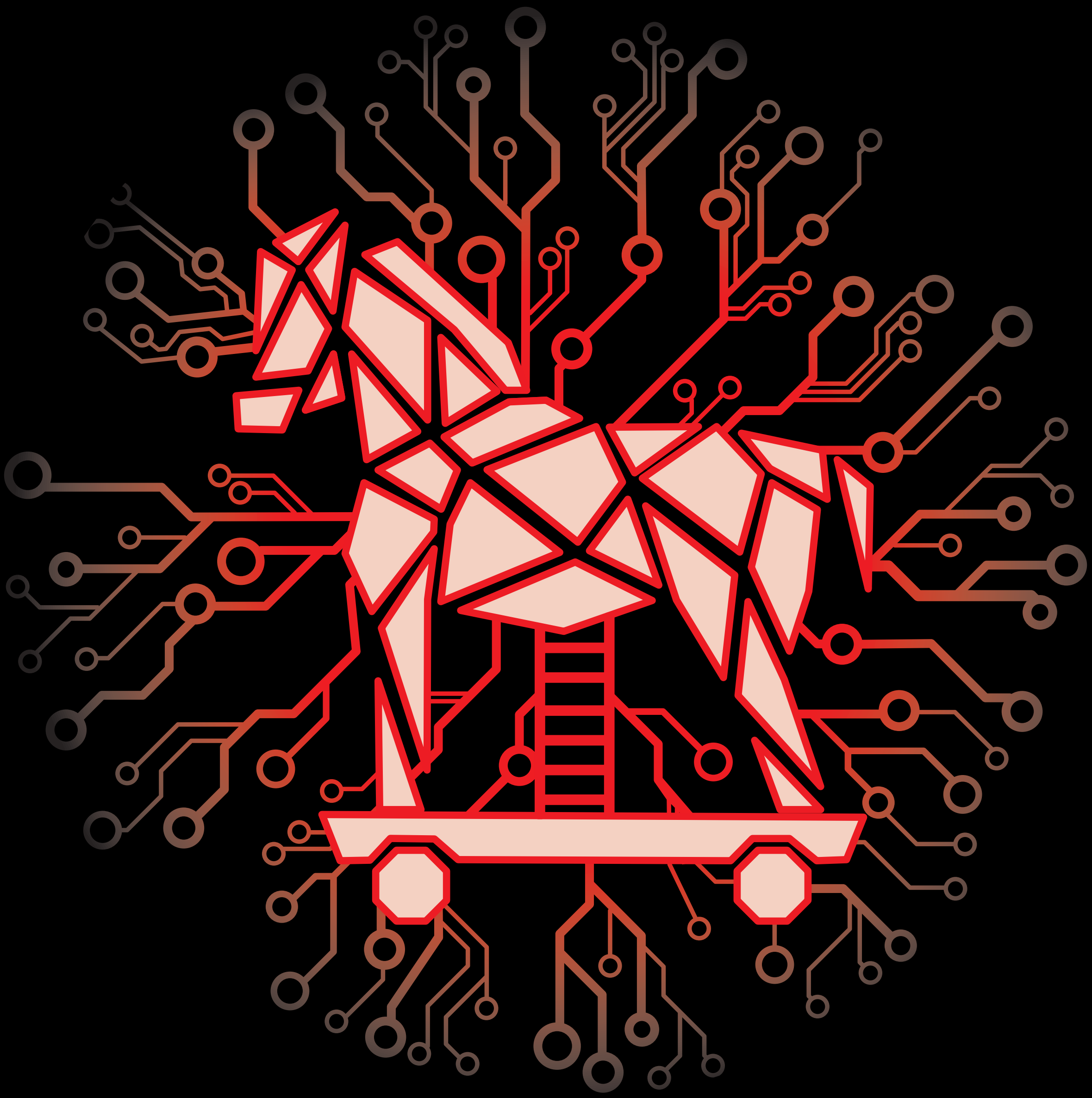
Deloitte.



Red Teaming Operations

Improving organizational resilience

Introduction 3
How Red Teaming started 5
Improving organizational resilience 6
Threat Intelligence 9
Red Teaming Operations 10
War Games 13
Purple Teaming 14
Threat Intelligence-Led Red Teaming 16
Global Red Team 18
Contacts 20

Introduction

The Red Team’s mission is to continuously increase the resilience of an organization against sophisticated attacks. By acting from an adversarial perspective, the Red Team uncovers digital, physical and social vulnerabilities and challenges executives’ and employees’ ability to react under real conditions. This approach enables the organization to develop and implement effective security measures. Red Teaming Operations help to evaluate threats, protect critical assets and respond appropriately to real attacks.

Tell me things others don't, and make senior officials feel uncomfortable.

George Tenet
former Director of Central Intelligence, CIA

How Red Teaming started

Red Teaming is a defensive approach that has been developed over the last couple of centuries. The key concept is utilizing an offensive mindset to better understand an adversary and plan for what would otherwise be unplannable. By doing this it becomes possible to identify weak points and gain a better understanding of the operational environment. The original purpose still holds true, especially in the cyber area.

Red Teaming technique has been derived from the practice of War Gaming in 19th century Germany, in which a pre-selected scenario had to be analyzed under time constraints. The idea was to get a better command of unpredictable events – so called frictions – in military conflicts. The weather, the terrain, lacking or false intelligence, logistics problems, the movement and effect of troops deployed, all of these had incalculable effects on the success of the original plan. The original setup, was a board game consisting of realistic-looking terrain pieces and game tokens for simulating battle sequences with detailed rules. This original method is now mostly referred to as a "War Game".

However, the term "Red Team" became more commonplace primarily due to the US military during the cold war. US military units, so called aggressor units, were trained to act, behave and operate as Soviet units. The purpose behind this was to mentally prepare soldiers for a different set of military techniques, maneuvers, weaponry and even terrain that were commonplace for the Soviet army but uncommon for the US army.

More recently, the day after the 9/11 attacks, George Tenet, who was the head of the CIA at the time, issued an order as short as it was unusual: he ordered a CIA unit called Red Cell to be set up. Their mission: to provide information that no one else provided and to worry the decision-makers. Why is that unusual? Because Tenet was actually in charge of an agency whose main task was already to obtain and evaluate information about national security. After the devastating events, he wanted a team that would radically and systematically challenge conventional thinking and help minimize the risk of more unexpected terrorist attacks.

During 2011, the National Cyber Security Center in the UK (part of GCHQ/MI5) issued guidelines for a UK Cyber Security Strategy which the Bank of England took into consideration when in 2013 they established CBEST, a program to create Red Teams, the equivalent of CIA's Red Cells, to test the resilience of UK Financial institutions. Driven by the Dutch Central Bank, the ECB followed by creating TIBER (Threat Intelligence Based Ethical Red teaming) to test the resilience of European financial institutions. Since then many other authorities in the Middle East and Asia have followed this example.

Throughout history Red Teaming has had a two-fold purpose: to help identify new techniques and approaches that an attacker might utilize as well as train the defensive teams into visualizing such attacks and improving their response capabilities. The end goal is to improve overall resilience; a message that resonates accross history, nations and businesses alike.

Improving organizational resilience

No matter how well an organization protects itself against attacks, there will always be a vulnerability. Security is not a perpetual state, there is always the risk of a successful attack. In addition to preventive protection measures, organizational resilience, i.e., the ability to maintain or restore business processes after a disruption, is an important element of a company's IT and IT security.

Organizational resilience requires the ability to anticipate threats, to prepare for possible attacks, to remediate the harmful effects of attacks in order to be able to resume business activities as soon as possible and, if necessary, to adapt one's own security measures. To be resilient, an organization must:

- Obtain information about existing threats from appropriate sources.
- Draw the right conclusions from this information.
- Be aware of the influence of cognitive and social aspects on decision-making.
- Introduce appropriate technical and organizational security measures and ensure their long-term effectiveness.

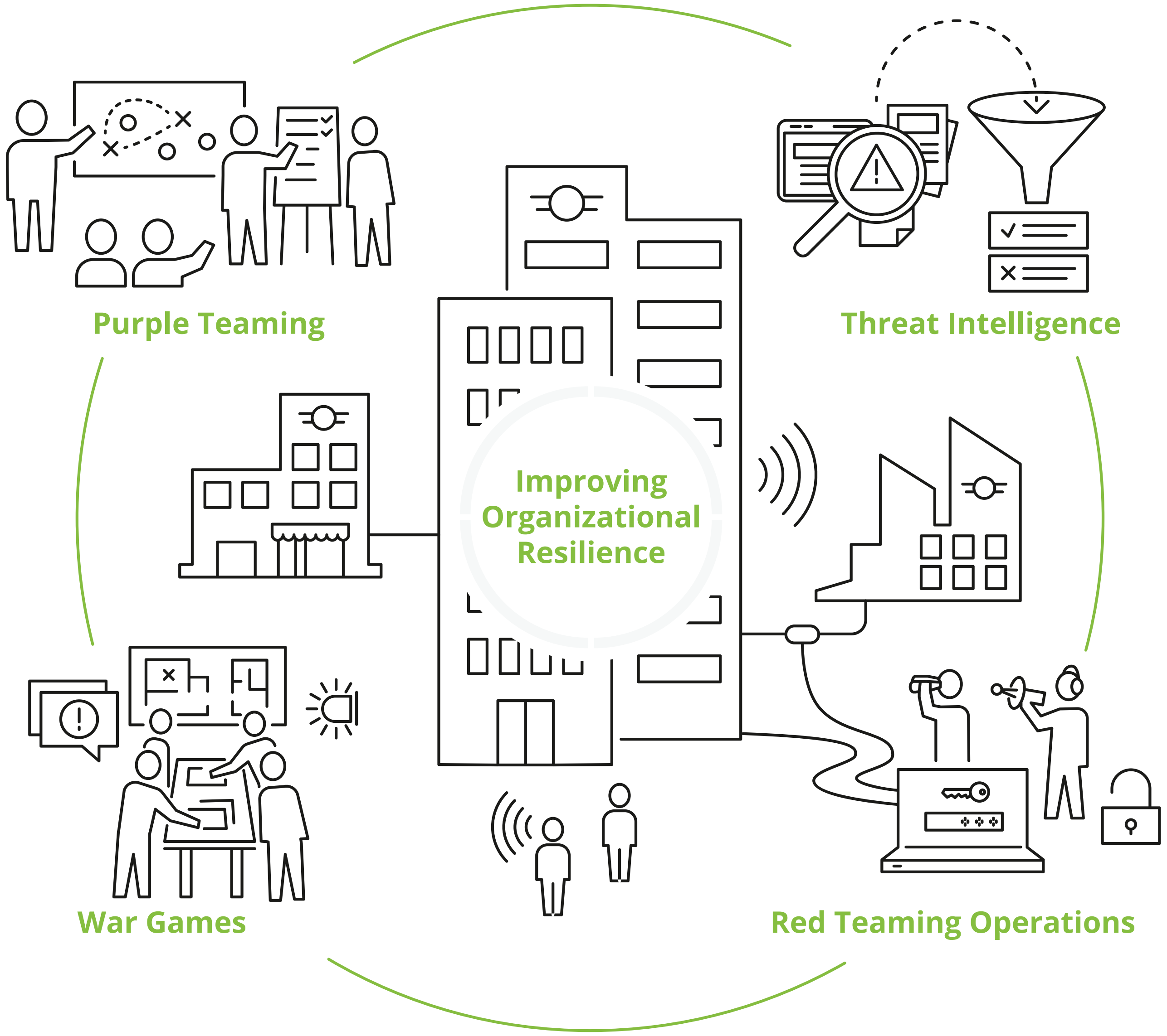
Deloitte supports companies in this process with Red Teaming Operations. Starting with a joint assessment of the status quo of the organization's resilience, Deloitte offers a tailored combination of our service elements:

- Continuous provision of information on risks and relevant threats.
- Performance of realistic tests and simulations to validate organizational resilience to cyber-attacks and assess potential adverse effects.
- Development and support of an improvement program tailored to the specific needs of the company.

Deloitte's methodology of utilizing an adversarial point of view towards keeping organizations secure has improved the resilience of many clients around the globe. They expect high-quality services and a coherent future-proof approach to make sure their businesses thrive in the digital age.

Security is a process not a product.

Bruce Schneier



Four elements to improve organizational resilience

Threat Intelligence

Red Teaming Operations

War Games

Purple Teaming

Threat Intelligence

A good understanding of existing threats is essential for the improvement of any organization's resilience and adaptability.

The term “intelligence” has its origin in the military and information services and describes the collection, processing and dissemination of data for a specific purpose.

Deloitte's Cyber Threat Intelligence capability offers services to provide information about the intent, opportunity and capability of malicious actors. The tailored intelligence products help organizations how to deal with these threats. Cyber Threat Intelligence focuses on identifying cyber threats to organizations.

Intelligence products are mapped to the business objectives of an organization to determine whether the intelligence products created are adding value for the organization. A precise knowledge of complex and fast-moving developments in this area forms the basis for all actions focused on resilience. Deloitte provides clients with effective assessments that allow a 360-degree view of the existing specific threat landscape. The goal is to reduce uncertainty by developing products that are actionable, timely and relevant, enabling intelligence consumers to execute more informed decisions towards reducing risk.

Two elements are essential: the quality and diversity of the underlying information and the continual and professional evaluation of this information to produce actual intelligence are of key importance of the Cyber Threat Intelligence service.

Against this background, Deloitte's information procurement is extremely broad and diverse. Open Source Intelligence is a central element of this process. This primarily involves searching the internet for suitable information. In addition to advanced analyst-driven searches using automated search engines, this explicitly includes the Open, Deep and Dark Web, Deloitte uses human analysts where it matters the most. Therefore, Deloitte develops and uses software and tools with innovative techniques, such as machine learning algorithms, to obtain and classify relevant information from thousands and thousands of primary sources.

Cyber Threat Intelligence requires the involvement of clients at all times. Apart from a standardized, in-house developed self-assessment and thorough understanding of the global threat landscape, Deloitte's analysts plan and design possible attack scenarios in workshops together with clients. The development of these scenarios is based on statistical analysis that is examined in relation to the customers’ goals and allow to make forecasts about the current and future threat landscape.

Red Teaming Operations

In Red Team Campaigns, Deloitte simulates realistic adversarial attacks against an organization to identify and exploit vulnerabilities and demonstrate how this could harm business-critical assets. The purpose of a Red Team Campaign is to validate the resilience of an organization.

Red Team Campaigns are based on specific attack scenarios derived from previous analysis of the threat landscape. An integral element of the scenarios are statements about likely attacker groups with their respective intent, expertise and capabilities. An attack scenario describes a clearly defined objective including a statement on the negative effects a successful attack would have for the organization.

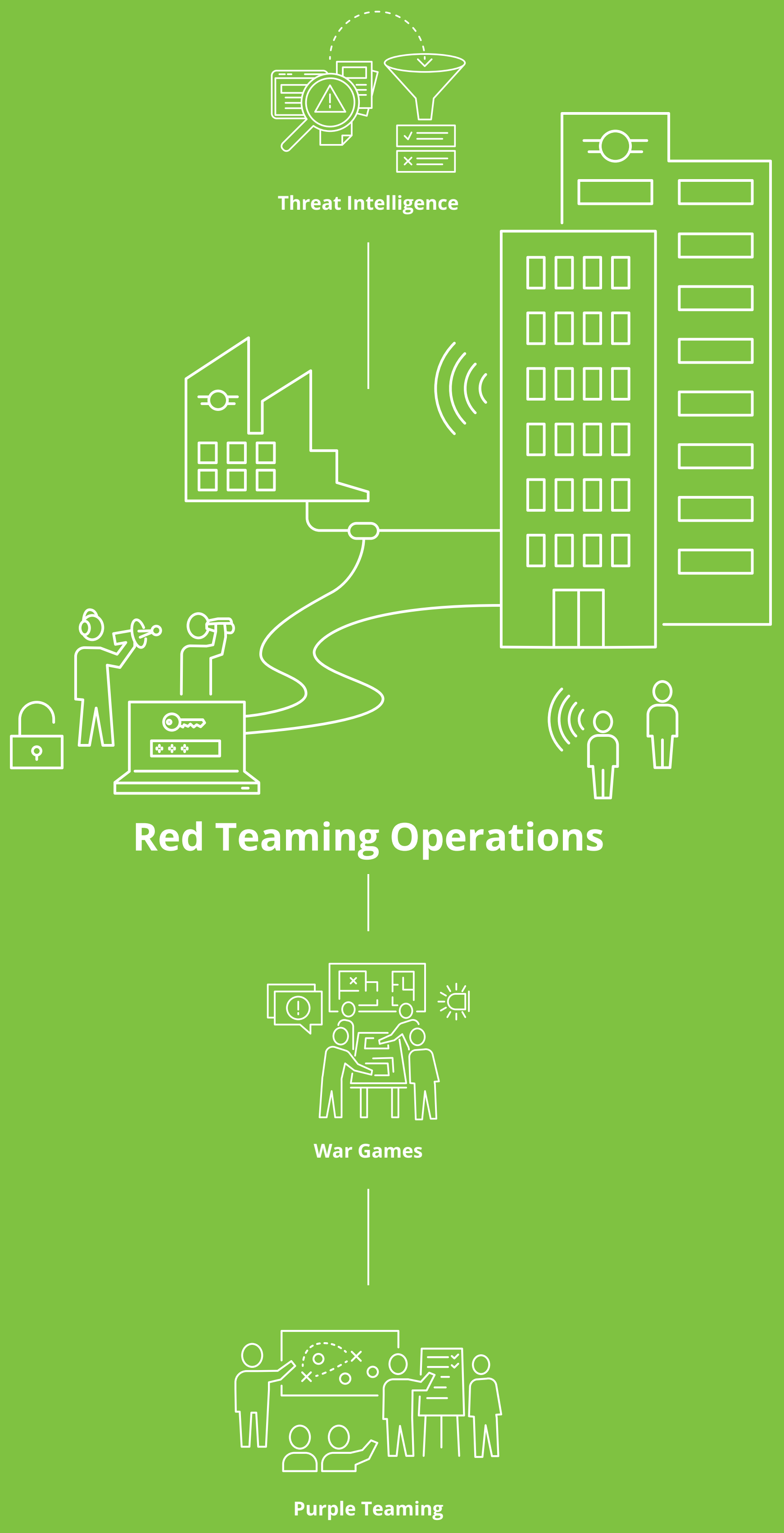
The Red Team tries to identify and exploit unknown vulnerabilities and attack vectors that can be used to target company assets, simulating the disruption of processes or theft of confidential data. When developing and executing these scenarios, Deloitte's Red Team performs an evaluation of the physical security of facilities, networks and applications but also opportunities for a targeted exploitation of people (i.e., social engineering). The attack scenarios comprise elements of physical penetration tactics, social engineering and hacking techniques, combined in such a way that allows the Red Team to reach the set objectives. This, amongst others, might contain:

- Attempts to trick employees into disclosing confidential information or performing inadequate actions and thus unintentionally support the attack of the Red Team.
- Reconnaissance of the premises to identify vulnerabilities in physical security perimeters or processes that then allow entry into restricted areas of the organization.
- The use of appropriate tools and techniques to penetrate networks and/or applications, and subsequently perform lateral movements towards the targeted asset.

Hence, Red Team Campaigns provide insights about whether the organization is able to protect, detect, respond and recover from the simulated cyber-attack and whether the controls and processes are being effectively applied.

Before and during Red Team Campaigns, Deloitte consultants are in close consultation with the client to define and observe any restraints or constraints that apply to the specific test.

Within the test report, Deloitte describes the approach and the attack path of the simulated cyber-attack. Respective observations and recommendations around people, processes and technology are given to further improve the client's resilience. Deloitte also outline the business impact of the Red Team Campaign.



Threat Intelligence

Red Teaming Operations

War Games

Purple Teaming

War Games

War Games are scenario-based simulations that challenge and test an organization's responsiveness. During these exercises, the simulated conditions of a realistic crisis situation provide the members of a company's crisis team with an opportunity to practice and test their strategy, plans and skills.

Corporate crises are disruptive, multifaceted events that can hit any organization unexpectedly. Previous crisis experience demonstrates that rapid, targeted action can significantly reduce the duration and impact of a crisis. A well-rehearsed, efficient, and self-assured crisis management team is a significant cornerstone of a resilient organization. Apart from the design and documentation of the necessary processes and procedures, regular training of those involved is indispensable for the development and maintenance of an adequate ability to react.

Within the framework of Deloitte's War Games, crisis teams are prepared and trained for crisis situations in a safe learning environment. The scope and scenario of the exercises are designed in accordance with the client to ensure an optimal fit to their needs and abilities.

The selection of a suitable scenario is significantly influenced by the probabilities determined by our Intel Service. This gives organizations the opportunity to improve their internal competencies under guidance in a scenario that is most relevant for them. Thus, the simulation directly prepares organizations for a possible crisis.

Since corporate crises are difficult to predict and highly diverse, War Games are not aimed at pre-testing specific cases, but at providing the necessary frameworks and pre-requisites to effectively deal with these situations.

In order for behavior patterns to be reliable in stressful situations, they need to be rehearsed. This behavioral confidence is permanently stimulated during the War Games. The reactions of the crisis management team provoke a new counter-reaction from Deloitte's Red Team, so that a playful competition between two teams develops.

The ability of the active protagonists to react to any situation is a direct indication of the company's resilience.

Purple Teaming

Purple Teaming exercises are focused on enhancing the detective (Blue Team) and offensive (Red Team) capabilities. The Blue Team attempts to detect the Red Team's activities whereas the Red Team tries to stay as covert as possible.

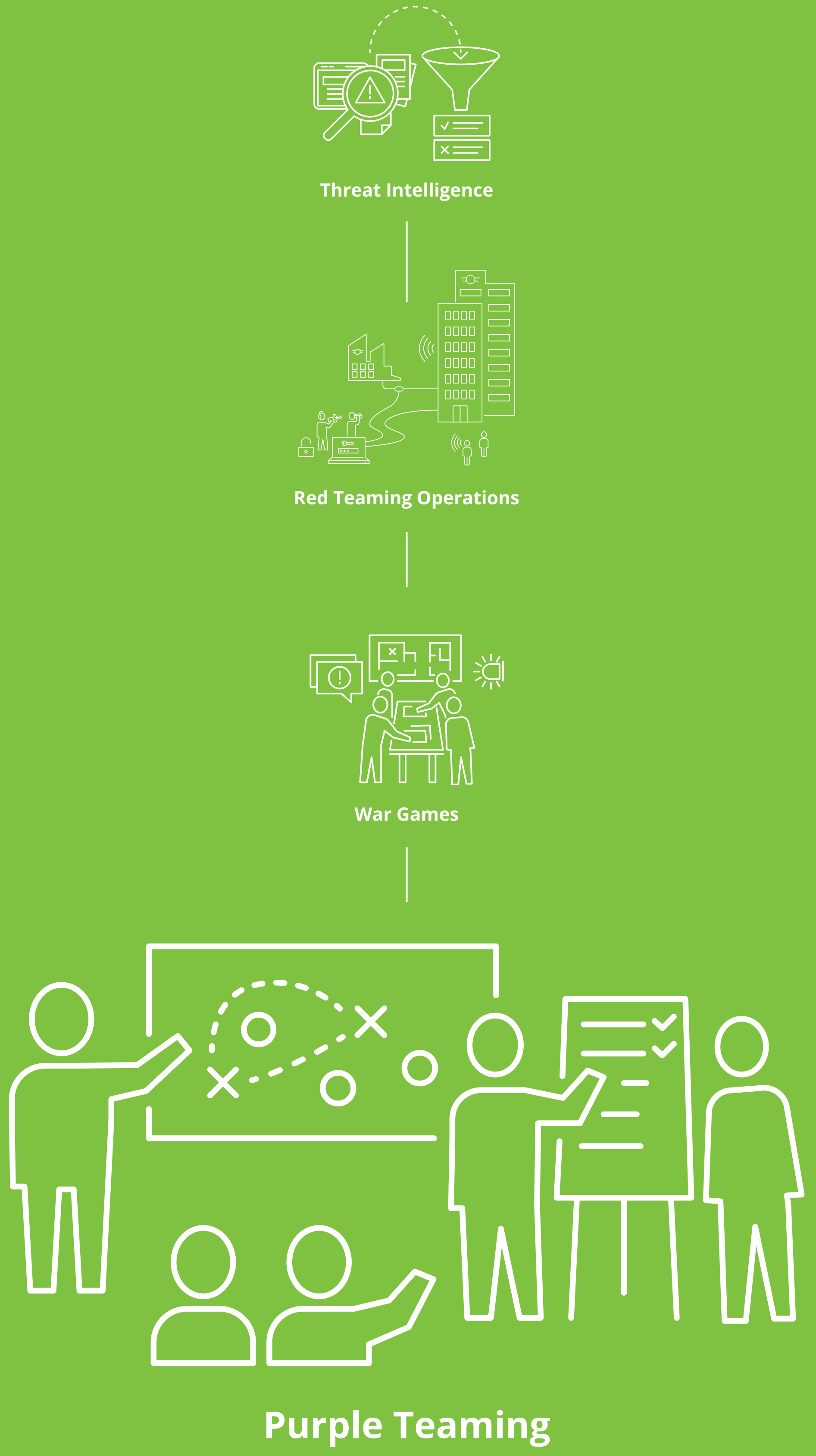
Performing a Red Team Campaign is the best way to evaluate the overall effectiveness of the security controls around people, processes and technology. One of these controls examines the effectiveness of organizations' Security Operations Center: Are their SOC analysts able to detect the Red Team? Answering this question can be quite hard, as there can be multiple factors which contribute to the result of detecting an adversary.

A SOC can be compared to the human immune system. It will be able to detect a cyber-attack if it has had experience with similar situations. It is almost impossible for SOC analysts to detect an attacker if they have never seen one or analyzed their activity before. The Purple Teaming exercises have been developed to address this gap in three phases.

Every exercise requires preparation and so does the Purple Teaming exercise. Deloitte's team should ideally perform a Red Team Campaign within the client's infrastructure without notifying their SOC team in order to get the required indicators of compromise (IOCs).
The goal of this phase is to develop an attack path which other malicious parties would also abuse. The Red Team minutely records all the steps they take which will be used in the second phase.

The SOC is involved in the second phase, in which they are informed of the performed Red Team Campaign and the used attack path. The SOC can now start to form an idea why they were (or weren't) able to detect some of the attack techniques used by the Red Team.
Deloitte's Blue Team specialists provide additional context on how this can be detected. Should the data source be present and the retention of this data be adequate Deloitte specialists assist the client in locating the IOCs and help them with the high-level design of the use case, making sure they don't develop tunnel vision towards the IOCs.

During the third phase, the attack techniques from the attack path are replayed by the Red Team, the scenario will be very similar to the initial one and depending on the outcome of the second phase can be executed bypassing certain limiting elements in order to achieve the most beneficial result.
The SOC is obviously aware this will eventually happen but not of the exact moment in order to get the most natural response to an incident. This will provide additional insight in how the detective capabilities of the SOC have been increased. During this phase all improvements are evaluated as well as their detections. Any missed techniques which could have been detected will be investigated and recommendations on improvement will be made. Should it be small tweaks, the present Red Team members will replay their attack to generate new data to validate the changes.



Threat Intelligence

Red Teaming Operations

War Games

Purple Teaming

Threat Intelligence-Led Red Teaming

The rapidly growing security challenges are not only a hot topic for individual companies, but also an important discussion point for Governments, the European Union, and other international institutions.

In 2013, the UK Financial Policy Committee recommended to HM Treasury that they and regulators work with core UK financial systems and infrastructure providers to create a framework to test the resilience to sophisticated cyber-attacks: CBEST. The Committee aimed for boards of financial firms and infrastructure providers to recognize their responsibility for responding to attacks using continuous vigilance and investment to strengthen their operational resilience. Since then, other International authorities have adopted this approach, e.g., the ECB adopted the TIBER-EU framework.

Threat Intelligence based Red Team engagements typically follow a similar approach.

Generic Threat Landscape Phase

The (optional) Generic Threat Landscape (GLT) Phase involves an assessment of the national financial sector threat landscape. It comprises the identification of relevant threat actors with their specific Techniques, Tactics and Procedures (TTPs). This is the basis for the development of attack scenarios at a later stage. The Generic Threat Landscape may be updated on an ongoing basis as new threat actors and TTPs emerge and pose risk to the entities.

Preparation Phase

This phase involves the formal launch of the Intelligence-led tests and the establishment of the teams responsible for managing the tests. Further, the scope of the tests are determined, approved and attested by the entity's board, and validated by the relevant authorities. Finally, the Threat Intelligence and Red Team providers are procured to carry out the tests.

Testing Phase

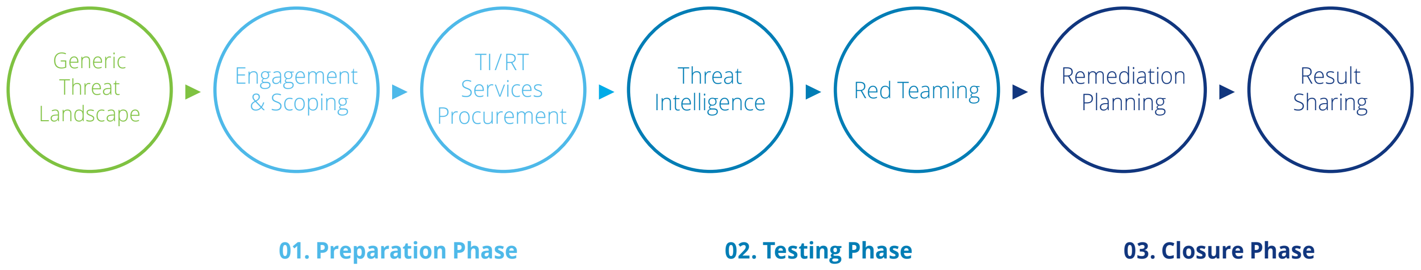
The Testing Phase includes Threat Intelligence and Red Team Tests. The Threat Intelligence provider produces a Targeted Threat Intelligence (TTI) report for the entity, setting out threat scenarios for the tests. The Red Team provider uses the TTI report to develop attack scenarios and execute intelligence-led Red Team Campaigns of specified critical live production systems, people and processes.

Closure Phase

The Closure Phase includes remediation planning and result sharing. The Red Team provider drafts a Red Team Test report, which will include details of the approach taken to the testing and the findings and observations from the tests. Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The entity will take on board the findings to agree on and finalize a Remediation Plan in close consultation with the supervisor and/or overseer.

Benefits of Threat Intelligence-Led Red Teaming:

- Access to advanced and detailed cyber threat intelligence prepared by knowledgeable, skilled and competent cyber threat intelligence analysts with a detailed understanding of the financial services sector
- Realistic penetration tests that replicate sophisticated, current attacks based on current and targeted cyber threat intelligence
- Highly qualified penetration testers who understand how to conduct technically difficult testing activities whilst ensuring that no damage or risk is caused
- Standard key performance indicators (KPIs) that can be used to assess the maturity of the organization's ability to detect and respond to cyber attacks
- Access to benchmark information, through KPIs, that can be used to assess other parts of the financial services industry
- A framework that is underpinned by comprehensive, enforceable and meaningful codes of conduct administered by a specialist professional body



Threat Intelligence-Led Red Teaming Process

The following frameworks are currently implemented by various authorities across industries and geographical locations:

CBEST

CBEST was introduced in 2013 by the UK Financial Authorities - Bank of England (BoE), Her Majesty's Treasury, and the Financial Conduct Authority - as a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviors of threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. CBEST differs from other security testing undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks on critical systems and essential services. The inclusion of specific cyber threat intelligence ensures that the tests replicate, as closely as possible, the evolving threat landscape to remain relevant. This provides a holistic assessment of a financial services or infrastructure provider's cyber capabilities by testing people, processes and technology in a single test.

GBEST

GBEST is a new scheme based on the CBEST model and is being rolled out across UK Government Departments. The scheme aims to be very similar to CBEST but with some minor differences; for example, a GBEST assessment is expected to take slightly longer than an average CBEST.
The overall scheme is coordinated by the Cabinet Office and the National Cyber Security Centre (NCSC) provide validation of the Threat Intelligence and general technical assurance. Each exercise is procured, led and ultimately owned by the Government Department carrying out that specific exercise.

TBEST

Throughout 2016 and 2017, CREST worked extensively with the Department of Culture, Media and Support (DCMS) and OFCOM to launch the TBEST scheme. CREST took a similar role in the creation of this program and provided practical adaptations of the CBEST scheme to align it to the needs of the telecommunications sector.

iCAST

To further strengthen the cyber resilience of authorized institutions (AIs) in Hong Kong, the Hong Kong Monetary Authority (HKMA) developed a Cyber Fortification Initiative (CFI), comprising three components: (i) a Cyber Resilience Assessment Framework (C-RAF); (ii) a Cyber Intelligence Sharing Platform; and (iii) a Professional Development Programme (PDP).

As with CBEST, under iCAST, the traditional penetration test is augmented by adding threat intelligence to formulate end-to-end testing scenarios (from attack initiation to achieving pre-defined test objectives) to allow testers to more closely simulate real life attacks from competent adversaries. In addition, an iCAST assessment provides KPIs that help benchmark the AI's ability to detect and respond to such attacks.

AIs aiming to attain an "intermediate" or "advanced" maturity level are required to execute an iCAST during the "maturity assessment" process.

TIBER-EU

In May 2018, the European Central Bank (ECB) adopted the Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER- EU).

TIBER-EU provides a common framework for European and national institutions and authorities in the financial sector (and beyond) to test their existing systems for vulnerabilities and increase resilience to complex cyberattacks with the help of Red Teaming. The framework relies on controlled, individualized, and intelligence-based Red Teaming. In this way, critical functions and their underlying systems, i.e., people, processes, and technologies, are to be sustainably secured and strengthened by simulated attacks.

Each country in the European Union is encouraged to adopt the same framework in the domestic market, e.g., TIBER-NL in The Netherlands or TIBER-BE in Belgium.

Global Red Team

Deloitte's Red Team bundles experience and knowledge from multiple areas and all regions across the globe.

Deloitte's multidisciplinary teams consist of cyber security specialists, economists, computer scientists, intelligence analysts, former military officers and criminologists amongst others. Deloitte professionals work across countries and continents in order to provide a localized approach in the required language and cultural context.

The Red Team embodies all the important characteristics that define the four core elements of Red Teaming: excellent analysis and research skills in the area of Threat Intelligence, extensive practical strategy and tactical experience in military and civil simulations in War Gaming. Added to this are creativity, foresight, and a wealth of experience in Red Team Tests. Concrete, industry-specific experience in the implementation of detection and incident response capabilities round off the range of skills in Purple Teaming.

The team is supported by the technologies and competencies of the global network of Deloitte's Cyber Intelligence Centers (CIC). This enables a holistic view of possible threat scenarios and resilience strategies.

In order to continuously optimize their work, the Red Team draws on the extensive international Deloitte Network of professionals. This global collaboration enables Deloitte to deliver creative solutions faster to clients globally.

How can Deloitte best support your company? To assess how Deloitte can support in systematically increasing the organizational resilience through Red Teaming Operations, simply follow the next three steps:

1

Within the framework of a half-day workshop a Deloitte professional will present the Red Teaming Operations services in detail and in person. In a structured interview the organizations present situation is assessed. Current security concepts, processes and technology are analyzed along with the security risks and the status of security training and education measures.

2

On this basis, the opportunities for improvements are discussed. A tailored offer is prepared that addresses the fields of action identified.

3

Deloitte offers the coordinated and continual deployment of our Threat Intelligence, Red Teaming Operations, War Games and Purple Teaming services to improve the organizational resilience.

Contacts

Thailand

Parichart Jiravachara
Partner I Cyber Risk
+66 2034 0130
pjiravachara@deloitte.com

You can find more information on our website

www.deloitte.com

Deloitte.

About Deloitte Thailand
In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.