NIS2 Requirement	How WithSecure can help		
Policies on risk analysis, security policies	**WithSecure Consulting:** Services include risk framework alignment, risk analysis, security assessments and penetration testing, which align with NIS2's requirement for regular risk analysis and vulnerability assessments.		
Incident management	**WithSecure Elements XDR:** Provides anomaly detection and incident response capabilities, enabling early threat detection and automated responses. Provides assurance to auditors and regulators of adequate cloud security risk and governance controls.	**WithSecure Incident Response Service:** Ensure quick response to and management of cyber security incidents, with forensics support for comprehensive analysis.	**WithSecure Managed Detection and Response (MDR):** A managed service that continuously monitors and responds to incidents, enhancing end-to-end threat detection and incident response capabilities. The inclusion of incident handling expertise ensures organizations comply with NIS2's mandates for operational security measures and breach mitigation.
Business continuity and recovery	**WithSecure Elements Exposure Management:** Continuously address threats with risk-based prioritization as part of your vulnerability management and asset management with Elements. Offers continuous recommendations by simulating attack paths, identifying critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.	**WithSecure Consulting:** Helps establish and test business continuity plans, ensuring organizations can quickly prepare for and recover from incidents.	
Supply chain, vendor and service provider security	**WithSecure Elements Collaboration Protection:** Provides protection across cloud platforms used by suppliers and partners, ensuring secure access and data exchange. Adds protection to Microsoft 365 native security capabilities, addressing advanced cyber threats such as malware, ransomware, compromised accounts, phishing and targeted attacks.	**WithSecure Consulting:** Supply chain state analysis to measure, understand, and communicate your organizations risk	
Security in network and information systems	**WithSecure Elements Exposure Management:** Identify and assess your digital exposure, providing continuous visibility into vulnerabilities of your attack surface. Offers continuous recommendations by simulating attack paths, identifying critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.	**WithSecure Elements Extended Detection and Response (XDR):** Protects assets by detecting and responding to threats. Provides assurance to auditors and regulators of adequate cloud security risk and governance controls.	**WithSecure Co-Monitoring Service:** Threat hunters automatically handle elevated risks detections and provide you with remedial guidance. The service validates and investigates detections to establish criticality and next actions, as well as ensures complete visibility and protection by constantly monitoring your IT environments.
Evaluation of cyber security and risk management effectiveness	**WithSecure Elements Exposure Management:** Discover your attack surface, understand your attack and get support for risk assessment. It provides an overview of Internet facing assets and risks to be used for risk management. Offers continuous recommendations by simulating attack paths, identifying critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.	**WithSecure Consulting:** Cyber security risk management and strategy development for compliance and operational resilience.	
Cyber security training and hygiene	**WithSecure Elements:** Includes all security capabilities in one platform, from identifying, protecting, detecting and responding to advanced threats. Supporting function: Elements provides an overview of Internet facing risks and their migitation which can be used for training purposes	**WithSecure Consulting:** Test your preparedness and train your skills with a tailored scenario-based cyber crisis management exercise.	
Encryption and secure communication	**WithSecure Elements Collaboration Protection:** Monitors encrypted communications across collaboration platforms, ensuring compliance with encryption standards. Adds protection to e.g. Microsoft 365 native security capabilities, addressing advanced cyber threats such as malware, ransomware, compromised accounts, phishing and targeted attacks.	**WithSecure Exposure Management:** Provides continuous assessment of Internet exposed encryption settings for industry compliance. Offers continuous detection of critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.	**WithSecure Consulting:** Advice on design and implementation, compliance checks and audits of encryption settings
Personnel security, access control, and asset management	**WithSecure Elements Identity Security:** Detects potentially compromised identities that are used by attackers to access Microsoft 365 or other cloud-based services. Helps organizations monitor and manage potential insider threats or external attackers compromising staff credentials, reducing the risk of identity-based breaches. Ensures that all endpoints and assets (both physical and cloud-based) are monitored and protected, helping organizations meet NIS2's asset management requirements.	**WithSecure Exposure Management:** Provides continuous assessment of identity-based risks in your environment. Continuous detection of non-compliant access control e.g. exposed assets and continuous mapping of Internet exposed assets for supporting asset management. Offers continuous recommendations by simulating attack paths, identifying critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.	
The use of multi-factor authentication or continous authentication	**WithSecure Consulting:** Advice on design and implementation, compliance checks and audits of MFA implementation	**WithSecure Elements Exposure Management:** Continuous detection of non-compliant attack surface e.g. detection of static authentication (lack of MFA). In combination with asset criticality categorization and risk categorization can monitor your most critical assets and provide recommendations.	