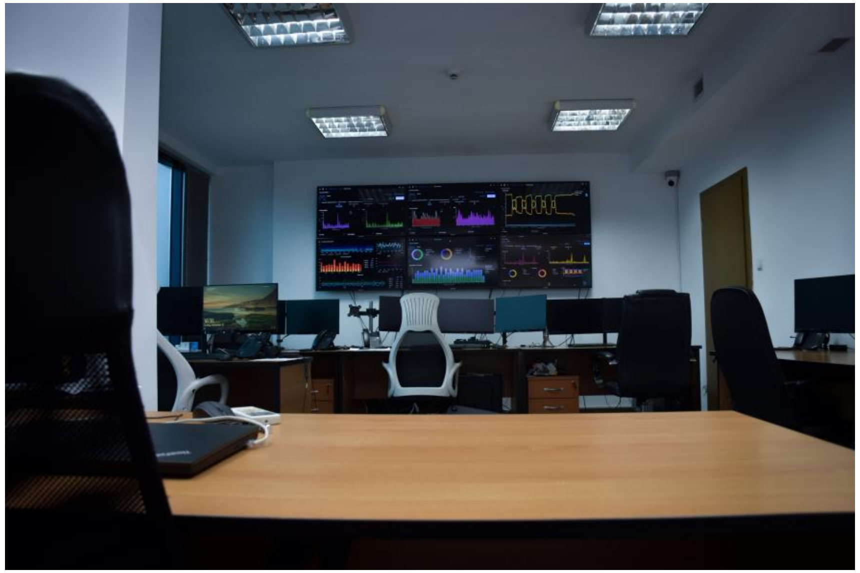
CYBER ONE

Cybersecurity Solutions

More information about us

CYBERONE is a company founded by Israeli and Bulgarian cybersecurity specialists in 2018. The company provide Israeli know-how and variety of technological solutions related to cybersecurity and information technology. The main priority of the company is the successful and effective provision of cybersecurity solutions to businesses in Europe.

Since 2019 the company established their own advanced Security Operation Center in Sofia, Bulgaria. Together with our partners we strive to provide quality cybersecurity and IT services. In addition, we provide complete software and hardware solutions for Cybersecurity and data protection.



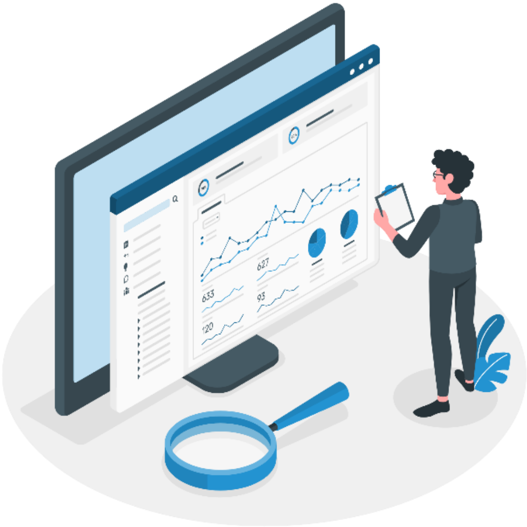
How can we protect you?

Passive protection

Implementation of mechanisms for passive control and protection of IT infrastructure

Proactive protection

Providing regular penetration tests and vulnerabilities scan



Monitoring

Implementation of innovative solutions for monitoring servers, workstations and networks

What is a penetration test?

Penetration tests simulate real scenarios of malicious attacks against web applications and systems, as well as internal and public network infrastructure. The process of conducting such tests is fully controlled and according to customer requirements. The procedures and attack techniques executed are the same as those used by malicious individuals during actual attacks allowing the organization to determine how prepared they are for such scenarios. At the end of each test a professional report is issued with detailed information, examples, photos and recommendations for resolving the reported vulnerabilities.

- ✓ Identification, verification and assessment of vulnerabilities in networks and web applications
- ✓ Testing for vulnerabilities that cannot be detected with automated tools and methodology
- ✓ Recommendations for mitigation of all reported vulnerabilities
- ✓ Proof of Concept

Why do you need a penetration test?

CYBER ONE

The process of recovering from a security breach can cost your business thousands or even millions of dollars including expenditures on customer protection programs, regulatory fines and loss of business operability.

A pentest will uncover the holes within your network, application, and data security you didn’t know about. You may need to fix misconfigurations in a service or fix a compromised web server you forgot about.

A penetration test is a proactive solution for identifying the biggest weaknesses and risks in your IT systems and for preventing your business from serious financial and reputational losses.

The last thing you want is a publicized data breach. Your customers will lose trust in your organization and their loyalty begins to falter after a major data breach.

A pentest could also reveal poor practices within your security team. The results of your penetration test will most probably reveal flaws within the network that you might not expect as well.

Advantages for your company

CYBER ONE

- Shows your security team in real-time how attack vectors impact the organization.
- A pentest uncovers major vulnerabilities
- Pentest prioritizes your vulnerabilities into low, medium, and high risks
- Gives you an opportunity to fix vulnerabilities
- Identify problems you didn't know existed
- Show you the strengths within your environment
- Identify security controls you need to implement
- Help you enforce your security strategy
- Reveal poor internal security processes
- Give your organization and team more confidence
- Enhance the performance of security technologies
- Help inform governance and compliance improvements
- Train your security team on how to better detect and respond to threats
- Allow your team to optimize incident response process
- Test your team's ability to conduct remediation and incident reporting
- Improve your business continuity
- Protect your most critical data
- Helps your team map the cyber kill chain related to your organization
- Provides your Management and Leadership Team with insightful reports
- Helps your organization align with industry security standards
- Strengthen customer trust and loyalty
- Gives you a new perspective on your network, application, and data
- Assess the potential impact of a successful attack on your organization
- Can help your organization prioritize budget and spending on security
- Better understand your readiness in mitigating cyber threats
- Prevent a potential downtime for your business
- Uncover hidden vulnerabilities before the criminals do

[Web Penetration Test]

CYBER ONE

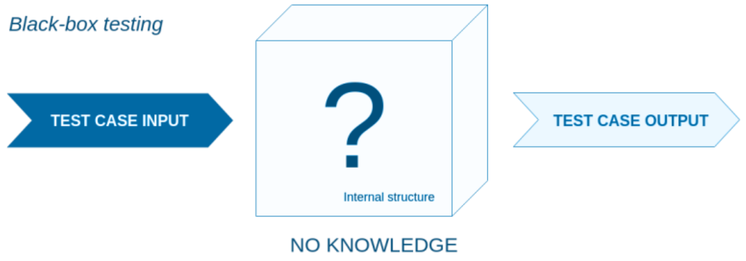
This service is a combination of automated and manual security testing (our policy is to prioritize the latter). The main goal of conducting this type of services is the proactive detection of weaknesses in information security and vulnerabilities in an organization.

1. Reconnaissance is conducted to identify services, technologies, including their versions, configuration and operation.
2. An initial automatic vulnerability scan is performed with a minimum of 2 popular scanners such as Acunetix and Netsparker.
3. The results of automatic scanning, as well as the findings of our specialists are checked and the collected information is used for follow-up actions aimed at gaining access in one way or another.
4. A comprehensive security check of the applications within the agreed scope is performed, using our checklist of checks and vulnerability detection methods, compliant with world standards, as well as good practices.
5. An attempt is being made to escalate access through the vulnerabilities found.
6. A final report is prepared, which includes detailed information on all found vulnerabilities, as well as recommendations for mitigation, references, etc.
7. The report also includes a section dedicated to people management, which describes in detail everything in as little technical language and terminology as possible.
8. After agreeing on a deadline for mitigation of all vulnerabilites, the client has the opportunity to receive a retest on the agreed scope within 6 months of the initial tests.
9. An additional report is delivered based on the results from the retest.

[Web Penetration Test]

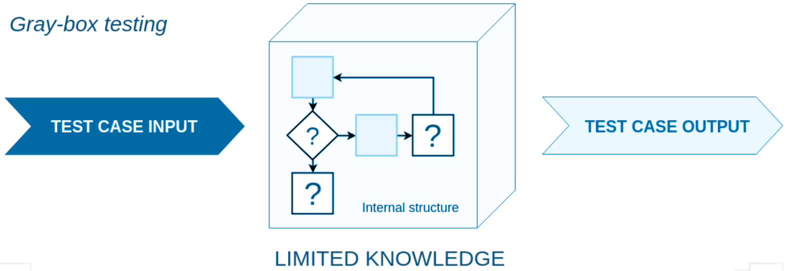
Blackbox Web Penetration Test

- No prior information about the technology or the applications of a company is required.
- You do not need to grant any access to the application or system.
- The results are based on the initial access that our specialists had.



Graybox Web Penetration Test

- It is possible for the client to provide partial access for the applications in the scope.
- Partial information on the technologies and infrastructure of the applications in the scope is provided.
- It is recommended that you use this approach in business applications, as well as applications that are only used by people with pre-granted access.



Reconnaissance ❯ Scanning ❯ Gaining Access ❯ Privilege Escalation

[Internal Network Penetration Test]

CYBER ONE

One aspect of a common security concept that is often overlooked is the internal network within an enterprise. The general belief is that the internal network (intranet) is not accessible from external assets and is therefore not likely to be prone to an attack. On the contrary, the weakest link in almost all cyber defense framework is the employees of the organization. They have access to internal assets and are responsible in terms of security practices. The main reason for this is that most attacks are expected to come from the outside. However, according to the latest research, the number of internal attackers is increasing rapidly and becoming more and more popular.

We can test the security of your local network remotely via VPN or locally on-site.

- Target identification
- Host discovery
- Fingerprinting vendor(s)
- Outlining the scope
- Port scanning
- Service identification
- Service enumeration
- Vulnerability Assessment
- Automated testing
- Manual probing

- Verification of identified issues
- Testing for common vulnerabilities
- Exploitation of vulnerabilities
- Testing for logical flaws in organizational units
- Usage of known exploits
- Usage of custom scripts or modified public exploits
- Leveraging identified vulnerabilities

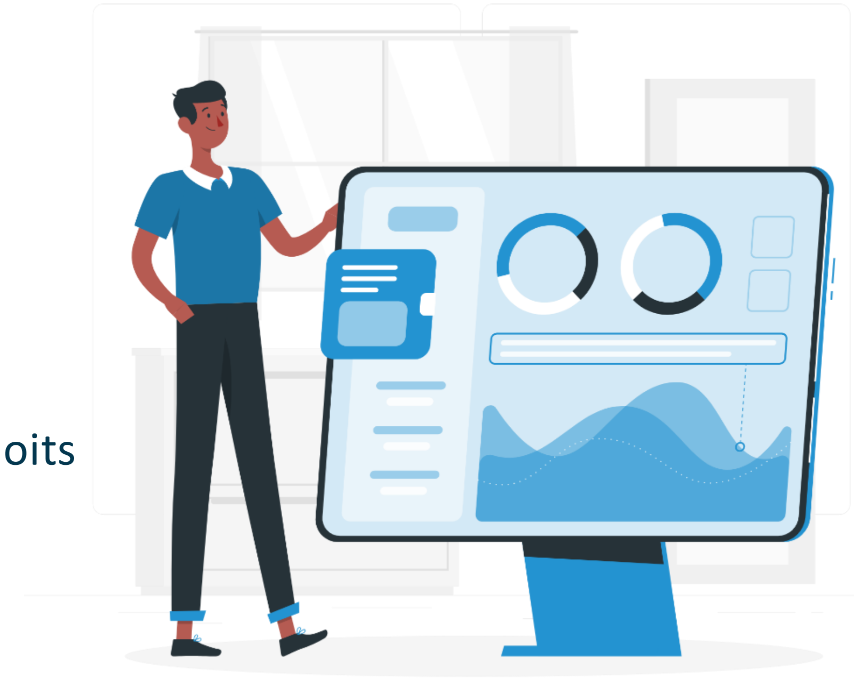
[External Network Penetration Test]

Unlike internal, external network penetration testing simulates a black box attack on an enterprise’s Internet infrastructure. For testing purposes, the penetration tester receives only scope range (which typically includes IP range, topology, domains/subdomains, etc.). The test is run remotely and requires no user intervention.

Both types of network security audits include testing of web applications and web services as well. Tests performed can simulate a malicious targeted attack. A report is issued at the end of the penetration test in order to provide an easily comprehensible description of the findings as well as recommendations on how to mitigate the vulnerabilities.

Both solutions represents a compact solution consisting of:

- Target identification
- Host discovery
- Fingerprinting vendor(s)
- Outlining the scope
- Port scanning
- Service identification
- Service enumeration
- Vulnerability Assessment
- Automated testing
- Manual probing
- Verification of identified issues
- Testing for common vulnerabilities
- Exploitation of vulnerabilities
- Testing for logical flaws in organizational units
- Usage of known exploits
- Usage of custom scripts or modified public exploits
- Leveraging identified vulnerabilities



CYBER ONE

Contact us:

www.cyberone.bg
office@cyberone.bg

+359 88 260 0493

51D “Cherni Vrah” blvd.
Sofia, Bulgaria