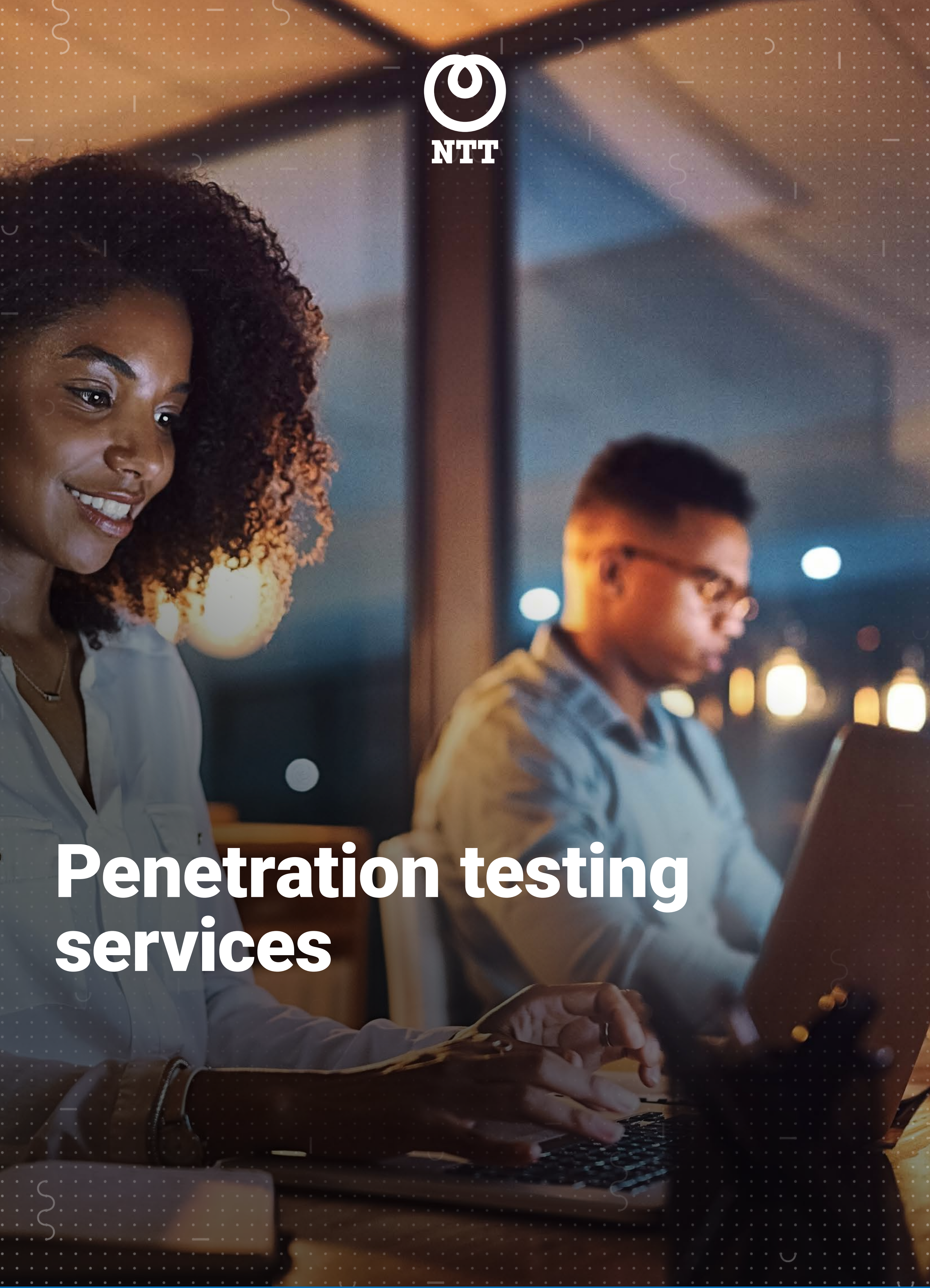
NTT



Penetration testing services

Table of Contents

Introduction

In an **increasingly digital world,** business operations and processes are becoming fully intertwined with **new technologies.** These technologies bring with them **some potential risks** to your IT infrastructure, giving attackers the possibility to disrupt and steal sensitive data.

Penetration testing services allows an organization to subject these new technologies to **cyberattacks** in a **controlled fashion** to make their IT infrastructure **more resilient and determine if the technologies deployed are working as expected.**

We have an experienced team of consultants acting as ethical hackers, with more than 45 years of combined experience. Our team has a proven track record in discovering **critical vulnerabilities in the most complex environments.** They've extensive prior background in designing and implementing high-end IT infrastructures, with expertise in testing environments covering a variety of infrastructure, system and application technologies and frameworks, and a broad range potential attack vectors.

Our approach **evaluates** organizations' current **operating environments** and with tailored **business-**specific **risks** enables organizations to accurately target areas with the most risk, focusing attention where it's needed most. These approaches challenge your current environment from different points-of-views starting **from the outsider threat to the malicious insider,** assuring each layer of access is tackled.

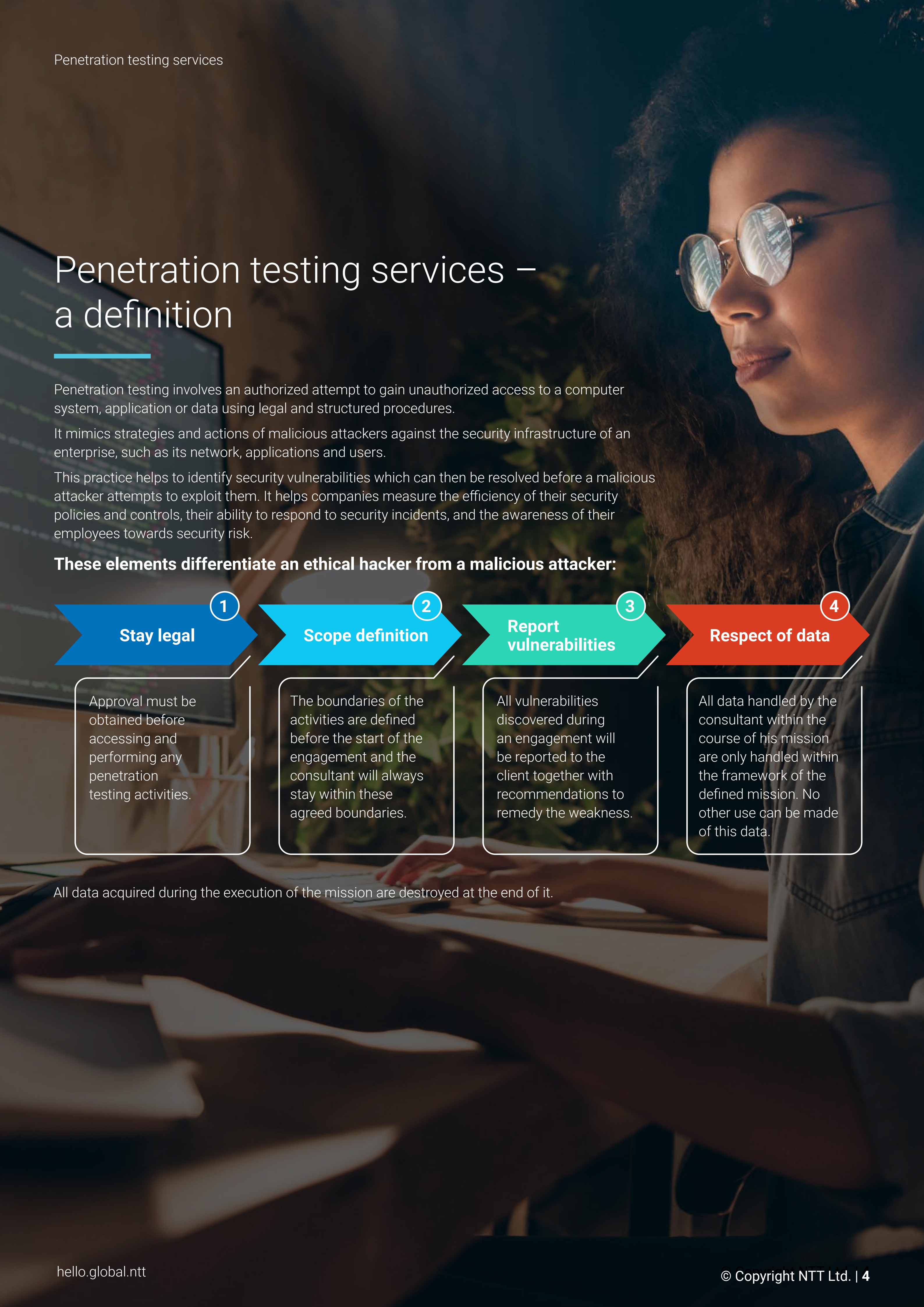
Our engagements are **immensely versatile** and can be **tailored** specifically for each organizations' demands. Our preferred method is to start with questions that **challenge your current IT landscape:**

- **What's the real impact** if an employee's machine is compromised while homeworking?
- Is my **organization ready** to withstand a sophisticated but realistic cyberattack?
- Are we able to **identify active threats** and shut them down?

These questions are the starting point to build out a scenario that would challenge each aspect of your IT Environment.

This document aims to provide a broad view of our offensive security capabilities, and contains a set of different projects, it doesn't contain everything the team has experience with. Feel free to reach out if you didn't find what you're looking for in the offering or have a special request. We'll suggest an approach that's both distinct and fulfills your needs.

For further questions, please contact your account manager.



Penetration testing services – a definition

Penetration testing involves an authorized attempt to gain unauthorized access to a computer system, application or data using legal and structured procedures.

It mimics strategies and actions of malicious attackers against the security infrastructure of an enterprise, such as its network, applications and users.

This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker attempts to exploit them. It helps companies measure the efficiency of their security policies and controls, their ability to respond to security incidents, and the awareness of their employees towards security risk.

These elements differentiate an ethical hacker from a malicious attacker:

1 **Stay legal**

Approval must be obtained before accessing and performing any penetration testing activities.

2 **Scope definition**

The boundaries of the activities are defined before the start of the engagement and the consultant will always stay within these agreed boundaries.

3 **Report vulnerabilities**

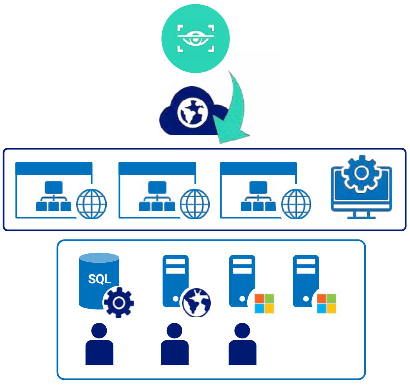
All vulnerabilities discovered during an engagement will be reported to the client together with recommendations to remedy the weakness.

4 **Respect of data**

All data handled by the consultant within the course of his mission are only handled within the framework of the defined mission. No other use can be made of this data.

All data acquired during the execution of the mission are destroyed at the end of it.

Infrastructure



External perimeter

External penetration testing service is a security assessment of an organization's internet-facing perimeter. By nature, they're the most exposed systems as they are out in the open and are therefore the most easily and regularly attacked.

These services and systems are examples of typical targets:

- web servers
- mail servers
- remote access services (VPN)
- other remotely accessible servers

The aim of an external penetration testing service is to find ways to compromise your accessible and externally available systems and services, gain access to sensitive information, and discover methods an attacker could use to attack your clients or users. In these exercises, the security professionals conducting the assessment will replicate the activities of real hackers, after granted permission to attempt to gain control of systems. They'll also test the extent of any weaknesses discovered to see how far a malicious attacker could dive into your network and what the business impact of a successful attack would be.

External penetration testing service usually tests from the perspective of an attacker with no prior access to your systems or networks. It makes sense to first cover off the fundamentals and consider internal testing only after both regular vulnerability scanning, and external penetration testing services are being performed.

An external perimeter penetration testing services commonly look at following categories of elements:

- reconnaissance and OSINT
- port scanning
- enumeration of web services
- examination of remote access services like VPN, SSH, RDP, etc.
- discovery and validation of publicly leaked user credentials and documents
- file sharing protocols
- e-mail services
- DNS and bind attacks
- outdated software
- others

Internal perimeter

Every organization has different perimeters, an internal perimeter includes everything after the DMZ from a network point of view. It's the network that's typically used by employees to do their day-to-day activities.

Internal infrastructure penetration testing services target a company's internal network and systems. This test takes the point of view of several actors, the two most important being:

- An attacker that gained a foothold in the internal network (through phishing, malware, external breach, VPN credentials).
- A disgruntled employee who wants to cause damage to the organization.

The threat landscape of the internal network differs across clients depending on sector, network size, and number of employees. Lots of different devices are now connected and impose a potential danger to your business ranging from IoT, workstations and servers to the whole active directory infrastructure.

The typical internal network servers, services and supporting infrastructure including (web) applications, Microsoft Active Directory services, DHCP, DNS, routing and switching systems will be found and assessed on the internal network.

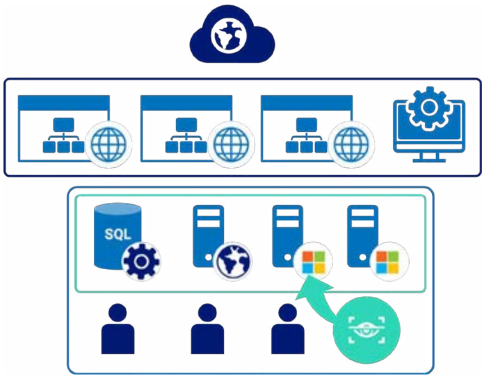
We'll discover issues on the level of network services, their configuration and the software delivering these services, and on the underlying operating system level. This approach is more focused on identifying instances of known security issues, typically in common off-the-shelf software (i.e., disclosed security vulnerabilities).

In comparison to an external perimeter this test will solely look at the internal local network of an organization. As most organizations put significant efforts to protect it.

Common things that are tested during an internal penetration testing service are:

- information gathering and network discovery
- port scanning
- enumeration of web services
- eavesdropping on the network
- discovery and validation of publicly leaked user credentials and documents
- file sharing protocols
- e-mail services
- DNS and bind attacks
- outdated software and obsolete operating systems
- others

As a result of external or internal perimeter assessments, we'll provide a report that contains a milestone-driven attack narrative and detailed explanation of the identified weaknesses. It'll also include a set of recommendations to combat these weaknesses.



(Azure) Active Directory

For most companies their Active Directory environment is paramount and approximately 90% of Global Fortune 1000 companies use it. It usually stores and protects the 'crown jewels' of the organization. This is why most Advanced Persistent Threat (APT) groups target this environment.

The main goal of this kind of assessment is to evaluate resiliency against attacks of what some companies describe as their most important data. While gaining control of the entire Active Directory environment could be a goal by itself, it's not the most prevalent. The outcome of this assessment will provide an overview and detailed explanation of the steps you can take to reduce and **even remediate all the security risks in your domain(s).**

We ll assess your environment based on known security configuration issues. These misconfigurations include, but are not limited to:

- lack of proper user accounts and group protection
- missing security patches
- pilfering of open shares and other unprotected resources
- lack of network protections like unencrypted protocols, IPv6, etc.
- Kerberos-related issues
- privilege escalation vulnerabilities
- trusts between domains and between objects
- assigned permissions on objects
- lack of endpoint protection
- insecure authentication mechanisms

As a result of the assessment, we ll provide a report that contains a milestone-driven attack narrative and detailed explanation of the identified weaknesses. It'll also include a set of recommendations to combat these weaknesses.

Cloud

A lot of companies are moving their infrastructure to the cloud. Cloud environments have their own set of security challenges. It's important cloud infrastructure is configured correctly.

Cloud platforms have become an extension of on-premises environments and are often interconnected. Cloud isn't more or less, secure than its on-premises counterpart, but it does require a different approach when it comes to security.

In this type of assessment, we look at the configuration of your cloud infrastructure to make sure everything is configured in a secure way. Checks include, but are not limited to:

- key-material handling
- access to cloud platform
- access to services (e.g., blob storage permissions)
- logging/monitoring configuration
- network configuration
- cloud Architecture review

Typical solutions we're experienced with:

- Azure
- AWS
- Office 365

At the end of the assessment, we ll deliver a report with several recommendations related to your cloud infrastructure. These will range from actual security threats to recommendations for hardening the security of your cloud environment.

ICS - OT/Scada

Most ICS networks consist of regular IT infrastructure combined with PLC's and other industrial hardware. ICS differs from regular IT systems in the way they're meant to be used:

ICS is built to work and last. Software updates are often postponed because thorough tests must be performed to make sure the device is compatible and can operate as it should. Updates disrupting the ICS chain can lead to severe consequences such as loss of productivity or accidents caused by invalid device instructions. Missing updates, however, expose the device to known vulnerabilities or exploits that are sometimes publicly available.

Hardware used in ICS has limited computing power in terms of networking and processing. Overflowing the PLC hardware might lead to crashes or unexpected behavior, and it's therefore important that networks are properly segregated to limit the amount of network traffic. A single attacker can overflow several devices by sending many packets.

Hardware used in ICS networks is often not secure by design, as their only purpose is to perform a certain job which is why network security is mostly overlooked. As a result, popular network communication protocols between ICS devices are proven to be insecure, which allows an attacker to easily control several devices once an initial breach has happened.

The company ICS environment is an interesting target for an attacker as it's easy to exploit due to missing patches or outdated software. A lot of attacks start from a breached (employee) IT environment further used as hop to your ICS network. Once inside, the adversary might get control over various business processes altering or disrupting the normal production flow.

At NTT, we know how critical ICS is to your company and have extensive knowledge on how to approach such devices without risking disrupting your workflow. Industrial network penetration testing services differ from a regular IT infrastructure, as devices need to be handled with extra caution. We won't perform intrusive network scans, use exploits that might disrupt a device in a production environment, send messages to devices using industrial network protocols or tamper with the on-device UI. We continuously monitor the devices' state so we can intervene as quickly as possible.

A typical ICS penetration testing service covers both on-device level as well as network-level to make sure we cover all attack vectors.

The following controls are covered in an ICS penetration testing services:

- assessment of ICS network-wise security controls (VLAN config, broadcast traffic, network access)
- assessment of device network protocols (modbus, DNP)
- assessment of outdated and/or vulnerable devices and software.
- assessment of device-specific software (web servers, databases, ...).

The assessment results in a report of findings which you can mitigate in order to improve security of both network and devices. Vulnerable devices or networks are identified and can be patched or segregated to limit access.

© Copyright NTT Ltd. | 6

Wireless

Nowadays it's safe to assume that every company has some form of wireless network in their vicinity. While this offers convenience for their employees, it doesn't come without risk. The objective of a wireless network penetration testing service is to assess the security strength of the targeted wireless network environments. The focus of this engagement is to measure the security risk of the Wi-Fi network against attackers in reach, in terms of confidentiality but also from a data exchange integrity and availability point of view.

With this engagement, you'll have a clear view on the security risk introduced by the wireless network configured in a specific physical location (typically an office building), and what the likelihood is of a successful attack conducted by an adversary physically in reach of the wireless signal. The security impact on the confidentiality of the data exchanged in the wireless communication is also given as a result, as well as the threat to the availability of the service (i.e., capability of an adversary to take down the network). Finally, the impact measured on the system (and data) integrity is also given, for example if spoofed access points are deployed successfully in your existing network.

In addition to the security tests, the assessment can also include an interview with the network administrator and a configuration review of the wireless access points, if a white-box approach is chosen.

Container/sandbox escape (Citrix, Kiosks, PoS, etc.)

In a digital world, interactive kiosks can be found everywhere to improve customer experiences from airports to business lobbies, from taxis to ATM systems.

These systems are customer facing and exposed to the wider public. As these systems often handle personal identifiable information (PII), they can be prime targets for bad actors to steal data or get a foothold in the internal network.

Kiosk software is sometimes run in a physical or virtual container to prevent manipulation or tampering of the underlaying operating system or protect unauthorized access to the internal network.

As a result, escaping these containers might grant access to several other instances of other clients or allow an attacker to access the host system. Furthermore, an escape can also be an interesting pivot point to other devices inside the internal network as the controlled container.

There are multiple kinds of containers which determines the way a test is performed:

- software containers (docker, Citrix, Windows containers, kubernetes, appspace)
- hardware containers (point of sale devices, ATM, infoboards, kiosks)
- a combination of both (e.g. a containerized ATM application)

We'll try to break out of software containers by exploiting configuration mistakes or excessive permissions to escalate privileges outside the container. The Specific escape techniques to be used will depend on the used container technology and on the running application (e.g., interaction with other systems outside the container).

As a result of the assessment, we'll provide a report that contains a milestone-driven attack narrative and detailed explanation of the identified weaknesses. It'll also include a set of recommendations to combat these weaknesses.

> Every company has some form of wireless networks in their vicinity. **While this offers convenience for their employees, it doesn't come without risk.**

Host Hardening

Host hardening is used to evaluate the security strength of a typical end point installation and configuration. Because these systems are still commonly targeted for malicious activities, it's important to properly understand their potential security weaknesses and associated risks. The methodology used for Host Hardening consists of a practical technical security evaluation of the desktop environment.

In essence the following scenarios and phases will be evaluated:

Security vulnerabilities and weaknesses: Any potential security weakness and vulnerability will be submitted to a practical confirmation where possible. Typically, this will include validations of the security controls set by the GPO or other locally configured solutions.

Deployment of malware and malicious software through various means: Here the consultants will attempt to install malicious software, in a controlled manner, on the system(s) in scope through various means including USB sticks, mail or other web traffic. Not only will the locally configured security controls (e.g., antivirus and malware) be evaluated, but other network security controls in place will also be checked. This latter is especially important to determine, once a system has been compromised, how the malware is capable of communication with a system on the outside for control or extraction purposes.

Remote connections: The way systems are connected to the remote VPN solution and concentrator will be assessed taking into account previously obtained documentation. This is essential to ensure that systems that are currently in violation of the security policy (e.g., missing patches or updates) are properly mitigated before access is granted to the internal network. This scenario will also cover a general security assessment of the remote VPN solution.

General security compromise through physical or user access: This scenario will simulate malicious behavior of a local desktop user, or external user, without credentials capable of obtaining access to a particular system (e.g., stolen laptop).

These technical findings will be further refined and analyzed towards a more business-oriented view of the associated risks and threats. Apart from the technical findings and risk view, the work also intends to result in recommendations and suggestions for security improvements.

> The methodology used for Host Hardening **consists of a practical technical security evaluation of the desktop environment.**

Physical intrusion

Security is only as strong as its weakest link. You can have the best team, the strongest perimeter, the most hardened servers, but if an attacker can just walk through the front door, take the server out of the rack, and walk outside, it was all for naught. Lots of companies have sensitive data stored in their offices, and not all staff are aware of proper security procedures. An ill fitted door can be as much of a security risk as an unpatched system.

We can either assume a consulting role, or an offensive role, to help you identify and possibly mitigate the possible existing risk. For example, a specific target such as a room to reach, an item to obtain, or it can be a more abstract goal, such as 'see what you can find'.

In an offensive role, we assume the role of threat actors. We stake out your companies' premises and look for weaknesses. We then produce a plan of attack and execute it. We'll rely on non-destructive techniques to try and reach our goal, unless given permission otherwise:

- lock-picking
- latch slipping
- hinge-pin extraction
- electronic lock bypassing
- abusing ill-fitted doors
- tailgating

In a consulting role we assess the physical security by inspecting it. You take us on a guided tour through the facilities, during which we look at the physical security equipment that's present.

At the end we'll provide a detailed report that includes a detailed explanation of the identified weaknesses. We'll also provide a set of recommendations to improve the physical security of the target. And of course, if we have taken anything during the assessment, we'll return that as well.

Application

Web Application/API/Web Service Penetration Testing

Web applications play a critical role in the current business landscape. These applications are frequent targets of cybercriminals looking for easy access to your client, employee and financial data. These losses of data result in reputational and financial damages. To assure that the cybercriminals have little to no chance of compromising your web application, a security assessment is needed. Web applications usually go together with various API and web services.

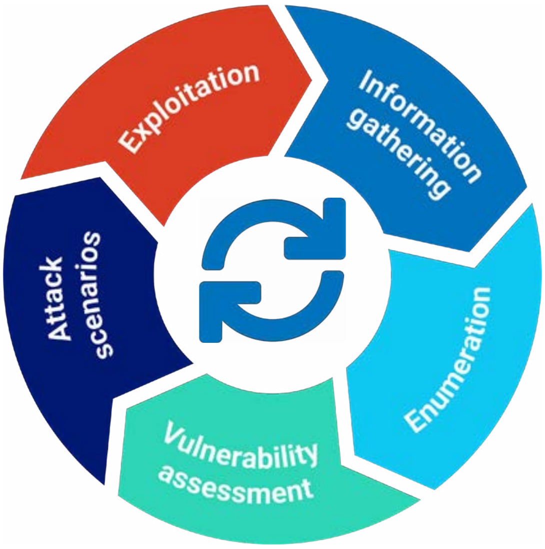
These services contain or handle sensitive data, and therefore need to be subjected to a security validation. Web services can be various technologies such as REST, RPC, WSDL.

This includes:

- information gathering/leakage
- configuration/deployment management
- identity management
- authentication testing
- authorization testing
- session management testing
- data/input validation testing
- error handling
- cryptography
- business logic testing
- client-side testing

A web application/API/web service penetration testing service is a technical assessment of a web application from a security point-of-view. The goal is to identify vulnerabilities in the assessed web-based software's application layer.

The testing methodology which has been adopted by us is aligned with OWASP's Testing Guide. All test categories are covered during a web application penetration testing service (apart from some of the denial-of-service related tests). We have highly reputable and certified testers (OSWE, GIAC GWAPT) and the team has proven track record in discovering highly sophisticated vulnerabilities in major business solutions.



To assure that the cybercriminals have **little to no chance of compromising your web application, a security assessment is needed.** Web applications testing usually goes together with various API and web services.

Mobile Application Penetration Testing Service

Mobile applications, followed by web applications, have the most adoption in our current interconnected world. Mobile applications are developed for various means and for multiple platforms. As they can't rely solely on the security of the device it's installed on, the applications themselves need be robust and secure.

The testing methodology used to perform mobile application penetration testing services are aligned with OWASP's Mobile Security Testing Guide (MSTG), together with the OWASP Mobile Application Security Checklist.

These tests include the following but are not limited to:

- Local Secure Data Storage testing
- Android/iOS Network API testing
- identity management
- authentication architecture testing
- authorization testing
- session management testing
- data/input validation testing
- tamper/reverse engineering testing
- Android/iOS cryptography API

> Mobile applications can't rely solely on the security of the device **they're installed on so the applications themselves need be robust and secure.**

Our detailed report will contain a list of technical findings, including the target, how it was discovered, its potential impact and how to mitigate it. The report also contains potential attack scenarios based on the developed threat model, combining several issues that may result in particular business impact.

Thick client penetration testing service

In contrast to Web Applications, Desktop applications are run locally, depicting a different risk profile when it comes to the overall security integrity of the application and its related data. From a security perspective, it should be considered that these applications are run on systems of which the overall security posture is unknown. Taking this into account, the affected application, which is subjected to a security assessment, should be able to protect itself from malicious activities regardless of the underlying system or other security controls.

A penetration testing service on a thick client is quite different from a more typical web or mobile application assessment, and will require a different approach. After gaining a deep understanding of the functionality and behavior of the application in scope, a specific methodology will be followed that has been created in-house based on extensive experience. The following layers will be reviewed, depending on the application itself:

- application architecture, functionality and behavior
- network communication
- encryption and hashing algorithms
- local system permissions
- application user roles and permissions
- client-side attacks
- server-side attacks

During a parallel and subsequent threat and risk analysis, these technical findings will be further refined and analyzed towards a more business-oriented view of the associated risks and threats. Apart from the technical findings and risk view, the work also intends to result in recommendations and suggestions for security improvement.

SAP

The interest of Threat Actors in attacking SAP applications is due to its wide deployment and the sensitive information that's stored on these systems. Gaining unauthorized access by these attackers could cause financial fraud or disrupt business operations, by for example, deploying ransomware. It's vital to perform regular penetration testing services to ensure a secure operation.

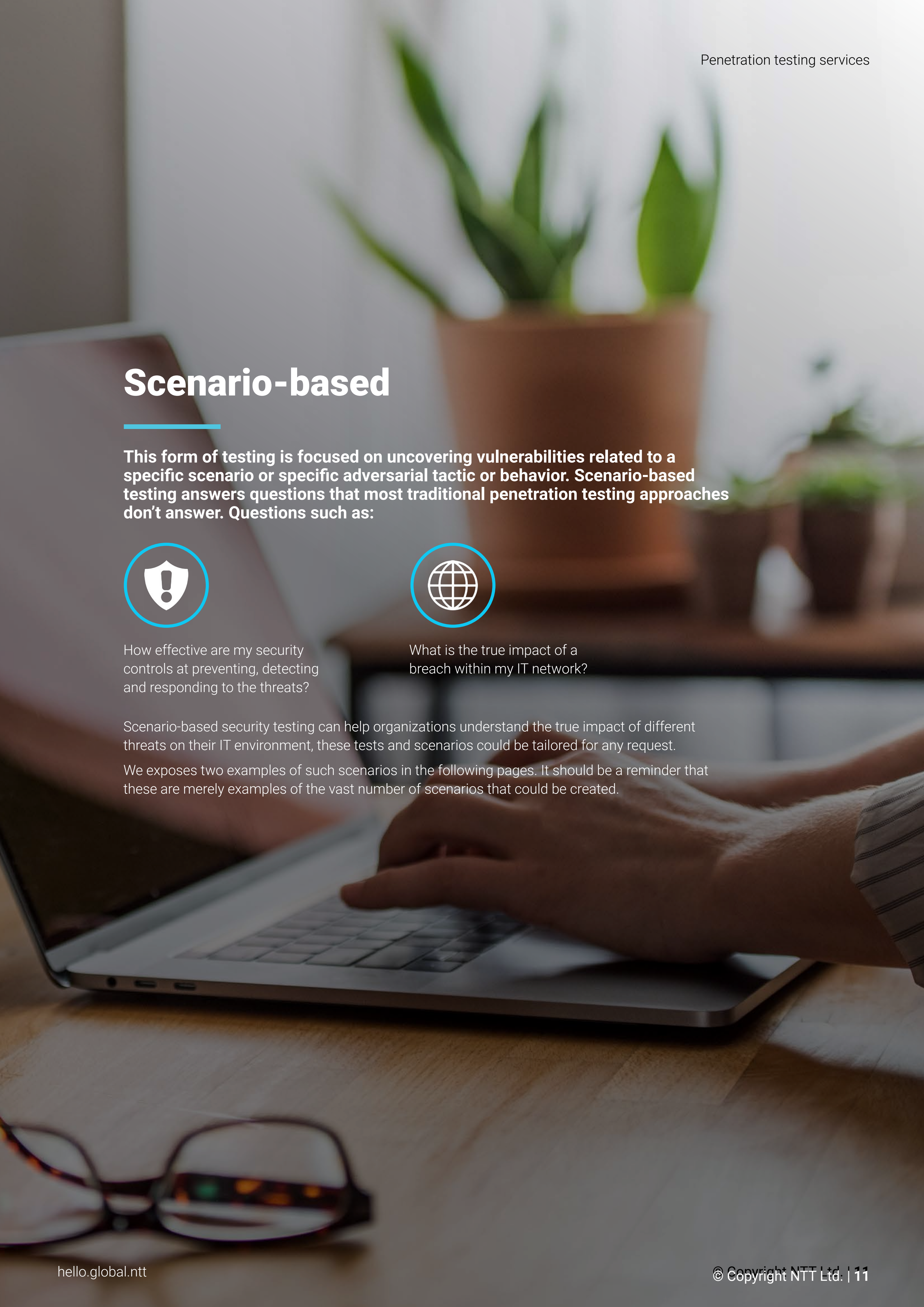
Based on previous experience, we noticed that developers assume SAP applications are secure out of the box due to several security features being implemented by the vendor. While this assumption is valid to a certain extent, theres still a wide array of vulnerabilities that could be present on these systems.

While an SAP security assessment could be considered as a web application penetration testing service, we deem it as much broader than this. Next to our distinctive testing methodology based on OWASP's Testing Guide, we ll emphasize specific SAP-related vulnerabilities and business logic flaws. This would allow us to mimic techniques that real attackers would use to gain access to the critical data stored on the SAP systems.

These SAP-specific vulnerabilities include, but are not limited to:

- missing security patches
- unencrypted communication, e.g., DIAG and RFC interfaces
- overly permissive authorization
- missing authentication
- unsecured high-privilege accounts

The output of this assessment will provide an evaluation of the security level of your implementation and details on how well your organization would endure attacks on its SAP applications. Additionally, it includes recommendations for improvements.



Scenario-based

This form of testing is focused on uncovering vulnerabilities related to a specific scenario or specific adversarial tactic or behavior. Scenario-based testing answers questions that most traditional penetration testing approaches don’t answer. Questions such as:

How effective are my security controls at preventing, detecting and responding to the threats?

What is the true impact of a breach within my IT network?

Scenario-based security testing can help organizations understand the true impact of different threats on their IT environment, these tests and scenarios could be tailored for any request.

We exposes two examples of such scenarios in the following pages. It should be a reminder that these are merely examples of the vast number of scenarios that could be created.

© Copyright NTT Ltd. | 11

Homeworking

Assessing your infrastructure, your people and your applications against security weaknesses and outsider threat vectors has become more important than ever.

Our ethical hackers can help you uncover security weaknesses by assessing the security awareness of your people by means of sending phishing emails in a controlled manner, assessing your internet-facing infrastructure for weaknesses that could allow malicious threat actors to compromise your entire IT infrastructure, and by assessing your corporate laptops that are being used by your people for potential weaknesses that could allow theft of corporate data.

This assessment contains the following components:

- **Phishing campaign:** three different phishing mails ranging in difficulty are sent to your people to have a benchmark on their security awareness.
- **External perimeter:** your organization s internet-facing perimeter is reviewed for vulnerabilities.
- **Laptop OS hardening:** the laptops given to your employees are tested for security weaknesses that could allow attackers to easily take over the machine.

By having these components assessed, you'll have a clear indication of your company s resilience against real external adversaries. By properly protecting these components, it'll make it much harder for threat actors to obtain an entry point into your organization. The assessment will uncover potential security risks and will assist you in mitigating these.

> Along the way, you'll be able to see where the **strengths and weaknesses are and which attacks you need to look out for.**

Compromised Laptop / Assume breach

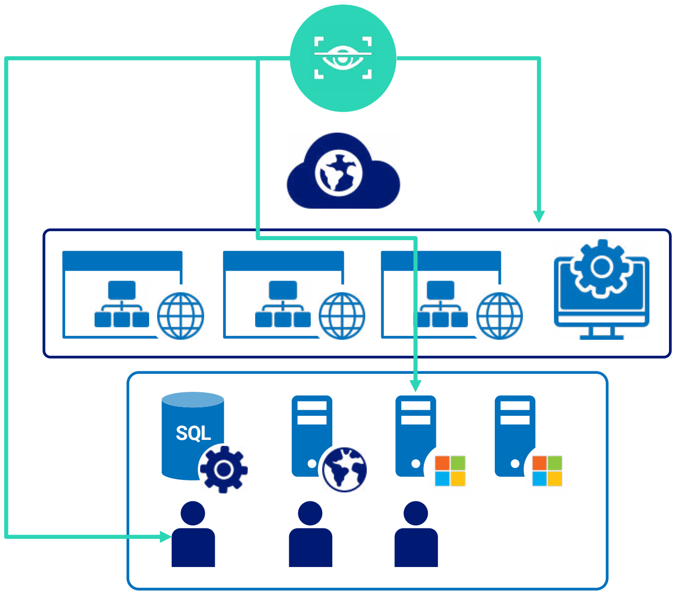
This scenario is one of the most cost-effective ways to test your organization s resilience against modern attackers. It'll assess the security maturity of your people, processes and technology.

Nowadays we can assume real adversaries have access to unlimited resources, i.e., time and money. While this approach is not feasible for most companies to simulate, we start from the assumption that an adversary will somehow gain access to your internal infrastructure, be it by breaching an exposed server on your external perimeter, a successful phishing attempt or finding working credentials somewhere on the internet. In this scenario, we typically start the assessment on a laptop with a user that has the same permissions and access rights as that of a typical employee. We basically simulate a standard user who wants to steal sensitive information from your company or a remote attacker that has successfully compromised a regular user s laptop.

The outcome of this scenario-based exercise will clearly demonstrate any attack paths that a typical attacker would use against you. Along the way, you'll be able to see where the strengths and weaknesses are and which attacks you need to look out for. This exercise usually uncovers structural issues that can be easily tackled by implementing new policies or new security measures. By repeating this exercise on a regular basis an organization can gradually improve their security posture and be more prepared in case of an active breach.

This type of engagement is at the border of a red team type of approach while keeping the engagement rather light compared to a real red team exercise.

Adversary Simulation



Red team

A Red Team engagement 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.

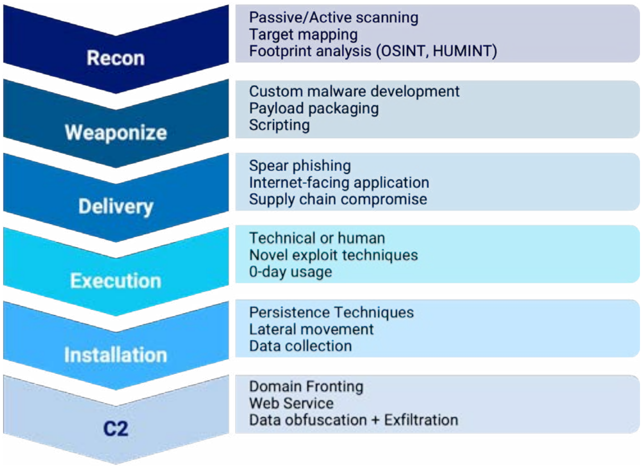
As adversarial capabilities have evolved over the years, so has the information security industry. Network defenders have realized that it's impossible to guarantee the security of every computer system within a large corporate network. Following this realization, there has been a shift in effort from preventing all unauthorized network entry to having the capability to detect and effectively respond to an ongoing attack. A Red Team assessment helps to verify that this capability is effective.

Other security assessment services, namely vulnerability assessments and penetration testing services (explained above), aim to identify and exploit computer system vulnerabilities so that they can be prioritized for remediation. Typically, such tests are conducted over a short period of time (days), on well-defined assets 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, a Red Team assessment focuses less on specific vulnerabilities, and more on an organization's ability to detect and respond to an ongoing attack. A Red Team assessment takes place over weeks to months with a specific agreed goal to achieve (e.g., modify a record in a core database). IT security staff are not informed in any way (except the stakeholders of the exercise (white-team)), and all the organization's defenses, policies and procedures are put into play. The attackers use a different, more refined methodology that would not apply during a shorter-term penetration testing service and which mirrors the actions a real advanced attacker attempting to gain access to the organization's critical assets and data.

Performing these engagements regularly creates a feedback loop that improves employee security awareness, validates and improves the implementation of security operations, hones 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, we'll provide a report that contains a milestone-based attack narrative mapped against the MITRE ATT&CK Framework and detailed explanation of the identified weaknesses. It'll include a set of recommendations to combat these weaknesses.



Recon	Passive/Active scanning Target mapping Footprint analysis (OSINT, HUMINT)
Weaponize	Custom malware development Payload packaging Scripting
Delivery	Spear phishing Internet-facing application Supply chain compromise
Execution	Technical or human Novel exploit techniques 0-day usage
Installation	Persistence Techniques Lateral movement Data collection
C2	Domain Fronting Web Service Data obfuscation + Exfiltration

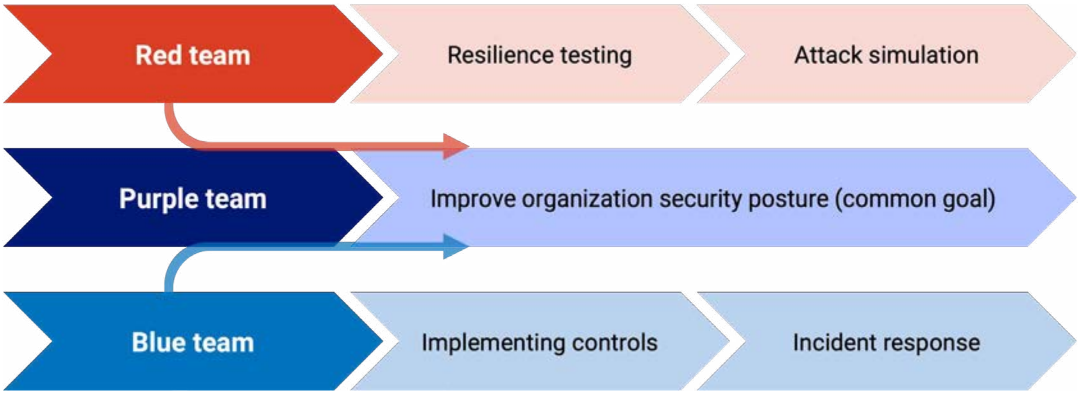
A Red Team engagement **simulates a real adversary attempting to gain access to an organization's most critical assets and data** using the **same tools, techniques and procedures** as a r**eal attacker.**

Purple team

The goal of purple team exercises is identical to red team engagements: assessing the detection and response capabilities of a company. The difference lies in the methodology of the assessment. During a purple team assessment, a close collaboration between NTT and the company's IT security staff (aka blue team) is set in place. While during a red team engagement the defenders are not informed about the Tactics, Techniques, and Procedures (TTPs) used by the attackers, during purple teams they are. By leveraging this approach, the blue team can continuously customize, adapt and improve its detection and response capability during the engagement.

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

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



The return of investment for an organization 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.

The goal of purple team exercises is identical to red team engagements: assessing the detection and response capabilities of a company. **The difference lies in the methodology of the assessment and the close collaboration between NTT and company's IT staff.**

Security Awareness

The attitude of employees towards an organization's assets is of vital importance and needs to be trained periodically to assure its effectiveness. A security aware mindset is one that understands there are actors at play that attempt to steal, damage or misuses companies' data and it's important to stop that from happening.

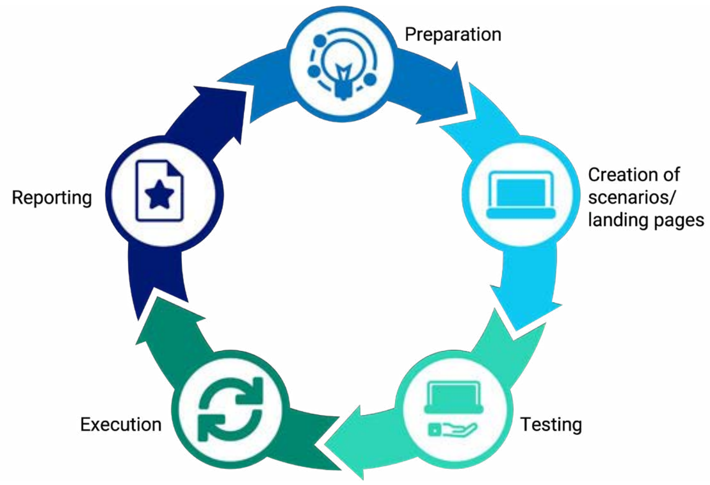
Security awareness is made to help users and employees understand the role they play in preventing/combatting security breaches. An effective security awareness journey is proven to be more cost effective than other solutions to prevent security breaches and should be integrated as part of your first defense layer.

(Spear) Phishing

Phishing is an attack in wich tries to gain information from an employee. Generally, an attacker will ask to one or multiple victims to give something to gain information (credentials), or to try to make the victim do something (e.g., load a page which runs code on the victim's computer).

With our phishing campaigns, we train and raise awareness for phishing in your company by emulating these types of attacks:

- A web-based attack is an e-mail which prompts the users to click a link and additionally asks them to submit their credentials to view something.
- A Malware-based attack is an e-mail which entices the users to download a file which contains code that will run on the target's machine.
- A Smishing (SMS Phishing) attack is where users are enticed to click a link from an SMS.



The phishing campaign follows a well-defined scenario for which the active participation of client stakeholders is recommended (a simulated phishing campaign can only be effective if it's credible and in-line with company culture and way of working).

The outcome of the phishing assessment is a well-documented report detailing what has been done, including statistics on end-user behavior, an overview of the most important technical findings, as well as the resulting attack scenarios and their potential (business) impact as perceived by our project team.

Secure code training for developers

Software and data exchange are at the core of the digital society we live in. The latest events in the world show that entire sections of our society can get paralyzed in a matter of seconds or even create human damage, by actively exploiting weaknesses in our information systems. It's therefore crucial to ensure that any developed software applications are completely secure by design.

Security by design during a software development lifecycle requires best practices and guidelines to mitigate the vulnerabilities and security risks associated. Therefore, we've developed a secure coding training program that focus on an approach to give to all developers the knowledge to understand the different types of vulnerabilities that can be exploited in insecure software (based on the OWASP Top 10) as well as advice on how to avoid them.

Our tailor-made training materials and training content, based on real-life examples and given by experienced ethical hackers, will help to improve the security awareness of your developers and the quality of delivered code by instilling a secure by design mindset.

The following topics are usually addressed during the training, but can be tailored upon request:

- Introduction to application security
- Threat Modelling
- Introduction to the OWASP project
- OWASP top 10 2017
  - A1: Injection
  - A2: Authentication
  - A3: Sensitive Data Exposure
  - A4: XML External Entities
  - A5: Broken Access Control
  - A6 Security Misconfiguration
  - A7: Cross-Site Scripting (XSS)
  - A9: Insecure Deserialization
  - A10: Insufficient Logging and Monitoring
- Insecure Direct Object Reference
- Cross-Site Request Forgery (CSRF)
- Server-Side request Forgery (SSRF)
- Docker security
- Library Security
- DevSecOps

The duration of the training is typically two days.

Security awareness program

Following security analysis, 90% of severe security breaches in 2020 were due to human mistakes. Securing a company requires the involvement of all parts of the organization and shouldn't only rely on software or IT measures. And, improving the security awareness of your employees is a key element of it.

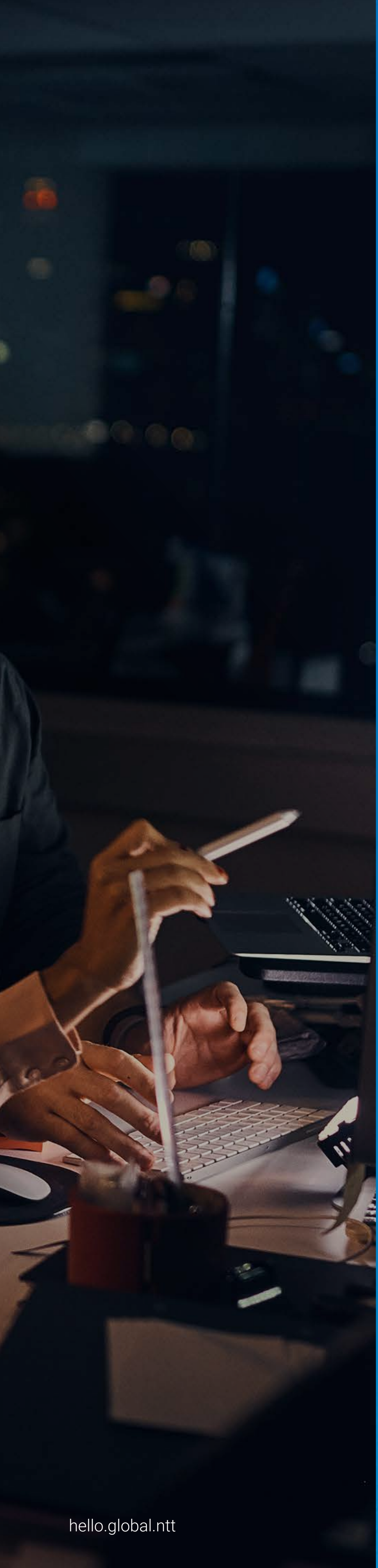
Our security awareness program, through a unique combination between Proofpoint Security Awareness Training, a SaaS (Software as a Service) solution, and consultancy delivered by us, will drive you all along your security awareness journey.

Proofpoint Security awareness training can deliver more than 150 modules and includes different styles (e.g., interactive, gamification and videos) and lengths (i.e., less than 5 minutes up to a full extended training, including tests of up to 30 min). It can be adapted to the specific needs of your company by including logos, adding links to existing policies and procedures, and containing personalized messages of your company s executive management. It can generate statistics and report about the evolution of your security awareness program like:

- anonymized data on the number of invites for training per department
- completion rate of training per week
- results of training tests, consolidated per department

A security awareness program can't be summarized by watching a few videos. It's about executing a well-coordinated program. It's about repetition to sharpen employees' attention and create a culture change towards information security. The closer the trainings can be positioned against real situations, the more users will be adaptive to it. Our consultants will help you tune your program, making it the most effective based on your need and your level of security maturity by capitalizing on our expertise and experience. This may go up to specialized in-person or virtual classroom dedicated to certain employee with specific needs.

Our security awareness program, through a unique combination between Proofpoint Security Awareness Training, a SaaS (Software as a Service) solution, and consultancy delivered by us, **will drive you all along your security awareness journey.**



Why us?

Our penetration testing services is only one element of our global security offering, which covers the full spectrum of the NIST Security framework . It means that the outcome of our penetration testing services is oriented towards delivering results that are useful and easy to integrate within your global cybersecurity strategy.

Our methodology is based on the understanding of your business requirements and associated risks when performing a security assessment. This helps us to better rate the likelihood and impact of vulnerabilities and weaknesses to reflect the actual risk to your business assets.

Our consultants spend about 25% of their time on research and development, which is reflected in their daily security assessment activities and results in our proprietary technical tools and methodologies. This also allow us to obtain regular CVE findings from major software and hardware vendors for which we're regularly recognized.

All our people are strongly vetted before joining our penetration testing services - including military grade screening. We only work with internal employees.

Our penetration testing services has an experienced team of consultants acting as ethical hackers, with more than 45 years of experience combined. Most of our team members own certifications like OSCP, OSWE, OSCE, OSWP, GWAPT, GXPN, CEH, CPSA, CISSP. Our team has a proven track record in discovering critical vulnerabilities in the most complex environments, including but not limited to financial, medical, industry, retail, public, and military sectors.

NTT

Together we do great things