LevelBlue

NIS2 Maturity Accelerator

Prepare for NIS2 compliance and increase cybersecurity resilience.

The Network and Information Security Directive 2 (NIS2) enforces requirements to enhance cybersecurity resilience of critical infrastructure, improve risk management practices, and ensure more robust incident reporting across Member States of the EU.

Understanding NIS2

Established by the EU, NIS2 applies to medium- and large-sized public and private entities providing essential services or critical infrastructure within or to the EU. It broadens the scope of the original NIS Directive to include sectors such as energy, healthcare, transportation, digital infrastructure, and public administration.

Penalties for non-compliance include fines of up to EUR 10,000,000 or 2% of total annual worldwide turnover for essential entities, and may also include prohibition from managerial functions, cease and desist orders, and public disclosure of infringements.

NIS2's framework is built around three key areas:

1. **Governance:** Focuses on ensuring robust cybersecurity leadership within organizations by establishing clear roles, responsibilities, and strategic oversight at senior levels.
2. **Cybersecurity Risk Management Measures:** Focuses on achieving risk management outcomes using appropriate technical, operational, and organizational measures to secure network and information systems. This includes managing risks within supply chains and supplier relationships to ensure that both new and existing suppliers are resilient and that viable alternatives are available in case of disruptions.
3. **Reporting Obligations:** Focuses on enhancing the transparency of cybersecurity operations through the mandatory reporting of cybersecurity incidents and risks.

Benefits

- Access a team of LevelBlue consultants with deep subject matter expertise in governance, risk, and compliance.
- Streamline compliance processes to align with NIS2 while optimizing resources.
- Assess supply chain risks and develop supplier oversight measures.
- Strengthen cybersecurity resilience with targeted risk management practices.
- Identify and address security weaknesses relating to NIS2 obligations.
- Establish robust incident reporting workflows.
- Ensure preparedness for audits and inspections by authorities.

LevelBlue

NIS2 Maturity Accelerator

LevelBlue, formerly Trustwave, helps you prepare for NIS2 compliance through a modular, focus area-based approach to address your specific requirements:

1. **Requirements Gathering:** LevelBlue works with you to identify the in-scope areas based on NIS2.
2. **Gap Analysis:** LevelBlue conducts a gap analysis to identify weaknesses in your current in-scope security and resilience programs as they pertain to NIS2.
3. **Roadmap Development:** LevelBlue works with you to develop a prioritized roadmap tailored to your needs, based on findings from the gap analysis.

Implementation Support: LevelBlue can also help you implement changes to your security environment in alignment with NIS2 requirements. These services may include implementing the corrective actions from the roadmap or any other activities that you are looking to achieve to increase your cybersecurity resilience, such as providing LevelBlue Managed Vendor Risk Assessment or LevelBlue Digital Forensics and Incident Response. Implementation services are not included in the LevelBlue NIS2 Maturity Accelerator service but may be purchased separately.

Microsoft and NIS2

LevelBlue is endorsed and validated by Microsoft as a leading cybersecurity partner. Microsoft provides comprehensive security solutions to help organizations prepare for NIS2 by strengthening cybersecurity resilience, enabling regulatory compliance, and safeguarding critical infrastructure and services. This includes Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender Threat Intelligence, Microsoft Purview, and Microsoft Azure.

Build, test, and run a secure organization

LevelBlue's range of capabilities help you get the right service to suit your specific needs:

Cyber Advisory Services:

- Digital Forensics and Incident Response
- Threat Detection and Response
- Managed Vendor Risk Assessment
- Scenario-Based Crisis Simulation
- Data Protection
- Governance, Risk, and Compliance
- Security Colony
- Technology Partnerships
- Executive and Technical Training
- Threat Intelligence as a Service

Security Testing Services:

- Penetration Testing (Network, Application – Internal, External, Wireless)
- Vulnerability Scanning (Discovery, Network, Application, Database)
- Red/Purple Teaming
- Intrusion Detection and Prevention
- Database Security (DbProtect, AppDetectivePRO)
- Secure Email and Web Gateways
- Physical Assessments

Managed Security Services:

- Managed Threat Detection and Response
- Co-Managed SIEM/SOC
- Security Technology Management
- Managed Web Application Firewall
- Proactive Threat Hunting