semperis

WHITE PAPER

NIS2 and Your Identity Infrastructure

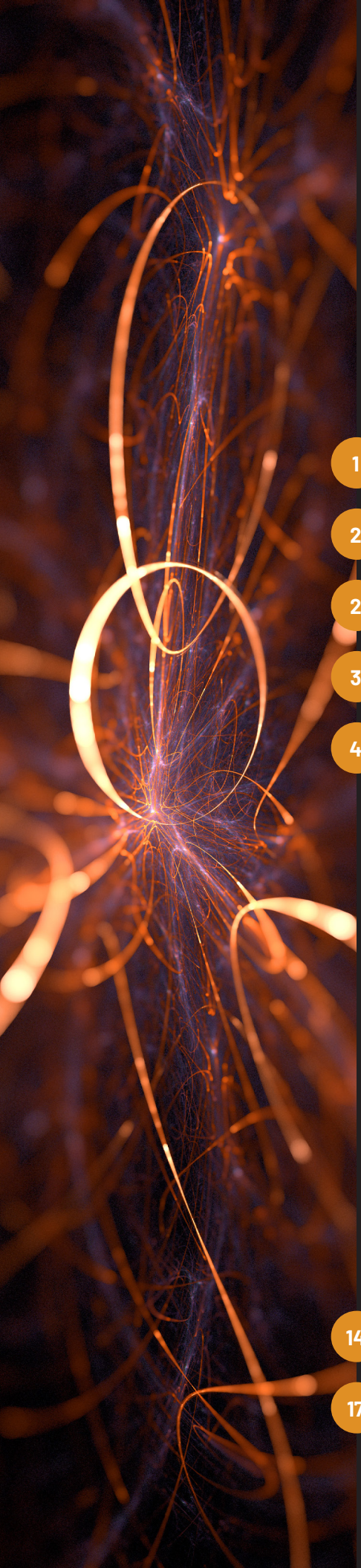

TABLE OF Contents

semperis

Introduction

With the global escalation of destructive cyberattacks, cybersecurity and business continuity management are now central to the overall resilience of critical societal services and infrastructure.

In 2016, the European Union (EU) signed into law the Network and Information Security Directive (NIS), requiring implementation by member states by May 2018. The initial directive aimed to address the risk to societal services from increasingly aggressive and capable threat actors. NIS related to critical industry sectors, including utilities, health, and transport, and the legislation directed all covered entities to implement robust controls for risk management, protection from cyberattacks, and reporting of security incidents. The alternative was to incur significant fines.[1]

In October 2024, the updated directive, NIS2,[2] came into force in EU member countries. NIS2 addresses multiple gaps in the implementation of the original directive, expanding its scope by including new requirements to improve supply chain security, adding regulated industries,[3] increasing focus on third-party supply chain risk, and tightening incident reporting and sharing requirements.

This paper will look at how specific aspects of NIS2 will impact the requirements of operating secure and resilient identity systems.

---

1 DIRECTIVE (EU) 2016/ 1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 6 July 2016 - concerning measures for a high common level of security of network and information systems across the Union

2 Directive - 2022/2555 - EN - EUR-Lex

3 These include (for example) postal/courier services; waste management; manufacturing; production and distribution of chemicals; food production, processing, and distribution; and digital providers.

Why are these regulations needed?

When NIS was introduced, the impacts of cyberattacks on critical sectors were already becoming clear. NotPetya—a costly nation-state attack on another nation's critical infrastructure—caused significant damage, including a week-long outage at the Maersk logistics company that disrupted its global Active Directory (AD) infrastructure. Around the same time, organised crime capitalised on ransomware, driving up societal costs. In 2017, Triton malware targeted a refinery's safety system in the Middle East, spreading to 15,000 sites and demonstrating a shift toward attacking critical systems where lives could be at stake. By 2024, the number of ransomware attacks peaked at 5,263, with one Fortune 100 company paying $75 million in ransom.[4]

Shifting from NIS to NIS2

The NIS directive significantly raised the stakes for critical national infrastructure providers across the EU. The regulation required an uplift of security capabilities for a wide range of sectors, establishing:

- Guidance regarding security controls and incident management
- Significant fines for breaches as defined by member states
- Risk management requirements focusing on the ability to identify risks and prevent, detect, and handle incidents
- Defined executive responsibilities
- A requirement for Computer Security Incident Response Teams for each member state
- High-level assurance and regulatory enforcement
- Clearer definition of essential services in the EU
- Security governance requirements

Organisations covered by the directive—Operators of Essential Services (OES), as the regulations dubbed them—had to develop their capabilities significantly, often from low maturity, and the potential consequences of failing in security went up.

On 17 October 2024, just as organisations had adapted to the original 2018 regulation, NIS2 came into effect, adding a significant number of wide-ranging requirements to the original regulation. Some of the key areas for organisations in scope[5] include:

- Tighter regulations regarding security risk management
- More stipulations for cross-country collaboration concerning incidents
- Stricter requirements for incident reporting
- New third-party risk management requirements, including vulnerability management
- Further stipulations around management responsibilities
- Specified fines of up to 2% of global turnover

Additionally, the regulation explicitly calls out board-level accountability *and* the option for member states to outline criminal liabilities for individuals for infringements of the regulations.[6]

4 Cyber Threat Monitor Report 2024 | NCC Group

5 This report does not cover the transnational and EU-wide governance measures in any detail.

6 Section 131

Which entities are in NIS2 scope?

NIS2 expanded the sectors in scope in their lists of essential and important entities.

Essential Entities (Sectors of High Criticality)	**Important Entities** (Other Critical Sectors)
Energy	Postal and Courier Services
Transport	Waste Management
Banking	Chemicals
Financial Market Infrastructures	Production, Processing, and Distribution of Food
Health	Manufacturing
Water	Digital Providers
Digital Infrastructure	Research
ICT Service Management (B2B)	
Public Administration	
Space	

The new directive specifies more narrowly who needs to comply and with what. Under previous rules, member states were not sharing data to a sufficient degree, enforcement was too lax, and organisations did not commit sufficient resources to the cyber resilience of their essential services.

What controls do essential and important entities need to implement?

The directive does not prescribe which detailed controls to apply. Rather, the expectation is that entities identify a relevant and comprehensive security controls framework; examples include the NIST Cyber Security Framework 2.0 or the ISO/IEC 27001:2022 international standard. Controls required are outlined in Chapter IV, article 21 of the directive.

Controls for NIS2	
Policies on risk analysis and information system security	Policies and procedures to assess the effectiveness of security measures
Incident handling	Basic cyber hygiene practices
Business continuity, disaster recovery, and crisis management	Policies for encryption and use of cryptography
Supply chain security, including entity-to-supplier relationships	Human resources security, access control policies, and asset management
Security of systems acquisition, development, and maintenance	Multifactor authentication or continuous authentication solutions

This overview of controls is supplemented by section 57, describing active cyber protection.

Active Cyber Protection	
Prevention	Detection
Monitoring	Analysis
Mitigation	

In the following sections, we outline our interpretation of how you can enhance your NIS2 compliance through your identity system security measures.

Why identity security

NIS2 compliance is a large undertaking for any organisation in its scope. Such organisations are likely to be complex, have significant legacy systems, and have large geographical and technological coverage. We see identity security as essential in critical infrastructure cyber resilience for three key reasons.

1. Together with data-level security, identity management is the new security perimeter.
2. Threat actors have significantly advanced their tradecraft as it pertains to identity-driven attacks.
3. Identity systems are a key foundation (and thus dependency) for most large organisations' information and communications technology (ICT) services.

It is well-established that identity has become the new battleground for defenders and attackers. Microsoft sees 600 million attacks a day against the Entra ID identity infrastructure, and they suspended nearly 64 million abusive administrative accounts in 2023.[7] Meanwhile, IBM reported in 2024 that 74% of data breaches start with privileged credential abuse.[8] In addition to the significant volume of identity-based attacks, the most prolific ransomware actors leverage these attacks for extortion. Ransomware as a service groups such as RansomHub, ALPHV Blackcat, and PlayCrypt all leverage AD account discovery and AD account creation and re-enablement to establish persistence in targets, move laterally, and escalate privileges for further impacts.[9,10,11]

Additionally, identity systems play an important role in the overall resilience of the organisation. NIS2 requires an understanding of the risk of your ICT-based essential services, which tend to rely on user and service accounts. The resilience of AD is also notoriously difficult. Full AD recovery is a significant, multi-step activity.[12,13] It is fraught with difficulties due to a high volume of changes and outbound dependencies for services such as certificate management, DHCP, and DNS.[14]

7 Microsoft Digital Defense Report 2024
8 https://www.ibm.com/reports/data-breach
9 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
10 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
11 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
12 https://www.semperis.com/resources/guide-microsoft-ad-recovery/
13 https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-guide
14 AD Forest Recovery—Configure DNS Server service | Microsoft Learn

Security risk management

To manage your overall cyber resilience, you will need a strong focus on asset management and the risks associated with such assets.

Whereas NIS2 is relatively high-level in its descriptions of requirements for security risk management in critical national infrastructure organisations, it does make clear that risk management practices must follow industry standards. The directive explicitly calls out the requirement to "have in place appropriate access control policies." Thus, when mapping your dependencies to ICT services, a strong focus on your identity infrastructure is advised.

NIS2 reference
Section 77-83
Requirement
Entities must foster a culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures.
Implication for organisation
An organisation needs to be able to identify assets that could be impacted by cyber risks. This will invariably involve a view of key processes forming part of the essential or important function, as well as key ICT capabilities and their dependencies.

KEY CONSIDERATIONS

- Establish a security risk management programme based on a comprehensive standard such as the NIST Cybersecurity Framework 2.0, ISO/IEC 27005: 2022,[15] or the Information Security Forum's Information Risk Assessment Methodology 2.[16]
- Ensure you understand the security risks to your identity system (on premises and in the cloud) associated with loss of integrity, confidentiality, or availability of your essential services.
- Understand and mitigate downstream impacts on other ICT services in the case of a compromise or outage of your identity system.

15 ISO/IEC 27005:2022(en), Information security, cybersecurity and privacy protection—Guidance on managing information security risks

16 Information Risk Assessment Methodology 2 (IRAM2)—Information Security Forum

Supply chain security

Supply chain attacks have grown significantly in recent years. High-profile attacks such as those against SolarWinds, MOVEit, and Snowflake have increased the awareness of threats to large organisations that depend on third-party partners. Last year, Verizon reported that around 15% of attacks consisted of a supply chain component.[17] In 2023, the World Economic Forum reported that 90% of organisations are concerned about the cyber resilience of third parties and that 39% had already been impacted in one way or another by a supply chain security incident.[18]

NIS2 reference
Section 85-87
Requirement
ICT services provided by third-party suppliers require assurance of security and resilience.
Implication for organisation
An organisation needs to be able to identify which of its assets could be impacted by cyber risks to third parties. This will invariably involve a review of key processes forming part of the essential or important function, as well as key ICT capabilities and their dependencies.

Third-party cybersecurity breaches impacted many organisations, and it is clear that well-funded, motivated, and highly advanced threat actors increasingly see this as a high-yield path to a successful attack. Microsoft maintains a focus on such attackers, as identity systems such as AD and Entra ID are key attack vectors.

To remain resilient and maintain NIS2 compliance regarding your supply chain security risk, it is strongly advised to create a programme of work to manage key vendors, attain information on key identity vulnerabilities, and build a defence-in-depth model around both cloud and on-premises capabilities. This approach requires preventative controls, detective controls, and crucially, an ability to restore identity systems to a clean, trusted state if they are compromised.

In addition, if you have an outsourced service provider managing your AD, you must emphasise the security capabilities of that managed services provider. Be keenly aware of their ability to keep threat actors out and maintain a cyber-resilient identity system for your organisation.

Your organisation's supply chain security and risk management cannot stand alone, though. Be aware that the EU will perform its own cross-country and sector security risk assessments of critical supply chain.[19] You are responsible for your organisation's identity systems, so it is good to be aware of broader findings that may emerge from such EU-wide assessments.

KEY CONSIDERATIONS

- Manage a record of the risk of critical suppliers, including your identity system services provider.
- Establish a governance, risk, and compliance policy and standards body that maintains supplier standards.
- Establish a vendor security risk assessment process that reviews your suppliers' security policies and ensures adherence to the selected standard(s)(e.g., ISO/IEC 27001:2022, System and Organisation Controls 2 Type 2).
- Establish a contractual agreement with critical suppliers to ensure the appropriate security controls are in place.
- Integrate such supply chain risk management into the broader security risk management framework.

17 2024 Data Breach Investigations Report | Verizon

18 http://www.weforum.org/publications/global-cybersecurity-outlook-2023/

19 Section 91

Vulnerability management

Closely related to the assurance of supply chain security risk are the vulnerability management aspects of commercial off-the-shelf ICT technologies. Vulnerabilities keep increasing; NCC Group reports an increase from just under 30,000 in 2023 to more than 40,000 in 2024. Only a small number of these are actively exploited, but just one opening can lead to untold damage.[20] As an example, Emsisoft reported that nearly 3,000 organisations were affected by the MOVEit breach, which was accomplished by exploiting a zero-day vulnerability.[21]

Management of vulnerabilities in critical identity systems can be a significant undertaking. Attackers search for unpatched vulnerabilities in your internet-facing enterprise IT to get to critical enterprise assets and exploit vulnerabilities that can allow access to your Operational Technology environments. Those critical ICT services are supported by your identity systems, so rapid identification and patching of vulnerabilities is essential.

NIS2 reference

Section 85-87

Requirement

Ensure swift identification of vulnerabilities and remediation and disclosure per international standards such as ISO/IEC 30111 and ISO/IEC 29147.

Implication for organisation

Your identity systems are a major source of security vulnerabilities. Threat actors will use these vulnerabilities, and they will often chain initial access vulnerabilities with identity system vulnerabilities for privilege escalation, lateral movement, or persistence.

KEY CONSIDERATIONS

- Establish a vulnerability programme and continually assess the indicators of compromise (IOCs) in your identity systems.
- Overlay this information on asset management, with a focus on critical services and internet-facing systems.
- Establish a remediation programme and prioritise the remediation of your AD vulnerabilities and indicators of exposure (IOEs).
- To strengthen identity and access management (IAM) security posture, formulate a matrix to remediate your IOEs, starting with all critical, high, and medium severity findings. Rank findings in each category from the easiest to most difficult to remediate.
- Build a patch-management process focusing on remediation of identified vulnerable but critical services and their high-impact vulnerabilities.

20 https://www.nccgroup.com/us/cyber-threat-monitor-report-2024/

21 https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/

Identity and access management

It is of vital importance that you establish strong controls around IAM. NIS2 identifies such controls as key, and your identity systems are essential in this achievement.

Any misconfiguration or vulnerability in your on-premises and cloud identity infrastructure could provide an attacker with the opportunity to compromise foundational security controls and provide them with a direct path to disrupt or compromise an essential or important service. Both AD and Entra ID are complex systems requiring strong experience and skills in configuration and operations, requiring continuous monitoring for IOCs and incoming attacks. Managing such a foundational capability is difficult in large organisations without automation.

NIS2 reference
Chapter IV, article 21
Requirement
Access control, multifactor authentication, multifactor and continuous authentication
Implication for organisation
IAM and privileged account management ensure your organisation allows only authorised access to your critical ICT services. Loss of control of your identity systems will undermine your ability to maintain such security controls.

KEY CONSIDERATIONS

- Implement a least-privilege model of access so specific roles have only the privileges they need to perform their roles.
- Continuously identify vulnerabilities and misconfigurations of your identity infrastructure.
- Establish a programme to monitor IOCs, and identify specific expertise to continually assess and remediate them.
- Implement just-in-time and privileged access management principles to safeguard your most privileged accesses (also known as Tier 0 for AD).
- Review the Entra ID Connect Sync rules to be sure proper segregation of access exists between AD and Entra ID, and only the principals necessary for Entra ID services are synchronised.
- Execute active penetration testing or red teaming and ensure the identity infrastructure is part of the scope. This activity can provide you with additional assurance for your identity security posture and resilience.
- Ensure detection, logging, and reporting are in place for threat hunting.
- Invest in automation of identification, scanning, and remediation capabilities for the identity infrastructure.

Monitoring and detection

Due to the high number of methods focused on attacking AD, monitoring and detection become key to resilience and containment.

When thousands of users operate across your key ICT systems, it is vital that you have logging in place for the appropriate detection of unusual behaviours, malicious actions, and other red flags. This requires you to take a multitude of actions, including appropriate configuration and hardening of your identity systems and integration with a team enabled to monitor and respond in case of any suspected incidents.

KEY CONSIDERATIONS

- Configure and manage security measures on your identity infrastructure.
- Ensure logging is enabled and a trained team is monitoring for suspicious and potentially harmful events.
- Enable secured logs on your identity infrastructure.
- Consider identity-focused analytics tools for a richer data set.

NIS2 reference

Section 57

Requirement

Active cyber protection requires detection and monitoring capabilities, including internal and external monitoring capabilities and tools.

Implication for organisation

To effectively execute on the requirement for active cyber protection, effective cybersecurity monitoring and detection must be in place. Organisations should map their critical ICT services and establish effective logging and monitoring that includes the identity infrastructure.

Business continuity management

To comply with NIS2, you need to secure your infrastructure and ensure you can recover to a secure state in case of an outage or breach.

Your identity infrastructure is key for the use of most, if not all, digitally enabled services. Without a disaster recovery plan for AD and Entra ID, you are unlikely to be able to restore your overall services after a major destructive event. Testing AD can be a significant challenge due to the dependencies and challenges of full forest recovery. Microsoft guides their customers to follow a 28-step process, and even a slight deviation can curtail a successful recovery. To compound the challenge even further, once AD is restored, it still cannot be trusted for use without extensive forensic analysis to remove persistence mechanisms that enable the attacker to retain a footprint after restoring.

NIS2 reference
Chapter IV, article 21
Requirement
Business continuity processes, such as backup management, disaster recovery, and crisis management
Implication for organisation
Identity infrastructure is highly complex, with many interdependencies. It is a core foundation of your ICT services, and it is challenging to restore, making assurance of your ability to restore identity systems a high-priority endeavour for most complex organisations. Such capabilities must be defined and tested to ensure you can rely on them in a cyber breach situation.

KEY CONSIDERATIONS

- Define a plan for identity infrastructure recovery and restore that includes specific members of the team designated for specific recovery tasks.
- Confirm measures to ensure clean-state recovery, including air-gapped backups.
- Establish a realistic test environment and perform frequent restore testing.
- Ensure ongoing business continuity management and disaster recovery testing extend across secondary identity infrastructures, including those added through acquisitions.
- Ensure ICT disaster recovery activities are implemented and integrated with broader business continuity and crisis management plans and exercises.

Incident notifications

NIS2 and subsequent clarifications[22] significantly increase OES requirements for reporting on attacks and near-misses. An incident is regarded as significant when it causes—or could cause—severe operational disruption or financial losses. Initial incident reporting is expected within 24 hours, with a full incident report to regulators due 72 hours after detection. As a result, organisations need rapid identification of breaches and visibility into causes and attacker tactics, techniques, and procedures.

AD forensics is challenging. Attackers will try to attain privileged access, and once this access is achieved, they have broad powers to delete audit logs. Numerous threat actors, such as RansomHub, LockBit, and Ghost, have all made effective use of such techniques.[23]

NIS2 reference
Section 101-108
Requirement
Staged approach to incident notification: initial after 24 hours, first full report after 72 hours, and another full report after 1 month
Implication for organisation
Organised threat actors will rapidly move to the identity system and try to elevate privileges; thus, visibility of this infrastructure is key in performing initial and complete post-breach forensics.

KEY CONSIDERATIONS

- Ensure you can detect and respond to IOCs against your identity infrastructure and report with precision within 72 hours of a malicious event.
- Conduct a thorough security review and identify attack pathways leading to Tier 0 assets, including identification of shadow administrators, nested groups, and local administrative rights, to understand your access risk profile. Ensure the integrity of your identity system logs and your ability to monitor changes within AD in real time.
- Devise an incident response plan that includes clearly defined roles for each member of your team and details their responsibilities during incident response.
- Establish an ability to collect forensically sound data on your AD and perform a forensic investigation to determine the origin and methods of attack.
- Ensure your identity forensics capabilities are integrated and tested as part of your broader incident response readiness.

22 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en

23 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a

Tool specialisation

NIS2 guidance intentionally lacks specificity, so it covers many aspects of security across a breadth of information systems. The translation of such a high-level regulatory framework is difficult across a complex ICT environment. Often, a specialised toolset designed to secure these systems will allow you and your organisation to shift from day-to-day operations to a strategic focus while efficiently implementing policies and procedures to keep your identity systems secure.

Consider evaluating purpose-built identity security solutions—such as those from Semperis—which offer a layered security approach through community and paid tools that directly address the challenges of complying with NIS2.

How can Semperis help?

Semperis provides specialised capabilities that address NIS2 challenges.

Challenge	How Semperis can help	Solution
Risk management To comply with NIS2, it is vital that your organisation's appointed risk manager has tools for ICT resilience.	• Mapped dependencies to enable restore of AD • Visibility into identity system security posture • Proactive risk identification and management for NIS2 compliance	• Active Directory Forest Recovery (ADFR) can map and automate forest recovery, including relevant dependencies. • Purple Knight provides point-in-time security assessment of AD. • Directory Services Protector (DSP) provides continuous threat and vulnerability detection. • DSP provides tamperproof tracking by capturing every change made in AD and identifying and automatically rolling back malicious changes. • Migrator for Active Directory streamlines AD modernisation by mapping AD dependencies and migrating objects to a greenfield environment.
Supply chain security If you outsource your AD operation, you will need a strong focus on third-party risk. Regardless, if you are leveraging Entra ID, Microsoft will be a third-party supplier to your organisation.	• Complete view of the security posture of outsourced identity infrastructure services • Evidence of resilience and restorability of your identity infrastructure services	• DSP enables continual detection of IOEs, enables automatic rollback of unintended changes and proactive monitoring and security of service accounts. • ADFR enables automated, clean restore to any hardware or cloud solution.

Challenge	How Semperis can help	Solution
Vulnerability management It is vital to be able to identify, prioritise, and mitigate vulnerabilities and IOEs.	• Semi-automated, research-led view of software vulnerabilities and misconfigurations • Point-in-time vulnerability and misconfiguration scanning • Continuous, automated vulnerability and misconfiguration scanning	• Lightning Intelligence provides clear security posture insights across hybrid AD and Entra ID environments in an easily deployed SaaS solution to simplify security posture assessments. • Find and fix existing security vulnerabilities with Purple Knight. • Use DSP for continuous threat and vulnerability detection and automatic rollback of unintended changes.
Identity and access management You rely on the integrity, security, and resilience of AD and Entra ID to achieve privileged access and IAM objectives.	• Identification and eradication of misconfigurations and vulnerabilities • Rapid restore in case of an outage to enable teams to continue working securely • Understanding of attack paths used to gain administrative access	• DSP enables the continuous monitoring of security posture of AD and Entra ID. • ADFR fully restores your AD forest up to 90% faster than manual recovery. • Forest Druid (no cost community tool) discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • Forest Druid supports AD teams in mapping attack paths automatically.
Monitoring and detection Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection.	• Meet AD and Entra ID monitoring requirements to detect attacks and accurately report incidents • Comprehensive control of the rich, constantly changing AD environment and attack surface • Visibility into AD-focused attacks and changing vulnerabilities	• DSP enables continuous assessment of AD IOEs, automated rollback of malicious changes, and ML-based AD attack detection. • DSP provides tamperproof logs, and highly specialised AD and Entra ID threat analysis enables up-to-date, industry-leading insights and automation for identity security and enrichment of Security Operations Centre visibility through security information and event management integration. • Semperis products are enhanced by deep research from the AD-focused threat team.

Challenge	How Semperis can help	Solution
Business continuity management To comply with NIS2, you need to be able to restore your identity infrastructure rapidly, and have tests to validate that you can.	• Early detection or avoidance of a security breach of your identity infrastructure and dependent ICT services • Proven, clean-state restore with validated recovery point objectives and recovery time objectives • Well-maintained ICT services	• ADFR automates the complicated AD recovery process and recovers AD up to 90% faster than manual recovery. • ADFR accelerates post-breach forensics to remove persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant recovers Entra ID objects and multi-tenant service principals to a known-good state.
Incident response and forensics NIS2 imposes strict incident reporting requirements on organisations.	• Secure logs for forensic analysis • Enhanced ability to detect malicious actions • Rapid incident reporting when attacks impact AD and Entra ID	• DSP's tamperproof change tracking enables change visibility even with security logging turned off, if logs are deleted, agents are disabled or not working, or if changes are injected directly into AD or Entra ID. • Lightning Identity Runtime Protection uses AI models to detect ongoing AD attacks that are traditionally buried in logs and difficult to detect.

Conclusion

NIS2 is a regulation applying to essential and important sectors in the EU. To comply with the regulation, we recommend you establish seven major capabilities for the resilience of your AD and Entra ID services.

1. Establish a programme for risk management and ownership for your identity system.
2. Establish a comprehensive and automated exposure, threat, and vulnerability monitoring programme and integrate this capability into your security operations centre.
3. Reduce the attack surface of your AD and Entra ID infrastructure through continuous monitoring for IOEs and IOCs.
4. Ensure you meet the requirements and have effective means of managing identity system risk in your supply chain.
5. Build a tested incident response capability for your ICT services, including your identity system, to enable rapid incident response, reporting, and forensic capabilities.
6. Have an automated and tested recovery process to enable you to rapidly restore your AD to a trusted state in the case of a destructive incident.
7. Establish a project of continuous improvement, including best practices from experienced professionals in the cybersecurity industry.

In our experience, achieving these capabilities and maintaining them over time is not possible without significant automation. Semperis' market-leading products can provide you with these threat-led, automated capabilities.