



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

UPDATES ON THE EU CYBERSECURITY POLICY FRAMEWORK

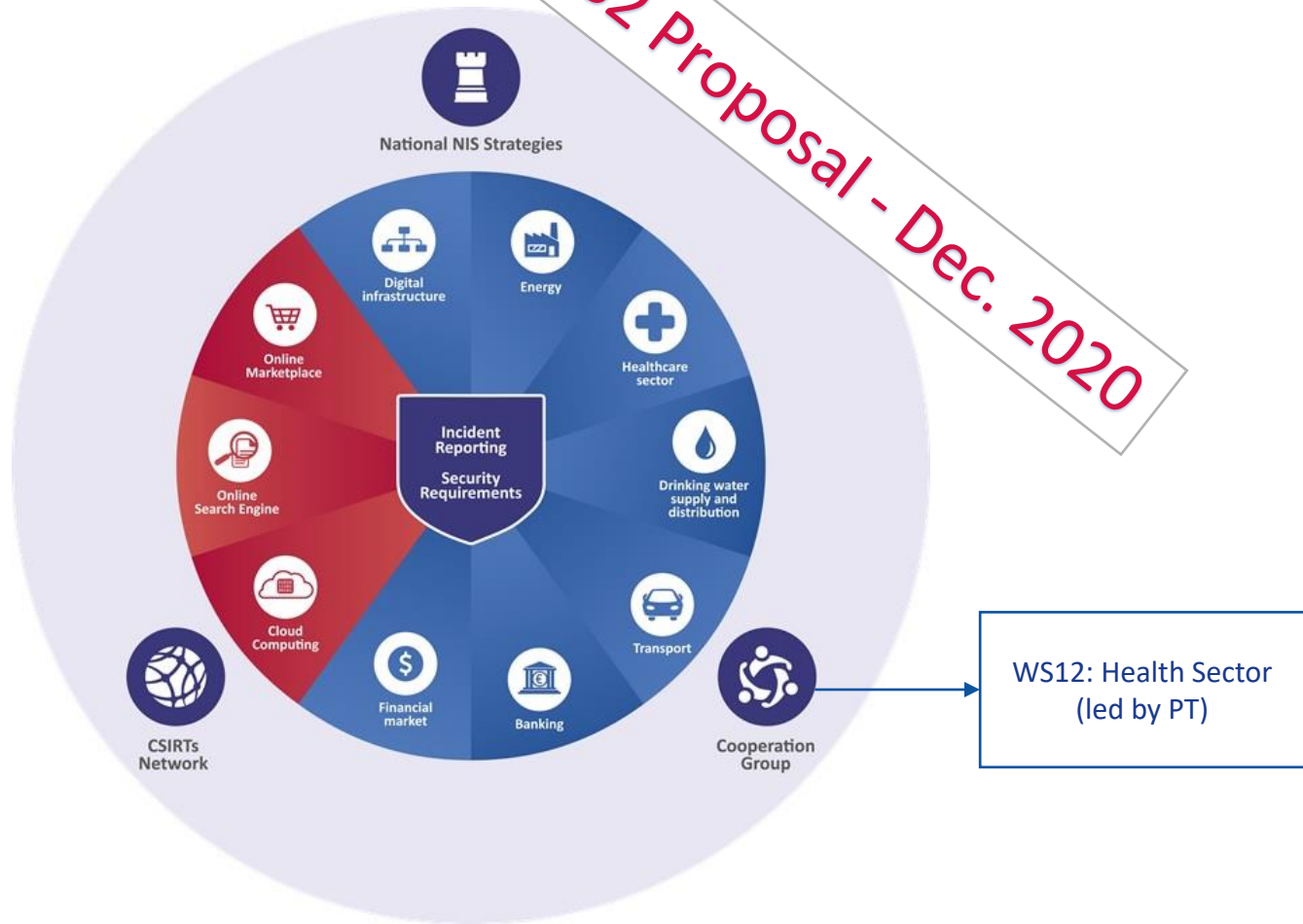
Dr. Athanasios Drougkas
Cybersecurity Expert

7th eHealth Security Conference

10 | 10 | 2022

THE NIS DIRECTIVE

NIS2 Proposal - Dec. 2020



NIS2 PROPOSAL

Sectors with essential entities

Sectors with important entities

Essential entities under NIS2		
Digital infrastructures	Telecom networks (mobile, fixed, satellite)	Previously under EEECC
	Core internet infrastructure – IXPs, TLDs, DNS, CDNs*	Already in NIS1
	Trust services (webcertificates, e-signatures)	Previously under EIDAS
	Cloud and datacenters*	Already in NIS1, now essential
Energy	Electricity	Already in NIS1
	District heating and cooling	New in NIS2
	Oil	Already in NIS1
	Gas	Already in NIS1
	Hydrogen	New in NIS2
Transport	Air – aviation	Already in NIS1
	Rail	Already in NIS1
	Water - Maritime transport, port management, vessel traffic services	Already in NIS1
	Road – road authorities and intelligent transport systems	Already in NIS1
Finance	Financial market infra, banking, trading, central counterparties	Already in NIS1
Health	Health care providers, EU reference laboratories, medicinal research, manufacturing of pharmaceuticals, critical medical devices	Already in NIS1
Drinking water	Suppliers and distributors	Already in NIS1
Waste water	Collection, disposal and treatment	New in NIS2
Public administration	Central government and regions	New in NIS2
Space	Operators of ground-based infrastructure, supporting space-based services, excluding providers of satellite communications	New in NIS2

Important entities under NIS2		
Digital services	Online marketplaces, online search engines, social networks	Already in NIS1, but social networks is new
Posts and couriers	Postal service providers and providers of courier services	New in NIS2
Waste management		New in NIS2
Chemicals	Manufacturing, production, distribution	New in NIS2
Food	Food production, processing and distribution	New in NIS2
Manufacturing	Medical devices and in vitro diagnostic medical devices	New in NIS2
	Computers, electronics and optical products	
	Electrical equipment	
	Machinery and equipment n.e.c. (not elsewhere classified)	
	Motor vehicles, trailers and semi-trailers	

THE NISD2.0 PROPOSAL MAIN PILLARS

MEMBER STATE CAPABILITIES



National authorities
National strategies
CVD frameworks
Crisis management frameworks

RISK MANAGEMENT & REPORTING



Accountability for top management for non-compliance
Essential and important companies are required to take security measures
Companies are required to notify significant incidents & cyber threats

COOPERATION AND INFO EXCHANGE





Cooperation Group
CSIRTs network
CyCLONe
CVD and European vulnerability registry
Peer-reviews
Biennial ENISA cybersecurity report

CYBER RESILIENCE ACT -CRA

- **Rules for placing on the market** of products with digital elements to ensure the cybersecurity of these products
- **Essential requirements** for product design, development and production and obligations for economic operators (manufacturers, distributors etc.)
- Essential requirements for vulnerability handling to ensure product **cybersecurity throughout the lifecycle**
- **Rules on market surveillance** and enforcement of requirements

Commission proposal published in September!



CRA Scope: *The CRA proposal applies to all products with digital elements connected directly or indirectly to another device or network except for specified exclusions such as open-source software or services that are already covered by existing rules, which is the case for medical devices (MDR, IVDR)*

CRA - ESSENTIAL REQUIREMENTS

Essential product requirements

- Properly installed, maintained, used for their intended purpose or reasonably foreseeable use, and, where applicable updated
- Security by design
- Delivery of products without known vulnerabilities
- Secure default configuration
- Access control
- Limited attack surface
- Security update capabilities
- etc.

CRA – OBLIGATIONS FOR MANUFACTURERS

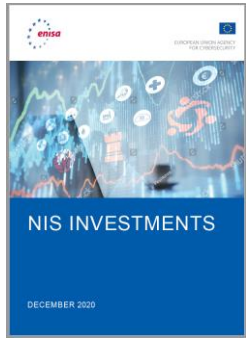
Obligations for manufacturers

- **Vulnerability** handling including identification and documentation of vulnerabilities, remediation of vulnerabilities without delay, security testing, public disclosure of fixed vulnerabilities, secure distribution of updates etc.
- **Undertaking product cybersecurity risk assessment**, documentation, due diligence for third party components, provisions to ensure product conformity throughout the lifecycle including implementing corrective measures etc.
- **Reporting obligations** for actively exploited vulnerabilities, incidents having an impact on products with digital elements, corrective measures that users can apply, vulnerability handling for open source components etc.

OTHER POLICY FILES

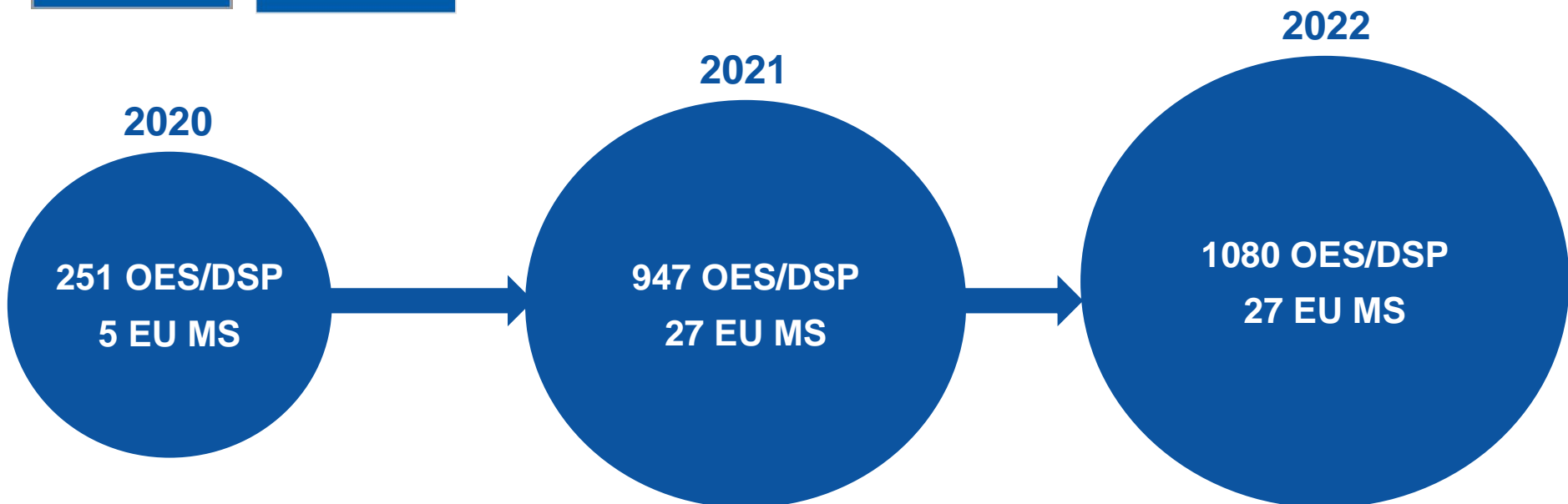
- AI Act
- Chips Act
- Data Act
- **European Health Data Space**

2022 NIS INVESTMENTS REPORT

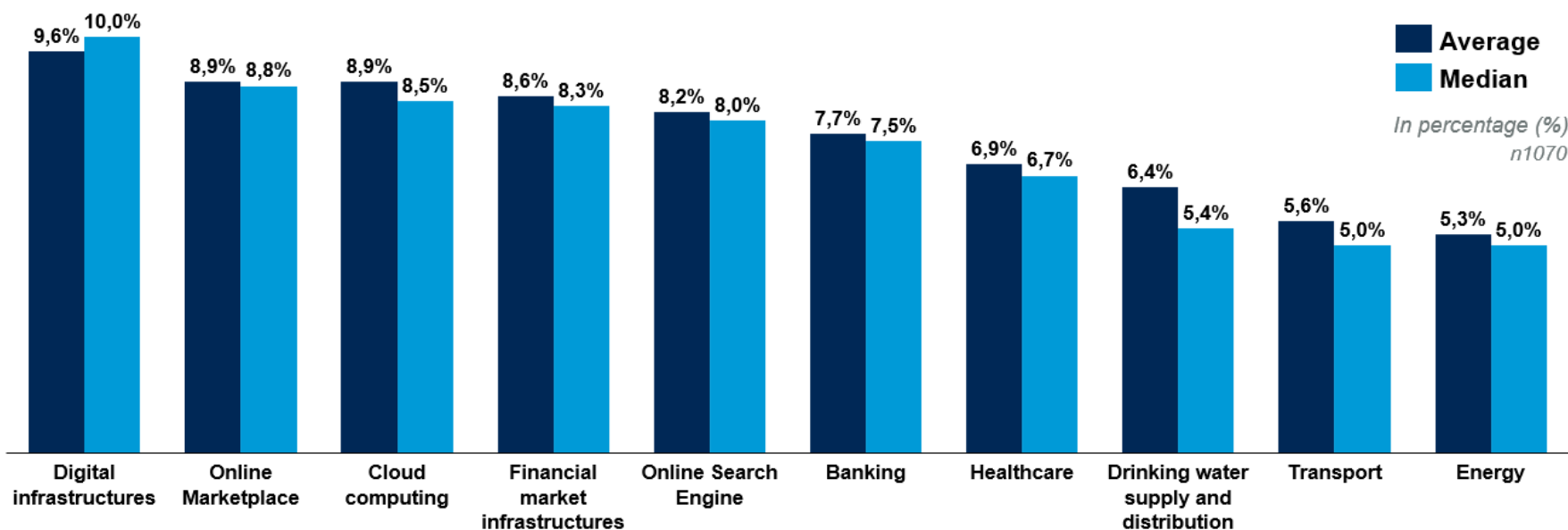


Sectorial deep dive in health (2022):

- 189 Health OES in total
- Additional questions on medical devices, cloud and awareness

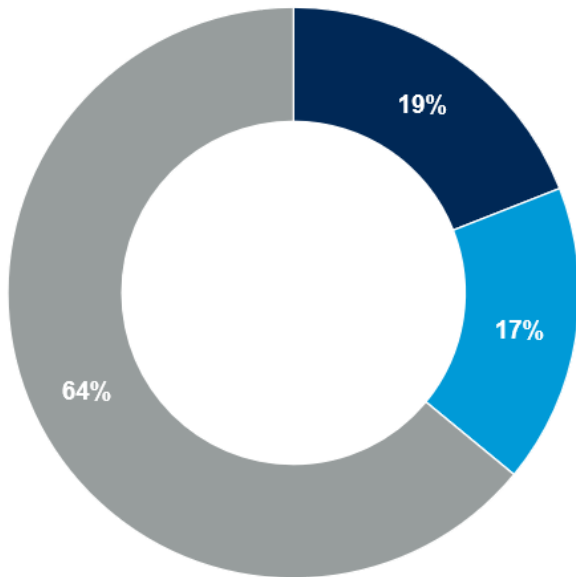


INFORMATION SECURITY SPENDING AS % OF IT BUDGETS



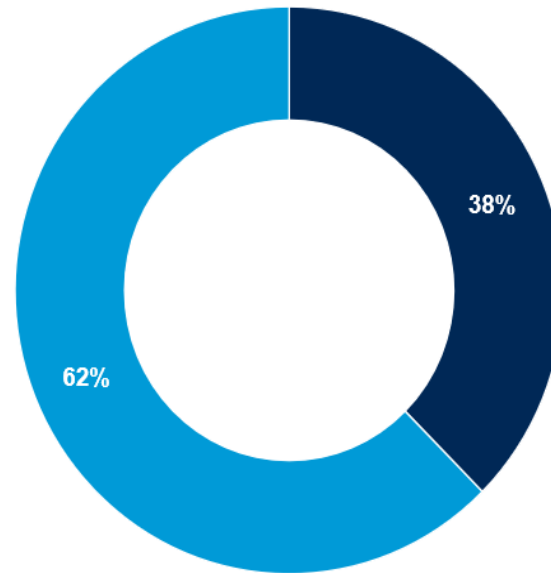
NB: Absolute values vs. percentages (e.g. Health OES were 94% LE)!

MEDICAL DEVICE SECURITY



Connected medical devices in Health

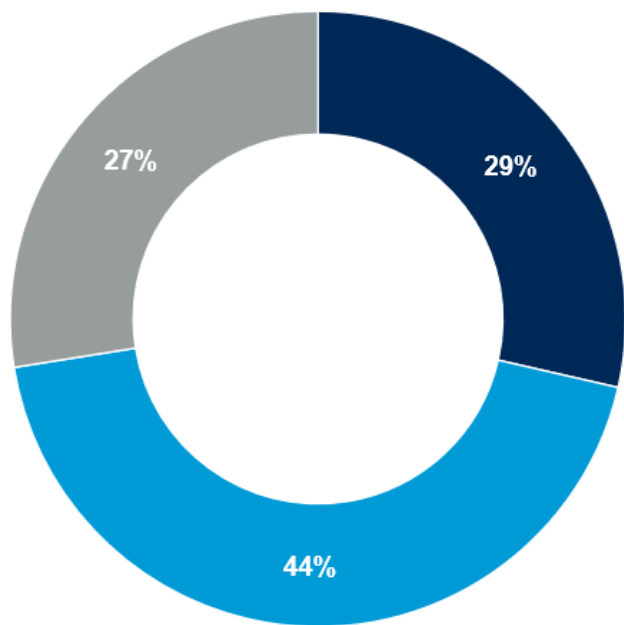
- No, but we are planning to deploy connected medical devices in 2022
- No, we are not planning to deploy connected medical devices in the short term
- Yes, we are already using connected medical devices



Security solutions for medical devices

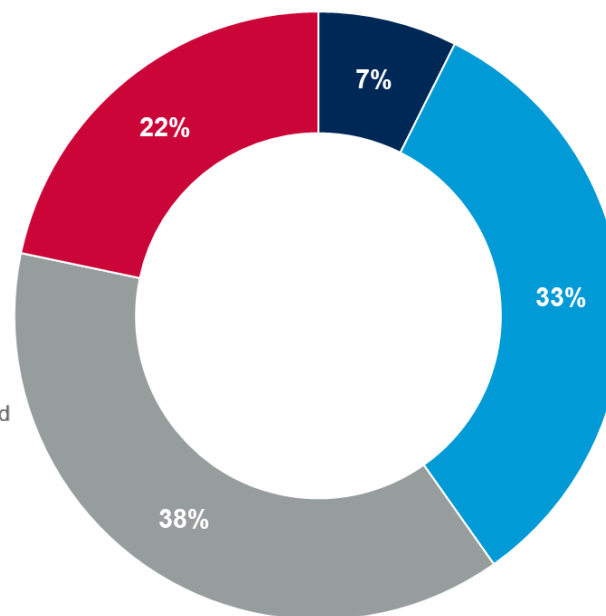
- No, we do not have deployed any security solutions for medical devices
- Yes, we have deployed security solutions specific for medical devices

PROTECTION AGAINST RANSOMWARE?



Ransomware defense programs

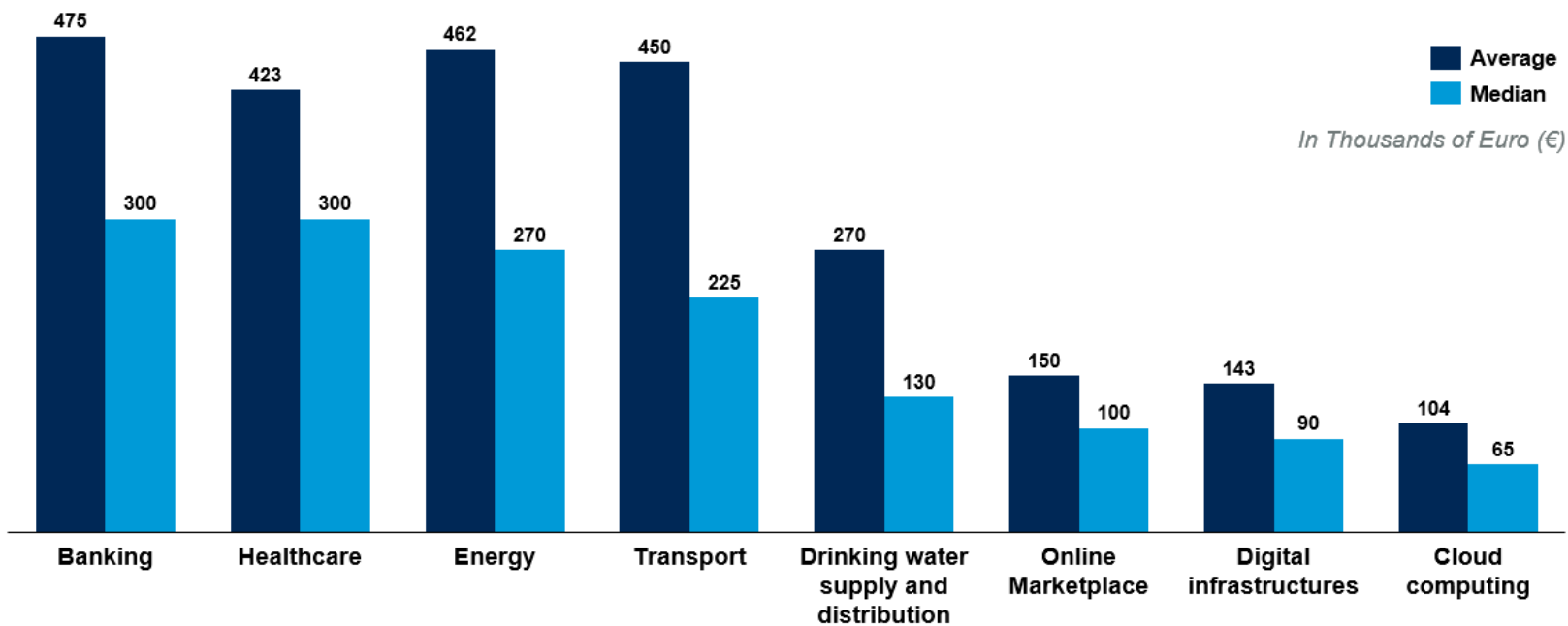
- No, but we are currently developing a dedicated ransomware defense program
- No, we do not have a dedicated ransomware defense program
- Yes, we have a dedicated ransomware defense program



Awareness raising for non-IT staff

- No awareness program for non-IT staff is in place, but we are planning to implement it next year.
- No awareness program is in place for non-IT staff
- Yes, our general awareness program also covers non-IT staff
- Yes, we have a dedicated awareness program in place for non-IT staff

COST OF INCIDENTS



Estimated direct costs of incidents

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

