

Staying compliant: enhancing DORA compliance and insight with Corelight

corelight

Summary



The Digital Operational Resilience Act (DORA) is an EU regulation that entered into force on 16 January 2023 and has officially applied since 17 January 2025.

The DORA is designed to ensure that financial institutions can withstand, respond to, and recover from severe operational disruptions and cyber threats. Rather than treating IT security purely as a compliance checkbox, DORA establishes a comprehensive mandate to build systemic, year-round digital resilience across the EU financial sector.

- Establishing frameworks to identify and mitigate potential threats

- Requiring incident reporting, regular resilience testing, and third-party risk oversight

- Encouraging the sharing of cyber threat intelligence to improve collective defense

Core Elements of DORA Requirements:

- ICT Risk Management: Establish frameworks and asset visibility to mitigate operational threats.
- Incident Detection & Reporting: Continuously monitor networks and produce high-fidelity evidence for regulators.
- Resilience Testing: Conduct threat-led penetration tests to validate defenses and address vulnerabilities.
- Third-Party Risk Oversight: Actively monitor vendor network connections rather than relying on paperwork.
- Threat Intelligence Sharing: Integrate and share threat data across the industry for collective defense.

Most financial entities have completed their substantive implementation projects and are now focusing on continuous improvement: closing visibility gaps, sharpening detection, and producing the evidence that demonstrates resilience year-round, not just at audit time.

Corelight - solving the technical challenges of DORA

While DORA introduces process, policy, and governance frameworks, Corelight focuses specifically on addressing the core technical elements of the regulation. Organizations can use Corelight offerings to help comply with technical pillars of DORA by enhancing an organization's ability to monitor, detect, and analyze network risk.

Advanced threat detection and incident management

- **Continuous network monitoring:** built on the open-source Zeek framework, Corelight delivers comprehensive visibility into network traffic to detect anomalies and potential threats in real time.
- **Incident detection and response:** deep visibility into network activity identifies malicious behaviors such as lateral movement, data exfiltration, and reconnaissance, the activity endpoint tools often miss or attackers know how to evade.
- **Log enrichment for analysis:** Corelight enriches network logs with contextual data, strengthening root cause analysis.

Digital operational resilience testing

- **Support for Threat-Led Penetration Testing:** Corelight logs, alerts, and insights enable organizations to assess the true resilience of their network and understand how real-world attacks unfold.
- **Resilience Validation:** By providing telemetry during simulated attack scenarios, Corelight helps validate the strength of existing defenses and identify vulnerabilities within network infrastructure, providing data to prove and improve digital resilience.

Streamlined incident evidence

- **Detailed Incident Insights:** Corelight generates detailed, structured data on network events that support reporting mandates. This data includes high-fidelity timestamps, context, and attack vectors to support timely regulatory reporting.

- **Automated Threat Detection:** Corelight's solutions support automated threat intelligence and detection, meaning incidents are identified quickly and accurately, reducing the time needed to evaluate, respond, and report.

ICT third-party service provider risk monitoring

- **Actual Security Insight:** Corelight provides deep visibility and continuous monitoring of network traffic involving vendors who are connected to an organization’s network. This helps organizations gain real-time insight into actual security issues and data flows, ensuring active risk oversight rather than passive reliance on third-party paperwork.

corelight

Asset Management

- **Complete Visibility of the Landscape:** Corelight assists organizations in establishing a complete picture of their network environment by automatically discovering and identifying active assets (systems, hardware, and network components) as they communicate across the infrastructure.

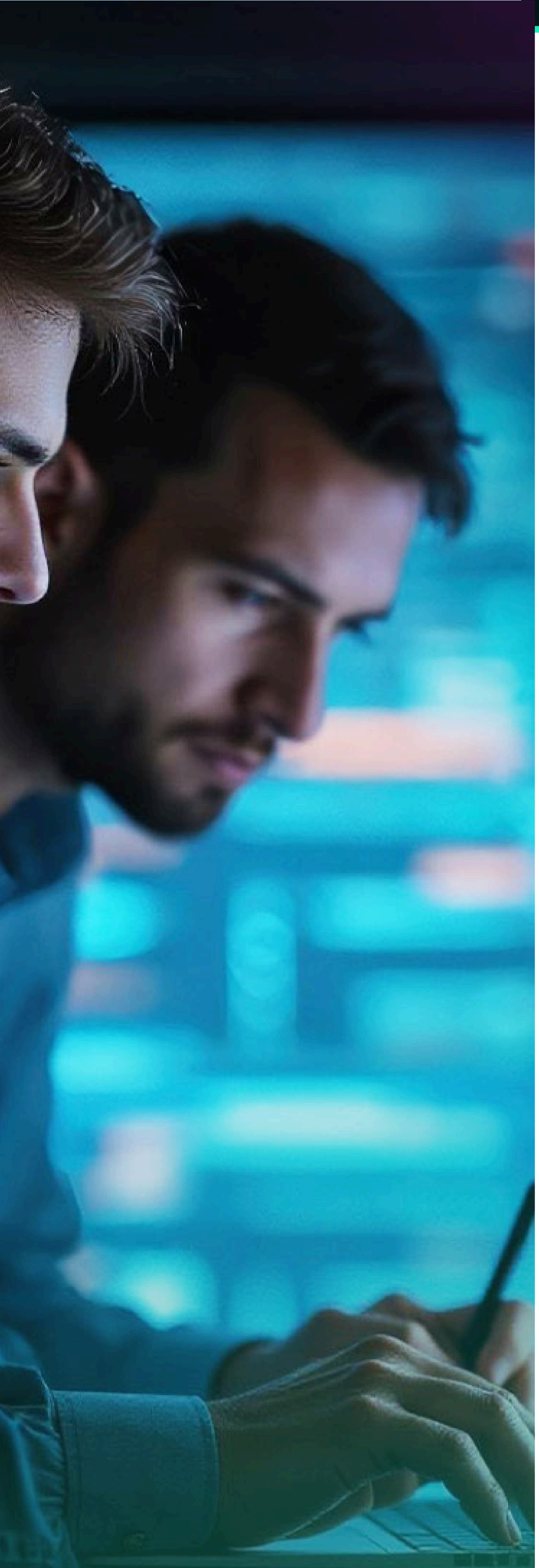
Automated compliance and document support

- **Comprehensive Data Logging:** Corelight's high-fidelity network logs create an unalterable, detailed record of network activities, providing a solid, data-backed basis for compliance documentation.
- **Audit Support:** With structured and organized open data, Corelight simplifies compliance audits, allowing technical teams to definitively demonstrate their security posture and resilience efforts to auditors.

Enhanced treat intelligence and information sharing

- **Integrated Threat Intelligence:** Corelight supports integration with various threat intelligence sources, enhancing the detection of known threats and assisting in tracking significant threats proactively.
- **Customizable Data Sharing:** Corelight can be configured to securely share relevant security information and indicators of compromise (IoCs) with industry peers, contributing to collective defense efforts that align with DORA's information-sharing guidance.





Why Open NDR?

Network detection and response (NDR) platforms built on open source technologies like Zeek and Suricata offer SOCs greater flexibility and choice compared to closed platforms. Moreover, an open NDR platform can act as a security team force multiplier via the power of their global communities, such as the ability to accelerate responses to zero-day exploits via community-driven detection engineering.

Open-source: Enterprise solutions built on open-source software ensure that customers aren't dependent on a single vendor for technical advances, and they're also not beholden to the vendor financially. Customers have a lot more freedom to move off the platform if they're not happy, and they benefit from innovation from the vendor, from other vendors and even individual contributors to the open-source project. It's a more powerful way to develop software.

Open data: Incident response and threat hunting is detective work, and teams depend on access to the evidence. NDR solutions that just give you the "answers" in the form of "the right alerts" are probably not what a sophisticated blue team is looking for. If someone at a crime scene tells you, "The butler did it," but doesn't let you see any fingerprints, cell phone records, or other evidence, you'd be hard pressed to take their word for it.

Open architecture: Your needs change over time, and perhaps your organization has specialized requirements. In that case, the flexibility of an Open NDR platform is critical: You can modify it with third-party packages or with packages your own security team develops to meet your needs.

corelight

Why Corelight?

For over 20 years, the founders of Corelight have been building and improving open-source Zeek software.

Corelight can be a powerful ally for organizations required to have robust risk management and operational resilience by providing visibility, threat detection, incident response, and documentation capabilities. Through Corelight's capabilities in monitoring, testing, and reporting, organizations can improve their compliance with DORA while strengthening their overall cyber resilience.

We have the only Open-NDR platform designed to understand and protecting your network. Corelight users have open access to their metadata and the ability to customize and extend their capabilities—together with a vibrant community.

Corelight's Open Network Detection and Response (NDR) replaces patchwork visibility with a single source of network truth —so you can know if you've been breached, and if control measures have been evaded.

Our complete, coherent, interconnected data gives your team an enduring advantage without disrupting workflows to resolve incidents, perform forensics, and triage alerts. Replace your patchwork of data sources with Corelight's rich, interlinked Zeek data.

Corelight radically simplifies the deployment of Zeek by providing an optimized, high-performance enterprise-grade solution.

Sensors significantly outperform open-source tools and provide rich, actionable network data (Zeek logs) that incident responders and threat hunters need to protect and efficiently respond to network events

The creator and core technologists behind the project carefully engineered a solution to run in the mission-critical environments where they have spent most of their careers. They developed numerous optimizations for higher performance and added dozens of new capabilities that are required by large enterprises and mission agencies.

corelight

To learn more about the Open NDR Platform, request a demo at

http://corelight.com/contact

info@corelight.com | 888-547-9497

All rights reserved. © Copyright 2025 Corelight, Inc.