THREATQUOTIENT

EXECUTIVE BRIEF

Enhancing Cyber Resilience: How ThreatQ Aligns with NIS2 Directive Requirements

Safeguarding critical infrastructure against cyber threats has become an important concern for governments and organisations and to address this challenge, the European Union (EU) introduced the NIS2 Directive in January 2023, as a means to bolster the cyber resilience of critical infrastructure. The directive outlines stringent requirements for identifying and mitigating risks, reporting incidents, sharing information, and undergoing supervision. In this executive brief, we'll share how ThreatQ, an industry-leading Threat Intelligence Platform (TIP), addresses the NIS2 Directive's mandates, enhancing cybersecurity for organisations subject to these regulations.

Understanding the NIS2 Directive

The NIS2 Directive requires that organisations responsible for critical infrastructure take comprehensive measures to enhance their cybersecurity. These measures encompass several disciplines including Risk Management, Incident Reporting, Information Sharing, and Supervision.

Discipline	Corresponding Article	Description of Measure	Capability Provided by TIP / SOAR
Risk Management	Article 14	Identifying and assessing vulnerabilities, threats, and impacts to critical infrastructure.	• Identifying and Assessing Risks • Prioritizing Remediation Efforts
Incident Reporting	Article 15	Reporting incidents that significantly impact critical infrastructure.	• Improving Incident Response
Information Sharing	Article 16	Sharing threat intelligence and best practices with other organisations.	• Sharing Threat Intelligence
Supervision	Article 17	Allowing supervisory authorities to monitor the security posture of organisations and address emerging risks.	• Monitoring Security Posture

ThreatQ is an industry-leading security operations platform that combines the capabilities of both a Threat Intelligence Platform (TIP) and Security Orchestration, Automation, and Response (SOAR) platform. Together, these cybersecurity capabilities are well equipped to help organisations address the measures outlined above.

1. Risk Management (Article 14)

Effective risk management is at the core of the NIS2 Directive. A TIP can play a pivotal role in this regard:

Identifying and Assessing Risks
TIPs excel in identifying and assessing risks by providing organisations with real-time threat intelligence. They aggregate data from various sources, including open-source threat feeds, internal sources, and global threat intelligence sharing communities. This rich dataset enables organisations to evaluate vulnerabilities and threats to their critical infrastructure comprehensively.

Prioritising Remediation Efforts
Not all threats are equal in terms of likelihood and impact. Organisations rely on TIPs to help prioritise remediation efforts by offering insights into the severity of different threats. Through the threat intelligence platform, security teams can discern which vulnerabilities demand immediate attention, making risk management more efficient and targeted.

Representative Example
Consider a power grid operator using ThreatQ. The platform collects data on emerging threats to the energy sector, including information on vulnerabilities in critical systems. Using ThreatQ, the operator identifies a high-severity threat that could potentially disrupt energy distribution. With this insight, they can prioritise patching and fortifying the vulnerable systems to mitigate the risk effectively.

2. Incident Reporting (Article 15)

Incident reporting is essential to keep authorities informed of cybersecurity incidents that impact critical infrastructure. Both TIPs and SOAR platforms and Security Orchestration, Automation, and Response platforms streamline the incident reporting process:

Improving Incident Response
A TIP enhances incident response by offering real-time threat intelligence and automating various tasks. When a security incident occurs, the TIP provides analysts with the latest threat information, enabling quicker and more informed decision-making.

A SOAR platform can assist in tasks such as alert investigation, evidence collection, and reporting, ensuring that organisations can report incidents to relevant authorities in a timely and effective manner.

Representative Example
Imagine a telecommunications company using ThreatQ. In the event of a distributed denial-of-service (DDoS) attack targeting their network, ThreatQ immediately identifies the attack vectors and affected systems. Automation within ThreatQ triggers a pre-defined incident response plan, which includes incident documentation and notification to regulatory authorities as required by the NIS2 Directive.

3. Information Sharing (Article 16)

Sharing threat intelligence and best practices is vital for the collective defense against cyber threats. A TIP promotes collaboration:

Sharing Threat Intelligence
A TIP facilitates the sharing of threat intelligence with other organisations, making it easier to stay informed about the latest threats. Security teams can participate in threat-sharing communities and share their own findings. This collective approach strengthens the entire ecosystem's ability to respond to evolving threats effectively.

Representative Example
Picture a financial institution using ThreatQ. The organization participates in a threat intelligence sharing group focused on financial sector threats. When they uncover a new malware strain affecting their systems, ThreatQ enables them to share this intelligence with other member institutions, helping the entire sector fortify their defenses against this specific threat.

4. Supervision (Article 17)

Supervisory authorities play a crucial role in ensuring organisations' compliance with the NIS2 Directive. A TIP supports this aspect as well:

Monitoring Security Posture
Supervisory authorities can utilize a TIP to monitor the security posture of organisations. By integrating with the platform, authorities gain visibility into an organization's threat intelligence, risk assessment, and incident response capabilities. This information helps them identify and address emerging risks to critical infrastructure.

Representative Example
A government agency responsible for overseeing the transportation sector partners with organisations in the sector to monitor their cybersecurity efforts. By integrating ThreatQ, the agency can efficiently assess each organization's readiness to address threats that might disrupt transportation services. They can provide guidance and support based on real-time threat intelligence, enhancing the sector's overall resilience.

Conclusion

The NIS2 Directive presents a comprehensive framework for enhancing the cybersecurity of critical infrastructure. ThreatQ, as an industry-leading threat intelligence platform, is uniquely positioned to help organisations address the directive's requirements effectively.

With ThreatQ, organisations can identify and assess risks, prioritise remediation efforts, improve incident reporting, share threat intelligence, and facilitate supervision by authorities. These capabilities not only enhance cybersecurity but also ensure compliance with the NIS2 Directive, ultimately safeguarding critical infrastructure against cyber threats.

In today's digital landscape, ThreatQ proves itself as a vital tool for organisations and authorities striving to bolster their cyber resilience and uphold the standards set by the NIS2 Directive.

For further information including references from financial institutions partnering with ThreatQuotient, contact us at **www.threatq.com/demo/**

Sales@ThreatQ.com • 703.574.9885