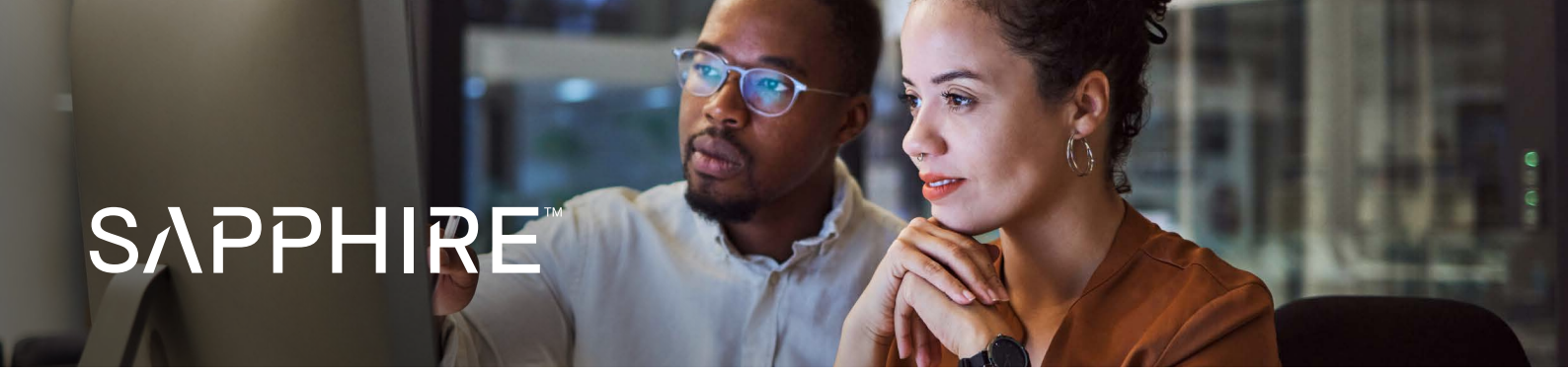


Comply With NIS2 To Ensure Your Organisation Is Robust To Evolving Threats

The modern cybersecurity landscape has no boundaries, with many organisations relying on increasingly interconnected digital technologies. The complex interdependencies of global systems and critical information infrastructures are under constant threat from malicious actors, within which the continuous digitisation results in any large-scale incident in even just one sector, resulting in cascading consequences elsewhere.

With this evolution of our industries comes an increase in cybercrime and cyber-attacks that target many more than previously thought. The transportation industry, for example, faces threats related to access offerings, social engineering and ransomware. Similarly, the finance, energy and education sectors have reported more persistent and sophisticated Distributed Denial-of-Service (DDoS) campaigns. At the same time, even small organisations with lower security standards are becoming increasingly targeted, with successful attacks of smaller volumes aiming to maximise revenue on the side of attackers.

NIS2 enhances the security of our organisations and critical infrastructures, leading to a more robust global ecosystem

The global cybersecurity market is projected to grow to around £300B by 2029. however global ransomware damages alone are predicted to exceed £210B by 2031, with a new attack on a consumer or business to occur roughly every 2 seconds.

Ultimately, the need to identify and mitigate this chain of targeted threats and attack vectors remains a challenge, and it is critical to ensure we enhance our preparedness, security and resilience of our critical information infrastructures.

The Network and Information Security Directive 2022 (NIS2) represents the first critical EU-wide legislation on cybersecurity and provides legal norms to strengthen the resilience of related entities, with a particular focus on protecting critical infrastructure. Drawing on the previous directive, NIS1, the new directive updates and expands the scope to meet current risks and future challenges, also extending the essential and vital entities that fall within the directive's scope

Essential	Important
Energy	Postal/Courier
Transport	Manufacturing
Health	Food
Water	Waste Management
Space	
IT	

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Scope Coverage

The NIS2 Directive extends the scope of NIS1 to provide a comprehensive coverage of the critical sectors and services for global societal and economic activities, ranging from energy and healthcare industries to waste management and postal services.

Establish Risk and Security Management Systems

- Business Continuity and Disaster Recovery
- Incident Handling and Reporting
- Manage Endpoint and Network Security
- Supply Chain Security

Understanding the Risks

NIS2 establishes key measures covering all entities active in scope of the directive to strengthen an organisation's security posture by defining requirements based on the risk management concept.

The Importance of Reporting

NIS2 defines the reporting obligations of severe cybersecurity incidents in a two-stage approach and highlights the importance of doing so. In 2017, for example, Equifax – a large credit reporting agency – suffered a massive data breach that exposed nearly 150 million records of sensitive information. The breach occurred a couple of months beforehand, but delays in detection and reporting hindered the ability to respond to the incident effectively. Timely and transparent reporting is essential for minimising damages and fostering collaboration to address emerging threats that impact all sectors.

Protecting our Supply Chains

Cyber risks arising from our supply chains and the relationships with third-party suppliers should be adequately managed in coordination with NIS2. As well as this, if your organisation is within the EU and your supplier is outside the EU, they must still comply with the requirements of NIS2, and vice-versa.

Operational Technology

While NIS2 does not explicitly mention OT security, there are many indications that OT and critical cyber-physical systems are within the scope of the directive and, ultimately, should also comply. As well as this, the NIST CSF (v1.1)

> NIS2 is expected to be fully defined in late 2024 and in operation early 2025 – ensure your compliance readiness now!

guidelines also map with key NIS2 measures that cover the protection of our OT environments.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

How Can Sapphire Help

Sapphire hosts a large collection of services which can help you become compliant with the NIS2 directive and protect your organisation's security posture and consumer relationships.

Some of our key services include:

Third Party Risk Management

Ensure you review the security of your third-party suppliers and the potential risks they may pose to your organisation.

Benefit from automated third-party risk assessments and timely reporting of your third-party risks.

Governance, Compliance and Risk

Sapphire can provide consultancy on compliance and risk in accordance with NIS2, as well as gap analysis to bridge compliance and certification against NIS2.

Security Testing

Sapphire's certified penetration tests and vulnerability analysis can provide visibility into the current threat posed to your risk and security management systems.

Benefit from access to Sapphire's streamlined reporting, collaboration, and management portal for all testing activities end-to-end.

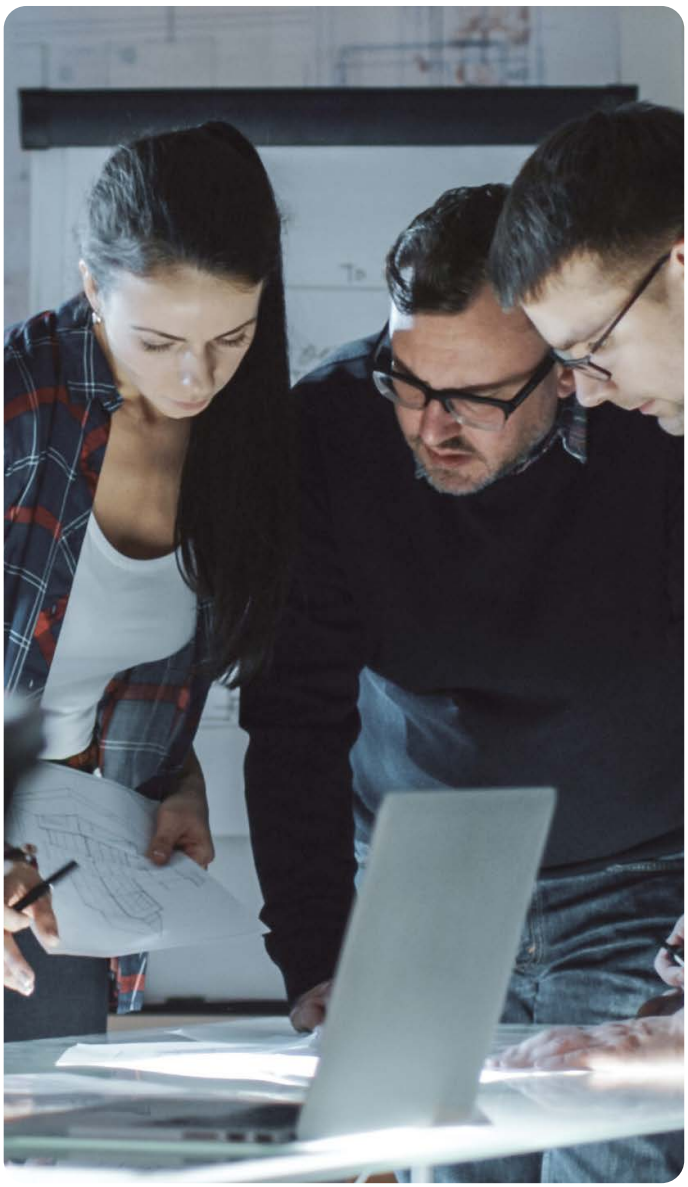
Threat Intelligence

Supplement and enrich your organisation's security capabilities with Sapphire's real-time intelligence data from an unrivalled array of sources across every language, supported by credible evidence, to ensure you remain robust to current and future threats.

Security Awareness Training

One of the biggest risks to the security of our organisations is our people. Sapphire's managed security awareness training can equip your organisation with bespoke, actionable skills to prevent and mitigate threats that start with your people.

Cultivate a security-first and safety-first culture among your employees within every department to promote responsibility and accountability.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Sapphire's Service Offering

Service /Offering	Foundation	Enhanced	Advanced
Security Risk Assessment	✓	✓	✓
Policy & Procedure Review	✓	✓	✓
Supply Chain / Third-Party Risk Management	✓	✓	✓
Third-Party Risk Assessments Of Critical Suppliers	✓	✓	✓
Third-Party Threat Intelligence		✓	✓
On-Site Visits			✓
Authentication (2FA/MFA) Testing	✓	✓	✓
Penetration Testing	✓	✓	✓
Vulnerability Assessment	✓	✓	✓
Compliance & Legal Review	✓	✓	✓
Security & Awareness Training	✓	✓	✓
Threat Intelligence		✓	✓
Vulnerability Management		✓	✓
Risk Management		✓	✓
Asset Discovery		✓	✓
Internal Audits		✓	✓
Identity & Access Control Management		✓	✓
Crisis/Disaster Response & Recovery		✓	✓
Business Continuity Planning & Testing		✓	✓
Incident Management Response & Reporting		✓	✓
Network Security & Configuration Review		✓	✓
Forensic Analysis			✓
MXDR & Endpoint Management			✓
Breach Attack Simulations			✓
Red Teaming			✓
Physical Security Audit			✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001