INFIGO SECURITY ASSESSMENT SERVICES

Real security testing
for real results

SECURITY ASSESSMENT SERVICES

Just as car manufacturers crash their cars to see if they are safe for the open road, **the only legitimate way of checking if your infrastructure can handle a real cyber-attack is to attack it for real**. Infigo IS will attack your **networks, applications, and everything between but instead of a trail of destruction we will produce reports** that will help you patch vulnerabilities, keep cybercriminals at bay, and appease regulatory bodies

We know you and your organization cannot waste your time on a sub-par deal. So, here are just a few reasons why Infigo IS is the best company for your every security assessment need:

- we have **more than 15 years** of penetration testing history
- we do **more than 350 security assessments per year**
- we are **regularly invited to NATO's yearly cybersecurity exercise**
- our team lead is also **a SANS certified instructor** (less than 100 in the world) teaching penetration testing to generations of security professionals all over the world
- our security specialists have certificates from leading international security organizations – **CEH, Offensive Security, ISC2, ISACA, SANS**
- we use various models and best practices like **OWASP, PTES, NIST**, but we also developed our own methodologies stemming from many years of security assessments
- we did security assessments for the biggest banks in Europe and the Middle East, space agencies, international retail chains, car manufacturers, oil distributors, and many, many more

What are security assessments?

A security assessment is any process that **tests the real security status of a product or a service** – during the testing phase, security specialists use the same procedures and tools as cybercriminals so the organization knows how a product, or a service, will behave under attack by a malicious actor. Of course, **security specialists will never harm any system** they test, and before every test, they go through rules of engagement.

Every security assessment is different in scope and complexity, and not all are interchangeable. Infigo IS performs the following:

- vulnerability scanning
- penetration testing
  - internal networks
  - external networks
  - wireless networks
  - web applications
  - thick client applications
  - mobile applications
  - social engineering
  - specialized tests (SCADA, info kiosks, payment gateways...)
- red team exercises
- source code audits

The Report

The security assessment report is **a vital part of the operation**, as it serves for fixing any found vulnerabilities. Our reports contain an **Executive Summary**, high level, non-technical summary of the assessment with business impact associated with found vulnerabilities, **General testing summary, testing scope, methodology, and vulnerabilities findings** with security specialist's comments, security risk score, and recommendations for remediation.

Three types of approach

Usually associated with penetration testing, there are three types of approaches, each suitable for a different scenario or scope of the test. Infigo IS advises clients on every aspect, so the tests are focused and appropriate for the test goal.

Zero-knowledge

With a zero-knowledge approach, testers have no knowledge of the target system – with this approach it can be said it closely corresponds to an attack any cybercriminal would try. It is up to the testers to gather intel, exploit any weaknesses in running applications or misconfigurations, and try to escalate gained privileges. Most suited for publicly available resources.

Partial knowledge

With a partial knowledge approach, testers have limited knowledge of the target system – organizations can provide testers with login credentials for a low-level privilege account. In that case, it would mimic a disgruntled employee or just an unfortunate breach; the goal would be to see how much damage an attack of this kind could cause. Since testers are already in the system, it is all about exploitation and lateral movement.

Full knowledge

With a full knowledge approach testers have full access to the source code, network topology, credentials, documentation, everything that the organization has. This enables testers to sift through the often massive amount of data, finding vulnerabilities in as many systems as possible. Depending on the scope, the full knowledge approach can be lengthy in nature.

Vulnerability scanning

Vulnerability scanning is a test that every organization should be doing on **a regular basis**. It has **the widest scope** and identifies many so-called low-hanging fruit weaknesses and can be done for external and internal networks, applications, and services. Depending on the target, security specialists will use different tools – usually, we do not use the same tools for network and application vulnerability scans.

The problem with vulnerability scanning tools is that they have challenges with complex applications or with business logic, so **it is important to know when the limitation of the tools exceeds their usefulness**.

Vulnerability scanning can also generate a lot of false positives, but with Infigo IS, a security specialist will manually verify the results and remove them.

Penetration testing

Penetration testing is **a more focused** kind of security assessment with **the goal of finding as many, if not all, vulnerabilities in a target scope**. That is why the scope is extremely important to define – it can be an IP address, network, application, service...

This kind of test never produces a false positive result, and it especially focuses on logic vulnerabilities that cannot be discovered by any type of a tool. Of course, security specials will find others, more common vulnerabilities, like misconfiguration or weak login credentials, but penetration testing requires a lot of manual work that is gained only with experience.

Each penetration test is conducted in accordance with legal, technical, and ethical standards **without disrupting daily business operations**.

Red Team Exercise

The ultimate security test is a red team exercise – while vulnerability scanning tries to find the low-hanging fruit, and while penetration testing tries to find all vulnerabilities in a narrow set of targets (or even one target), **a red team exercise tests the organization as a whole**.

A red team usually has one goal, but how they achieve it, it is up to them – they can exploit software, hardware, people, procedures, physical security, just about anything.

As always, there isn't a single security assessment test that causes harm or destruction to an organization's property, and a red team exercise isn't any different.

In the end, **a red team exercise will give the organization a great understanding of what its complete security posture looks like**, what their weaknesses are, and what it should do to elevate its maturity level.

Since it is at the top of security assessment tests, it is advisable to go through lower levels (vulnerability scanning and penetration testing) before deciding on a red team exercise.

Source code audit

Before releasing your application into the world, it is **a good security practice to do a code audit**. In that way, security flaws get flagged and dealt with before somebody tries to exploit them in the wild. It is also prudent to do **a code audit before third-party application purchase**.

Our security specialists search for potential vulnerabilities in the areas of authentication, authorization, data validation, encryption, error handling, logging, and session management.

Types of penetration tests

External network penetration test

It simulates **an external attacker** trying to penetrate your public-facing infrastructure – in today's world, every organization has servers, network equipment, remote access, and many other points that are exposed for the whole world to see.

Internal network penetration test

It simulates an attack where **an attacker is already inside your network** – while the external network penetration test focuses on gaining access, the internal network penetration test focuses on elevating privileges (for example, getting an administrator account) and gaining as much control as possible.

Wireless network penetration test

The goal of the test is to assess the possibility of **breaking into a corporate network via the wireless network**; this test is carried out with specialized tools and equipment for the most accurate results. The test can also include identification and mapping areas of wireless accessibility that **is required for the PCI DSS standard, and ISO 27001**.

Web applications penetration test

The most common penetration test as web applications are usually among the most exposed components of the information infrastructure. The test searches for vulnerabilities like code injection, cross-site scripting, request forgeries, and many more, but the special focus goes towards business logic vulnerabilities that are hard to find but can be detrimental to the information system as a whole.

Thick client apps penetration test

Thick or fat clients are **applications running on workstations** (for example, Windows applications) commonly based on two-tier (client-server) or three-tier (client-application server-database) architecture. Our tests cover client, server, and network side attacks with additional information gathering (for example, binary analysis and application architecture).

Mobile apps penetration test

With the extremely high number of mobile apps floating in our private and corporate lives, mobile applications penetration testing has become increasingly important to every security-minded organization. **Our tests try to attack not only the application** (static and dynamic analysis, reverse engineering...) **but also the server-side** that handles application/user requests.

Social engineering

Social engineering is in its essence just **hacking people**, not software or hardware. The goal is to trick people to do something they should not do, click something they should not have, execute a file that never should be executed. We make custom tests, engineered especially for the industry sector or organization, with custom-made payload files and C&C (command and control) servers.

Specialized penetration tests

Some devices or/and services demand a special, **one-of-the-kind approach** where Infigo IS excels. From SCADA systems, over digital power meters and IoT devices (especially smart devices), to mobile payment schemas (for example, HCE) we use custom hardware and custom-designed attacks to expose weaknesses in the design or circumvent built-in security measures.

68% of business leaders feel their cybersecurity risks are increasing, and, unfortunately, they are right

What happens next is up to you - let us make your life easier

www.infigo.is

INFIGO IS d.o.o.
Karlovačka 24a
10020 Zagreb
Croatia
+385 1 4662 700
info@infigo.is

INFIGO IS d.o.o.
Hasana Brkića 2
71000 Sarajevo
Bosnia and Herzegovina
+387 33 821 245
info@infigo.ba

INFIGO Software Design LLC
2902, Level 29, Marina Plaza
Dubai Marina, Dubai
PO Box 5000307
United Arab Emirates
+ 971 4 512 4081
info@infigo.ae

INFIGO IS d.o.o.
Tivolska cesta 50
1000 Ljubljana
Slovenia
+386 1 777 89 00
info@infigo.si

INFIGO IS d.o.o.
Ul. Metodija Shatorov Sharlo br. 30/2-17
1000 Skopje
North Macedonia
+389 (0)2 3151 203
info@infigo.mk