SOLUTION BRIEF

Developing Cyber Resilience for Financial Institutions with TIBER-EU

Overview
The financial services industry remains among the most targeted industrial sectors in the world, facing an evolving threat landscape with a wide range of dedicated threat actors.

Regulators and consumers reasonably expect these organizations to effectively protect their data. As they attempt to fulfill this expectation, financial institutions must also fully comply with the various established security-related standards, rules and regulations.

There are several frameworks and regulations that define world-class cyber security standards in the financial sector, but most do not take an active approach to testing how defenses hold up during an actual attack.

The TIBER-EU framework was developed as the first EU-wide guide on how authorities, security providers and financial entities should work together to test and improve cyber resilience of those entities using controlled cyber attacks.

FireEye Mandiant can test your defenses and help improve your security posture by conducting TIBER-EU tests that mimic the tactics, techniques and procedures of real-life attackers, reveal your organization’s strengths and weaknesses and enable you to reach a higher level of cyber maturity.

The TIBER-EU Framework
The Threat Intelligence Based Ethical Red Teaming (TIBER) EU is a framework published by the European Central Bank for delivering “a controlled, bespoke, intelligence-led red team test of entities’ critical live production systems.”

The aims of TIBER-EU are as follows: to improve the protection, detection and response capabilities of entities; to enhance the resilience of the financial sector; and to provide assurance to the authorities about the cyber resilience capabilities of the entities under their responsibility.

TIBER-EU is a common framework across the Eurozone, with national implementations adopted on a voluntary basis by single jurisdictions (e.g., TIBER-NL, TIBER-DK, and TIBER-BE). The framework’s purpose is to provide guidance to critical financial institutions (“entities”) on setting up intelligence-led red team tests to improve protection, detection and response capabilities against sophisticated cyber threats. Entities may include banks, stock exchanges, payment institutions, credit rating agencies and asset management companies.

The overall objective of a TIBER test is to enhance the cyber resilience of tested entities, revealing their strengths and weaknesses before they are exploited by real threat actors.

FireEye Mandiant TIBER Engagements

FireEye Mandiant TIBER engagements use a blend of cyber threat intelligence and red team operations:

- **Threat intelligence:** Includes all actions necessary to fulfill the requirements of the Targeted Threat Intelligence Report (TTIR) for tested entity. The TTIR provides accurate and up to date attack scenarios to ensure that the red team test is aligned to the tested entity’s threat profile.

- **Red teaming:** Consists of a multi-phase, targeted attack against the tested entity and its assets using scenarios derived from the TTIR. After the tests are completed, the red team provider presents its results, which include a high level summary of the engagement and the outcomes, a detailed breakdown of all findings with technical details and techniques used, analysis of root causes and attack path flows and recommendations for both immediate fixes and strategic changes to improve the entity’s security posture.

Mandiant has access to a vast body of threat intelligence collected from our incident response experts responding to thousands of significant breaches across the globe and across industries, with the financial sector as one of the most critical areas.

This victim intelligence is combined with unparalleled adversary intelligence gathered by FireEye Threat Intelligence, machine intelligence gathered through the globally deployed FireEye sensor install base, and campaign intelligence gathered via FireEye’s seven global advanced SOCs which protect hundreds of FireEye Mandiant Managed Defense customers 24x7x365. This results in unmatched, actionable threat intelligence, ensuring that TTIRs reflect threat intelligence on the latest attacker groups, their targets, objectives and tools, tactics and procedures (TTPs).

![Figure 1. How threat intelligence and red teaming fit into TIBER engagements.](image-url)
FireEye has more than 170 intelligence analysts and researchers located in 22 countries, speaking 30+ languages and monitoring many diverse threat actors. We collect between 600,000 and one million malware samples per day for analysis from more than 70 different sources. We currently track more than one million attacker personas and identify approximately one million stolen payment cards per month on the dark web.

FireEye monitors hundreds of threat groups, including over 40 APT threat groups, 10 FIN threat groups, and hundreds of uncategorized (UNC) groups. Comprehensive profiles of these threat groups are built and maintained, and include target industries, attack motivation and TTPs. In many cases, these TTPs are mapped to the MITRE ATT&CK™ framework, providing opportunities to effectively design, test and measure detection and response capabilities using the widely adopted taxonomy of that framework.

The Depth of FireEye Red Teaming

FireEye Mandiant incident responders have been on the frontlines of the world’s most complex breaches since 2004, gaining a deep understanding of both existing and emerging threat actors, as well as their rapidly changing TTPs. By applying knowledge of the latest attacker techniques and toolsets, to red team exercises, we support organizations in their efforts to assess and mature the effectiveness of their cyber resilience capabilities.

Mandiant consultants have heavy representation worldwide, including well-situated senior consultants across the EU. They have worked on critical red team engagements, including the UK CBEST initiative and other critical nation infrastructure (CNI) clients throughout Europe.

Figure 2. Elements of the extensive, multifaceted FireEye intelligence offering.

Figure 3. The Mandiant team tests the client security team’s capabilities against every phase of the attack lifecycle.
Mandiant red team engagements use a systematic, targeted and reproducible methodology, fully mapped to the MITRE ATT&CK framework. Leveraging intelligence from the Generic Threat Landscape Report and the Targeted Threat Intelligence Report, attacker behavior is simulated across each phase to accomplish the agreed upon attack scenarios and objectives.

### Table 1. Example red team objectives.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Task</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funds transfer</td>
<td>Break into the entity’s secure financial services</td>
<td>Take control of client operator workstations and stage a payment transfer message to an outside entity</td>
</tr>
<tr>
<td>PII theft</td>
<td>Access sensitive customer records</td>
<td>Bypass internal security controls and access customer databases or information stores</td>
</tr>
<tr>
<td>Deploy ransomware</td>
<td>Evaluate client susceptibility to wide-scale ransomware attack</td>
<td>Verify internal defenses against ransomware auto-spreading capabilities</td>
</tr>
<tr>
<td>Domain control</td>
<td>Acquire full domain control</td>
<td>Escalate internal privileges and access rights to gain full control of client domains and networks</td>
</tr>
<tr>
<td>Insider threat</td>
<td>Assess client defenses against physical penetration and rogue devices</td>
<td>Deploy rogue device with external communication capabilities and attempt to escalate access</td>
</tr>
</tbody>
</table>

The red team assessment ultimately provides the client with a fact-based risk analysis, and both tactical and strategic recommendations for both immediate and long-term improvements. Post engagement workshops can be tailored to specific client needs and can target board-level executive briefings as well as technical blue-team leader roundtables.

**Sustained, Proven Support for TIBER-EU Initiatives**

The TIBER-EU framework provides guidance to financial entities on how to conduct a threat-intelligence ethical red team engagement, but organizations still need to partner with a competent security firm to conduct these simulations. Industry leading threat intelligence and extensive red team expertise from FireEye Mandiant can help. Our experts regularly conduct red team engagements worldwide, across all industries sectors and government and have ready access to our world leading threat intelligence. Engagements can be tailored to meet your needs, as Mandiant can operate either as a red team provider, a threat intelligence provider, or both.

---

2. Forrester (September 7, 2018). The Forrester New Wave™: External Threat Intelligence Services, Q3 2018