



BUREAU
VERITAS



RAISE YOUR CYBER RESILIENCE WITH SECURA'S

PENTESTING SERVICES

Does your system, network or cloud configuration contain weaknesses? You need to know before an attacker uses these against you. We can help you assess and test your digital security. Over the last two decades, our customers have asked us to perform security tests on virtually every imaginable target. Let us help you.

THESE PENTESTING SERVICES HELP YOU:



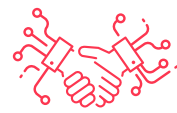
Know your weaknesses

You gain insight into potential cyber attack entry points and into vulnerabilities.



Strengthen your defenses

You receive concrete recommendations, so that you can protect your systems.



Stay ahead of attackers

Our specialists have up-to-date knowledge of tactics that attackers use, to help you stay ahead.

WHY PENTESTING IS CRUCIAL TO PROTECT YOUR ORGANIZATION

Even the most robust systems are at risk of falling behind. Attackers keep evolving their methods, exploiting both legacy issues and the latest vulnerabilities that your defenders may not even be aware of yet. While your organization has likely invested heavily in security measures, penetration testing (pentesting) goes a step further, by actively probing your technical defenses to determine if they are effective. Through simulated cyberattacks, our ethical hackers identify potential weaknesses before malicious actors can exploit them.

Our pentesting services combine Vulnerability Assessments and Penetration Testing (VA/PT). A **vulnerability assessment** identifies as many weaknesses as possible without exploiting them, so focusing on breadth. **Penetration testing** (pentesting) simulates an attack to exploit vulnerabilities, emphasizing depth and the real impact of a breach. Combined, these methods give a comprehensive security review.

Secura started as a technical pentesting company in 2001. This means our team has seen two decades worth of Tactics, Techniques and Procedures (TTPs) of threat actors. We have capabilities similar to nation-state actors and use this knowledge to help you strengthen your cyber defenses.

WHAT SYSTEMS DO WE ASSESS AND TEST?

Your organization's environment is unique, and so are your security needs. That's why we offer tailored assessments and tests across a wide range of systems and infrastructures, from IT to OT and IoT. Whether you need to validate the defenses of a critical **web application**, an **internal infrastructure**, a **connected device** or an **OT network**, we have the specialists to help you. We follow internationally recognized standards and frameworks where possible.



IT security testing

The aim of a penetration test is to illustrate as clearly as possible what the consequences of a certain issue with your IT security could be, and what that would mean to your organization. Many organizations choose to implement a structural approach to their IT security as a direct result of this test. We can perform a wide range of IT tests and assessments, from application to mobile and to cloud. If you have multiple systems or applications, we recommend determining the testing priority with a Threat Modeling session.



OT security testing

Many critical processes, for instance in industrial environments, rely on Operational Technology (OT). With the growing convergence of IT and OT, the dependence between the two is increasing. Both IT and OT systems must be reliable, making testing crucial for all systems. However, different approaches are required for each environment. Secura's specialized OT team can help you assess the security of your OT systems. Many of the services we offer for IT can be applied to OT environments, with modifications.



IoT security testing

IoT devices are increasingly becoming a focus of our testing and assessment services. Attackers target not only the network interfaces as is common in IT, but also the hardware, firmware, cloud based backends and related mobile applications, which are often not well understood. At Secura's specialized lab for device assessments, we thoroughly assess these components and use reverse engineering and firmware hacking techniques to identify potential vulnerabilities in smart office management, logistics and transportation systems, energy, retail or healthcare IoT.

IT PENTESTING SERVICES

- **Internal Penetration Test**
- **Mobile Application Assessment**
- **Web Application Assessment**
- **Cloud Assessment**
- **Endpoint assessment**
- **Domain Name System assessment**
- **Configuration review assessment**
- **Wi-Fi Assessment**
- **Firewall review assessment**
- **External Attack Surface Assessment**
- **IT Threat Modeling**

SPECIALIZED OT SERVICES

- **OT Vulnerability Assessment and Penetration Testing**
- **OT Threat Modeling**
- **OT Perimeter Assessment:** evaluates the security of the boundary between Information Technology (IT) and Operational Technology (OT) systems
- **ICS Cyber FAT-SAT:** an extension of the conventional FAT/ SAT with a focus on cybersecurity

IoT PENTESTING SERVICES

- **(Enterprise) IoT Assessment:** evaluates the security level of the (I)IoT devices and back-end services (customer isolation, cloud-based provisioning system, etc.)
- **(Enterprise) IoT threat modeling:** helps identify the best-suited secure design for devices and back-end services
- **Consumer IoT evaluation and certification**



INTERNATIONAL NORMS AND STANDARDS




It is important that the depth and width of your security test is unambiguous. That is why we use international norms and standards whenever possible. The standards we use depend on the assessment goal, the environment to be tested (architecture, platform, application, et cetera), sector requirements and regulations per country.

The most important norms we use are:

- Application Security Validation Standard (ASVS) for web and Mobile applications (M-ASVS)
- OWASP Application Security Testing Guide
- SANS-top 25: the most common and most dangerous errors when making software
- Sectoral standards such as PCI-DSS, BIO, DigiD and others.

HOW WE TEST: DIFFERENT TYPES OF PENTESTING

Security testing can be divided into three main types: black-box, grey-box, and crystal-box testing.

-  **Black-box testing** simulates an external attacker with no prior knowledge of the system, focusing on identifying easily exploitable vulnerabilities. It's useful for identifying potential entry points an attacker could exploit.
-  **Grey-box testing** uses credentials to assess access levels and internal vulnerabilities, making it ideal for sensitive data systems. This is the most common testing method, often combining black box techniques.
-  **Crystal-box testing** involves full access to source code or configurations, allowing for a more detailed vulnerability analysis, particularly in security functions like input validation and cryptography.

In practice, these testing types are often mixed, to make the most of our time and to mimic current TTPs: A cybercriminal might have purchased credentials from the dark web. Typically we start out from a black-box approach to determine if we can find a way to get accounts and further access - sometimes also using valid accounts we were given to determine if that would be possible - and then move on to the grey-box post-login part.



WHAT OUR CLIENTS SAY

“The team went beyond”

“We worked with Secura for a very critical project for Product Security. The entire team was very knowledgeable and excited to deliver the outcome. The team also went beyond what we had requested and advised us to make corrections through the course of the project which we really appreciated.”



BEYOND A SCAN: HOW WE DELIVER HIGH-QUALITY TESTING



Highly specialized testers

Secura's penetration testing team performs hundreds of security tests each year. All testers are certified to a minimum standard, but most have multiple certifications, such as OSCP, OVSE, eCPPT, GIAC GPEN. This team can perform virtually any security test.



Certified partner

We are accredited for pentesting by CREST and were the first company to be certified for the Dutch 'CCV-keurmerk Pentesten' certification. Our product security lab is accredited by Common Criteria. Secura is one of only a few companies accredited by the Dutch government for the BSPA (Baseline Security Product Assessment) scheme.



Quality Assurance Process

Even if we do not find anything in a given test you will be able to check our research report and have independent people validate that we did all the correct tests and interpreted test results correctly. Our four(+) eye principle means that each report is seen by at least two experienced testers.

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. Our customers range from government and healthcare to finance and industry. We offer technical services, such as pentesting and red teaming, but also provide audits, forensic services and awareness and behavior programs. We help clients all over the world to raise their cyber resilience.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.



EXAMPLE CASES | PENTESTING SERVICES



For a large online retailer, Secura performed a grey-box application 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 client was able to fix these issues while we were testing.



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 in 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.



BUREAU
VERITAS

INTERESTED?

Contact us today to start raising your cyber resilience.



info@secura.com



+31 (0) 88 888 3100



[secura.com](https://www.secura.com)