CYREBRO

CYREBRO &
The NIS 2 Directive

Help Your Customers Comply with the NIS 2 Directive

What is the NIS 2 Directive?

The European Union is enhancing the cybersecurity of its member states by replacing the current Network and Information Security (NIS) Directive. As a result, the new Directive changes the security requirements for critical infrastructure facilities and businesses, leading to a broader coverage of companies and more significant fines for non-compliance.

European Union Cybersecurity Governance

The NIS2 directive will be transposed into national law by EU members states no later than 17 October 2024.

This means that companies doing business with entities in the EU will also have to be compliant as the national laws come into effect or face possible legal consequences and hefty fines. Furthermore, any other region that deals with EU entities should check their security standards to ensure they are meeting the new requirements of the Directive.

What type of businesses are subject to NIS 2?

NIS 2 complements and expands the definition of essential companies from the original NIS Directive and adds new sectors that will now need to comply with the new Directive. Medium and large companies in selected sectors are included. At the same time, it gives member states some flexibility to identify smaller companies (with less than 50 employees or €10M annual turnover) that have a high-risk profile as also being subject to the Directive.

Company profile:

50+ employees **€10M+ annual turnover**

- Healthcare
- Transport
- Food
- Providers of public electronic communications networks of services
- Energy
- Digital service providers
- Space
- Waste water and waste management
- Banks and financial market infrastructure
- Digital infrastructure
- Public administration
- Digital services such as social networking services platform and data centre services
- Water supplies
- Postal and courier services
- Manufacturing of certain critical products

As part of the Directive, entities deemed "essential" will be regularly assessed, while "important" entities are planned to be assessed only after a significant threat incident has occurred.

CYREBRO Capabilities for NIS 2

In order to be compliant, appropriate measures to prevent and remedy cyber threats and restore security must be established. No matter where your customers are on their cybersecurity journey, it's critical to significantly increase their defense level with incident response measures.

CYREBRO helps meet the strict cybersecurity incident handling requirements of NIS 2. With CYREBRO you will be able to offer your customers enhanced cybersecurity and risk management in a single, centralized Platform.

Strategic Monitoring & Early Threat Detection

CYREBRO proactively searches for and identifies malicious or risky activities, correlating across all your security tools and systems, providing a sophisticated level of protection. CYREBRO's solution includes a SIEM powered by ML, and we build and update rules and detection algorithms that are optimized based on our continuous development and understanding of new threats.

Rapid Incident Response & Threat Management

CYREBRO's SOC analysts work 24/7/365 to respond in real-time and provide identification, malicious indicators and visibility into the SOC's investigation of incidents. With our experts' know-how, and ample threat intelligence, we provide actionable steps for remediation.

Forensic Investigation

If an attack occurs, it's imperative to isolate and eradicate the threat and ensure it can't happen again. CYREBRO's forensic investigation capabilities allow you to help your customers do just that – reduce their business risk.

Lower Labor Costs

Making sure your company and your customers can access experienced personnel to manage cybersecurity can be challenging and costly. Proper threat detection requires multiple roles and skill sets coupled with years of experience analyzing threat behavior. With CYREBRO, you leverage our expert team of cyber professionals and access the expertise you need at a fraction of the cost of building and maintaining a SOC.

Contact us
www.cyrebro.io
info@cyrebro.io

New York Office: 38 High Avenue. 4th Floor. Nyack, NY, 10960
Israel Office: 52 Menachem Begin street, Tel Aviv