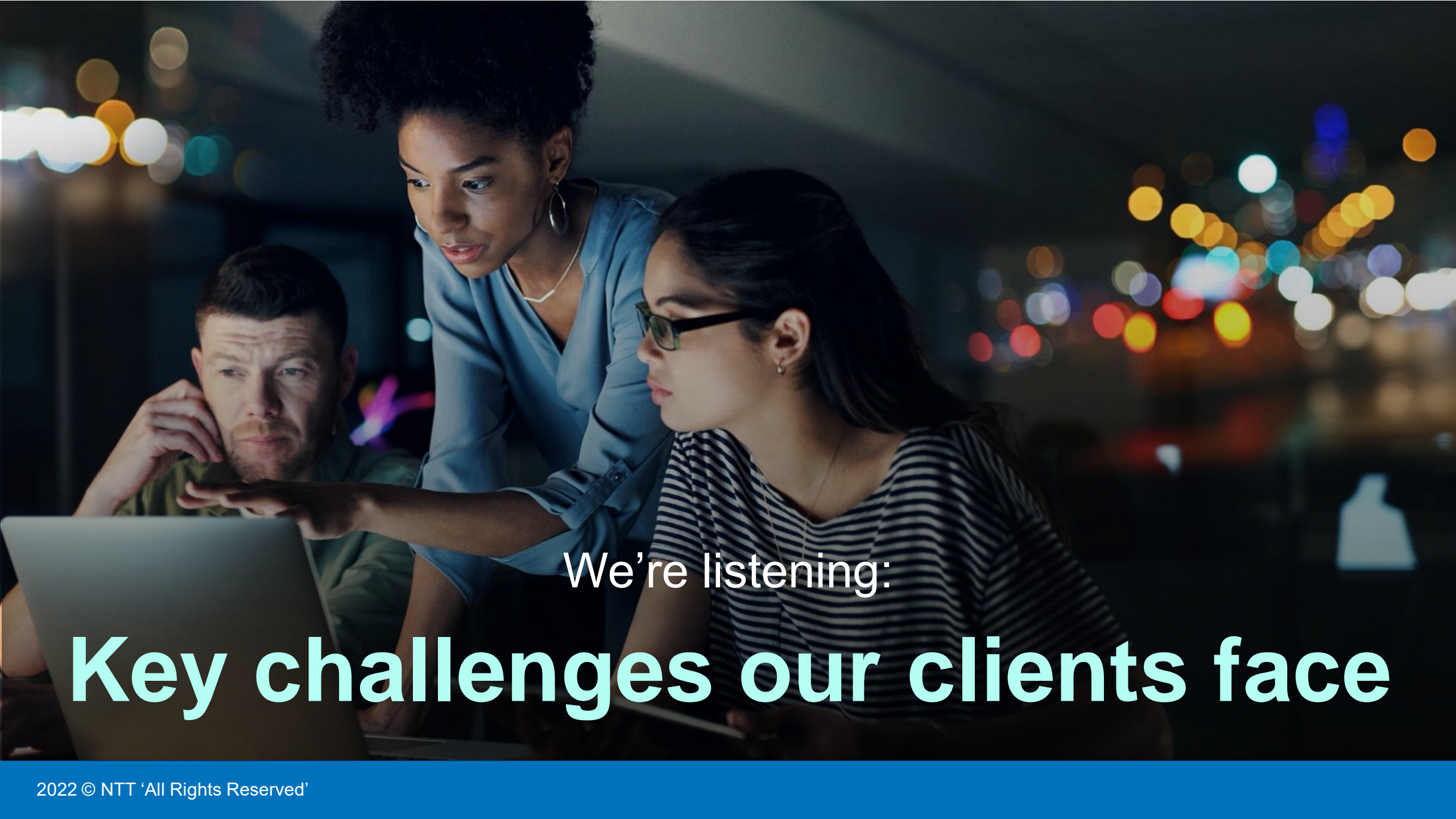
Security operations do not need to be centralized.

- If you do not address security by engaging IT, OT and relevant stakeholders across your business, it's very likely your cybersecurity posture will have gaps, leaving your business vulnerable.

Example: Potential attack vectors to the OT environment

Level 4/5: Enterprise
- PC
- WS
- Mai server
- DNS Server
- Web server

DMZ
- Remote access server
- Patch management server
- Application server
- Historian mirror

FW

Level 3: Operation & Control
- EWS
- Historian
- SW

Level 2: Supervisory control
- WiFi
- HMI
- SCADA
- SW

Level 1: Control
- Plc/RTU
- Plc/RTU
- Plc/RTU

Level 0: Process
- Sensor/actuators
- Sensor/actuators
- Sensor/actuators
- Sensor/actuators

From the outside

Inadequate device configuration management

From within
No malice, i.e. a user unintentionally plugs in an infected USB

From within
Malicious, i.e. a user intentionally introduces malware to a network

We're listening:

Key challenges our clients face

Key challenges we hear from clients
and where we can help

Strategic

An IT/OT Cybersecurity Strategy and security program that provides you with confidence that you will be cyber-resilient in the event of a cyberattack

Ensure alignment between IT and OT stakeholders on OT security posture and approach

Calculate and justify ROI for security investments

Gain the intelligence necessary to make security decisions that align with business objectives

Visibility across the OT and IT environment to help drive intelligent decisions

Operational

Clear inventory of assets and supporting infrastructure within their scope of operations

A properly segmented security architecture that provides higher operational uptime and reduces spread of threats from IT to OT environment

Continuous threat intelligence and detection of anomalies, vulnerabilities, known and zero-day threats across the IT and OT environment

The ability to respond to and recover from threats and attacks, quickly and effectively

Expertise and professional support to guide and support my team along our journey

IT and security leaders are asking fundamental questions:

Where and how do I start?

How do I engage **OT leaders?**

What are the top **3-5 most important things** that I need to be doing well?

How can I ensure that **what I'm doing is working?**

How can I manage my **OT security program?**

How can I assure stakeholders that we are **focused in the right areas?**

How can I get **visibility into all my assets** and how they are connected?

How do I take a **business risk** approach to **securing my OT environment?**

How we help to secure your OT environment

Realize the business benefits of IT and OT convergence while effectively managing risk.

Our OT Security solutions helps you to build an agile cybersecurity posture that spans both your IT and OT environments and is aligned to your risk-profile.

Leveraging NTT's advanced threat intelligence capabilities, our solution improves visibility of threats and vulnerabilities across your OT and IT infrastructure enabling you to identify, protect, detect, respond and recover more effectively than before.

Secure OT

Realize the business benefits of IT and OT convergence
while effectively managing risk.

A cybersecurity posture that spans your IT and OT environments and meets compliance needs

Visibility of your OT assets and communication flows across your OT environment.

Visibility of and early detection of threats before they spread from your IT to OT environments.

Segmentation and control across your OT network and devices.
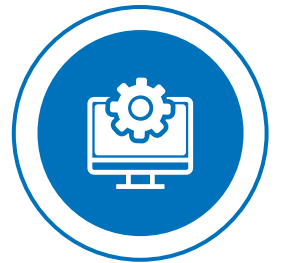
Managed security services to support your IT and OT operations.

We can help you with our
secure by design approach

5 key pillars

1 We'll work with you to ensure security is a key tenant of a business' **overall business strategy**
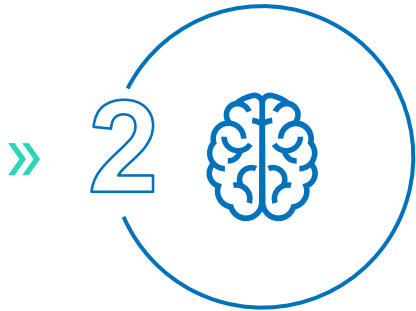
2 We'll create a **security strategy** aligned to what the business' risk-tolerance is, and in line with what the business wants and needs to achieve

3 Our experts will help you build an intelligence-driven **cybersecurity posture**
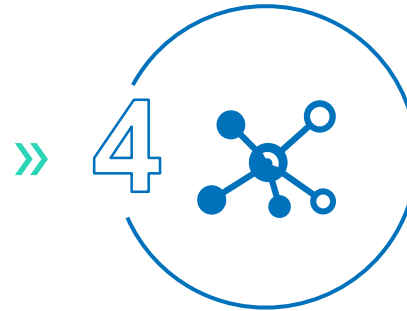
4 We'll help you to **build-in, rather than bolt-on security** to your digital programs, be it your network, data center, cloud, employee or customer experience initiatives
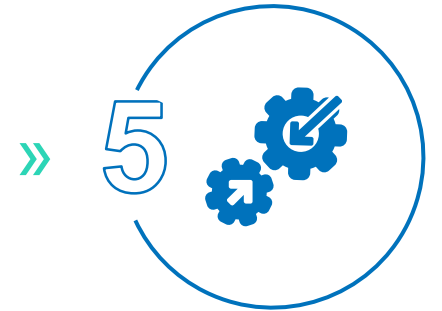
5 We **design an integrated security architecture** that enables businesses to be agile in the face of a changing threat landscape and technology ecosystem

NTT

How
we deliver

Visualize and execute successful security programs that are secure by design with our Security Consulting Services

Select, align and design the right controls and capabilities across all security domains
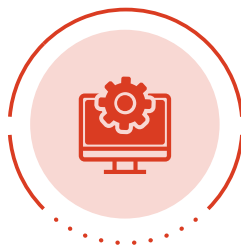
Implement and support with our Technical and Support Services to architect, source, implement and maintain security controls

Optimize via our Managed Services to monitor and manage your security posture to effectively respond to threats

We offer the full lifecycle of
cybersecurity services

Security Consulting Services

To design your security strategy, an optimal architecture for your business and evaluate and validate.

Managed Services

Monitoring, managing, supporting and optimizing your security posture to detect and respond to the latest threats.

Technical and Support Services

Identify and select the right tools and controls, develop detailed designs, deploy and optimize, monitor and maintain.

Validate

Discover

Design

Deploy

Operate

Cybersecurity Advisory for **Operational Technology**

Our **Cybersecurity Advisory** service for OT is a business-outcome driven consulting engagement with a flexible, modular framework that spans the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimizing existing security controls, to designing your next-generation OT security architecture, policies and control framework.

We engage your key stakeholders and subject matter experts through a series of workshops and interviews to analyze the maturity of capabilities of your organizations aligned to industry recommended best practices and expertise.

Together, we determine the gaps between your security posture today versus where you should be and how your organization bridges the gap to meet future requirements.

We then benchmark the results against other organizations in your industry and region to develop a highly tailored recommended roadmap focused on improving the efficacy of your OT cybersecurity program supporting operational resiliency.

An action-oriented roadmap to support budget and resource allocation or simply aligned to an existing strategy for confirmation and reassurance.

Cybersecurity Advisory (CA) for OT
Understanding your cybersecurity capability maturity posture.
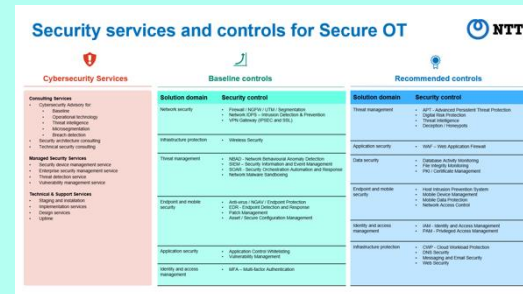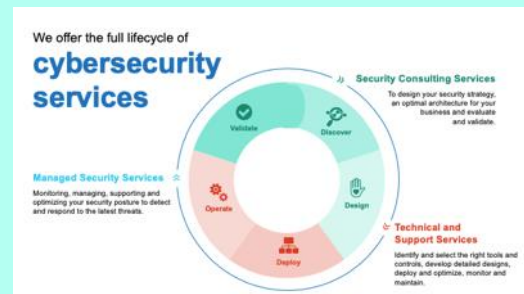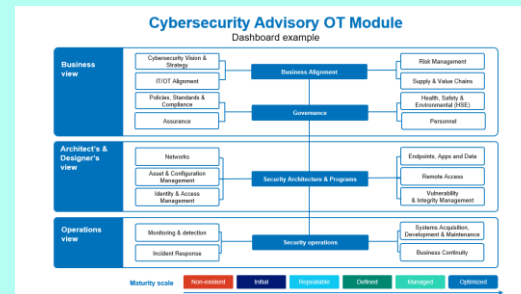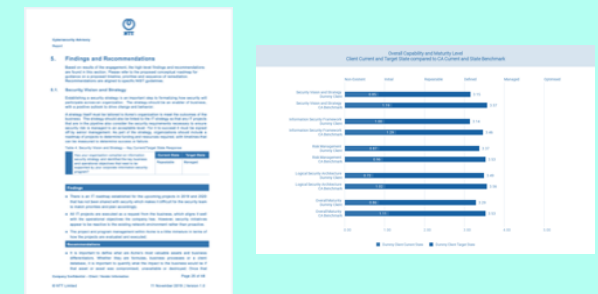
Cybersecurity Advisory OT Module

Dashboard example

Business view

| Cybersecurity Vision & Strategy |
| IT/OT Alignment |

Business Alignment

| Risk Management |
| Supply & Value Chains |

| Policies, Standards & Compliance |
| Assurance |

Governance

| Health, Safety & Environmental (HSE) |
| Personnel |

Architect's & Designer's view

| Networks |
| Asset & Configuration Management |
| Identity & Access Management |

Security Architecture & Programs

| Endpoints, Apps and Data |
| Remote Access |
| Vulnerability & Integrity Management |

Operations view

| Monitoring & detection |
| Incident Response |

Security operations

| Systems Acquisition, Development & Maintenance |
| Business Continuity |

Maturity scale

| Non-existent | Initial | Repeatable | Defined | Managed | Optimized |

Why choose NTT Ltd.?

We're focused on your business outcomes as we help you to create an intelligence-driven security posture across your digital business.

We can **help** you from wherever you are on your **cybersecurity journey.**

We provide the **security skills** and **expertise** you need.

We can support your **global footprint** and regional presence.

We share our **extensive cross-technology expertise** to ensure your digital solutions are **secure by design.**

We provide the **industry, regional** and **global insights** through our research and experience with more than 4000 clients.

We partner with all of the **leading security technology** providers.

We invest in **security capabilities** you need now and in the **future.**

We offer advanced threat intelligence capabilities to **help you make informed risk-management decisions.**

Innovation
with our clients

Co-innovation with our clients

NTT

Automotive factory

Increase cyber-resiliency in ICS
(against malware, etc.)

- Asset visibility and verification in ICS
- Microsegmentation based on data flow analysis
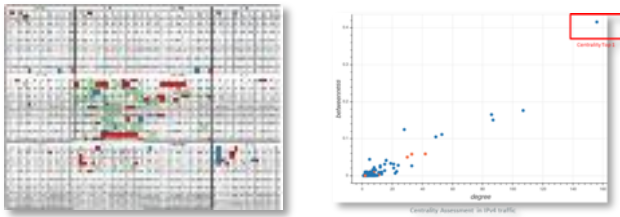
City gas factory

Critical infrastructure protection
(against targeted attack)

- Implementation of OT security sensor
- 24/7 Monitoring
- Incident response together with client and ICS vendors

Connected car

Secure smart mobility
(against new threats)

- Architecture design and prototyping threat detection for connected car
- Completed viability study and demonstration with real car
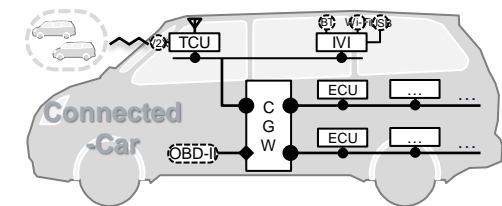
Resilient security solutions for connected cars

The next steps

NTT
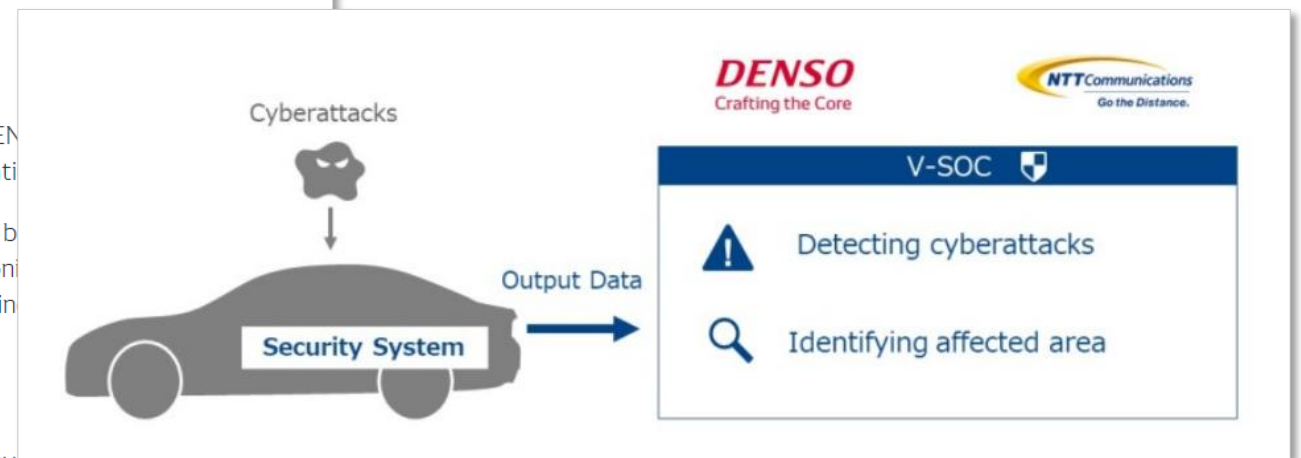
Understand your current cybersecurity posture and create an actionable roadmap that takes you to where you need to be with our:

Cybersecurity Advisory for OT

Zapraszamy do rozmowy

Dominik Czyż

Senior Solutions Manager, Intelligent Infrastructure & Cybersecurity

M: +48 502 787 562

E: dominik.czyz@global.ntt