HACKTHEBOX

GOVERNANCE & COMPLIANCE

NIS2 DIRECTIVE

Europe’s most extensive cybersecurity directive to date

NIS2 is a groundbreaking EU directive that elevates the priority of organizational security with the power to fine, suspend, and transform how critical entities protect against digital threats.

The directive introduces several key enhancements and obligations to address evolving the threat landscape and improve the overall security posture of critical infrastructure and essential services—with the ultimate goal to empower and align practices for a more cyber resilient European Union.

With stricter requirements for risk management and incident reporting, wider coverage of sectors, and more hard-hitting penalties (including personal liability) for non-compliance, hundreds of thousands of EU organizations will need to reassess their cybersecurity posture.

Key changes & action required

Compliance to NIS2 comes only with concrete and proactive pivotal changes. These are not a one-off task, but require constant maintenance and assessment to ensure business compliance:

Executive Role
NIS2 takes cybersecurity to a board level by introducing heavy personal liabilities in case of non-compliance. Security becomes a top business priority!

Expanded Scope
The directive is highly relevant across industries (15) classified as “essential” or “important”, for a total estimation of 160,000+ companies affected.

Duty of Care
Article 21 mandates a series of required security practices: risk assessment, digital hygiene, crisis management, supply chain security, and more.

Reporting
NIS2 requires an early warning of significant incidents within 24 hours of discovery, followed by an intermediate warning at 72 hours, and a final report within a month.

⚠ Non-compliance penalties can amount to €10 million or 2% of global turnover, or even criminal charges. NIS2 has the power to fine, suspend, and transform how organizations safeguard against digital threats.

Cyber strategy & governance

Senior leadership and boards of directors are responsible for reviewing and implementing an organizational risk management strategy. Hack The Box has the goal to provide to CISOs all tools necessary to comply to NIS2 Duty of Care requirements and leverage highly effective threat intelligence practices to stay informed about new risks:

→ Identify, prioritize, and assign risk ratings to essential business processes

→ Develop a common risk language for technical and business stakeholders

→ Implement proactive security measures

→ Continuously assess workforce and procedure with realistic simulations

Cyber workforce development plans baked into the fabric and objectives of your organization

Access guided courses, hands-on labs, and live-fire team exercises with Hack The Box.

	HTB Academy	Dedicated Labs	Professional & Cloud Labs	Crisis Control	Capture The Flag (CTF) & Ranges	Analytics & Reporting
Digital Hygiene & Cyber Education	✓			✓		✓
Risk Analysis	✓	✓				✓
Crisis & Incident Management	✓	✓		✓		✓
Business Continuity				✓	✓	✓
Supply Chain Security		✓	✓		✓	✓
Network Security	✓		✓		✓	✓
Cryptography & Encryption		✓			✓	✓
IR & SOPs Assessment				✓		✓

Boost your cyber performance to meet tight incident reporting deadlines!

NIS2 and other recent developments—SEC ruling, FTC safeguard rule, or the Cyber Incident Reporting for Critical Infrastructure Act of 2022—are raising the bar for incident reporting requirements. In order to meet them, companies need to shape threat-ready SOC teams and professionals.

Hack The Box workforce development plans are designed to enhanced key capabilities:

- **Incident detection**
- **Triage & assessment**
- **Containment & remediation**
- **Regulatory awareness**

Create and maintain a high-performing cyber team.
Talk to our team to get started.

Improving the cyber performance of 800+ large companies, governments, and universities

Google · Booking.com · Lufthansa · PUMA · EA SPORTS

SIEMENS · PURDUE UNIVERSITY · pwc · StateFarm

standard chartered · Raytheon An RTX Business · UNIVERSITY of SOUTH FLORIDA · verizon