ORPHEUS

REPORT

ORPHEUS & DORA 2025

ORPHEUS & DORA 2025

Throughout DORA, there is regular referral to and requirement for threat intelligence. The regulation is designed to ensure financial services sector adopts 3rd generation cyber security practices, including getting ahead of threats via intel, testing and collaboration.

DORA is built upon the following 5 key pillars
1. ICT Risk
2. ICT related incident reporting
3. Digital operations resilience testing
4. ICT Third party risk
5. Information sharing

Orpheus can directly support financial services business with each of the 5 pillars.

1. ICT RISK

Development of risk management frameworks

DORA emphasizes the need for financial institutions to have effective risk management frameworks in place. This includes the identification, assessment, and mitigation of cyber risks.

Cyber threat intelligence plays a crucial role in understanding the evolving threat landscape, enabling institutions to proactively identify and assess potential cyber risks.

Orpheus' threat intelligence managed services and our threat-led attack surface management solution allows businesses to see their external attack surface contextualised with the threat landscape.

This means not only can they identify their
external facing infrastructure and digital risks but can see which of those assets and vulnerabilities are most at risk of being exploited, specific to their industry and countries of operation.

These vulnerabilities are given risk scores and a businesses external attack surface is given an overall risk score as well (providing metrics used to set measurement of risk).

2. ICT RELATED INCIDENT REPORTING

Consistency in reporting to help identify and respond to cyber incidents
DORA requires financial institutions to establish robust incident detection and response capabilities. Cyber threat intelligence provides valuable insights into emerging threats, attack vectors, and indicators of compromise (IOCs).

By leveraging this intelligence, institutions can enhance their detection capabilities and respond promptly to cyber incidents, minimizing potential damage.
The Orpheus services and platform are able to identify key threat actors related to a business and share methods of attack, IOC’s and more to enable businesses to stay ahead of impending cyber incidents and reduce them.

3. DIGITAL OPERATIONS RESILIENCE TESTING

DORA mandates regular cybersecurity testing and auditing for financial institutions. Cyber threat intelligence assists in identifying potential vulnerabilities and areas of weakness that need to be addressed.

By incorporating threat intelligence into testing and auditing processes, institutions can simulate real-world cyber threats and evaluate their resilience measures effectively

Article 25 - Testing of ICT tools and systems

- Vulnerability assessments and scans

Orpheus provides a threat-led data layer on top of a standard vulnerability scanner.
This allows teams to not just complete vulnerability scans but to ensure the vulnerability management process is resource efficient by ensuring businesses can prioritise the vulnerabilities which pose the biggest risk to the business.
Additionally, Orpheus, is 1 of only 6 businesses to be accredited by both of the UK’s financial regulators to deliver the threat intelligence elements of intel-led pentesting

4. ICT THIRD-PARTY RISK

The purpose is to ensure a sound monitoring of ICT third-party risk
Article 28-30 Management of ICT Third-Party Risk

Orpheus provides a continuous monitoring of the external attack surface of third parties, contextualised with the threat landscape to present a view of third-party risk profiles and a score which aligns with the likelihood of a vulnerability being exploited.

This solution is also applied to third parties during onboarding due diligence phase as well.

5. INFORMATION & INTELLIGENCE SHARING

Guidelines for sharing information on cyber threats & vulnerabilities.
DORA recognizes the importance of information sharing among financial institutions and regulatory authorities to effectively combat cyber threats

Cyber threat intelligence serves as a key component of such information sharing initiatives.

It enables the timely exchange of threat indicators, attack patterns, and mitigation strategies, fostering a collaborative approach to cyber resilience.

This information is available to be shared with relevant 3rd parties within the platform, highlighting the relevant threat intelligence and the individual businesses exposures to those threats.

DORA & THREAT INTELLIGENCE

Throughout DORA, they regularly touch on the need for getting an understanding of the threat landscape, with regards to a business understanding their own risk profile, how businesses evolve their operational resilience according to changes in their threats and vulnerabilities as well as requiring information & threat intelligence to be shared within their networks.

ABOUT ORPHEUS CYBER

Orpheus is the only UK-government accredited cyber threat intelligence company providing cyber risk rating services. Our powerful and award-winning technologies collect huge volumes of cyber risk data, which we analyse using Machine Learning and our highly skilled team to enable you to stop your cyber risks before they happen.

ORPHEUS

Orpheus Cyber
Orpheus-cyber.com
contact@orpheus-cyber.com