Threat Intelligence-Based Ethical Red teaming in Belgium (TIBER-BE)

Samuel Goret

Technological progress leads to innovative possibilities and capabilities. Although it might enable you to get more things done in a day and simplifies complex tasks for users, the systems and infrastructure themselves are becoming increasingly complex. This added complexity entails all kinds of risks, and risks are where malicious actors see opportunities. The threat of bad actors capitalising on the risks incurred by ever ongoing change is only amplified by the existence of geopolitical tensions, bringing us to intent, goal, purpose or rather motive. If inequality, jealousy and greed are added to that mix, technology becomes a unique, fast and ever evolving playground for cutting-edge, highly adaptive and organised criminals, as well as nation state actors with a different worldview. In addition, there are the so-called "hacktivists" (cyber activists) or disgruntled employees (so called insider threat). Although the final goal of the various kind of actors listed above differs (disruption, financial gain, extortion or political objectives), they have all adopted technology as a new kind of weapon in a new kind of war. One might state that hacking is not a novelty, but the organised aspect of it has evolved at a rapid pace and can now be considered a business model. In contrast to conventional "defensive" security like firewalls, anti-malware tools, detection tools, SOC (Security Operation Centre), etc., offensive security tests the applications, systems and infrastructure from an attacker's point of view (including on-premises tests on physical security systems, like badge/access systems, or help desk staff through manipulative phone calls). This literally means acting as a bad actor and trying your best to get into the network, find the core critical systems and then demonstrate the capability to strike (in our case without really hitting the big red button). "To strike" could mean gaining financial benefit, exfiltrating trade secrets for later use, customer data, user credentials … or just encrypt all systems and cause major disruption for the FMIs or the economic system as a whole. This is the opposite of ethical hacking with its agreed rules of engagement, adherence to laws and high morality.

Fundamental principles of the TIBER-BE framework

Following the earlier implementations of the BoE's CBEST framework and DNB's TIBER-NL initiative, the ECB came up with a TIBER-EU framework for the European countries to implement, with varying degrees of freedom to consider the specificity of the local landscape. This harmonisation was duly needed as there was already a diverse range of tests at national level without clear guidelines for the financial institutions (FIs) and FMIs active on a pan-European scale. The NBB was the first NCB to customise the EU framework to better serve the Belgian concerned institutions (CI) and FMIs with headquarters in Belgium. It could thus reap the benefits of earlier work, while establishing a memorandum of understanding (MoU) for cross-jurisdictional collaboration, result- sharing and fostering mutual recognition of both the tests and the people involved. It should be highlighted that the TIBER framework is independent of the NBB's responsibility as prudential supervisor and overseer.

This is what *Threat Intelligence-Based Ethical Red teaming* (TIBER) is all about:

- *Threat Intelligence-Based* refers to analysing the global cyber security threat landscape with its current tactics, techniques and procedures (TTPs) used by real hackers, the current geopolitical landscape or the important events that change the way of working (e.g. COVID-19 pandemic leading to wide recourse to working from home). Threat intelligence (TI) has two major components: the *generic* threat landscape (GTL) investigates the cyber threat landscape from a financial sector's perspective. *Targeted* threat intelligence (TTI) focuses on the particular CI in scope, together with its distinct critical economic functions, infrastructure, staff, systems, software and processes.
- *Ethical* means the intent is to find relevant evidence, leading to concrete improvements and increased confidentiality, integrity and availability.
- *Red teaming* comes from the military exercises and simulation methodology where Red (attacker) vs Blue (defender) teams engage in realistic scenarios. In this kind of exercise, both the Red Team (RT) and the Blue Team (BT) start with minimal (grey box) to no information (black box) about each other's available intel, capability, techniques, tools or goals.

Performing TIBER-BE exercises

A typical TIBER tests consists of specific phases.

The first phase is the initiation and preparation phase serving to identify the major stakeholders. The *White Team* (WT) is a group of selected few of the CI knowing about the TIBER test. The *involved authorities* can vary greatly depending on the scope and often involve more NCBs in multi-country exercises, but the lead should always be with the NCB of the country where the headquarters of the CI resides. The *threat intelligence supplier* (TI) and the *Red Team supplier* (RT) are next to be identified. The choice of suppliers is such that it complies with all regulations and requirements of the involved authorities (e.g. CBEST and PASSI respectively UK and France). The suppliers should also have the required capabilities to effectively and efficiently provide return on investment and should vary sufficiently to broaden the types of approaches for simulated attacks. The last two stakeholders are the *Blue Team* (BT) and the *TIBER Cyber Team* (TCT). The BT is the existing defensive security organisation of the CI and is by design unaware of the existence, planning or any aspect of the TIBER test. The TCT consists of members of the authorities, mainly our NBB TIBER-BE test managers (their role is described in the box below).

BOX 14

The role of the TIBER-BE test manager

The typical tasks of a TIBER-BE test manager, key member of the TCT, are to:

- Provide insight into the GTL, together with the GTL supplier, as starting point of a TIBER project
- Guide the White Team through the TIBER process, methodology and deliverables to avoid pitfalls and provide maximum added value for the CI
- Act as catalyst and moderator between several stakeholders to ensure optimal collaboration, acting as a go-between and escalation point where needed, while ensuring confidentiality of the identity of the CI and the potential findings

▶

- Be a neutral party but optimally use its sphere of influence during the whole process to keep the project on the rails, especially in the active testing phase and closure phase in order to mitigate any potential conflict of interests
- Deliver 360° feedback at the end of a test for all stakeholders as an opportunity to grow and learn for upcoming tests
- Analyse the lessons learnt from past tests to improve the TIBER-BE templates, guidelines and methodologies, whilst sharing experience with the TIBER-EU authorities (ECB, NCBs, etc.) and partners
- Discuss changes in the GTL on a pan-European level, with the involved parties and with its peers within the organisation.

During the second phase or test phase, with the GTL as starting point, the TI provider will firstly analyse the CI and its concrete threat landscape to generate the TTI and, secondly, the RT supplier will execute the selected realistic scenarios in a red-teaming setting, in accordance to the CI's risk appetite. This is by far the longest part of the project, with periods where the RT tries to execute the scenarios, with some "lay-low" periods to avoid detection and periods of fast decision-taking to take advantage of limited windows of opportunity. The action taken in this phase and the findings (e.g. the Red Teaming test summary) are strictly confidential.

The final phase or closure phase will provide an opportunity for all involved parties to learn and improve. This is done by re-playing the attack together with the BT and the RT (the so-called Purple teaming or PT), by agreeing on a remediation plan and sharing feedback between the institution, the suppliers, the TIBER team and other involved authorities in the form of a 360° evaluation, led by our TCT.

TIBER-BE is distinct from other Red Team penetration tests. For example, should the RT be blocked in a certain scenario, for instance because the CI's defence capabilities are successfully detecting and stopping every phishing attempt, there is the possibility of using a "leg-up". A leg-up bypasses the current roadblock and enables the Red Team to continue its work as if the intermediate step, in the above example the phishing, would have been successful. Such a leg-up can, for example, be providing direct network access, valid credentials or additional insight into technology to help the Red Team advance and make sure the TIBER exercise still has the best possible added value.

Another aspect is that, on top of the planned scenarios, there is the possibility of building a scenario "X" as the project evolves. In this special scenario, unexpected yet interesting findings, can be leveraged to make fully use of the suppliers' TI and RT capabilities in order to reach the most critical systems and thoroughly test the cyber defences of the CI, from an angle that might be very different than the usual TTP's of currently identified threat actors. This mimics potential future threats.

Continuously improving the TIBER Framework and perspective

To boost collaboration with the CIs within the TIBER-BE sphere of influence, the NBB organises and leads the TIBER National Implementation Committee (NIC). This makes it possible for CIs and suppliers to discuss their experience and for the NBB to boost the involvement of the different partners. No specificities can be shared during meetings of this forum, but this makes it even more interesting to analyse the high-level findings and share recommendations on both cyber resilience and TIBER methodology in order to understand the emerging patterns and how to implement improvements for the whole financial sector. After all, TIBER is not about implementing a certain patch against a certain vulnerability, or even about generic pattern findings like top ten cyber security risks. It is about choosing the right organisational, methodological and systemic continuous improvements that provide the highest value added considering the real and recently emerging cyber threats. One of the main focus is to test the capabilities of the Blue Team. Although individual test results are strictly confidential, a few insights into identified issues and risks can be shared, as these are well known to bad actors and not characteristic of the financial sector, while understanding that the risks and high-value targets remain distinctive, the sector can still benefit from improving generic defences. Network access control (NAC or network segregation) is not always correctly implemented in all parts of the network, making pivoting and lateral movement from a low-value target or machine to a high value one "relatively" easy for a skilled hacker. Another pattern that can be identified is the hard-shell syndrome: it is hard to get into the institution given decent perimeter defences, both logical (websites, end-user devices and virtual private networks) and physical (doors, locks, security cameras) are well-established, guarded and monitored. But once a malicious actor has gained access to the internal network, there are fewer barriers in place to prevent privilege escalation, exfiltration of confidential data or breach critical systems without being detected. It is worth noting here that a substantial degree of compromise come from insider threats, actors that are already inside the network or even employees. Using decoys (also known as honeypots and canaries) is another good practice that is not used to its full potential yet. Extending and refining the granularity of defence mechanisms inside the core network, as well as implementing multi-layer detection capabilities is thus paramount to a modernised cyber resilience.

From past experience, the TIBER-BE team could already draw some interesting lessons. One attention point is refining the so called Purple Teaming phase: scenario replay, cooperative red-teaming, simulation, knowledge-sharing and instating the right mindset to make sure the Red and Blue Teams act as one, with the same final objective in mind, namely raising the CI's detection and response capabilities. Another point of focus is sharing results with regulators without endangering the CI, whilst ensuring that the remediations are put in place correctly and in good time. Some CIs are already top of the class and the usual mimicking of current bad actors will not help learn any new lessons since all known threat actor *modus operandi* (MOs) are detected and mitigated instantaneously. For these mature institutions, one could consider putting scenario "X" first to increase the return on investment of the TIBER exercise. Certain red-teaming activities involve trying to physically gain unauthorised access to a company's assets. The coronavirus pandemic poses a serious challenge for this kind of test as access control is tightened and it is not easy to blend in if only a few people are present on the premises. This also poses difficulties for the other parties involved in the test, as it is challenging to securely exchange highly confidential documents that are normally only to be consulted on site. It should also be highlighted that the upcoming Digital Operations Resilience Act (DORA) will potentially increase the current scope and may change the flexibility and freedom of action of the framework. This might also have an impact on the three-year cycle, potentially reducing the effectiveness of the methodology. Moreover, globalisation and the growing international dimension beyond the EU increase the difficulty of correctly managing expectations and ensuring an optimal outcome, for a realistic effort and feasibility.

In addition, the growing outsourcing to Software as a Service (SaaS), cloud or other specialised third parties affects diverse aspects such as scope, legality and responsible disclosure. TIBER intends to test the CI, not the SaaS providers. The test also needs to respect the terms of service of parties that are in fact not part of the test but hosting the CI's services. The recent shift towards agile project methodology can in some cases also result in paying less attention to non-functional requirements, in this case security aspects. Recent and rapidly evolving internet-facing technologies (cloud, blockchains, Internet of Things, mobile, artificial intelligence, robotic process automation) extends the attack surface and yields unfamiliar attack vectors and experimental TTPs. Malicious actors have at the same time boosted their deceptive capabilities. Finding suppliers with the skills to understand and mimic these innovative TTPs is hard. There is a scarcity of skilled RT providers in the EU, given that including non-EU providers involves supplementary challenges and risks, such as data safe-haven questions, General Data Protection Regulation and geopolitical implications and certification recognition. Finally, recent incidents in cyber security point out the steep rise in supply-chain types of attack, targeting the weakest link in a supply chain to compromise assets very early on. A simple example is tampering with ATMs during the manufacturing phase long before they are shipped to a bank instead of trying to attack ATMs that are already installed. A more complex example might be to compromise code compilers used to produce software that is later used to push certificates from a trustworthy source to banking application users. In other words, the security of a company is as good or rather as weak as the weakest link in all its combined supply chain components as malicious actors take the path of least resistance, not necessarily the most obvious one.

The feedback from the various involved institutions after the first TIBER tests so far is very positive. The sector appears to be convinced of the methodology and the added value of this opportunity to raise cyber security awareness, gain valuable insight into present and future threats, improve intrusion detection/protection capabilities and cyber resilience in the broader sense. All of which is contributing to higher confidentiality, integrity and availability with the final goal being to improve financial stability, in line with the NBB's key mission.