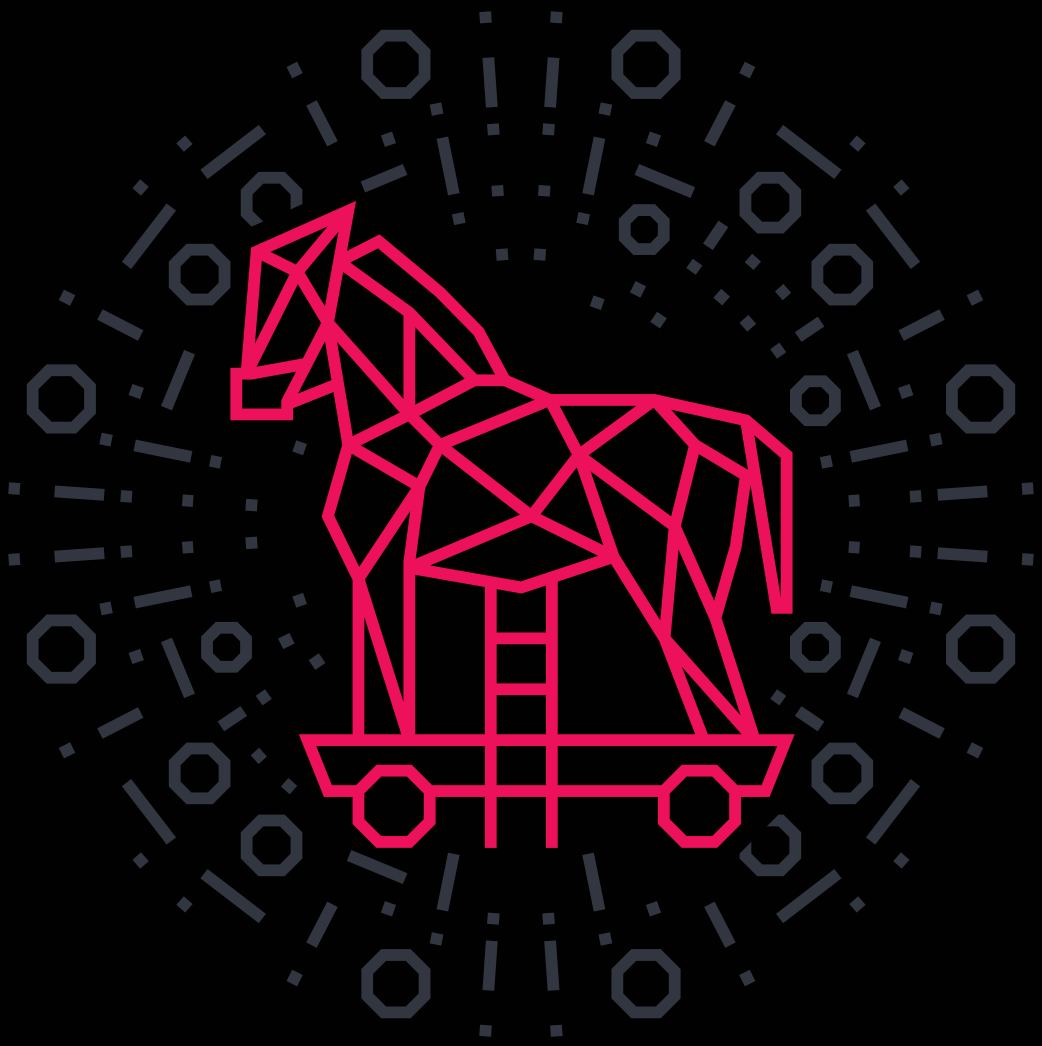
Deloitte.



Red Team

Improving Organizational Resilience

Introduction

The Red Team’s mission is to continuously increase the resilience of your organization against sophisticated attacks. By acting from a hostile perspective, we uncover digital, physical and social vulnerabilities and challenge your executives’ and employees’ ability to react under real conditions. This approach enables us to develop and facilitate individual, effective security trainings for your company. Red Team Services help you to evaluate threats, protect your assets and respond appropriately to real attacks.

Our Concept

Knut Schönfelder is Senior Manager at Deloitte and leads the Red Team.

What does the term "Red Teaming" mean to you?
The systematic application of analysis techniques from the perspective of an attacker. A Red Team helps organizations to critically review their assumptions and plans and to identify weaknesses.

Where does the concept of Red Teaming come from?
Red Teaming is a method developed by the German military in the 19th century. They realized that there are circumstances that were not taken into account in the original planning but which could jeopardize the success of a plan. Confronting the intended approach with unpredictable events is now a recognized method of critical testing. Nowadays, the military regularly use Red Teams to challenge aspects of their own plans, programmes and assumptions.

We intent to transfer this methodology to the public and private sector in a meaningful way. A trained Red Team offers today's companies and corporations a convenient opportunity to improve its organizational resilience, in other words anticipate, prepare for and respond to disruption.

If you search the internet for the term "Red Teaming", you find a great variety of descriptions and providers. What makes Deloitte's service so special?
Many of these offers cover only some aspects of our service. For us, Red Teaming is significantly more than just a penetration test where hackers look for new ways into a company's network. We want to also assess the implications of attacks, identify and monitor risk and systematically improve organizational resilience with our service.

Deloitte is offering a comprehensive Red Teaming?
Our offering is a continuous service going beyond the cyber world. Moreover, we combine four elements we consider central: Intel Service, War Games, Red Team Tests, and Resilience Training. Our Intel Service delivers analyses, provides scenarios, and gets the ball rolling. We regularly challenge our customers at many different levels with our War Games and Red Team Tests. War Games train internal decision-making processes in special situations, Red Team Tests examine organizations for weak points and verify them. We continually summarize our findings in a variety of reports and incorporate deficits identified in the Resilience Training we conduct with our clients. We also address assumptions and assessments that prevail in the companies we support. These often turn out to be unproven or uncertain ("bias") and may thus give a false sense of security.

"Red Teaming is the systematic application of analysis techniques from the perspective of an attacker."

I see a further distinguishing feature in what I think is the unique composition of the Red Team. It brings together cyber experts, political scientists, economists, engineers, experts in social media analysis, and intelligence experts, with a mixture of civilian and military backgrounds. With this combination, we manage to take almost every creative point of view into account in our approach.

You say Red Teaming in itself is nothing new. Why is it important again today?
It is still important – in fact, it is more important than ever! We are living in what is probably the fastest moving and most complex world that history has ever seen. Our lives are marked by constantly changing demands. Our Nations and companies also live in this world. Consequently, the development of systems and forms of organization that will remain secure in the future is moving away from the rigid security that is perceived as onerous, towards flexible resilience. Instead of just building ever higher walls, we help our clients to deal actively and confidently with attacks and thus to nullify them.

"Our offering is a continuous service going beyond the cyber world."

There are already some good approaches at the European level, especially in the financial sector, on which we base our system, among other things.

All in all, good Red Teaming furthers an organization's resilience in a decisive and above all lively way.

That sounds like a huge task ...
... which we face with confidence, with the system developed by our team. We are not alone in this. In addition to our own workforce as a Red Team, we receive valuable support from many areas of Deloitte, particularly in the area of our Intel Service, which enable us to provide our clients with all the analyses they need. And of course, as a Deloitte team, we also benefit from the extensive network and experience of other colleagues in the fields of auditing, consulting, finance and many more. We are happy to pass on the sum total of all our experience and knowledge to the clients who use our Red Team service.

“Tell me things others don’t, and make senior officials feel uncomfortable.”

George Tenet
former Director of Central Intelligence, CIA

Red Team | How “Red Teaming” started

How “Red Teaming” started

Red Teaming is a method developed by the German military in the 19th century, originally for training Prussian officers. The idea was to get a better command of unpredictable events – 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.

Baron von Reisswitz’ “tactical war game” has historical significance. The original setup, which you can view in Berlin’s Schloss Charlottenburg, was a board game consisting of realistic-looking terrain pieces and game tokens for simulating battle sequences with detailed rules. Two players had to carry out their operational plans step by step. Each move was allowed to take exactly two minutes, the duration of an artillery barrage. Apart from the decision when and where to deploy one’s own troops, the course of the battle was also determined by a roll of a dice, taking the place of the incalculable “frictions”. This original method is now mostly referred to as a “War Game” and has become an integral part of the planning process.

Red Teaming derived from the practice of War Gaming in which a pre-selected scenario had to be analyzed under time constraints. Organizations – both civilian and military – critically test their assumptions and planning with the help of specially set up Red Teams. They identify weak points and gain a better understanding of their operational environment, especially in the cyber area.

A current example is the US foreign intelligence agency, CIA. 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 any more unexpected terrorist attacks.

Red Teaming

There is one thing we are quite sure of: 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 IT and company security.

Organizational resilience requires the ability to anticipate threats, to prepare for possible attacks, to minimize and tolerate 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 risks from appropriate sources
- draw the right conclusions from this information
- be aware of the influence of cognitive and social aspects on decision-making and
- introduce appropriate technical and organizational security measures and ensure their long-term effectiveness

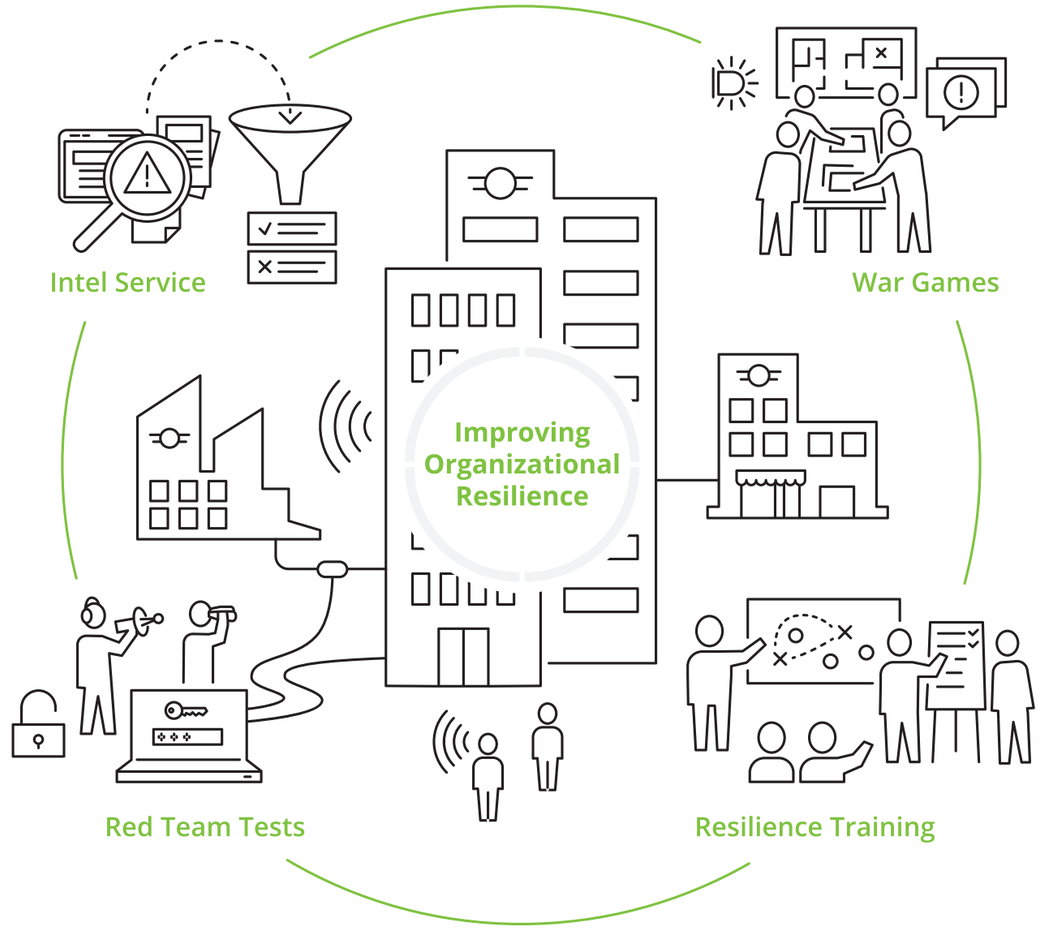
We want to support companies in this process with our ongoing Red Teaming Service. Starting with a joint assessment of the status quo of organizational resilience, we guarantee a tailored combination of our service elements:

- continous provision of information on risks and relevant threats,
- performance of regular tests and simulations to validate vulnerabilities and assess potential adverse effects
- development and support of a training and education program tailored to the specific needs of the company

Our proven Resilience Framework, a guided self-assessment, serves as a reference for determining and monitoring the status of organizational resilience and evaluating the effect of our measures.

„Security is a process not a product!“

Bruce Schneier



The four elements of Red Teaming

Intel Service

Red Team Tests

War Games

Resilience Training

Intel Service

A good understanding of risks and threats is essential for the improvement of universal resilience and adaptability.

The English term “intelligence” or “intel” has its origin in the military and intelligence services, and describes the collection, processing and dissemination for a specific purpose.

A precise knowledge of complex and fast-moving developments in this area forms the basis for all actions focused on resilience.

Our Intel Service provides our clients with effective assessments that allow 360-degree view of the existing, individual threat landscape. Beyond this, in cooperation with the companies we support, we develop scenarios based on these findings, by means of which our customers’ resilience can be improved and maintained in the long term.

Two areas are essential to the offer: firstly, the quality and diversity of the underlying information is of central importance. The continual, professional evaluation of this information is the second decisive component of our service.

Against this background, our information procurement is extremely broad and diverse. Open Source Intelligence (OSINT) is a central element of this process. This primarily involves searching the internet for suitable information. For us, in addition to advanced analyst-driven searches using search engines, this explicitly includes the Deep and Dark Web. Software and tools using artificial intelligence (AI) enable us to obtain and classify relevant information from thousands and thousands of primary sources.

The Intel Service implies the involvement of our clients at all times. Apart from a standardized self-assessment developed by us, which serves as an important indicator, we plan and design possible attack scenarios in workshops together with the users of our offer. The development of these scenarios is based on statistical assumptions that are placed in relation to our customers’ goals and allow us to make forecasts about the future threat landscape.

Red Team Tests

In our Red Team Tests, we simulate a realistic adversarial attack against an organization. We seek to identify and exploit vulnerabilities and demonstrate how this could harm business-critical assets. The purpose of a Red Team Test is to assess the resilience of an organization.

Our tests 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 respective organization.

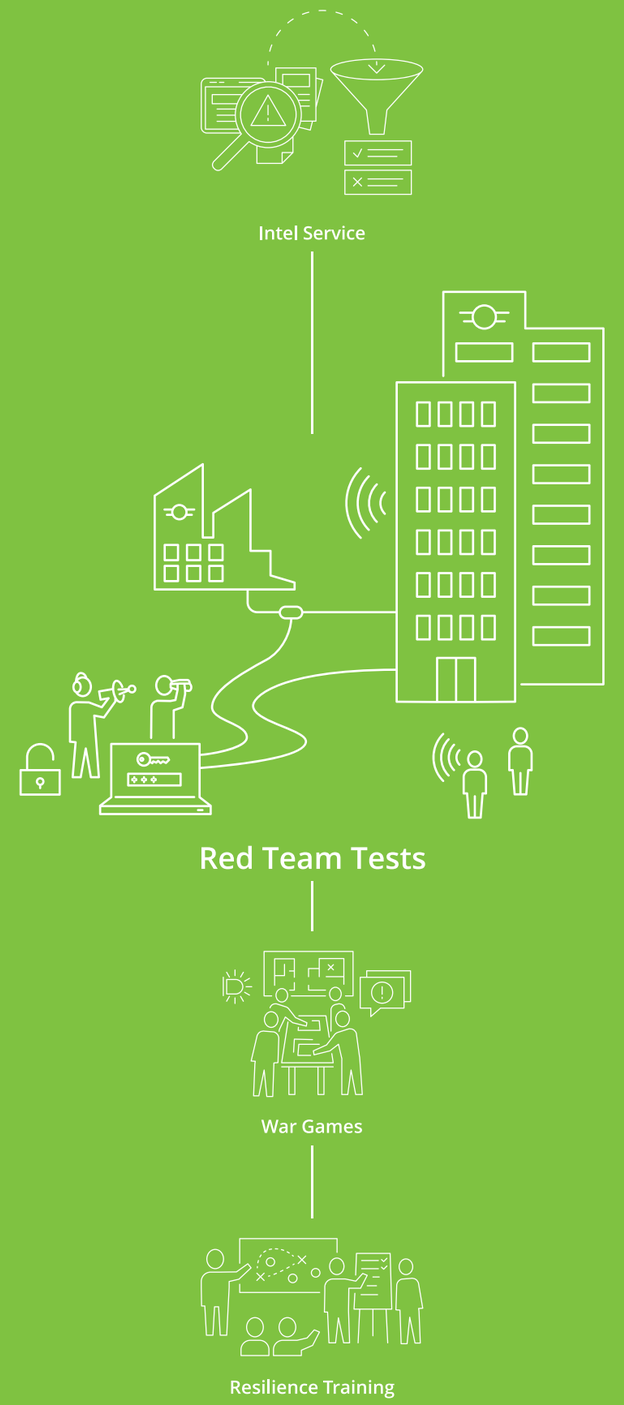
The aim of the Red Team Tests is to identify and exploit unknown vulnerabilities and attack vectors that can be used to target company assets by e.g. simulating the disruption of processes or theft of confidential data. When developing these scenarios and executing the tests, we are performing an evaluation of the physical security of facilities, the security of 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, among other things, might contain:

- Attempts to trick employees into revealing confidential information or performing inadequate actions and thus unintentionally support the attack of the Red Team
- Reconnaissance of the physical perimeter 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 a network and / or applications, and subsequently perform lateral movements towards the targeted asset

Our tests hence provide insights about whether adequate security controls have been established and whether they are being effectively applied. The ultimate purpose is a realistic assessment of organizational resilience.

Before and during our Red Team Test, we are in close consultation with our customers to define and observe any restraints or constraints that apply to the specific test.

Within the test report, our experts describe the approach and the respective findings and observations. Here we also outline the severity of the findings with regard to the organization's resilience. This is complemented by specific recommendation for improvement in technical controls, processes, policies and capabilities.



War Games

War Games are scenario-based simulations that challenge and test an organization's responsiveness. The members of crisis teams are the central actors in these exercises.

Corporate crises are multifaceted and can hit any organization spontaneously and unexpectedly. Various past crises have demonstrated that rapid, targeted action can significantly reduce the extent of a crisis. A well-rehearsed, fast, and self-assured crisis management team is a significant cornerstone of a resilient organization. Apart from sound 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 our War Games, crisis teams are prepared and trained for emergencies in a safe environment. The scope and scenario of the exercises are specifically agreed in advance and adapted to the needs and abilities of our client.

The selection of a suitable scenario is significantly influenced by the probabilities determined by our Intel Service. This gives our clients the opportunity to improve their internal competencies under guidance and at the same time to practice a scenario which is vital for the organization and thus to directly prepare the organization for a possible crisis.

Since corporate crises are difficult to predict and highly diverse, our War Games are not aimed at pre-testing specific cases, but at individually adaptable staff work. Behavior patterns rehearsed in safety offer the necessary backing in stressful situations.

This behavioral confidence is permanently provoked by our team during the War Games. The reactions of the crisis management team provoke a new counter-reaction from our 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.

Resilience Training

In cooperation with our clients, our Resilience Training eliminates vulnerabilities and deficits.

We are a permanent sparring partner for our clients. The mere recognition of fields of action by Intel Service, Red Team Testing and War Gaming does not create a higher resilience. Ongoing, goal-oriented training involving all relevant actors guarantees maximum success on the way to a resilient organization.

Our training is based on the identification of the topics to be trained. Our team coordinates this with you as the client; it relates back to your self-assessment, among other things. Building on this, we include our findings from the areas of Intel Service, Red Team Tests and War Games in the design of the training program. The exact target group of the individual training courses is laid down individually for each topic jointly with our clients. In this way, the distinct training program can reach the necessary participants in a targeted manner and deliver maximum added value. The scope and type of training are tailored precisely to the needs of our clients and are constantly adapted.

Our experienced trainers accompany the training groups during the various stages. For this, they draw on their expertise in a variety of disciplines and thus ensure an integrated learning concept.

The training possibilities range from awareness training to staff training and concrete improvements in organizational and structural conditions.

An example of such training is Bias Testing. This is about making oneself aware of unconsciously prevailing biases, i. e., errors of thought, and instilling concrete, mental mechanisms in staff to protect them from these misconceptions. Bias Testing and Training help to reduce or avoid weak points arising from the human element and are effectively strengthened by options for action developed in Red Teaming. Our clients' learning outcome is accompanied by our team, and training plans are continually adapted. This enables us to respond individually to our clients' needs and actively control the further development of individual target groups within the company. This is an important part of building and expanding the company's resilience and contributes significantly to reducing current and avoiding future weaknesses.

Our Resilience Training thus completes the circle of the four core elements of our Red Teaming offer.

Intel Service

Red Team Tests

War Games

Resilience Training

Threat Intelligence-based Ethical Red Teaming

The rapidly growing security challenges are not only a core topic for individual companies, but also an important discussion point at national, European and international level.

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

The TIBER-EU process consists of an optional, introductory phase and three mandatory phases:

Generic Threat Landscape Phase

The (optional) Generic Threat Landscape (GLT) Phase involves a generic 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.

01. Preparation Phase

This phase involves the formal launch of the TIBER-EU 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 TI and RT providers are procured to carry out the tests.

02. Testing Phase

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

03. Closure Phase

The Closure Phase includes remediation planning and result sharing. The RT 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.

TIBER-EU Process

TIBER-EU tests must be carried out by independent, external providers. This applies to both the Threat Intelligence and the Red Teaming areas. The external service provider carries out the tests in collaboration with the entity and prepares the necessary analyses in the form of a Targeted Threat Intelligence Report and a Red Team Test Report.

With its Red Teaming approach, Deloitte offers individualized solutions from a single source. With our extensive experience and interdisciplinary competencies, we can map the entire process of the TIBER-EU framework from start to finish and cover both Threat Intelligence and Red Teaming with our team. The wide-ranging, in-depth expertise of our team enables us to respond specifically to the needs and circumstances of each individual client. We offer a tailor-made solution with maximum effectiveness within the scope defined by the TIBER-EU Framework.

A special starting point for our team is the creation of the "Generic Threat Landscape" in the first process step. This addresses the most significant threats to the banking sector and provides the basis for developing attack scenarios for Red Teaming tests. This threat landscape can likewise be included in the Targeted Threat Intelligence Report. That is why exceptional importance attaches to it. The Red Team uses a combination of proven Threat Intelligence techniques and innovative artificial intelligence (AI) to create this generic threat landscape. The focus is not only on current threats to the client but also on future trends and developments. In order to ensure the continual benefit of Red Teaming results and to be permanently available to our customers, the Red Teaming approach not only applies to one-off tests and reports, but also offers the prospect of permanent monitoring. Thereby a client's resilience can be guaranteed on a longterm and sustainable basis in view of the very dynamic and highly complex area of cyber-security. In combination with our innovative Red Teaming approach, the client can be optimally and individually supported beyond the TIBER-EU framework.

TIBER-EU objectives:

- Development of cyber-resilience in the target entities and in the financial sector in general
- Standardized and harmonized Red Teaming processes within the EU with sufficient flexibility to adapt to national conditions
- Providing authorities with a guide to establishing, implementing, and managing Red Teaming at national and European level
- Support for cross-border Red Teaming for multinational entities
- Enabling an exchange between authorities through common standardized Red Teaming processes and thus regulatory relief of individual member states
- Creation of a common protocol for cross-border collaboration, exchange of results, and analysis

Our Team

Our Red Team bundles expert knowledge from the most diverse areas.

The interdisciplinary team consists of cyber-specialists, economics experts, computer scientists, intelligence analysts, former military officers, and political scientists, and thus covers the key fields of organizational resilience. Thus, in addition to the relevant expertise, 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 Intel Service, 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 Testing. Concrete, industry-specific experience in the creation and implementation of development plans round off the range of skills in the Resilience Training discipline.

Our specialists contribute their individual experience in Threat Intelligence, Open Source Intelligence, Social Media Analysis, Social Engineering, Penetration Testing, Red Team Testing, War Gaming, and Trend Analysis to all elements of our Red Teaming. Our team is supported by the technologies and competencies of the Deloitte Cyber Intelligence Center (CIC) in Frankfurt. This enables a holistic view of possible threat scenarios and resilience strategies.

The Deloitte Network
In order to continually optimize our work, the Red Team draws on the extensive international Deloitte Network. Intense collaboration with Deloitte's own expert centers enables groundbreaking innovations to be incorporated into Red Teaming processes. In cooperation with the Center for the Long View (CLV), the Deloitte Center of Excellence for scenario planning, a future-proof scenario analysis of possible Threat Landscapes can take place.

By involving the Deloitte Neuroscience Institute, neuroscientific methods such as eye tracking or the measurement of brainwaves can be used to better understand the effects of unconscious processes on decision-making and derive relevant measures from them.

In cooperation with the Deloitte Analytics Institute, the Deloitte Competence Center for Analytics, the Red Team can access additional data analyses and interactive data visualization and thus actively contribute complex data fields such as Big Data Analytics to strengthening your resilience.

The Red Team is effectively strengthened by the inclusion of these and other Expert Centers, thus offering you a completely rounded-off service package from one source.

How can we best support your company? To assess how we can support you in systematically increasing your organizational resilience through Red Teaming, we propose the following next steps:

1

Within the framework of a half-day workshop we present our Red Teaming concept in detail and in person. We then conduct a structured interview with you to assess your present situation. For this, we examine – on the basis of the relevant standards – your security concepts, processes and organization, your analysis and evaluation of security risks and also the status of your training and education measures.

2

On this basis, we give you an initial assessment of your present resilience and discuss with you the opportunities for improvement.

3

We prepare an individual offer for you in which we address the fields of action identified with the help of the coordinated and continual deployment of our four services (Intel Service, Red Team Tests, War Games, Resilience Training).

Contact

Peter J. Wirnsperger
Partner, Head of Cyber Risk
Phone: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Ralph Noll
Partner, Cyber Risk
Phone: +49 (0)211 8772 2285
rnoll@deloitte.de

Knut Schönfelder
Senior Manager Cyber Risk, Head of Red Team
Phone: +49 (0)40 32080 4447
kschoenfelder@deloitte.de

Which questions do you have about our Red Team service?

We will be happy to provide the answers.

You can find more information at our website www.deloitte.com

Deloitte.

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 286,000 professionals are committed to making an impact that matters.