3ˆ EDIZIONE

CYBERSEC 2024

ROMA, ITALIA

LA CYBERSECURITY NELL'ERA DELL'AI

6-7 MARZO

www.cybersecitalia.events

CYBERSECURITY ITALIA EVENT

CYBERSECURITYITALIA

RELATORE

ALESSIO FASANO

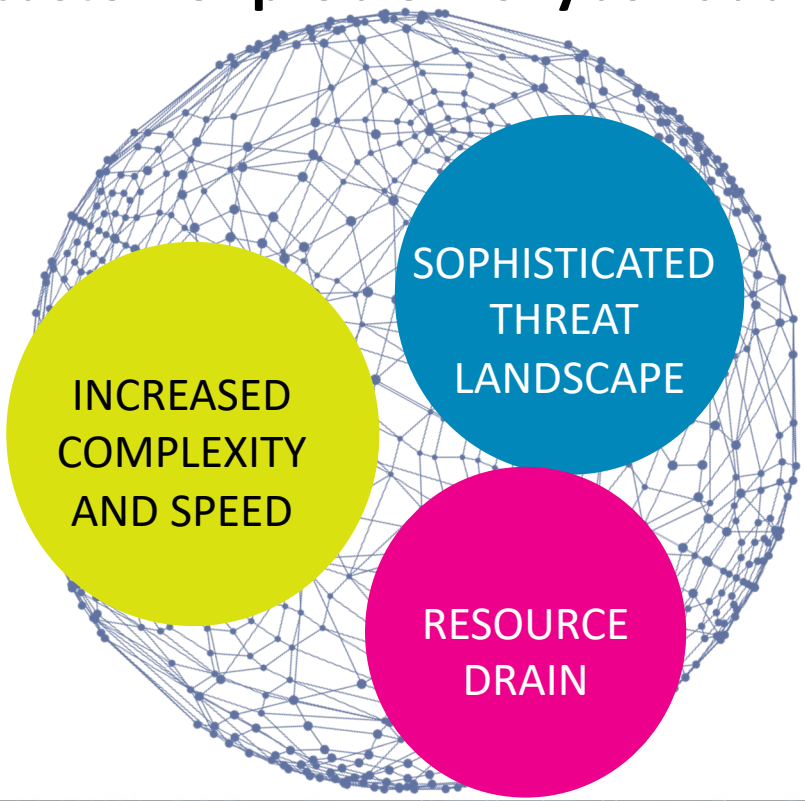
COUNTRY MANAGER ITALIA - GRECIA - CIPRO - MALTA
SKYBOX SECURITY

Evolving Business Challenges

Today's dynamic cyber landscape

The customer problem Skybox addresses

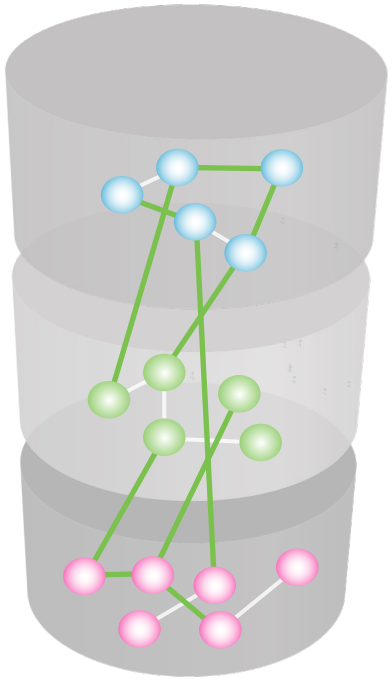
- Digital transformation
- Seismic shift to remote working
- Accelerated cloud migration
- Fragmented networks
- Technology convergence and complexity
- Vanishing perimeters
- Growing attack surface



- Mergers, acquisitions, divestitures
- Shifting business models
- Teams are stretched and top talent is scare
- Recessionary pressures on budgets
- Exponential rise in vulnerabilities
- Dramatic increase in ransomware samples
- Malware-as-a-service

Regulation compliance

What is changing and how it helps growing company's maturity about cybersecurity



INCREASING THE NUMBER OF SECTORS COVERED

NIS2 extends the scope of NIS by adding new sectors, such as telecom, social media platforms and public administration (i.e. entities of central and provincial governments). Furthermore, NIS2 establishes that all medium-sized and large entities are required to comply with the proposed security rules. NIS2 also removes the possibility for Member States to tailor the requirements in certain cases.

STRENGTHENING SECURITY REQUIREMENTS

NIS2 includes a list of seven elements that all companies must address or implement as part of the security measures they take, including **risk analysis and information system security policies**, incident response, business continuity and crisis management, supply chain security, **assessment of effectiveness of risk management measures**, and encryption and vulnerability disclosure.

IMPROVING COOPERATION AT EU LEVEL

NIS2 includes rules on

(i) measures to increase the level of trust between competent authorities,
(ii) information sharing between competent authorities, and
(iii) procedures in the event of a large-scale incident or crisis

New Organizational Requirements

Risk Management

Organizations are required to implement **strategies aimed at mitigating cyber risks** in accordance with the new Directive. These strategies encompass various actions such as **managing incidents effectively**, fortifying supply chain security, **bolstering network defenses, improving access controls**, and implementing encryption protocols.

Corporate Accountability

NIS2 mandates that corporate management assume responsibility for supervising, endorsing, and receiving training on the organization's cybersecurity protocols, as well as addressing associated risks. Violations could lead to penalties for management, potentially involving liability and temporary exclusion from managerial positions.

Reporting Obligations

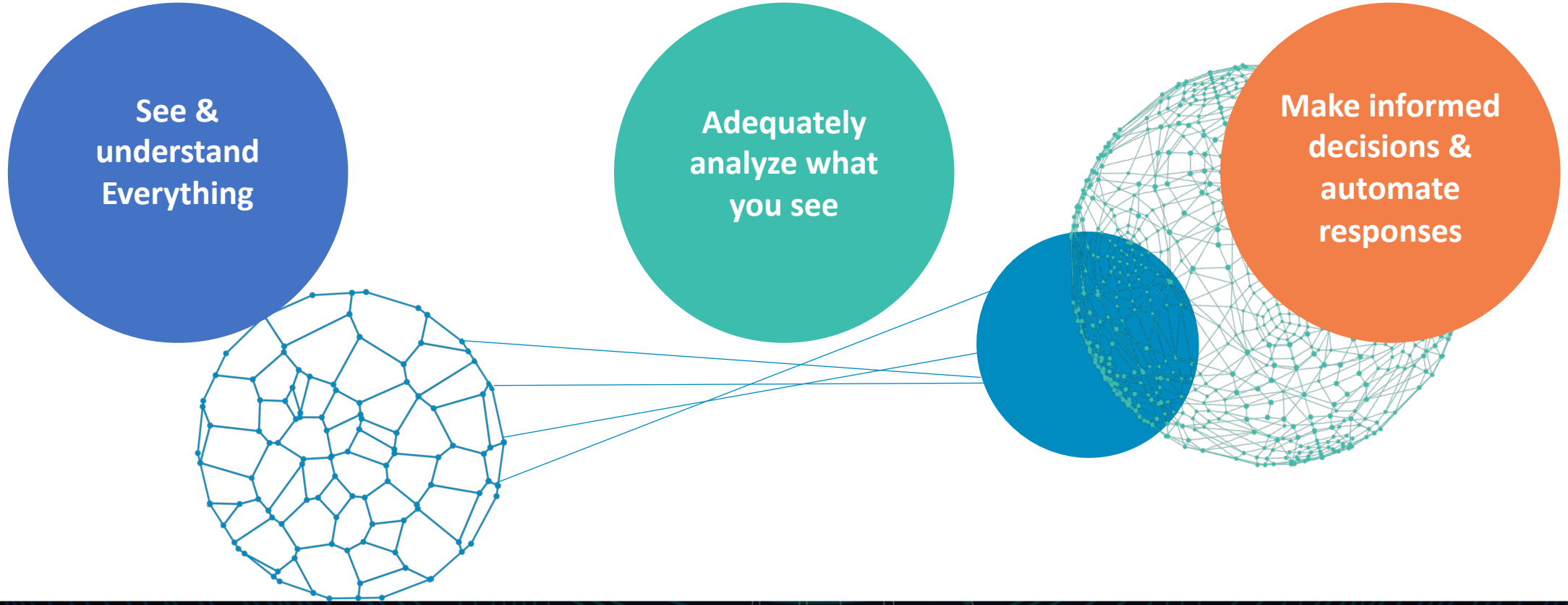
Critical and vital entities must establish procedures for promptly reporting security incidents that have a significant impact on their service delivery or recipients. NIS2 establishes precise deadlines for notifications, including a 24-hour "early warning" requirement.

Business Continuity

Organizations need to strategize on how to guarantee business continuity in the event of significant cyber incidents. This strategy should encompass aspects such as system recovery, emergency protocols, and the establishment of a crisis response team.

What's Needed

Better overall Security Posture Management



What's Needed

A continuous exposure management program

+ Adaptive and continuous understanding of the growing attack surface

+ Unification of security configuration and policy management with risk assessment and management processes

+ More automated and coordinated configuration and remediation management across IT, SecOps, NetOps

SKYBOX SECURITY

THANKS FOR YOUR ATTENTION

ALESSIO FASANO
COUNTRY MANAGER ITALIA - GRECIA - CIPRO – MALTA
Alessio.Fasano@skyboxsecurity.com
Mob. +393472488405