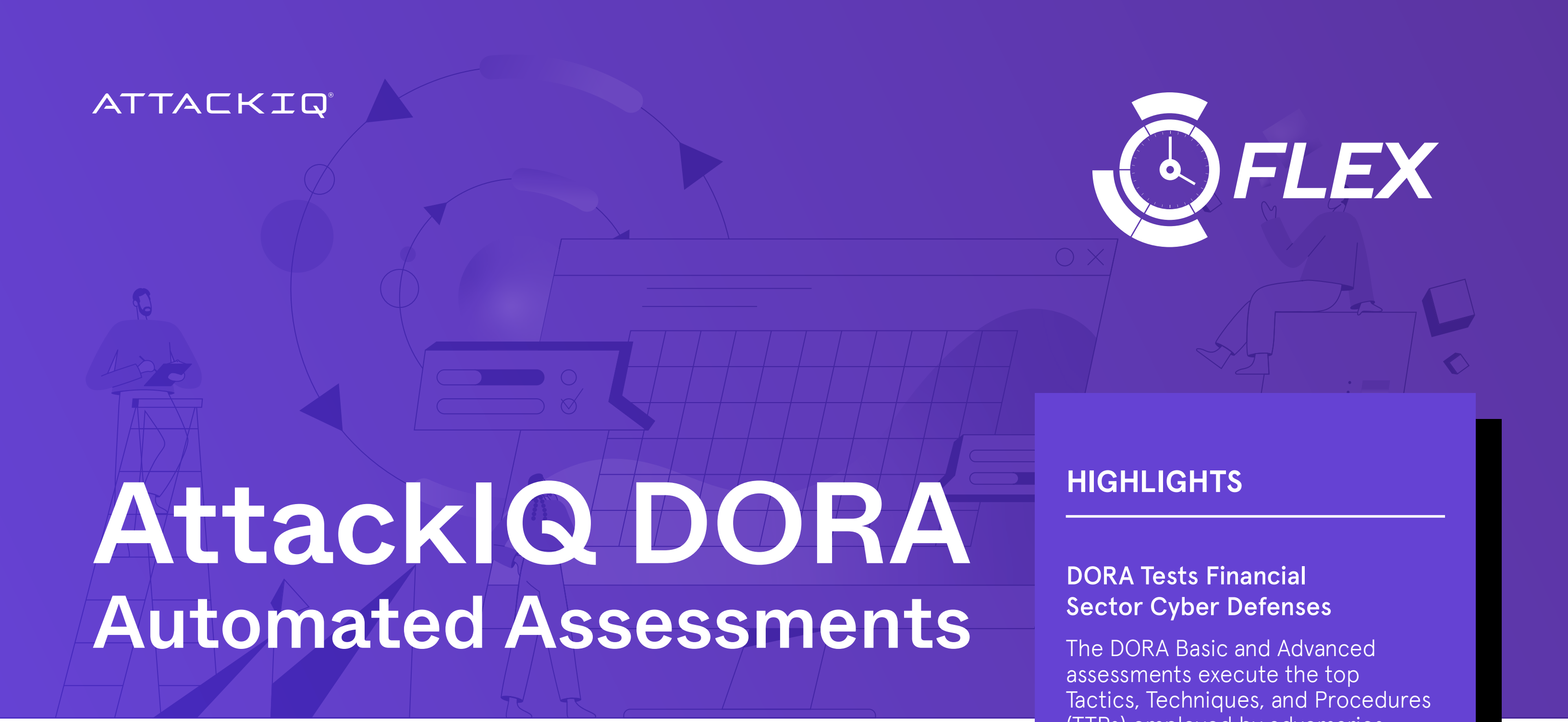


AttackIQ DORA Automated Assessments

The Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) in the European Union is not limited to financial organizations. DORA aims to enhance the digital operational resilience of all entities in the financial sector, but it also impacts a broader range of organizations. Specifically, DORA covers:

1. **Financial entities:** This includes banks, payment service providers, electronic money institutions, investment firms, and insurance companies, among others.
2. **Critical Third-Party Providers:** These are companies that provide ICT (Information and Communication Technology) services to financial entities, such as cloud service providers, data analytics companies, and other digital service providers.

DORA establishes a comprehensive framework to ensure that financial entities can withstand, respond to, and recover from all types of ICT-related disruptions and threats. It imposes requirements on governance, risk management, incident reporting, testing, and information sharing.

In summary, while DORA primarily targets the financial sector, it also extends to third-party providers that offer critical ICT services to financial entities, thereby affecting a wider range of organizations beyond traditional financial institutions.

HIGHLIGHTS

DORA Tests Financial Sector Cyber Defenses

The DORA Basic and Advanced assessments execute the top Tactics, Techniques, and Procedures (TTPs) employed by adversaries known to target financial services organizations. These TTPs reflect our latest intelligence and threat research into the top methods used by EU financial sector adversaries.

Comprehensive Reporting Covers Recommendations and Mitigations

The DORA Assessment Report provides comprehensive recommendations and mitigation strategies forany testing scenario that was not prevented. Recommendations are derived from the extensive knowledge base of the AttackIQ research team, enriched with insights from MITRE ATT&CK standards and industry best practices.

MITRE ATT&CK Aligned

The DORA assessment aligns with MITRE ATT&CK, offering actionable insights in a framework leveraged by cybersecurity practitioners worldwide.

Fully Automated Testing for DORA

The Digital Operational Resilience Act (DORA) legislation within the European Union (EU) is designed to ensure that financial institutions are well-equipped to withstand and recover from cyber threats and operational disruptions. DORA achieves this by setting requirements which include establishing and maintaining an information and communication technology (ICT) risk management framework, reporting and classifying ICT incidents according to a specific taxonomy, conducting regular testing of ICT systems and tools, and managing risks associated with third-party ICT service providers. DORA establishes a clear oversight framework to ensure compliance. Failure to do so can result in various administrative, financial, and criminal penalties.

Threat-Led Penetration Testing (TLPT), MITRE ATT&CK, TIBER-EU, and Breach and Attack Simulation (BAS) platforms are core components that work together to support DORA. DORA has established the requirement for financial institutions to conduct regular TLPT. MITRE ATT&CK provides the blueprint and establishes the comprehensive library of attacker tactics, techniques, and procedures (TTPs) which can be used by TLPT. TIBER-EU, a European framework for simulating cyberattacks, helps define best practices for conducting threat informed red teaming exercises.

Threat-Led Penetration Testing is a DORA Requirement

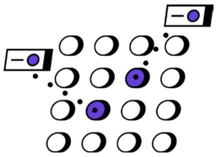
DORA mandates that financial institutions maintain strong "digital resilience" which is the ability to withstand and recover from cyberattacks. One key requirement of DORA is Threat-Led Penetration Testing (TLPT); excerpts of the DORA requirements for TLPT follow:

Article 26.1

Article 26.1 of the regulation explicitly states that Financial Entities shall "provide for advanced testing of ICT tools, systems and processes based on TLPT." Article 26.1 provides extensive guidance on exactly what is required.

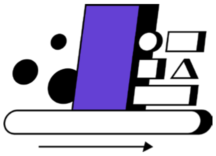
Article 3.17

Article 3.17 of the regulation explicitly states that "threat-led penetration testing (TLPT) means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems"



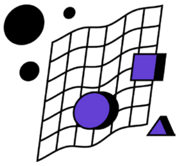
Threat-Led Approach

The regulation emphasizes threat-led penetration testing, meaning testers consider real-world attacker behaviors to design their tests.



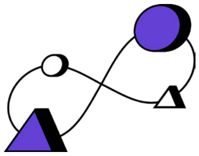
Mandated Testing

DORA mandates annual penetration testing for critical applications and systems, with advanced threat-led testing required every three years.



Critical Focus

Penetration testing needs to cover at least the critical functions and services of a financial entity.



Live Production Systems

DORA specifies that threat-led penetration testing should be performed on live production systems supporting critical functions.

BAS is a Critical Component of TLPT

Breach and Attack Simulation (BAS) is a critical component of TLPT under DORA. Here's how it works:

TLPT focuses on mimicking real-world attacker behavior: DORA emphasizes testing an organization's resilience against actual cyber threats.

Continuous Validation Testing with BAS provides the foundation: AttackIQ Flex, together with our fully automated BAS solution, Ready, continuously emulates attacker tactics, techniques, and procedures (TTPs) documented in MITRE ATT&CK. This allows TLPTs to test specific vulnerabilities relevant to the financial sector.

Pentesting and BAS can work together to derive maximum value. Pentests can be used to identify weaknesses in targeted areas of vulnerability. BAS can exploit those vulnerabilities and much more. Based on the vulnerabilities identified in the pentest, a BAS simulation can be designed to test how an attacker might exploit them and any other related attack vectors.

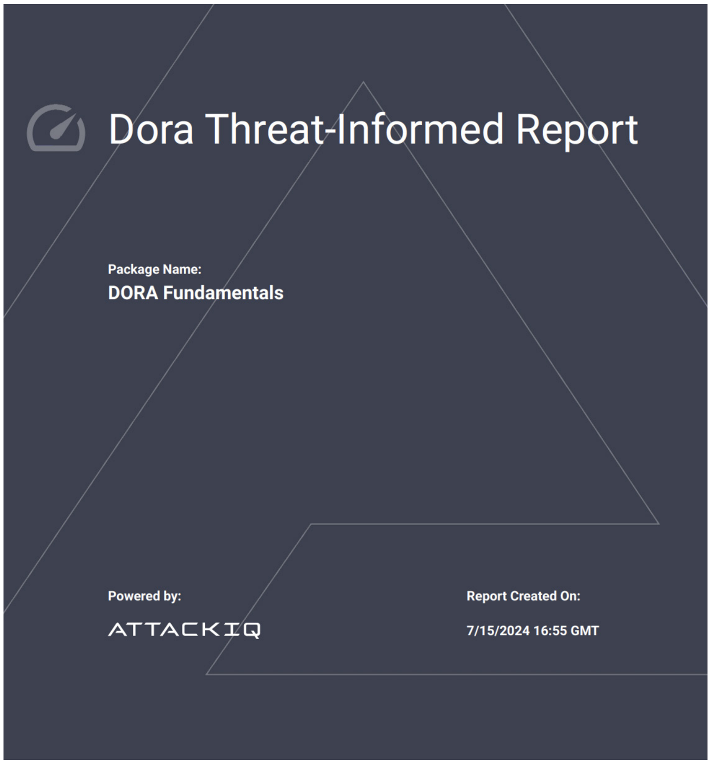
BAS can also rapidly verify if mitigations are working on a continual and ongoing basis. This combined approach provides a more complete picture of an organization's security posture, uncovering both exploitable vulnerabilities and the effectiveness of security controls against real-world attack simulations.

BAS has extensive depth and breadth within testing scenarios. BAS also has reach into many test scenarios that pentests may not cover, due to resource availability, or expense.

DORA emphasizes the importance of TLPT. While both penetration testing and BAS are valuable tools, BAS simulations ensure TLPTs are aligned with the most relevant and current cyber threats faced by financial institutions.

How It Works

1 Select Your Test — 2 Run Your Test — 3 View Your Results — 4 Fix Your Gaps

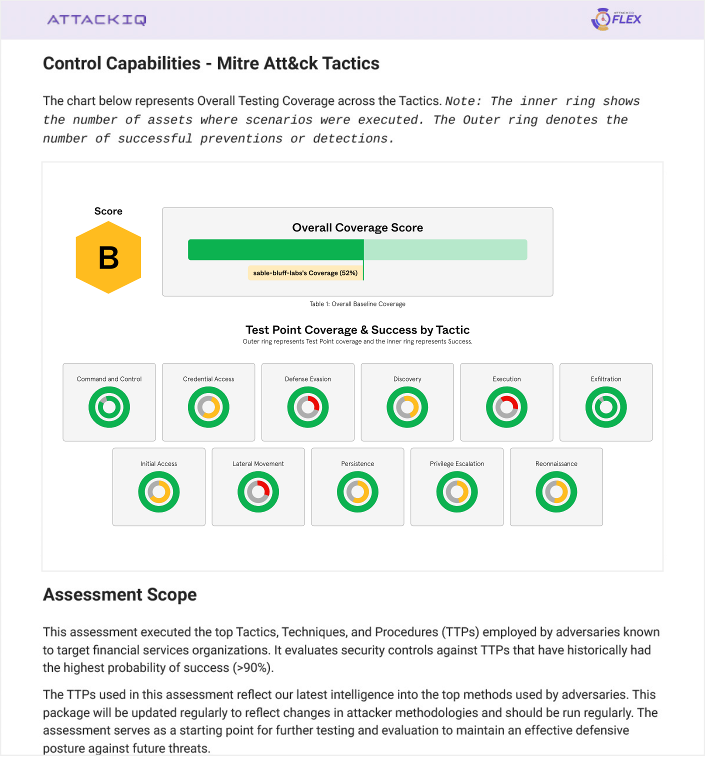


Dora Threat-Informed Report

Package Name:
DORA Fundamentals

Powered by:
ATTACKIQ

Report Created On:
7/15/2024 16:55 GMT



Control Capabilities - Mitre Att&ck Tactics

The chart below represents Overall Testing Coverage across the Tactics. *Note: The inner ring shows the number of assets where scenarios were executed. The Outer ring denotes the number of successful preventions or detections.*

Table 1: Overall Baseline Coverage

Assessment Scope

This assessment executed the top Tactics, Techniques, and Procedures (TTPs) employed by adversaries known to target financial services organizations. It evaluates security controls against TTPs that have historically had the highest probability of success (>90%).

The TTPs used in this assessment reflect our latest intelligence into the top methods used by adversaries. This package will be updated regularly to reflect changes in attacker methodologies and should be run regularly. The assessment serves as a starting point for further testing and evaluation to maintain an effective defensive posture against future threats.

The Business Value of DORA Assessments

Assess EU Financial Sector Threat Actors

Leverage AttackIQ's advanced adversary emulation software which fully emulates cyberattacks and the TTPs employed by real-world adversaries targeting the EU financial sector.

Testing for All EU Financial Institutions

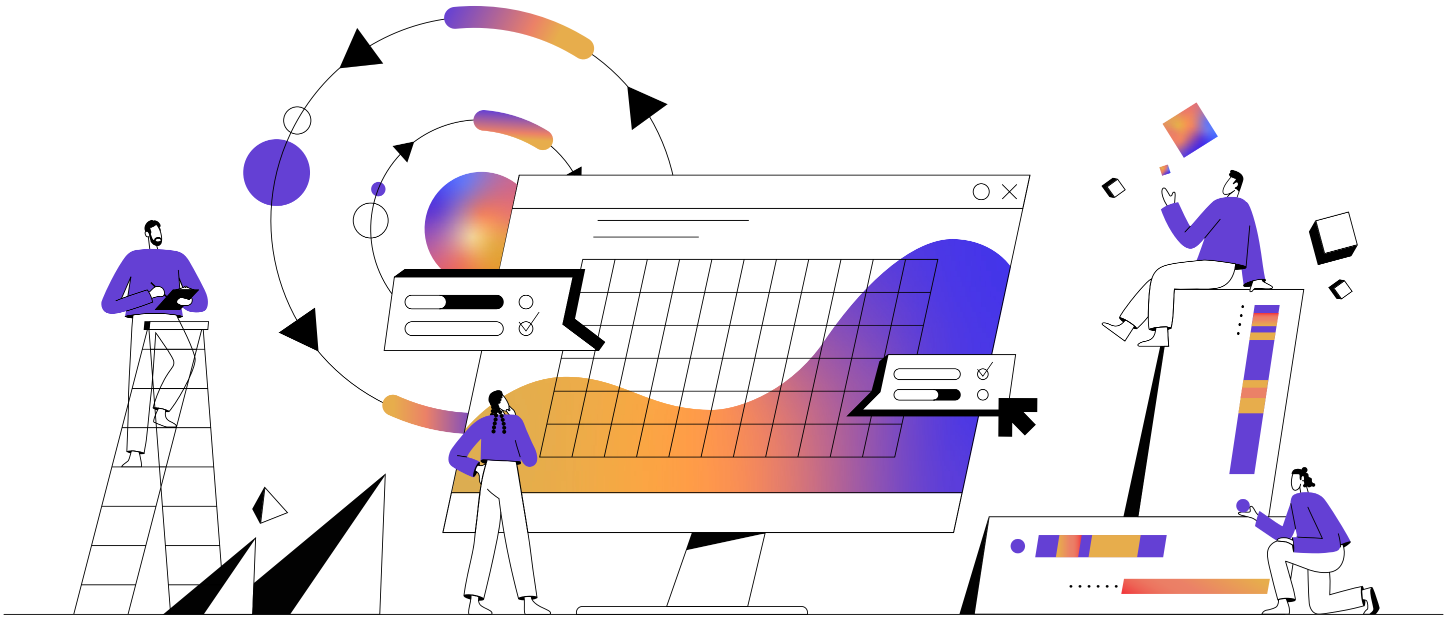
Financial organizations of all types can harden their defenses and align with DORA, ensuring they can interdict threat actors before they can achieve their objectives.

Save Time and Resources

Provide an economical means of validating DORA security controls while balancing the need for expensive and time-consuming manual testing.

Meet DORA Compliance

DORA establishes a clear oversight framework to ensure compliance. Failure to comply with DORA can result in various administrative, financial, and criminal penalties.



ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation (BAS) solutions, built the industry's first BAS Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

For more information visit www.attackiq.com and follow AttackIQ on Twitter, LinkedIn, and YouTube.