THREATQUOTIENT

EXECUTIVE BRIEF

Empowering Financial Institutions to Meet DORA Requirements

The Digital Operational Resilience Act (DORA) is a crucial legislative framework that mandates operational resilience for financial institutions within the European Union. DORA takes hold in January of 2025, and it requires organisations to prepare for and withstand various operational disruptions, including cyberattacks and technology failures.

In this executive brief, we'll outline how ThreatQ, a security operations platform that combines Threat Intelligence Platform (TIP) and Security Orchestration Automation and Response (SOAR) capabilities, plays a pivotal role in helping financial organisations meet the requirements of DORA with a range of cybersecurity and operational resilience capabilities.

DORA Chapters II-VI	Corresponding Articles	ThreatQ Cybersecurity & Operational Resilience Capabilities
II. ICT Risk Management	• Article 6: ICT risk management framework • Article 9: Protection and prevention • Article 10: Detection • Article 11: Response and recovery • Article 13: Learning and evolving • Article 14: Communication	• Risk Assessment and Mitigation
III. ICT Related Incident Reporting	• Article 17: ICT-related Incident Management Process • Article 18: Classification of ICT-related Incidents and Cyber Threats • Article 19: Reporting of Major ICT-related Incidents and Voluntary Notification of Significant Cyber Threats • Article 20: Harmonisation of Reporting Content and Templates • Article 21: Centralisation of Reporting of Major ICT-related Incidents • Article 23: Operational or Security Payment-related Incidents Concerning Credit Institutions, Payment Institutions, Account Information Service Providers, and Electronic Money Institutions	• Incident Detection and Response • Reporting and Compliance • Cybersecurity Incident Reporting

IV. Digital Operational Resilience Testing	Article 24: General Requirements for the Performance of Digital Operational Resilience Testing	Resilience Testing and Scenario Analysis
V. ICT Third-Party Risk	Article 28: General Principles Article 29: Preliminary Assessment of ICT Concentration Risk at Entity Level Article 30: Key Contractual Provisions	Third-Party Risk Management
VI. Information Sharing	Article 45: Information-sharing Arrangements on Cyber Threat Information and Intelligence	Threat Intelligence Sharing and Collaboration Reporting and Compliance

The key DORA topics and articles applying to financial entities are represented in chapters II - VI. These chapters address various aspects or domains within ICT and cyber security, providing a comprehensive digital resiliency framework. The table above maps these 5 chapters to the cyber security and operational resilience principles supported by ThreatQ.

Threat Intelligence Sharing and Collaboration

DORA emphasises the importance of sharing and collaborating on threat intelligence to enhance operational resilience. ThreatQ's TIP capabilities provide the means to aggregate, normalize, and share threat intelligence data from a number of sources through an ecosystem of nearly 400 product and feed integrations available from our online marketplace.

With TAXII Server support ThreatQ users can share STIX-formatted threat intelligence with simplified collection and user management, seamless data access control, and robust integration with the ThreatQ Threat Library.

ThreatQ Community also provides a private cybersecurity community focused on intelligence sharing globally. The ThreatQ Community includes members from a wide range of industries and regions that are committed to sharing threat intelligence as a means of helping to level-up the collective group's threat detection and response capabilities.

ThreatQ Smart Collections are central to addressing DORA requirements. Users can quickly create highly refined data collections using flexible filter controls, and then use these Smart Collections to drive analysis in dashboards, investigations in ThreatQ Investigations, automations in ThreatQ TDR Orchestrator, sharing across a community of users and much more.

Incident Detection and Response

DORA requires organisations to have robust incident detection and response capabilities. ThreatQ TDR Orchestrator is a no-code platform that allows organisations to automate and orchestrate security processes.

ThreatQ TDR Orchestrator uses a data-driven approach for automation and includes integration with Generative AI to augment security professionals and enable them to quickly gather contextual information on elements like indicators, adversaries, malware and many others to optimise threat detection and response.

By assessing the severity and credibility of different IoCs, ThreatQ Investigations helps teams prioritise their response efforts. This ensures that the most critical threats are addressed first, enhancing the overall efficiency of the incident response process.

Resilience Testing and Scenario Analysis

Financial institutions are encouraged to conduct resilience testing and scenario analysis to assess their preparedness. ThreatQ assists in this by enabling the creation of threat intelligence-based scenarios. Organisations can model cyberattacks, test their incident response procedures, and evaluate their overall resilience.

Third-Party Risk Management

DORA underlines the importance of managing third-party risks. ThreatQ allows organisations to assess the operational resilience of their third-party vendors by collecting and analyzing threat intelligence data related to these vendors. For instance, ThreatQ can monitor and assess cyber risks associated with payment processing partners, ensuring a thorough risk management process

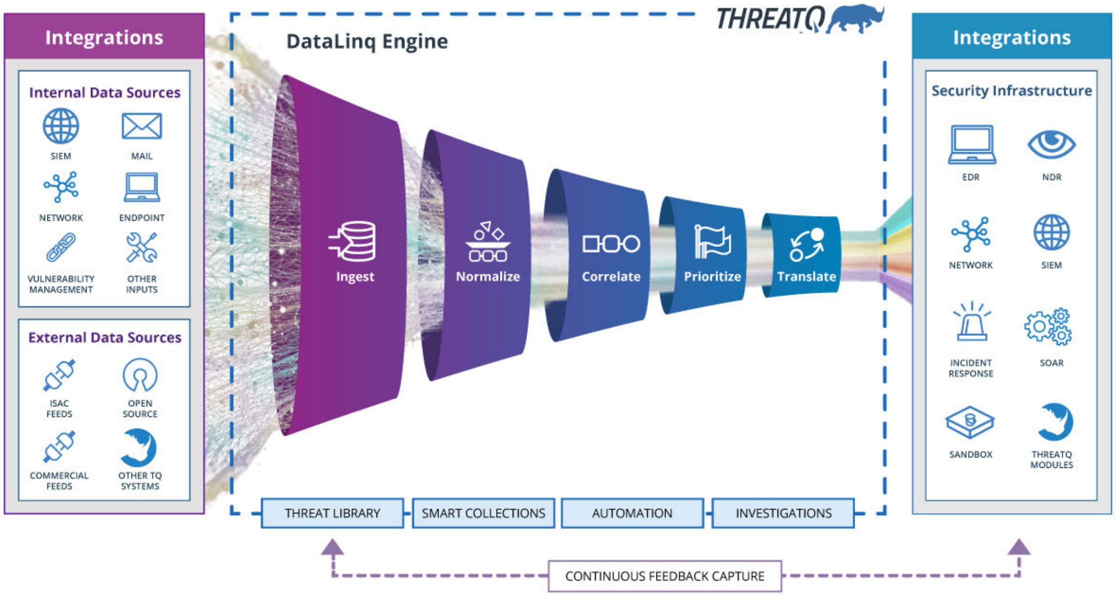
Reporting and Compliance

Compliance with DORA mandates robust reporting capabilities. ThreatQ provides customizable reporting and dashboards, allowing organizations to track and demonstrate their operational resilience efforts. Financial institutions can generate reports that show their compliance with DORA requirements, including details on threat intelligence sharing and incident response activities.

Risk Assessment and Mitigation

ThreatQ helps financial institutions identify and mitigate operational risks. By aggregating and analysing threat intelligence data, organisations can pinpoint vulnerabilities and potential risks.

Organisations are increasingly adopting risk-based vulnerability management. A data-driven approach is essential for organisations to effectively mitigate risks. By leveraging data, organisations can enhance agility, prioritize vulnerabilities accurately, and make informed decisions. The ThreatQ Platform, supported by the DataLinq Engine, provides the necessary tools and capabilities to implement a robust data-driven vulnerability management framework. Adopting this approach enables organisations to reduce the risk of security breaches, protect their assets, and improve overall security posture.



Data Privacy and Protection

DORA underscores the importance of data privacy and protection, particularly for financial institutions. ThreatQ supports this aspect by helping organisations manage and protect sensitive threat intelligence data. It ensures that only authorised personnel have access to specific threat information, thus aiding compliance with data protection regulations.

Cybersecurity Incident Reporting

Timely incident reporting is another key aspect of DORA. ThreatQ provides a centralised repository for incident data, allowing financial institutions to record and report security incidents promptly.

Continuous Improvement

Operational resilience is an ongoing process, and ThreatQ's analytics and reporting capabilities facilitate this directly, while ThreatQ's data-driven approach to security also provides a continuous feedback loop that enables teams to store and use data to improve future analysis. Financial institutions can use the platform to continuously monitor their resilience efforts, make improvements, and adapt to the evolving threat landscape.

Conclusion

ThreatQ's Threat Intelligence Platform is an ideal approach for financial institutions seeking to meet the requirements of the Digital Operational Resilience Act (DORA). It empowers organisations to enhance their operational resilience through threat intelligence sharing, incident detection and response, resilience testing, third-party risk management, reporting and compliance, risk assessment and mitigation, data privacy, incident reporting, and continuous improvement.

With ThreatQ, financial institutions can better prepare for and withstand operational disruptions, ensuring compliance with DORA and fortifying their cybersecurity posture in the ever-evolving threat landscape. It's a powerful and flexible tool that can significantly aid in achieving operational resilience.

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