
NTT
Red Team Operations
Readiness through offensive security

Introduction

Every organization needs to plan for a potential breach, no matter how strong its security defenses are. In order to detect a breach and contain it, the organization's incident response team (blue team) needs to practice their approach and methodologies on a regular basis to keep abreast of the latest techniques and tactics.

Our research (Global Risk Value Report 2019) has shown that the costs of a data breach and recovering from it is 12,7% of an organization's revenue and the recovery time is on average 66 days. A well-trained incident response team has shown great value to cut down the incurred costs to recover from a data/security breach.

With an ever-evolving threat landscape and IT perimeters growing year after year, it's of utmost importance to have an effective strategy and up-to-date capabilities to detect and defend against sophisticated attackers.

NTT Red Team Operations (RTO) can simulate real-world attacks with similar TTPs as real threat actors. These operations are performed in a controlled manner to train and improve detection and mitigation strategies.

A growing number of organizations are looking for services that can simulate real-world attacks executed with similar tactics, techniques and procedures (TTPs), as seen 'in the wild', so they can evaluate their current state of readiness for detecting and responding to breaches. These exercises uncover gaps within the security fabric of an organization, which are not visible in normal day-to-day operations.

NTT Red Team Operations is a seasoned team of red team operators acting as ethical hackers, with more than 45 years of experience combined. Our team has a proven track record in discovering critical vulnerabilities in the most complex environments.

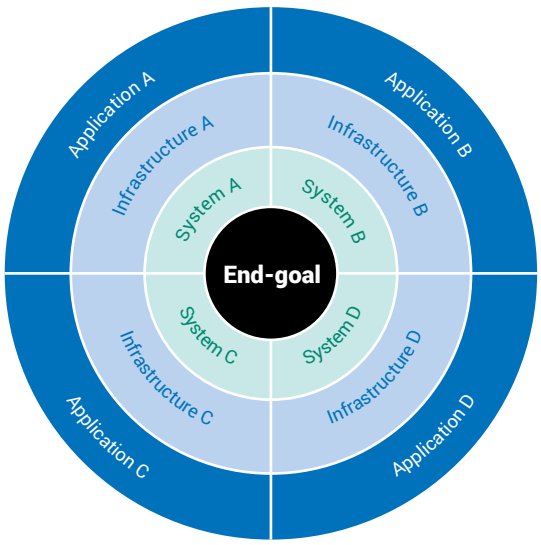
They have extensive prior background in designing and implementing high-end IT infrastructures, with expertise in testing environments covering a variety of system and application technologies, frameworks, and a wide range of potential attack vectors.

This document aims to provide a broad view of our offensive security capabilities. While it contains examples of different projects, it's only a subset of all that NTT can offer to you. Most of our clients have special requests based on their reality and for which NTT tailors a customized approach that fulfils their specific needs.

Red Team vs penetration testing

Penetration testing services aim to identify and exploit vulnerabilities so that they can be prioritized for remediation. Typically, such tests are conducted over a short timespan (days), on well-defined assets and scope, and IT security are instructed to temporarily lay off certain defenses and response procedures so that a more complete worst-case assessment can be performed.

In comparison, red teaming always targets specific objectives and relies on stealth and evasion. A strong focus is set on reconnaissance in which information is collected that will help the Red Team Operators to effectively plan their attacks avoiding detection by the client security team (blue team). Only a limited set of people (white team) is aware of the incoming/ongoing attack on the organization and the blue team is kept in the dark. The red team will not attempt to identify all vulnerabilities, but will try to find a way to achieve the predefined milestones by exploiting vulnerabilities and security gaps in deployed technologies, company processes and people's behavior. Experienced red teaming operators will then be able to chain vulnerabilities from different levels to successfully achieve their target, uncovering previously unidentified security gaps. Blue teams will be challenged and put under pressure by simulating a real attack, which can be measured by the organization to further improve the responsiveness and effectiveness of their defense strategies.



Red team

- Broad and objective-based
- All phases of cyberattacks
- Stealthy
- Attack paths/threats reported

Scenario-based penetration testing is a healthy mix of both classic penetration testing and red teaming. Similarly, in penetration testing, the goal is to identify as many exploitable vulnerabilities as possible within a given timeframe and on limited scope. Like red teaming, the combination of the different phases of the scenario aimed at reaching a specific goal (elevate privileges, compromise a specific server, and more). In scenario-based penetration testing, the organization and the security teams are aware of the tests and should not intervene to stop any attack.

Pentesting

- Limited and precise
- No further than exploitation
- No blue team exercises
- Vulnerabilities reported

Red Team operations

Adversary Simulation

A Red Team Operation simulates a real adversary attempting to gain access to an organization's most critical assets and data using the same tools, techniques, and procedures as a real attacker.

As adversarial capabilities have evolved over the years, so has the information security industry. Network defenders have realized that it's impossible to guarantee the security of every computer system within a large corporate network.

Following this realization, there has been a shift from preventing all unauthorized network entries to having the capability to detect and effectively respond to a current attack. A Red Team Operation helps to verify that this capability is effective.

A Red Team Operation takes place over weeks to months with a specific, agreed goal (for example, modifying a record in a core database). IT security staff aren't informed in any way (except the stakeholders of the exercise: the white team), and all the organization's defenses, policies and procedures are put into play. The Red Team Operation uses a refined methodology which mirrors the actions made by a real advanced attacker attempting to gain access to the organization's critical assets and data.

NTT Red Team methodology is in line with the MITRE ATT&CK framework which is a curated knowledge base and model for cyber adversary behavior. This allows NTT to accurately map all the actions on this model, while making it clear for the blue team what actions they need to take to defend against those attacks.

Recon	• Passive/active scanning • Target mapping • Footprint analysis (OSINT/H|UMINT)
Weaponize	• Malware development • 0-day research • Custom phishing mail creation
Delivery	• Send phishing campaigns • Upload malware • Launch 0-day issues against target
Execution	• Victims exploited by phishing mails • Malware executed on a DMZ server • 0-day exploit verified by executing a command
Installation	• Phishing credetials used on VPN • Malware tries to persist on the machine
C2	• Identify outgoing channels • Establish a stable connection • Execute commands and send output.

Performing these engagements regularly creates a feedback loop that improves employee security awareness, validates and improves the implementation of security operations, sharpen incident response procedures, and trains security personnel on how to act effectively in the face of a breach or incident.

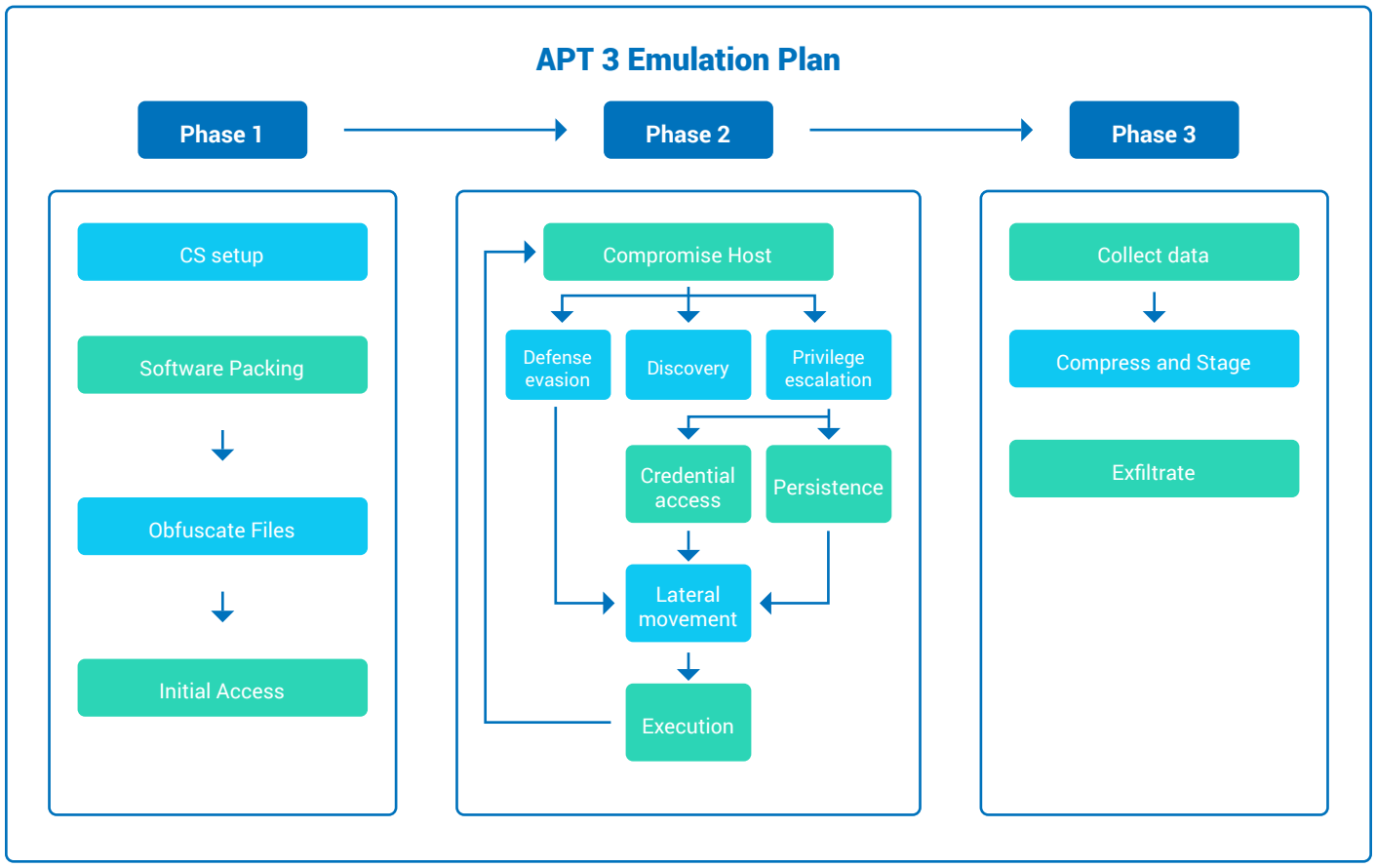
As a result of the assessment, NTT will provide a report that contains a milestone-based attack narrative mapped against the MITRE ATT&CK Framework and a detailed explanation of the identified weaknesses. It will include a set of recommendations to combat these weaknesses.

Adversary Emulation

Unlike typical Red Team operations where attacks are planned and calibrated based on the specific environment of the target organization, adversary emulation aims to mimic a threat based on real-world intrusion cases. Usually, these cases were originally executed by Advanced Persistent Threats (APTs) such as nation states or cybercrime groups.

These intrusion campaign plans, and their phases are well documented through many threat intelligence reports focusing on malware reverse engineering, initial compromise techniques and command and control usage. These are mapped against the MITRE ATT&CK framework and any missing gaps are filled in by using other known adversary tactics, techniques and procedures (TTPs) and behaviors.

NTT red team operators can execute these plans to test client resilience against APT style attacks.



Threat Intelligence-based Ethical Red-Teaming (TIBER)

TIBER, short for Threat Intelligence Based Ethical Redteaming, is a framework for controlled and customized cyberattack testing that has been released by the European Central Bank (ECB) in 2018. It is a novel way to test the resilience and detection capabilities of a company by utilizing the tools, techniques, and procedures (TTPs) of real-life threat actors as defined by the threat intelligence team.

The TTPs used are based on threat intelligence information specifically targeting the financial sector.

A conventional Red Team Operation involves several participants such as the blue team and the white team. In addition to this a threat intelligence provider and a dedicated TIBER cyber team also participate. The latter is responsible for overseeing the test and making sure it meets the regulatory requirements based on the TIBER framework.

TIBER has been adopted by most European financial institutions and regulated by a national authority.

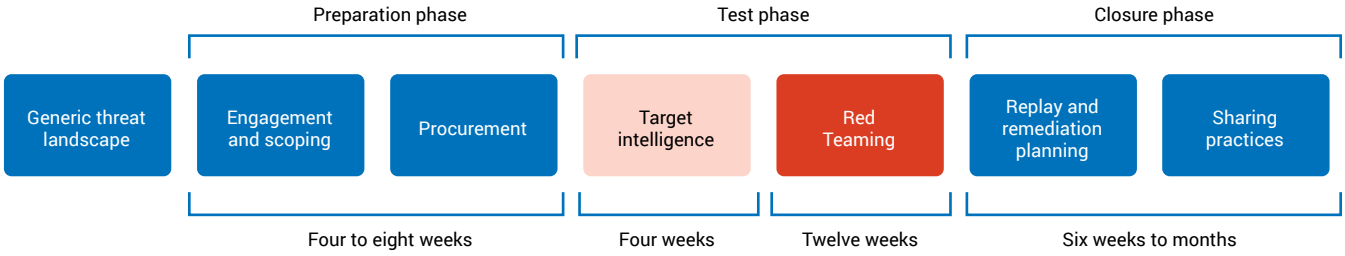
A typical TIBER exercise consists of three phases: preparation, testing and closure. The preparation phase consists of setting the rules of engagement, as well as defining the roles and responsibilities of each stakeholder, such as the security incident escalation chain, security protocols to follow, and so on.

The testing phase is the core of the exercise and is further split into two sub-phases. The first one, supplied by the threat intelligence provider, creates a targeted threat intelligence report, setting out possible scenarios for the future test and any useful information on the targeted entity. This report is shared with the red team who, during the second subphase, develops attack scenarios based on the information available in the report and executes them on the production environment of the client.

After all tests and scenarios are concluded, the closure phase allows to share information with the client on the taken approach, on any finding discovered during the tests and on possible improvements to make in terms of technical controls, policies, or procedures. This phase is usually finished with the delivery of an extended report.

While the framework was initially created for financial institutions, it could also be used by other industries to perform similar types of threat intelligence-based red team missions.

The TIBER Framework test process and the roles involved



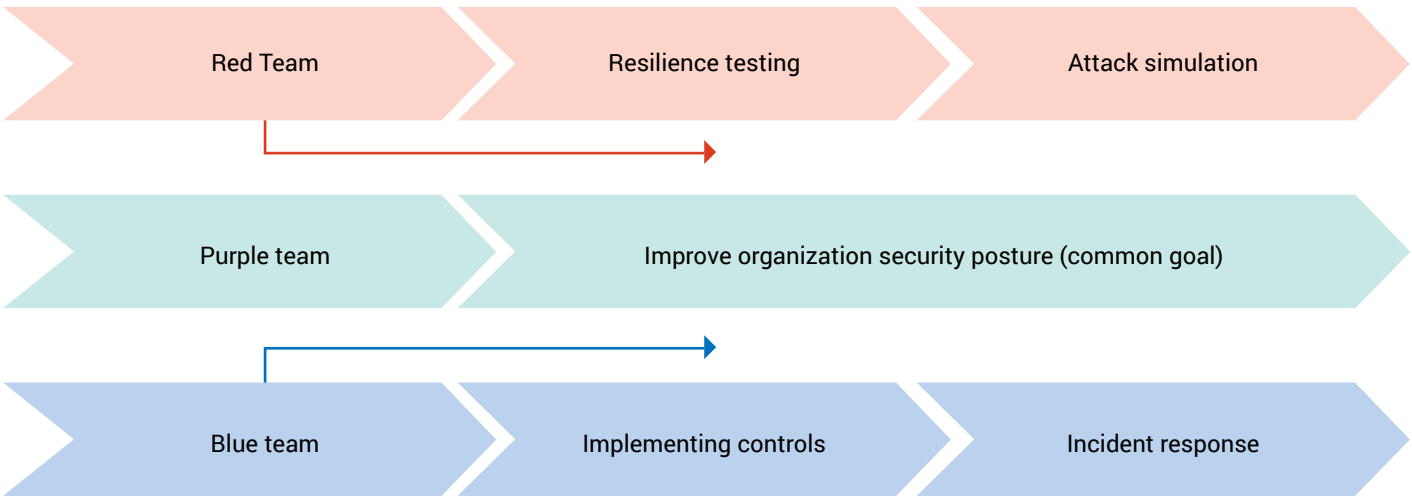
Purple Teaming

The goal of a purple team exercise is identical to a red team engagement: assessing the detection and response capabilities of a company. The difference lies in the purpose of the engagement which is more oriented towards a continuous improvement and learning of the blue team during the engagement. During a purple team assessment, there is close collaboration between the company's IT security staff (blue team) and NTT. While the defenders aren't informed about the TTPs used by the attackers during a red team engagement, it is the case with a purple team engagement. By following this approach, the blue team can continuously customize, adapt and improve its detection and response capability during the full lifecycle of the engagement.

Both teams are working together to improve the overall security posture of the organization by continuously sharpening and tweaking their detection and mitigation strategies.

The most common ways to have an efficient purple team are:

- **Reactive mode:** red team performs TTPs and synchronizes with the blue team after each milestone reviewing which attacks were detected and mitigated and which slipped through the net.
- **In-person collaboration mode:** The red team and the blue team sit together and have continuous discussions. While the red team performs their TTPs, the blue team can give live feedback on what exactly was triggered. The Red Ream could adapt their TTPs to evade the mitigations for the blue team to further harden their security controls.

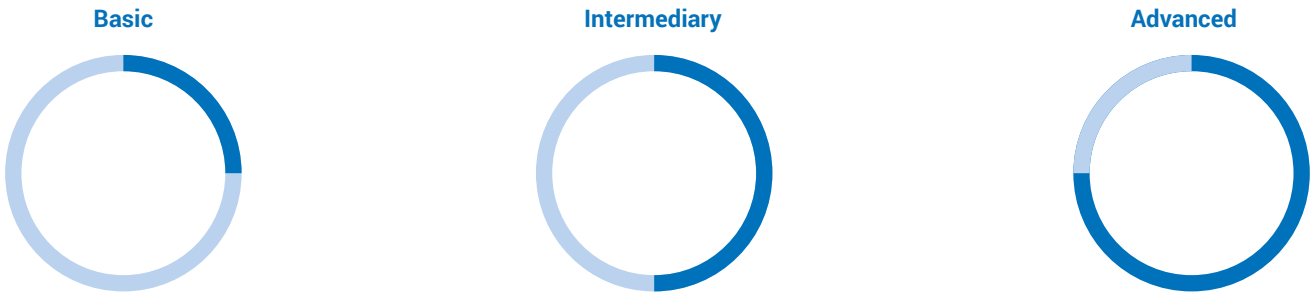


The return on investment for an organization performing purple teaming is quite significant. The short feedback loop between the attackers and defenders results in little time lost from the actual attack to the implemented mitigation strategy.

Fine-tuning cybersecurity defenses

Organizations might want to validate and perform tests on specific (technical) controls implemented within their larger cyber security defense layer. Testing and validating controls such as firewall filtering, endpoint detection and response (EDR), email security sandboxes, network detection capabilities and more, help to determine their effectiveness against advanced and common attacks and threats.

These tests establish a baseline which assists organizations to close any gaps that were identified during the tests. NTT Red Team Operations has developed packaged attacks that range from basic difficulty up to advanced APT level so defenses can be tested, gradually uncovering any possible gaps.



NTT has different teams (incident response teams, security and Operations Consulting Services, Managed Security Services, and more) that could assist **clients closing those gaps, based on the observations of the fine-tuning tests.**

Social Engineering

Physical intrusion is the most straightforward scenario that's often combined with other attack vectors such as Wi-Fi and internal network breaches. All information systems physically exposed in company premises are directly vulnerable to physical intrusions.

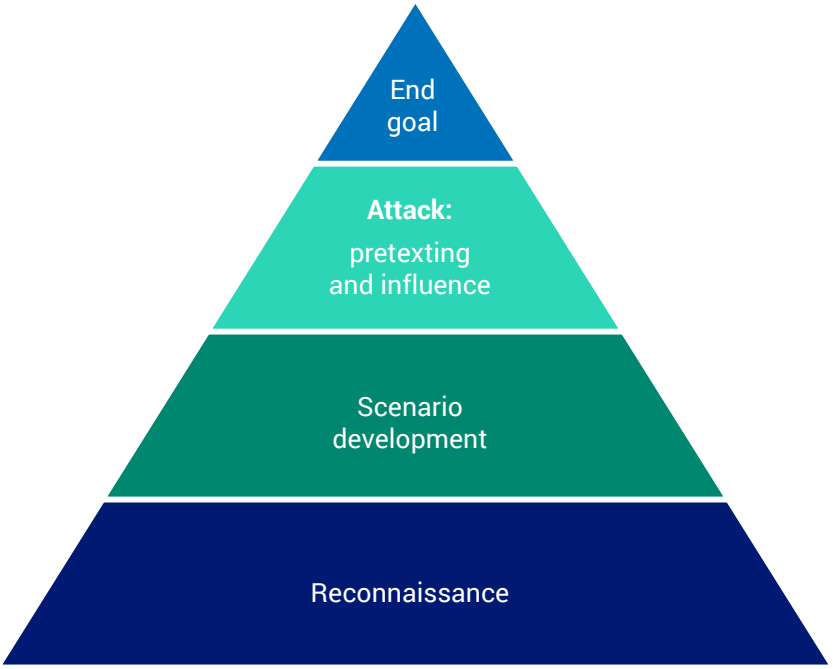
A 'breaching the perimeter' scenario focuses on the first two layers of defence: the physical protections and the person. NTT ethical hackers will assess the security awareness of the employees and attempt to obtain privileged access to information systems from inside the company buildings.

The company assets will be assessed with tools such as wireless antennas, embedded systems to attach via USB or RJ45 and any other ways to bypass physical controls, like badge cloning devices. The ethical hackers will prepare several scenarios in which they use pretexting and influence techniques against company employees to reach the predefined objectives.

The goal(s) of a social engineering attack are defined at the start of the engagement. Examples are:

- intrusion in high-security areas
- obtain an entry in the internal network, via an RJ45 outlet or others
- deploy malware on an employee's laptop
- steal confidential information

Reporting of the mission will highlight **the vulnerable paths in the physical protections,** as well as **the security awareness improvement areas**



Vulnerability research

Making the difference

Our Red Team Operators strive to make an impact in the world of cybersecurity. Dedicated time is spent on researching vulnerabilities in well-known vendor products.

We continuously increase our skills through training and research into products widely used by organizations around the world. As a result, the team has an arsenal of exploits previously unknown to the public, which is used to demonstrate the strengths and capabilities during NTT red team operations.

We're also very active in Capture The Flag (CTF) competitions and bug bounty hunting.

Recognised certifications (Offensive Security, SANS, …)	**40+** disclosed vulnerabilities (CVEs)	**CTF team**	**Active** in Bug Bounty


NTT