proofpoint.

Version 1.0 DRAFT
October 2023

The EU NIS2 Directive: Strengthening Cybersecurity across Europe

Enhancing EU NIS2 Compliance

The EU Network and Information Systems Directive 2 (NIS2) stands as a cornerstone of cybersecurity regulation, emphasizing the paramountcy of fortified network and information systems across enterprises. Proofpoint, with its suite of solutions — AEGIS, ITDR, and SIGMA — demonstrates a seamless alignment with the explicit Articles within NIS2. This tailored alignment underscores Proofpoint's commitment to bolstering enterprise cybersecurity by Breaking the Attach Chain while ensuring regulatory adherence. This article meticulously elucidates how each Proofpoint solution correlates with specific NIS2 Directive Articles, illustrating a pathway towards both enhanced security posture and compliance.

Contents

High level Overview

PROOFPOINT AEGIS

A comprehensive AI/ML threat protection platform that disarms today's advanced attacks, including BEC, phishing, ransomware, supply chain threats and more.

Key features

- Advanced Email Threat Protection incl. Supplier/Third-party Risks within trusted communication.
- Email incident management - SOC automation
- Security awareness training
- Domain protection (DMARC)

AEGIS facilitates NIS2 compliance in the following key areas.

- Incident management
- Risk management
- Information sharing

NIS2 mapping (Aegis)

- Article 18 (Supplier Security): AEGIS provides comprehensive visibility into attack vectors, helping organizations to understand risks posed by suppliers, thus aiding in achieving compliance with Article 18 of NIS2 which underscores supplier security.

- Article 20 (Incident Reporting): The facilitation of rapid reporting, analysing, and remediating potentially malicious emails through the Closed-Loop Email Analysis and Response (CLEAR) component directly corresponds with Article 20's emphasis on incident reporting.

- Article 19 (Security Monitoring): AEGIS's automated prioritization and classification of suspected phishing emails aligns with Article 19, which mandates security monitoring to swiftly identify cybersecurity incidents.

PROOFPOINT ITDR

An advanced identity threat detection and response solution designed to safeguard organizations against identity theft and vulnerabilities within identity systems.

Key features

- Continuous discovery and remediation of Identity vulnerabilities
- Detection of lateral movement and privilege escalation
- Deception technology to thwart attackers

ITDR aids organizations in meeting NIS2 requirements pertaining to

- Access control
- Vulnerability management
- Incident management

NIS2 mapping (ITDR)

- Article 17 (Identity and Access Management): ITDR's robust detection of vulnerabilities in identity fabric aligns with Article 17's focus on robust identity and access management.

- Article 16 (Preventative Measures): Proofpoint Spotlight, by preventing identity threats and detecting lateral movements, echoes the preventative measures emphasized in Article 16.

- Article 19 (Incident Detection): The high-fidelity detection of privilege escalations by Proofpoint Shadow resonates with Article 19's focus on incident detection, ensuring enterprises are well-prepared to identify and respond to threats.

PROOFPOINT SIGMA

An integrated information protection platform that provides unmatched visibility into data risk by analysing content, behaviour and threats from a single cloud-native console, stopping data loss while saving time and operational cost.

Key features

- Content-aware protection
- User behaviour analytics
- Threat intelligence

SIGMA assists organizations in adhering to NIS2 stipulations for

- Data protection
- Incident management
- Risk management

NIS2 mapping (Sigma)

- Article 16 (Security Measures) and Article 17 (Management of Personal Data): SIGMA's people-centric security approach directly aligns with the security measures and management of personal data as stipulated in Articles 16 and 17 of NIS2. By preventing data loss through varied user scenarios and securing remote working environments, SIGMA encapsulates the essence of these crucial NIS2 articles.

Conclusion: Elevate Your Cybersecurity Posture with Proofpoint

Proofpoint's solutions offer a compelling avenue for organizations to align with the EU NIS2 Directive and augment their overall cybersecurity resilience. Through the deployment of these solutions, organizations can effectively mitigate the risk of cyberattacks and fortify the protection of their critical assets.

Proofpoint's solutions can facilitate compliance with various sections of the NIS2 Directive, including:

- Article 14: Risk management
- Article 16: Incident management
- Article 18: Information sharing
- Article 20: Access control
- Article 22: Vulnerability management
- Article 28: Data protection

In tandem, Proofpoint's solutions also underpin compliance with the fundamental tenets of the NIS2 Directive, encompassing:

- Security by design
- Default security
- Data protection

The Benefits of Proofpoint Solutions

Employing Proofpoint's solutions for NIS2 Directive compliance yields an array of advantages, including:

- Reduced susceptibility to cyberattacks.
- Heightened protection of critical assets
- Enhanced cybersecurity risk management
- Conformance with EU regulations

Supplier/Third-party Risks

Supplier or third-party risk is a crucial topic addressed in the EU NIS2 Directive. The directive acknowledges that supply chains and third-party vendors can introduce significant cybersecurity risks, and it mandates organizations to implement measures to manage and mitigate these risks effectively.

The NIS2 Directive emphasizes the importance of proactive risk management in relation to suppliers and third parties. Organizations are required to identify, assess, and address potential vulnerabilities arising from their reliance on external entities within their digital ecosystems.

Specifically, the NIS2 Directive outlines the following requirements for organizations:

- Identify and Assess Supplier/Third-party Risks: Organizations must conduct thorough assessments of the cybersecurity risks posed by their suppliers and third-party vendors. This includes evaluating their security practices, incident response capabilities, and overall security posture.

- Implement Risk Mitigation Strategies: Based on the identified risks, organizations must implement appropriate measures to mitigate and manage these risks. This may involve contractual obligations, security audits, continuous monitoring, and collaborative efforts to enhance cybersecurity practices.

- Monitor Supplier/Third-party Performance: Organizations must continuously monitor the cybersecurity performance of their suppliers and third parties. This includes evaluating their adherence to security standards, incident reporting, and overall risk management practices.

- Information Sharing and Collaboration: The directive encourages organizations to share relevant cybersecurity information with their suppliers and third parties. This open communication fosters a collaborative approach to addressing potential threats and vulnerabilities within the supply chain.

The NIS2 Directive's emphasis on supplier and third-party risk management reflects the growing significance of supply chain cybersecurity in today's interconnected world. As organizations rely heavily on external entities for critical IT services and products, vulnerabilities within these relationships can expose them to cyberattacks.

By mandating organizations to proactively manage supplier and third-party risks, the NIS2 Directive aims to strengthen the overall cybersecurity posture of the EU's digital infrastructure. This approach helps organizations protect themselves from evolving cyber threats and maintain the integrity of their critical systems.

NIS2 articles:

- Article 14(3)(d): Organizations must identify and assess the risks posed by their suppliers and third parties.
- Article 16(6): Organizations must notify their suppliers and third parties of any cybersecurity incidents that could affect them.
- Article 18(2): Organizations must share information about cybersecurity risks with their suppliers and third parties.
- Annex II: This annex provides guidance on how to manage supplier and third-party risk effectively.

The NIS2 Directive represents a significant step forward in the EU's efforts to enhance cybersecurity across its member states. By addressing supplier and third-party risk management, the directive helps organizations safeguard themselves from emerging cyber threats and maintain a robust security posture.

Proofpoint Supplier Threat Protection and Proofpoint ITDR directly address the supplier and third-party risk management requirements outlined in the EU NIS2 Directive. These solutions provide organizations with comprehensive tools to identify, assess, and mitigate cybersecurity risks originating from their supply chains and third-party vendors.

Proofpoint Supplier Threat Protection

Supplier Risk Assessment: Identifies and assesses the cybersecurity risks posed by suppliers and third parties, analysing their email security posture and potential vulnerabilities.

Malicious Email Detection: Detects and blocks malicious emails originating from compromised supplier accounts, preventing phishing attacks, malware distribution, and business email compromise (BEC) scams.

Threat Intelligence Sharing: Shares threat intelligence with suppliers and third parties, enabling them to take proactive measures to protect their systems and prevent further attacks.

Proofpoint ITDR

Identity Threat Detection: Detects and responds to identity-based threats, including compromised credentials, lateral movement, and privilege escalation attempts.

Continuous Vulnerability Discovery: Continuously scans for vulnerabilities in identity systems, including Active Directory, cloud services, and endpoints.

Deception Technology: Employs deception techniques to mislead and trap attackers, providing early warning of intrusions and preventing further damage.

By implementing Proofpoint Supplier Threat Protection and Proofpoint ITDR, organizations can effectively comply with the NIS2 Directive's requirements for supplier and third-party risk management. These solutions help organizations protect their critical assets, detect and respond to cybersecurity incidents, and improve their overall cybersecurity posture.

NIS2 mapping (Supplier/Third-party Risks)

- Article 14(3)(d): Proofpoint Supplier Threat Protection and Proofpoint ITDR enable organizations to identify and assess supplier and third-party risks effectively.
- Article 16(6): These solutions provide timely notifications of cybersecurity incidents involving compromised supplier accounts or identity-based threats.
- Article 18(2): Proofpoint Supplier Threat Protection facilitates threat intelligence sharing with suppliers and third parties to enhance collective cybersecurity.

Annex II: Both solutions align with the guidance provided in Annex II for managing supplier and third-party risk.

In conclusion, Proofpoint Supplier Threat Protection and Proofpoint ITDR are valuable tools for organizations seeking to comply with the EU NIS2 Directive's requirements for supplier and third-party risk management. These solutions help organizations safeguard their critical assets, strengthen their cybersecurity posture, and protect themselves from evolving cyber threats.

Addressing Email-Borne Threats

Proofpoint Advanced Email Protection aligns with the EU NIS2 Directive's requirements for email security and incident prevention. It provides comprehensive protection against a wide range of email-borne threats, including phishing attacks, malware, and ransomware, helping organizations comply with the directive's mandates for cybersecurity risk management and incident response.

Key Features and Benefits

- Advanced Threat Protection: Leverages multi-layered detection techniques, including sandboxing, machine learning, and reputation analysis, to identify and block malicious emails before they reach users' inboxes.

- Zero-Day Protection: Protects against unknown and emerging threats with advanced threat intelligence and heuristic analysis, preventing zero-day attacks and targeted campaigns.

- URL Defence: Protects against malicious links embedded in emails, preventing users from accessing phishing sites, malware distribution points, and other harmful destinations.

- Impersonation Protection: Detects and blocks email impersonation attempts, including business email compromise (BEC) scams and spear-phishing attacks, safeguarding sensitive information and financial assets.

NIS2 mapping (Addressing Email-Borne Threats)

- Article 14(1): Proofpoint Advanced Email Protection supports the implementation of appropriate technical and organizational measures to manage cybersecurity risks, specifically addressing email-borne threats.

- Article 16(1): The solution enables organizations to detect and report cybersecurity incidents related to email promptly and effectively, minimizing the impact on critical systems and data.

- Article 16(2): Proofpoint Advanced Email Protection contributes to the prevention of cybersecurity incidents by blocking malicious emails and preventing attacks from reaching users' inboxes.

- Article 18(1): The solution facilitates information sharing regarding email-borne threats, enabling organizations to collaborate and strengthen their collective cybersecurity posture.

In conclusion, Proofpoint Advanced Email Protection aligns with the EU NIS2 Directive's requirements for email security and incident prevention. It helps organizations protect their critical assets, comply with the directive's mandates, and strengthen their overall cybersecurity posture.

Incident Management

Proofpoint TRAP and Proofpoint CLEAR align with the EU NIS2 Directive's requirements for incident management and threat mitigation. These solutions enable organizations to effectively detect, analyse, and respond to cybersecurity incidents, minimizing the impact on their critical systems and data.

Proofpoint Threat Response Auto-Pull (TRAP)

Threat Response Auto-Pull: Automatically quarantines or deletes malicious emails identified through Proofpoint's threat intelligence and analysis capabilities.

Post-Delivery Analysis: Analyses emails after delivery to detect and remediate threats that may have bypassed initial security filters.

Out-of-Band Email Management: Leverages CSV files and Proofpoint SmartSearch to identify and remediate threats based on specific criteria.

Proofpoint Closed-Loop Email Analysis and Response (CLEAR)

End-User Reporting: Empowers employees to report suspicious emails with a single click, enhancing incident detection and response.

Automatic Email Prioritization: Prioritizes reported emails based on threat intelligence, reducing noise and enabling security teams to focus on critical incidents.

Automated Remediation: Automatically quarantines or deletes malicious emails, preventing further exposure and limiting the impact of attacks.

By implementing Proofpoint TRAP and Proofpoint CLEAR, organizations can effectively comply with the NIS2 Directive's requirements for incident management and threat mitigation. These solutions help organizations protect their critical assets, minimize the impact of cybersecurity incidents, and improve their overall cybersecurity posture.

NIS2 mapping (Incident Management)

- Article 14(2): Proofpoint TRAP and Proofpoint CLEAR support the implementation of appropriate technical and organizational measures to manage cybersecurity risks.
- Article 16(1): These solutions enable organizations to detect and report cybersecurity incidents promptly and effectively.
- Article 16(3): Proofpoint TRAP and Proofpoint CLEAR facilitate the analysis and mitigation of cybersecurity incidents, minimizing their impact.
- Article 16(4): These solutions contribute to the documentation and reporting of cybersecurity incidents, enabling continuous improvement in incident response.

In conclusion, Proofpoint TRAP and Proofpoint CLEAR align with the EU NIS2 Directive's requirements for incident management and threat mitigation. These solutions help organizations strengthen their cybersecurity posture, effectively respond to cybersecurity incidents, and protect their critical assets from evolving cyber threats.

Domain Abuse

Proofpoint Email Fraud Defence (EFD), which includes DMARC (Domain-based Message Authentication, Reporting, and Conformance) capabilities, aligns with the EU NIS2 Directive's requirements for email security and incident prevention. It helps organizations protect their email domains from spoofing and phishing attacks, ensuring the integrity and authenticity of their email communications.

Key Features and Benefits:

- DMARC Enforcement: Enforces DMARC policies to prevent unauthorized use of an organization's email domain, reducing the risk of impersonation attacks and phishing campaigns.

- Granular Reporting: Provides detailed reporting on email authentication results, enabling organizations to identify and remediate potential vulnerabilities in their email infrastructure.

- Threat Intelligence Integration: Integrates with Proofpoint's threat intelligence to identify and block known malicious actors and techniques targeting email domains.

- Brand Protection: Protects an organization's brand reputation by preventing the distribution of fraudulent emails that could damage customer trust and impact business operations.

NIS2 mapping (Domain Abuse)

- Article 14(1): Proofpoint EFD supports the implementation of appropriate technical and organizational measures to manage cybersecurity risks, specifically addressing email domain spoofing and phishing attacks.
- Article 16(1): The solution enables organizations to detect and report cybersecurity incidents related to email domain abuse promptly and effectively, minimizing the impact on brand reputation and customer trust.
- Article 16(2): Proofpoint EFD contributes to the prevention of cybersecurity incidents by enforcing DMARC policies and blocking unauthorized use of email domains.
- Article 18(1): The solution facilitates information sharing regarding email domain spoofing and phishing attacks, enabling organizations to collaborate and strengthen their collective cybersecurity posture.

In conclusion, Proofpoint EFD aligns with the EU NIS2 Directive's requirements for email security and incident prevention. It helps organizations protect their email domains, comply with the directive's mandates, and strengthen their overall cybersecurity posture.

Security Awareness

Proofpoint Security Awareness Training (PSAT) aligns with the EU NIS2 Directive's requirements for security awareness and training. It provides comprehensive training for employees to recognize and avoid cybersecurity threats, helping organizations comply with the directive's mandates for human-centric cybersecurity and risk mitigation.

Key Features and Benefits:

- Personalized Training: Delivers tailored training content based on individual user roles and risk profiles, ensuring relevant and effective education for all employees.
- Simulated Phishing Attacks: Conducts simulated phishing campaigns to test employees' ability to identify and report phishing emails, raising awareness and reducing susceptibility to real-world attacks.
- Threat Intelligence Integration: Integrates with Proofpoint's threat intelligence to incorporate the latest attack techniques and trends into training modules, keeping employees informed of evolving threats.
- Measurable Results: Provides detailed reporting and analytics to track employee training progress, identify areas for improvement, and demonstrate compliance with regulatory requirements.

NIS2 mapping (Security Awareness)

- Article 14(4): Proofpoint PSAT supports the implementation of appropriate technical and organizational measures to raise awareness of cybersecurity risks and educate employees on how to mitigate them.
- Article 16(5): The solution contributes to the identification and remediation of vulnerabilities related to human error and lack of cybersecurity awareness, reducing the likelihood of successful cyberattacks.
- Article 18(3): Proofpoint PSAT facilitates information sharing regarding cybersecurity awareness best practices, enabling organizations to collaborate and strengthen their collective cybersecurity culture.

In conclusion, Proofpoint PSAT aligns with the EU NIS2 Directive's requirements for security awareness and training. It helps organizations educate their employees, reduce their susceptibility to cyberattacks, and comply with the directive's mandates for human-centric cybersecurity.

Safeguarding Sensitive Information

Proofpoint SIGMA aligns with the EU NIS2 Directive's requirements for data protection and data loss prevention (DLP). It provides comprehensive protection for sensitive data, preventing unauthorized access, disclosure, or destruction, helping organizations comply with the directive's mandates for data security and incident response.

Key Features and Benefits:

- Content-Aware Protection: Identifies and protects sensitive data across various formats, including text, images, and code, preventing data leakage and ensuring compliance with data privacy regulations.
- User Behaviour Analytics: Monitors user behaviour to detect anomalous activities that could indicate data exfiltration attempts, insider threats, or accidental data loss.
- Threat Intelligence: Integrates with Proofpoint's threat intelligence to identify and block known malicious actors and techniques targeting sensitive data.
- Cloud Data Protection: Protects sensitive data stored in cloud environments, including SaaS applications, cloud storage, and collaboration platforms.

NIS2 mapping (Safeguarding Sensitive Information)

- Article 28(1): Proofpoint SIGMA supports the implementation of appropriate technical and organizational measures to protect personal data, safeguarding sensitive information from unauthorized access or disclosure.
- Article 16(1): The solution enables organizations to detect and report cybersecurity incidents related to data loss promptly and effectively, minimizing the impact on critical data assets.
- Article 16(2): Proofpoint SIGMA contributes to the prevention of cybersecurity incidents by blocking unauthorized data transfers and preventing data loss from occurring.
- Article 18(1): The solution facilitates information sharing regarding data breaches and data loss incidents, enabling organizations to collaborate and strengthen their collective data protection practices.

In conclusion, Proofpoint SIGMA aligns with the EU NIS2 Directive's requirements for data protection and data loss prevention. It helps organizations protect their sensitive data, comply with the directive's mandates, and strengthen their overall data security posture.

Conclusion

Proofpoint's solutions—AEGIS, ITDR, and SIGMA—exemplify a tailored alignment with the specific Articles within the EU NIS2 Directive. This alignment not only underscores the capacity of Proofpoint solutions to bolster cybersecurity but also illuminates the pathway towards seamless regulatory compliance. As enterprises navigate the complex regulatory landscape, the synergy between Proofpoint solutions and the NIS2 directive emerges as a beacon of resilience, ensuring both cybersecurity fortification and regulatory adherence coalesce into a robust security framework for the digital age.