GROUP-IB

NIS 2 compliance for EU businesses

Meet cybersecurity requirements before the deadline

With NIS 2 non-compliance proving detrimental — resulting in millions in fines, business activity suspension, and more, become compliant while there's still time!

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785

Group-IB: Meeting the requirements for the new Network and Information Security Directive (NIS 2.0)

With the compliance deadline set for October 17, 2024, ensure your NIS 2.0 readiness to stay resilient in the face of emerging cyber threats and avoid the financial and legal implications of non-compliance.

What is NIS 2.0?

The European Union (EU) has signed the NIS 2 Directive to enforce better cybersecurity and resilience within organizations across the region. A step above its predecessor, NIS 2.0 covers more sectors and includes aggressive repercussions for non-compliance. This directive primarily targets organizations in the critical infrastructure supply chain. Key objectives include implementing cyber safety measures, ensuring cooperation and information exchange, and mandating the reporting of cyber incidents.

Achieve NIS 2 Compliance: Group-IB Solution Map

NIS 2 Requirements	Group-IB Solutions	Benefits
(a) policies on risk analysis and information system security;	Group-IB Threat Intelligence	**Comprehensive Insights into Emerging Threats** • Group-IB Threat Intelligence provides detailed analysis of new and evolving threats.
(b) incident handling;		**Enhanced Incident Handling Capabilities** • With Group-IB Threat Intelligence,understand attacker identity and infrastructure through related attribution and graph tools. • Improve response and management of incidents. • Analyze risks comprehensively and improve security posture
(c) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;		**Partner Breaches Monitoring** • Monitor breaches such as Ransomware DLS. • Real-time awareness of threats impacting partners.
(d) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;		**Vulnerability Intelligence** • Utilize Threat Intelligence (malware section) for vulnerability intelligence.

NIS 2 Requirements	Group-IB Solutions	Benefits
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Group-IB Attack Surface Management (ASM)	**Third-Party Risk Assessments** • Ensures robust supply chain security. • Addresses security-related aspects of relationships with suppliers or service providers. • Mitigates potential vulnerabilities from external dependencies.
(b) incident handling; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Group-IB Extended Detection and Response (XDR)	**XDR (Extended Detection and Response)** • Monitors the entire network infrastructure. • Provides comprehensive incident monitoring and response functionality, along with its modules **NTA (Network Traffic Analyzer)** • Provides continuous network monitoring and data collection and supports threat hunting activities. **BEP (Business Email Protection)** • Secures email flow by blocking malicious and unwanted emails. **EDR (Endpoint Detection and Response)** • Host monitoring and response functionality.
(b) incident handling	Incident Response Readiness Assessment	• Analyzes incident detection, response, containment, and recovery processes. • Assesses preparedness of company assets, processes, resources, and personnel for potential incidents.
(a) policies on risk analysis and information system security (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Compromise Assessment	• Evaluate blind spots in your existing cybersecurity infrastructure • Ensure prompt detection and mitigation of security breaches. • Verify adequate protection against potential threats.
(a) policies on risk analysis and information system security (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Penetration Testing	• Simulate real-world cyberattacks to identify vulnerabilities. • Enhance overall security posture by addressing weaknesses. • Assess effectiveness in managing cybersecurity risks and testing defenses against threats.

NIS 2 Requirements	Group-IB Solutions	Benefits
(a) policies on risk analysis and information system security (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Security Assessment	• Comprehensive risk analysis and security policies evaluation. • Identify strengths and weaknesses in security measures. • Refine policies to better mitigate cyber threats. • Strengthen security posture and defense capabilities against existing and potential threats.
(a) policies on risk analysis and information system security	Compliance Audit and Consulting	• Conduct compliance audits and consulting services to adhere to policies on risk analysis and information system security. • Align security practices with regulatory requirements and industry standards.
(a) policies on risk analysis and information system security (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Red Teaming	• Simulate cyberattacks to mimic real-world threat scenarios. • Identify and proactively address security gaps within organizations. • Identify weaknesses and vulnerabilities within organizations. • Enhance security measures based on assessment findings.
(g) basic cyber hygiene practices and cybersecurity training	Training and Education	• Tabletop exercises - interactive, real-world formats for training and education on incident handling. • Basic cyber hygiene awareness to foster a culture of cybersecurity within organizations • Empowering employees with the needed skills to recognize and mitigate potential security risks effectively.
(b) incident handling	Incident Response	• Access skilled Group-IB's global Incident Response team for rapid analysis and support. • Ensure thorough containment, remediation, and recovery from severe cyber attacks. • Group-IB Incident Response Retainer - a pre-negotiated statements of work provide proactive and reactive cybersecurity services. • Agreements tailored to diverse budgets and business needs. • Minimize downtime during cyber attacks with structured agreements.

Complete all your NIS 2 requirements

	Group-IB Solutions			
NIS 2 Requirements	***Cybersecurity Services**	**Threat intelligence (TI)**	**Extended Detection and Response**	**Attack Surface Management (ASM)**
(a) policies on risk analysis and information system security;	☑	☑		
(b) incident handling;	☑	☑	☑	
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;		☑		☑
(e) security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;		☑	☑	☑
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	☑			☑
(g) basic cyber hygiene practices and cybersecurity training;	☑			
(i) human resources security, access control policies, and asset management;			☑	☑

* Security services to select: IR readiness assessment, compromise assessment, penetration testing, security assessment, compliance audit & consulting, red teaming, IR, IRR, education and training

Identify and close your security gaps to achieve NIS 2 compliance.

Start now with Group-IB!

Group-IB has been a trusted partner for businesses worldwide as regards security compliance, with over 50 critical compliance checks performed every year.

Every member of our consulting team is a certified auditor with extensive experience in compliance auditing for corporations in fields such as healthcare, financial services, critical services, and manufacturing.

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+
Successful investigations of high-tech cybercrime cases

300+
employees

600+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1[*]
Incident Response Retainer vendor

120+
patents and applications

7
Unique Digital Crime Resistance Centers

[*] According to Cybersecurity Excellence Awards

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- FORRESTER
- AiteNovarica
- KuppingerCole ANALYSTS
- Gartner
- IDC
- FROST & SULLIVAN

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785