



# The NIS2 Directive and Fortinet Solutions

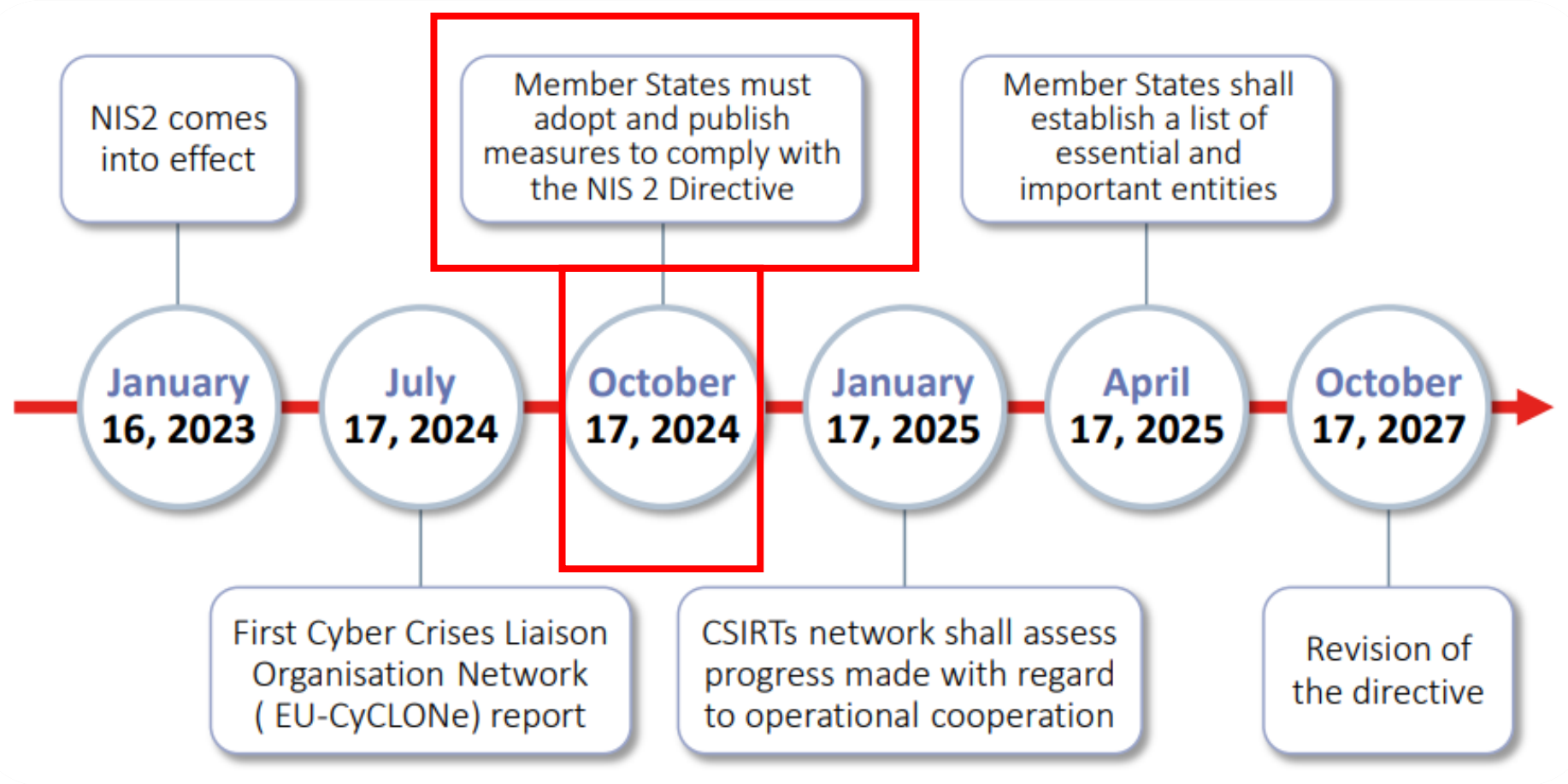
Alexandru Tălpeanu, Channel Systems Engineer

# Background



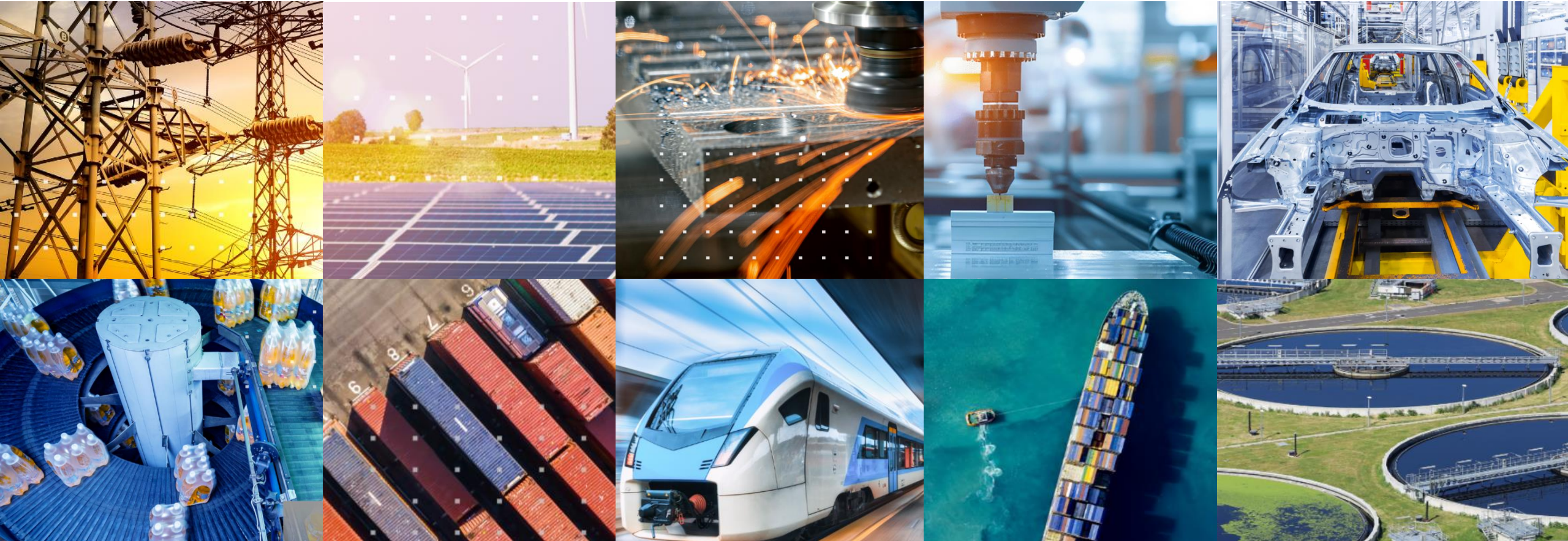
- The first EU-wide law on cybersecurity, the NIS(1) Directive (Directive 2016/1148/EC) came to force in 2016
- NIS Directive is about
  - Information Security
  - Notification of breaches
  - Cybersecurity measures
- NIS Directive helped to **improve the level of security of networks and information systems** across the EU
- Paved the way for significant change in mindset
- Two groups
  - Operators of essential services
  - Digital service providers

# The time is now!





# A BIT OF CONTEXT...





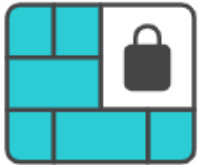
# CRITICAL INFRASTRUCTURE CONTEXT



The Ukraine conflict highlighted a complicated pattern of convergence between state-sponsored APTs and ransomware operators.



APT actors are using flaws to target European critical infrastructure and use them to disrupt physical operations.



**1,100 / week**  
cyber attacks on  
utilities in 2022



**\$1 billion**  
loss to ransomware  
in 2023



# MANUFACTURING CONTEXT – TYPES OF THREATS

## Ransomware Attacks

In the manufacturing sector, time is money, and any delay in manufacturing can result in significant losses. For this reason, ransomware attacks are particularly effective.

## Equipment Sabotage

Malicious actors attempt to damage or disable critical equipment within a manufacturing facility to cause significant disruption to production processes.

## Supply Chain Attacks

Third-party vendors pose a risk, as they are often targeted by malicious actors as a way to gain access to sensitive systems or data within the manufacturing organization.

## Intellectual Property Theft

Attackers may target manufacturing organizations to steal valuable trade secrets, product designs, or customer data, which can be sold or used to gain a competitive advantage.

## Industrial IoT Attacks

Operators in this sector deploy connected devices to monitor and control production processes. These devices can be vulnerable to attacks, particularly if they are not properly secured.

## Phishing Attacks

Phishing attacks are a major threat to this sector, as employees can be tricked into leaking valuable data, including intellectual property and customer information.

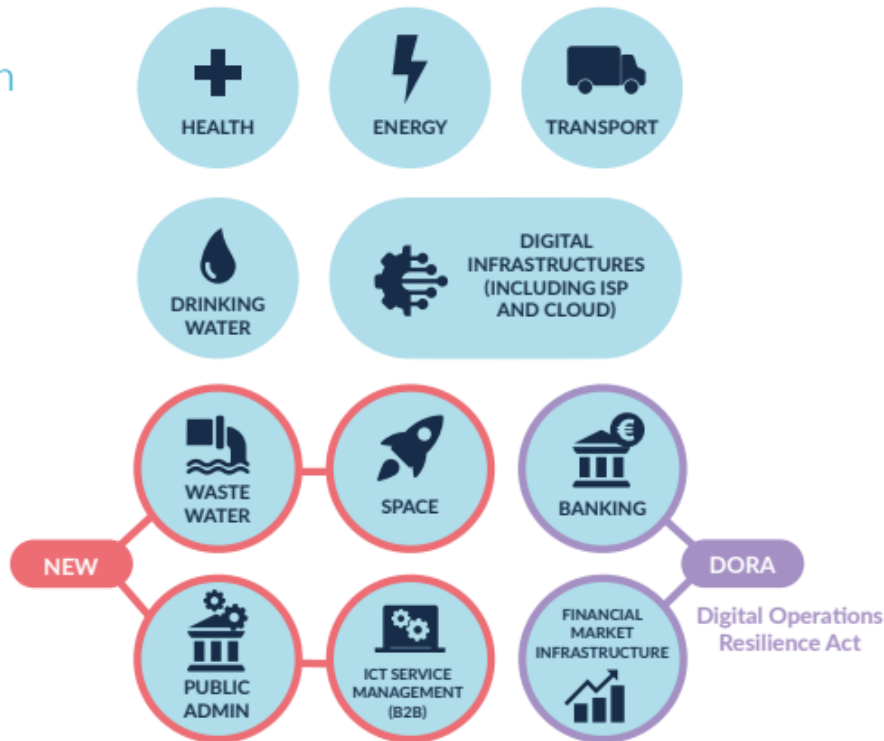


# SECTORS & ENTITIES IN SCOPE

NIS2 includes new sectors whilst broadening the criteria for inclusion of entities, categorised as “**essential**” or “**important**”, within existing sectors.

The sectors are divided into two groups: “**Sectors of High Criticality**” and “**Other Critical Sectors**”.

Annex 1 -  
Sectors of High  
Criticality





Annex 2 -  
Other Critical  
Sectors



SECTOR	SUB-SECTOR	LARGE ENTITIES (≥ 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
--------	------------	---	--	------------------------

## Annex I: Sectors of high criticality









	ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Special case: public transport: <u>only</u> if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	BANKING	Credit institutions (attention: DORA lex specialis – see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties (attention: DORA lex specialis – see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	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	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Special case: entities holding a distribution authorization for medicinal products: <u>only</u> if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
	WASTE WATER	( <u>only</u> if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
		DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
		TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
		Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
		Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
		Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
		Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
	SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE





SECTOR	SUB-SECTOR	LARGE ENTITIES (≥ 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
--------	------------	---	---	------------------------

## Annex II: other critical sectors

 <b>POSTAL AND COURIER SERVICES</b>		IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>WASTE MANAGEMENT</b>	( <i>only</i> if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>CHEMICALS</b>	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>FOOD</b>	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>MANUFACTURING</b>	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>DIGITAL PROVIDERS</b>	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>RESEARCH</b>	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
 <b>ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES</b>	All sizes, but only subject to Article 3(3) and Article 28			

## Notes:

*Entities designated as Critical entities under Directive (EU) 2022/2557, (CER Directive) shall be considered Essential entities under NIS2.*

*Lex Specialis may apply where sectoral regulations are at least equivalent.*

*There are certain exceptions to the above guide, please consult the text of the Directive for a full and comprehensive list of all exceptions.*

# MANAGEMENT RESPONSIBILITIES

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities.

Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

	<b>Approve the adequacy</b> of the cybersecurity risk management measures taken by the entity;
	<b>Supervise the implementation</b> of the risk management measures;
	<b>Follow training</b> in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity
	<b>Offer similar training to their employees</b> on a regular basis;
	<b>Be accountable</b> for the non-compliance

# ENFORCEMENT & PENALTIES

<b>A</b>	Issue <b>warnings</b> for non-compliance
<b>B</b>	Issue <b>binding instructions</b>
<b>C</b>	Order to <b>cease conduct</b> that is non-compliant
<b>D</b>	Order to <b>bring risk management measures</b> or reporting obligations in compliance to a specific manner and within a specified period
<b>E</b>	Order to <b>inform the natural or legal person(s)</b> to whom they provide services or activities which are potentially affected by a significant cyber threat
<b>F</b>	Order to <b>implement the recommendations</b> provided as a result of a security audit within a reasonable deadline
<b>G</b>	<b>Designate a monitoring officer</b> with well-defined tasks over a determined period of time to oversee the compliance
<b>H</b>	Order to <b>make public</b> aspects of non-compliance
<b>I</b>	Impose administrative <b>fin</b> es
<b>J</b>	An essential entities <b>certification or authorisation concerning the service can be suspended</b> , if deadline for taking action is not met
<b>K</b>	And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily <b>prohibited from exercising managerial functions</b> (applicable to essential entities only, not important entities).

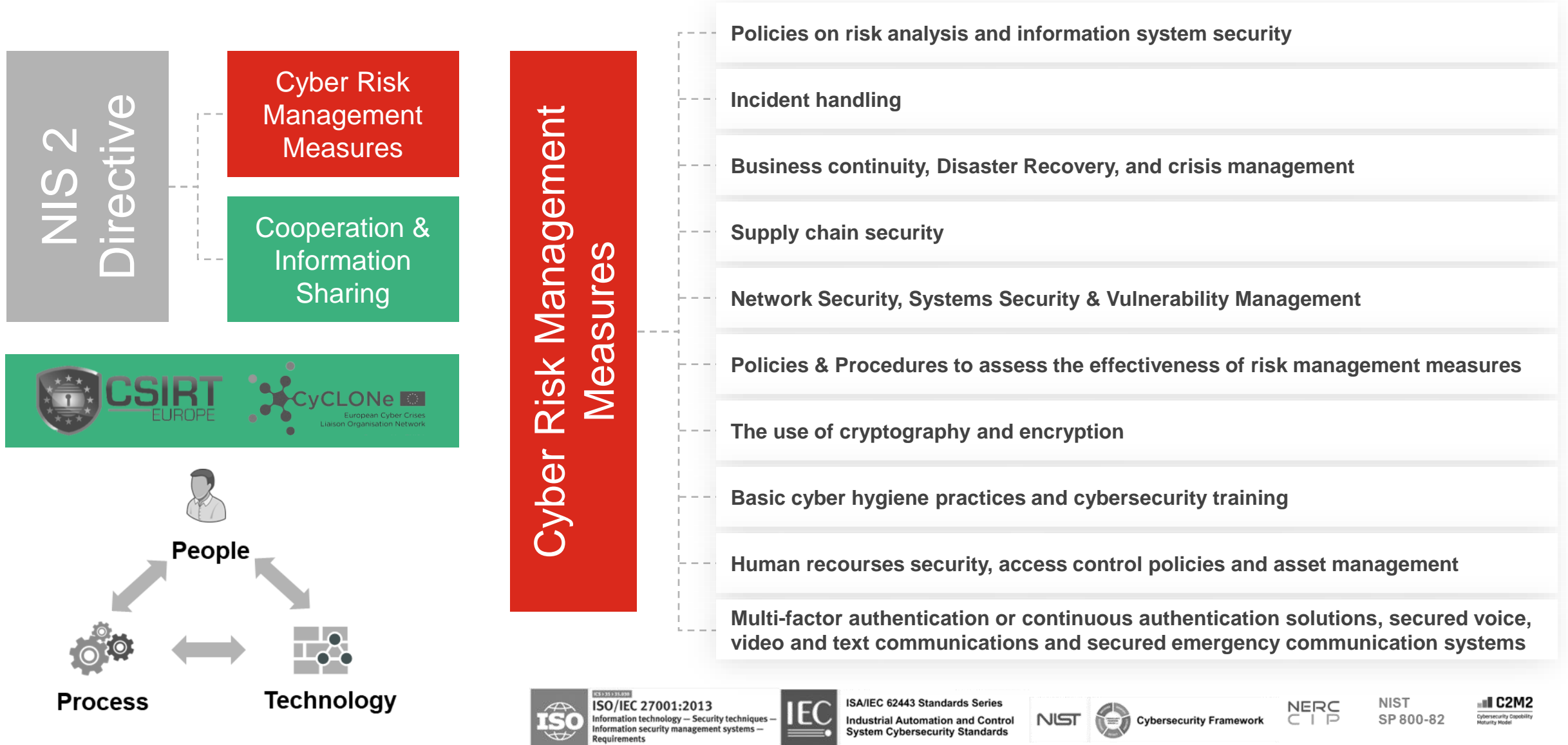
A maximum of **at least 10,000,000 EUR** or up to **2% of the total worldwide annual turnover** of the undertaking to which the **ESSENTIAL ENTITY** belongs in the preceding financial year, whichever is higher.

A maximum of **at least 7,000,000 EUR** or **1,4% of the total worldwide annual turnover** of the undertaking to which the **IMPORTANT ENTITY** belongs in the preceding financial year, whichever is higher.





# NIS2 Compliance pillars for EEs & IEs



# NIS2 Management Measures and Fortinet Products

Cyber Risk Management Measures



## Technology Framework

## Fortinet Solutions

Policies on risk analysis and information system security

- Digital Risk Management tool
- Security orchestration and event management & correlation
- Generative AI.



FortiSIEM



FortiSOAR



FortiAI



FortiRecon

Incident handling

- Threat Detection & response,
- Easy integration across security functions, monitoring and reporting systems. (Fabric Connectors)



FortiSOAR



FortiSIEM



FortiEDR



FortiNDR

Business continuity, Disaster Recovery, and crisis management

- Resilient architectures
- Smart High-Availability
- Efficient Disaster Recovery



HA



FortiADC



FortiSOAR

Supply chain security

- DevSecOps
- Code vulnerability Assessment & Management



FortiCNAPP



FortiDevSec



FortiRecon



FortiDAST

Network Security, Systems Security & Vulnerability Management

- Access Control
- Network segmentation
- API Security
- Deep traffic inspection
- Vulnerability sharing
- Data protection



FortiGate NGFW



FortiWeb



ZTA



FortiScanner

Policies & Procedures to assess the effectiveness of risk management measures

- Asset management
- Risk profiling
- Security monitoring, auditing, and testing



FortiTester



FortiSIEM



FortiSOAR



FortiAnalyser

The use of cryptography and encryption

- Asset management
- Risk profiling
- Security monitoring, auditing, and testing



FortiGate SecGW



SSL



IPsec

Basic cyber hygiene practices and cybersecurity training

- Security Awareness Training



Fortinet Awareness Training



Fortinet Training Institute

Human resources security, access control policies and asset management

- Access Control
- Identity Management
- Asset management



FortiToken



FortiAuthenticator



FortiPAM



FortiClient

Multi-factor authentication or continuous authentication solutions

- Access Control
- Identity Management



FortiToken



FortiAuthenticator



FortiPAM

# Fortinet Fabric Portfolio

## Secure Networking



### Network Security



FortiGate  
Firewall



FortiGate VM  
Virtual Firewall



FortiCNF  
Cloud-native  
Firewall



FGaaS  
Firewall-aaS



FortiGate  
Rugged NGFW

### Enterprise Networking



FortiSwitch  
Switching



FortiAIOps  
AI For Networking



FortiAP  
Access Point



FortiNAC  
NAC



FortiSwitch  
Rugged Switch



FortiExtender  
LTE/5G



FortiAP  
Rugged AP



FortiExtender  
Rugged Extender



FortiManager  
Centralized Management

## Unified SASE



### Secure Access



FortiSASE  
SSE



FortiClient  
ZTNA



FortiMonitor  
DEM



FortiGate  
SD-WAN



FortiProxy  
SWG



FortiCASB  
CASB

### Cloud Security



FortiGate VM  
Virtual Firewall



FortiWeb  
(WAAP)



FortiGate CNF  
Cloud-native  
Firewall



FortiADC  
Application  
Delivery

## Security Operations



Lacework  
FortiCNAPP



FortiEDR/XDR  
EDR/XDR



FortiDeceptor  
Deception



FortiRecon  
DRPS



FortiAuthenticator  
Cloud



FortiToken  
MFA



FortiNDR  
NDR



FortiSIEM  
SIEM



FortiSOAR  
SOAR



FortiSandbox  
Sandbox



FortiPAM  
PAM



FortiNext DLP  
DLP



FortiAnalyzer  
Analytics



SOCaaS



MDR Service



IR Service



FortiMail  
SEG

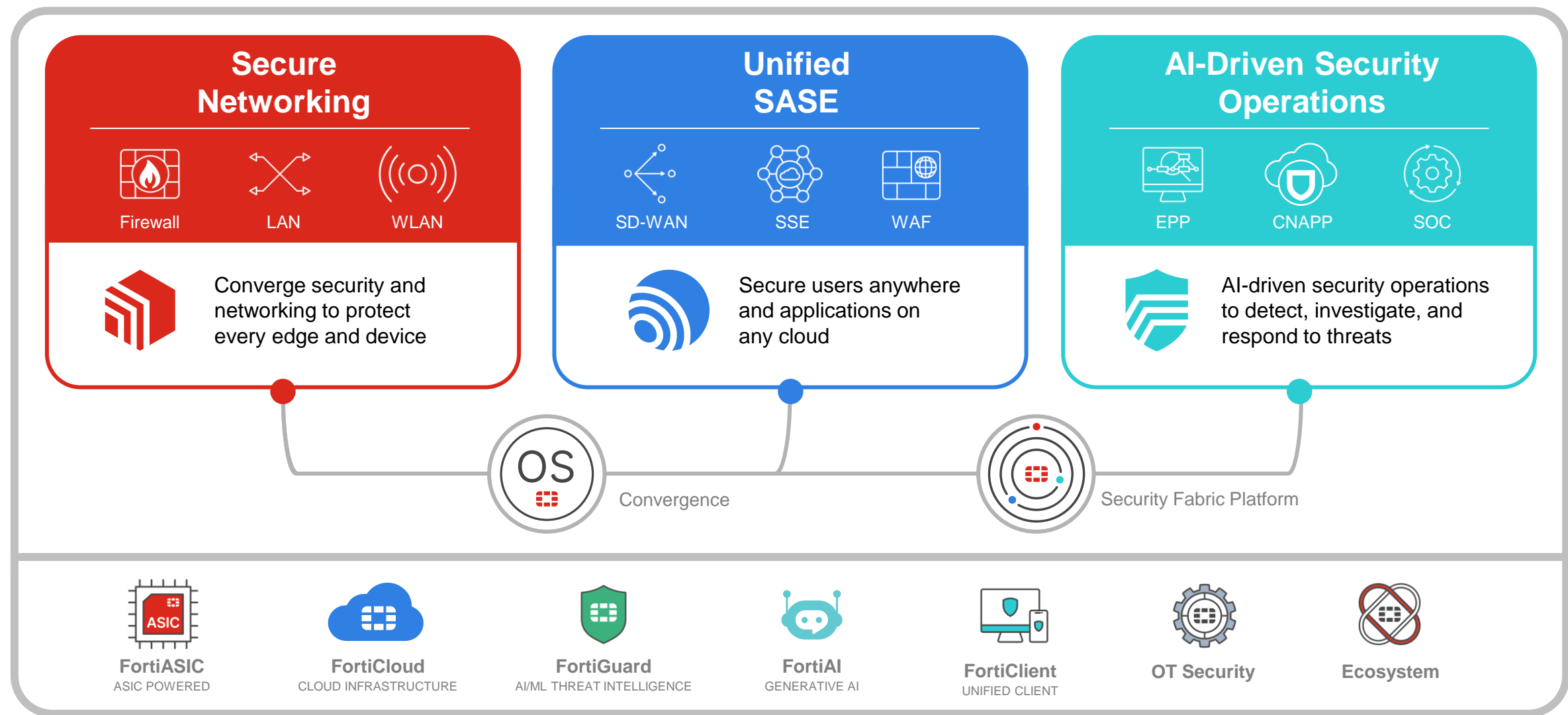


FortiTrust  
Identity





# The Most Comprehensive & Advanced Cybersecurity Platform

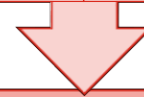


# Incident Reporting

## Significant Incident

Caused or can cause severe **operational disruption** of the services or **financial loss**

Has affected or can affect **other natural or legal persons** by causing considerable material or non-material damage



## Immediate Action

Inform recipients of service about measures or remedies that recipients might take



## 24 hours / Early Warning

of becoming aware of significant incident, an early warning to the authorities to be made

Confirm whether the incident has a cross-border impact



## 72 hours / Official Notification

of becoming aware of significant incident, an incident notification to be made to the authorities about the severity and impact and the indicators of compromise



## 1-month full report / Final Report

Provide report on incident description, severity, impact, threat, root cause, mitigation, cross border impact

Intermediate Status Report before the Final Report might be requested



