cymulate

SOLUTION BRIEF

Digital Operational Resiliency Act (DORA)

Automatically Test and Validate ICT Security Controls

Increasing Resiliency Against Cyber Attacks

The Digital Operational Resilience Act (DORA) was created by the European Union (EU) to ensure that the banking and financial systems that keep our economies running and the Information and Communication Technologies (ICT) that underly them, are resilient to the risks and digital threats facing the financial sector.

Cyber attacks represent the largest area of risk for financial systems, making the testing and validation of ICT security controls for a financial institution and their third-party service providers a critical component in achieving DORA compliance.

Digital Operational Resiliency Testing

Financial institutions and their third-party providers operating within the EU are now required to develop and integrate a detailed ICT risk management framework and conduct operational resilience testing of critical ICT systems and controls to comply with the DORA regulation.

The Cymulate platform enables DORA compliance by delivering digital operational resilience testing using real-world breach and attack simulations and continuous automated red teaming for:

- **ICT Security Controls**
- **Immediate & Emergent Cyber Threats**
- **Security Operational (SecOps) Response**

Through frequent testing and validation of ICT security controls, immediate threats and operational response, financial institutions and providers can implement a common process of continuous testing and improvement which measures risk and exposure to cyber threats and enables the organization to achieve an acceptable level of risk given their business profile.

Security operations teams can monitor the risk and exposure level for drift based on the latest immediate threats updated daily in the Cymulate platform by our threat research team, as well as when changes are applied to the IT environment and security controls.

The findings and reports generated by the Cymulate platform provide the proof and evidence needed to show the commitment towards continuous improvement and to meet the digital operational resilience testing needs of the DORA regulation.

Solution Benefits

ICT security control validation

Automated testing and validation that ICT security controls are resilient to the latest cyberthreats.

Optimize ICT security controls

Configure and tune ICT security controls and policies to close gaps and weaknesses that could expose financial systems to cyber threats.

Reduce ICT exposure risk

Frequently monitor cyber risk and threat exposure levels to maintain an acceptable level of risk from cyber attacks.

Achieve DORA compliance

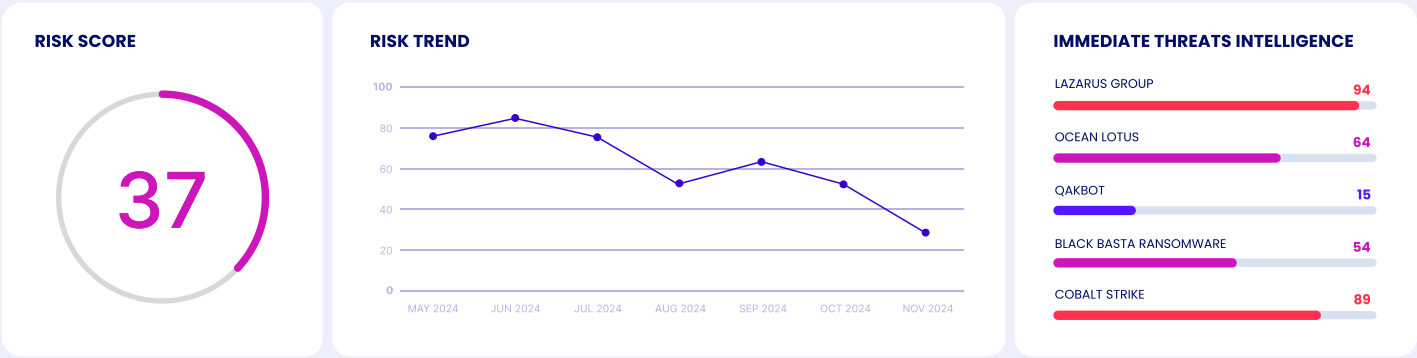
Provide proof and evidence of digital operational resiliency testing of ICT security controls to meet DORA compliance for cyber attacks.

ICT Security Control Testing and Validation

The Cymulate platform delivers production-safe testing and validation of your ICT security controls using a wide range of automated test scenarios and templates. These best practice templates can be scheduled to run on a weekly / monthly basis to perform assessments of key ICT security controls and processes including:

- **Email and Web Gateways**
- **Web Application Firewalls**
- **Antivirus & Endpoint Security**
- **Cloud Workload & Container Security**
- **Lateral Movement & Data Loss Prevention**
- **Advanced Persistent Threat Scenarios**
- **Phishing**

The dashboards and findings from the assessments highlight areas of risk, identifying gaps and weaknesses that could be exploited by threat actors to disrupt financial operations. The detailed findings offer mitigation guidance to configure and tune your ICT security controls to increase resiliency and lower the risk of a cyber breach. The reports provide the proof you need to achieve DORA compliance with evidence of the effectiveness of your ICT security controls to prevent and detect the latest cyber attacks.



Why Choose Cymulate?

Depth of attack simulations

The assessment contains a comprehensive suite of over 7,000 malicious payloads to fully validate the effectiveness of your web application firewalls.

Production safe

The full suite of test cases is completely production-safe with no malicious payload or code execution that could impact your production environment.

Automated testing

The assessment is fully automated, enabling continuous validation and performance optimization of your web application firewall effectiveness every week.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation. For more information, visit www.cymulate.com.

Get a Demo