NIS 2 DIRECTIVE: HOW THE EU SECURITY REGULATIONS AFFECT YOUR BUSINESS

Aleksander Gorkowienko

Senior Managing Consultant
Spirent Communications

Agenda

Our meeting today

1. What is the EU Network Information Systems Directive (NIS), and why has it been updated?
2. Core requirements of the NIS 2 Directive.
3. Who has to comply? Does NIS 2 apply to your businesses?
4. Implications of non-compliance with NIS 2?
5. How Spirent SecurityLabs can help?
6. Q&A

Spirent™

What is the EU Network Information Systems Directive (NIS), and why has it been updated?

The EU Network Information Systems Directive (NIS)

Reasons for creating the Directive

- The EU launched the Network and Information Systems (NIS) Directive in 2016 following the raising number of cyberattacks and increased cybersecurity concerns
- Strengthening member states' cybersecurity capabilities
- Increased collaboration on cybersecurity between member states
- Encourage EU states to supervise and improve cybersecurity across their Critical National Infrastructure (CNI)

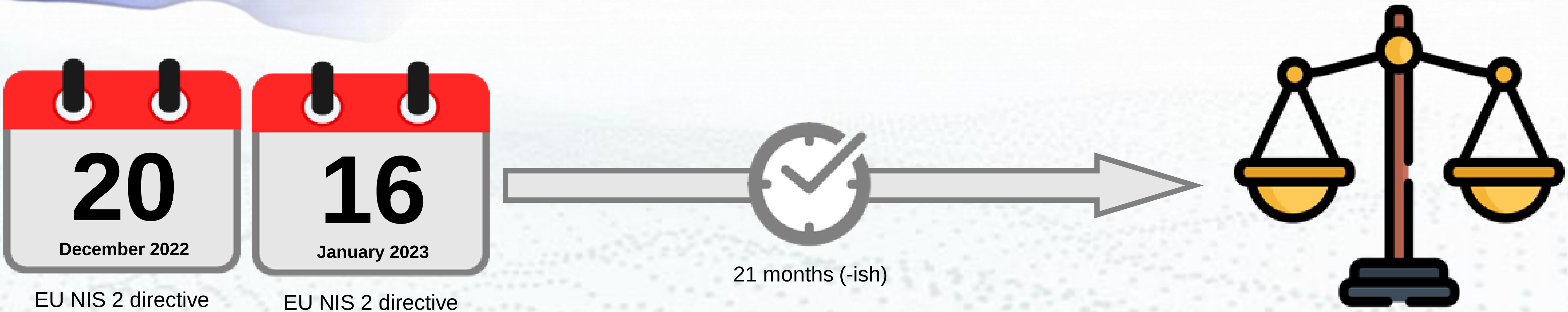
Reasons for the upgrade in 2023

- Since the NIS directive being launched, the cyber **threat landscape has substantially changed** and the directive doesn't meet the needs of the cyber security landscape in 2023
- Cyberattacks and data breaches have increased exponentially, specifically as people become more reliant on digital technology.
- Better protect vital **supply chains** and **critical national infrastructure** from cyberattacks that caused serious disruption in a few recent years
- **Gaps in the original NIS legislation**, and inconsistencies in how member states have implemented the Directive

NIS 2 timeline

In **December 2022**, the European Union confirmed they are expanding the scope of the existing Network and Information System (NIS) Directive

Following the publication of the EU NIS 2 directive in the Official Journal of the European Union, the directive came into force on the **20th Dec 2022**. Member states have **21 months** to incorporate it into their national law (until 17 October 2024) .



EU NIS 2 directive publication

EU NIS 2 directive enters into force

21 months (-ish)

17 October 2024 NIS2 becomes a national law for all EU member states

NIS 2 "upgrade" overview

Key objectives

- Remove inconsistency between member states in relation to cybersecurity requirements and implementation of measures
- Better protect vital supply chains and critical national infrastructure from cyberattacks that caused serious disruption in a few recent years
- Set the baseline for cybersecurity risk management measures and reporting obligations across all sectors covered by the directive, such as energy, transport, health and digital infrastructure

Scope extension

NIS 2 expands its scope to include the following new industries:

- Electronic communications
- Digital services
- Space
- Waste management
- Food
- Critical product manufacturing (i.e. medicine)
- Postal services
- Public administration

Note: Industries included in the original NIS directive remain within the scope of NIS 2. Smaller organisations, which are mission-critical to a member state's also are included in the NIS 2.

Core requirements of the NIS 2 Directive

Core NIS 2 requirements

According to NIS 2, organisations should actively manage cybersecurity risks in the following areas:

1. Risk analysis and information security policy
2. Incident prevention, detection, and response
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems
6. Use of cryptography and encryption
7. Vulnerability disclosure
8. Collaboration

Core NIS 2 requirements

Risk analysis and information security policy

- Organisations should take a proactive approach to cyber risk management
- According to NIS 2, companies should evaluate the potential impact of cyberattacks on their critical assets
- Regular and systematic assessment of risk is a critical part of approach to cybersecurity
- Strong information security policies should be in place
- Organisations should be aware of new security vulnerabilities and also cyberattacks on the other industry members

Core NIS 2 requirements

Incident prevention, detection, and response

- Organisations should have incident response plans with a transparent chain of command
- Organisations should also have incident prevention and backup plans in place
- All plans should be regularly tested engaging all engaged personnel and relevant technology
- Maintain a basic level of digital hygiene and have regular cybersecurity education in place

Core NIS 2 requirements

Business continuity and crisis management

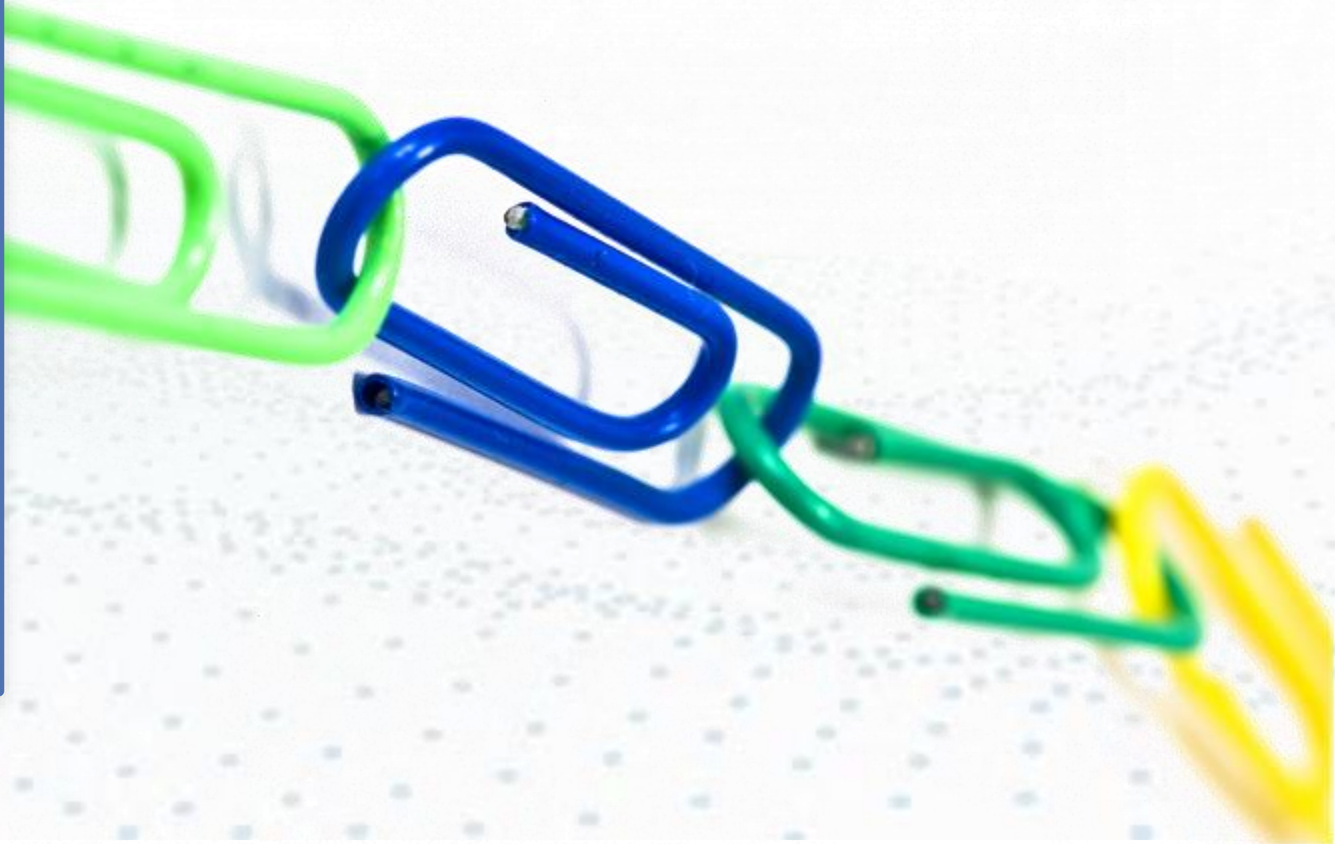
- Businesses can continue their operations in the event of a cyberattack
- Organisations should have a mandatory working plan for how the company should be dealing with a cyberattack and how the business can recover from it as soon as possible. minimising disruption
- NIS 2 includes a focus on resilient backup solutions, including cloud

Core NIS 2 requirements

Spirent

Supply chain security

- NIS 2 requires organisations to take into consideration the vulnerabilities of each of their suppliers and service providers. Their cybersecurity practices, development standards and data storage should be scrutinised
- Organisations should maintain a close relationship with suppliers and clearly understand the cybersecurity risks and implications
- Organisations should work together with suppliers on improving their services and products



securitylabs

Core NIS 2 requirements

Collaboration

- NIS 2 aims to simplify cybersecurity incident management within EU, facilitate collaborative data sharing and better solutions to address cyber incidents
- More data sharing between authorities is encouraged
- Authorities should participate in incident response at the EU level rather than local/national
- EU-Cyber Crisis Liaison Organisation Network (EU CyCLONe) is going to be established: aiming to coordinate and manage responses to cybersecurity incidents within EU borders

Core NIS 2 requirements

Incident reporting

- NIS 2 mandates companies to submit an initial **“early warning”** report **within 24 hours** of becoming aware of any “significant” incident *.
- A full **incident notification within 72 hours**
- A **final report within one month** after the submission of the incident notification to any relevant competent authority, Computer Security Incident Response Team (CSIRT). Notification to customers/recipients of services may also be required in certain situations.
- The final report must include a **detailed description** of the incident (the likely **cause** of the incident, the **mitigation measures** applied, and evaluated **impact** of the incident).

Vulnerability disclosure

- More transparent vulnerability disclosure and management will be required.
- If an organisation identifies a cybersecurity vulnerability within their network, **NIS 2 requires them to disclose it**.
- Public disclosure of the found vulnerabilities is critical: it will support the fight against cybercrime and ensure that the same vulnerability is not exploited elsewhere.

** A “significant” incident is any incident that has caused or is capable of causing severe operational disruption of the service or financial losses or if the incident has affected or is capable of causing considerable losses to others.)*

Who has to comply? Does NIS 2 apply to your businesses?

Who needs to comply?

Essential Entities

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT-service management
- Public administration entities (excluding the judiciary, parliament, and central banks)

Important Entities

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Food production, processing, and distribution
- Manufacture of medical devices, electronic products, and transport
- Digital providers
- Research

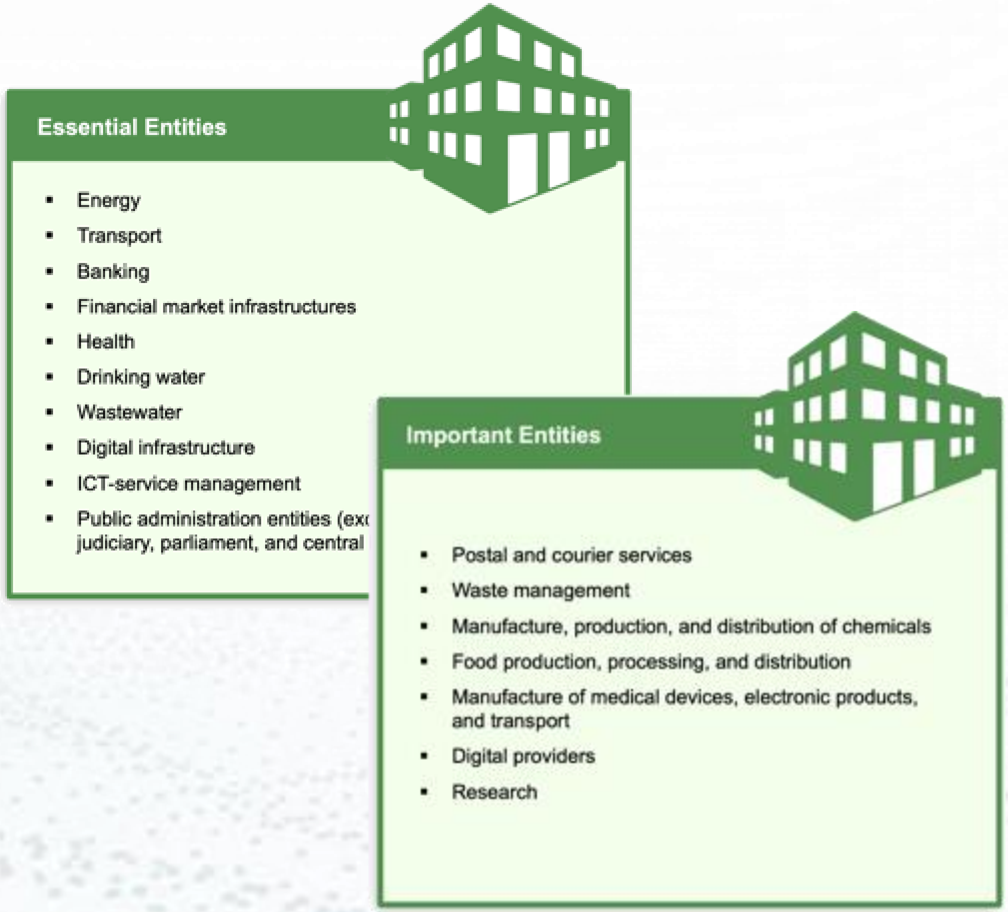
Who needs to comply?

NIS 2 <u>is</u> applicable to:

- Not only “essential” business entities! Now we have “essential” and “important entities”.
- Any organisation with more than 50 employees
- If your annual turnover exceeds €10 million
- Any organisation previously included in the original NIS directive
- All medium-sized and large organisations operating within the relevant sectors fall within NIS2’s scope

NIS 2 <u>is not</u> applicable to:

- Organisations that conduct activities in areas such as defence or national security, public security and law enforcement.
- Judiciary, parliaments and central banks are also excluded from its scope.



Essential Entities

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- ICT-service management
- Public administration entities (exc judiciary, parliament, and central

Important Entities

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Food production, processing, and distribution
- Manufacture of medical devices, electronic products, and transport
- Digital providers
- Research

Does NIS 2 Apply To UK Businesses?

Yes or No?

NIS2 does not directly apply, but oh, totally **YES!** Many UK businesses operate within the EU, which will require them to comply with NIS 2 in to maintain the same level of security standards as EU member states.

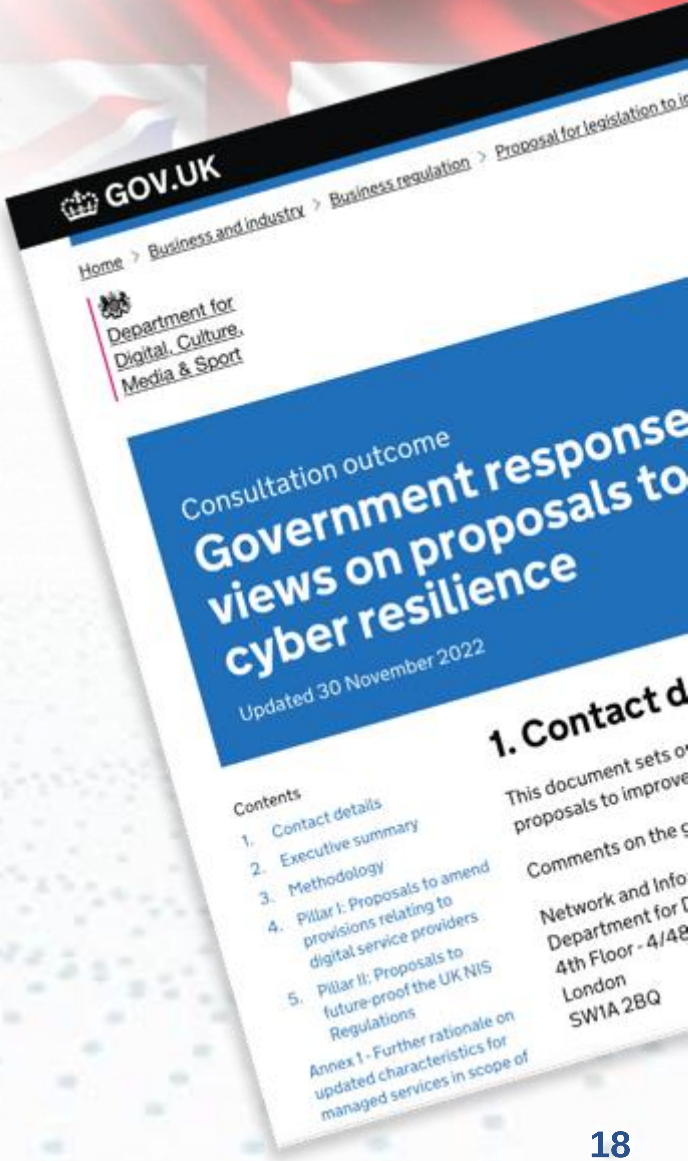
What?

In the UK there will be [indirect] alignment with NIS 2, e.g. where it applies to managed service providers, IT outsourcing, and core requirements (incident reporting, supply chain security, business continuity, etc.). There will be more mandatory alignment soon!

When?

The UK update is part of the government’s £2.6bn ($3.2bn) National Cyber Strategy so “will be made as soon as parliamentary time allows”. Probably the new legislation will come into effect in 2024.

It is highly recommended to keep an eye on the government news and have your business well-prepared in advance.



GOV.UK

Home > Business and industry > Business regulation > Proposal for legislation to i

Department for Digital, Culture, Media & Sport

Consultation outcome

Government response views on proposals to cyber resilience

Updated 30 November 2022

Contents
1. Contact details
2. Executive summary
3. Methodology
4. Pillar I: Proposals to amend provisions relating to digital service providers
5. Pillar II: Proposals to future-proof the UK NIS Regulations

Annex 1 - Further rationale on updated characteristics for managed services in scope of

1. Contact d

This document sets o
proposals to improve

Comments on the g

Network and Info
Department for D
4th Floor - 4/48
London
SW1A 2BQ

Implications of non-compliance with NIS 2?

Implications…

- NIS v2.0 comes with much stricter enforcement requirements than NIS v1.0.
  Penalties are substantial!
- Fines are the same as imposed for GDPR violations
- NIS 2 for cybersecurity = GDPR for data protection

- Being security audited and ordered to follow set recommendations
- On-site security inspections
- Requested on-demand security scans

- For essential entities of **€10 million** or **2% of the total worldwide turnover** (whichever is higher)
- For important entities of **€7 million** or **1.4% of the total worldwide turnover** (whichever is higher)

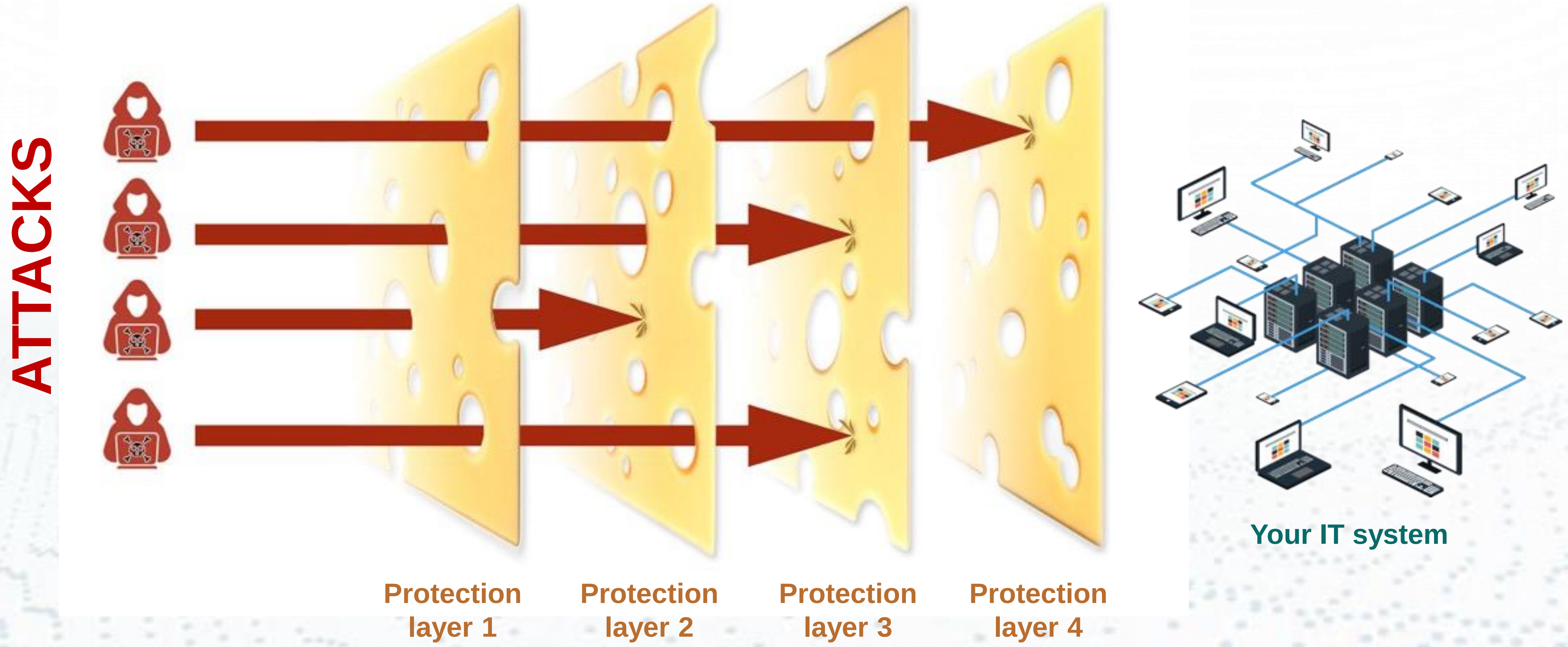
How Spirent SecurityLabs can help?

Your first steps on the path to compliance

- ✓ Map your network
- ✓ Identify all your IT assets
- ✓ Identify critical systems
- ✓ Conduct security testing
- ✓ Reduce the attack surface
- ✓ Patch and update
- ✓ Never “assume” security. Always have it tested!

- ISO 27001 certification can help
- Compliance with security guidelines issued by the European Union Agency for Cybersecurity (ENISA)
- One step further: compliance with ISO 22301 (business continuity management)
- Review your business and technological processes from the security point of view

Apply “defense in depth” approach



Core NIS 2 requirements

According to NIS 2, organisations should actively manage cybersecurity risks in the following areas:

1. Risk analysis and information security policy
2. Incident prevention, detection, and response
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems
6. Use of cryptography and encryption
7. Vulnerability disclosure
8. Collaboration

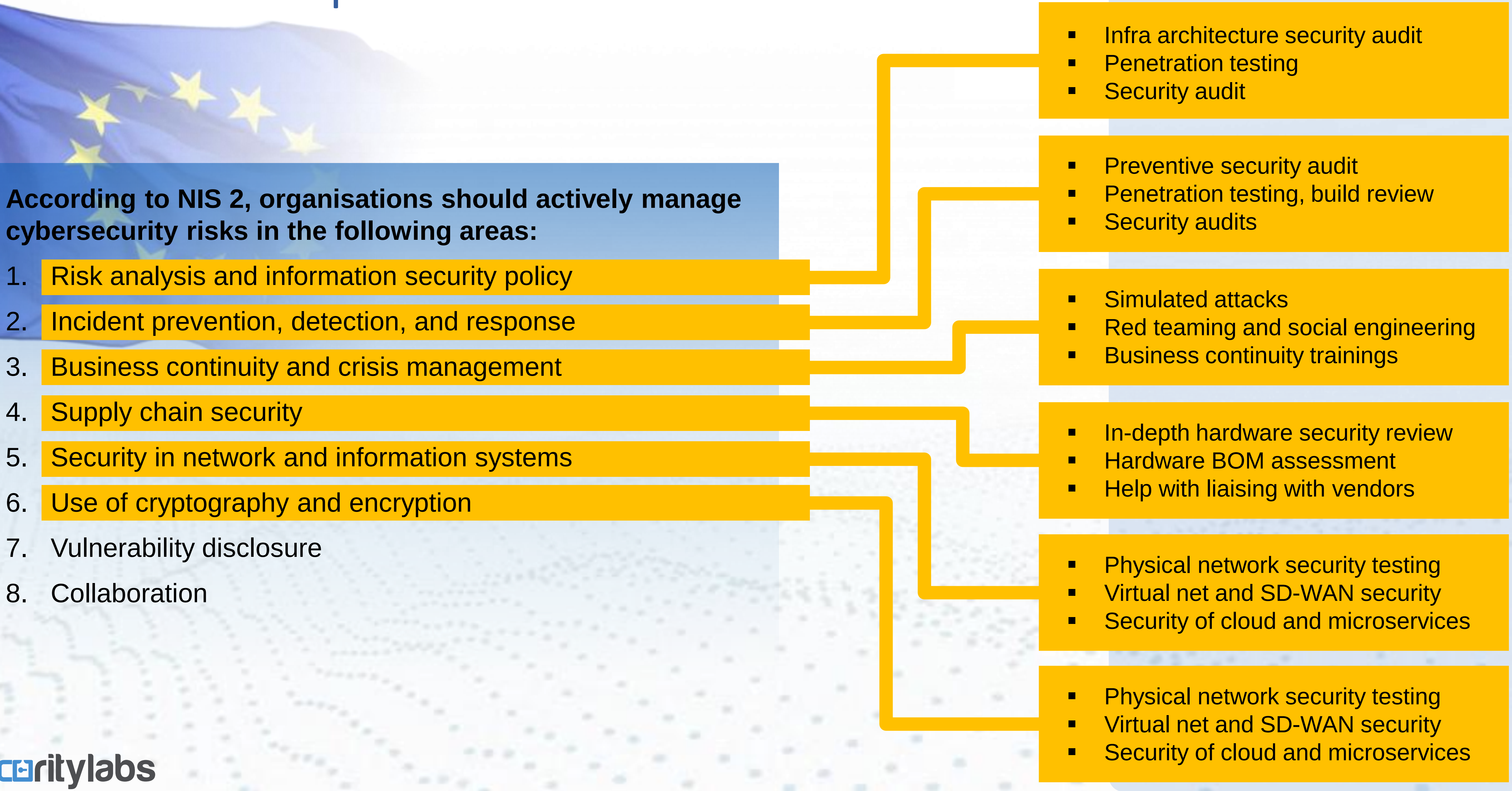
Core NIS 2 requirements

According to NIS 2, organisations should actively manage cybersecurity risks in the following areas:

1. Risk analysis and information security policy
2. Incident prevention, detection, and response
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems
6. Use of cryptography and encryption
7. Vulnerability disclosure
8. Collaboration

5G
securitylabs
services

Core NIS 2 requirements



According to NIS 2, organisations should actively manage cybersecurity risks in the following areas:

1. Risk analysis and information security policy
2. Incident prevention, detection, and response
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems
6. Use of cryptography and encryption
7. Vulnerability disclosure
8. Collaboration

- Infra architecture security audit
- Penetration testing
- Security audit

- Preventive security audit
- Penetration testing, build review
- Security audits

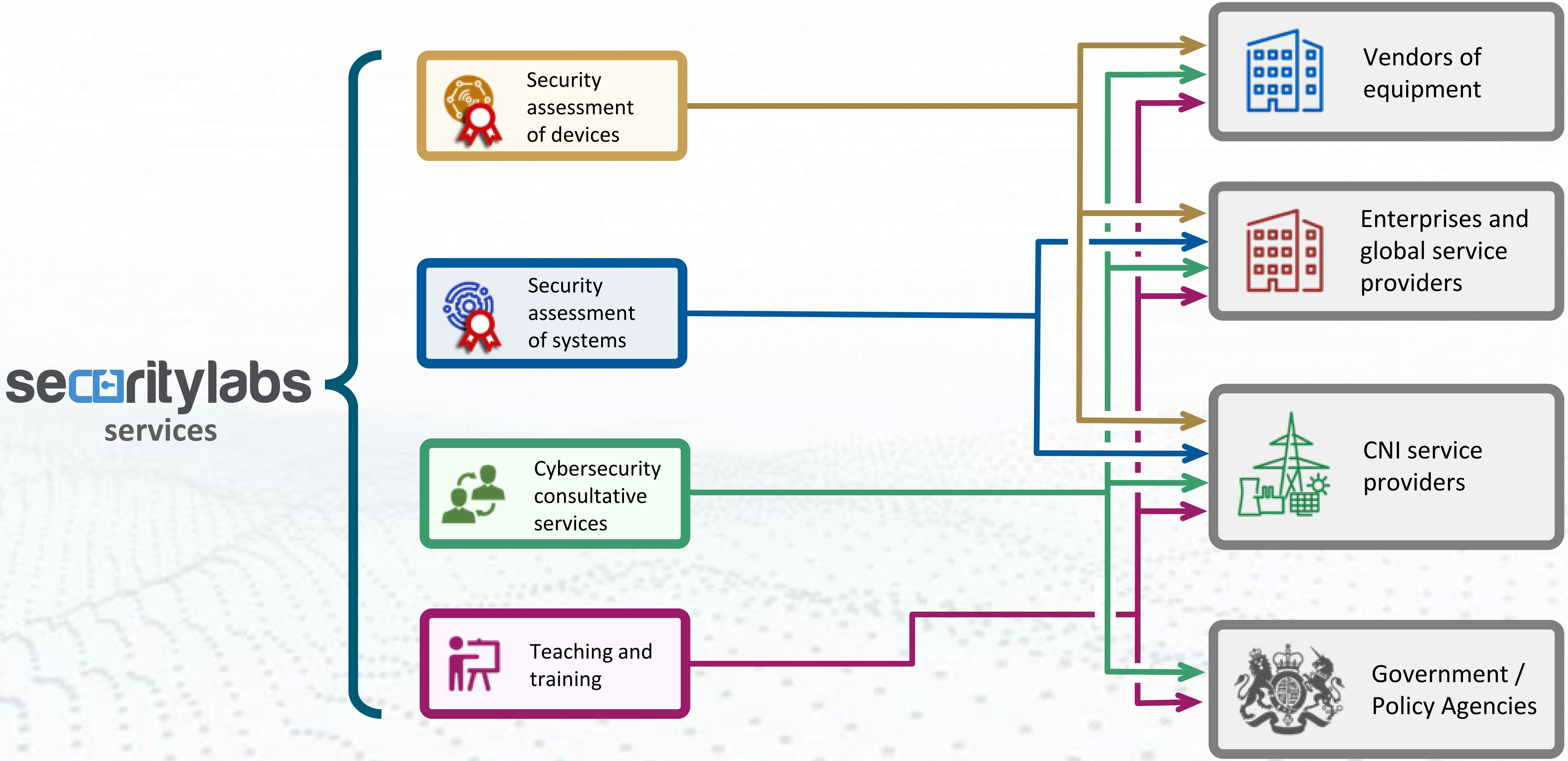
- Simulated attacks
- Red teaming and social engineering
- Business continuity trainings

- In-depth hardware security review
- Hardware BOM assessment
- Help with liaising with vendors

- Physical network security testing
- Virtual net and SD-WAN security
- Security of cloud and microservices

- Physical network security testing
- Virtual net and SD-WAN security
- Security of cloud and microservices

Path to NIS2 compliance with Spirent SecurityLabs



securitylabs services

Security assessment of devices

Security assessment of systems

Cybersecurity consultative services

Teaching and training

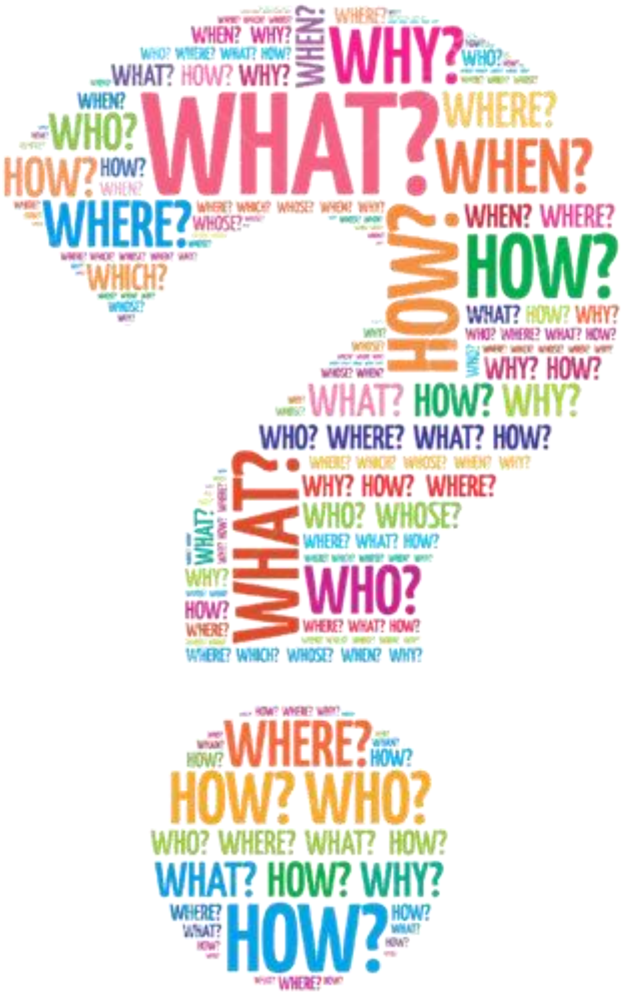
Vendors of equipment

Enterprises and global service providers

CNI service providers

Government / Policy Agencies

Q&A



Thank you!

https://www.spirent.com/Products/SecurityLabs

securityLabs@spirent.com

securitylabs

Aleksander Gorkowienko
e: aleksander.gorkowienko@spirent.com
m: +44 (0) 7974431025