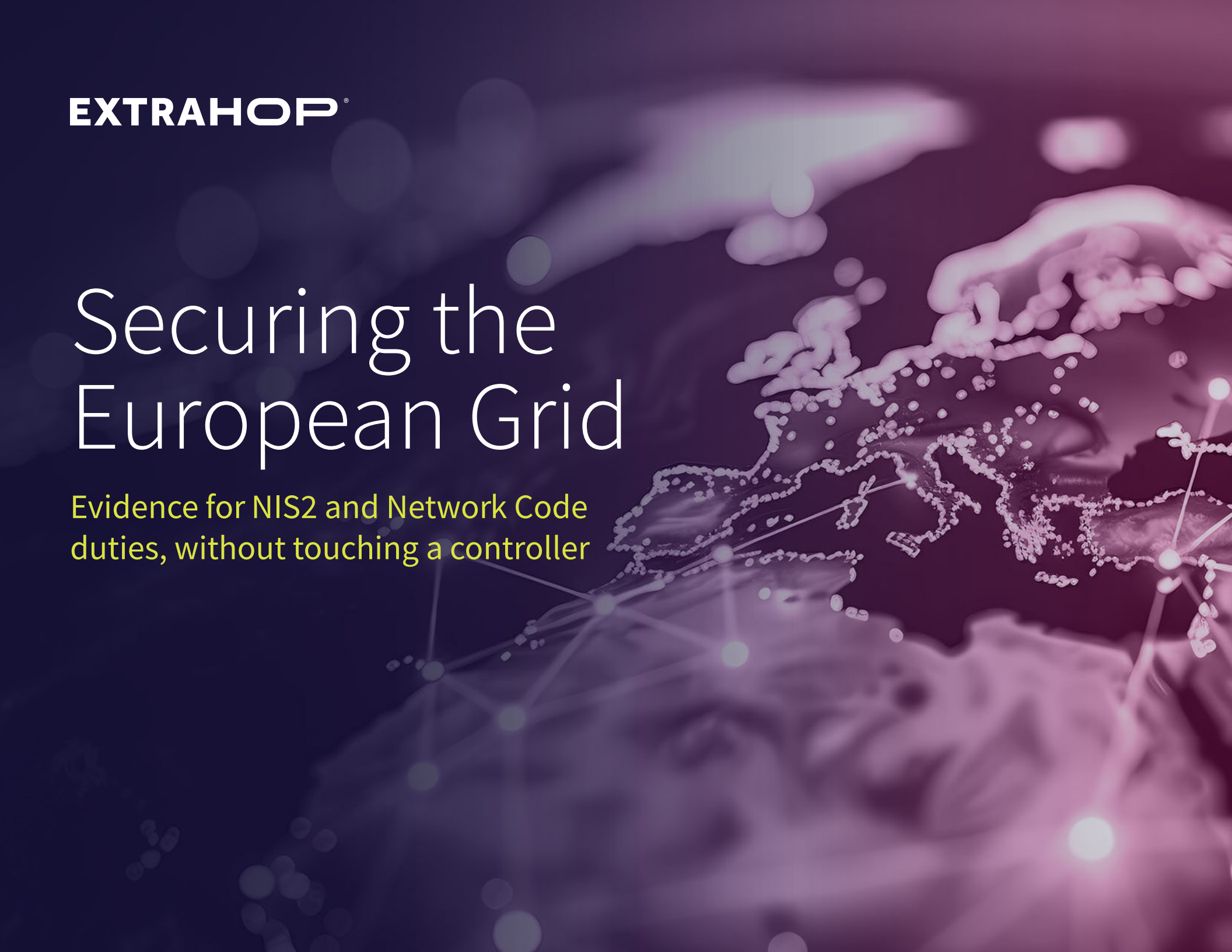
EXTRAHOP

Securing the European Grid

Evidence for NIS2 and Network Code duties, without touching a controller



What's in This eBook

The Regulatory Picture
Two Regimes, One Monitoring Requirement 3

The Size of the Problem
What the Public Record Already Shows 4

Monitoring is an Explicit Obligation
What It Requires, and What Answers It 5

Reporting Runs on a Four-Hour Clock
What It Requires, and What Answers It 6

Availability is a Named Reporting Limb
What It Requires, and What Answers It 7

Continuity Testing Carries a Fixed Correction Window
What It Requires, and What Answers It 8

Scoping Follows Business Process Impact
What It Requires, and What Answers It 9

National Frameworks Carry Their Own Expectations
Where It is Mapped 10

The Solution
One Platform, Two Disciplines 11

Key Capabilities
Nine Capabilities, Tagged by Product 12

Where the Regions Differ
Where the EU Differs from North America 13

Sources, and How to Start
ExtraHop Can Help. 13

The Regulatory Picture

Two Regimes, One Monitoring Requirement

European electricity operators answer to two cybersecurity regimes at once. **NIS2** (Directive (EU) 2022/2555) sets the horizontal baseline. The **Network Code on Cybersecurity** (Commission Delegated Regulation (EU) 2024/1366) adds electricity-specific rules, applies directly in all 27 Member States, and names security monitoring, anomaly detection and intrusion detection as explicit obligations.

The Compliance Clock

Four hours	To report a qualifying cyber-attack	Network Code Art. 38(3) — six times tighter than the NIS2 24-hour early warning, and additive to it.
13 June 2028	Designation backstop	Network Code Art. 24(6) — the date by which every competent authority must have notified its high-impact and critical-impact entities.
€10m or 2%	Of group worldwide turnover	NIS2 Art. 34(4) — the floor on national maximum fines for essential entities, whichever is higher. The Network Code sets no fines of its own.



The Size of the Problem

What the Public Record Already Shows

Attacks Now Reach Operating Plant

CERT Polska disclosed in August 2026 that a second Polish plant lost its steam turbine and water treatment system on 29 December 2025, interrupting cogeneration at a site serving 50,000 residents. A UK generator stayed offline four days in July 2026. Both attacks reached the operating plant, and both left supply intact.

ENISA Names Limited OT Visibility

The NIS360 2026 assessment places electricity in the high-maturity band, then states that “visibility into OT environments is oftentimes limited.” ENISA sets OT asset visibility and monitoring as the sector’s next step.

Agents Cannot Reach These Assets

IEDs, RTUs, protection relays, and substation gateways have no capacity to host software. Monitoring the wire rather than the device is what makes the estate observable at all.

Two Regimes, Cumulatively

NIS2 and the Network Code apply together. Article 38(8) is the only bridge: a NIS2 Article 23 notification carrying the required content also constitutes Network Code reporting.



Obligation 1 of 6

Monitoring is an Explicit Obligation

Article 38(1)(a) sets a minimum capability for entities designated high-impact or critical-impact: security logs that enable anomaly detection, security monitoring, intrusion detection and vulnerability assessment, for every asset inside the defined perimeter.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Security monitoring and anomaly detection NCCS – Art. 38(1)(a)(i)-(ii)	CSOC capability to provide security logs enabling anomaly detection, conduct security monitoring, detect intrusions, and assess vulnerabilities, for all assets within the cybersecurity perimeter.	Agentless monitoring of all network interactions inside the perimeter, with real-time behavioural machine learning and baselining to surface signature-less east-west activity.
Detection and handling of cyber-attacks NCCS – Art. 39(1), 39(3)(c)	Effective processes to identify, classify and respond to attacks affecting cross-border flows, with management procedures based on “the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters.”	Tracks attack progression across the perimeter in real time — lateral movement, credential abuse, protocol anomalies — so teams can classify severity and scope blast radius from observed activity.
Incident handling as a risk-management measure NIS2 – Art. 21(2)(b) with Art. 6(8)	Incident handling is defined as “any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.” Detection is a definitional component.	Provides the detection and analysis layer for converged IT and OT, and the evidence of control efficacy relevant to Art. 21(2)(f).
Supply chain and remote access oversight NCCS Art. 33(2) – NIS2 Art. 21(2)(d)	Supply chain controls covering supplier access to entity assets, zero-trust design and lifecycle monitoring; NIS2 requires security in supplier relationships.	Observes actual supplier and remote-maintenance sessions against baseline, addressing ENISA’s call for governance of remote and supplier access.

Obligation 2 of 6

Reporting Runs on a Four-Hour Clock

Article 38(3) allows four hours from the moment an entity knows an attack is reportable. NIS2 Article 23(4) adds a 24-hour early warning, a 72-hour notification and a one-month final report, and both sequences apply at once.



WHAT IT REQUIRES, AND WHAT ANSWERS IT

Four-hour attack reporting

NCCS – Art. 38(3)-(4)

THE REQUIREMENT

Share information on a reportable cyber-attack with the CSIRT and competent authority without undue delay and no later than four hours of becoming aware it is reportable. An attack is reportable where its criticality is assessed as “high” to “critical.”

HOW REVEALX CONTRIBUTES

One-click investigation from detection to packets supplies the criticality evidence inside the window, without waiting on log aggregation across dispersed sites.

Incident notification cadence

NIS2 – Art. 23(4)

THE REQUIREMENT

Early warning within 24 hours flagging suspected malicious acts and cross-border impact; notification within 72 hours with severity, impact and available indicators of compromise; final report within one month with root cause.

HOW REVEALX CONTRIBUTES

Continuous forensic capture and long-term metadata hold the record each stage needs. Automated Retrospective Detection re-checks stored traffic when a new indicator emerges, so the one-month root-cause report reaches activity that was invisible when it happened.

Obligation 3 of 6

Availability is a Named Reporting Limb

Article 27, point (2) requires an estimate of the risk to confidentiality, integrity and availability for every high-impact and critical-impact process. NIS2 places availability first in its definition of an incident, and that definition carries no intent element.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Availability in the entity risk report NCCS – Art. 27, point (2)	Entities must report, for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity and availability of information and relevant assets, using the risk impact matrix in Article 19(2).	RevealX™ NPM measures availability for the services behind each process, using wire data on latency, throughput and error rates across substation automation, SCADA services, and energy management systems. The operator brings measurement to the availability limb rather than judgement alone.
Availability inside the incident definition NCCS – Art. 39(1), 39(3)(c)	An incident means an event compromising the availability, authenticity, integrity or confidentiality of data or of the services offered by network and information systems. The definition carries no intent element. An incident becomes significant where it has caused or could cause severe operational disruption, which triggers the 24-hour, 72-hour, and one-month reporting sequence.	RevealX NPM detects and characterises service degradation, including degradation with no attacker involved, and quantifies the disruption an operator weighs against the significance threshold. The judgement and the notification remain the operator's.
Which reporting duty applies NIS2 Art. 23(3) – NCCS Art. 38(4)	A severe operational disruption with no attacker involved can be a significant NIS2 incident. Under the Network Code, only cyber-attacks are reportable, and the TSO classification proposal excludes an event whose root cause is assessed as not malicious.	RevealX NDR and RevealX NPM read the same wire data, so a team can establish whether an event was malicious and therefore which of the two reporting duties it has triggered.

Obligation 4 of 6

Continuity Testing Carries a Fixed Correction Window

Article 41(13) to (16) require business continuity plans tested at least every three years, deficiencies corrected within 180 calendar days and re-tested, and the outcome documented.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Annual testing of attack management NCCS – Art. 39(3)(d)	Test overall cyber-attack management procedures at least every year, with at least one scenario affecting cross-border electricity flows directly or indirectly.	Supplies the ground truth to validate exercise outcomes and confirm detection and escalation performed as designed.
Continuity and exercise testing NCCS – Art. 41(13)-(16), 39(3)(d)	Entities must test business continuity plans at least every three years or after major changes to a critical-impact process, and document the outcome. Deficiencies must be corrected within 180 calendar days and re-tested. Entities must separately test cyber-attack management procedures every year. ENISA identifies OT-appropriate, non-disruptive testing as a sector need.	RevealX NPM observes from a tap or SPAN port, so a test runs without polling controllers. RevealX NPM supplies the baseline a test is measured against and records whether a recovery path behaved as designed. The operator performs the test and the remediation.
Continuity as a risk-management measure NIS2 Art. 21(2)(c) – NCCS Art. 41(9)(a)	NIS2 requires business continuity measures, including backup management, disaster recovery and crisis management. The Network Code requires the entity crisis management plan to cover processes depending on the availability, integrity, and reliability of IT services.	RevealX NPM monitors mission-critical SCADA services continuously and surfaces infrastructure degradation before it reaches grid continuity.
Effectiveness of risk-management measures NIS2 – Art. 21(2)(f)	Entities must hold policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	RevealX NPM supplies before-and-after baselines, evidencing that a control performs as intended and that its introduction left grid operations inside normal limits.

Obligation 5 of 6

Scoping Follows Business Process Impact

Article 26(4)(c) has an entity score every business process against the electricity cybersecurity impact index, then derive its assets and perimeter from the processes above the threshold. Article 24(3) lets an authority aggregate that index across a group of entities.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

Asset inventory and perimeter definition

NCCS – Art. 26(4)(c), 26(7)-(8)

THE REQUIREMENT

Register all high-impact and critical-impact assets in an asset inventory, which the competent authority may inspect; define perimeters so access to them can be controlled.

HOW REVEALX CONTRIBUTES

Continuous, real-time discovery and classification of IT and OT assets — including the unmanaged estate agent-based tools miss — with mapped interdependencies.

Verification and audit

NCCS – Art. 31(2)-(3), 27(1)

THE REQUIREMENT

Critical-impact entities must demonstrate compliance across all assets in the critical-impact perimeter via independent third-party audit or a national verification scheme, and report per-control implementation status.

HOW REVEALX CONTRIBUTES

Acts as an independent network observer, evidencing that controls are operating as documented rather than as configured.



Obligation 6 of 6

National Frameworks Carry Their Own Expectations

Germany's BNetzA IT-Sicherheitskataloge, the BDEW/OE/VSE whitepaper used across Germany, Austria, and Switzerland, and the UK NCSC Cyber Assessment Framework each add their own.

WHERE IT IS MAPPED

USE CASE	JURISDICTION	FRAMEWORK	REVEALX	HOW REVEALX CONTRIBUTES
Electricity sector monitoring	European Union	NCCS – Reg. (EU) 2024/1366	NDR	Delivers the Article 38(1)(a) CSOC capability floor agentlessly across high-impact and critical-impact perimeters, and supports the Article 38(3) four-hour reporting clock.
Incident handling and detection	European Union	NIS2 – Dir. (EU) 2022/2555	NDR	Supplies network evidence to assess malicious intent and cross-border impact within 24 hours, indicators of compromise within 72, and root cause within one month.
Availability risk reporting	European Union	NCCS – Art. 27, point (2)	NPM	Measures availability for the services behind each high-impact and critical-impact process, supporting the availability limb of the entity risk assessment report.
Operational resilience and continuity	European Union	NIS2 Art. 21(2)(c) – NCCS Art. 41	NPM	Monitors mission-critical SCADA services continuously and supplies the baseline against which continuity plan testing is measured.
Zone classification assurance	Germany	BNetzA IT-Sicherheitskatalog – EnWG §11(1b), now §§5c–5e	NDR	Evidences that the six-zone classification of energy-installation systems reflects actual behaviour, supporting certified ISMS scope for zones 1–3. The zones rank criticality rather than segment the network.
Supplier and procurement assurance	Germany, Austria, Switzerland	BDEW / OE / VSE – Whitepaper v3.0 (2024)	NDR	Utilities attach the whitepaper to tenders, so suppliers commit contractually to its requirements. RevealX observes whether a delivered system behaves as specified, which matters because no conformity-assessment scheme exists.
Critical process detection	United Kingdom	NCSC CAF v4.0 – Ofgem / DESNZ	NDR	Supports the "Detecting Cyber Security Events" objectives with the automated event discovery and monitoring needed to reach "achieved" status under the Ofgem CAF overlay.

The Solution

One Platform, Two Disciplines

RevealX NDR
Confidentiality and Integrity

ExtraHop RevealX NDR delivers the network intelligence European electricity operators need to evidence internal visibility. RevealX unifies the view across transmission control centres, substation automation, generation plants and distributed renewable sites. Security teams detect sophisticated threats and reconstruct them to the standard the regulations demand.

The network holds the one record an attacker cannot edit. Logs and endpoint agents can be modified or disabled. IEDs, RTUs, and protection relays have no capacity to run agents at all. RevealX monitors the wire instead of the device, so an operator keeps visibility even when a substation gateway or a maintenance laptop is compromised.

Article 39(3)(c) of the Network Code requires cyber-attack management procedures “based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters.” The phrase describes east-west network observation. RevealX applies machine learning to that traffic and flags unauthorised commands in IEC 61850 or DNP3, lateral movement toward the plant floor, and credential abuse against engineering workstations.

RevealX NPM
Availability

Article 27 of the Network Code asks each entity to estimate the risk of a compromise of confidentiality, integrity and availability for every high-impact and critical-impact process. RevealX NDR answers the first two. RevealX NPM answers the third, using the same wire data to measure latency, throughput, and error rates across substation automation, SCADA services, and energy management systems.

Availability carries its own regulatory weight. NIS2 places availability first in its definition of an incident, and the definition carries no intent element. A severe operational disruption can therefore become a significant NIS2 incident with no attacker involved. RevealX NPM characterises the disruption so an operator can judge significance and act inside the Article 23(4) clocks.

One out-of-band sensor produces NDR, NPM, IDS, and packet forensics at once, so a new obligation is covered by the platform already on the wire rather than by another point tool. Security and operations teams work from one ground truth, which matters when a team has four hours to report and must first establish whether an event was malicious at all.

Key Capabilities

Nine Capabilities, Tagged by Product

	CAPABILITY	WHAT IT DOES
RevealX NDR	Security Monitoring Across the Perimeter	RevealX delivers the Article 38(1)(a) capability floor across every asset inside high-impact and critical-impact perimeters. Article 3(16) defines a cybersecurity operation centre by security monitoring, log analysis, and cyber-attack detection.
	Evidence for a Four-Hour Clock	RevealX holds a write-once record of network transactions outside the monitored estate. Teams classify an attack and report inside the Article 38(3) four-hour window, then supply indicators of compromise at 72 hours and root cause at one month under NIS2 Article 23(4).
	Line-Rate Decryption	RevealX analyses modern encrypted traffic, including TLS 1.3 and perfect forward secrecy. Decryption runs at line rate and adds no latency to time-sensitive grid control operations.
RevealX NPM	Availability Evidence for Article 27	RevealX NPM measures availability for the services behind each high-impact process, using over 5,000 wire data metrics covering substation latency, RTU sessions, and application performance.
	Continuity Testing Without Disruption	Article 41(13) requires business continuity plans tested at least every three years, with the outcome documented. RevealX NPM supplies the agentless baseline a test is measured against and records whether a recovery path behaved as designed.
	Root Cause Across SOC and NOC	One click runs from the metric to the record, and one more to the packet. Teams separate a cyber-attack from an operational fault in one investigation, which removes the friction between grid operations and IT network teams during an incident.
RevealX Platform	Agentless OT Discovery and Inventory	RevealX discovers every asset on the network, including PLCs, RTUs, IEDs and substation gateways that cannot run software. The resulting run-time inventory records what is actually communicating, which is what an inspectable Article 26(7) register has to be reconciled against.
	European Protocol Depth	RevealX decodes and decrypts more than 90 protocols at line rate. Native support covers IEC 61850, DNP3, and Modbus. IEC 61850 dominates European substation automation.
	Out-of-Band by Design	RevealX observes traffic from a tap or SPAN port, which meets ENISA's call for OT-appropriate, non-disruptive approaches. Controllers stay untouched: no agents, no active scanning, no polling.

Where the Regions Differ

Where the EU Differs from North America

Three distinctions separate the Network Code from a NERC CIP-015 programme. The Network Code scopes obligations by **business process impact**, using the electricity cybersecurity impact index rather than asset category. It provides for inspection, independent audit and national verification schemes but sets **no administrative fines of its own** — monetary exposure runs through national NIS2 transposition and national energy law. And NIS2 and the Network Code apply **cumulatively**, bridged only by Article 38(8), under which a NIS2 Article 23 notification carrying the required content also constitutes Network Code reporting. Entity-level duties attach on designation, which Article 24(6) requires by 13 June 2028; the first Article 27 report follows 12 months later and must list the implementation status of every selected control.

Sources, and How to Start

ExtraHop Can Help

ExtraHop RevealX surfaces the lateral movement and internal threats legacy tools miss, and produces the evidence a competent authority asks for. Contact us to schedule a demonstration for your high-impact and critical-impact perimeters.

> “ExtraHop gives us a holistic view of any situation and the ability to understand how each event impacts all the connected systems. This is a major advantage for us.”
>
> **OT SECURITY SPECIALIST**
> Central Europe’s Leading Electricity Company

Regulatory Sources

Commission Delegated Regulation (EU) 2024/1366 (Network Code on Cybersecurity), consolidated text of 14 September 2025; Directive (EU) 2022/2555 (NIS2); ENISA NIS360 2026; CERT Polska, Energy Sector Incident Report – 29 December 2025, 30 January 2026, and Follow-Up Report of the December 2025 Energy Sector Incident, 8 August 2026; CERT-EU, Cyber Brief 26-09, 3 September 2026; BNetzA IT-Sicherheitskataloge under EnWG §11(1a)/(1b), continuing transitionally under EnWG §§5c–5e after the German NIS2 act of 6 December 2025; BDEW / Oesterreichs Energie / VSE Whitepaper v3.0, 30 September 2024; NCSC Cyber Assessment Framework v4.0.

Regulatory statements reflect the operative text of the instruments cited as at September 2026. Network Code entity-level obligations attach on designation by the national competent authority. This brief provides information only and does not constitute legal advice. Applicability depends on designation and national transposition.

About ExtraHop

ExtraHop is a leader in real-time network intelligence, empowering organizations with the high-fidelity context they need to power security and IT AI automation, detect risks faster, and respond with confidence.

ExtraHop anchors AI agents with the real-time, ground-truth foundation they need to operate reliably in the SOC and NOC. For security, that means surfacing threats and providing definitive evidence to investigate and respond to novel AI attacks and unsanctioned usage at machine speed. For IT operations, it means identifying and resolving performance issues in seconds to keep critical systems running.

Engineered for unmatched scale, the ExtraHop RevealX platform delivers a complete, unified view of the network for the largest enterprises in the world. Capturing and analyzing network data across data centers, campus, branch, cloud, and AI environments, ExtraHop combines behavioral analysis with deep visibility into encrypted traffic to uncover what others miss.

To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1233A 10.28.26

EXTRAHOP®