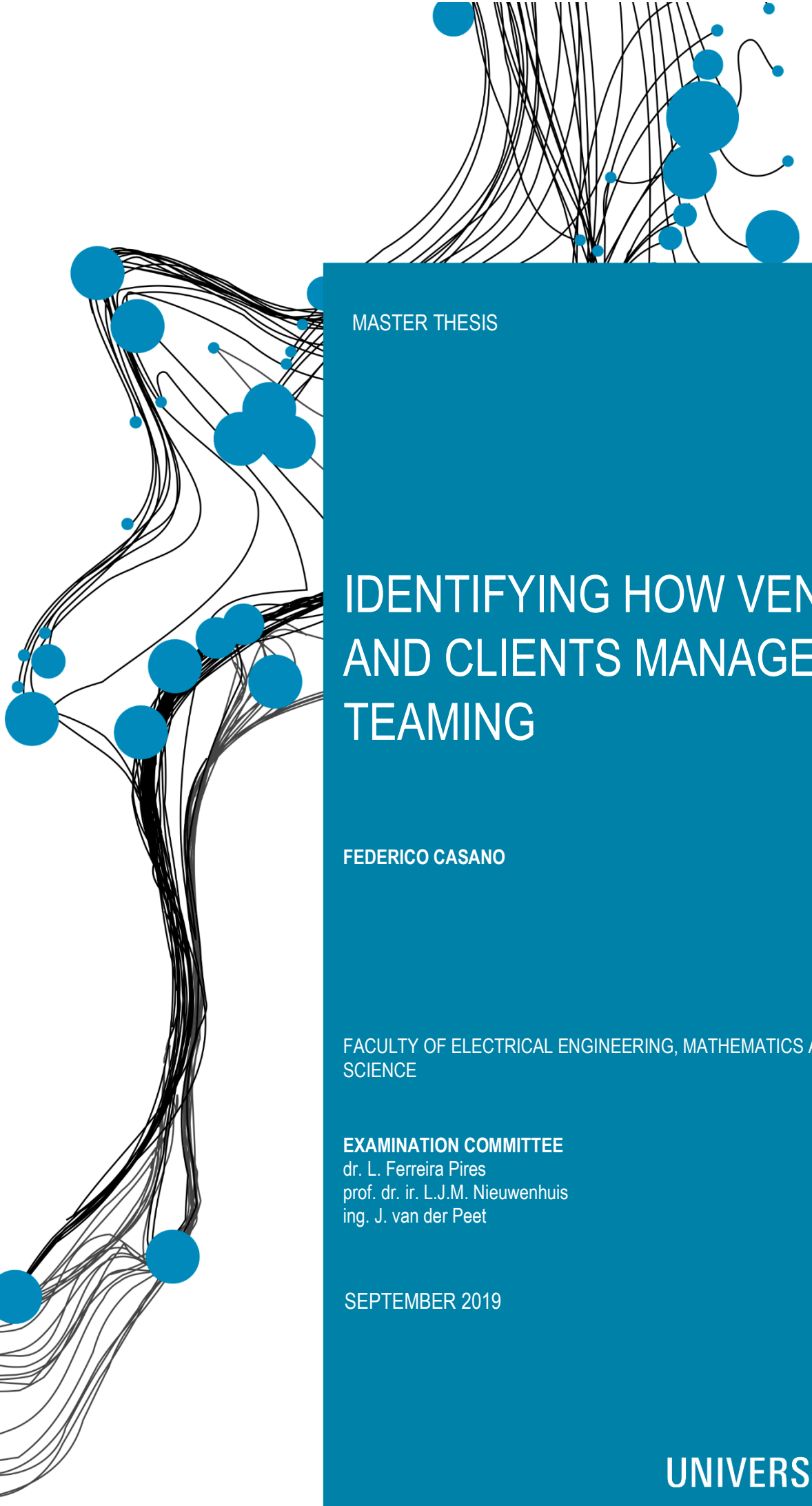

MASTER THESIS

IDENTIFYING HOW VENDORS AND CLIENTS MANAGE RED TEAMING

FEDERICO CASANO

FACULTY OF ELECTRICAL ENGINEERING, MATHEMATICS AND COMPUTER SCIENCE

EXAMINATION COMMITTEE
dr. L. Ferreira Pires
prof. dr. ir. L.J.M. Nieuwenhuis
ing. J. van der Peet

SEPTEMBER 2019

UNIVERSITY OF TWENTE.

Abstract

The master thesis presents red teaming, that is an adversary attack simulation which challenges people and systems. This thesis illustrates its main phases, along with its benefits and limitations. Moreover, it discusses the use of red teaming as solution to reduce uncertainty in cybersecurity investments, consequently allowing focused investments in companies regardless of their size, lastly improving their overall cybersecurity. It also provides a unique insight into the service through the analysis of data collected by interviewing red team vendors and clients (CISOs), and thereby identifying strengths and weaknesses in the service. Follows, an examination of two reports given by the providers of the service, and an introduction to the TIBER-EU framework, describing its benefits and challenges. Indeed, the framework aims to improve the resilience of organizations' infrastructures through red teaming, recommending the service and in this way increasing its key role in cyber defense practices. In addition, the dissertation delves into the Cyber Threat Intelligence subject, highlighting why it results in a good combination with red team activities.

Keywords: red teaming, red team clients, CISOs, red team vendors, uncertainty, red team insight, TIBER-EU framework, cyberattacks simulation, Cyber Threat Intelligence.

Master Thesis report: *"Identifying how vendors and clients manage red teaming"*

"If you know the enemy and know yourself, you need not to fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu, The Art of War

Author's Biographical Sketch

Federico Casano is a graduate in Computer Science at the University of Genova. Post-graduating at the University of Twente and Trento in a double degree path sponsored by the European Institute of Innovation & Technology. The major of his master is Cybersecurity along with a minor in Innovation and Entrepreneurship.

He attended the first year at the Department of Engineering and Information Sciences of the University of Trento, where he lived in the Collegio Bernardo Clesio, a college for excellent students. At the present he aspires to become a Cyber Security expert.
During his studies he became interested in Offensive Security. In the last 4 years, he studied Cyber Security and obtained few certifications from American Universities and multinational companies.

In March 2017 he participated in the closed-door meeting NATO Advanced Research Workshop: "New Generation Cert: from Response to Readiness - Strategy and Guidelines".
While in April 2018 he participated in the NATO Locked Shields: the world's largest and most advanced international technical live-fire cyber defense exercise.

He has been Teaching Assistant of the Offensive Technologies course at the University of Trento, Operating Systems at the University of Twente and Security and Cryptography at the University of Delft.

At the moment he is curator of the cyber security column at the website crimint.it

During the spare time he does martial arts and he is a volunteer of the Red Cross.

Acknowledgments

I would like to thank the executives clients of Deloitte for their participation in the survey who supported my work in this way and helped me get results of better quality. I am also grateful to the members of my team for their patience and support in overcoming numerous obstacles I have been facing through my research.

I would like to thank my fellow working students and interns for their feedback, cooperation and of course friendship. In addition, I would like to express my gratitude to all the staff of Deloitte.

Nevertheless, I am also grateful to my supervisors at the University of Twente, Prof. Ferreira Pires and PhD Abhishta, and my supervisor at Deloitte, ing. Jos van der Peet. Special thanks also goes to my examiner Prof. Nieuwenhuis for his advices.

I would like to thank my friends for accepting nothing less than excellence from me. Last but not least, I would like to thank my family: my parents, my sister and my great-aunt for supporting me spiritually throughout writing this thesis and my life in general.

Table of Contents

1 Introduction

The structure of this chapter is as follows: Section 1.1 presents the motivation for this work. Section 1.2 defines the research objectives. Section 1.3 describes the approach that was followed to achieve the objectives. Section 1.4 presents the structure of this report.

1.1 Motivation

This work was driven by the objective of demonstrating that investments in cybersecurity can be improved through the use of practices such as red teaming. In the current scenario in which companies continuously struggle to find the correct balance between business (i.e., making profits) and cybersecurity, the role of the Chief Information Security Officer (CISO) is crucial. Overloaded by responsibilities, the CISOs are the ones who try to secure the assets of the company in order to perform all the business services required by the leaders of the organization.
Even if the request of funds to the Executive Committee of the company for the implementation of cybersecurity defenses appears not to be an issue [1], the allocation of the investment is still a big question mark.
The strategy used, when uncertainty about which components need more protection is high, is to give a small investment to each asset of the company, with the hope to protect all of them up to a certain level [2]. Adopting this approach, the risk is that the organization's assets are not sufficiently protected, especially the primary ones, the "Crown Jewels" of the company. Indeed, even if this approach reduces the budget invested, resolving the over-investment tendency, to defer remaining investments until security breaches actually occur can turn into something hazardous for the company. Simply classifying the assets (you do not know what to protect if you do not see what you have) without a correlation with risks, allows attackers to exploit expected vulnerabilities (if you have forecasted them) causing a significant impact on the financial health of the organization [3].
Red teaming, as an information gathering tool, is a response to the security needs of the CISOs and their organization. Indeed, it allows small, medium, and big corporations to invest money more efficiently, directly to the valuable and risky assets, inferring knowledge about the potential threats through the simulation of real-life attacks (i.e., using the same techniques and tactics of cybercriminals). Red teaming addresses investment issues, reducing uncertainty, and safeguarding the *weakest links*.

In this research we often refer to red teaming with RT. Also, with the term "red team projects" we mean the red team assessments and tests performed by vendors of the service. Also, we often refer to red team members as red team operators.

1.2 Objectives

The master thesis aims to:

- Give a unique insight into red teaming from stakeholders perspective, showing an unprecedented overview of red teaming.
- Verify if red teaming reduces uncertainty and consequently allows focused investments in companies regardless of their dimension, lastly improving their overall cybersecurity.
- Identify strengths and weaknesses in the red team service.

In particular, through the analysis of data collected during interviews, to a cluster of CISOs, it points out the profit of organizations asking for the service. The goal is to demonstrate that red teaming is an essential security countermeasure. Besides, one of the benefits of red teaming is training of the company's personnel. Chief Executive Officers (CEOs), CISOs, system architects, blue teams, developers, and security engineers, all of them would have the opportunity to practice against real attacks in a secure manner. It would be an excellent gymnasium for all the employees not only security specialists (red teaming involves the company in a 360 degrees process), improving the total cyber hygiene[1] of the organization. In conclusion, "only when they are attacked do they truly learn what the cost of attacks is" [1].
Last but not least, in a situation in which hunting hackers and putting them in jail is still utopian, red teaming poses itself as an alternative solution to reduce the cybercrime business case. If the overall cybersecurity importance increases, along with defenses, attackers are supposed to allocate more resources to perform valuable attacks, but in this way, their profit would decrease, making them unwilling to perform crimes. (Also the monitoring system would be more efficient, being part of the main defenses adopted by the companies.)

We believe that red teaming, as information gathering tool, is an efficient strategy for reducing uncertainty in firms solving under- and over-investments issues, which are adverse situations for the economy of the companies (it is stated in the literature that uncertainty can lead to less effective spending [1], [2]). We also believe it can improve cybersecurity indirectly as a whole, reducing the overall number of cybercrimes. If cybersecurity is deemed more important and more funds are diverted to it, the attackers would need to invest more and their Return On Investment (ROI) goes down. Furthermore, the only literature we found regards guides (e.g., the one published by the U.K. Minister of Defence [4]) about how to properly perform red teaming and elaborated descriptions of the concept. In any case, they mainly focus on red teaming as a general concept, not delving profoundly into red teaming as a service offered by consulting companies like Deloitte.
This research aims to understand how vendors and clients that ask for red team services (the stakeholders) manage red teaming. The involvement of the red teamers and clients is genuinely believed as one of the most appropriate ways to validate our assumptions.
To the best of our knowledge, such a survey is not available, this is the first one, and should help providers of the service and the academic world to perfect red team as a service, finding out its benefits and limitations.
Also, it is expected to be beneficial for the evaluation of the role that red teaming has as cybersecurity defense, among the other countermeasures in the market. The survey demonstrates that after the request for red team services, other barriers are less necessary. It poses itself also as an obstacle to the spread of a "lemons market," so defined by economist Akerlof [5]. "Most users cannot tell what is vulnerable, so developers are not compensated for efforts to strengthen their code" [6]. In other words, the lack of knowledge of the customers implies less quality in vendors' products.
To summarize, the interviews to executives and red team vendors are a method to assess qualitatively red teaming from the stakeholders' point of view, demonstrating that is an essential solution against cybercrime and to improve it according to customer needs, if required.

1.3 Approach

To achieve the main objectives of this research, the following steps were taken:

[1] Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security [32].

1. Perform a literature review study on Economics of Cyber Security, by looking at the subject in terms of cybersecurity investments, threats, and mitigations strategies.

2. Perform a literature review study on Red Teaming, by looking at the subject as a general concept (e.g., as perceived in traditional in military environments) and as a service (i.e., as firms sell the service testing clients' infrastructures). The study includes two anonymized reports, provided by the vendors, written at the end of the service (analyzed in Appendix A).

3. Execute an explorative approach in the following steps:

    a. Interview service managers through a questionnaire and collect their answers, focusing on how red teaming is handled at the managerial level, combining the results with public information available, therefore confirming and elaborating information collected in the initial literature review phase.

    b. Interview red team members through a questionnaire and collect their answers, focusing on how red teaming is performed, combining the results with public information available, therefore confirming and elaborating information collected in the initial literature review phase.

    c. Interview red teaming clients and collect their answer through a questionnaire, focusing on how they perceive red teaming, on their overall experience with the service and on how they manage their company cybersecurity.

Deloitte as sponsor helped me to contact the executive department of their clients in the private sector (in the Netherlands and abroad), and then planned direct or remote meetings. I recorded the answers and started analyzing the data after a significant group reached. In the end, the output of the analysis has been presented anonymously, as reported in this dissertation.

1.4 Structure

The remainder of this thesis is structured as follows.

Chapter 2 gives the background to our work. We introduce and discuss both uncertainty and weakest link concepts in some detail.

Chapter 3 defines what is red teaming, illustrating the main phases, along with its benefits and limitations. Also, the differences with penetration testing are described. Then, social engineering attack techniques, have their own section since they are core of red teaming operations and are a distinction with penetration testing.

Chapter 4 introduces the TIBER-EU framework, which aims to improve the resilience of organizations' infrastructures, and discusses the role of red teaming inside of it. The chapter explains Cyber Threat Intelligence and why it results in a good combination with red team activities. In addition benefits and challenges of the framework are described.
It is not goal of the chapter analyze in detail the framework, instead our objective is to introduce it, in order to point out its benefits: 1. Red Teaming spread, removing misinforation about the topic and its execution and 2. Combination of Cyber Threat Intelligence and Red Teaming.

Chapter 5 describes the interview process followed for the development of this dissertation.

Chapter 6 offers an insight in red teaming from a vendor perspective based on interviews. It provides a service overview, analyzing each stage. At the end, service improvements are proposed by red team vendors.

Chapter 7 illustrates the answers obtained interviewing clients who asked for the service, who have a pivotal role in the success of the entire activity.

Chapter 8 concludes this report and gives recommendations for further research. It also mentions the limitations that our research unavoidably faced.

2 Background

This chapter is structured as follows: Section 2.1 introduces the reader to the reality in which we currently live and where firms deal with cybercrimes. Section 2.2 talks about the concept of uncertainty, a situation which diminishes overall cybersecurity and makes it harder for companies to invest properly, e.g., weakening Return On Security Investment (ROSI) efficacy. In Section 2.3 red teaming is briefly proposed as an approach to reduce uncertainty. Also, the weakest link notion, pursued by cybercriminals is introduced.

2.1 Growing need for cyber investments

The world is in the midst of a massive technological change (Fourth Industrial Revolution), which puts more and more people in contact with the digital world. Companies and governments are forced to tackle issues related to sophisticated technologies such as Big Data, Machine Learning and the Internet of Things. However, new discoveries in addition to promising growth opportunities for countries, increase the risk of illegal cyber activities, increasing the attack surface along with the number of vulnerabilities.

In the last years, to cope with the cybercriminals the percentage of budget invested in security has rapidly risen. In 2017, cybercrime costs increased with organizations spending nearly 23 percent more than 2016, on average about $11.7 million, according to a study performed in seven countries: Australia, France, Germany, Italy, Japan, United Kingdom and the United States [7]. However, the perception is that the amount of money spent is not enough and governments more than companies should invest more because they are still not able to keep the pace with the technologies used by hackers.
Countries are incredibly inefficient at fighting cybercrime, and cyber threats impose excessive costs on society. For instance, it is predicted that cybercrime damages will cost the world $6 trillion annually by 2021 [8]. Put in perspective to the costs and profits for an organization, it is observed that the budget spent is not sufficient to guarantee a high level of security to a company. Indeed, despite the expenditure, companies still lose money to malware and other attacks. One of the main reasons for that is the different nature between traditional crimes and cybercrimes. Indeed, while there is a structured and optimized system to contrast local crimes like car theft, for global cybercrimes the situation is more complicated due to strong externalities [9]. A simple example of externalities are the consequences of an attack that targets a specific company. Indeed, the impact of that attack potentially affects not only the owner network but thousands of customers as well [10].

2.2 More efficient cyber investments diminishing uncertainty

Academic papers that struggle to optimize cybersecurity investments recommend that the best idea is to approach the problem in a reactive way, trivially hunting the cybercriminals and putting them in jail [9]. Although this is suggested as the most efficacious strategy in reducing cybercrimes, there are many limiting factors. As stated in Section 2.1, cybercrimes are global and often the attacks are carried out from countries different from the country where the attacked party is located. This leads to problems of regulations: for instance, if international hackers steal information from a multinational company in the Netherlands, is it a Dutch crime or a crime in another country because the HQ of the company is located elsewhere? In addition, technologies like Tor network or proxies are used by the criminals to conceal their identity, making backtracking to the source challenging.

Since arresting the cybercrime phenomenon seems infeasible, the more logical strategy is to apply defenses against it in terms of cybersecurity countermeasures. Thus, companies spend part of their budget adopting software or hardware to protect themselves, according to a quantified risk. The same applies to governments.
Nevertheless, the purchase of security controls and the evaluation of ROSI are influenced by the market. Many of the existing surveys are written by entities such as anti-malware software vendors or police agencies, which all of them have a biased opinion of the facts, though tending to be objective. The data that can be analyzed from online statistics contain both unintentional (e.g., biases) and intentional (e.g., software vendors promote their products) errors leading to under- and over-reporting.
For instance, even if the public opinion could make us think that there are many cybercriminals the reality is different. Few gangs out there have the resources to commit certain types of attacks at large scale [9]. This applies to botnet, ransomware or phishing attacks. For what concerns the latter, the purchase of antivirus products for preventing cybercrimes is not sufficient if not accompanied by law enforcement countermeasures [9].

The above mentioned externalities modify the perception that companies have of the threats, increasing their uncertainty level. This increment can be translated not only with request of more allocation of budget to defeat cybercrime but also with ineffective distribution.
Hence, a viable strategy to protect the company infrastructure could rely on the defender's knowledge about future attacks and the sunk[2] costs incurred when upgrading defenses reactively. Differently from what is currently done, organizations could invest less, but with more precision, and change their posture: "rather than over-invest proactively, companies could wait to observe which attacks work and use this knowledge to better allocate security spending" [2]

Return on Security Investment

Return on Security Investment is a tool that can help organizations to assess their cost effectiveness [11]. Also, executives interviewed during the research phase of this dissertation demonstrated a lack of awareness about the topic.

The concept of ROSI comes from the finance sector, although in that domain, people speak more generally about ROI. But when we switch to the security domain, things change. In security as in other sector, executives need to justify the request of budget, and ROSI calculation can provide answers to essential financial questions, such as:

- Is an organization paying too much for its security?
- What financial impact on productivity could a lack of security have?
- When is the security investment enough?
- Is this security countermeasure beneficial?

[2] In the sense that money is spent irrevocably.

But why do we talk about ROSI and not ROI when it relates to security?

$$ROI\% = \frac{(\text{Gain from Investment} - \text{Cost of Investment})}{\text{Cost of Investment}} \times 100$$

Figure 2.1: ROI formula [12]

ROI calculation is weak and inappropriate if applied to cybersecurity. "Security is not generally an investment that results in a profit. Security is more about loss prevention. In other terms, when you invest in security, you don't expect benefits; you expect to reduce the risks threatening your assets [11]."

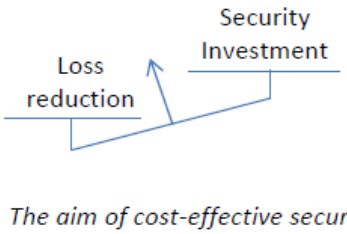

Figure 2.2: Balance between loss reduction and security investment [11]

The ROSI assessment defines in a quantitative way[3] how much loss you avoid thanks to your investment, considering several components of risk.

$$\text{ROSI (\%)} = \frac{\text{ALE} * \text{Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}$$

Quantitative Risk Assessment Formula

Figure 2.3 ROSI Formula [13]

Where:

- **Risk Exposure** = Annual Loss Exposure (**ALE**)
- **ALE** = Single Loss Exposure (**SLE**) * Annual Rate of Occurrence (**ARO**)
- **SLE** = Estimated cost of a negative security event
- **ARO** = Estimated probability of the negative security event occurring in a year

[3] A quantitative assessment associates numerical values to the risks taken into account in the analysis.

Figure 2.4 describes the ROSI calculation graphically, showing, as expected, that there is a conjunction point between Costs of Software Security Failures and Costs of Software Security Measures.

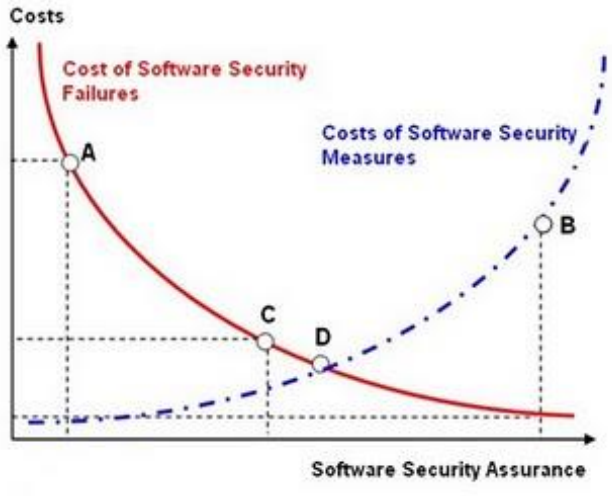

Figure 2.4: ROSI calculation graph [14]

It is essential for executives in companies who have the role and duty to protect their company from cybersecurity attacks to consider the graph and calculation in Figure 2.4. ROSI assessment is a tool, used for many years by now, capable of identifying the right tradeoff between risks/loss and security investments in countermeasures. The tool is often taken into account when asking for products or services to cybersecurity vendors.

2.3 What are the possible approaches to reduce uncertainty?

As stated by the Secretary of Defense of the United States, Donald Rumsfeld [15]:

There Are Known Knowns – There Are Things We Know We Know.
There Are Known Unknowns – That Is To Say We Know There Are Some Things We Do Not Know.
But There Are Also Unknown Unknowns – The Ones We Don't Know We Don't Know.

The above citation stresses that we need to investigate those situations or subjects that appear clear to us, because, even if we are confident about our knowledge, risks might come from situations that are so unexpected that they would not be considered.
Therefore, to reduce uncertainty it seems a reasonable direction to focus and prioritize investments in the most critical assets of the company, anticipating unexpected risks. This can be done through information gathering, increasing our awareness, like with penetration testing or red teaming.

Red teaming, which pursues the weakest links, as we explain in the next chapter, is an ad hoc solution for the unknown unknowns (unexpected or unforeseeable conditions), which pose a potentially greater risk because they cannot be predicted based on past experience.

Weakest links identification

The literature contains information about the attacker posture to the crime. It is known that cybercriminal operates in a strategically way pursuing the weakest link [2] (as red teaming does, since it mimics real attacks). It is, in general, a flaw in the system that could compromise its entirety. The weakness is merely a vulnerability, like an error in the code, or a misconfiguration.
Due to its nature, the weakest link is the one that hackers gravitate towards aiming to break into the system and gaining control of it. The weakest link is not necessarily the "cheapest" to exploit but "information systems are often structured so that a system's overall security depends on its weakest link" [2], and thus it could be exploited first to maximize profits, possibly taking into account variables such as ROI.
The flaws "are out there" waiting to be exploited by a malicious user, security researchers or cybercriminals, though the intent differs. Since the software that we use every day can be (legally or not) analyzed, it can happen that vulnerabilities are discovered and exploited before being published online. And then, after some time, they are fixed by the vendors. Like a continuous cat and mouse struggle, the process of finding a hole (hacker/cat) and fix it (software vendor/mouse) becomes a repeating game. After a weak point is fixed, new vulnerabilities are published waiting to be solved again. It occurs to see this pattern in discussed circumstances, for instance, if a new vulnerability has been found in a protocol, developers work to patch it releasing a new version of the protocol. For example, Heartbleed, a famous buffer overflow vulnerability found in the SSL protocol implementation, was patched by developers with a new version. In general, if a defense is in place attackers find a way to break it, and developers struggle to create a new stronger barrier (waiting to be exploited).

Nonetheless, even if the procedure above seems easy to perpetrate (from hacker's point of view), that is not the case. At first glance systems or software take the form of a black box for attackers. The hackers do not know anything about the environment that they are going to control.
The same applies to defenders. They know what to protect but not from whom. In this high level of uncertainty about which is the weakest link and which one would result in a door for damaging the system, CISO may decide to protect many assets, but only up to a point [2], with the intent to protect as many systems as possible. The budget that they have available, although quite copious is limited in some cases, and they need to distribute it among the assets of the company.
If uncertainty is too high the defenders might even take the decision to not protect any assets, unaware of where to put money [2].

The cases above do not consider a "wait-and-see approach." [3] In the beginning, only a portion of the budget could be invested waiting for security breaches to occur, gaining information from them. While companies can wait for attacks committed by cybercriminals, the adoption of specific approaches to increase knowledge, such as performing red teaming, operations help to identify the weakest links (mimicking cybercriminal actions). Then, the remaining budget may be spent only on targeted systems. Thus, this "wait-and-see approach" permits to under-invest, until a clearer idea about the security of the system is obtained.

3 Red teaming

This chapter defines red teaming. Section 3.1 is totally dedicated to the definition of this concept. Section 3.2 delineates the main phases of a red teaming service. Section 3.3 points out the difference between a service that could seem very similar at first impact: penetration testing. In Section 3.4 we discuss Social Engineering: core part of red teaming and distinction with penetration testing. Section 3.5 explains the benefits of red teaming, and Section 3.6 discusses its limitations.

3.1 Definition

Red teaming has its roots in the Kriegsspiel sessions of the Prussian General Staff [16] but after 9/11 it took the shape we know today. Around midnight on Sept. 12, 2001, after the terrible and unprecedented terrorist attacks, Director of Central Intelligence George Tenet in a meeting with his chief of staff, John Moseman, and the CIA's deputy director of intelligence, Jami Miscik, opted for a new approach to the mitigation of national threats. He formed a new team with the role of stimulating decision making processes in a uncommon way, through contrarian thinking. All of them were confident that there were additional plots against U.S. national security. Thus, in the evening of the same day, he gave the following instructions to the newly formed group: "Tell me things others don't and make [senior officials] feel uncomfortable" [17]. The name of this CIA's group is Red Cell.

Although various definition of red teaming are given in publications, for the purpose of this report the one proposed by the U.K. Minister of Defence [4] is used. This is a general definition that does not entirely and exclusively apply to red teaming services offered by private companies.

Red Teaming is the independent application of a range of structured, creative and critical thinking techniques to assist the end user make a better informed decision or produce a more robust product.

Often, in the literature (representative article [18]), we hear the term Threat Modeling[4].
Professionals protect their systems against hackers (in the sense of cybercriminals, although the term initially identified skilled computer enthusiasts not necessarily committing illegal acts), by assessing the security of their network and systems from the perspective of the attacker [19]. They aim to predict the malicious behaviors that cybercriminals could adopt.
However, the multitude of potential attacks and the resources at disposition to the attackers makes this job very difficult. Indeed, often they need help of specialized companies to properly test their own infrastructure.

Along with analysis of code or suggestion of the adoption of software/hardware countermeasures, among the services offered to private companies by experts like Deloitte there is red teaming. It is a process in which the behavior of an attacker is simulated considering all its attack vectors, which means that it not only includes network or websites but also physical security and employee involvement. If there is a way to break into your system they will find it. Indeed, they do not need a plethora of vulnerabilities to gain access, since one is enough.

Complementary teams definitions

The following definitions regard teams mentioned and discussed in this dissertation, which are complementary to red team. These teams may be involved in red team projects for their characteristics:

[4] https://en.wikipedia.org/wiki/Threat_model

- **Blue team** - is a group of individuals who monitor systems to ensure security, responding to cyberattacks and incidents, identify vulnerabilities, implement cybersecurity countermeasures and verify their effectiveness after implementation.
- **Purple team** - is a team of vendor red and blue team members, who help training the client blue (or red) team based on the exercise outcome. Furthermore, it facilitates the repetition of part of the attack simulations performed during the execution stage.
- **White team** - is a team of the company requiring the assessment who defines jointly with the provider the rules of engagement. The team members are, including client's CISO, company's representatives who oversees the attack simulation, read the final report, and decide how to involve the blue team of the company in the test.

3.2 Main phases and tactics

The three stages in the red teaming process, after the customer contacts the vendor to buy the service are Scoping, Execution, and Reporting.
In Scoping, the service provider, understanding the needs, along with the client define the attack simulation outlines, i.e., the subjects that will be tested, making sure to have all the permissions to move inside the client's environment. Then, the Execution stage starts, where the service takes all the components in the organization in scope (human, physical and cyber), but only explores them as far as necessary to achieve the pre-agreed objectives, therefore approaching realistically as an attacker. This is followed by full exploitation of vulnerabilities and persons using private as well as public techniques and knowledge, while numerous controls are put in place to minimize potential impact to operations. In the end, the red team attempts to breach as far as possible in the assigned time.

The steps taken during the Execution stage are:

1. **OSINT -** Once the scope and scenario related to possible foreseen cybercrimes are defined, also known as the "terrain" in which red team members will play their role, mimicking adversaries, information gathering takes place. Red team members try to get as much information as possible, like IP addresses, network infrastructure, email addresses, company culture and many more, through Open-source Intelligence (OSINT[5]), physical reconnaissance or other means.

2. **Breach** - Breach into the system: this can be done by breaking physical perimeter and gaining physical access, by tricking employees into installing malware via phishing[6], or by exploiting a vulnerability in the network perimeter (e.g., a vulnerable webserver).

3. **Foothold & persistence** - Install hardware implant to gain remote access (physical approach) or install a software implant to gain remote access.

4. **Lateral movement & privilege escalation** - Gain control of the assets defined in the Scoping stage.

5. **Action on objectives & exfiltration** - Compromise new machines if necessary to achieve the objectives and exfiltrate the information obtained.

[5] The term indicates data used in an intelligence context, collected from publicly available sources.
[6] Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords and credit card details, by disguising as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, with a look and feel identical to the legitimate site [33].

In the Reporting stage, the results of the service, including recommended countermeasures, are examined with the client. Then the service can stop there, be repeated (less usual) or leave room for training and strategy analysis, occasionally in the form of workshops.
It is also possible that the Purple team is involved at the end of the process.

3.3 Difference between Penetration Testing and Red Teaming

It is important for the completeness of this dissertation to understand the differences between penetration testing (PT), or commonly called pentesting in the literature (and as a slang word), and red teaming (RT), by learning why the latter is specifically required in place of PT.

Below, in a bullet point style, we mention and describe the differences between the two services:

- **Scope** – PT only targets pre-agreed systems and applications, whereas RT includes all infrastructure, indeed it involves not only the systems of the client's company but also the employees and the company's physical assets. Only by evaluating these last two elements as well, can all the components of the company be tested. Thereby this approach allows RT to additionally take the "insider threat" (i.e., an ill-intentioned employee) into account.
  As revealed by the past malicious attacks committed by cybercriminals, human factors and physical security are elements that could quickly be exploited, becoming a vector for illegal actions.
  If required by the client, red team operators can test both employees and building securities, highlighting flaws used often by hackers to perform social engineering attacks (i.e., enter the building pretending to be an electrician or sending a phishing email trying to gather employee credentials).
- **Tools** – Both services work with tools that can be found online. Moreover, often, security experts run also their own coded scripts.
  Although in both services the tools used are commercial, for what concerns RT we need to talk about dedicated professional software, offering specific features (like persistence once broken into a system[7]), which can cost even thousands of Euros[8]. Furthermore, the variety of tools used in RT is higher compared to PT. For instance, tools to perform phishing attacks are required as well.
- **Vulnerabilities role** – While PT ideally aims to discover all the vulnerabilities inside a system, RT tests specific functions or features. This means that not all the vulnerabilities are possibly reported. There may be no need for red team members to seek and exploit all vulnerabilities since even only one could allow them to achieve their goals. However, all the vulnerabilities observed are reported, even if they were not exploited. It would be unethical not to notify the client of the vulnerabilities, so leaving the organization open to exploitation.
  Hence, instead of aiming to report a complete list of vulnerabilities, RT helps in the process of impact analysis, pointing out what could actually happen in case of cybersecurity incidents.
  For example, RT operators can be tasked to execute a monetary transaction for a bank. It is clear that the vulnerabilities, if found, are just a mean to reach the final goal, that is to assess the cybersecurity of that particular company's function or feature.

[7] Once inside a system, cybercriminals apply techniques to create persistence avoiding to lose access in case of interruption of the connection or security countermeasures.
[8] An example is Cobalt Strike: software for Adversary Simulations and Red Team Operations. Its license for one year costs $3,500. URL: https://www.cobaltstrike.com/

3.4 Social Engineering

Social engineering is a relevant peculiarity of red teaming that needs to be discussed.
As indicated by security researchers, academics and cybersecurity vendors, cybersecurity is also about people.
As described in Section 3.3, red teaming tests involve also people, in particular, their cybersecurity awareness. Indeed, among the first steps in the execution stage of the service, in which the red team members try to find a way to get inside the systems of the company, there is social engineering.
As reported by FraudWatch International, 95% of cybersecurity breaches are due to human error [20], which represents a significant value, indicating how the companies' vulnerabilities very often lay on their personnel. Therefore, social engineering is widely used by red team operators. For instance, once inside a building, they can wait for the cleaning lady, pretending to be an employee who forgot the office key and ask her to open the office. Once inside, they can install a physical keylogger or use other techniques to collect sensitive information.

As indicated in the example above, social engineering exploits employee behavior, possibly the weakest link of the company, in order to obtain a "foothold" inside the company network.
Kevin Mitnick[9], who is a worldwide expert of social engineering, defines the human role for cybersecurity inside the company as follow: "*The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element*".

But why is the human mind so easily manipulated and therefore hacked by red team member and cybercriminals alike?

In the context of information security, the social engineering definition is: "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes[10]." Hackers and RT members exploit human psychology with the goal to get sensitive information or entice them to perform actions they would normally not perform, like executing malicious code.
The situational theory of publics, developed by Professor James E. Grunig in University of Maryland, College Park [21], defines under which circumstances people would take action, or feel part of a collective. Three points explain when the interlocutor is willing to communicate and when communication is more effective:

1. **Problem recognition** – the subject thinks the problem is relevant to them.
2. **Active involvement** – the subject thinks they will suffer the consequences of the threat.
3. **Constraint recognition** – the subject thinks their actions are limited by factors outside of their control.

The elaboration likelihood model (ELM) of persuasion [22] describes the ways humans change their attitudes or decide to perform actions they would not perform without external, stimuli proposing two major routes to persuasion:

1. **Central route**
    - Stimuli are weighted by the subject and the final decision is carefully elaborated.
    - High amount of cognitive effort.
    - Associated with "rational perfectly informed decisions" in Economics.

[9] https://en.wikipedia.org/wiki/Kevin_Mitnick
[10] https://en.oxforddictionaries.com/definition/social_engineering

- Persuasion happens through the careful elaboration of information.

2. **Peripheral route**
   - Communication that typically does not result in careful cognitive effort in understanding the message.
   - Subject is convinced by under-analyzing apparently relevant "cues" that are in reality unrelated to the subject matter.
   - Persuasion happens through "adjunct elements" to the communication.
   - Likeability of the subject, physical attractiveness and trust.

The peripheral route is vastly used as a "cheap" route to convince people to perform an action: buy a product, subscribe to a service, visit a location, etc. Its results are especially effective when physical contact is not a factor. Indeed, this mechanism is often used by marketing strategies or, in our case, by social engineering.

In particular, six factors that affect likelihood of human persuasion, in the process of hacking a human, were identified:

1. Reciprocation - subjects form implied or explicit obligations towards each other, called **Normative commitment.**
2. Consistency - subjects tend to be consistent with previous decisions, even if all evidence shows that these were *bad* decisions, called **Continuance commitment.**
3. Social proof - subjects tend to act similarly to their peers to "fit in," called **Affective commitment.**
4. Likeability - subjects tend to **trust** people they like, find convincing or attractive.
5. Authority - subjects **fear** punishment (that an authority can impose) and will comply.
6. Scarcity - subjects will **react** quickly and possibly irrationally to stimuli when they believe that their freedom of choice is a function of time or resource availability.

Red team members use therefore their own skills and knowledge of the topics to perform social engineering attacks of various types. We already mentioned an example where they persuade cleaning staff to deliver the keys of the offices, but many other situations are possible, since their imagination and ability are the only limits.

One of the most common social engineering attack performed is **phishing**, where the attackers aim at collecting sensitive information, such as login credentials, sending emails that might redirect victim navigation to fake websites or entice the victim to execute a payload.
It can be carried out in one single stage attack or multiple (e.g., two) stages attack.

Single stage attacks, steps depicted in Figure 3.1, usually aim at collecting sensitive information about "general" targets. There is no specificity in the attacks (e.g., they attack all costumers of mybank.com).

Figure 3.1: Phishing - Single stage attack [23]

Two-stage attacks instead involve an initial reconnaissance that gathers information needed for second stage. They are used to increase the credibility of attack, for example, getting proper legal references, employee names or a valid set of users in CC to phishing email.
This type of attack is used in case of spear phishing[11] where the target is an individual (e.g., CEO, manager or a person of interest) or a company, and additional information about the objects is required in order to increase the probability of success.
Spear phishing is a commonly used technique. In 2018, 71.4% of targeted attacks involved the use of spear-phishing emails [24].

Figure 3.2 accurately shows the steps of two-stage attacks and how the process of data collection can be repeated if necessary.

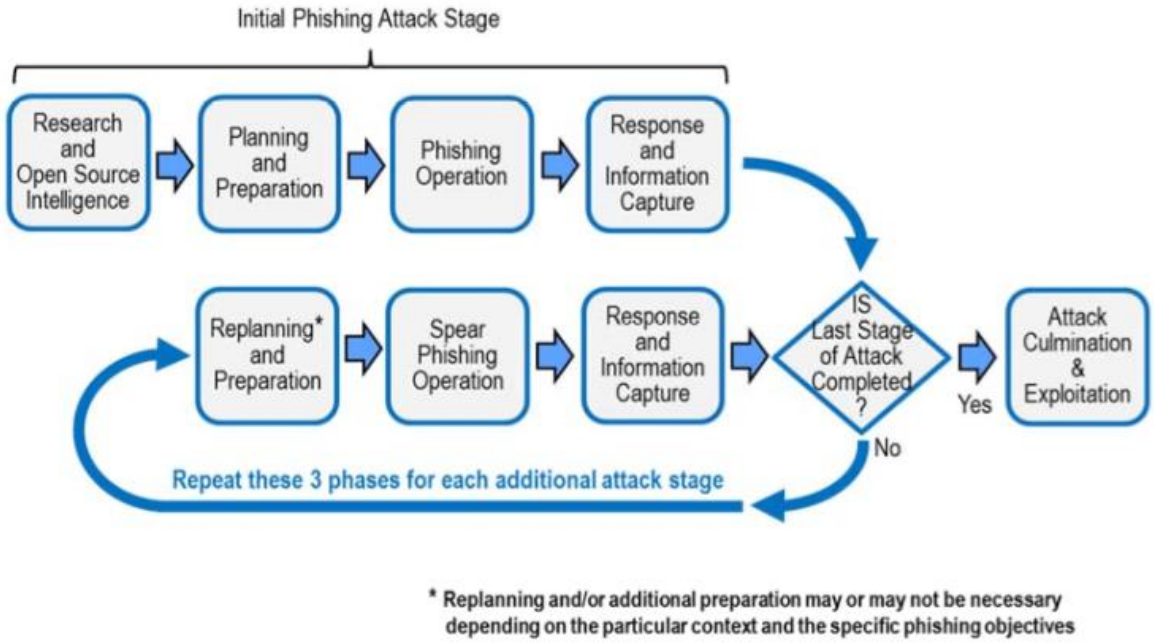

Figure 3.2: Phishing - Multiple stages attack [23]

Other examples of types of social engineering attacks committed are:

- **Tailgating** – The attackers follow the line of the employees entering the front door during peak hours, aiming to avoid security checks at the entrance.
- **Different setting** – The use of uniforms, for instance, of a courier service company, may allow attackers to access restricted zones without being asked for proper documents.
- **Shoulder surfing** – Simply observing an employee over his shoulders can reveal useful data, such as what he types on the keyboard.
- **Distractions** - Any kind of distraction, with or without partners in crime, can turn into a vector for sensitive data collection.

To sum up, social engineering is an integral part of red teaming. It can be adopted to test single company features (e.g., entrance security checks) or it can be part of a broader execution phase.

[11] Spear phishing definition: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing#spear-phishing

Regardless of the case, it remains a form of hacking, with which the attacker does not focus solely on the technical aspects of hacking into systems, but instead focuses on the human element.[12].

3.5 Benefits

Throughout this dissertation, the core benefits that red teaming services entail (according to literature) have already been mentioned. We summarize them in this section.
It is essential to bear in mind that the benefits are the driving motivation for this research.

The main benefits of red teaming are:

1. **Reduce uncertainty**: by increasing the knowledge of the systems and network, the service allows the executives to concentrate their effort on what needs to be protected, excluding what is already secured. This can be translated into more efficient investments along with a long-term increment of the ROSI for a company. Indeed, targeted protection potentially avoids financial loss due to cybercrime.
2. **Increase company cybersecurity level**: the overall cybersecurity goes up (especially if the service is performed periodically).
3. **Reduce cybercrime**: if malicious actors have to invest more resources in attacks, their profit could decrease dramatically, so it would make no sense for them to commit the crime. The lack of profit could diminish the global cyber criminality since the criminals "would lose their job".
   In addition, if consulting companies shared the information among their clients about their vulnerabilities and misconfiguration (in an anonymous way), the level of information sharing reached, accompanied by vulnerabilities fixes, would be another layer for attacks prevention.
4. **Increase personnel skills**: at the end of the service, the red team vendor provides to the client a detailed report outlining all the steps taken and vulnerabilities exploited. Despite the utility of the report, the red teaming provider may want to go further, indeed jointly with their clients, facilitates training sessions, explaining what went wrong during the execution stage. This is an excellent opportunity for companies to learn and improve their skills in short and long term perspectives. Last but not least, the provider helps companies improve their cybersecurity strategies if necessary.

In conclusion, red teaming is both preventive and detective, by showing paths likely taken by attackers in foreseen events and blocking them, and by giving to the client a clear idea of what strategies or countermeasures need to be implemented in order to prevent those incidents, although it does not suggest which specific technologies they should buy.

3.6 Limitations

Red teaming is output-driven, not process-driven, in the sense that all the steps are carried out for output sake. Being structured in this way, it is fundamental that the operation is performed in a planned way, with reasonable steps decided carefully. It means that the staff has a paramount role, and if not properly trained, this might lead to misleading results with a potentially negative impact for the company (e.g., damaging the company's infrastructure).
Another paramount part of the service is clearly the output (i.e., the report), which needs to be clear

[12] We thank Professors Luca Allodi and Bruno Crispo, University of Trento, for the academic material about the topic of this section [23].

and studied carefully jointly between providers and customers. If the joint study is not performed and/or the output is of low quality the entire service could be useless.

4 Red Teaming and Cyber Threat Intelligence: TIBER-EU Framework

The goal of this chapter is to introduce the TIBER-EU framework (Section 4.1) and describe how this framework can optimize the service. To examine this, an expert about the framework who helped in the development of the framework in the Netherlands has been consulted. Section 4.2 describes its structure. In Section 4.3 we explain Cyber Threat Intelligence and why it results in a good combination with red team activities. In Section 4.4 the role of red teaming inside the framework is discussed. Section 4.5 summarizes its benefits and Section 4.6 discusses the challenges of the framework.
It is not goal of this chapter to analyze in detail the framework (the official paper can be easily found online[13]). Instead our objective is to introduce the framework, in order to point out its benefits: 1. Red Teaming increasing adoption, removing misinformation about the topic and its execution and 2. Combination of Cyber Threat Intelligence and Red Teaming.

4.1 Overview

"What adversaries are most likely to attack us? Have you discovered any significant security events in our industry? Are other industries observing similar intrusions? What will happen to us if we imitate these attacks in our environment?" are all questions of clients of consultancy companies, like Deloitte [25]. The TIBER-EU Framework stimulates companies to adopt red teaming, considering it the most appropriate service to answer the above questions.

To support the theories presented in Chapters 1 and 2, we introduce the Threat Intelligence-based Ethical Red Testing (TIBER-EU) Framework released in May 2018 by the European Central Bank (ECB). This framework aims to improve the resilience of financial infrastructures and institutions against sophisticated cyberattacks by providing guidelines on how to efficiently perform red teaming. "TIBER-EU establishes a formal EU-based directive as to how companies should source and conduct an intelligence-led red team assessment. The strategy hinges on red teams attacking live systems and processes so that the business can better understand its detection and remediation capabilities in light of an actual attack" [26].

Two core parts of the process are threat intelligence and red team assessment, services that according to the requirements of the framework must be carried out by external vendors (one for each or the same for both).

4.2 Structure

The framework structures the assessment in three phases briefly commented by us, that as we expected, are in line with the stages discussed in Chapter 3: Preparation, Testing and Closure [26].

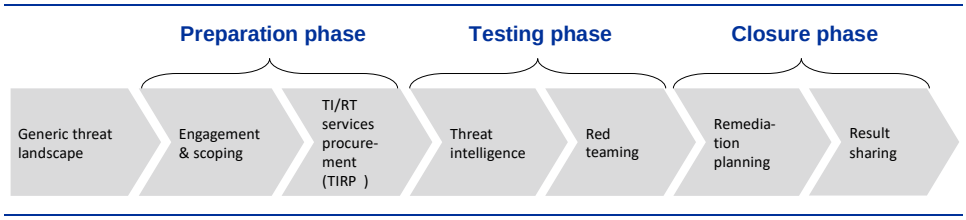

Figure 4.1: TIBER-EU framework structure [27]

[13] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

- **Preparation** - In the preparation stage, red team members define the scope along with the White Team, consisting of the executives of the company requiring the service.
  The rules of engagement and the risks during the entire process are also defined.
- **Testing** - The red team assessment is launched. The red team vendor used common and uncommon tactics and techniques, including its developed software and procedures to attack the system with little to no warning, but within the boundaries of what local and national law allows [26].
- **Closure** - The results part of the project in which the findings are shared inside the EU community aiming to provide better security controls and increase the overall knowledge about cyber threats.

The official paper describing the framework [27] highlights that writing a report and discussing it in a final meeting, including all the stakeholders, is crucial in the Closure phase. That confirms that the red team service is output-driven.

4.3 Cyber Threat Intelligence – Testing: Phase One

The Testing drives business leaders to make informed decisions. Indeed, in this stage through the use of accurate and updated tools, the vendors help clients make informed decisions to correctly identify sensitive assets and therefore invest the cybersecurity budget in countermeasures only where required. The massive quantity of data ingested at this stage is used to create realistic scenarios that will be tested during the red teaming phase. Based on these scenarios, companies can not only test their infrastructure against current threats but also against foreseen threats, anticipated through the analysis of the data collected from different sources. It is evident that cyber threat intelligence combined with red teaming increase considerably the effectiveness of the latter.

Optimization of red teaming activities with cyber threat intelligence

The general purpose of intelligence-led exercises is to mimic the Tactics, Techniques and Procedures (TTPs) of the attacks of real-world opponents. Red team exercises aim to verify if the defensive measures and the existing control systems of an organization are effective. They also test the maturity of the ability to respond and recover in the light of a real attack. Thus, the more information about attacks and threats is available before the attack, the more the test will be worthwhile.

To highlight the importance of intelligence exercises as a requirement/input for red teaming tests, we are going to examine the following two points:

1. **Adversary simulation**
   During the determination of the scope, defining red teaming exercise boundaries, roles, and responsibilities, an intelligence-led approach allows stakeholders to make informed decisions. Cyber threat intelligence outputs foreseen scenarios, analyzing real past events and known facts. These scenarios are added value for red teams since they perform tests as realistic as possible and lastly they improve red team members skills and expertise since they may force them to work with unexpected and unusual TTPs. The exercises not guided by intelligence are based on specific and targeted scenarios that tend to adapt to the strengths of a particular red team.

2. **Threat scenarios development**
   As pointed out in the previous bullet point, intelligence leads to the creation of more accurate scenarios that will be successively tested by red teams, but accuracy is not the unique benefit in scenario development. Cyber threat intelligence accelerates the identification of the techniques and resources adopted by relevant attackers, saving time in the entire testing phase. Therefore, an intelligence-led exercise will be more accurate and efficient than a non-intelligence driven one.

Figure 4.2 shows and briefly describes the steps of threat intelligence [25].
It is not our intention to go through each step in threat intelligence, rather we aim to convey the message that cyber threat intelligence reinforces red teaming.

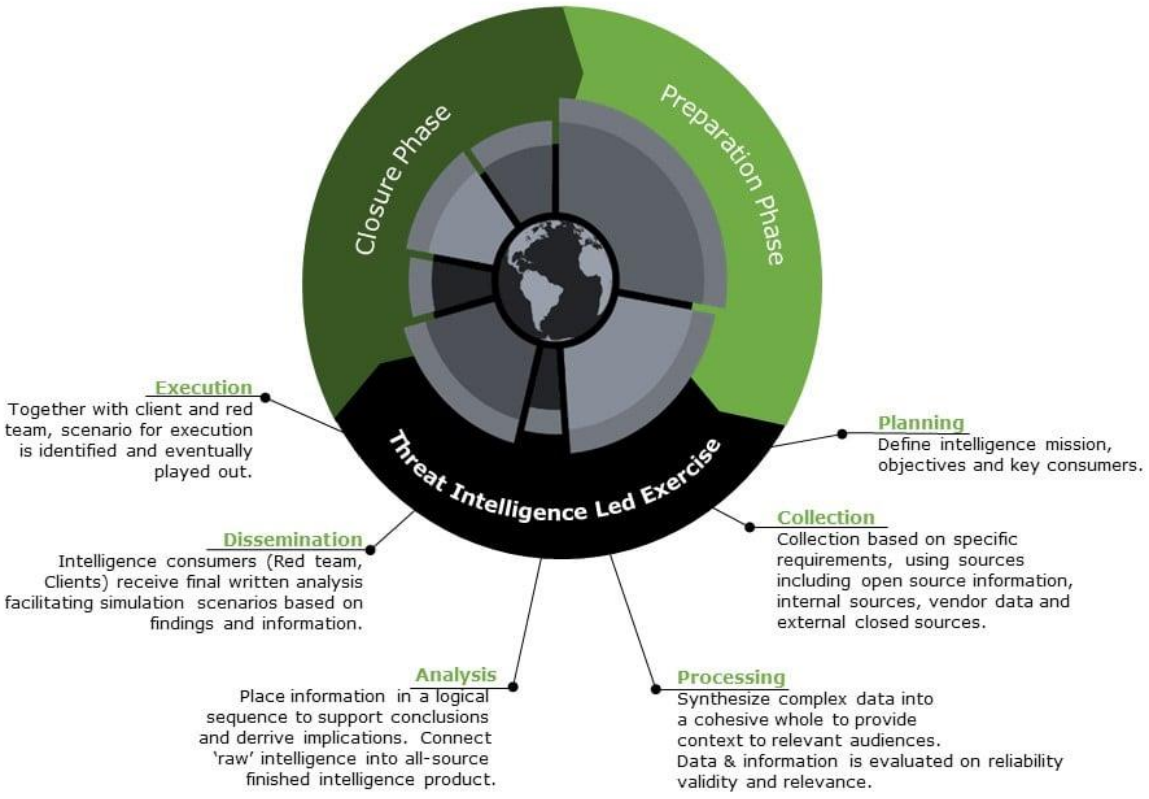

Figure 4.2: Steps of Cyber Threat Intelligence exercise [25]

4.4 Red Teaming – Testing: Phase Two

The second part in Testing stage involves the execution of red team projects. Stakeholders will be informed about how real-world adversaries target companies and to what extent they could gain access to the established objectives. An offensive team, possibly along with a defensive and executive team, assess defensive capabilities, recommending at the end short-term and long-term strategies or products, in order to build more resilient and robust cyber defenses.

It must be noticed that vendors often provide both threat intelligence and red teaming services.

4.5 Benefits

To fulfill today's companies requirements in cybersecurity, frameworks are often used. They allow firms to follow a structured approach in the pursuit of cybersecurity goals. Besides, they are an opportunity for companies to adapt their strategies and follow controlled steps that otherwise they would not have covered without the use of a framework.
New frameworks, such as TIBER and Bank of England's CBEST take an interest in business critical systems and establish adequate cybersecurity baselines.

The frameworks enforce the following points that are at the base of a well-executed red teaming project:

- **Real tactic simulation** - The national authorities who decide to comply with the framework must perform tests guided by a threat intelligence assessment which identifies the TTPs that should be used to attack specific systems of interest [28]. The information gathering process must be a reflection of what a hacker would do when attacking the company.
  Cyber threat intelligence, ethically and legally sourced, includes its benefits: adversary simulation, threat scenarios development, and overall test acceleration (see Section 4.3).
- **Concealment of the simulation** - No personnel except the White Team (executives including CISO) should be warned about the test. The disclosure of this information would hamper the reproduction of a realistic attack scenario.
- **Learned lessons** - The test intends to evaluate the systems of the tested company. However, with a comprehensive report supported by a debriefing we can suppose that the correct countermeasures can be applied later on. But in the end the results pointed out in the report are only indicative and the executives of the client's company will make a business decision on what to implement, when and how, regardless of the results.
- **Biases** - External providers must conduct the assessment, internal providers would be influenced by biases.
- **Industry agnostic** - The framework, though catered for the financial sector, can be considered industry agnostic, allowing for adoption by various other industries.

Though the adoption of the framework is not compulsory, it represents a clear sign of how the attention concerning red teaming projects has increased and how the assessments are considered valuable. That is confirmed by the fact that 2/3 of financial companies in the Netherlands are paying for framework improvements and adoption in the country, according to our interviewed expert. In addition, the topic has been discussed also in the last 43^{o} G7 Italia 2017, our expert highlights, demonstrating a worldwide interest, with the aim to increase worldwide cyber resilience.

In a situation in which formal standards are still not published to regulate red team services, TIBER-EU poses itself as a new standpoint to the subject.

4.6 Challenges

The following challenges regard the framework itself directly, but apply indirectly to the red team service as well:

- **Framework assurance** - As stressed by our expert, if the framework is not followed correctly, just a single flaw could bring economic damages for one company and in that case the entire framework could lose reputation by this situation, diminishing the red teaming image.

- **Voluntary acceptance** - Red team services but also the TIBER-EU framework are not mandatory. Although, only with the widespread adoption we can give solidity to the red teaming worldwide image and longevity to the framework which makes use of it.
- **Law Requirements** - Each red team assessment must be compliant with the current laws. Although it can seem only a marginal problem in some circumstances, this can hinder the test. For instance, German Criminal Code Section 202(c) establishes very stringent requirements on the conduct in this matter. This means that also the test will reflect the strict requirements, moving away from the reality in which hackers do not take laws into account in pursuing their profits when committing cybercrimes.

5 Interview process

In this chapter we describe how we performed the interviews. In Section 5.1 we define a semi-structured interview approach that we used as base for all the interviews. The red team survey population and interviews are presented in Sections 5.2 and 5.3, while the clients survey population and interviews are specified in Section 5.4 and 5.5.
During the interview, additional questions were asked, which were not in the questionnaire, based on answers given during the interview.

5.1 Semi-structured interview approach

The method adopted for the interviews, in our explorative approach, is a semi-structured questionnaire: a combination of closed and mainly open questions (inspired by the work carried out by Moore [1]).

Other methods like Delphi are adopted when the information at the beginning of the process is scarce, but even if a more precise result could have been obtained, more interview sessions would have been required. The utilization of a website could have eased the interaction between interviewee and interviewer, but it would have asked for extreme dedication from executives and red teamers, and an amount of time that owing to their hectic life would have hampered the quality of the answers.

A semi-structured methodology brings advantages and disadvantages. Among the advantages, there is the possibility for the researcher to acquire unexpected data, not available through closed questions, permitting the analysis of new uncovered material. Another advantage is the personal reaction of each interview subject to the matter. A structured methodology would not have left space for personal opinions, feeling and strategies in securing the organization.
One definite drawback is the comparison of answers. Even though our intent was to interview a large number of executives across the private sector, the interviews are constituted by unstructured portions that are consinstently personal, so our findings have to be interpreted as explorative. Nevertheless, we claim that the interview approach we adopted is the most appropriate tool for investigating these advanced issues. We hope that many of the results we report can be merged with other future findings. This report is expected to be a starting point for future researches possibly applying structured interviews and therefore obtaining more comparable data.

5.2 Red team survey population

Aiming to inspect the red teaming process and attributes from a different angle, a group of stakeholders of the service was interviewed: red team project managers involved in the service in its entirety, from the selling phase until the wrapping phase, and red team operators, or rather, those who execute the service, and collaborate to the correct development of the scope and report.

Therefore, I recruited a group of red teamers from the vendor, four specialists of red teaming, both project managers of the service and red team members (see Table 5.1). The specialists interviewed are employees of the company Deloitte Netherlands which assisted in this dissertation. The sample of red teamers has been selected based on their availability and my convenience (e.g., based on their experience and their job tasks).

Type of Participant	Number of Participants
Red team project managers	1
Red team members	2
Both red team project managers and members	1
Total	**4**

Table 5.1: Red team population interviewed in this research

5.3 Red team interviews

The questionnaire has been answered in its entirety in all the sessions.
The cluster of red teamers has been interviewed individually in person at the Deloitte offices in Amsterdam, and the interview duration varied between 30 minutes up to 1 hour.

Questions for **project managers of the service** are split into seven categories: general questions, purchase phase, red teaming attack, tools and processes, report phase, benefits and improvements.
The general questions are designed to gather information about the overall red teaming process, for example how it differs from penetration testing, what are its phases, what are the customers and how are the teams structured.
Purchase phase questions delve into the purchase stage. They provide information such as how a company buys the service and how much it costs.
Red teaming attack questions focus on aspects like how long it takes, how the scope is defined and what the security properties (see Section 6.2.3) and scope tested are.
Tools and processes questions concerned the software and steps utilized during the entire project, while the report phase questions delved into the creation of the report and its goals.
At the end of the interview, we asked about the benefits of red teaming and possible further improvements based on the experience and perceptions of the interviewee.
The full list of questions can be found in Appendix C.

Questions for **red team members** are not split into categories. The interviews of this group were quite open, since we pushed the interviewee to contribute to the research, giving unexpected details and data regarding red teaming as a whole.
The goal of these interviews was to get an insight of red teaming from a member perspective, validating or elaborating the results acquired by interviewing the project managers of the service.
Appendix D contains the full list of questions in the questionnaire.

5.4 Clients survey population

I recruited a group of four CISOs for this study (the number of participants has been reached jointly with Deloitte, sponsor of the study, which facilitated the connection with them). The interviewees are Deloitte clients (see Table 5.2).
All the participants have been selected from the private sector. A couple of past similar (in style) researches have demonstrated that including public and defense sector [29] modify the outcome of the analysis negatively since both sectors work differently compared to the private sector. It is preferable for data comparison to focus only on one sector, in this report the private sector.

The industries are picked up from different branches: transportation, finance and insurance. The typology depends on the network of companies contacted and the willingness of the executives to participate.
The participants that have been contacted are members of national Dutch companies but also foreign ones. Only people who work for Dutch companies accepted our invitation.

Country	Sector	Industry	Number of Participants
Netherlands	Private	Transportation	1
Netherlands	Private	Finance	1
Netherlands	Private	Finance	1
Netherlands and abroad	Private	Insurance	1
Total	**1**	**3**	**4**

Table 5.2: CISOs population

5.5 Clients interviews

The group of clients has been interviewed individually in person at the companies' offices, and the duration of the interviews varied between 30 minutes up to 1 hour.
The interviewees have answered all the questions in the questionnaire.
For confidentiality concerns, at the beginning of the interviews, the interlocutors signed a consent form. That form stressed that the information collected, including sensitive data, is presented in an anonymous fashion, with respect to company's regulations. In addition, the interviewee had the right to interrupt the conversation at any time or skip any question.

Questions were split into three categories: grounding questions, macro-level, and micro-level questions.
The grounding questions have been designed to gather information about the subject's background and role within the organization.
Macro-level questions focused on how red teaming is perceived, managed and prioritized in general.
Micro-level questions delved into the experience of a recent red team assessment. We asked about the decision-making process, their satisfaction with available information, and any link to the metrics used in prioritizing threats.
The Appendix B contains the full list of questions in the questionnaire.

6 Red teaming from a vendor perspective

In this chapter we examine how red teaming is perceived and performed by red teamers, trying to understand why, how, and when some steps are taken, focusing mainly on figuring out the red team member job and tasks. Section 6.1 briefly describes the initial purchase stage of red teaming. The red team project overview is illustrated in Section 6.2. Section 6.3 proposes service improvements from a vendor perspective.
In Appendix A an overview of the report written at the end of red team projects is provided.

To facilitate the reading of this chapter, the results obtained interviewing red teamers are presented in a narrative way throughout all the sections. The choice of a narrative style derives from the equivalent explanations of the interviewees, thus is not necessary express a comparison. Therefore, the statements of each section are not personal conclusions of the author himself but derive from the answers to the interviews taken during our research.

6.1 Purchase phase

The purchase phase is where clients or possible new clients contact vendors asking for RT.
In this phase, the vendor provides the proposal in which an overview is given of what is expected to happen during the exercise. No other documents are given to the client.

Often large companies buy the service since they can afford the price. However, the service can be sold to every type of company, also the smallest ones. The service can be tailored for small or medium companies' needs, analyzing small features (i.e., small scenario).
Although, also the healthcare sector, because of the grown awareness in the security domain (especially after GDPR), is getting interested in the topic, the clients, worried about the consequences of an attack, are mainly from the financial sector, since they are (potential) targets of many cyber criminals.

The costs of the service, clearly part of this phase, depend on many factors; like scope, duration and technologies/staff involved in the test.

6.2 Red team project overview

6.2.1 Scoping phase

Once the scope is defined jointly with the client (otherwise it would be non-beneficial since clients need to focus only on some assets), the red team members involved in the project have their own briefing session in which they get an idea of what will be the next steps to perform a successful test.
In the scoping phase, aspects like liability are also considered, since testing could damage the client's network, even if this is unlikely to happen because precautions are taken before starting attacks, like reducing exploits impact when used.

6.2.2 Project duration

In the project/testing phase that generally **lasts 1 week up to 3 months**, red team also considers the attacker's potential profit, since some cybercrimes can be only committed if enough resources are available. In a rare event, however, some project can last up to 6 months or be as short as 2 days.
In Figure 6.1 the red team project duration, for each category of projects, is expressed in weeks as form of a bar chart.

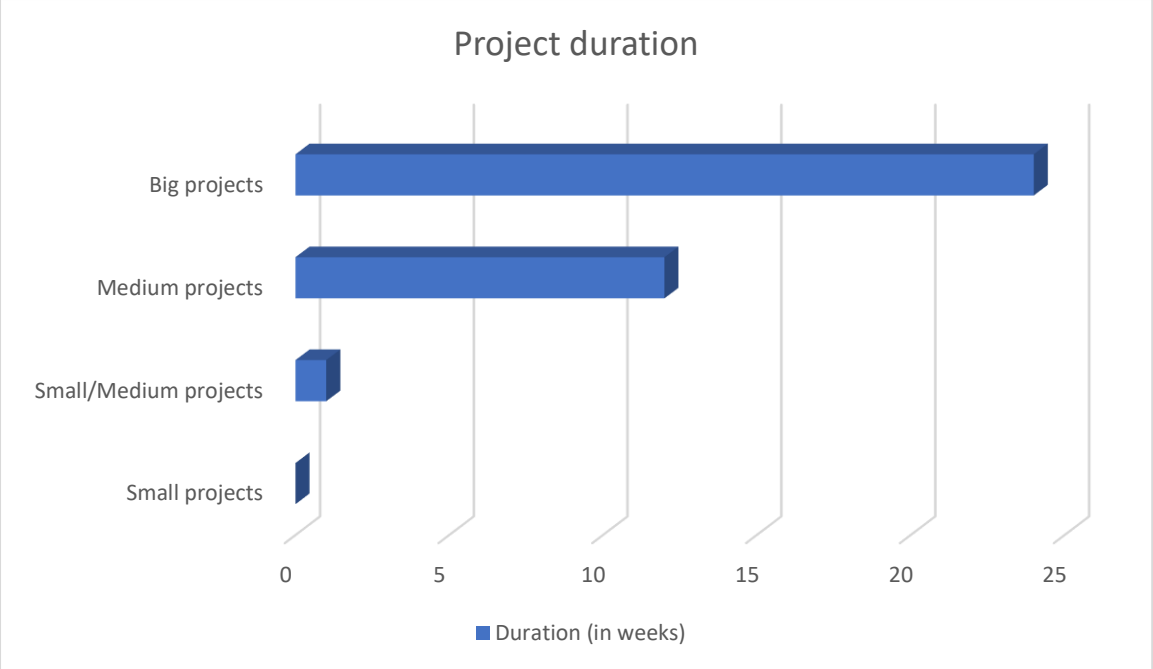

Figure 6.1: Red team projects duration

6.2.3 Properties and areas tested

The properties tested are depicted in the security sphere in Figure 6.2, widely known as CIA triad, but some considerations are necessary.

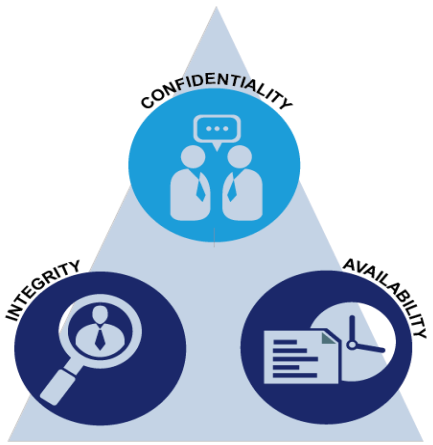

Figure 6.2: CIA triad - security properties [30]

Denial of service attacks are not performed, but the red team only shows that they are feasible, since carrying them out could undermine the client's company availability property. Accountability and non-repudiation (elements of the integrity property) are touched only if specifically required by the client, the latter specifically with internal phishing or person impersonation.
Below a list is presented of all areas that can be tested during a red team test [19]. Evidently, not all the points are tested during each project, but if necessary red team operators are trained to address all of them.

Internet Security
- Network Surveying
- Port Scanning
- System Identification
- Services Identification
- Vulnerability Research
- Internet Application Testing
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Trusted Systems Testing
- Password Cracking
- Denial of Service Testing
- Containment Measures Testing

Information Security
- Document Grinding
- Competitive Intelligence Scouting
- Privacy Review

Social Engineering
- Request Testing
- Guided Suggestion Testing
- Trust Testing

Wireless Security
- Wireless Network Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

Communications Security
- PBX Testing
- Voicemail Testing
- FAX Review
- Modem Testing

Physical Security
- Access Controls Testing
- Perimeter Review
- Monitoring Review
- Alarm Response Testing
- Location Review
- Environment Review

6.2.4 Team structure

The team is formed each time according to the expertise of the red team operators.
Solo red teaming is a bad idea, since the risk of overlooking stuff is high. A team works usually in pairs not necessarily in the same room, but also virtually on a global scale. They do not do that alone. Sometimes they could work temporarily alone, but definitely in delicate situations where one red team operator gains administrator privileges in a client's machine or transfers money then team members work for sure together, continually sharing all the actions taken, and in that case even including the client.

All members of the red team are kept up-to-date during all the test with meetings, including briefing and debriefing. Client representatives, corresponding to the white team (i.e., those who define the rules of the game), are also kept up-to-date (usually) with daily meetings. They are also asked if they noticed anything abnormal (i.e., out of scope).

6.2.5 Steps taken

Figure 6.3: Red team operations attack lifecycle [31]

The red team is trained with red teaming guidelines which in some ways define amongst others, the duty of specifying which steps need to be taken and when. Although these guidelines are developed,

like the one written by the U.K. MoD [4], the red team does not follow linear steps or flowcharts. On the contrary, they execute their actions according to their own experience. Considering the diversity of situations that they could face, a flowchart is not suitable for red teaming, since it would turn into a massive tree with many flaws (not covering all the possible scenarios). Instead, they created a framework, like an empty flowchart, where they define the structure but not the commands and precise instructions.
They do not use the Open-Source Security Testing Methodology Manual[14] (OSSTMM) either, which is adopted by penetration testers.

In Figure 6.3 a cyber kill chain is depicted, which shows the red team operation attack lifecycle. A cyber kill chain describes the typical steps taken by attackers to penetrate an organization's networks and systems. Other kill chains have been proposed[15] [16].
Even if the starting point changes in relation to project requirements, usually red teaming starts with the **access to the client network** with a provided laptop with least privileges account, assuming somebody is already in the network like a malicious unhappy employee. Of course, if clients ask for external testing they start with phishing or a physical attack or the exploitation of a vulnerability in the external perimeter (e.g., vulnerable company's webserver).
OSINT (see Section 3.2) adopted for gathering info about the company from public sources, is always part of the initial stage of the process, the **reconnaissance phase,** especially pursuing phishing and physical scenarios.
Once inside the network, the red team enumerates specific services running along with their version (e.g., hostnames, the operating system running and MAC addresses), which give the red team a good chance for lateral movement or privilege escalation. Few versions could be vulnerable to known exploits (available also online[17]) allowing the team to **establish persistence** inside the systems (e.g., remote shells).

At this point of the test, employees are not aware of the running test, thus if caught scanning the network, the red team would lose access to the company laptop. Usually only senior managers or CISOs, members of the white team, are informed about the running test. Indeed red teaming is meant to stay undetected, and employee are supposed to respond to ordinary attacks, not planned. In general, the red team takes all the necessary steps to reach the objectives defined in the scoping phase, and if they get caught during the service they start again from the last point where the defensive team did not seem them.

Once the network has been enumerated with the goal to **escalate privileges,** the red team operators indeed perform actions to obtain administrator powers by pursuing the weakest link, in order to achieve the project objectives. This is often achieved via lateral movement tactic, i.e., moving to another machine in the network with the same privileges but with different accounts (e.g., domain admin), so getting more privileges. The use of Trojans or passing the hash[18] techniques, can be handy for this approach.
After **administrator privileges** are obtained, the red team is able to perform any kind of action, like

[14] http://www.isecom.org/osstmm.html
[15]Lockheed Martin – Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[16] Microsoft Kill Chain - https://www.microsoft.com/security/blog/2016/11/28/disrupting-the-kill-chain/
[17] Famous exploits database - https://www.exploit-db.com/
[18] Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case [34].

inserting a backdoor or exfiltrating information. Therefore, the assessment can continue, gathering information as admin, at this point, and therefore with the new acquired data compromise new machines, but only if necessary to achieve the objectives.

Only when **the objectives are achieved** the "game ends." Admin privileges are not business-relevant enough. The findings need to show that they can be used to steal Personal Identifiable Information (PII), IP addresses, money or other assets of the company. Failure to make a business impact fails to answer the "so what" question that the business inevitably will ask before approving budget to fix issues. The board of executives will not understand the potential impact that admin privileges can have, or they will implement additional measures that protect their crown jewels. Therefore, a good red team will strive to make this business impact an inescapable fact.

A red team does not sign a contract for patching like security researchers. Instead once they find a vulnerability, the company agrees to fix it before public disclosure. Red teams do not publicly disclose information gathered about the company. They are privately contracted and all the results are confidential. Also, all the above project steps described in this section are performed with commercial/professional but also personal tools depending on the scenario. For instance, Deloitte red team members implemented a tool called "Go Dark" that lowers the noise of the red team systems throughout the test.

6.2.6 Role of client blue team

The contact with the blue team strictly depends on the red team project purposes. If the client require to train the blue team during the process, then it is aware of what is happening and it is in constant connection with red team. Otherwise, the blue team is informed only at the end of the service. The red team has a list of indicators of compromise that will be checked with employees. In other words, the red team logs every step and actions taken, and at the end, they compare their logs with what the blue team found. Then, workshops or Purple team involvement could follow (see Section 3.2).

6.2.7 Role of Cyber Threat Intelligence

Clients who require red team services do not gain any knowledge about the probability of threats from previously observed attacks by the vendors. Only through cyber threat intelligence clients can predict future risks. So far, the service is mainly used inside the TIBER-EU framework (see Section 4.3).

6.3 Service improvements from a vendor perspective

In this section we propose possible red teaming improvements according to red teamers suggestions, beliefs and opinions, collected throughout the interviews.

Improvements

By interviewing red teamers we collected some food for thoughts and considerations that could improve the service in the near future.
We list them below, grouped into three categories: View, Automation, and Time Efficiency.

- View

  - Visualization of red teaming actions. Use monitoring dashboards based on the input of red teaming engagements to visualize red teaming engagements automatically and potentially in real-time.
  - Quantification and benchmarking of RT. Defining a methodology to compare red team results in different companies, with different engagements and in different industries.

- Automation
  - Automation of red team decision making. Within the engagements, red teams tend to perform similar steps during their attacks based on the things that they see. For learning purposes and for performing engagements, it would be beneficial to automate the decision making at least up to a certain extent.

- Time Efficiency
  - Antivirus evasion. Red teams spend a lot of time bypassing the client specific AV, which ultimately does not add a lot of value for the client. In the future, they expect to have to bypass this step by maybe whitelisting it or avoiding workstation/laptop access during red teaming as a whole.
  - Successful phishing. Some clients are really focused on a successful phishing exercise. However, phishing will always be possible one way or another, therefore spending a lot of time for a working scenario is not efficient and in the future the red teams expect to bypass this.
  - Shortcuts in the process. In the objectives definitions, usually red team asks clients: "Where are your crown jewels[19]?" or "What kind of data should we try to reach?". The answer could be: "Database with credit card details".
    In that case, clients could already give the server name of the database because it would speed up a lot the vendor assessment.

In short, red team vendors seek a way to quantify red teaming benefits in terms of return on security investment. Indeed, they believe the service is seen, so far, as an expense by the clients, who do not perceive the economic profits originating from the use of the service.

[19] Paramount assets necessary for the correct functioning of the primary company business activities.

7 Clients interviews

In this chapter, the answers collected during the interviews of a group of CISOs, clients of Deloitte, are presented and elaborated. In Section 7.1, we discuss what the executives think about RT. In Section 7.2 we give a picture of the level of cybersecurity of the organizations interviewed, briefly analyzing how they identify their threats and wondering if they have enough information about doing it. Section 7.3 shows issues in cybersecurity investments and discusses if RT can be a remedy to those issues. Section 7.4 gives an insight of RT from a client perspective analyzing, for instance, why they ask for the service, what they assess, and when they test their infrastructure. Section 7.5 aims to assert if RT reduces uncertainty. Section 7.6 analyzes if the companies' cybersecurity increased after RT and training. Lastly, in Section 7.7 strong and weak points of past assessments are presented, according to clients perceptions.

The sentences in italics correspond to literal answers given by the interviewees. That contributes to bring out the different opinions of the CISOs differently from Chapter 6, where red teamers' answers lead to the same conclusions.

7.1 How Companies Perceive Red Teaming

CISOs of the companies interviewed perceive RT as a **wake-up call**: *RT tests the real security. You step out from your comfort zone or the feeling that nothing can happen to you. Then you really get to know your vulnerabilities that can be used by hackers in real life.*
CISOs, before red teaming, applied countermeasures in the borders of their own network, improved the cyber resilience of their company and also the governance. That gave them a sense of comfort and confidence in the cybersecurity of their own company. However, to verify their beliefs they asked for RT and they discovered that there were unexpected vulnerabilities. *You will always find a gap, something that you didn't think about, it's always the case. RT tests the real security.*

RT is also considered **indisputable** since *you can assess from non-biased perspectives what is your state of security.*

RT answers to we have all these kind of security measures but how good do they work? It tests a **real-world scenario** that needs to fit the risk profile of the company (i.e., their crown jewels and their threat model) otherwise it would be less useful. For example, the same company could face different cyber threats if located in another country. The tests are performed using the **latest techniques**, *RT keeps the pace with nowadays techniques, as hackers do.*

In addition, RT is considered as a **versatile** pyramid of tests starting with vulnerability scanning moving up to social engineering where RT can be done on one single part/feature of the organization (people, process or a system) but also on a full organization scale. *And in case of an institution, this is when TIBER comes in to take all the surface of an institution including third parties, trying to emulate threat actors.*

7.2 Companies Cybersecurity Level

All the CISOs interviewed believe they have a good level of security, proper/mature level, but are aware that it can always be improved. One of them reported that he is satisfied with the

cybersecurity they have, but they lack personnel, therefore they need to find a balance, trying to improve the company's cybersecurity at a faster pace. *It's only a matter of personnel and budget.*

Then they do not perceive RT as a solution for a bad cybersecurity situation. They solve bad situations in advance before asking for RT.

Thereby RT cannot be identified as the absolute solution, rather it is carried out to verify the effective cybersecurity of the company *itself* or even a recently acquired company abroad. *RT is used to verify and make sure you're really up-to-date.*

The service indirectly increases the company's cybersecurity level. Indeed, it is used as a measurement tool for the real security of the organization, showing what are the gaps that companies need to address to increase their cybersecurity level.
It helps CISOs visualize where they need to focus their attention, changing their mindset, figuring out in which areas they need to invest more.

7.2.1 How do you identify which threats are most important and prioritize them accordingly?

The companies perform their crown jewels analysis, usually annually. First, they need to identify the business units in their organizations and where the biggest risk is, which strictly depends on the value chain of the companies. Therefore, the involvement of the business board of directors, interviewing them, is necessary to understand which assets are that could cause the biggest impact on the organization in case of failure. In addition, a correct use of the risk assessment matrix is essential.

Also, a "worst case" scenario tabletop exercise that maps risks to external threats is in some cases adopted.

More mature companies have their own Security Operation Center (SOC) and use many threat intelligence reports, in addition to a control framework for their governance and outside sources (like white papers from consultant vendors). Furthermore, they identify with their cyber intelligence team groups of hackers from hacktivists, state-sponsored or organized crime groups. Most of the material is public, but they also share private information with other organizations.

In some cases, in this identification process of threats, RT can assist CISOs to focus on what they need to do first, i.e., the main areas that need to be protected.

7.2.2 Do they have enough information for managing overall cyber risks?

All the CISOs interviewed report that they have adequate information about and they are satisfied with the information that they have, where all the teams collaborate, also thanks to proper security governance frameworks put in place.

More mature companies are even more confident than less mature ones, since they have continuous communication between their SOC and business board of directors.
For those who use cyber intelligence, a margin of improvement exists and this is confirmed by the fact that the market for cyber intelligence is only 5-10 years old and all the experts are from intelligence services because it is difficult to find true experts of the subject in other private sectors. *You need to have a lot of expertise to know what you're buying.*

7.3 Cybersecurity Investments

7.3.1 Are any evidence or metrics used in making cyber investment decisions?

None of the CISOs interviewed use metrics for making cyber investment decisions.
Ideally, you have cyber incidents and metrics about the subjects, then you implement countermeasures, and then you see a decrease in that. Anyway, the ideal approach in making cyber investment decisions is hard because it requires that all metrics are defined.
CISOs do not utilize metrics since they perceive cybersecurity as something not tangible, therefore not everything can be quantified. *Cybersecurity is also about feelings and intuitions. It's not always directly quantifiable.*

Although they do not present any sort of metric to the business executives of the company, CISOs do not have any issues in asking for investments, since the executives trust them and accept their requests.

7.3.2 ROSI: Relationship with Red Team Services

The business board of directors always asks "what is my ROSI?", but it is hard to answer that question. Not everything can be quantified, especially keeping in mind the worst case scenario.

The majority of CISOs interviewed do not use ROSI; one of them did not know what it was.
One company tried to use it as much as possible but not in relation to RT. Instead, for what concerns RT, they calculate gaps identified during the assessment, trying to understand the budget needed to fill the gaps.

7.3.3 Are there any Changes in Investment after Red Teaming services?

We asked the interviewees if they change the way they invest after RT, verifying if the service improves also the cybersecurity investments.

The CISOs confirmed that the service changed the roadmap for cybersecurity investments, modifying the priorities and adding or postponing projects (rarely removing, for redundancy reasons). *The output of the test was an input for our security program.*

A couple of executives stated that:

- *It helps prioritize all the high risks elements of the company, so prioritizing the countermeasures.*
- *After the service, we changed our roadmap (priorities and projects), therefore our cybersecurity investments.*

Moreover, even if the service does not provide any evidence-based measures (e.g., number of attacks that can be prevented), the results justify the request of new budget to the board of directors. *It's easier to ask for more budget when you show the results of RT.*

Then, we asked how they know that their new solutions are working or not, with reference to RT, and the answer was precise: *we ask for another red teaming. We retest to verify if it is working or not.*

7.3.4 Are you able to Spend Money more Accurately after red teaming services?

The group of CISOs interviewed argue that they are able to spend money more accurately after the tests, due to the reduction of uncertainty.
Indeed, they are more confident in the prioritization of projects (cyber investments) so they can spend money more accurately, saving budget. *With RT you understand better what your weaknesses are and then you start applying countermeasures faster. There you have an economic return.*

A couple of CISOs admitted having issues with investments. They need to think about a lot of projects but RT helps them focus. Therefore, they can postpone some countermeasures which are less necessary at that moment, spending money more accurately and in certain cases saving budget.

We also asked our group of CISOs interviewed what they think about their peers that do not execute red team assessments, wondering if these peers spend too much on cybersecurity investments.
The interviewees believe that RT is still a service that only a few companies request and m*ost of the companies have a checkbox mentality (e.g., buy a new firewall or intrusion detection system) to defend against attacks.*
Our executives wonder why the peers buy all those products considering RT as a solution to focus only on the acquisition of the necessary countermeasures, saving costs. *RT reduces costs delaying projects* (CISOs can postpone less urgent tasks) *and focusing on the most important ones.*

7.4 Red Teaming: Why, Who, Where, What, When, How

7.4.1 Red teaming: Why CISOs ask for red teaming?

In this subsection, we analyze two answers received by two CISOs interviewed, who replied to the related question (title of this subsection):

- **CISO 1** – requested red team assessments after getting in touch with the TIBER-EU framework. The framework allowed him to discover RT, since before that RT was only a vague concept to him.
- **CISO 2** – while in this case RT was already performed before TIBER-EU framework spread, many other reasons led to the request of the service. Although, one of them stands out from the others: the closure of the gap between policy making and operations.
  Usually, policy makers don't know operations well enough to write rules and regulations and how to do that properly and operationally. On the other hand, operators (people actually working in the company) *cannot write rules because that's not their job.*
  So there's always a gap between them, also because the operational part is continuous but regulations are written every now and then. Hence, there's a mismatch, which leads to vulnerabilities.
  As a result, in order to understand the vulnerabilities between the policy and operational gap, RT is performed. Indeed, it challenges your own confidence and your own organizational structure.

7.4.2 Red Teaming: Provider selection

RT has an immature market so far, and only a few vendors offer the service. We asked our group of interviewed how they pick among these competitors.

Although the price is one important factor of choice, it is not the main one. The biggest factor is the

previous experience with vendors and the quality of their services, sometimes confirmed after conversations with peers. *Price is important but quality comes first.*
Clients ask for the service from companies that they trust, bearing in mind that if a failure occurs during the assessment of the infrastructure, they could potentially be subjected to economic and reputational damage, disclosing sensitive data or interrupting vital functions for the business of the company.
The quality, the maturity and the level of confidence that you feel with the guys during the test is the main factor of choice. You want them to have experience, good references, good quality assurance of the work and good reporting. You need to trust the vendor because they know your vulnerabilities.

The superiority of technology is not a driver in the choice since *many tools can be found online basically for free.*

Lastly, CISOs do not base their choice on reports published by research and advisory firms like Gartner[20] or Forrester[21], since they are skeptical about the truthfulness of the data published. Furthermore, those research and advisory firms cannot help with what concerns RT because they do not really know the teams and their experience. *We are not talking about technology but about people and their competences.*
Gartner evaluates a technology that works wherever you are but with a service is different. A red team in the Netherlands could act differently compared to another team of the same provider in the USA.

Sometimes for sake of comparison different providers are contacted, evaluating who performs better compared to the others.

7.4.3 Red Teaming: Assets tested

For which assets companies ask for RT?
RT always focuses on the vital parts of the companies, strategic and critical assets (i.e., their crown jewels), taking into consideration the worst case scenarios.
RT is a combination of logical and physical attacks that test a few critical functions of a company.

More mature companies, beforehand in the TIBER engagements (i.e., the tests performed following the framework) and with their cyber intelligence team, create a scoping document in which the critical economic functions are described, which are their crown jewels. Hence, they put a flag on those critical functions and red team members have the objective to reach these flags, so testing their defenses.

7.4.4 Red Teaming: What is the most important part of the assessment?

During the interviews, we wanted to verify if the CISOs' opinions are in line with our research, which considers the output of the test (i.e., the report) the most valuable part of the assessment.

Surprisingly, all of them except one consider the execution phase as the most important part.
They believe that the white team involved during the process knows the findings before the report is published. They also believe that the personnel in charge of the defense of the company from

[20] https://www.gartner.com/en
[21] https://go.forrester.com/

cyberattacks enhances their skills during the process and not after the discussion of the report.
One client also expressed that the provider could spend less time in the report phase: *the red team spends too much energy writing the report, energy which could be applied in other parts of the process.*

Instead, the client that agrees with our research refers that RT is output-driven and that the report needs to be of high quality, affirming that *the blue team (if the organization has one) learns a lot with the report.*

7.4.5 Red Teaming: When the service is requested

The majority of the clients interviewed required RT at least twice but no more than four times, so far.

Usually, RT is performed annually or when they want to verify something specific, especially if the risk profile of the company changes. More attack-targets clients perform RT every few months or maybe twice per year. The most severe RT (i.e., testing many aspects if not the whole organization) are performed approximately every two years.

We asked the clients how the vendor can help them build a stable relationship in the assessment of the security of their networks in a long term perspective.
All of them have already a stable relationship with the providers and plans for the future years.

A couple of points emerged after the interviews:

- Further information about other services provided, like a bullet list of one page or flyer, would be useful for future projects, because they do not have a concrete idea of the provider's services.
- The provider does not assist the client in the analysis of the risk profile of the company in the months after RT, even if the same risk for attacks could change.
  The provider should check if the countermeasures and the roadmap of the cybersecurity investments suggested after the assessment are still valid after a couple of months.
  Indeed, since the client modifies the roadmap according to the findings, it is essential that the investments are still relevant after months in the light of new/different threats.

7.4.6 Red Teaming: How it is perceived in relation to other defense strategies

RT is adopted by the clients as part of a defense strategy, that is to say, that many other countermeasures are in place and other services are performed along with RT. Thus, RT is seen as *part of a continuous engine of improvements.*

The involvement of the employees and also customers, increasing their awareness is part of the defense strategy. Since RT embraces social engineering (as we stated previously in Section 3.4), the service can be an excellent tool to test employees of all the departments and increase their awareness about cyberattacks.
That is testified by one of the CISOs, who would like to ask the provider to include phishing attacks in the annual red team tests, increasing their awareness and therefore preventing attacks: *you can have all the security measures in place, but if you have only one person that intentionally or not compromises the system, you are vulnerable.*

7.5 Is Uncertainty about Risks and Attack Vectors Diminished after the whole Red Team Service?

Uncertainty has a pivotal role in our research, following our objectives. Therefore, we asked questions to the clients aiming to figure out if uncertainty about risks and attack vectors diminished after the red team test.

The clients do not get a clearer idea about the most sensitive assets to protect since they know them already before the test. Indeed, RT is not meant for that, since it tests critical assets and does not find new ones.
Nonetheless, it reduces uncertainty, as stated at the beginning of our research, especially if combined with cyber threat intelligence.
CISOs know what they should do: *uncertainty is gone. It gives confidence and more awareness about prioritization.*

Based on the findings, they know which investments need more attention and which ones can be postponed. *They assessed the infrastructure site but also applications and that gave us a lot of information on what to prioritize in the roadmap. We also used the output of RT to make the roadmap more concrete due to the real evidence.*

The results of RT showed us the long term goals, adding stuff to the wish list.

In addition, one of the CISOs argues that uncertainty not only decreases for executives in charge of the security developing a roadmap of cyber-investments, but also for the other executives responsible for the business of the company.

7.6 Is Company's Cybersecurity Level Increased after Red Teaming and Training?

Based on the objectives of our research, one of the goals of the interviews was to figure out if the company's cybersecurity level increased after the red team assessment.
CISOs believe that red teaming increases cybersecurity level although a couple of interviewees stated that this is the case only if some requirements are satisfied:

- **Proper management of the findings** - *RT helps you show where you are. Only if you then take advantage of that information properly, then your cybersecurity level increases. If you don't understand that properly, don't have budget nor experts, your cybersecurity level doesn't increase.*
- **Continuous process** - *Only if RT is a continuous process the cybersecurity level can increase.*

We also asked the interviewees if they perform some training (e.g., hacking workshops or phishing campaigns) for the company's personnel at the end of the assessment, which is considered by us as a factor for cybersecurity improvements.
The actual situation emerged from the interviews is that training is not always requested after the assessment, and not always provided by the RT vendor.
In the case of blue team presence inside the company, training sessions could be hosted only if needed and if the blue team was unaware of the attacks.
However, they can contact other providers for training, which can be assisted by the CISO expertise, considering them more specialized in coaching than the RT vendor.

A CISO of a company interviewed that does not have a blue team but people working on security and external companies monitoring the network events asked for training, considering all the employees as a blue team. Indeed, they tested them with phishing campaigns to increase their awareness about the subject and workshop to increase their skills. B*ecause the threats evolve (exploits, vulnerabilities, ...,) but people can keep the idea of denying all and accept only one thing. It's not only awareness but a mindset. Shaped also thanks to training.*

In conclusion, CISOs believe that in general RT increases the cybersecurity level, either alone or combined with training. In particular, it improves detection and response to cyberattacks: *it helps detect attacks and take appropriate countermeasures as soon as possible, it also improves the response to real attacks.*
In addition, RT also reduces the impact of the attacks and prevent them, in case countermeasures are correctly applied: *it reduces the impact of the attacks but also prevents them if you fix a vulnerability.*

7.7 Assessments evaluation

7.7.1 Strong points

Our intention is not to provide a list of all the benefits of red teaming but only to point out some aspects considered positive by the clients, based on their recent experiences:

- **Client satisfaction** - clients were very enthusiastic about the test. *Nothing to be improved. The provider was very helpful. A lot of contact with the client. Then, the vulnerabilities were explained in a not too technical way.*
- **Blue team involvement since the beginning** - *Last service was more helpful than the ones before because the blue team was more involved. This time we informed the blue team in advance of the attacks. Instead, in the first time only the white team was aware.*
- **Client 1: Enlightening outside perspective** - *Really helpful: raised attention on senior management level, gave results that helped with awareness programs, and tested IT specialists getting an outside perspective. To notice that they weren't aware of the attack. If you warn the blue team upfront it's not RT. Because it doesn't really emulate a cyberattack.*
- **Client 2: Enlightening outside perspective** - *Gave an insight that we didn't expect, showing a lack of monitoring on the internal network.*
- **Blue team response and countermeasures improved** - *Compared to the previous assessments, the blue team responded more efficiently and the new countermeasures applied worked, meaning an overall improvement in security.*

7.7.2 Weak points

Our intention is not to provide a list of all the disadvantages of red teaming but only to point out some aspects considered negative or lacking by the clients in their recent tests:

- **Report evaluation and workshop** - The clients in the future want to evaluate the report together with the blue team and the red team. They also would like to prepare workshops together with the red team after the service.
- **Worldwide competition missing** - *Although the RT market is a bit more mature than the Cyber Intelligence market, healthy competition and proper experience are missing. There are a few leading parties and they get all the exciting engagements, where they keep their experience. So it's really hard for new companies to penetrate the market.*

- **Business impact too technical** - *The business impact is described in the report but in a too technical way not taking into consideration the company's value chain. It's important when talking with board management. They trust us and they give us budget, but would be important for us and for other companies that all the executives understand the business impacts caused by the attacks. In our case, we have a high trust level with the board of directors but perhaps for other companies is different, making request of budget more arduous.*

8 Conclusions

This chapter provides the conclusions of our work. We describe the general conclusions (Section 8.1), reflect on the objectives of this research (Section 8.2) and identify possible future work (Section 8.3). In Section 8.4 we discuss our research limitations.

8.1 General conclusions

In the current scenario in which companies continuously struggle to find a proper balance between business and cybersecurity, red teaming stands out, demonstrating itself as a vector to improve investments in cybersecurity. Indeed, according to the data collected throughout the interviews, red teaming helps CISOs in prioritization, showing which are the projects that need immediate attention and reduce uncertainty in investments.

The service not only facilitates CISOs to define a more accurate and efficient roadmap of investments, saving costs, but it also increases the overall cybersecurity of the organization. It challenges the employees to improve their skills in the detection of attacks and response to them.

Furthermore, due to its spreading, the service can play the role of a global countermeasure against cybercrime, tuning worldwide organizations in the hackers' channel, predicting and understanding their moves.

To conclude, red teaming is an offensive real-life scenario approach against cybercrimes. It attacks the companies before they get attacked, potentially anticipating catastrophic events, where the lessons learned through simulation allow companies to set their barriers and protect their infrastructure in the more vulnerable aspects.

8.2 Reflections on the objectives

In this subsection we reflect on each our objectives defined in Section 1.2.

Give a unique insight into red teaming from stakeholders perspective, showing an unprecedented overview of red teaming.

In our research, we succeeded in presenting a unprecedented insight into red teaming from stakeholders perspective. By interviewing vendors (Chapter 6) and clients (Chapter 7) we were able to confirm and elaborate on the notions learned during the literature study.

Our dissertation is not supposed to be a manual of how to properly execute red teaming. Instead, it comments on the red teaming service from both vendor and consumer perspective, providing conceptual background, proper definitions and insight.

Verify if red teaming reduces uncertainty and consequently allows focused investments in companies regardless of their dimension, lastly improving their overall cybersecurity.

Through the collection and analysis of the answers collected from the clients interviewed, we can conclude that red teaming is a vector to reduce uncertainty, giving confidence and more awareness about prioritization.

Thanks to the confidence and awareness acquired about prioritization, CISOs are able to spend their budget in the most necessary cybersecurity investments at that moment, so postponing the less important ones. Therefore, the CISOs are able to spend money more accurately, in this way saving costs.

Lastly, the service alone or accompanied by training improves the overall cybersecurity of the

company, especially if it is performed periodically and the findings are properly managed.

Identify strengths and weaknesses in the red team service.

Strengths and weaknesses of the service are presented in this dissertation, based on the vendors' opinions, clients experiences, and literature review. In Section 3.5 and 3.6 we summarize the benefits and limitations of red teaming, validated both by the vendors interviews (Section 6.3) and the clients interviews (Section 7.7)

8.3 Future work

We propose that for Deloitte and the academic world a quantitative analysis would be valuable, which seeks to understand red teaming by using mathematical and statistical modeling. Indeed, this analysis would aim to represent red teaming in terms of numerical values, possibly bringing to light objective data that could give valuable insights into the service. Thus, we leave that analysis to future research requiring more resources and time.

Also, throughout our research, we collected data from one single vendor (due to contract restrictions). We are confident that future researchers could use our work as a starting point for a vendor-independent investigation. It would potentially remove bias from a red teaming provider's perspective.

Furthermore, this report could be an input for following studies through the adoption of a structured interview approach, possibly obtaining more comparable data (see Section 5.1).

8.4 Research limitations

Firstly, due to the nature of the data collected and the information that companies can disclose, the client interviews led exclusively to a qualitative analysis. A quantitative approach would have required more data than interviews with a limited number of clients could provide, moreover private companies hardly reveal confidential information. Despite the effort of creating a high degree of trust with the interlocutor, diffidence is another aspect that affects the quality of the answers.

Secondly, red teaming does not have a mature market yet. This implies that little information is available and only mature clients (rare to find and contact) can add significant value to this research.

Lastly, the Deloitte fingerprint influences this research in its entirety, which implies that possibly other vendors would slightly differ in some aspects of the red teaming service. Regrettably for confidentiality reasons we could not contact Deloitte competitors to access that information.

Appendix A

Red team Report Overview

The goal of this appendix is to offer a detailed examination of the report written at the end of the red team projects. We consider this section an added value to the dissertation, since the report in relation to the interviews provides a clearer idea of how red team as a service is accomplished. Besides, since the report is important for the client it is essential to delve into it.
Section A.1 introduces the report. Section A.2 comments its structure: Management Summary (Section A.2.1), Attack Flow (Section A.2.2) and Detailed Observations (Section A.2.3).
Section A.3 specifies by who the report is written and how.

Two anonymized reports have been provided by the red team vendor for analysis in our research. Also, the sections of this chapter present in a narrative way the results obtained by interviewing red teamers, and the results obtained collecting information contained in the provided reports.

A.1 Report Development

After the execution stage is completed a report is written by the red team to the client with the findings.
As we highlighted before in this dissertation, we observed that red team services are output-driven, in the sense that the final report overcomes the entire test for importance. Our observation was confirmed by the red teamers we interviewed.
The report is a proof of what went right and wrong throughout the assessment and can be used as a starting point for analysis and decisions in order to implement additional security strategies or countermeasures in general, like hardware, software or employee focused.

This report overview considers a fictitious company as a use case. Hence, we do not want to refer to any existing company.

A.2 Report Structure

The report consists of three parts: Management Summary, Attack Flow, and Detailed Observations. The subsections are indicated, when mentioned, by the words in bold.

A.2.1 Management Summary

In this section of the report, an overview of the attack steps is given (i.e., the **project approach**) in relation to the objectives defined with the client in the Scoping phase.
Along with the project approach, the **business impact** is described. The vendor offers a perspective of what would be the negative consequences of a real attack. For instance, an attacker could obtain sensitive information, which could cause an impact of the companies reputation.
Key improvement capabilities leave space to suggestions for improvements to help protect against and detect advanced cyber-attacks, based on **positive observations** (i.e., controls which could effectively hamper or slow down a potential attacker, such as an effective network segmentation).
To help the client to succeed in fulfilling the **next steps,** a **recommendation heat map** is added to the report. In order to facilitate structural remediation efforts, suggested improvement capabilities are summarized in the heat map depicted in Figure A.1. The capabilities are plotted in two dimensions: contribution to risk mitigation and estimated complexity, and each category is assigned

with a recommended priority and positioned in an expected resolution period.

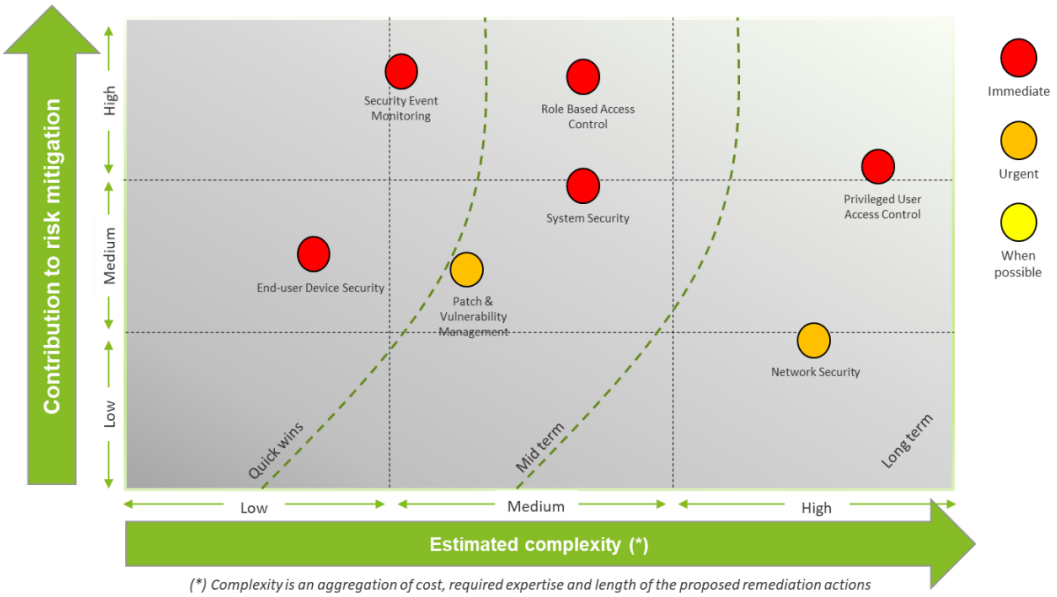

Figure A.1: Heat map summarized capabilities [taken from anonymized reports]

A.2.2 Attack Flow

The attack flow section consists of the executed steps. The execution chapter starts after a brief **introduction** describing the approach and the objectives of the assessment.

The attack flow depends on the goals and on the security weaknesses of the company attacked but for the sake of explanation Figure A.2 depicts an **overview of the engagement execution** of a random case study.

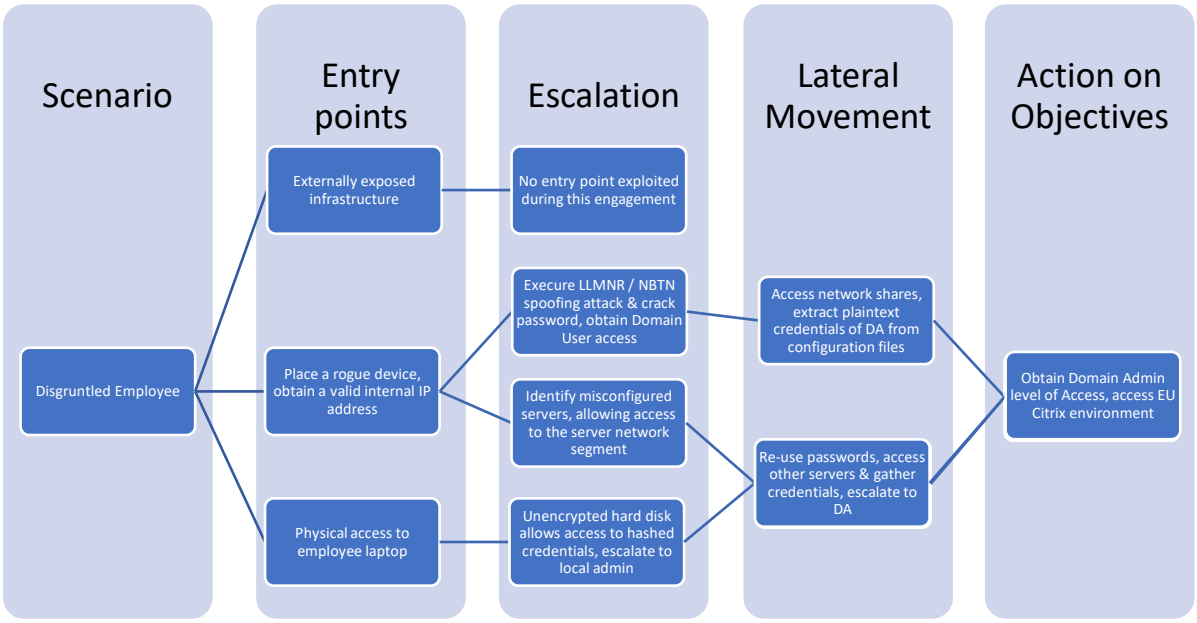

Figure A.2: Attack flow graph [taken from anonymized reports]

At the end of the execution section of the report, after **brief descriptions of all the steps taken** throughout the engagement, the overview of the execution abstracts from the actions performed

and gives a high-level idea of the entire process.
The execution of the disgruntled employee scenario (the red team received a company laptop with least privileges account) is displayed in the flow diagram in Figure A.2. As we can see from the graph the external infrastructure assessment did not lead to exploited entry point during the engagement, while the company laptop and a rogue device successfully allowed the team to escalate privileges, thus moving inside the network, hence obtaining domain admin level of access, and finally reaching the prearranged objectives.

A.2.3 Detailed Observations

To effectively steer remediation efforts, it is necessary to have a clear picture of the risk to various critical business functions (CBFs) within the client company.
By identifying CBFs and the people, process and technology components relevant to those functions, it is possible to focus on strategic remediation efforts, e.g., for the capabilities Security Event Monitoring or Role Based Access Control where the most value is at risk.

The report contains several detailed observations tagged with a security domain and capability. In addition, they are grouped in similar capabilities for the client's convenience to streamline prioritization and remediation efforts.

The vendor also assembles the capabilities in short, mid and long term strategies in order to prioritize the cybersecurity investments and implementations of countermeasure.

- **Short term improvements** (6 weeks) apply spot fixes, such as, improving Security Event Monitoring.
- **Mid-term improvements** (6 months) identify additional affected systems, correcting capabilities like System Security, changing, for example, default passwords or disabling insecure services.
- **Long term improvements** (24 months) structurally improve capabilities, such as, Network Security through network segmentation.

During the engagement, many observations are recorded. Therefore, at the beginning of the detailed observations section, an **overview of observations** is presented. Table A.1 outlines the identified observations, the security domain and capability, as well as the relative importance.

Observation	Security Domain	Capability	Importance
1 – Shared passwords for administrative accounts	Identity & Access Management	Privileged User Access Control	I
2 – Default credentials	Infrastructure	System Security	I
3 – Database servers running with excessive privileges	Identity & Access Management	Role Based Access Control	I
4 – Insecure configuration of shares and FTP servers with sensitive data	Identity & Access Management	Role Based Access Control	I
5 – Unauthorized access to Client EU Citrix environment and breakout capabilities	Infrastructure	System Security	I
6 – Lack of workstation hardening	Infrastructure	End-user Device Security	I
7 – Usage of LM hashes	Infrastructure	System Security	I
8 – Lack of monitoring capabilities	Security Operations	Security Event Monitoring	I
9 – No Network Access Control	Infrastructure	Network Security	II
10 – Insufficient network segmentation	Infrastructure	Network Security	II

Table A.1: Overview of observations table [taken from anonymized reports]

Later in the report, **each observation is expanded** with documented screenshots, an elaborated description of the vulnerability and recommendations to fix it adequately. This is exemplified in Figure A.3.

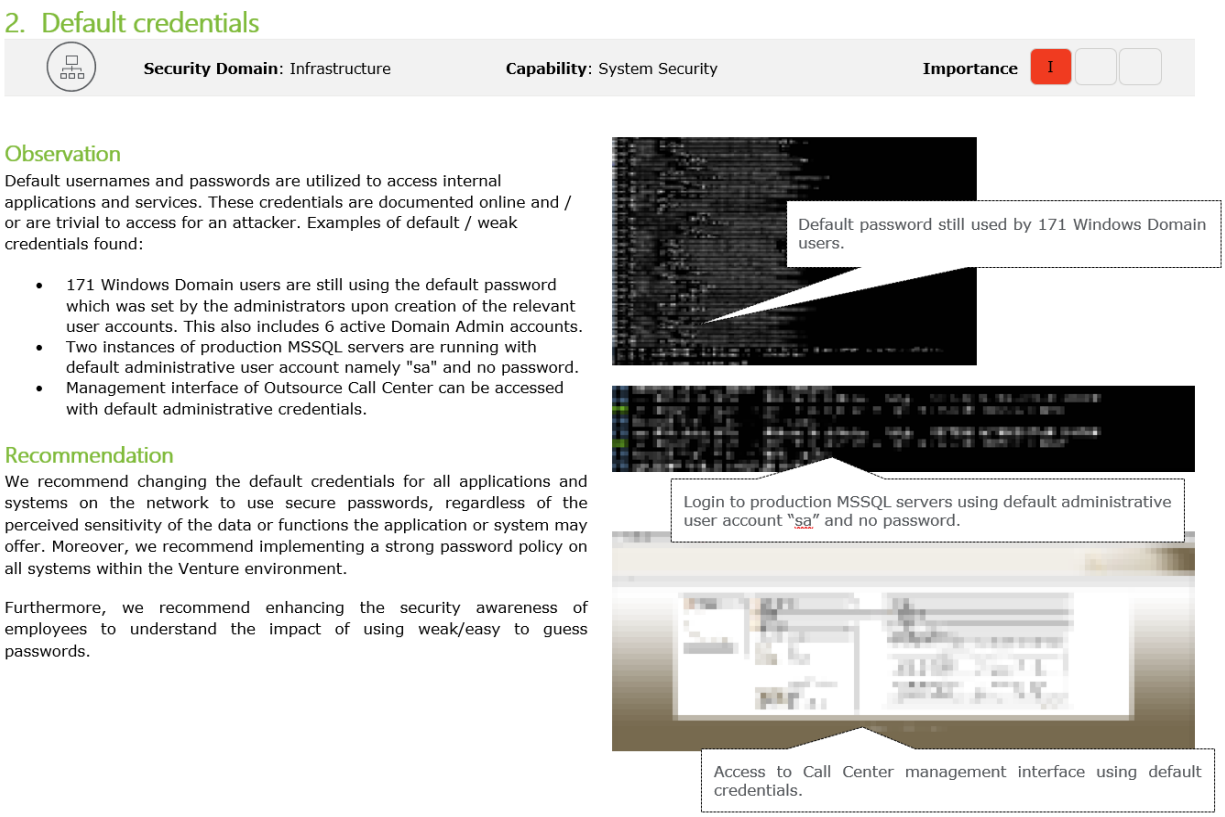

Figure A.3: Example of how an observation is documented (anonymized screenshots) [taken from anonymized reports]

A.3 Who writes the report?

The report is carefully written by red teamers inside the company who are sufficiently experienced. Therefore they are supposed to be able to write in a proper technical language and to describe the whole process precisely.

Each red team member writes some parts of the report, and at the end, all these parts are combined in the final version.

Appendix B

Client interview questions

B.1 Grounding questions

- Please briefly describe your background.
- Please briefly describe what red teaming is for you.

B.2 Macro-Level questions

- How would you define your company cybersecurity level, is red teaming a solution for a bad situation?
- How do you identify which threats are most important and prioritize them accordingly?
- Do you feel like you have adequate information in managing overall cyber risk and prioritizing accordingly? Is there any way in which this could be improved?
- When thinking about infosec spending decisions, are any evidence or metrics used in making cyber investment decisions?
- Do you use ROSI? If so, how do you find it useful in relation with red teaming? If not, why?
- Is red teaming part of a defense strategy or a strategy itself?
- For which assets do you ask for red team services?
    - After the conclusion of the service do you have a clearer idea about which are your most sensitive assets to protect?
- When do you request red teaming?
- Why do you ask for red team services?
    - How many times did you use the service?

B.3 Micro-Level questions

- How do you choose between competing service providers?
    - price
    - superiority of technology (if so: how was this determined?)
    - vendor leadership according to 3rd parties (Forrester waves, Gartner magic quadrant, etc.)?
- Can you talk about one or two of your most recent significant red team projects?
    - What was helpful about them?
    - What was missing?
- Do you change the way you invest after red teaming? Does the service provide evidence-based measures (reduced attacks, etc.)? How do you know it is working or not?
- Is your uncertainty about risks and attack vectors diminished after the whole red team service?
- Are you able to spend money more accurately after red teaming services? If yes, did the service improved significantly the way you invest, or you did not have any issue about cybersecurity investments?
- Do you believe that the report review is the most crucial stage of the process and why? If not, why?
- How could Deloitte help you, to build a stable relationship in the assessment of the security of your networks in a long term perspective?
- Do you request training at the end of the service? If not, why?
    - Do you have a blue team? If not, why?
    - Does training increase the overall cybersecurity? Did it prevent attacks?

Last questions at the end of the interview:

- Do you feel like your peers are spending too much on cybersecurity and that red teaming would reduce their future costs?
- Is your company cybersecurity level increased after red teaming?

Appendix C

Red team project managers questions

C.1 General questions

- What is the major difference between Pentesting and Red Teaming?
- What are the phases of a Red Teaming service, from the purchase to the report and after?
- What are your customers?
- Do you inform your customers in an anonymous way of the common vulnerabilities found? In other words, do they gain knowledge about the probability of other threats from observed attacks?
- Are the members of the red team selected every time according to the scenario of the customer's company?
- Do you usually have a briefing session before starting?
- Are you trained with red teaming guides?
- Do the red team members work together (also same room)?
- Do you have meetings during the attack phase (weeks or month of the attack)?
- Do you help them after the attack suggesting which kind of products they should buy?
- Do you usually work along with a Blue Team?
- What are the other contributions, in the service, of other teams like White, Purple,…?
- When you attack a company only senior manager are aware?
- Is war gaming part of the process?
- Do you usually pursuit the weakest link or the one that could have more impact in the organization? (i.e. Do you start from low level security points or the other way around?)
- Do you consider attacker cost/profit. in the attack?

C.2 Purchase phase

- How does a company purchase the service?
- How much does the service cost?
- Do you provide any kind of document like SOC to the company?
- Do you provide other documents?

C.3 Red teaming attack

- What is the role of Red Teaming?
- How long does it last?
- From whom and how is the scope defined?
- What are the legal considerations, if any?
- What are the properties (Confidentiality, Integrity,…) that a Red Team covers?
- What are the areas tested (Social Engineering, Wireless Security,..)?

C.4 Tools and processes

- What are the processes/approaches followed? For instance, the steps to evaluate layered security are kind of a spiral or a tree or other?
- According to the question above is the process standardized?
- Do you use the Open-Source Security Testing Methodology Manual (OSSTMM)?
- What are the tools used, covering each of the steps above?

C.5 Report phase

- Who reads the report?

- What are the goals of the report?
- How the report is structured?

C.6 Benefits

- What are the benefits of a Red Team attack?
    - Economical
    - Security
    - Red Team itself (what do you learn?)

C.7 Improvements

- What can be improved in your opinion?

Appendix D

Red team member questions

D.1 Cyber Threat Intelligence

- How would you define the cyber threat intelligence role before red team assessment?

D.2 Assets specification

- Is the client responsible for specifying which assets you need to test?

D.3 Tools and processes

- Please describe steps taken during the attack phase of the service.
- Do you use kind of a flowchart/framework or just personal experience?
- Do you use personal tools?

D.4 Teams involvement

- Do you work alone or in continuous contact with other red team members during projects?
- Are you in contact with white team/blue team?
- Do you train blue teams?

D.5 Report phase

- How the report at the end of the process is written?

D.6 Improvements

- What are for you strong points of the service? How do you think it can be improved?

Bibliography

[1] T. Moore, S. Dynes, and F. R. Chang, "Identifying How Firms Manage Cybersecurity Investment * 1 Study Overview," pp. 1–27, 2015.

[2] R. Bohme and T. Moore, "The Iterated Weakest Link A Model of Adaptive Security Investment," *Work. Econ. Inf. Secur.*, no. June, pp. 24–25, 2009.

[3] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Comput. Secur. J.*, vol. XIX, no. 2, p. 16, 2003.

[4] DCDC, "Red Teaming Guide," pp. 1–87, 2013.

[5] G. A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Q. J. Econ.*, vol. 84, no. 3, pp. 488–500, 1970.

[6] R. Anderson and T. Moore, "The Economics of Information Security : A Survey and Open Questions," *Science (80-.).*, vol. 314, no. 610--613, pp. 1–27, 2006.

[7] Accenture, "Cost of Cyber Crime Study." [Online]. Available: https://www.accenture.com/sa-en/insight-cost-of-cybercrime-2017?src=SOMS. [Accessed: 24-Jul-2019].

[8] C. Menlo Park, "Cybercrime Damages $6 Trillion By 2021," 2017. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. [Accessed: 25-Feb-2019].

[9] R. Anderson *et al.*, "Measuring the Cost of Cybercrime," *Econ. Inf. Secur. Priv.*, 2012.

[10] E. Durado and J. Brito, "Is There a Market Failure In Cybersecurity?," *Mercatus Center - George Mason University*, 2012. [Online]. Available: https://www.mercatus.org/publication/there-market-failure-cybersecurity. [Accessed: 25-Feb-2019].

[11] ENISA, "Introduction to Return on Security Investment: Helping CERTs Assessing the Cost of (Lack of) Security Investment," no. December, p. 18, 2012.

[12] Enterprise 2.0, "ROI for Samsung," 2013. [Online]. Available: https://makhangyung1.wordpress.com/2013/10/03/roi-for-samsung/. [Accessed: 20-Jun-2019].

[13] M. Middleton-Leal, "How to Calculate Return on Security Investment," 2018. [Online]. Available: https://blog.netwrix.com/2018/08/07/how-to-calculate-return-on-security-investment/. [Accessed: 20-Jun-2019].

[14] Owasp, "CISO AppSec Guide: Reasons for Investing in Application Security," 2013. [Online]. Available: https://www.owasp.org/index.php/CISO_AppSec_Guide:_Reasons_for_Investing_in_Application_Security. [Accessed: 20-Jun-2019].

[15] U.S. Department of Defense, "DoD News Briefing - Secretary Rumsfeld and Gen. Myers," 2002. [Online]. Available: http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636. [Accessed: 25-Feb-2019].

[16] Red Team Thinking, "HISTORY OF RED TEAMING." [Online]. Available: http://redteamthinking.com/red-teaming/history/. [Accessed: 25-Feb-2019].

[17] M. Zenko, "Inside the CIA Red Cell," 2015. [Online]. Available: https://foreignpolicy.com/2015/10/30/inside-the-cia-red-cell-micah-zenko-red-team-intelligence/. [Accessed: 25-Feb-2019].

[18] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *J. Comput. Sci. Coll.*, vol. 23, no. 4, pp. 124–131, 2008.

[19] C. Peake, "Red Teaming: The Art of Ethical Hacking," 2003.

[20] FraudWatch International, "What is Cyber Security Awareness Training and Why is it so Important?," 2018. [Online]. Available: https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/. [Accessed: 26-Apr-2018].

[21] Wikipedia, "Situational theory of publics," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Situational_theory_of_publics. [Accessed: 29-Jul-2019].

[22] R. Petty and J. Cacioppo, *Communication and Persuasion Central and Peripheral Routes to Attitude Change*. 1986.
[23] B. Crispo and L. Allodi, "Network Security Course," 2015. [Online]. Available: https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:netsec:2016:04-netsec_vulnerabilities-b.pdf.
[24] Symantec, "Internet Security Threat Report 2018," 2018.
[25] G.-J. Bruggink, "The best defence is a good offence," 2019. [Online]. Available: https://www2.deloitte.com/nl/nl/pages/risk/articles/the-best-defence-is-a-good-offence.html. [Accessed: 22-Mar-2019].
[26] Intregrity360, "TIBER-EU framework: What it is and why it's important," 2018. [Online]. Available: https://insights.integrity360.com/tiber-eu-framework-what-it-is-and-why-its-important. [Accessed: 14-May-2019].
[27] European Central Bank, "TIBER-EU FRAMEWORK How to implement the European framework for Threat," no. May, 2018.
[28] Forrester, "TIBER-EU Framework Offers An Opportunity To Improve FinServ Cyber Resilience," 2018. [Online]. Available: https://go.forrester.com/blogs/tiber-eu-framework-offers-an-opportunity-to-improve-finserv-cyber-resilience/. [Accessed: 15-May-2019].
[29] RAND, *The Defender's Dilemma - Charting a Course Toward Cybersecurity*. 2015.
[30] Zenithtechnologies, "The CIA Triad and Life Science Manufacturing," 2016. [Online]. Available: https://zenithtechnologies.com/zen-blog/the-cia-triad-and-life-science-manufacturing/. [Accessed: 20-Jun-2019].
[31] Sera-Brynn, "Understanding the Red Team Cycle," 2019. [Online]. Available: https://sera-brynn.com/understanding-the-red-team-cycle/. [Accessed: 20-Jun-2019].
[32] C. Brook, "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More," 2018. [Online]. Available: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more. [Accessed: 25-Feb-2019].
[33] Wikipedia, "Phishing," 2019. [Online]. Available: https://en.wikipedia.org/wiki/Phishing. [Accessed: 25-Feb-2019].
[34] Wikipedia, "Pass the hash." [Online]. Available: https://en.wikipedia.org/wiki/Pass_the_hash. [Accessed: 04-May-2019].