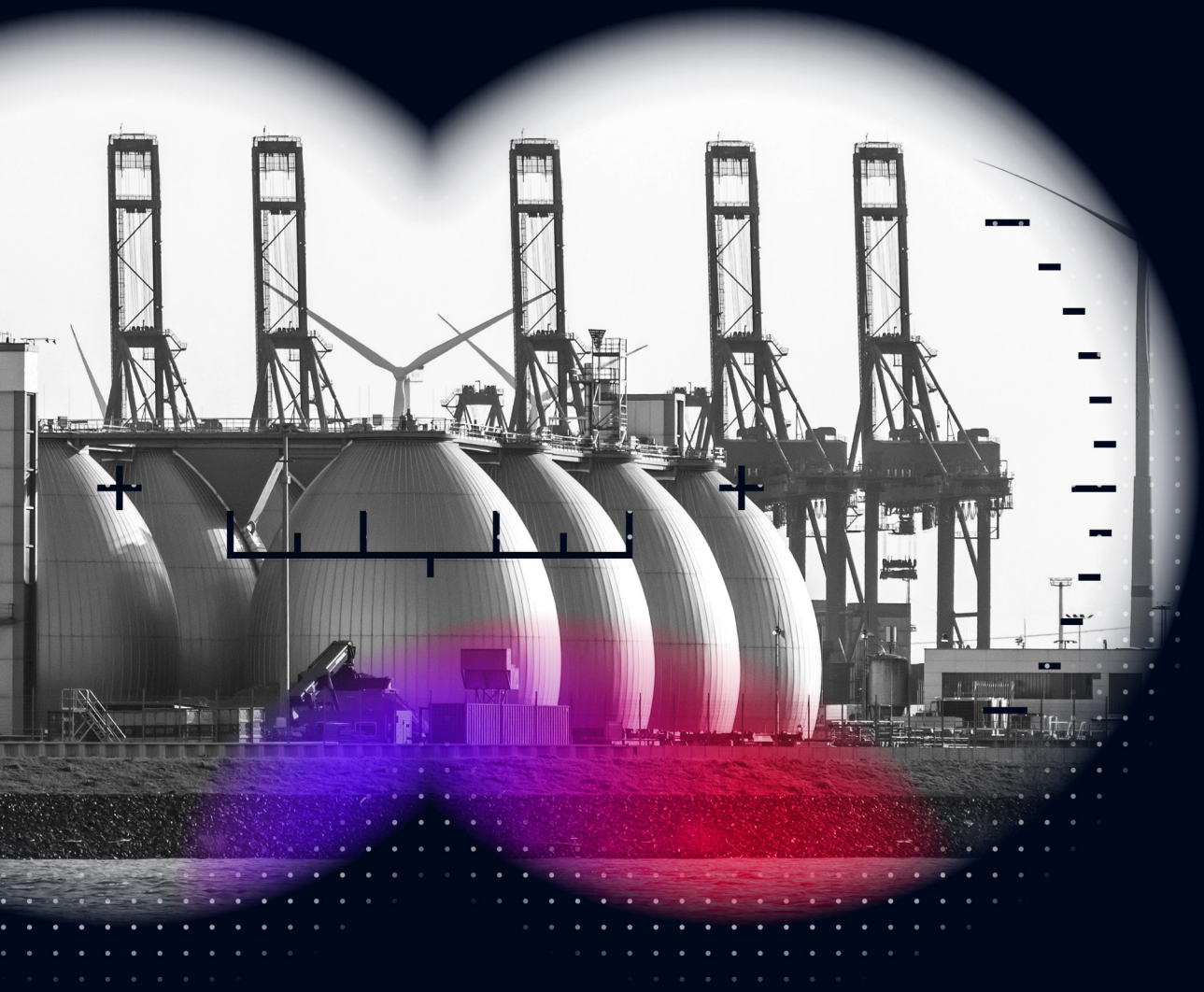

POINT OF VIEW

INTEL 471'S THREAT INTELLIGENCE FOR NIS2-READY CRITICAL INFRASTRUCTURE

INTEL471

Introduction

National implementations of the European Union's NIS2 Directive (EU) 2022/2555 must be enacted by October 18, 2024. These laws have dramatic implications for how tens of thousands of mid-sized and large "important" and "essential" operators of critical services manage cyber risks to lift the resilience of critical infrastructure across Europe. The need for timely, relevant, and accurate cyber threat intelligence (CTI) has never been greater.

The Center for Cybersecurity Belgium (CCB) describes NIS2 as "NIS1 on steroids," referring to the 2016 Network and Information Systems Directive (NIS1). NIS2 is bigger in scope, obligations, supervision, reporting, sanctions, and reach.

Most mature CTI practices are already developing Priority Intelligence Requirements (PIRs) for NIS2, according to the 2024 SANS CTI Survey: Managing the Evolving Threat Landscape.

Liability, awareness, reporting

NIS2 comes into force as more leaders seek CTI and geopolitical intelligence to help navigate complex global environments. Regional flashpoints, superpower rivalries, and unrelenting ransomware have reshaped the digital threat environment for every sector, demanding intelligence-led cyber risk management for IT, operational technology (OT) environments, and supply chain security.

Under NIS2, entities must implement "proportional" risk management measures to "ensure a level of security of network and information systems appropriate to the risks posed." Senior officers may be held individually liable for cyber risk management measures that they must oversee the implementation of.

To mitigate risk, entities should coordinate with their CTI partner to create reporting that fosters executive-level awareness of cyber risks and enables information sharing with competent authorities without exposing confidential data.

Operationalising CTI to proactively defend and mitigate cyber risks to critical infrastructure can reduce personal liability risks, help prioritise incident handling and vulnerability patching, and improve supply chain security.

Why partner with Intel 471?

Intel 471 partners with the world's largest critical infrastructure organisations, serving as their trusted "eyes and ears" to help their teams close intelligence gaps. It combines open-source intelligence (OSINT), human intelligence (HUMINT), and underground cyber sources to provide unmatched insights into threat actor activity and their evolving tactics, techniques, and procedures (TTPs).

- To enrich PIRs, customers submit Requests for Information (RFI) for our CTI experts to initiate custom research on threats and adversary TTPs.
- The company's Cyber Geopolitical Intelligence arms leaders with forward-looking insights into how hostile states use espionage, information warfare, and malware to disrupt critical infrastructure. It forecasts the most likely scenarios for cyber attacks, how and who they will impact the most, and provides hypothetical scenarios to stress test risk management.
- Customers use 471 Attack Surface Intelligence to continually monitor external digital assets, including cloud resources, for new vulnerabilities and prioritise remediation based on threats.
- The Intel 471 General Intelligence Requirements (GIR) framework — customers use this to map emerging threats to assets for proactive defence, threat hunting, and incident response.
- Customers steer risk management with Intel 471's expert HUMINT sourcing from global teams in Adversary Intelligence, Malware Intelligence, Vulnerability Intelligence, Identity Intelligence, and Fraud & Abuse Intelligence.
- Intel 471 develops custom threat hunt "packs" based on adversary TTPs to help threat hunting teams quickly investigate and identify suspected malicious behaviour in their environment, and close logging visibility gaps in security tools.

NIS2 risk management and incident reporting obligations

Under NIS2, entities must report significant incidents to authorities within ***24 hours*** and state whether it was suspected of being caused by unlawful or malicious actors. Within ***72 hours***, the entity must report an "incident notification" that details the severity and impact of the incident and IOCs. A final report within ***30 days*** requires a detailed description of the incident, including its severity and impact, the type of threat that triggered the incident, and details of mitigation measures.

NIS2 Sanctions

Essential entities can be fined €10 million or 2% of worldwide annual turnover, whichever is higher, for non-compliance with NIS2 risk management and incident reporting. Important entities can be fined €7 million or 1.4% of worldwide annual turnover, whichever is higher. Nations can set higher maximum fines than NIS2. Management faces potential personal liability. Competent authorities can issue binding instructions and order infringing entities to ensure risk-management measures comply with NIS2 or to fulfil the incident reporting obligations in a specified manner and period.

How Intel 471 CTI and threat hunting can help your NIS2 program:

- Anticipate emerging threats
- Understand threat actor objectives, motivations, and targeting
- Run TTP-led threat hunts within minutes, not weeks
- Access up-to-the-minute IOCs and adversary TTPs
- Continuously monitor supply chain risks
- Rapidly report incidents
- Map geopolitical events to cyber risks
- Map threats and exposures to external digital assets
- Develop expertly crafted Priority Intelligence Requirements (PIRs)
- Operationalise CTI for the C-suite, security operations, and tactical teams

Armed with Intel 471's premier CTI, NIS2 stakeholders can evaluate current and forecasted threats while working with our CTI experts to build PIRs that close intelligence gaps and provide visibility of the digital threat landscape.

Mapping NIS2 to CTI and threat hunting

NIS2 REPORTING OBLIGATIONS	HOW CONVERGED CTI AND THREAT HUNTING CAN HELP
Within 24 hours of becoming aware of the significant incident, indicate whether it is due to suspected unlawful or malicious acts or could have a cross-border impact.	• Develop Priority Intelligence Requirements (PIRs), real-time CTI updates, and PIR-driven threat hunting to determine whether an incident was caused by malicious acts. • Cyber Geopolitical Intelligence is essential due to the prevalence of nation-state threats against cross-border critical infrastructure. • Vulnerability Intelligence to prioritise patching critical assets. • Malware Intelligence to track and remove ransomware, info-stealers, and loaders.
Within 72 hours of the incident, provide an incident notification, including its severity and impact, as well as, where available, the indicators of compromise.	• Real-time CTI data to save time and accurately report an initial assessment, share IOCs *and* TTPs, and threat identification, and threat attribution. • Strategic, operational, and tactical CTI to support risk management and incident response. • Real-time vulnerability and malware intelligence to understand severity and impact, and determine remediation and response. • External Attack Surface Management to monitor attack surface exposures, prioritise remediation, and support root cause analysis. • Behavioural threat hunting to discover stealthy threats.
Final report within one month, including: • a detailed description of the incident, including its **severity and impact** • the **type of threat or root cause** that is likely to have triggered the incident • applied and ongoing mitigation measures	• Understand the type of threat and root cause • Use supply chain and third-party monitoring • Vulnerability Intelligence (ongoing mitigation measures) and Malware Intelligence (detections) • Cyber Geopolitical Intelligence for cross-border and regional awareness • Threat Hunting to proactively identify and remove threats in the environment • Threat hunters engage with incident response to perform reactive behavioural threat hunting against an associated actor • Adversary Intelligence for insights into the methodology of top-tier cybercriminals — target selection, assets and tools used, associates, and other enablers

Minimum Risk-Management Measures

NIS2 ARTICLE 21 MINIMUM RISK-MANAGEMENT MEASURES	HOW CONVERGED CTI AND THREAT HUNTING CAN HELP
Develop and document policies on risk analysis and information system security	• Document proactive risk management policy with threat hunting metrics and data to show success hunt metrics and continual improvements • Threat hunting to identify visibility gaps in security logging and tool configurations • Threat hunts establish an organisation's security baseline in order to easily single out atypical behaviour.
Incident handling → "any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident"	• Converged CTI and threat hunting to identify stealthy threats inside the environment • Work with our CTI experts to build PIRs and improve threat hunting • Gain visibility of relevant emerging threats and rapidly activate incident response should an incident occur. • Threat hunting helps find security tool configurations that result in logging failures • Staying ahead of threats with intel about underground activity • Use TTPs to guide threat hunts and find threats that can't be found by conventional signature-based file detection
Business continuity, such as backup management and disaster recovery, and crisis management	• Utilising the CTI Capability Maturity Model security architecture, document and maintain the structure and behaviour of the organisation's cybersecurity architecture, including controls, processes, technologies, and other elements commensurate with the risk to critical infrastructure and organisational objectives
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	• Third-party and supply chain monitoring solutions including Cyber Geopolitical Intelligence, external attack surface management, vulnerability management, breach monitoring • Proactively monitor and mitigate the risk associated with compromised credentials as their credentials hit the marketplace

NIS2 ARTICLE 21 MINIMUM RISK-MANAGEMENT MEASURES	HOW CONVERGED CTI AND THREAT HUNTING CAN HELP
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	• Threat hunting to close gaps in security logging visibility to improve security posture
Basic cyber hygiene practices and cybersecurity training	• Use CTI insights to inform cybersecurity awareness and skills assessment strategies • Direct communications with workforce management leadership to help identify cyber-related skills required for safe and effective operations of the workforce
Human resources security, access control policies, and asset management	• Use CTI to proactively inform Identity and Access Management (IAM) strategies, reduce incident detection times, accelerate remediation, and enable continuous improvements to safeguard critical assets and build resilience against identity-related threats • Implement alerts about leaked or compromised credentials and identities from open and commercial sources • Implement alerts about vulnerabilities impacting identity-related systems that threaten unauthorised access or identity compromise
The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications and secured emergency communication systems within the entity	• Use intelligence from External Attack Surface Management, vulnerability, dark web, breach, and identity domains to inform IAM strategies, reduce incident detection times, accelerate remediation, and enable continuous improvements to safeguard critical assets and build resilience against identity-related threats.

Conclusion

Compliance with NIS2-based laws will require ongoing improvements to risk management measures. This must account for evolving and emerging threats and their potential impact on business continuity and operational resilience.

Intel 471's CTI experts regularly assist organisations in developing intelligence plans that align with stakeholder needs to ensure the organisation can efficiently counter threats and reduce risk. This helps organisations to operationalise CTI to understand their risks, the nature of threats, identify vulnerabilities that impact risk, and perform data-driven risk mitigation.

Organisations of all sizes can leverage CTI to improve NIS2 compliance. For more information on harnessing CTI for NIS2 programs, please contact Intel 471 or join us on an intelligence planning exercise.

About Intel 471

Intel 471 empowers enterprises, government agencies, and other organisations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioural threat hunting solutions. Customers utilise this operationalized intelligence to drive a proactive response to neutralise threats and mitigate risk. Organisations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement and globally dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win. Learn more at intel471.com.