Microsoft

unitec
Accessible Expertise

Stee O’Brien

Westcoast

CYBER SECURITY EVENT


Managed Services


IT Infrastructure


Cloud Computing


Telecoms


Security


Disaster Recovery

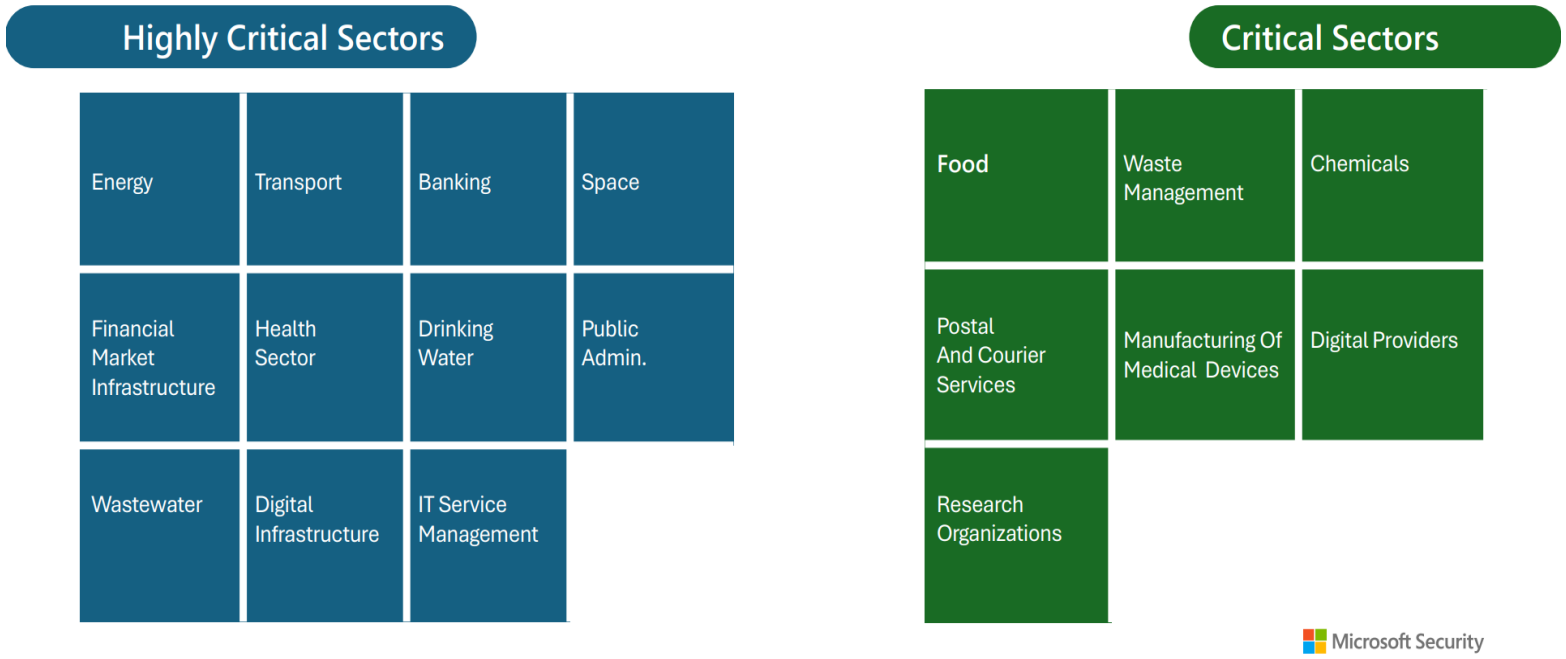
NIS 2.0 Directive

Stee O'Brien
Senior Business Development Manager

Understanding NIS2 Directive

NIS2 Objectives			
Manage Security Risk	Protecting Against Cyber Attack	Detecting Cyber Security Incidents	Minimizing The Impacts Of Cyber Security Incidents
Ensure cybersecurity risk assessments are carried out	Implementing technical & organizational measures	Staying on top of cybersecurity through training & risk management programs	Managing risks appropriately

Who NIS2 Impacts



Critical Infrastructure Sectors

NIS2 covers essential sectors such as energy, transport, banking, health, and public administration, ensuring their digital resilience.

Manufacturing and Services

Important entities in waste management, food production, and critical manufacturing are also required to comply with NIS2 regulations.

Digital Service Providers

Digital infrastructure, including cloud computing, data centers, and managed service providers, must follow NIS2 security requirements.

Key Compliance Requirements

Cybersecurity Risk Management Measures

Risk Management	Security Policies	Incident handling (prevention, detection & response to incidents)	Business continuity and crisis management
Supply chain security consider supplier vulnerabilities	Vulnerability handling and disclosures	Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)	
The use of cryptography and encryption where warrante	Basic cybersecurity hygiene & training	The use of MFA or continuous authentication	

Incident Reporting Obligations

Report incidents with significant* impact on the provision of services

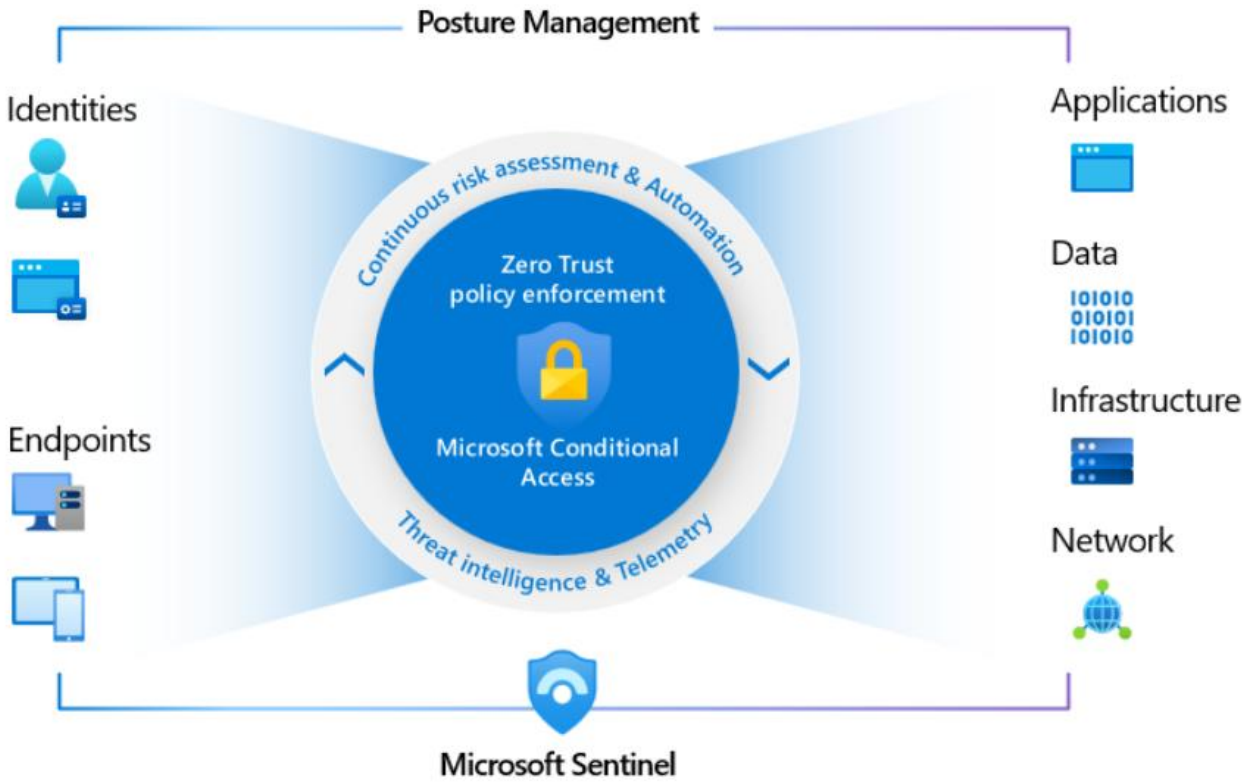
Within 24 hours	Within 72 hours an extensive report	Within 1 month a final report progress report

**=An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*

Computer Security Incident Response Team (CSIRT)	Competent Authority	Recipients of services

Microsoft Security

Microsoft Enabling NIS2 Compliance



- **Microsoft 365 Business Premium + E5 Security Add-On**

Target Audience: Small to medium-sized businesses (up to 300 users)

Base Features in Business Premium:

Microsoft 365 Apps (Word, Excel, Outlook, etc.)
Microsoft Entra ID Plan 1 (basic identity protection)
Microsoft Intune Plan 1 (device and app management)
Microsoft Defender for Business (endpoint protection)
Microsoft Defender for Office 365 Plan 1 (email protection)
Microsoft Purview DLP for email and files

E5 Security Add-On Includes:

Microsoft Entra ID Plan 2: Adds risk-based conditional access, PIM (Privileged Identity Management), access reviews, and entitlement workflows
Microsoft Defender for Identity: Detects identity-based threats across hybrid environments
Microsoft Defender for Endpoint Plan 2: Adds threat hunting, live response, and IoT device protection
Microsoft Defender for Office 365 Plan 2: Includes automated investigation and response, attack simulation training, and threat analytics
Microsoft Defender for Cloud Apps: Monitors SaaS usage, detects shadow IT, and enforces app governance
Microsoft Defender for IoT: Protects enterprise IoT devices

- **Microsoft 365 E5 (Full Suite)**

Target Audience: Large enterprises or organizations with complex needs

Includes Everything in Business Premium + E5 Security, plus:

•**Unlimited users**

•**Advanced compliance tools**: Microsoft Purview Information Protection, Advanced eDiscovery, Advanced Audit, Records Management

•**Insider Risk Management & Communication Compliance**

•**Power BI Pro**: Advanced analytics and data visualization

•**Microsoft Teams Phone Standard**: Cloud PBX and audio conferencing

•**Expanded Teams meeting capacity**: Up to 1,000 participants

Service Summery

	M365 & E5 Sec Add-on	M365 E5
User Limit	Up to 300 users	Unilimited
Security	Advanced (via add-on)	Advanced
Compliance	Basic	Advanced
Analytics	Not included	PowerBI Pro