e-BO Enterprises

a brief intro

Bart Claeys
bart.claeys@ebo-enteprises.com

Delivering TRUST for your
critical business

By technology integration of

IT, OT and Software systems

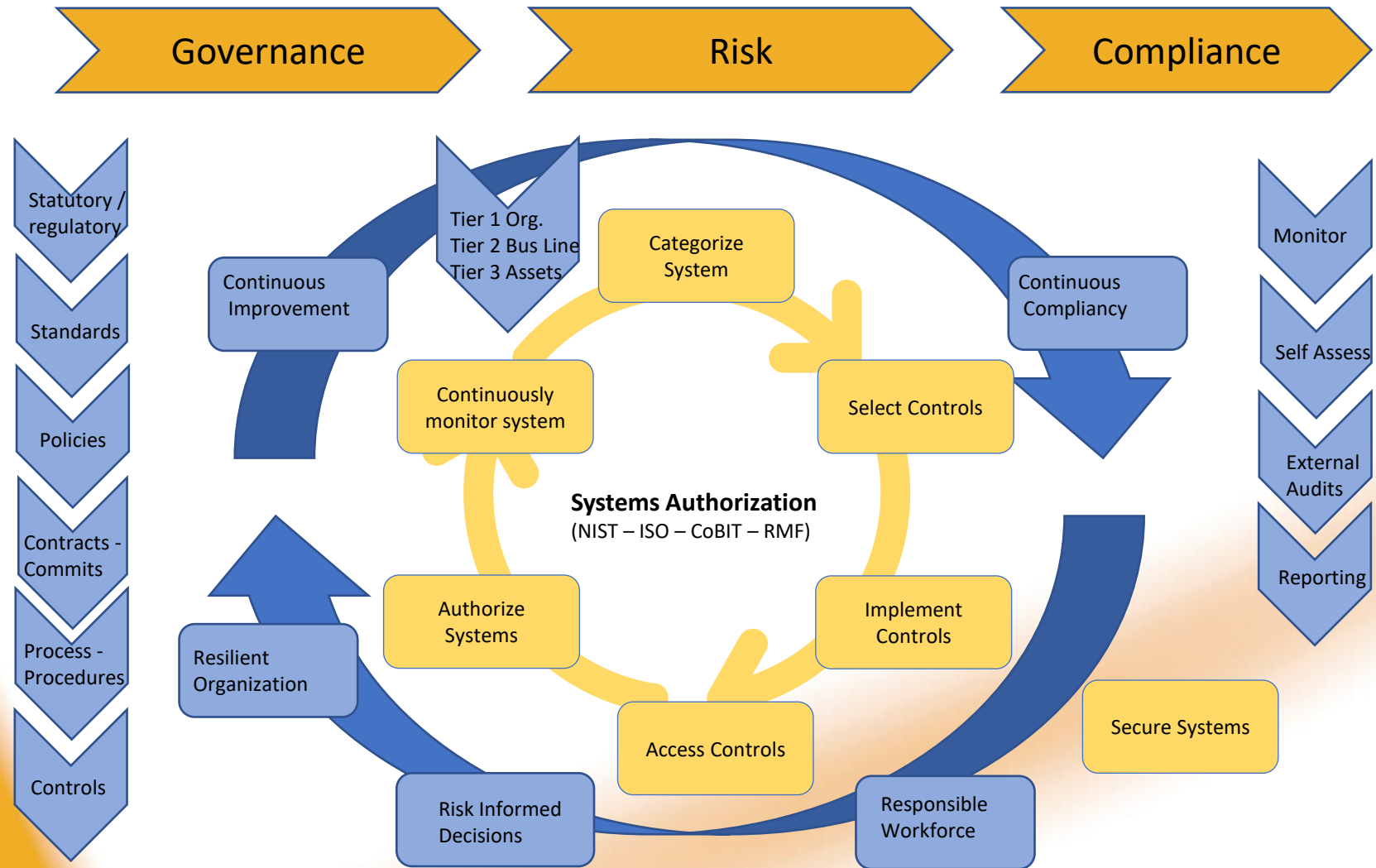Spanning the digital transformation journey in support of
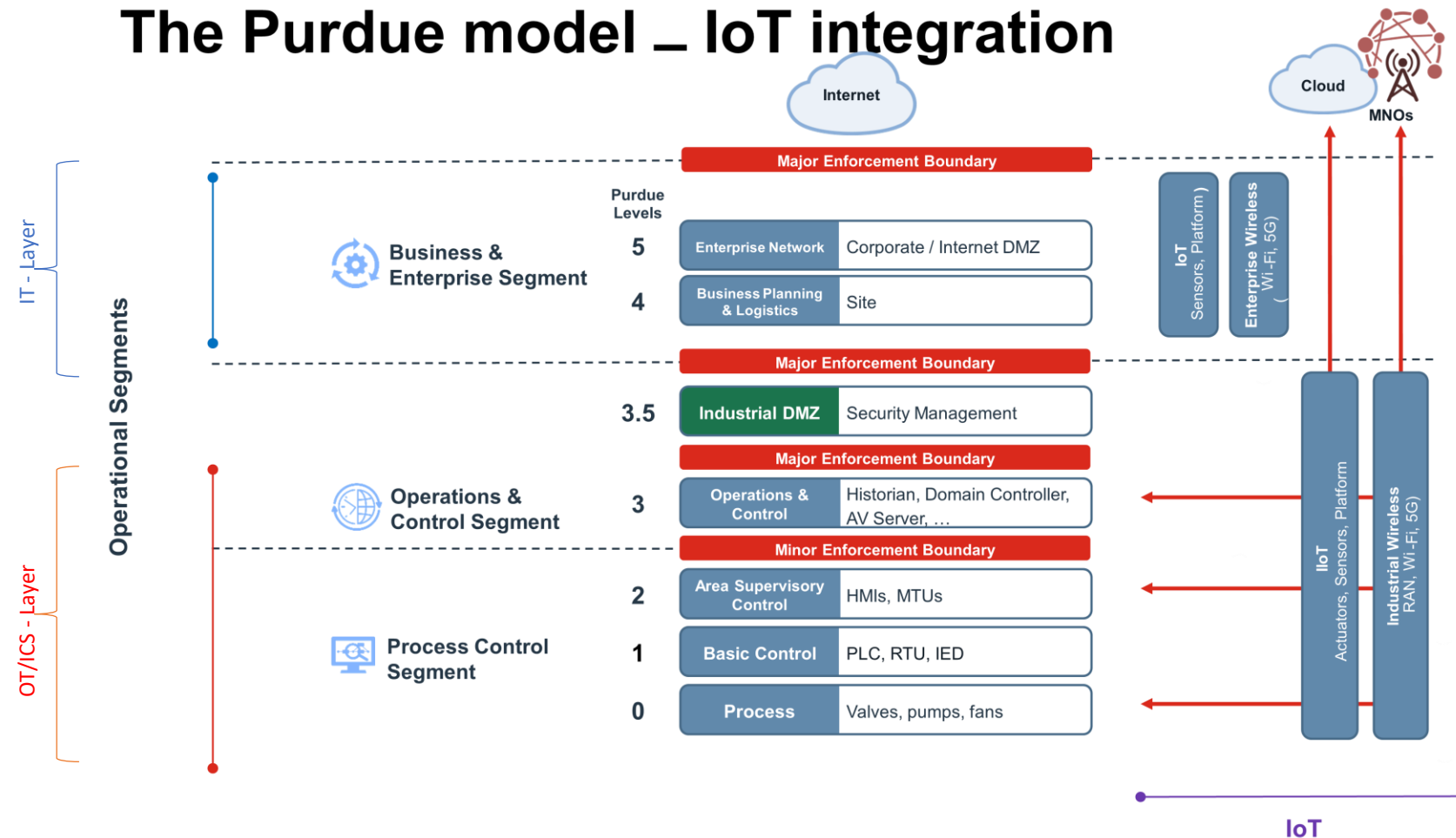
Industry 4.0 & 5.0 adoption

Bart Claeys

bart.claeys@ebo-enteprises.com

Operational Governance model

The Purdue Model as a base Framework

CyberSecurity Threat Landscape – Enisa

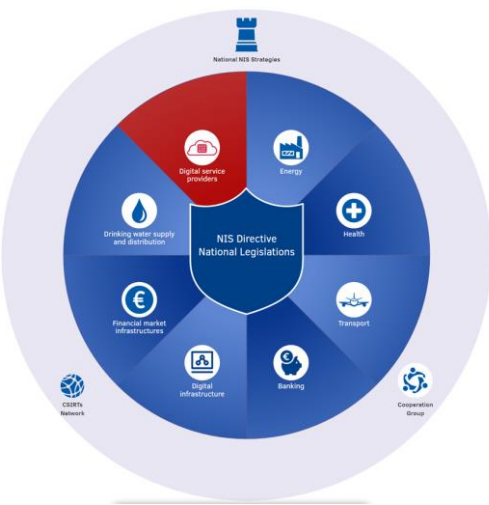Figure 1: ENISA Threat Landscape 2022 - Prime threats

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)

- 0.1K (2.1%)
- 0.14K (3.03%)
- 0.23K (4.81%)
- 0.37K (7.88%)
- 0.39K (8.24%)
- 0.95K (20.09%)
- 1.01K (21.4%)
- 1.48K (31.32%)

PRIME THREATS
- RANSOMWARE
- DDoS
- DATA
- MALWARE
- SOCIAL ENGINEERING
- INFORMATION MANIPULATION
- WEB THREATS
- SUPPLY CHAIN ATTACK
- ZERO DAY
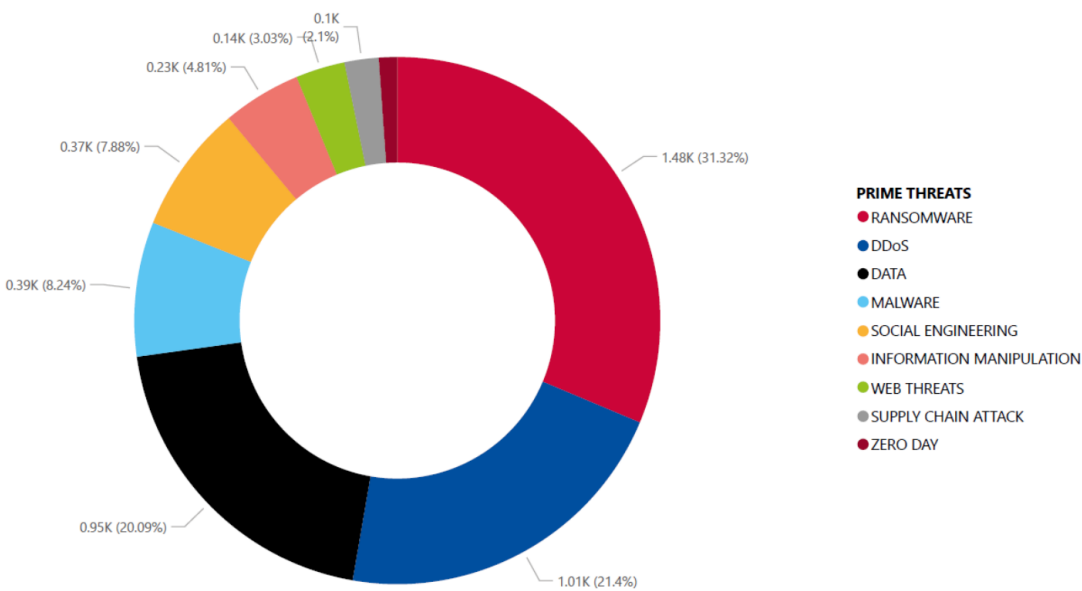
NIS-2 Scope Centre for CyberSecurity BE

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees or more than 50 million revenue)	Medium (more than 50 employees or more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. Energy	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society
2. Transport	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. Banking	Credit institutions (attention: DORA lex specialis)					
4. Financial Market Infrastructure	Trading venues, central counterparties (attention: DORA lex specialis)					
5. Health	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. Drinking Water						
7. Waste Water	(only if it is an essential part of their general activity)					
8. Digital Infrastructure	Qualified trust service providers		Essential	Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment				
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential	Important, except if identified as essential based on National risk assessment	
	Non-qualified trust service providers	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important
	Internet Exchange Point providers					
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations (excluding education institutions)	Member State(s) where established				
Entities providing domain name registration services		**One stop**: Only the MS where they have Main establishment	All sizes, but only subject to Article 3(3) and Article 28			

NIS2 Directive Enhancing Cybersecurity

- *Broader scope*
  cross sector and organizations
- *Risk Management & Cyber Resilience*
  Incident response plans
- *Incident Reporting & Cooperation*
  Report cyber incidents / quicker response
- *Security Measures & Requirements*
  Ensure baseline level security
- *Penalties & Enforcement*
  Stronger incentive to adhere to the requirements
- *Security Culture & Awareness*
  Well-informed workforce to protect valuable assets & respond to threats
- *Continuous Improvement*
  Regularly update & adapt to evolving threats
- *Cross-Border Cooperation*
  Coordinated response to potential cyber incidents

Industrial Security op's Centre

Securing
what's critical

Identify

Do we know our business goals and regulations? Do we know our risks, how they impact our operations, and can we handle the risks?

Respond

How long does it take before we can stop an attack?

Can we isolate the breached segment?

Operate

A fully functional plant, Happy operations manager

Detect

Can we detect any suspicious activity? How do we not get swamped with alarms?

Recover

How do we recover from the incident?

What can we learn from it?

How do we communicate to all stakeholders?

Protect

How do we build a fortress and protect our crown jewels?

IEC 62443 – ISO27001 – NIS2 ready

Foundations for a Sustainable OT Security Program

Define Goals

Creating extensive risk assessments and execution plans in line with the organisation's threat landscape

Establishing mitigation plans and backup strategies for recovering from successful attacks

Defining roles and responsibilities for OT security stakeholders (according to a governance-powered operating model)

Program design & controls
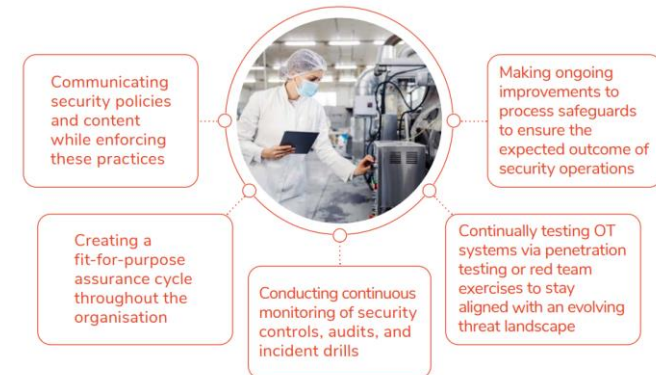
Effective and timely patch management

System hardening

Change management controls

Control Deployment

1. The OT programme management should carefully plan for the entire remediation period and have their main specialists evaluate architecture designs, planned controls and component purchases, and align these with other functional upgrades and planned downtime.

2. The management team should break the master schedule down into phases, with related timetables for purchase and integration.

3. The management team should share these planned timetables with engineering and plant operations teams to limit the impact on existing systems, ongoing operations, and feasibility checks.

4. With engineering-level approval, the OT programme managers should then share plans with executive teams for final purchasing approval.

Maximize Long term impact

Communicating security policies and content while enforcing these practices

Making ongoing improvements to process safeguards to ensure the expected outcome of security operations

Creating a fit-for-purpose assurance cycle throughout the organisation

Conducting continuous monitoring of security controls, audits, and incident drills

Continually testing OT systems via penetration testing or red team exercises to stay aligned with an evolving threat landscape

Evolution of Security Services – NIS2

Specialized Services

- **Specialized OT Security Services**

- **Compliance & NIS2 alignment**

- **Incident Response Services**

- **Risk Assessment & Management**

Continuous Enablement & Awareness

- **Training & awareness programs for OT staff**

- **Continuous monitoring of OT Networks & advanced anomaly detection**

- **Secure-by-Design approach for OT/ICS systems**

Collaboration & Communication

- **Cross sector collaboration among organizations & critical infrastructure sectors**

- **Managed security services, freeing organizations to focus on core operations while ensuring security of critical assets**

Corporate Market
- OT/ICS convergence
- Industrial Cyber Security
- Safeguarding physical assets
- Operational IT Service across Europe

Public safety – Firefighting

Enterprises service bus for fire brigades

Analyzing all applications and sensor data with graphical dashboards

Standardizing and exchanging data across zones

Unified communication services

Public safety- Defence

Defence classified networks through cloud technology for secured data distribution

Information exchange gateways for cross-domain security

Secured remote access

e-BO Market

Private 5G networks

Providing private 5G networks for critical and

zero latency operations (e.g. drones for surveillance, health care, …)

Renewable Energy
The beating heart of your wind farm is digital

OT Security protecting your assets

Public safety - Coast Guard

Maritime Situational Awareness & Incident

Response Management

Securing what's critical

Industrial OT Security
IEC62443 & NIS2 Compliancy

Offshare

One platform for every business activity in your offshore wind farm

OSS in a BOX
CONNECT·CONTROL·CONVERT

An integrated and cyber secure solution with all necessary equipment

Thank You

Mail: info@ebo-enterprises.com

Web: www.ebo-enterprises.com