SOLUTION BRIEF

NIS Directive

EU Network and Information Systems (NIS)

Feb. 5, 2022

The EU's 2016 NIS Directive requires all EU Member States (as well as the United Kingdom) to establish security safeguard and incident reporting requirements on a variety of digital and critical infrastructure-like services across the EU.[1] Numerous EU Member States and the UK have issued local regulations implementing the Directive for essential services and digital service providers.[2] The EU Commission also issued a 2018 implementing regulation on security safeguards expected for digital service providers.[3]

For purposes of this brief, we are focusing on the current, EU-wide NIS Directive. However, even if a safeguard is not specifically included in the Directive, it may still appear in implementing regulations from EU Member States or the UK. It is also worth noting that in 2020 the EU Commission proposed a significant expansion of the NIS Directive, called NIS 2, which is presently under negotiation among EU lawmakers. For more information about the NIS 2 proposal, please check out our blog.[4]

Below, learn more about the NIS Directive and how Rapid7 can help you achieve your compliance goals.[5]

Who is Affected?

The NIS Regulations apply to essential services and digital services operating in the Member State and UK territories that meet thresholds for size and criticality.[6] The EU Directive specified that these services include healthcare, banking, financial market infrastructure, water supply, transport, energy providers, digital infrastructure, and digital services (online marketplaces, cloud services, online search services).[7] EU Member States designate specific organizations as being regulated based on how strategically important the entities are to the State (i.e., market size, national security, economic impact, etc.).[8]

Rapid7 Solutions Overview

[1] EU Directive 2016/1148, Art. 1.2., 14, 16. The UK was an EU Member State when the Directive was enacted.

[2] See https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive See also, Bird & Bird Developments on NIS Directive in EU Member States (2020), https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf.

[3] EU Commission Implementing Regulation 2018/151. Note: EU Directives tell a Member State the broad outcome, but leaves details open to the State to "transpose" into national laws. EU Regulations issue more detailed requirements that bind Member States.

[4] The proposed NIS 2 Directive would, among other things, establish more stringent security requirements to more organizations. For an analysis of the draft NIS 2 in comparison to NIS 1, see https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive.

[5] Note: This brief is for informational purposes only and does not constitute legal advice.

[6] EU Directive 2016/1148, Art. 6.

[7] EU Directive 2016/11486, Annex II-II.

[8] EU Directive 2016/1148, Art. 6.

Below is a chart of Rapid7's solutions that can help organizations meet security requirements under the NIS Directive. Each of the products and services help organizations address their compliance needs in specific ways. The shaded cells highlight the key solutions for each security requirement.[9]

NIS Directive	InsightVM & Managed VM	InsightIDR & MDR	InsightAppSec & Managed AppSec	InsightCloudSec	Metasploit	Consulting Services
Have technical and organizational safeguards for networks and systems	✓	✓	✓	✓	✓	✓
Assess risks to network and system security	✓		✓	✓	✓	✓
Prevent, detect, and minimize the impact of security incidents		✓	✓	✓		✓
Monitor, audit, and test security of networks and systems	✓		✓		✓	✓

How Rapid7 supports compliance with NIS Directive requirements

The NIS Directive requires EU Member States to establish security and reporting requirements for essential services and digital service providers.[10] While the specific security requirements of each Member State may vary, the requirements must follow the broad outlines in the EU Commission's NIS Directive and implementing regulation. Because the EU Commission issued an implementing regulation on digital service providers, there is greater detail regarding security expectations for those providers than for essential services.[11]

Below, we summarize NIS Directive security requirements, with citations to the official text, and provide information on the primary Rapid7 solutions that can help fulfill the requirements. We organize the NIS Directive requirements into four basic categories: 1) Security sageguards; 2) Risk assessment; 3) Incident prevention, detection, and response; and 4) Monitoring, auditing, and testing.

1. NIS - Technical and organizational safeguards for networks and systems

- Essential and digital services must take appropriate technical and organizational

[9] For example, in helping to establish a comprehensive security program, Rapid7's Consulting Services is the primary go-to solution, and therefore that cell is shaded. However, each of Rapid7's other solutions also help support the maintenance and implementation of a comprehensive security program.

[10] EU Directive 2016/1148, Art. 1.2., 14, 1.

[11] EU Commission Implementing Regulation 2018/151.

safeguards to manage risks to the security of networks and information systems.[12]

- Essential and digital services must take appropriate measures to prevent and minimize the impact of security incidents.[13]
- Digital services must implement processes to identify vulnerabilities in information systems.
- Digital services' measures for security of systems and facilities must include asset management, secure system lifecycle management, data protection (encryption where applicable), security business continuity planning, and access controls.

Key Rapid7 solutions to help meet this practice:

- Rapid7 service: **Cybersecurity Maturity Assessment** - Measures the effectiveness of your cybersecurity program by evaluating the implemented controls and giving recommendations to improve control maturity. Control sets and frameworks we specialize in currently include PCI DSS, HIPAA, NYDFS, NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, CIS Controls, and more.[14]
- Rapid7 service: **Cybersecurity Policy Development** - Develops the governing documentation that allows the organization to know what is expected of them and their role in managing cybersecurity.[15]
- Rapid7 solutions: **InsightVM and Managed VM** - Perform comprehensive scanning to identify vulnerabilities. Detect misconfigurations, as well as identify missing patches and malicious software. Support the entire vulnerability management lifecycle, including collection of asset information, prioritization of vulnerabilities according to real-world risk, and remediation workflows to help reduce overall organizational risk.[16]
- Rapid7 solutions: **InsightIDR and Managed Detection and Response** - Monitor for threats and leverage contextual, environment-specific analysis and behavioral analytics. Automatically correlate activity on your network to the users and entities behind them, making it easy to spot risky behavior, as well as detect lateral movement and the use of stolen credentials.[17]
- Rapid7 product: **InsightCloudSec** - Continuously scan and monitor cloud resources throughout your cloud environment to ensure services are encrypting both data at rest and in transit. Help govern Identity and Access Management (IAM) and adopt a unified zero trust security model across your cloud and container environments.[18]
- Rapid7 product: **InsightAppSec and Managed AppSec** - Identify and report on application and API security risks for prioritization and remediation/mitigation. This solution integrates into DevOps workflows to prevent new risk from entering production environments.[19]

[12] EU Directive 2016/1148, Art. 14.1, 16.1.

[13] EU Directive 2016/1148, Art. 14.2, 16.2.

[14] Rapid7, Security Program Assessment, https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-assessment.

[15] Rapid7, Security Policy Development, https://www.rapid7.com/services/security-consulting/security-advisory-services/security-policy-development.

[16] Rapid7, InsightVM, https://www.rapid7.com/products/insightvm. Rapid7, Managed Vulnerability management, https://www.rapid7.com/services/managed-services/vulnerability-management.

[17] Rapid7, InsightIDR, https://www.rapid7.com/products/insightidr. Rapid7, Managed Detection and Response, https://www.rapid7.com/services/managed-services/managed-detection-and-response-services.

[18] Rapid7, InsightCloudSec, https://www.rapid7.com/products/insightcloudsec.

[19] Rapid7 InsightAppSec, https://www.rapid7.com/products/insightappsec. Rapid7 Managed AppSec, https://www.rapid7.com/services/managed-services/managed-appsec.

2. NIS - Assess risks to network and system security

- Measures taken for the security of networks and information systems must be appropriate to the risks and reflect the state of the art.[20]

Key Rapid7 solutions to help meet this practice:

- Rapid7 service: **Cybersecurity Maturity Assessment** - Evaluate the effectiveness of your cybersecurity controls, plus get a risk-based security roadmap as well as detailed recommendations.

- Rapid7 service: **Security Risk Assessment** - This service performs a qualitative risk assessment using a common baseline of security controls and evaluates to business impact. It also provides a repeatable process for organizations to follow when completed.[21]

- Rapid7 solutions: **InsightVM and Managed VM** - Get top-down visibility of risk to cyber assets (such as servers, endpoints, networking devices, and more) and business operations; this enables teams to prioritize assets and quickly focus on the items that pose the greatest risk. Identify where vulnerabilities and insecure configurations exist in their technology environment, which is the foundational basis for understanding and treating risk.

- Rapid7 product: **InsightCloudSec** - Provide your cloud environment with automated discovery and inventory assessment across cloud service providers and containers. It also allows for the alignment of governance, policy, and practices to be monitored and managed in cloud environments to understand a complete risk picture.

3. NIS - Prevent, detect, and minimize the impact of security incidents

- Digital services must implement incident handling measures, including processes to detect anomalies.[22]

- Essential and digital services must notify authorities of security incidents that have a significant impact on services.[23]

Key Rapid7 solutions to help meet this practice:

- Rapid7 product: **InsightIDR** - Detect incidents and attack activity, leverage behavior analytics, and get indicators of compromise so alerts are issued early in the attack. Accelerate investigations and containment with timelines that centralize audit logs, endpoint telemetry, user activity, network events, and other data so you know what happened and when.

- Rapid7 service: **Managed Detection & Response** - Get continuous detection and response for incidents occurring in your environment using InsightIDR. The service can manage organizational incident response functions as a whole or can augment existing in-house functions. Validated threats can be contained by the MDR SOC team. Full incident reports are sent to you alongside recommendations for any findings (e.g. containment, additional response, and remediation) and recommendations to

[20] EU Directive 2016/1148, Art. 14.1, 16.1.

[21] Rapid7, Security Program Development, https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-development.

[22] EU Directive 2016/1148, Art. 16.1(b). EU Implementing Regulation 2018/151 Art. 2.2.

[23] EU Directive 2016/1148, Art. 14.3-14.4, 16.3-16.4. EU Implementing Regulation 2018/151 Art. 3-4.

improve cyber resilience (e.g. mitigation for future attacks) to strengthen your security posture. Rapid7 MDR also includes Remote Incident Response engagements if the SOC detects live, hands-on-keyboard attackers in your environment, delivered by the same personnel on the Breach Response team.

- Rapid7 product: **InsightCloudSec** - Leverage Cloud Service Provider (CSP) services (e.g., Amazon GuardDuty) for best-in-class intelligent threat detection that continuously monitors for malicious activity and unauthorized behavior. These CSP services use machine learning, anomaly detection, and integrated threat intelligence built by the CSPs themselves to identify and prioritize potential threats.
- Rapid7 service: **Incident Response Plan Development** - This service develops an incident response plan that includes detection, monitoring, response, and recovery. This would include specific requirements for breach notification and reporting, where necessary.[24]
- Rapid7 service: **Breach Response and Retainer** - In the event of a compromise, retainer customers alert the Rapid7 team, who will respond within one hour to plan an approach. Our experts launch incident response activities within 24 hours.[25]
- Rapid7 service: **Compromise Assessment** - This service assesses an organization's systems for leading indicators of compromise and provides visibility into abnormalities. Verify compromise and validate remediation efforts. This service can also be used during the merger and acquisition due diligence phase to assess a target asset.[26]
- Rapid7 service: **Incident Response Readiness Assessment** - Get a full evaluation of your threat detection and incident response capabilities compared with best practices, and identify steps to take your program to the next level.
- Rapid7 product: **tCell** - Leverage runtime application self-protection to monitor and protect web applications, APIs, and microservices against OWASP Top 10 and Zero-Day Attacks. Monitor and block suspicious actors, immediately identify and remediate breaches, and integrate application security into your DevOps toolchain and SOC.[27]

4. NIS - Monitor, audit, and test security of networks and systems

- Digital services' security measures must account for monitoring, auditing, and testing, including vulnerabilities in networks and information systems.[28]

Key Rapid7 solutions to help meet this practice:

- Rapid7 solutions: **InsightVM and Managed VM** - Scan your environment for vulnerabilities, identify unaddressed flaws, and prioritize remediation according to assessed risk level. Compare the results of vulnerability scans over time.
- Rapid7 solutions: **InsightAppSec and Managed AppSec** - Scan your modern web applications for vulnerabilities as well as manage risk across your application portfolio and at various stages of the software development lifecycle. Simulate real world web application attacks to understand if safeguards are working as intended.

[24] Rapid7, Incident Response Program Development Services, https://www.rapid7.com/services/security-consulting/incident-response-services/ir-program-development-services.

[25] Rapid7, Incident Response Services, https://www.rapid7.com/services/security-consulting/incident-response-services.

[26] Rapid7, Compromise Assessment Service brief, https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-service-brief-compromise-assessment.pdf

[27] Rapid7, tCell, https://www.rapid7.com/products/tcell.

[28] EU Directive 2016/1148, Art. 16.1(d). EU Implementing Regulation 2018/151 Art. 2.4.

- Rapid7 service: **Penetration Testing Services** - Simulate real-world attacks on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure and show you what it will take to strengthen them.[29]
- Rapid7 service: **Cybersecurity Maturity Assessment** - Measure the effectiveness of your cybersecurity program by evaluating the implemented controls, and get recommendations to improve control maturity.
- Rapid7 service: **Vulnerability Management Maturity Assessment** - Measure the effectiveness of your vulnerability management program by evaluating the implemented processes, workflows and controls, and get recommendations to improve vulnerability identification through to remediation.

Penalties for Noncompliance:

Under the NIS Directive, EU Member State authorities have the power to assess compliance and compel evidence from regulated entities.[30] Under the NIS Directive, EU Member State authorities have the power to assess compliance and compel evidence from regulated entities.[31]

The specific powers and penalties are left up to the EU Member States. For example, the UK (a Member State at the time) announced fines of up to £17 million or 4% of a company's global revenues, depending on the severity.[32]

Further Reading:

- EU Commission "NIS Toolkit"[33]
- ENISA Guidelines on assessing Digital Service Provider security and Operator of Essential Services compliance with the NIS Directive security requirements[34]
- UK National Cyber Security Centre Cyber Assessment Framework[35]
- ENISA "NIS Investments" report on cybersecurity investment and NIS implementation[36]
- Rapid7, Overview of the EU's draft NIS 2 Directive and Comparison with NIS 1[37]
- Rapid7 white paper, Simplifying the complex: Common practices across cybersecurity regulations[38]

[29] Rapid7, penetration testing services, https://www.rapid7.com/services/security-consulting/penetration-testing-services.

[30] EU Directive 2016/1148, Art. 15, Art. 17. Member State authorities may supervise essential services at any time, and supervise digital services when they are aware of evidence of noncompliance.

[31] EU Directive 2016/1148, Art. 15.3, Art. 17.2(b).

[32] https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security

[33] http://data.consilium.europa.eu/doc/document/ST-12205-2017-ADD-1/en/pdf

[34] https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

[35] https://www.ncsc.gov.uk/collection/caf

[36] https://www.enisa.europa.eu/publications/nis-investments

[37] https://www.rapid7.com/globalassets/_pdfs/policy/rapid7-nis-summary-analysis-2021.pdf

[38] https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/whitepaper-simplifying-the-complex-120821.pdf