SIEMENS

Siemens Advanta Consulting

# OT Cybersecurity Lunch & Learn

July 2023



siemens-advanta.com/consulting

# Agenda

**Why is OT Security relevant for financing/M&A?**

What's the difference between IT and OT Security?

How is Siemens addressing IT and OT Security?

How can Siemens & Siemens Advanta Consulting help clients?

What are some client examples?




SIEMENS

# One vertical example: F&B organizations have become prime targets of cyber attacks in recent years and victims suffered devastating financial losses

## Potential impacts

"On average, F&B industry cyber attacks result in financial losses of **30'-40' USD** and take nearly **316 days** to detect, investigate, and remediate."

### Operational risks

- Operational disruption and downtime
- Loss of IP and competitive advantage – recipes, packaging design
- Process errors could result in quality issues, recalls, customer harm

### Safety and environmental risks

- Potential for injury, loss of life, environmental damage

### Financial, regulatory, and brand management risks

- Unplanned changes to facilities or processes without proper documentation
- Fines, penalties, FDA and regulatory consequences
- Reputation and brand impact

Mondelēz International

In 2017, Mondelez International confectionery, food and beverage company, **lost access to its logistic** **software**, due to NotPetya cyber attack. This attack severely disrupted its operations, resulting in substantial financial losses **exceeding 100' USD**.

MOLSON Coors

In March 2021, Molson Coors, a brewing and beverage giant, was hit by a cyber attack. The system outage caused **delays and disruption** to its brewery operations, production and shipments. As a result, Molson Coors paid a **2' USD** one-off cost to forensics experts, consultants and data recovery providers who helped Molson Coors restore operations.

JBS

In May 2021, JBS, one of the largest meat processing companies, experienced a cyber attack on its OT systems. North America **operations were shut down** and an **11' USD** ransom was paid to the attackers.

Coca-Cola

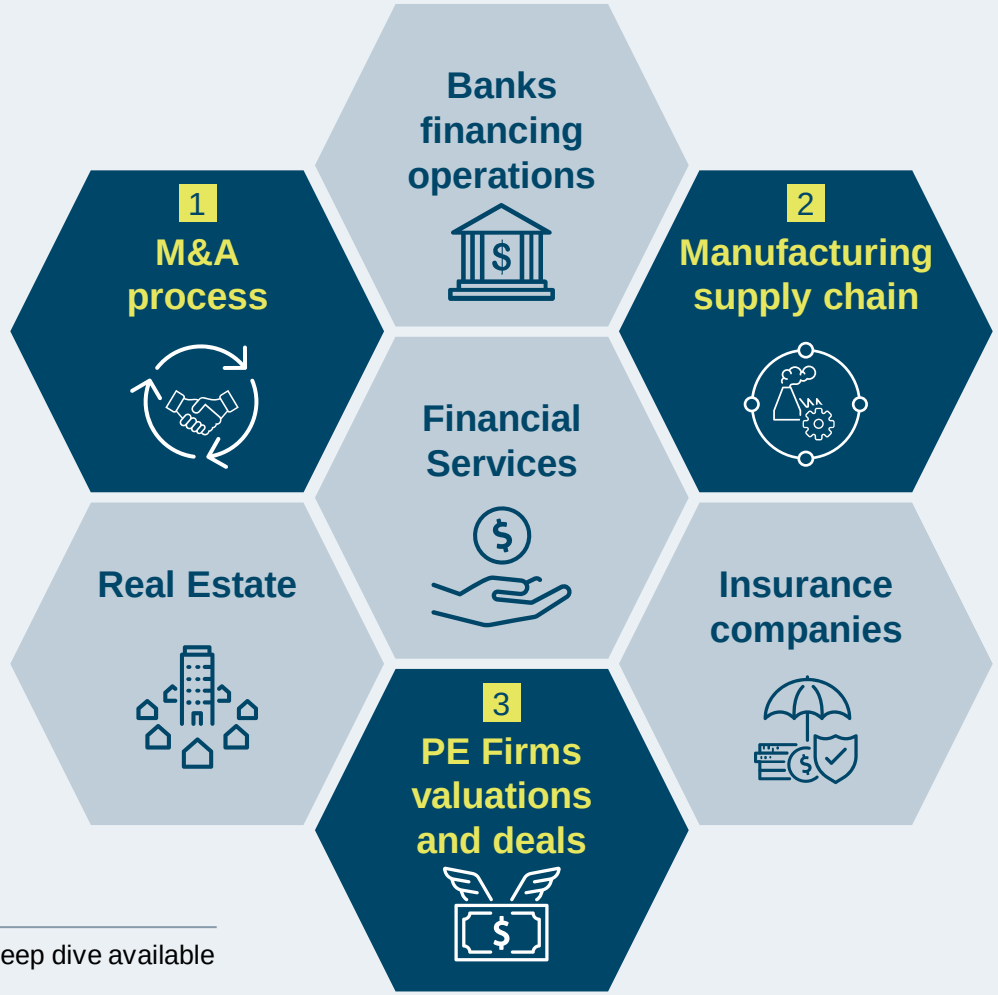
In April 2022, Coca-Cola fell victim to the Stormous Ransomware, which successfully **breached Coca-Cola's servers** and exfiltrated approximately **161GB of data**. In a separate incident in 2023, Coca-Cola experienced **another cyber attack in Mexico**, further highlighting the ongoing challenges and vulnerabilities faced by the company in terms of cybersecurity.

Source: Siemens Advanta Consulting, Capstone Logistics, Forbes




SIEMENS

# Today OT cyber threats are still a major challenge for investment managers across industries




x Deep dive available

**Typical cyber threats**

- Ransomware attacks
- Identity stealing
- DNS Attack
- .....




SIEMENS

# 1 OT cybersecurity risks are found along every stage of the M&A process: Firms need to proactively implement mitigation strategies

| Phase | Main activities | Key cyber risks | To mitigate cyber risks, firms are recommended to… |
|---|---|---|---|
| **Pre- M&A** | Due diligence<br>Valuation<br>Deal structuring and negotiation | • Limited visibility<br>• Inaccurate due diligence<br>• Compliance gap<br>• Budgetary considerations<br>• Time constraints | • … Identify **risk exposures** and evaluate **liability** to support negotiation and drive remediation<br>• … Identify **process misalignment and incompatibility** that will complicate value creation<br>• … Estimate **the level of investment** required to strengthen OT cybersecurity |
| **During M&A** | On-boarding and integration<br>Risk management<br>Value creation | • Integration challenges<br>• Vendor and third-party risks<br>• Ineffective security monitoring capability<br>• Compliance and legal consideration | • … Optimize **integration plans** and ensure **compatibility** to mitigate risk of technology disruption and unforeseen cyber attack<br>• … Build and mobilize **end-to-end frameworks** for acquisition risk management<br>• … Develop a **unified security framework** for the merged company ensures consistent OT cybersecurity practices across the organization |
| **Post M&A** | Risk management<br>Divestment and separation | • Vulnerability and emerging threats in merged OT environment<br>• Legacy system decommissioning<br>• Maximization of ROI | • ... Uncover unknown breaches to **prevent exposure of hidden liabilities** that impact sale<br>• … Produce **costed separation plans** to deliver appropriate transfer of security responsibility and secure divestment execution to retain value |

Source: Siemens Advanta Consulting, PWC




SIEMENS

# 2 Prevalent cybersecurity attacks in supply chains cause multi million-dollar losses for large corporations

| | Key OT cybersecurity concerns | Description | Case studies |
|---|---|---|---|
| **Procurement** | Supplier assessment and risk management | Some of the most high-impact cyber incidents were targeted toward supplier's system code, followed by data and internal processes | In February 2022, a major player in petroleum and energy sector announced a **delay in operations** and that redirect its oil shipments to different storage facilities due to cyber attack on two of its Germany-based suppliers  |
| | Communication channel security | Malicious actors targeting the transfer of sensitive information between clients and suppliers | |
| **Manufacturing** | Industrial Control Systems (ICS) vulnerability | Ransomware attacks can result in operational disruption, safety risks and financial extortion | In March 2019, Norsk Hydro, a global aluminum producer, experienced a cyber attack on its OT systems, including production lines and smelting operations, forcing the company to switch to manual operations. The incident resulted in financial losses of approximately **65' USD**   |
| | Third-party risks | A cyber attack on a single supplier can lead to long-term suspension of manufacturing operations across multiple plants for both clients and other connected suppliers | |
| **Logistics and distribution** | Logistic system vulnerability | The growing use of autonomous solutions in logistics intensifies cyber attack risks, leveraging wireless communication channels as entry points to disrupt the supply chain | The 2017 NotPetya attack disrupted computer systems and caused **widespread outages** in network infrastructure, causing an estimated **10" USD** in damages globally. Major companies like shipping giant Maersk estimated losses of **200'-300' USD** and Fedex reporting losses of **400' USD**  |
| | Third-party risks | An organization, irrespective of having a strong cyberdefined ecosystem, is vulnerable if its partner firms fail to implement cybersecurity solutions with the same level of stringency | |

Source: Siemens Advanta Consulting, EY, BBC news, Wikipedia



SIEMENS

# 3 PE firms need a proactive mitigation strategies to navigate cyber challenges during deal execution process

| Key process steps | Mitigation strategy that PE firms can … |
|---|---|
| PE deal valuation process – Due Diligence | • … Conduct **thorough due diligence**, followed by deeper **technical testing**<br>• … Conduct robust diligence to understand major **cyber and compliance risks**, access company's preparedness and develop post-sign plan to remediate gaps<br>• … Prepare **preliminary cost estimate** for remediation, ensuring realistic expectations and reserving budget for remediation |
| PE deal valuation process – On-boarding | • … Implement **risk mitigation measures**, including advanced endpoint protection, immutable backups, multifactor authentication and employee awareness measures<br>• … Create **a current, day one and future state operating model** for cybersecurity and data privacy, and develop a detailed roadmap for the first 100 days<br>• … Establish a **structured onboarding process** that sets clear security expectations, enabling portfolio companies to rapidly leverage fund-level programs and resources |
| PE deal valuation process – Value creation | • … Extend assistance through education, talent development, diagnostics, accelerators, advice on best practices, and facilitating the engagement of appropriate services and vendors<br>• … **Collaborate with portfolio companies** in regular data-gathering exercises to assess **portfolio cyber programs**, leveraging data-driven insights to reduce risk, identify synergies, implement best practices, and address common pain points |
| PE deal valuation process – Exit | • … Employ **intentional process** to enhance cyber program during value creation period, while involving **sell-side advisors** to prepare cyber team for **buy-side diligence**<br>• … Include **portfolio company's security leader** in the deal preparations early on to address potential concerns and develop a practical roadmap for longer-term improvements |

## The most forward-thinking PE firms are …

- Doubling their budget for security leaders
- Taking a shared services approach, hiring high-level CISO executives to:
  - help with PE company itself and
  - advise portfolio companies
  - vet potential investment. M&A, and otherwise

Source: Siemens Advanta Consulting, EY Parthenon, Hunt Scanlon Media




SIEMENS

# Agenda

Why is OT Security relevant for financing/M&A?

**What's the difference between IT and OT Security?**

How is Siemens addressing IT and OT Security?

How can Siemens & Siemens Advanta Consulting help clients?

What are some client examples?

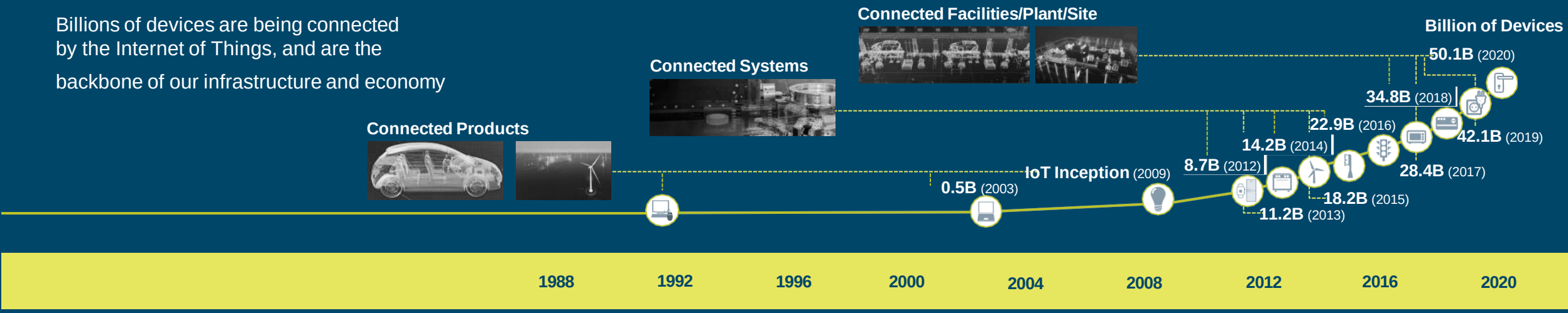



SIEMENS

# Digitalization creates …

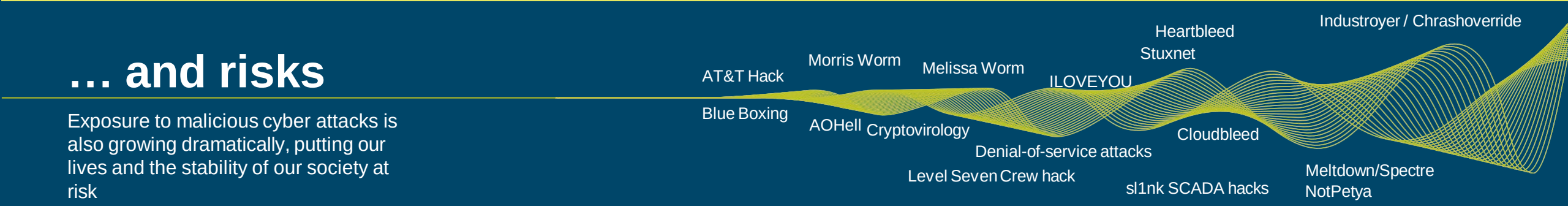
## Opportunities…

Billions of devices are being connected by the Internet of Things, and are the backbone of our infrastructure and economy




## … and risks

Exposure to malicious cyber attacks is also growing dramatically, putting our lives and the stability of our society at risk



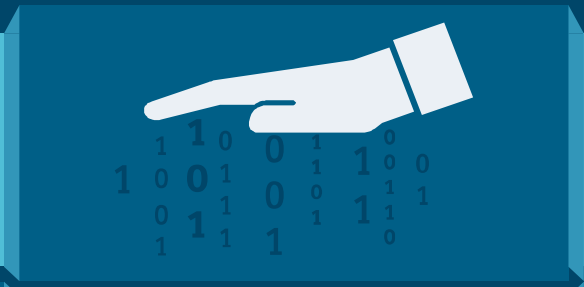

Source: Siemens Advanta Consulting




SIEMENS

# IT and OT with fundamental differences however differentiation is irrelevant addressing security

The IT/OT divide is mainly a difference in **viewpoints**. A great place to start is **understanding** each group's view of **cybersecurity priorities** and why those priorities are **different**.



| IT security | | OT security |
|---|---|---|
| **Confidentiality** | | **Safety + Availability** |
| **Integrity**<br>**Availability** | | **Integrity**<br>**Confidentiality** |
| Seconds to minutes range accepted | **Availability** | Network failure times <300 mS (down to zero packet loss) |
| Network specialists | **Installation** | Plant commissioning personnel (Automation experts) |
| Lines and stars | **Topology** | Rings and redundant lines and stars |
| Climate-controlled offices | **Location of use** | Harsh environment (temperature range, corrosive atm, vibration) |
| High density, concentrated switches with many ports (24-96) | **Device density** | Low density, widely distributed switches with fewer ports (4-24) |
| Refresh every 3 to 5 years | **Investment life cycle** | Refresh cycle can be as long as 20 to 30+ years |
| Business & customer interactions delayed by hours or minutes | **Risk Impact** | Loss of life, destruction of capital equipment, loss of production |




SIEMENS

# Typical technical challenges of organizations…

### Weak asset management
Missing ownership for assets or outdated data, network architecture unknown

### Lack of security monitoring
Ineffective of nonexistent security monitoring of production networks and services

### Lack of disaster recovery plans for cyber attacks
DRP, if existing, are not considering an approach to respond to cyber attacks to industrial control systems (e.g., ransomware)

### Improper network segmentation and access control
Networks are not segmented; routers and firewalls are improperly configured. Additionally, insecure (remote) access from Internet & Intranet are generally identified

### Insecure security framework and procedures
Without proper IT / OT operation processes, detection & resolving issues in production environment is hampered

Source: Siemens Advanta Consulting




SIEMENS

# ...and underlying organizational challenges in IT / OT cybersecurity

## Governance
Missing ownership and cross-functional policies for efficient decision making and risk management

## People
Weak risk-oriented culture, missing expertise and lack of clear roles and responsibilities

## Processes
Hampered detection and resolving of issues in production due to insecure IT / OT operation processes

## Technology
Complexities in the technology landscape leave organizations with a disjointed IT / OT security approach

**Cybersecurity in IT / OT needs a holistic approach focusing on governance, people, processes and technology**

Source: Siemens Advanta Consulting




SIEMENS

# Agenda

Why is OT Security relevant for financing/M&A?

What's the difference between IT and OT Security?

**How is Siemens addressing IT and OT Security?**

How can Siemens & Siemens Advanta Consulting help clients?

What are some client examples?

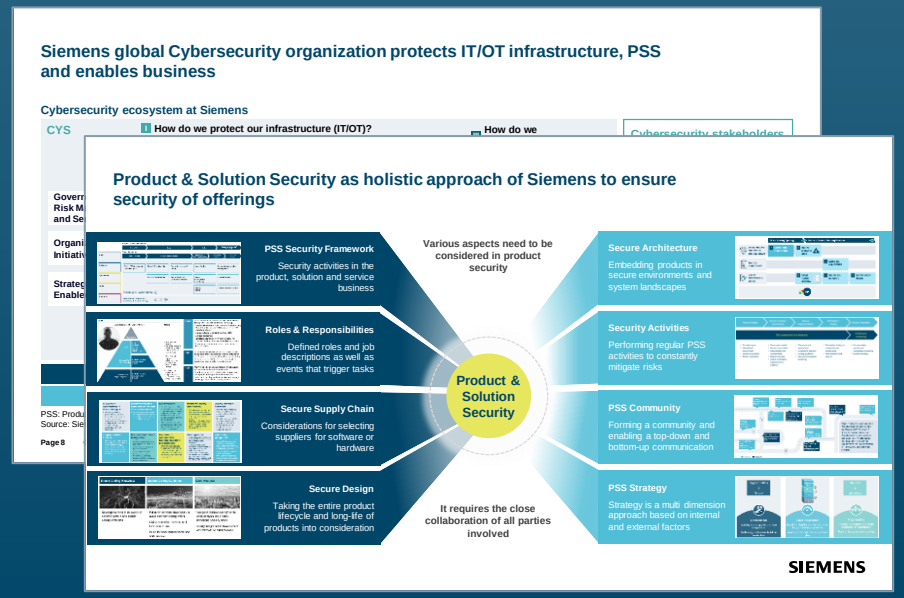



SIEMENS

# Siemens approaches cybersecurity as a combined function for IT / OT and takes a more general perspective by focusing on applications, factories, and products

## Organization

- No differentiation in IT vs. OT cybersecurity organization
- One combined organization ensuring overall security




## Focus is not on IT vs. OT, rather on

- **Applications**
  - Security of the application: CMDB, "Security Crafter" / internal security guidelines (SFeRA), patch level, exception handling, vulnerability monitoring
  - Secure connection: SSO & identity provider, tunneling, zero trust or ring fencing
  - Risk management: Asset classification and protection concept, Cyber security architecture board
  - Incident handling: CERT, on demand cyber squat
- **Products**
  - Product & solution security (PSS): PSS framework, architecture, activities, and community
  - Ensuring security: Security by design, SBOM, secure supply chain, PCERT
- **Factories & location**
  - Secure devices: Proxy channel devices, secure onboarding mechanisms (MASA), on demand DevOps pipelines
  - Physical Security: Audit site visits, physical access controls for OT testing stations
  - Network: Micro segmentation, Perdue reference architecture, network separation, zero trust (network transition center), secure channels, on site data centers

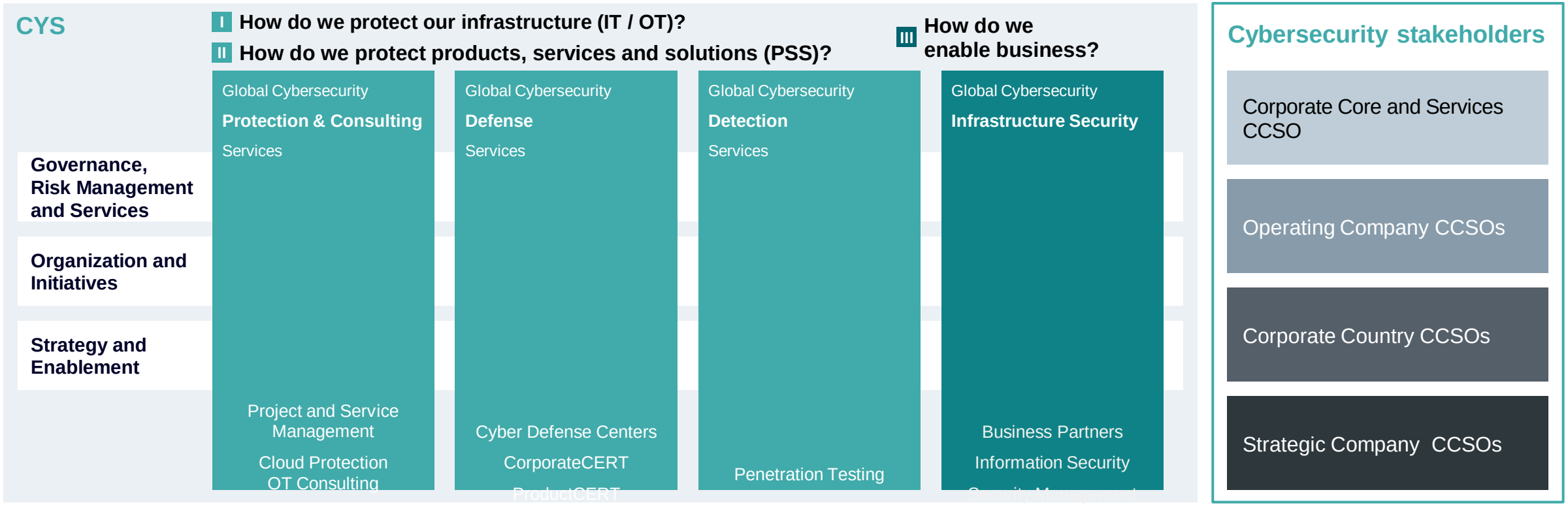
Source: Siemens Advanta Consulting

SIEMENS

# Siemens global Cybersecurity organization protects IT / OT infrastructure, PSS and enables business

## Cybersecurity ecosystem at Siemens




PSS: Product and Solution Security, i.e., ensuring security of Siemens products and solutions sold to customers

Source: Siemens Advanta Consulting

SIEMENS

# Agenda

Why is OT Security relevant for financing/M&A?

What's the difference between IT and OT Security?

How is Siemens addressing IT and OT Security?

**How can Siemens & Siemens Advanta Consulting help clients?**

What are some client examples?




SIEMENS

# With our strategy-first, roadmap-driven IT / OT security approach we are enabling our clients to prevent and fight cyber attacks

## Key questions

- Are my factories well equipped to fight cyber attacks?
- Do I have enough visibility across my IT / OT networks?
- Are the existing Security Operations Centers sufficiently aligned with business requirements?

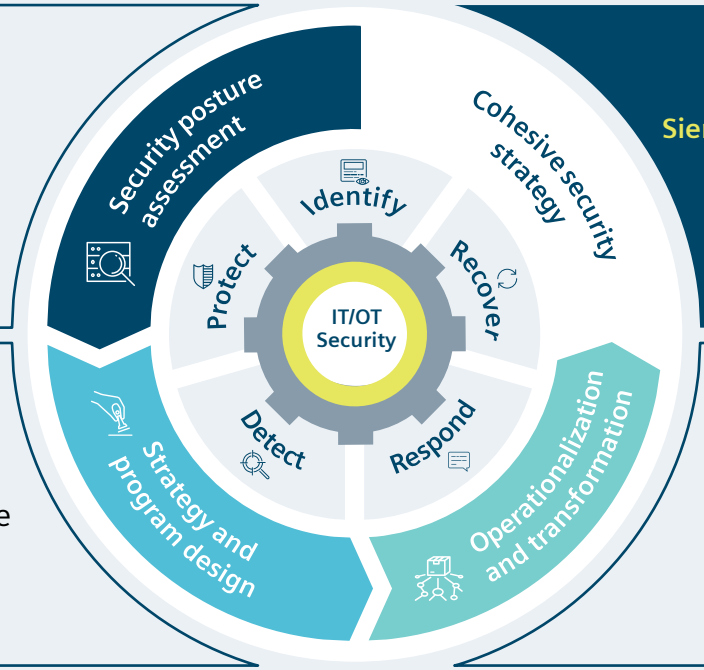
## Our understanding of IT / OT Cybersecurity Transformation

1

**Understand current posture**
Deep scan on current security operations

2

**Develop a holistic strategy**
Tie the organization to a single vision and goal and define the target operating model




Siemens Advanta's IT / OT Security Transformation

3

**Operationalize your journey**
Strategy execution to reach target posture

**Impact**

- Prevention of lost earnings of up to **$120-140 million** [1)]
- Prevention of costly production stops of up to **two weeks** [2)]
- Prevention of customer satisfaction due to **shipping delays**

**Clients** SIEMENS ... and major players from **energy, healthcare and food & bev. sectors**

Numbers from cybersecurity attacks: 1) Molson Coors 2) Palfinger
Source: Siemens Advanta Consulting




SIEMENS

# Our approach to cybersecurity services can be tailored to meet a wide variety of organizational needs

## 1 Is there transparency on existing security gaps?

### Assessment

**Maturity/risk assessment**
Evaluation of security posture against relevant industry standards

- IEC 62443
- NIST 800-82
- ISO 27001
- … [1)]

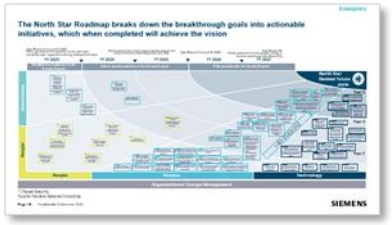
**Readiness assessment**
Evaluation of business readiness for specific scenarios

- Ransomware Readiness
- Island Mode Operations
- Breach & Attack

## 2 Is there a clear vision for the future state of security?

### Target Setting

**North Star Roadmap**
Define multi year security strategy and north star



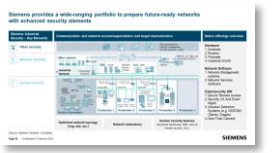

**Policies & Standards**
Development of policies & standards to define security intents and requirements


## 3 Are resources properly organized to improve security?

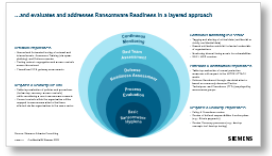
### Execution

**Security Program**
Set up and enable security program

**HW/SW implementation**
Multi-faceted security concept for industrial operations



**OT Services**
MDR[2)] services
SOC[3)] enablement
SOC[3)] operations



1) Other standards and frameworks can be used (e.g., depending on industry or regulatory requirements)
2) Managed Detection and Response
3) Security Operations Center
Source: Siemens Advanta Consulting

Deep-dive next



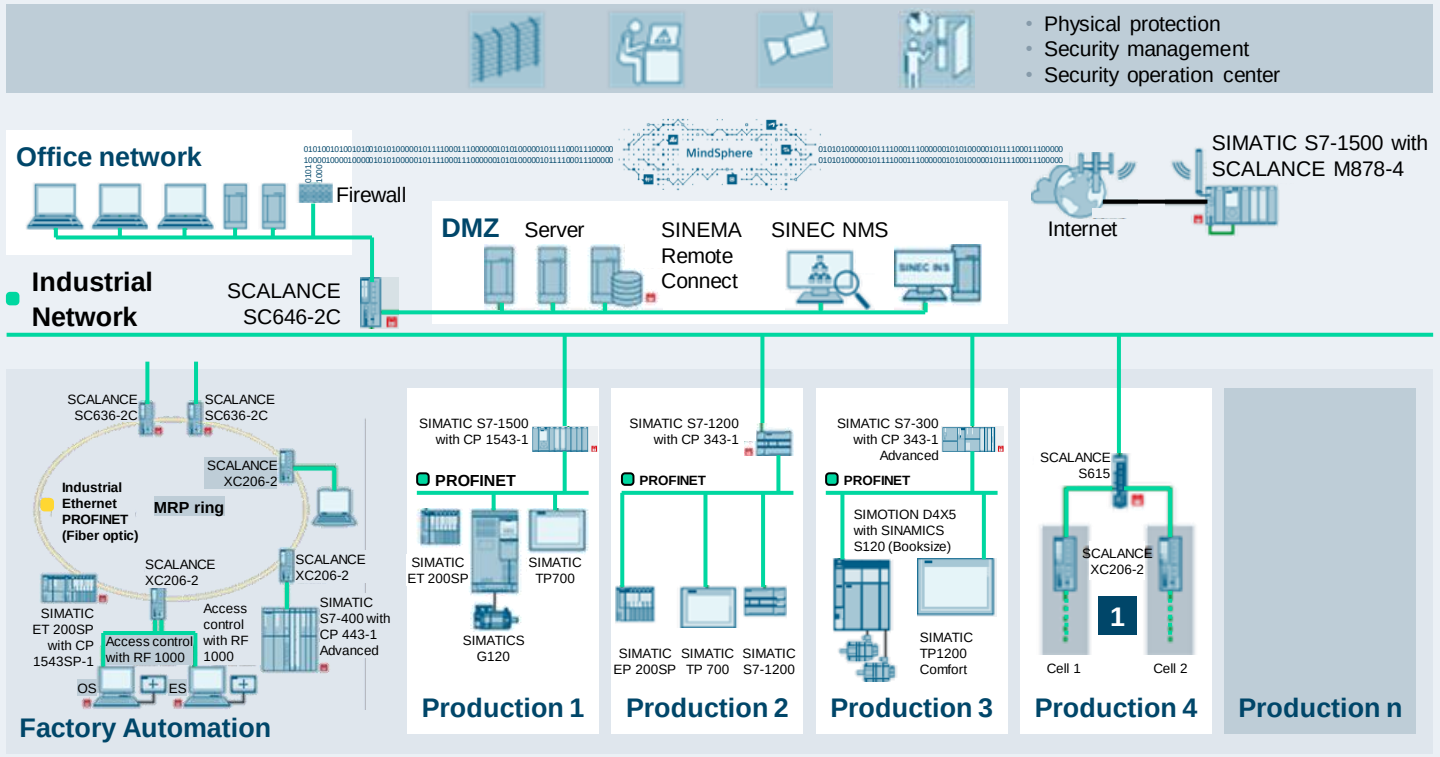

SIEMENS

# Siemens provides a wide-ranging portfolio to prepare future-ready networks with enhanced security elements

## Siemens Industrial Security

- Plant security
- Network security
- System security

## Communication and network access/segmentation and target characteristics




**Optimized network topology (ring, star, etc.)**

**Network redundancy**

**Custom security features**
(end-point hardening, DMZ, secure remote access , etc.)

## Select offerings overview

**Hardware**

1. Switches
2. Routers
3. Firewalls
4. Industrial WLAN

**Network SW/services**

1. Network Mgmt. systems
2. Network Services sw.
3. Network scanning (SINEC security inspector)
4. Sophisticated full NW monitoring (NIDS & HIDS) software (SINEC Security Monitor)

**Cybersecurity SW/services**

1. Secure Remote Access
2. Security Inf. & Event Mgmt.
3. Intrusion Detection Systems (e.g., NOZOMI)
4. Zero Trust Concept
5. 24x7 U.S.-based SOC
6. SIBERprotect™ SOAR concept

Source: Siemens Advanta Consulting




SIEMENS

# Agenda

Why is OT Security relevant for financing/M&A?

What's the difference between IT and OT Security?

How is Siemens addressing IT and OT Security?

How can Siemens & Siemens Advanta Consulting help clients?

**What are some client examples?**




SIEMENS

# We have proven our IT / OT cybersecurity expertise in various projects in different industries, internally and externally

## Establishing an IT/OT centric security program

**Industry:** Food & beverage
**Offering:** IT / OT Cybersecurity

- **Security Program Review**
- Definition of **target cyber posture**
- Establishment of key security control processes
- **Enablement of financial efficiency** implementing cross IT and OT security control technologies

## Cross functional cybersecurity risk management

**Industry:** Electric & Water Utility
**Offering:** IT / OT Cybersecurity

- Program & project management for the implementation of an **enterprise-wide cyber security program**
- Conducting a series of **cyber security audits**
- Identification of emergent risks

## International cybersecurity strategy

**Industry:** Electric municipal utility
**Offering:** IT / OT Cybersecurity

Development and deployment of an **international cybersecurity strategy** and program design incl.

- Establishment of a risk management program
- Development of effective board reporting
- Implementation of control and

## Cybersecurity program assessment

**Industry:** Industrial Process
**Offering:** IT / OT Cybersecurity

**Program assessment** with focus on

- IEC62443 and ISO27001 based security assessments for key operating procedures
- Business and technical impact assessment for selected incident response scenarios Roadmap/action plan to improve observed

Source: Siemens Advanta Consulting

SIEMENS

# We have a wide network of cybersecurity experts

## Siemens cyber-security expert network


Source: Siemens Advanta Consulting




SIEMENS

# YOUR CONTACTS
# @ Siemens Advanta


**Georg Schoener**
Associate Vice President

OT Cybersecurity Consulting

Mobile: +1 (407) 236 4374
E-mail: Georg.Schoener@siemens.com



**Andreas Aschenbrenner**
Associate Vice President

Cybersecurity and AI Consulting

Mobile: +49 (172) 2731972
E-mail: Aschenbrenner.Andreas@siemens.com

# Backup