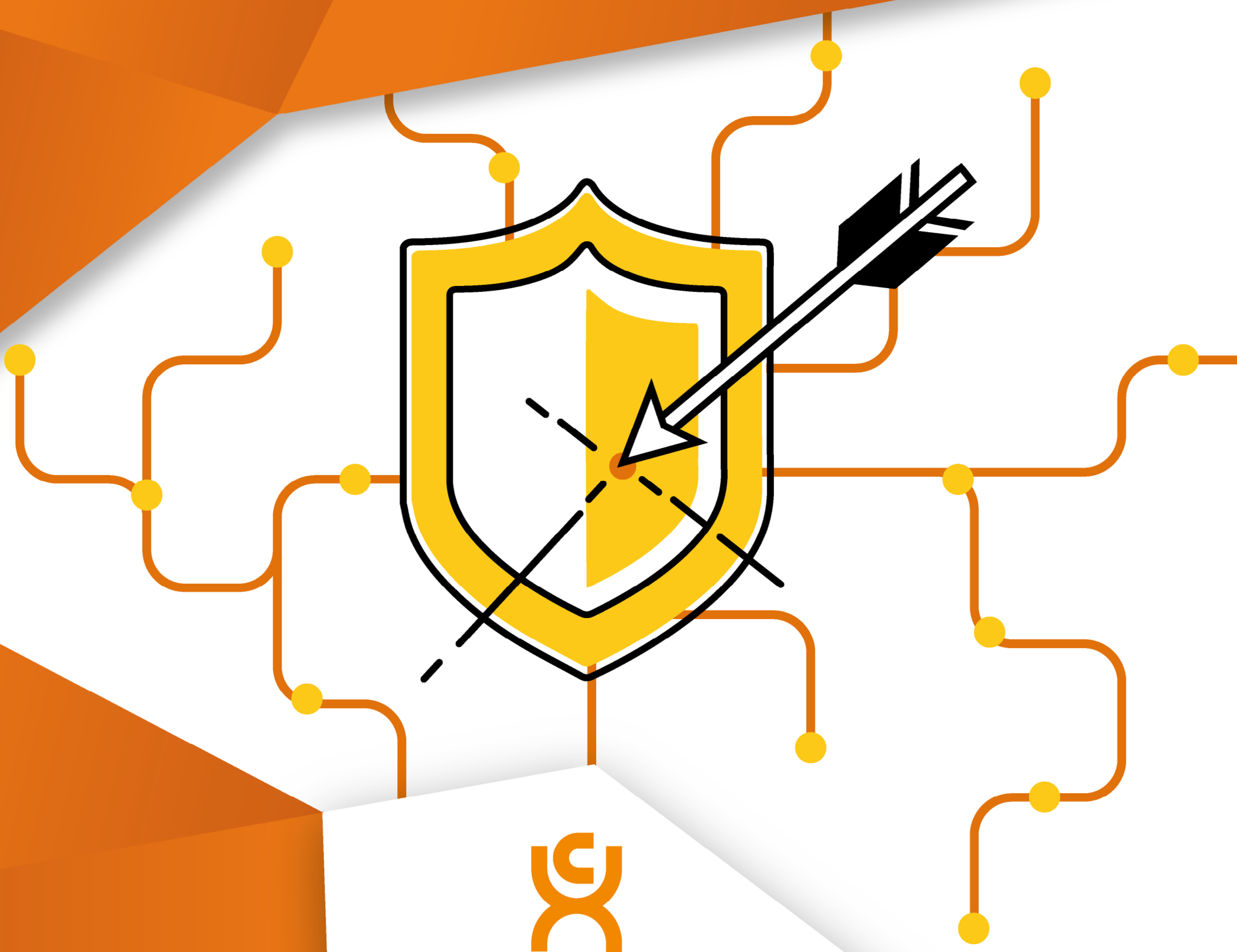
Buyers guide

Security tests



CYBERVEILIG NEDERLAND

Table of contents

Introduction

Cybersecurity measures are imperative to prevent, identify, reduce or restore damage as a result of a malfunction, outage or misuse of an information system or computer infrastructure. Many of these measures can be taken by organisations themselves. For some of them, they will want to turn to product suppliers or service providers for assistance.

Meanwhile, in the Netherlands and beyond, an array of this type of suppliers has become available, all of whom offer an extensive range of products and services. The challenge is to make a proper selection, which is quite difficult. The terminology used within the cybersecurity domain has a specialist nature that may seem comparable at first glance, but still appears to differ substantially in practice.

This document aims to be a tool for the domain of security testing. With this document, we offer more insight from the cybersecurity sector regarding the meaning of the different security tests and how they are interrelated.

Providing this information, we hope to enable you to send a more specific request to the market when in need of a security test. This document provides comprehensible definitions of the different services and shows the current possibilities in this area. This way, you will get a stronger perception of what suits you, whereas it will also enable you to better compare quotations. We consider this document a supplement to the previously published Cybersecurity Dictionary (see: https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/) of which the definitions were used as a starting point in this document.

We have written this buyers guide security testing primarily for executives responsible for security within an organisation, for those responsible for security, such as CISOs and for purchasers of security products and services. Obviously, this document will also be useful for other groups. The choice of topics however, emerged from the primary target group.

Before you start a security test

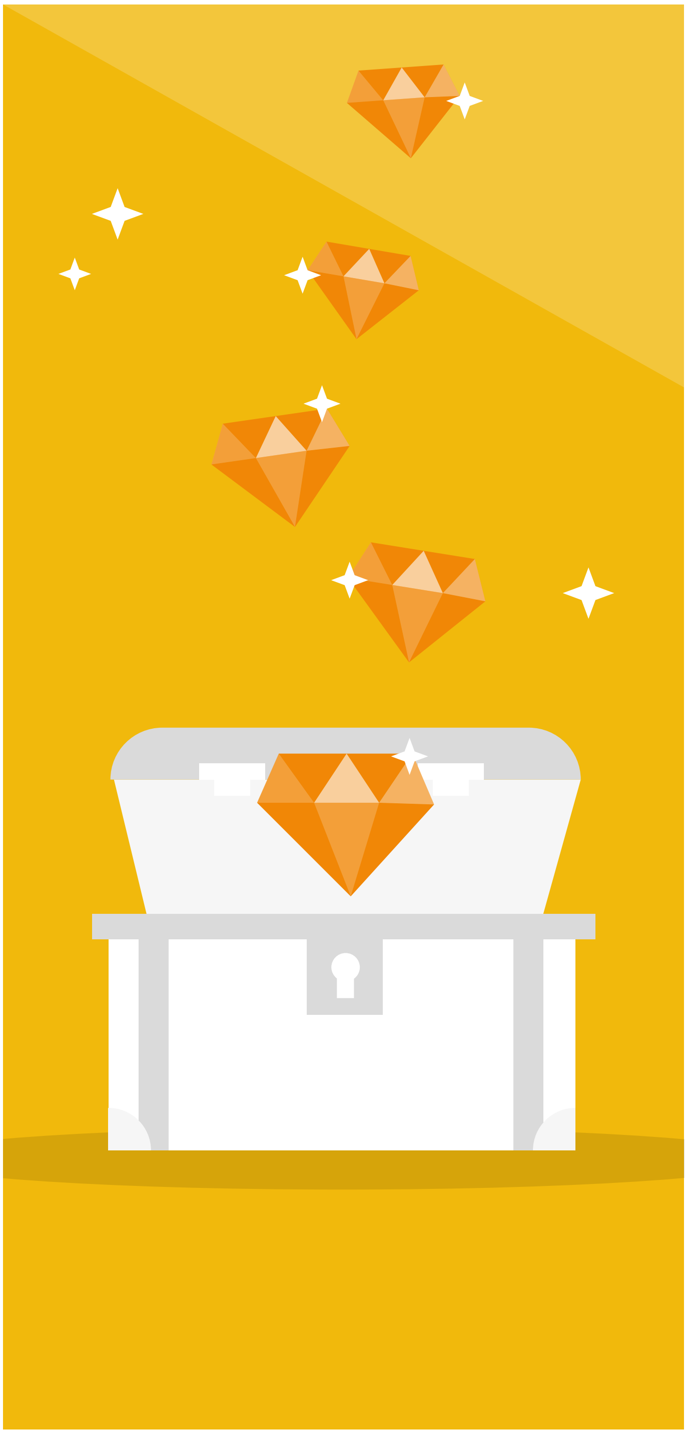
It is a good thing to realise that a security test in itself will not make an infrastructure, application or other asset any more secure.
It is primarily a means to provide you with insight in your vulnerabilities and, as a result, the actual risks for your organisation. On the basis of these insights, you can take measures to eliminate the identified vulnerabilities and – insofar required – to make educated choices regarding the future security policy of your organisation.

In order to ensure that the outcomes of a test provide proper insight, it will be useful to accurately formulate your needs in advance, before starting your search for a suitable service provider. This will prevent that a security test is implemented that does not (entirely) meet your needs, or provides an answer to the wrong security issue. Accurately formulating these needs may be difficult, if little knowledge or experience is available within the organisation, in the area of security (testing). By use of the following advice, we hope to be of assistance in this regard.

Sometimes, security tests are implemented as part of an audit. In the event of an audit, an organisation is being assessed against a previously established set of standards. The audit will assess whether the standard(s) is/are complied with. A security test is focused on finding any vulnerabilities and could be used for an audit, in order to assess whether certain security requirements were met.

Insight in crown jewels, the critical assets of your organisation

First and foremost, it is important that you have overview of your most critical digital assets, also known as crown jewels.
Which systems, processes and details are critical for your primary process? These deserve most attention in your security plan and, as such, also with regard to the choices you make with respect to security tests to be performed.



You do not always have unrestricted options when it comes to testing. Sometimes you need to comply with (mandatory) obligations. Stakeholders for instance, who demand that your organisation is able to provide insight in the vulnerabilities present and what has been done to remedy them. There may also be own (internal) obligations or watchdogs involved, expecting your organisation to implement security tests.

Regarding the different ways of testing, discussed later in this document, an important starting point is that a good overview is given of the digital assets present. For many medium-sized companies, but also for large companies, this is not always obviously available. In addition to the own local infrastructure, at present, many organisations make use of cloud services (software-as-a-service – SAAS, infrastructure-as-a-service – IAAS, platform-as-a-service – PAAS) and a hybrid IT-environment may be in place where complex links have been applied between systems. These interfaces often show vulnerabilities, that malicious persons make use of.

Therefore, a complete (or as complete as possible) inventory is an important precondition for an effective security test. Having part of your infrastructure not covered may cause blind spots and so-called shadow IT. These blinds spots in particular may provide opportunities for attackers. A test server, for instance, that is being forgotten, could be active in an infrastructure, outside the rules and contain vulnerabilities that could be misused. If those parts of an infrastructure are not sufficiently defined, they could be missed during a security test, leading to a false sense of security.

Threats, hazards and risks

The next step is to describe the threats and hazards that could affect these systems, processes or data. Threats are events that occur as a result of someone's negative intention, rendering systems to be useless, by means of an attack with ransomware, or digital burglary during which sensitive data is being captured. Hazards occur haphazardly, for instance as a consequence of a programming error or hardware breaking down, due to overheating. Although in case of security testing the focus is usually on intentional threats, it is also useful to pay attention to the accidental hazards. The tests described in this document primarily focus on threats.

In the context of the organisation, the threats and hazards must be regarded in terms of reality and it must be assessed what damage they could potentially lead to. These are known as risks. Based on the risk assessment, you can set the security level as desired and this will subsequently determine the scenarios to be tested. It is important, in the scenarios, to properly describe the possible damage that could be caused to the identified crown jewels. A security service provider can assist you in formulating the threats, risks and test scenarios.

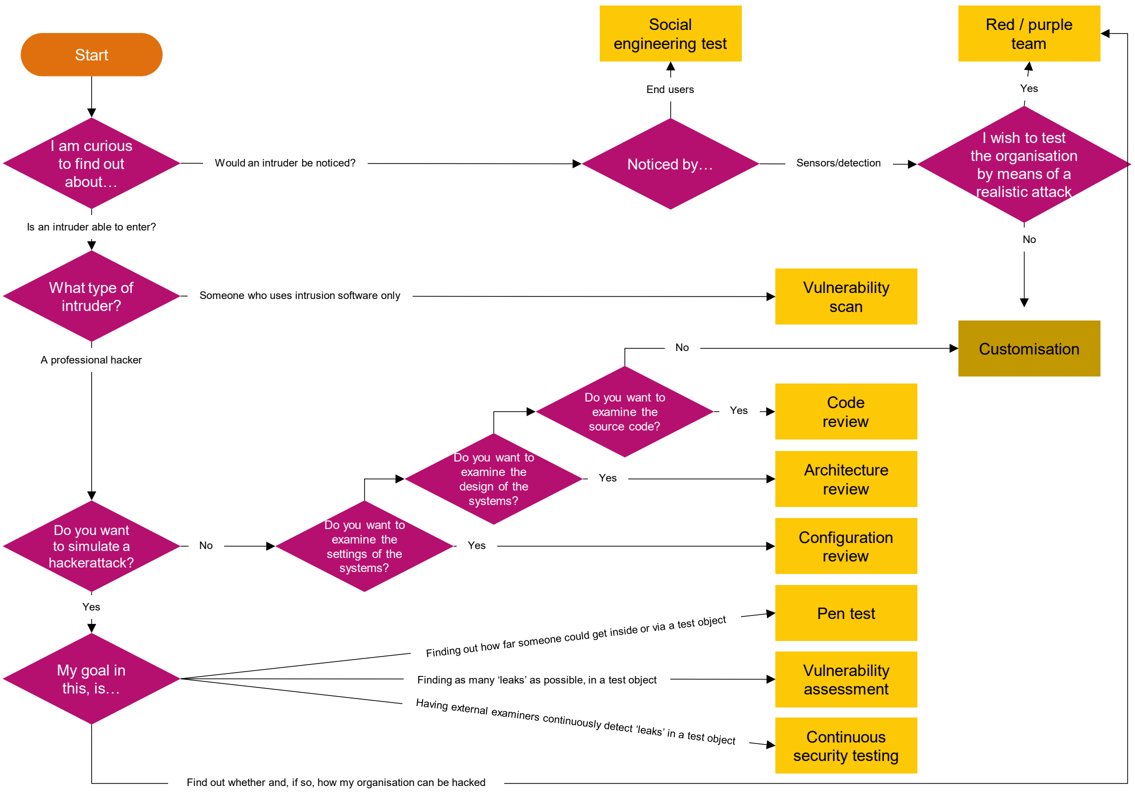
Security question

Security questions can be derived from all the information about crown jewels, threats, hazards and risks combined. For example: 'We want to know whether an attacker can access our financial system through the internet', or 'We want to know if our new commercial customer system will be able to safeguard the confidentiality of personal data', or 'We want to know whether the software code contains crucial errors that could lead to failure of the software'. These questions will decide the ultimate approach and the scope of the security test.

A security service provider can assist you in formulating your exact security questions and translate these into a suitable test approach and scope for the security test to be implemented.

Which security test do I use for which purpose?

There is an array of security tests available and every test serves a different purpose. Diagram below aims to provide insight in which types of security tests can be used for the various purposes, in order to detect the vulnerability level of an organisation regarding certain threats.


Start
I am curious to find out about…
Would an intruder be noticed?
Noticed by…
End users
Social engineering test
Sensors/detection
I wish to test the organisation by means of a realistic attack
Yes
Red / purple team
No
Customisation
Is an intruder able to enter?
What type of intruder?
Someone who uses intrusion software only
Vulnerability scan
A professional hacker
Do you want to simulate a hackerattack?
No
Do you want to examine the settings of the systems?
Yes
Configuration review
Do you want to examine the design of the systems?
Yes
Architecture review
Do you want to examine the source code?
Yes
Code review
No
Yes
My goal in this, is…
Finding out how far someone could get inside or via a test object
Pen test
Finding as many 'leaks' as possible, in a test object
Vulnerability assessment
Having external examiners continuously detect 'leaks' in a test object
Continuous security testing
Find out whether and, if so, how my organisation can be hacked

A glossary of security tests

The overview from the last paragraph shows that security tests can roughly be subdivided into 7 main groups:

1. Security review of a design or implementation
2. Vulnerabilities scan
3. Vulnerability assessment
4. Penetration test
5. Social engineering test
6. Red teaming
7. Continuous security tests

The paragraphs below provide an explanation of these tests.

Designimplementation security review

During this type of testing, it is analysed whether the design and the implementation of a given infrastructure or software is properly realised from a security perspective. For instance, the start-up phase of a new development project, in case the security design and functional design should go hand in hand. Another example is a security review as part of a due diligence trajectory in the event of a takeover.

In a design/implementation security review, different aspects can be considered:

1. Architecture review
2. Code review
3. Configuration review

Architecture review

BEGRIP

Architecture

BETEKENIS

The design and the structure of a computer system and network. The design controls the cohesion between business processes,applications, data and technology.

During this review, the design and structure of system to be investigated are regarded from a security perspective. This means that a passive ('paper') test will be performed on the design or architecture, on the basis of documentation and interviews. Thus, for instance, on the basis of best practices – e.g. guidelines for securing an internal network or application – it can be verified where the design may still be vulnerable. This type of review will also make it possible to do observations and make recommendations in terms of operational security technology, process-based/organisational improvement circles and human involvement. These could be, for instance, management processes for security that are not in order (applying timely updates, change management processes with limited attention to security etc).

The advantage of this type of review is that considerations and advice can take place from a broad perspective.
This will render added value to the design/initiation process in particular, or if there is need for a second opinion.
A disadvantage is that no actual technical assessment is being

performed on the possible vulnerabilities. So, in that respect it isn't an actual 'test'. The advisors concerned are in fact also strongly dependent on the information that they receive from

interviews and may, as such, miss out on details that are relevant to the analysis.

Code review

BEGRIP	BETEKENIS
Code review	Analysis of the source code of a program. The aim is to find weak spots. Searching is mostly done manually and not on the basis of an exhaustive list of vulnerabilities.

E Ensuring the most securely written code, as a basis for the safe functioning of a system or application, will offer adequate security guarantee. All the more, since many development partners are not being contracted primarily to take security of an asset, such as an application, to the highest level. Security may be the assignment's topic, but in practice it is not always as important as accessibility, speed and other business objectives. Also, in practice, parties hardly operate in conformity with the cycle for the development of safe software ('Secure Software Development Lifecycle').

During the review, the source code of the program will be analysed from a security perspective. It is assessed whether choices were made in the code that result in weak spots that could suffer from misuse. This is done on the basis of best practices and experience.

A review of the source code from a security perspective could help to identify and resolve known vulnerabilities, prior to the system going 'live'. A code review could also be an added value to a system that is operational already – e.g. based on new vulnerabilities identified. For instance by making use of new insights in errors and omissions, and taking account of the way malicious persons can actually take advantage of your application on the basis of the latest insights thereon.

Configuration review

BEGRIP	BETEKENIS
Configuration	The way in which hardware and software was configured for the desired goal.

During a configuration review, the configuration the hardware/software to be examined, will be inspected from a security perspective. On the basis of best practices and experience, a security tester will search for vulnerabilities in the configuration, that could form a security risk. It is also possible to have security requirements determined in advance, validated by the examiners during a configuration review.

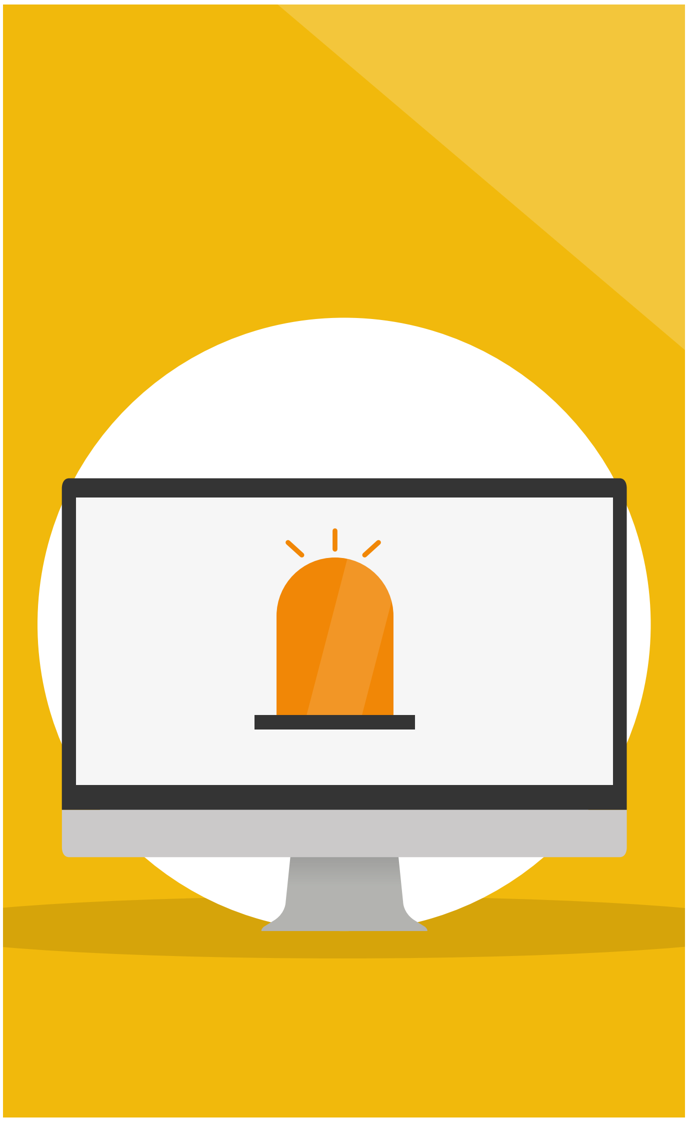
A firewall is a well-known object for a configuration review, but also other specific network components or equipment can be appropriate for a configuration review. Further enhancement of the security of components like printers and switches, is also known as ‘security hardening’ and forms an important method to prevent the risk of misuse of your systems in advance. In the event of hardening, the functions that are not being used in the systems, will be deactivated. As a result, they cannot be misused by third parties.

Vulnerabilities scan

BEGRIP	BETEKENIS
Vulnerabilities scan	An automated check that detects the weak spots in a system. Only in the event of a false alarm, they will be removed manually.

A vulnerabilities scan is an automated test during which security scanning software is being used to obtain an overview of possible vulnerabilities of an asset, for instance a web application. Any false reports (false positives) will usually be filtered from the test results. No extensive manual test will take place on the systems and applications being part of the scope of the test. Since some vulnerabilities can only be found by testing manually, a vulnerabilities scan usually provides a less profound result than a manual vulnerability assessment or penetration test. This type of test is excellently suitable though, to get a first impression of the vulnerabilities present in a digital environment.

Common tests focus, for instance, on the external infrastructure and are used to assess to what extent the organisation – examined from its 'exterior' from the internet – would possibly show vulnerabilities that could be misused to get unauthorised access to an organisation. However, there are also automated means that put specific emphasis on an internal IT-infrastructure or on specific applications inside them.



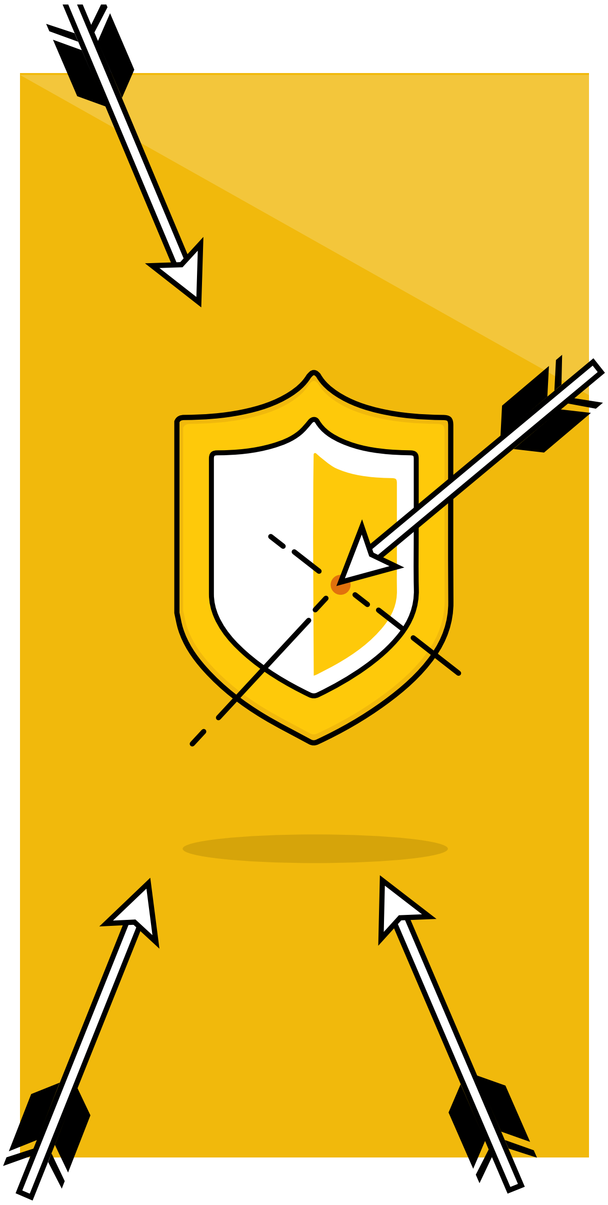
Vulnerability assessment

BEGRIP	BETEKENIS
Vulnerability	Manual check during which weak spots are tracked in a system. It is determined in advance how this will be done. During a vulnerability assessment, it is attempted to find all weak spots in a small area. This is what makes it different from a penetration test, during which it is attempted to get as deep into the system as possible.

DDuring a vulnerability assessment, the goal is to an as complete overview as possible of all vulnerabilities within a very specifically defined scope, such as a specific web application or IT-system. This concerns a manual test, where the vulnerabilities are looked for by the security investigators. In order to guarantee the completeness of the test, the investigators make the best possible use of checklists like the Certified Secure Web Application Security Checklist for web applications. In contrast to a vulnerabilities scan, the investigators test and validate the identified vulnerabilities manually. The outcome of such test is an as complete as possible overview of all vulnerabilities present in the application or infrastructure.

Penetration test

BEGRIP	BETEKENIS
Penetration test	Manual check during which the deepest possible penetration into a system is desired, in order to identify weak spots and to learn about their consequences. The weak spots are used to get even deeper into the system. Purpose of the test is not to find as many weak spots as possible. This is done during a vulnerabilities scan.



A A penetration test (abbreviated to pen test and sometimes intruder test or A&P test) aims to gain insight into how far a malicious person could get, if he breaks into the asset to be investigated, for instance, an IT-infrastructure, a WIFI network or an app(lication). The aim is to penetrate the environment as deeply as possible and at the same time, to inventory the most serious vulnerabilities, within the available time frame. The outcome of such a test is a report in which attack paths, vulnerabilities and action perspectives for the improvement of the security of the research object have been described. Sometimes the test is shaped around a number of concrete scenarios, for instance: ‘Can a malicious person read the email of the board members?’ or ‘Can a malicious person deactivate a certain system remotely?’

There are different variants of penetration tests:

Blackbox
Test without insider information of the object to be tested.

Greybox
A test during which the investigator has limited access to the object to be investigated, for instance via a user account with limited rights. This is a realistic scenario in case during an attack social engineering techniques (see next paragraph) were effectively made use of or during which a malicious user forms a threat to the object to be tested.

Whitebox
This concerns a test for which knowledge about design and architecture was shared beforehand.

Crystalbox
In this test, the source code was made available, as well as information about the configuration, in addition to knowledge about design and architecture. Sometimes this type of test is also called a white box test.

Timebox
This is a test that stops after a certain amount of time or budget has been consumed. Nevertheless, nearly all abovementioned tests are usually limited in terms of time and budget.

Sometimes these variants are also used in vulnerability assessments. An extensive description about penetration tests is available in the whitepaper security testing , which was published by the NCSC and was established with input from various market parties.

Social engineering test

BEGRIP	BETEKENIS
Social engineering	If an attacker misleads someone, for instance by responding to curiosity or helpfulness. This way, the attacker for instance attempts to obtain information to break into a digital system.

In this test, it is investigated to what extent an organsation is vulnerable to social engineering. An attack from this perspective is usually simulated by a so-called mystery guest or phishing simulation. In this case, the employees are being seduced (meaning: manipulated) to operate contradictory to security guidelines.

This could, for instance, lead to getting access to a building, login details, a system and/or specific data. It is also conceivable that physical access will lead to getting digital access. So called 'rogue devices' could for instance be left behind, ensuring remote digital access. Access to a digital system can also be obtained in other ways, such as via unprotected ports, limitedly protected Wi-Fi or via devices.

This type of testing is usually deployed with the aim to realise more awareness and to strengthen the (physical) security (of locations). These tests can also be part of a realistic attack simulation, also known as 'red teaming' (see next paragraph).

Red teaming

BEGRIP	BETEKENIS
Red teaming / adversary simulation	Exercise during which an organisation simulates attacks in order to discover how well they are protected against attacks. The red team stages attacks and attack methods of a selected opponent. The blue team tries to trace the red team's attacks and subsequently to fight them. If they should encounter a real attack, they will also address that. Sometimes there is also a white team. This team ensures that the exercise reaches its goal. For instance by determining which information will be issued to both teams. The collaboration between the red team and the blue team is also known as purple teaming. In case of a red team exercise, the emphasis is on collaboration between the teams, and on the simulation of opponents and attacks. In a penetration test it is attempted to penetrate a system as deeply as possible.

In order to be able to get maximum value from red teaming, it is important that the organisation has already taken different measures in the area of cybersecurity. A red team security test is a means to check whether these measures are indeed effective in practical situations. Just as malicious persons would do in practice, the 'red team', with its attacking security specialists, makes use of a combination of technical attacks, social engineering and weaknesses in business processes. The result is a clear picture of the resilience of the organisation against a realistic attack and it's also a good impression of how the organisation responds to it. The latter in particular is an essential aspect of a red team test: since an organisation also mainly wishes to know how quickly and adequately the defending team - blue team – will respond to attack actions.

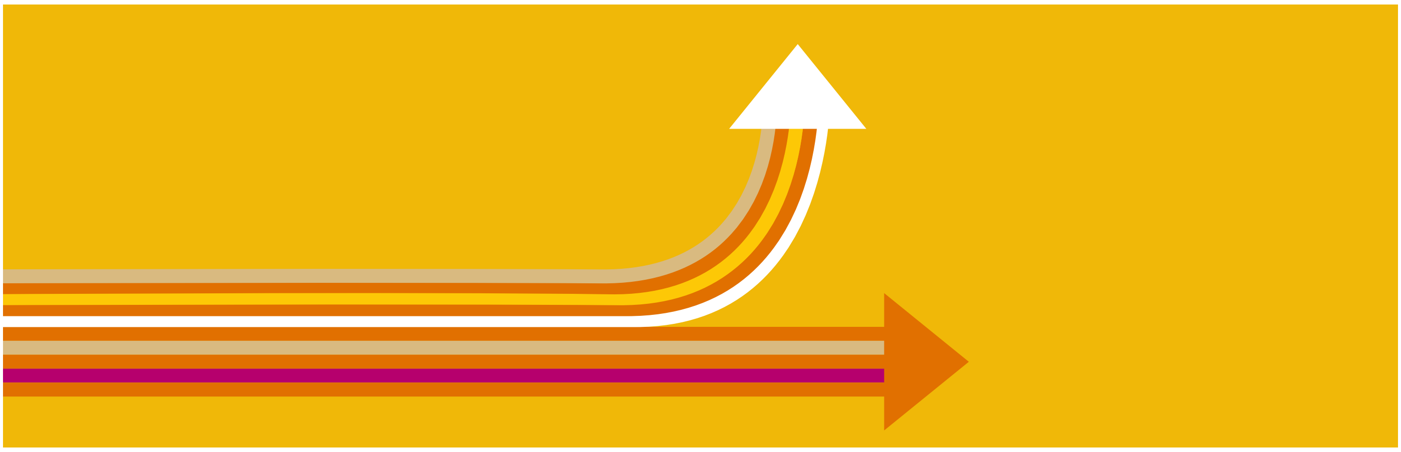
An extensive evaluation of the actions performed by the red team and the blue team is also known as a purple teaming session. Purple teaming can also take place real time.

Sometimes, the extensive collecting of threats information (threat intelligence) and the set-up of attacking scenarios, based on these details, is a separate part of a red team test. This is known as a Threat Intell Based Ethical Red team or TIBER test.

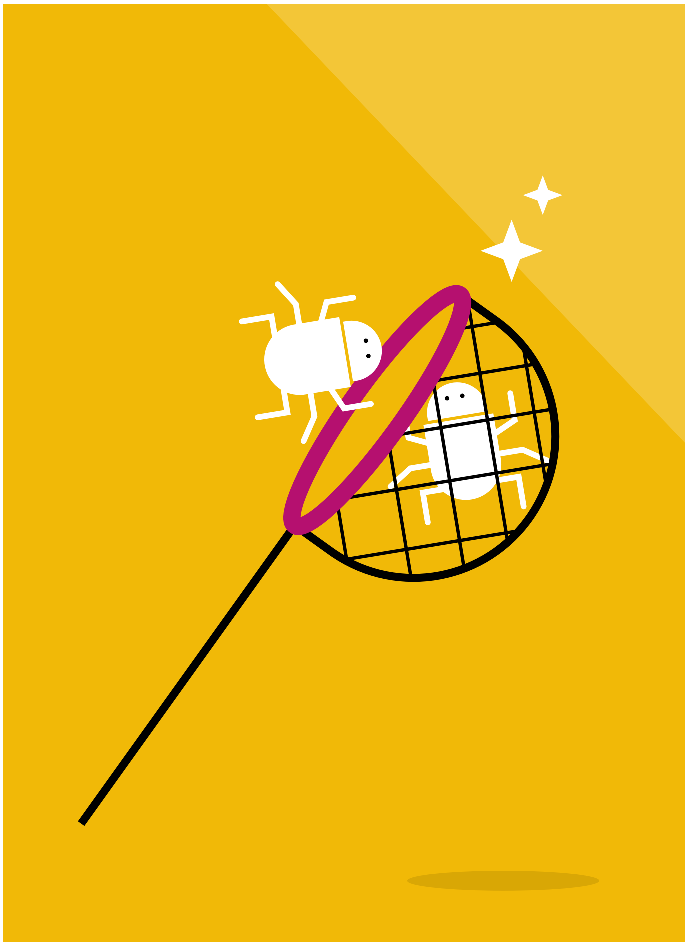
[1] https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten

Continuous security testing

Another approach of security tests is to security investigators to autonomously look for vulnerabilities in an infrastructure. Two possible ways to do this are via a bug bounty program or via coordinated vulnerability disclosure.



Bug bounty programma



BEGRIP	BETEKENIS
Bug bounty	Reward given to someone after he/she has identified and reported a security breach in a digital system. The reward is issued by the owner of the digital system.

In a bug bounty program, security investigators are actively invited to track vulnerabilities in certain systems. The owner of the system will make a certain reward available in advance. The height of the reward generally relates to factors like the seriousness of the vulnerability identified by the investigator and the degree in which this is accurately reported to the organisation.

Coordinated vulnerability disclosure (CVD)

BEGRIP	BETEKENIS
Coordinated vulnerability disclosure	Standard process used by security investigators to report weak spots in computer systems and products. They can only do this when observing the rules of play of the organisation for this type of reports. The National Cyber Security Centre (NCSC) has a manual that sets out what the rules of play should comply with. This method is the successor of the Responsible Disclosure. The main difference with the past is that the investigator is no longer solely responsible for the consequences of a security breach.

T There is a substantial community of hackers, involved with finding and reporting vulnerabilities. This community can be actively stimulated to look for vulnerabilities in your systems, when you report on your website that you are open to this. It is important, in that instance, that you are well able to receive this information. A manual about the best ways to approach this can be downloaded from the website of Cyberveilig (Cyber-safe) Nederland.

Colofon

This is a publication of Cyberveilig Nederland. It has been developed with great care. However, it might occur that the publication contains unfortunate mistakes. Cyberveilig Nederland accepts no liability for the accuracy or the completeness of the information in this publication.
Under no circumstances Cyberveilig Nederland will be held responsible or liable in any way for any claims, damages, losses, expenses, costs or liabilities whatsoever resulting or arising directly or indirectly from the use of information in this publication.

In this document definitions are used for terms that have been defined in the Cybersecurity Woordenboek, second edition (ISBN 9789083026411).

First edition: 1 July 2021.

More information about the activities of Cyberveilig Nederland can be found at cyberveilignederland.nl

Contact details
E-mail: info@cyberveilignederland.nl
Telephone: +31 88 - 118 25 10

Cover and design by Coolermedia

CYBERVEILIG
NEDERLAND