Rethinking Cyber Resilience: A Holistic Strategy for Critical Infrastructure

Lessons Drawn from Years of Securing Industrial Systems and Critical Operations

Andre SHORI
APAC Cybersecurity VP and CISO, Schneider Electric

The company is a global energy technology leader

Key figures for 2025

€40 billion

2025 revenues (+8.9%)

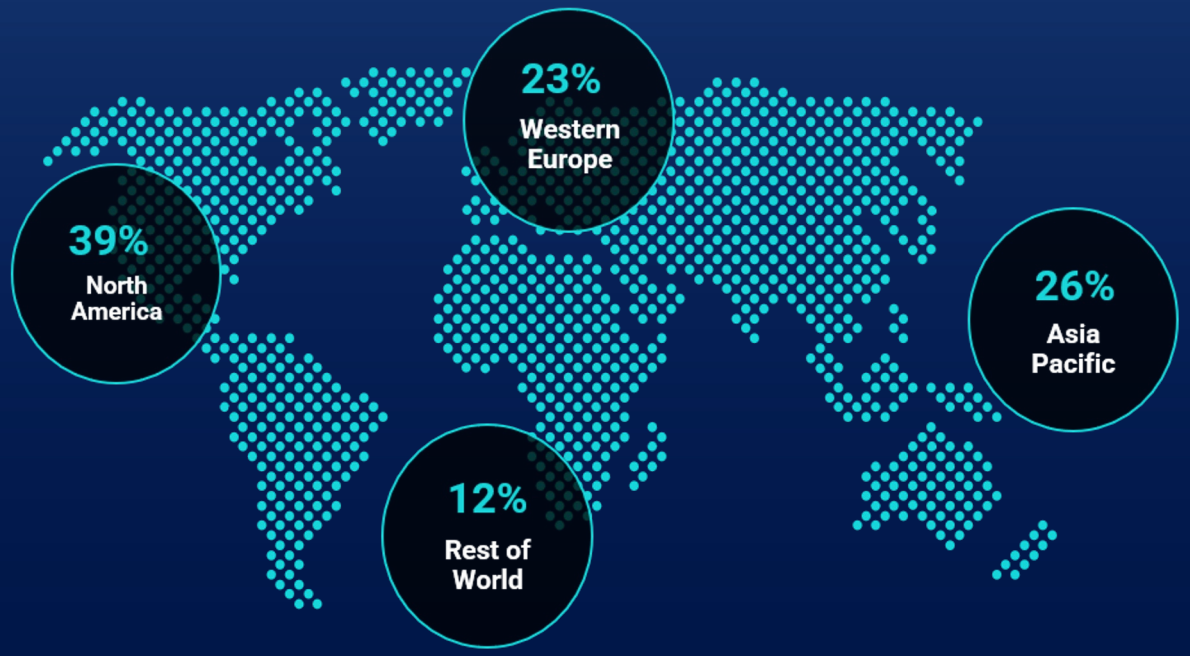
160,000

Employees in over 100 countries

Two businesses

- Energy Management
- Industrial Automation

A well-balanced global presence - 2025 Revenues breakdown



3 megatrends are transforming our world

- New Energy Landscape
- Digital & AI
- Multi-Polar World

4 end markets with global impact

BUILDINGS

DATA CENTERS

INFRASTRUCTURE

INDUSTRY

20 of the largest **energy** companies

40k+ **Water & Environment** installations in **150+** countries

25+ of the world's largest **Airports**

Ranked #1

TIME WORLD'S MOST SUSTAINABLE COMPANIES statista 2024

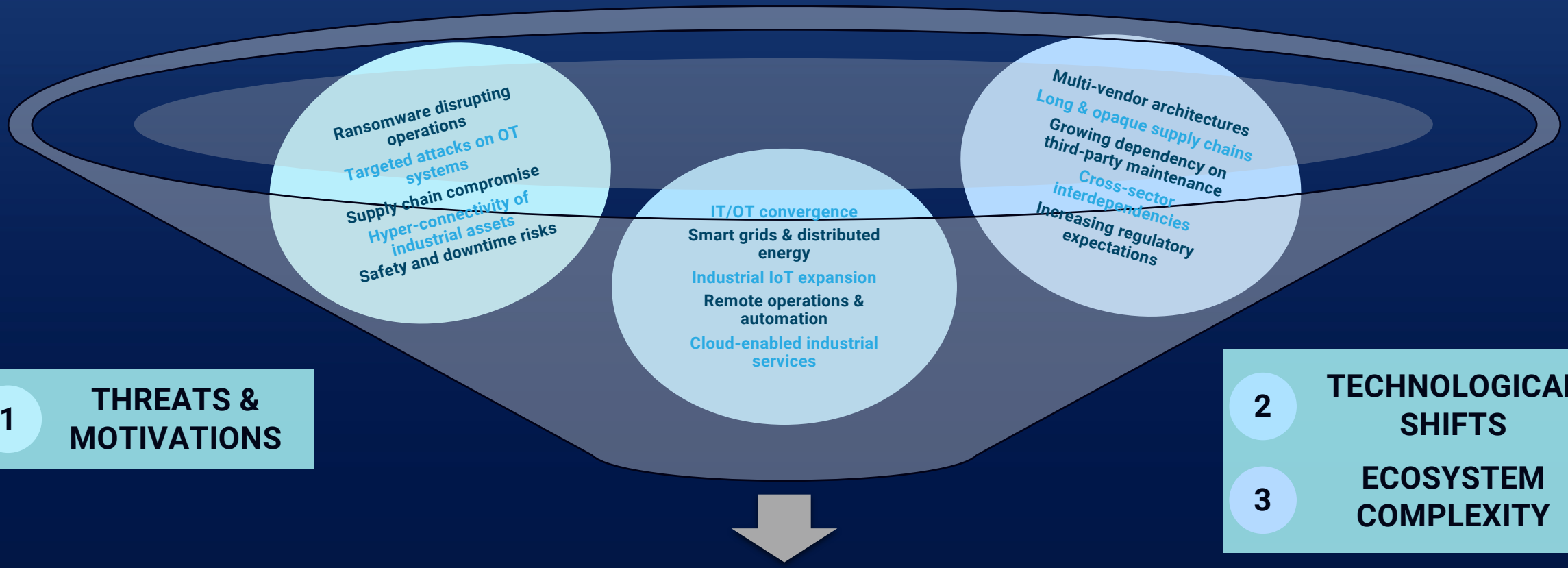
GLOBAL100 2025 THE WORLD'S MOST SUSTAINABLE CORPORATIONS ©

Andre SHORI, APAC Cybersecurity VP and CISO

Andre is the Asia Pacific Cybersecurity Vice President and Chief Information Security Officer at Schneider Electric, leading the region's IT and OT cybersecurity programs. In this role, he is responsible for implementing and enhancing cybersecurity initiatives across diverse markets. His mission remains centred on strengthening cyber relationships with customers, national authorities, partners, and employees alike.

With over 30 years of cybersecurity experience, Andre combines deep technical expertise with strong leadership across complex, multinational environments. Beyond his role at Schneider Electric, Andre actively contributes to the cybersecurity community as a Vice President of the Association of Information Security Professionals (AiSP).

CISOs face an intractable problem: increasingly numerous risks but scarce resources



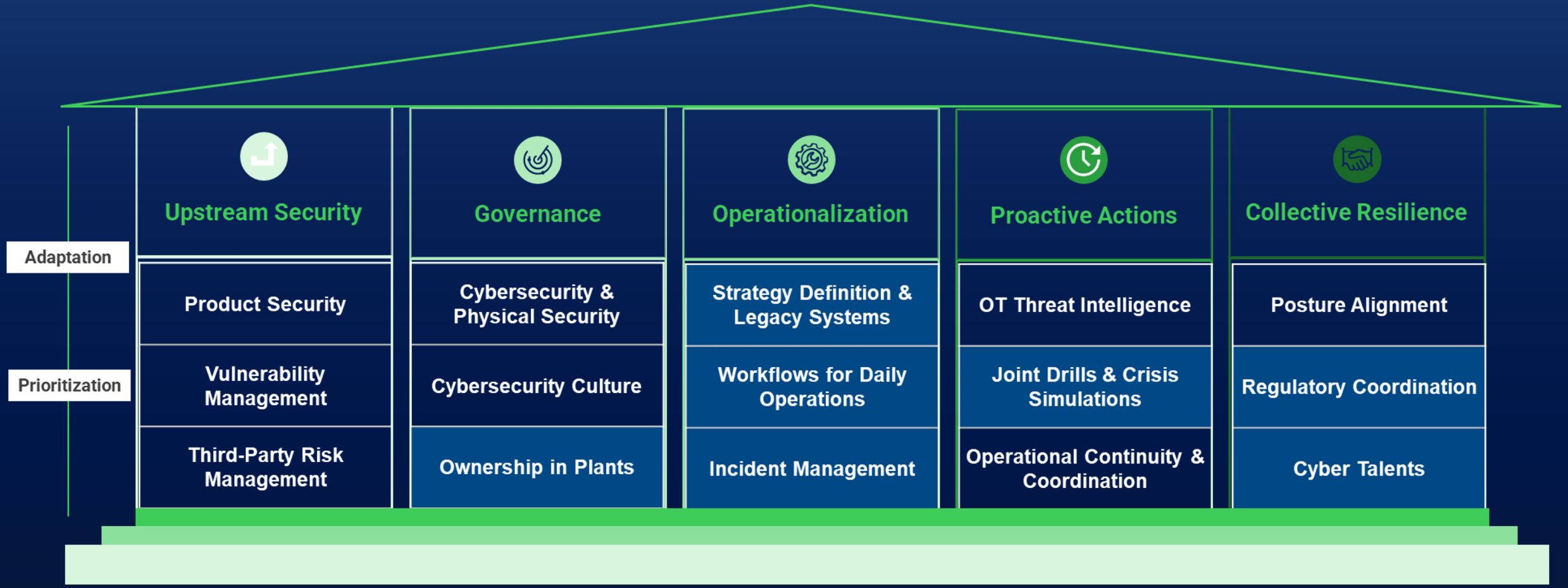
1 **THREATS & MOTIVATIONS**

2 **TECHNOLOGICAL SHIFTS**

3 **ECOSYSTEM COMPLEXITY**

How do we secure critical infrastructure holistically amid rising complexity, without diluting focus?

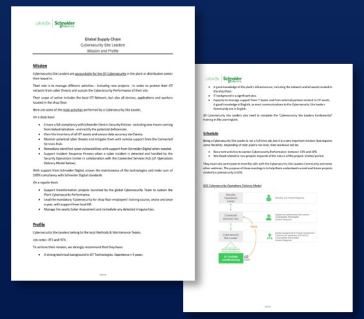
Adopting a holistic and actionable approach to protect critical infrastructure



Between cyber and industrial teams: cybersecurity ownership in plants with cyber site leaders (CSLs)

1. Formalized position

CSL is a formalized job with a dedicated job code within the organization



2. Reporting line

CSL is responsible for the cybersecurity of the plant as this role necessitates seniority and reports to the plant manager

3. Shopfloor education

CSL takes the role of proactive education of shopfloor employees

4. Performance monitoring and reporting

CSL receives reporting of continuous detection of anomalies during operations

5. Cyber Hygiene

CSL implements patching campaigns for all assets with proper inventories

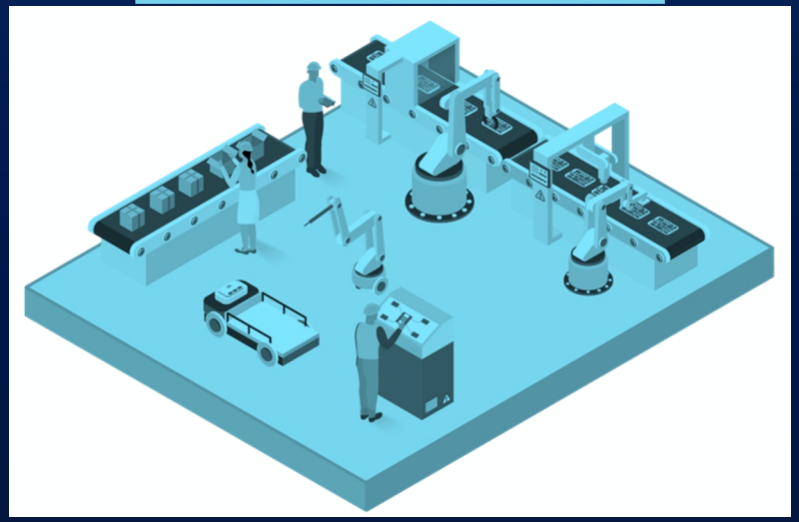
6. Continuous Compliance

CSL ensures continuous compliance with IEC62443 for new manufacturing means

Cybersecurity Site Leader

200+
Cyber site leaders Worldwide

Aligning upfront on how to secure the industrial environment

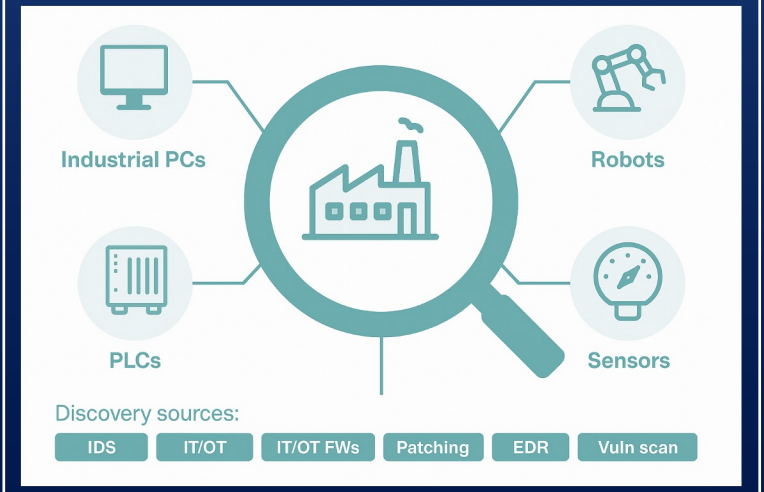


Use Case: Tackling Legacy Systems in Plants

Patching
Network Segmentation
Compensating Controls
Physical Isolation
Upgrade / Replacement

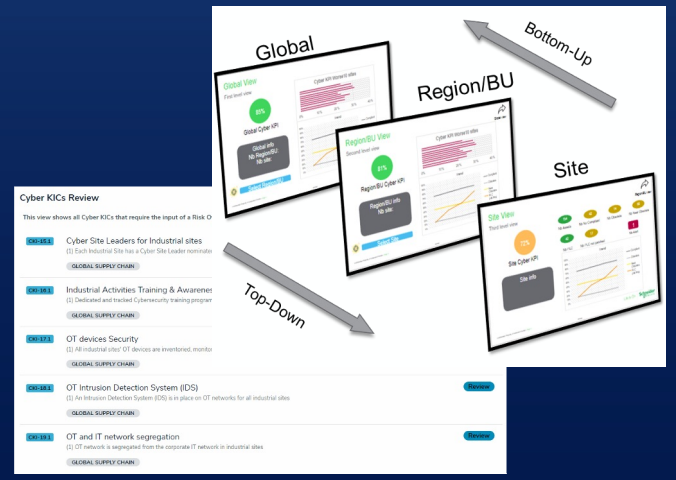
- What is the technical feasibility?
- What is the current risk exposure?
- What is the business criticality of the asset?
- What are the operational constraints?
- Are digital and industrial lifespans aligned?

Integrating operational workflows for a better alignment between cyber and industrial requirements



Visibility & Detection

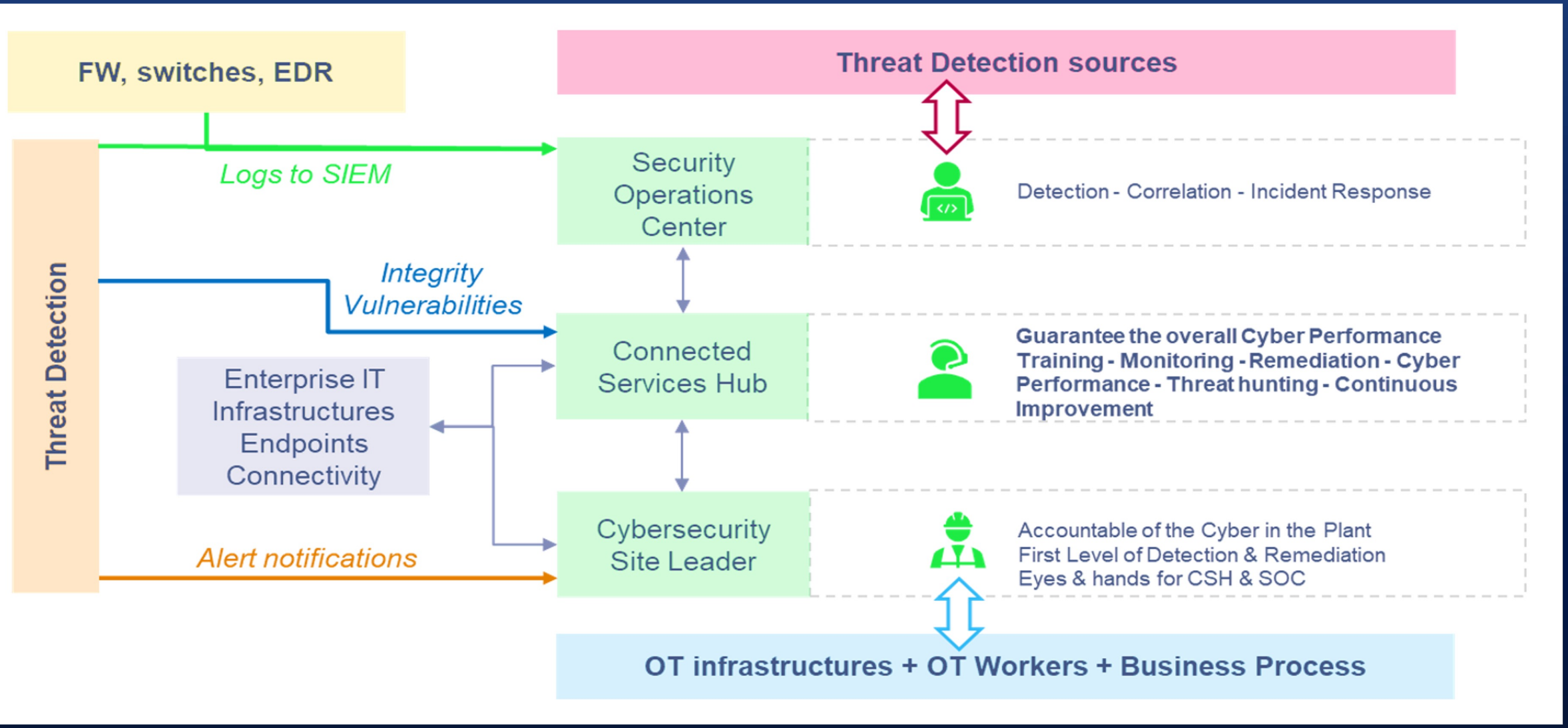
Patching & Maintenance



Monitoring & Evaluation

- ✓ Cybersecurity is featured on the plant dashboard, so shopfloor employees are aware about the topic.
- ✓ Cybersecurity is part of business performance.
- ✓ Cybersecurity performance is indexed in the plant's manager bonus.

By establishing a critical link between the SOC and the industrial field, IT and OT are brought together to operate as one during any incident



From theory to practice: carrying out cyber crisis simulations to test capacities and resilience

Cyber crisis simulations

- **Large-scale** exercises
- Requiring about 6 months of preparation
- Across **2 days** in real conditions
- Involving around **50 players** including **executives**
- Grounding scenarios on our **risk register**
- Triggering response process enhancement

Purpose and benefits

1. **Engage cyber and non-cyber senior executives** at country level in a real environment
2. **Test processes** especially Legal, Crisis Coordination, playbooks etc.
3. **Challenge** incient response to a complex cyber situation endangering its reputation
4. **Foster** cooperation between an OEM, a critical customer and a **national authority**

Tripartite exercises

Stakeholders from various sectors

- Renewable energies
- Gas and Electricity
- Energy storage
- Buildings

National Cyber Authorities Worldwide

High-level Scenario Example

We need to build resilience through some common guidelines and by speaking the same language

Government regulations and actions, the first step and a compass for a resilient cybersecurity strategy

Objectives:

- ✓ Preserving national security
- ✓ Strengthening expanding digital economies

Methodology:

- ✓ Collaborative approach or "multistakeholderism"
- ✓ Regulatory interoperability


REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

ACTS SUPPLEMENT

Published by Authority

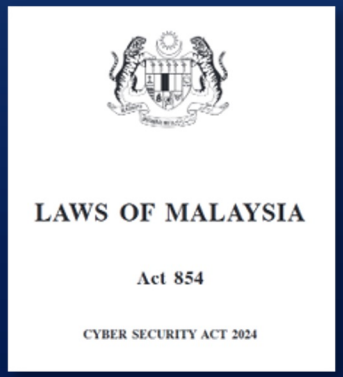
CYBERSECURITY ACT 2018

(No. 9 of 2018)

ARRANGEMENT OF SECTIONS

PART 1

PRELIMINARY


LAWS OF MALAYSIA

Act 854

CYBER SECURITY ACT 2024

Development of markers of trust allowing common understanding in the cyber ecosystem

Objectives:

- ✓ Mutual recognition of similar cyber standards
- ✓ Aligning on global/industry standards

Methodology:

- ✓ Collectively raising the bar across the value chain
- ✓ Collaboration between policymakers and industry on best practices

Addressing the cybersecurity talent gap with a tight collaboration between education and industry

Collaboration opportunities
Addressing collectively real-world cybersecurity challenges and foster innovation.

Curriculum Development
Shaping cybersecurity-related curricula so that students are equipped with the skills and knowledge needed in the industry.

Knowledge Sharing
Establishing forums for knowledge exchange, such as guest lectures, workshops, and seminars.

Industry Certifications
Discussing integration of industry-recognized certifications into academic pathways to enhance students' employability and industry readiness.

Research Partnerships
Collaborating on research projects to develop cutting-edge cybersecurity solutions tailored to the industrial sector, benefiting both sides.

Final Thoughts

- Rethinking cyber resilience means adopting a **holistic, lifecycle** approach.
- Resilience is a **strategic advantage** to operate confidently.
- Critical infrastructure protection rests upon **people and culture**.
- Cybersecurity is a matter of compliance, duty of care, and **societal responsibility**.
- There is no such thing as zero risk in cyber; **maturity** is a **continuous** effort.

THANK YOU