Vulnerability Assessment & Penetration Testing

One of Secura's most valued service lines, and the service line with the longest history within Secura, is Vulnerability Assessment and Penetration Testing (commonly known as VA/PT). Secura started testing for customers in the year 2000 and has been a renowned party in security assessments ever since. Our services span all domains, from IT and OT to IoT, and encompass a huge variety of types of tests. To help you understand our vision and our services, we will explain below what we do, and then highlight our value by presenting several customer cases.

Secura has worked in information security and privacy for more than two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. We offer a range of security testing services varying in depth and scope.

Vulnerability Assessment & Penetration Testing

There are many types of testing that are collectively known as 'Vulnerability Assessments and Penetration Testing' (VA/PT). Classical '**Penetration Testing**' means that tests are performed from the perspective of an attacker, and vulnerabilities are exploited to see 'how far can an attacker get'. However this is not always the most effective way of testing because it often makes more sense to perform a **Vulnerability Assessment**: test in such a way that as many vulnerabilities as possible are found without wasting time trying to exploit them to see how far you can get. Finding more vulnerabilities is often more valuable because it allows to reduce risks more effectively: exploring wide, instead of (only) deep.

How to Scope Your Vulnerability Assessment / Penetration Test?

Targets & Technologies

- Network & IT infra
- Applications
- Cloud
- OS & Appliances
- Wireless Technologies
- IoT

Types of Testing

- Black Box
- Grey Box
- Crystal Box

Frequency

- Manual (once)
- Manual (annual)
- Manual + Periodic Delta Testing (in case of continuous testing)

Application of Standards

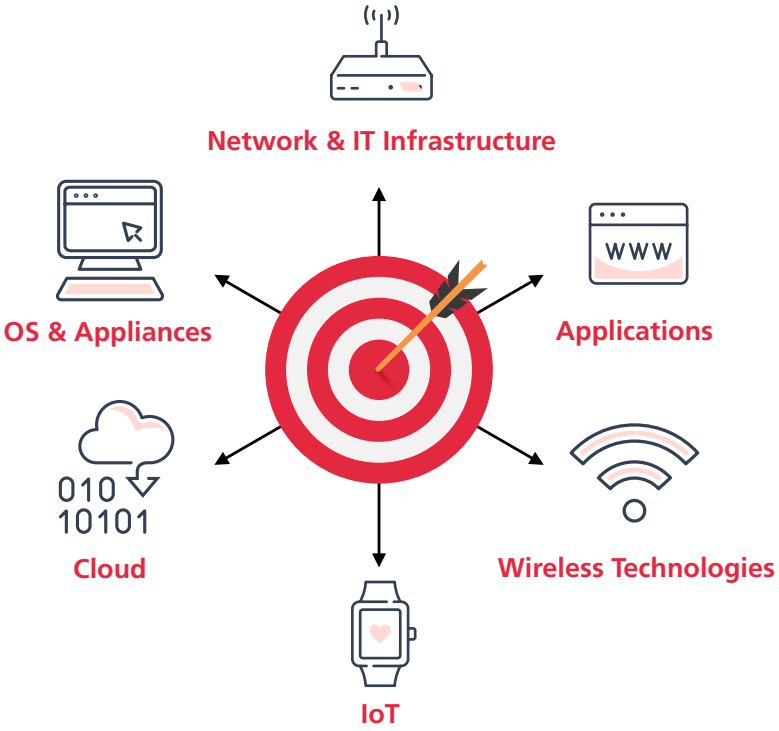
- None (i.e. effort based testing)
- OWASP ASVS
- CIS

Targets and Technologies

Over the decades, our customers have asked us to perform security tests on virtually every thinkable target. Some types of systems require extremely specific knowledge of the target, while others can be handled in much more generic ways. Therefore, while we definitely can perform, for instance, a penetration test on a bespoke application in a High-Performance Computing (HPC) environment, usually our customers ask to test their systems in environments that are more common. To give you an idea of the targets we test frequently, a selection is provided here:

Network & IT Infrastructure

External, internet visible IT systems are attacked daily. It is therefore often required to test these systems periodically or when significant changes are applied. Usually, vulnerability scans are the basis for such assessments, while manual verification of all findings and risk ratings are performed. However, it is equally possible to perform such assessments on internal networks, and also on very specific parts of the infrastructure (such as the e-mail infrastructure or VPN infrastructure).



Applications

Probably the most often tested targets are applications. This is obvious because applications must protect the data they process. Web applications are often exposed to the world and not always protected very well. Therefore Secura assesses the security of all varieties of applications, be it web-applications, APIs, Mobile applications or standalone (fat client) applications. Secura mostly uses renowned testing standards and methodologies for this, such as the OWASP ASVS standard. See below for more details on the applicability of such standards.

Wireless Technologies

WiFi, Bluetooth, 2G/3G/4G and other wireless technologies (such as Zigbee or WirelessHart in the industrial domain) remain a weak point in many infrastructures. Some can be easily disrupted or taken over, even at distance. Therefore, Secura has developed specific testing protocols for such technologies. Often combined with physical access testing or site surveys, knowing the susceptibility of your wireless infrastructure to attacks is an important aspect of becoming more resilient.

IoT

IoT devices are a growing target of our test and assessment services. Hardware, firmware and (cloud-dwelling) backends are all targets for attackers and often not very well understood. Secura can test all these aspects, and also apply reverse engineering and firmware hacking techniques to find out which weaknesses exist. Interesting to note in this context is that Secura is also active partner in the **INTERSECT** research consortium that includes all Dutch Technical Universities and many multinationals, and is focused on developing new technologies for testing and securing (Industrial) IoT devices.

OS & Appliances

The configuration of Operating Systems (OS) such as Windows, Linux, Unix and others, are at the core of the security posture of all IT environments. Securely deploying servers, endpoints and appliances using baselines and secure builds is a key component of managing risks in complex environments. This is why Secura assesses such configurations, often using baselines such as the CIS baselines as a model. But we don't stop there. Assessing security also has a lot to do with trust relations, rules auditing (firewall rules for instance) and reviewing access rights and authorisations. Specific services (such as webservers, middleware and databases) can also be assessed for secure settings.

Cloud

Cloud computing is so pervasive these days that we often don't even realise we use it anymore. However, due to the shared responsibility of the cloud customer and the cloud service provider, there are new risks that need to be assessed that deal with how the cloud provider and the customer have configured the services. Secura offers detailed assessments on the Cloud Service Provider configuration (Azure/AWS/Google and others) that allow the Cloud service customers to deploy in the cloud with the confidence that all security configurations are set correctly. Also, when using container technologies such as Kubernetes and Docker, Secura can provide assessment services. The actual deployment model (SaaS, IaaS, PaaS or FaaS) does not really matter, we have experience and knowledge in all models.

Types of Testing

The efficiency and outcome of testing is heavily influenced by the information available to testers upfront. We generally make a distinction between black, grey and crystal (also known as white) box testing.

A **black box** test is generally associated with a test where we do not know anything beforehand except the target addresses. Black box testing provides you with an answer to the question: "What could an average attacker with limited time and resources do?". Black box testing typically uncovers 'low hanging fruit', but lacks the depth necessary for an answer to questions such as "how well protected is my data really?". In black box testing, a vulnerability assessment is carried out, identifying entry points for an attacker. Further penetration of the deeper layers is then performed by exploiting concrete vulnerabilities. Since no credentials (usernames and passwords) are available to us, most business logic issues and authorisation model failures, will not be identified. However, you will have an excellent view of all attack surfaces an attacker could abuse, using black box testing.

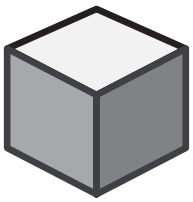
In a **grey box** test we have credentials to log in, often for various roles (e.g.: user, supervisor, administrator). This is hugely important if the application or device in question contains any sensitive data, such as medical, financial or other data that should only be available to certain users or roles. "Can a user access the data of another user?", is a question we can only answer adequately with a grey box test. This type of test is the most common for our clients. Black box testing is usually also a part of grey box testing, so that you will be able to differentiate between vulnerabilities that are available to external attackers, and vulnerabilities that can be exploited by authenticated users only.

Finally, in a **crystal box** test, we have the source code (or full configuration information of infrastructure components) while performing grey box testing. While we normally will not perform a full source code review during a vulnerability or penetration test, we do use the source code to identify vulnerabilities in security functions. Especially vulnerabilities in input validation, cryptographic handling and authorisation models can be found much more efficiently this way. Having access to the source code or detailed configuration information during a test allows us to answer the question: "How well protected is my data really?".

Keep in mind though, that the distinction between black, grey and crystal box testing is not a strict one, mixing forms is possible. For instance, a common combination when testing web application security is to perform black box testing on the infrastructure, and grey box testing on the application itself. Another common black box penetration test is a penetration test of the internal network (plug in and see how far you can get). In such an internal penetration test we have no information upfront and we try to get access to all the data via exploiting vulnerabilities (usually by gaining domain administrator rights during that process).

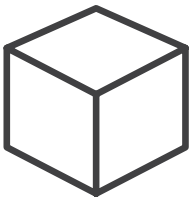
Black Box Testing

No information available, except target addresses



Grey Box Testing

Some information available, such as credentials to log in

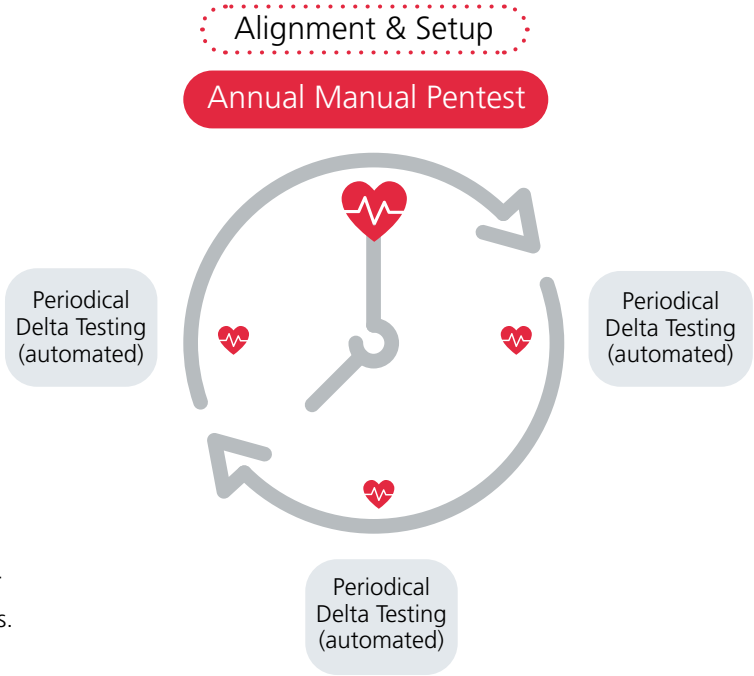


Crystal Box Testing

Full information available, including source code

Frequency of Testing

Our customers often ask us what the best frequency of testing is. Many settle for yearly assessments, or when major changes are made to applications or infrastructures. However, it is becoming more and more common to perform very frequent small incremental updates to applications (when using Agile, DevOps and CD/CI software development models). This makes it necessary to adapt the testing frequency also, and is the reason that Secura also offers a Continuous Scanning service where applications are tested first manually, then automatically every month, week or biweekly. Given the frequency, test reports for the automated test will be delta-reports, only providing differences with the previous reports.



Application of Standards

It is Secura's vision that security will more and more be supported by security metrics, and be made more measurable, reproducible and comparable through the adoption of (technical) standards and baselines.

OWASP ASVS

Secura performs application testing according to the OWASP Application Security Verification Standard (ASVS) for web, API and mobile applications. We not only test according to those standards but also report our findings using this structure. Besides testing and reporting according to ASVS, Secura also offers **Assurance services** according to the three levels of the OWASP ASVS standard:

Level 1: First steps, automated, or whole of portfolio view

An application achieves ASVS Level 1 if it adequately defends against application security vulnerabilities that are easy to discover, and included in the OWASP Top 10 and other similar checklists.

Level 2: Most applications

An application achieves ASVS Level 2 (or Standard) if it adequately defends against most of the risks associated with software today.

Level 3: High value, high assurance, or high safety

ASVS Level 3 is the highest level of verification within the ASVS. This level is typically reserved for applications that require significant levels of security verification, such as those that may be found within areas of military, health and safety, critical infrastructure, etc.

In a standard security assessment, Secura focuses on testing an application for all known vulnerabilities, including context and business specific tests. Clients who want to obtain assurance on the security of their applications according to the ASVS standard, may choose the ASVS Assurance service from us. This guarantees that we have checked all controls as relevant for the corresponding levels and provides a report that can be used by an auditor to show compliance to the standard.

Other Standards

Similarly, we perform configuration and hardening reviews, and apply the CIS baselines to them to provide insight into compliance to them.

Our VA/PT testing services are often also used to support audits and compliance schemes such as DigiD (for the Dutch national authentication scheme), Common Criteria and BSPA, for which Secura is an accredited test lab.

Results

All our Vulnerability Assessment and Penetration Testing services result in a written report in English, with Dutch as an optional alternative language. This report contains an introduction, a management summary describing all the important risks we identified, and a technical section describing the steps we took to identify the risks. This means that in contrast to many other providers, your developers and engineers will be able to repeat our actions using the information in the report, and validate for themselves what we found. As we have dedicated teams running these security assessments all the time, you also have assurance that all major risks are known to you and can be mitigated. In our report we tell you what to fix, and with what priority. We score vulnerabilities according to the **CVSS3.1 standard** and also can provide findings in other formats such as JSON (for integration with issue trackers) and as Excel sheet. Our recommendations are actionable and risk scored: you will know exactly what to do first.

The Team

Secura's pentesting team is made up of several dozen specialists, with varying experience levels (juniors, mediors and seniors) and specialisations. All testers are certified to a minimum standard (eWPT) while most have multiple certifications such as OSCP, OSCE, eCPPT, GIAC GPEN, SANS and many others. We actively encourage development of our specialists, and provide them with the opportunity to develop themselves and perform security research.

Tooling

Tools, including vulnerability scanners, are an important part of the services we provide, but we do not rely on them for everything. In fact, most of the work we do is manual testing, supported by tools such as Tenable Nessus Pro, Burp Suite, Sonarqube, AppScan and many others. We use (and develop) our own scripts for many purposes and maintain a large collection of smaller tools in our repository.

Specific tasks sometimes have specific tools, and this is why we also use tools such as IDApro for binary analysis, Cloud scanners for checking cloud configurations and CIS baseline scripts to check for compliance against the CIS baselines.

And when it comes to hardware and wireless technologies, our lab is equipped with Software Defined Radios (SDR), (de) soldering stations, logic analysers, and a slew of interfaces for testing hardware such as Bus Pirates, Facedancers, JTAGulators and many others.

We like to keep our lab and tools up to date, and are always looking for new and exciting ways to make testing better and more efficient.

Test Process

Secura follows a phased approach to all security assessments. First, the preparation of the assessment takes place, then information about the target systems, components or applications is collected, then the assessment is carried out and finally the report is written.

Phase 1: Preparation and Information Gathering

Good preparation is essential and ensures a time-efficient execution of the assignment.
The activities in this phase are:

- Determining a complete overview of the target systems in scope (e.g. IP addresses and URLs).
- Drafting and verifying indemnity statements (especially if third parties are involved).
- Designating and establishing technical and operational contact persons.
- Defining scan frequency and timing (in consultation with the client).
- Validate that login details required for the assessment have been delivered (if applicable).

By collecting as much information as possible (e.g. by using data from publicly available sources) we get a complete picture of the systems in the scope. The information that can be collected includes:

- Systems within the scope.
- TCP- and UDP ports with active services.
- Known vulnerabilities in underlying services.
- Application or frameworks used.
- (Sub-)domains.
- Functionality (authenticated) of user roles (if relevant).
- Accessible web services and/or APIs.
- (possible) External links.
- Any other relevant scope details: physical, people, process etc.

Phase 2: Test and Analysis

In this phase, Secura assesses which vulnerabilities can be identified by conducting an investigation by a team of experienced security specialists. The strength of the assessment is the way in which we use our technical knowledge and logic to find vulnerabilities. In order to work as efficiently as possible, we also use tools and scripts developed partly by Secura itself. The research results in raw data and potential vulnerabilities that are then manually checked for 'false positives '.

Phase 3: Report and Explanation

This phase consists of writing and reviewing the report If you wish, we will be happy to discuss the report with you and review the findings together.

Phase 4: Optional Retest or Periodic Follow-up Scans and Delta Reports

Retests or periodic vulnerability scans are a necessary complement for organisations working with ever-expanding IT infrastructures and ongoing application development processes with very regular updates. In these situations it is almost impossible (and also very cost-inefficient) to always have a (thorough) manual security assessment performed. That is why Secura can perform automated vulnerability scans periodically after a manual penetration test (either applicative or infrastructural, or both), whereby the frequency and timing are tailored to the customer's development methodology. This gives you the best of the unique expertise of a Secura security expert and frequent scanning to optimally mitigate security risks.

Whatever the type of test, we will always coordinate with our customers to determine if the services can be delivered remotely over internet, or onsite, or a combination of both.

VA/PT Services

We hope this overview has provided some background to our VA/PT service offering. And while the possibilities are endless, there are of course several VA/PT services that are more popular than others.

In a **Black-Box Infrastructure** (BBI) assessment or Black-Box Application (BBA) assessment, Secura tests the externally visible infrastructure or application from an attacker's perspective without information or login credentials upfront. What could an attacker do, given just a range of IP addresses or URLs.

In a **Crystal-Box Infrastructure** (CBI) assessment, Secura is provided with access to, and configuration details of, infrastructure components such as Windows Servers, firewalls, databases, routers, Unix/Linux servers or any other appliance or middleware. Together with the customer's engineers, we then review the security settings of the targets, and compare them to best practices or vendor recommendations.

In a **Grey-Box Application** (GBA) assessment, we test from an authenticated perspective, which vulnerabilities can be found in the application, including relevant APIs. Because many applications support multiple user roles, an important part of such tests is assessing the separation of these roles: can a user see data and functions from another user with the same or a different role.

A **Crystal-Box Application** (CBA) assessment takes the GBA some steps further, by having the source code and design information of the application available to the testers. This makes testing a lot more effective and makes it possible to find vulnerabilities that would otherwise be very hard to identify. For high-risk applications, such as when dealing with financial or patient information, this type of test would be the preferred method.

When deploying applications in the cloud, things can become quite complex due to the shared responsibility model. In a **Crystal-Box Cloud** (CBC) assessment, Secura tests not just the application or infrastructure from an external perspective, but also from the perspective of cloud security settings: usage of storage encryption, authentication settings, IAM configuration, logging and monitoring etcetera.

Internal Penetration Tests (IPT) are a great tool for improving the security posture of your internal network. If an attacker or a piece of malware gains a foothold in your network, it is essential to know what weaknesses exist that could be leveraged for them to gain access to the 'crown jewels' in your network. With an internal pentest our experts will test your resilience against these types of attacks.

Red Teaming (RT) is an increasingly popular method of testing that incorporate internal and external penetration testing with social engineering and physical access control testing to assess the cyber resilience of your whole organisation. Secura is also one of the accredited parties to perform TIBER Red Teaming exercises in the financial sector according to the scheme devised by the Dutch Central Bank and now rolled out across Europe in the TIBER-EU scheme.

Code Reviews (CR) are a part of any Crystal-Box Application assessment, but can also be performed as stand-alone projects, especially when code quality of specific research questions need to be addressed such as correct use of cryptographic primitives, software libraries or memory usage.

Example Cases

Below we provide several examples of the projects we have recently done for our customers. Secura performs over a thousand security assessments every year, and as a result we can provide many references if required.

For a large online retailer, Secura performed a grey-box application assessment. During this assessment, we identified several ways of manipulating content of the website, including ways that would impact visitors to the site negatively. We were also able to trick the payment API into thinking articles were paid for when they were not, leading to a possible fraud scenario. The customer was able to fix these issue even while we were testing.

For a government institution, Secura performed a black-box infrastructure and application assessment. This lead to the identification of several inadequately secured management interfaces and missing important patches for several other network services.

For an international job and labor broker, Secura performs biweekly automated and manual tests of their acceptance environment of the main web application. Yearly crystal-box application tests are performed on the production site, in conjunction with the frequent periodic scans so that this customer has a high level of assurance that security flaws will not be present in the production environment.

For a grid operator, Secura tested the smart meter 4G-communications modules and backend infrastructure. Cryptographic protocols were analysed and firmware was tested. As a result it was determined that all protocols had been implemented correctly and that proper safeguards had been provisioned in the backend to prevent manipulation.

For an international high-tech company, Secura performed an internal penetration test of their world-wide network, leading to a full compromise of the windows domain, despite many mitigations already being place. The remaining risks were subsequently addressed in an improvement plan. Additionally, SIEM use-cases were made so that future exploitation of these issues would be detected.

For a financial institution, Secura performed a Red Teaming exercise where several attack paths were uncovered that could have led to significant compromise, if abused by a malicious actor. Also, the Blue Team was trained and tested its responsive capabilities, leading to a valuable increase in insight into the bank's security and providing them with actionable recommendations for improvement.

For the Dutch government, Secura performed a source Code Review of the national COVID-19 contact tracing mobile app, on both iOS and Android.

Our Related Services

Whilst VA/PT might be a popular way to test security, Secura offers more, and sometimes more interesting ways of testing, depending on your testing targets and focus.

Technology Focus

If there is a need to gain the most detailed level of insight into your security posture, Secura can perform **Configuration Reviews** and **Source Code Reviews**. With all the source code, information and access available (see crystal-box testing above) it becomes possible to provide a detailed analysis of all settings and code aspects of servers, applications and cloud environments, giving our customers the best possible advice for increasing the security of their environments.

People & Process Focus

When you want to test the cyber resilience of not just an application, but your whole organisation, you will have to take other factors into account, such as physical security of buildings, offices or production plants. Secura has the skills and experience to test physical access controls, and this is often combined with **Social Engineering** (SE) exercises where the human aspects also come into play: is it possible for an attacker to gain entrance to your building by, for instance, simply faking an appointment, thereby being able to penetrate the internal network or leave rogue devices behind? And what information is leaking onto the internet and might this be abused by an adversary? Investigating Open Source Intelligence (**OSINT**) data allows Secura to paint a detailed picture of the exposure your organisation has on the internet.

Integrated Scope

In a **Red Teaming** exercise all these aspects come together, and based on scenarios, Secura tests the full spectrum of cyber-attacks: hacking, OSINT, physical access and social engineering. A Red Teaming exercise is often done when the basic security hygiene is under control (in terms of people, process and technology). A red teaming exercise gives valuable insight on how attackers may access (in a targeted manner) your digital "crown jewels".

Secura is one of the few parties in the world that performs **Red Teaming exercises in the Operational Technology** (OT) domain, for instance on Utilities and Grid operators, or Oil & Gas plants. In the OT domain it is not always possible however to test security in an offensive way due to the risks of disruption (although we know how to handle such risks). Therefore, a less intrusive way of testing OT environments is the **OT Risk Assessment**, which is more inspection-oriented but can be very valuable in providing a baseline security model for environments with industrial controls systems.

From our Red Teaming experience, we have also learned how to test the detective capabilities of SOC/SIEM implementations. Your security does not only depend on preventive measures, but also on the effectiveness of detective measures and Secura has developed a process and tooling under the name **Purple Box** that provides heavily controled simulated attacks in order to test detective capabilities of the SIEM and responsiveness of the SOC.

Of course, Secura understands that processes, policies and procedures are an integral part of your security posture, and we have services to assess those aspects also. If you want to assess your compliance to the controls of your security management system (e.g. ISO 27001, NEN7510), Secura can perform a gap analysis or a more formal audit, pinpointing possible risks gaps and weak spots.

Interested?

Would you like to learn more about our services? Contact us today:

Follow us:

+31 88 888 31 00

info@secura.com

secura.com