CyberQuest & DORA Compliance

Operationalising Digital Operational Resilience with an Intelligent SIEM Platform

Executive Summary

DORA isn't just another compliance checklist. It rewrites how financial institutions manage digital risk, demanding both real-time resilience and audit-ready transparency. The regulation imposes strict rules across five pillars, touching everything from ICT risk management to third-party oversight. Non-compliance isn't theoretical - it comes with hefty fines and reputational damage.

Many security teams struggle to keep up. Legacy SIEM platforms drown users in data, fragment workflows, and require multiple add-ons just to meet the basics. Manual reporting, inconsistent visibility, and delayed threat detection are still daily frustrations. For organizations under pressure to prove resilience and control, this is a serious liability.

That's where CyberQuest takes a different approach. With native DORA reporting, forensic-grade data handling, built-in UEBA, and flexible deployment models, it gives compliance teams and SOC analysts the tools they need without friction. No bolt-on modules, no licensing layers - just a purpose-built platform that turns compliance burden into operational insight.

This paper outlines how CyberQuest aligns with DORA's five pillars and why it stands out from legacy SIEM tools like Splunk when resilience, speed, and clarity are non-negotiable.

1. Introduction: DORA in Context

The Digital Operational Resilience Act (DORA) is the EU's sweeping response to growing systemic risks in the financial sector. It goes beyond traditional cybersecurity regulations, pushing institutions to prove they can withstand and recover from severe ICT disruptions - without loss of data, control, or trust.

DORA applies to a wide spectrum of financial entities: banks, insurers, investment firms, payment providers, and their ICT service partners. It formalizes a new standard: digital resilience is no longer an IT concern, it's a board-level obligation.

The regulation is structured around **five foundational pillars:**

1. **ICT Risk Management** - Institutions must implement and maintain governance frameworks, control mechanisms, and tools for continuously identifying, mitigating, and monitoring technology risk.
2. **Incident Reporting** - DORA mandates standardized reporting of significant ICT-related incidents to relevant national and EU authorities. The clock starts ticking the moment an incident is detected.
3. **Digital Operational Resilience Testing** - Firms must regularly test the effectiveness of their digital controls through threat-led penetration testing (TLPT) and scenario-based simulations.
4. **Third-Party Risk Management** - The regulation introduces strict oversight of external ICT providers. Institutions remain fully accountable for risks introduced through outsourcing or vendor reliance.
5. **Information Sharing** - DORA encourages the exchange of threat intelligence and incident information between institutions, regulators, and trusted communities to strengthen collective resilience.

Each pillar is interconnected. For example, poor visibility into third-party environments increases ICT risk, which impairs detection, slows reporting, and undermines resilience testing.

In this high-pressure, real-time environment, success depends on having a security platform that provides actionable insight, unified data pipelines, and fast, clear reporting. That's where CyberQuest makes the difference.

2. Challenges in Meeting DORA Requirements

For many organizations, DORA compliance is not just about aligning with a regulation - it's about navigating a sea of legacy tools, fragmented data, and manual processes that were never designed for real-time resilience.

Key pain points include:

- **Siloed visibility** - Security teams often lack a unified view across IT, cloud, and third-party infrastructure, making risk assessment and incident correlation incomplete.
- **Manual reporting overhead** - DORA's structured reporting format demands speed and precision. Many teams are still compiling reports manually, increasing time-to-submit and risk of errors.
- **Slow detection and noisy alerts** - Existing SIEMs flood analysts with thousands of alerts, many of them false positives. This leads to alert fatigue and delayed response to actual incidents.
- **Complex integration requirements** - Stitching together threat intelligence, vulnerability data, and behavioural analytics usually requires multiple licenses, integrations, or third-party tools.
- **Inflexible architecture** - In highly regulated sectors, deployments often span hybrid or air-gapped environments. Traditional SIEMs struggle with performance and resilience in these conditions.
- **Vendor and third-party blind spots** - DORA puts accountability squarely on the regulated entity, yet visibility into supplier activity is often limited or non-existent.

These challenges are not minor technical hurdles. They represent critical gaps in operational maturity that can directly impact compliance timelines, incident handling, and risk exposure.

What's needed is a platform that does more than store logs. One that streamlines detection, adds intelligence to data, and supports compliance from the moment an event is ingested to the moment a regulator asks for evidence.

CyberQuest addresses these challenges head-on - without adding operational drag or licensing complexity.

3. CyberQuest - A Purpose-Built Platform for DORA Readiness

CyberQuest is more than a SIEM. It's a digital resilience platform engineered from the ground up to meet regulatory demands like DORA - without complexity, bolt-on modules, or endless tuning.

Unlike legacy tools that require extra products for UEBA, threat intelligence, or incident response tracking, CyberQuest comes equipped with these capabilities out of the box. This all-in-one design helps reduce compliance friction, unify security workflows, and improve confidence when it matters most.

Here's how CyberQuest meets DORA's operational demands:

- **Native DORA Reporting**
  - Automatically generates initial, intermediary, and final incident reports in DORA-aligned formats.
  - Reports are pre-populated using case data, forensic logs, and alert timelines, with optional manual input to complete regulatory narratives. The **built-in DORA Journey module** assists teams in aligning posture to compliance checkpoints, and offers a central space to upload and manage DORA documentation within CyberQuest.
- **Forensic-Grade Log Integrity**
  - All logs are encrypted, digitally signed, and archived with non-repudiation in mind, ensuring that every log entry can be trusted, verified, and traced back to its origin without tampering.
  - This ensures audit evidence stands up to regulatory scrutiny, providing clear, verifiable proof of activity even months or years after an incident, regardless of storage medium or infrastructure changes.
- **Built-in UEBA with Risk Scoring**
  - Detects unusual behaviour across users, endpoints, and service accounts using machine learning and statistical baselining.
  - Prioritizes threats based on context, history, and impact - reducing alert noise while increasing detection accuracy.

- **Agentless and Hybrid-Friendly**
  - Works in air-gapped, cloud, and hybrid environments without sacrificing performance.
  - NetAlert technology offers deep, agentless visibility at Layer 2/3 - especially useful for OT, third-party, or restricted systems.
- **Case Management and Timeline Tracking**
  - Every incident generates a timeline with relevant alerts, actions, and artifacts.
  - This single view simplifies forensic and regulatory reconstruction and speeds up compliance reporting.
- **Automation and Response Playbooks**
  - Predefined playbooks execute actions such as account isolation, log enrichment, or alert escalation.
  - Helps reduce mean time to respond (MTTR) and ensure a consistent, auditable response every time.
- **270+ Built-in Connectors**
  - Collects and correlates data from security tools, cloud services, network appliances, ERP, IAM, and more.
  - Removes the need for custom ingestion scripts or external ETL tools.

CyberQuest doesn't just help you tick DORA boxes. It gives you confidence that every detection, decision, and report is based on real context, complete evidence, and a platform built for resilience.

4. Key CyberQuest Features Aligned with DORA Pillars

CyberQuest simplifies DORA readiness by aligning natively with each of the regulation's five pillars. Instead of relying on stitched-together modules or manual workflows, the platform delivers real-time, contextual insights with minimal operational overhead.

Below is a breakdown of how CyberQuest addresses each requirement:

DORA Pillar	CyberQuest Capabilities	What Makes It Unique
1. ICT Risk Management	- Continuous monitoring across IT, OT, and cloud - 270+ prebuilt connectors - Agentless NetAlert for deep network visibility - Real-time asset and identity correlation	- No need for custom integrations - Works in sensitive or air-gapped environments - Unified view across hybrid and third-party systems
2. Incident Reporting	- Built-in generation of initial, intermediary, and final DORA reports - Integrated case timelines with full artifact traceability - Alerts linked to regulatory thresholds	- Instant report generation from incident data - No external tooling needed - Reduces manual overhead and response time
3. Resilience Testing	- Correlation of red-team simulation data - MITRE ATT&CK mapping for adversarial behaviour - Replay and drill-up/down investigation tools	- Built-in support for TLPT and scenario-based test capture - Real-world behaviour analysis to validate defences
4. Third-Party Risk Oversight	- Ingests logs and identity events from suppliers, vendors, and cloud providers - UEBA applies behavioural scoring to third-party users and systems - Supports external SLA tracking and alerting	- Extends visibility without direct control over vendor infra - Detects compromise attempts via third-party vectors - Keeps accountability where DORA places it - with you
5. Information Sharing	- Tag-based alert classification - Exportable threat and indicator data - Role-based access for shared intelligence workflows	- Share context without exposing internal details - Compatible with ISACs, FS-ISAC feeds, and regulatory portals - Ensures traceability of what was shared, and when

5. Use Case: CyberQuest in a Financial Services Environment

In today's financial sector, fraud rarely follows a simple path. It's distributed, multi-vector, and often blends legitimate user behaviour with subtle policy violations. For many institutions, especially at national scale, the tools traditionally used for detection - whether SIEM or dedicated anti-fraud platforms - fall short.

This was exactly the case for a leading banking group facing growing pressure under DORA. Despite having invested in a layered ecosystem of monitoring, alerting, and compliance tools, the institution struggled to identify coordinated fraud campaigns that cut across departments, platforms, and suppliers. Individual tools saw fragments. None saw the full picture.

CyberQuest changed that.

What stood out wasn't just its ability to ingest logs or issue alerts - most platforms can do that. The breakthrough came from **CyberQuest's native support for inline JavaScript**, allowing teams to write their own detection logic, inference models, and enrichment routines directly inside the platform.

This flexibility gave their SOC a way to express real-world fraud logic - not theoretical scenarios, but actual behaviour observed in the wild.

- **Custom Correlation with Business Context**
  Analysts wrote custom logic to track sequences of events across core banking systems, user identities, transaction logs, and even HR data. These rules weren't based on IP addresses or raw log signatures - they were based on **behaviour, timing, and intent**.

- **Live, Multi-Source Enrichment**
  JavaScript rules reached into external databases to pull user roles, recent transactions, known aliases, or supplier metadata - in real time, as part of alert evaluation. What would normally take 3 or 4 disconnected tools was unified into a single, enriched event.

- **Inference and Hidden Pattern Detection**
  CyberQuest allowed the team to define relationships between users and entities that weren't directly linked - such as shared devices, overlapping time windows, or reuse of certain access paths. These invisible threads are where many fraud campaigns operate.

- **DORA-Aligned Response and Reporting**
  As these alerts were generated, CyberQuest automatically populated DORA-aligned reports with forensic timelines, incident metadata, and system impact summaries. No duplication. No delay.

The result:
What was once considered out of reach - not just for SIEMs, but even for **dedicated fraud detection platforms** - became reality. CyberQuest is now actively being used by national-level financial institutions to **track sophisticated fraud schemes in near real-time**, with clarity and speed that have earned it acclaim across the sector.

This is more than compliance. It's **next-generation operational resilience**, and it's redefining what's possible in fraud detection.

6. Compliance Without Complexity - Rethinking the SIEM Model

Traditional security platforms have grown bulky. Over time, they've evolved into sprawling ecosystems that demand constant tuning, expensive add-ons, and deep expertise just to cover the basics of regulatory compliance.

In the context of DORA, this model starts to show cracks.

Institutions find themselves layering separate modules for behaviour analytics, threat intelligence, case management, and reporting - each with its own licensing, learning curve, and maintenance cost. It creates operational drag. And when real pressure hits - during an incident or audit - gaps in coverage or visibility often emerge.

CyberQuest was built differently.

It delivers core compliance and resilience capabilities in a **single, integrated platform**, without forcing teams to bolt on modules or maintain a patchwork of external tools. Everything is built to work together from day one - log ingestion, correlation, enrichment, UEBA, response workflows, and DORA-aligned reporting.

What sets it apart:

- **No paywall for core features**
  UEBA, MITRE ATT&CK mapping, forensic timelines, threat scoring - all are included. There's no second bill for essentials.
- **Deploys anywhere**
  On-prem, hybrid, air-gapped - CyberQuest runs where the data lives, with minimal infrastructure overhead. It doesn't require cloud tethering to work.
- **Low-friction integration**
  With over 270 native connectors, the platform brings together infrastructure telemetry, business data, and third-party signals under one view - no middleware or complex data prep required.
- **Built-in reporting logic**
  DORA, NIS2, ISO 27001 - CyberQuest ships with predefined compliance report formats, reducing audit stress and manual effort.
- **Analyst-first design**
  From alert correlation to timeline reconstruction, everything is optimized for speed, clarity, and evidence. Compliance isn't a separate process - it's built into the way incidents are handled.

This reduces total cost of ownership, accelerates time-to-compliance, and gives teams room to operate - not just react.

7. Conclusion - From Burden to Advantage

DORA raises the bar - not just for compliance, but for how institutions think about operational resilience, real-time visibility, and accountability. It requires more than passive monitoring or fragmented tooling. It demands systems that can detect, respond, explain, and recover - fast.

For many, this feels like a burden. More reporting. More oversight. More complexity.
CyberQuest flips that narrative.

By combining real-time analytics, native compliance workflows, deep behavioural insight, and unmatched deployment flexibility, CyberQuest transforms DORA readiness from a checkbox exercise into a genuine operational advantage.

No separate modules. No manual data stitching. No reactive reporting.

Instead, it offers a platform where every alert, timeline, and report emerge from the same source of truth - ready for audit, ready for action.

For organizations that take resilience seriously, **this isn't just the future - it's the standard.**