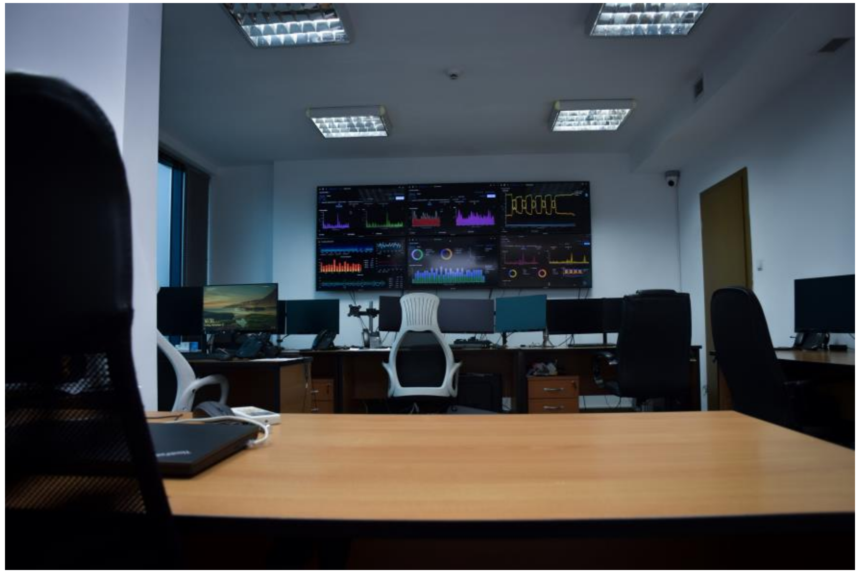
CYBER ONE

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?

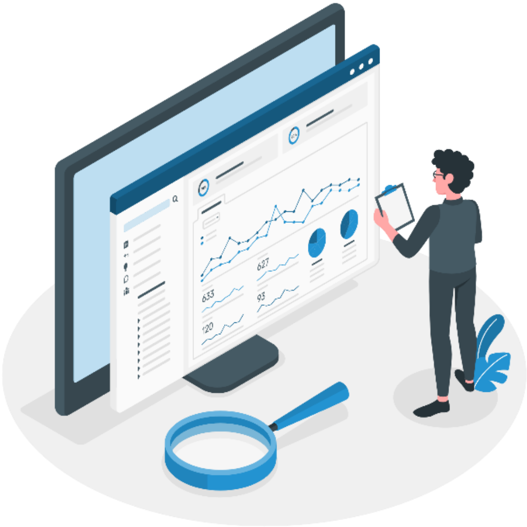
CYBER ONE

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 vulnerability assessment?

CYBER ONE

Vulnerability assessment is the process of identifying vulnerabilities commonly known in information systems only by using automated assessment methods. The term is often associated with penetration testing, and the two are widely used interchangeably. However, there are important differences between the two terms, so don't confuse them with each other. Penetration testing focuses on exploiting the vulnerabilities found and on other hand the vulnerability assessment only identifies vulnerabilities in the system without actually testing/exploiting them.

This service includes priority for automatic scanning vulnerabilities based on impact, severity, and likehood. **This is suitable for organizations that tend to get a general overview and awareness of cybersecurity.** The main purpose is to identify vulnerabilities that can lead to unauthorized information and data exposure. Depending on the system, the assessments fall into three categories.

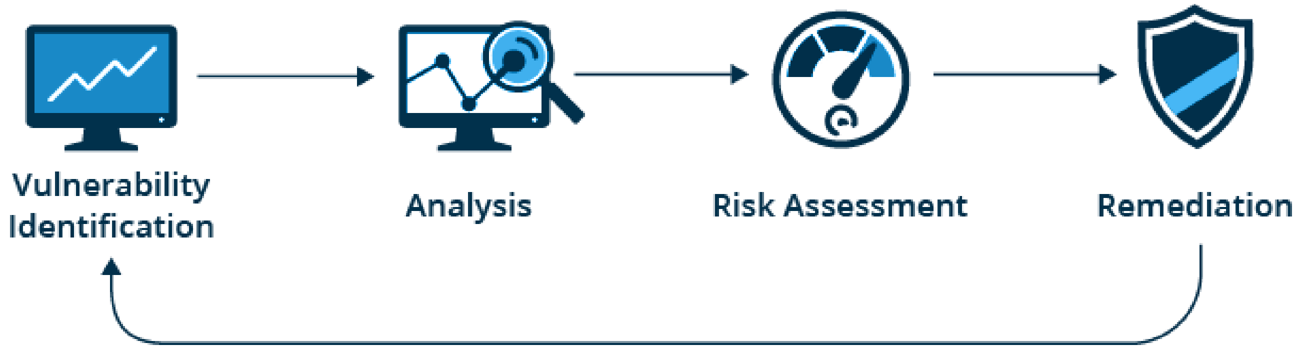
Host scans

Network scans

Application scans

Security scanning process

The security scanning process consists of four steps: testing, analysis, assessment and remediation.



1. Vulnerability identification (testing)

The objective of this step is to draft a comprehensive list of an application's vulnerabilities. Security analysts estimates the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually.

2. Vulnerability analysis

The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one. It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability. For example, the root cause of a vulnerability could be an old version of an open source library.

3. Risk assessment

The objective of this step is the prioritizing of vulnerabilities. It involves security analysts assigning a rank or severity score to each vulnerability, based on many risk factors.

4. Remediation

The objective of this step is the closing of security gaps. It's typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.

Delivery process

CYBER ONE

1. Assessment scoping

We can help you determine which part of your IT infrastructure can benefit most of a vulnerability assessment. It is always a good idea to eliminate IPs, domains or system which are inactive or part of a staging environment.

2. Signing agreement

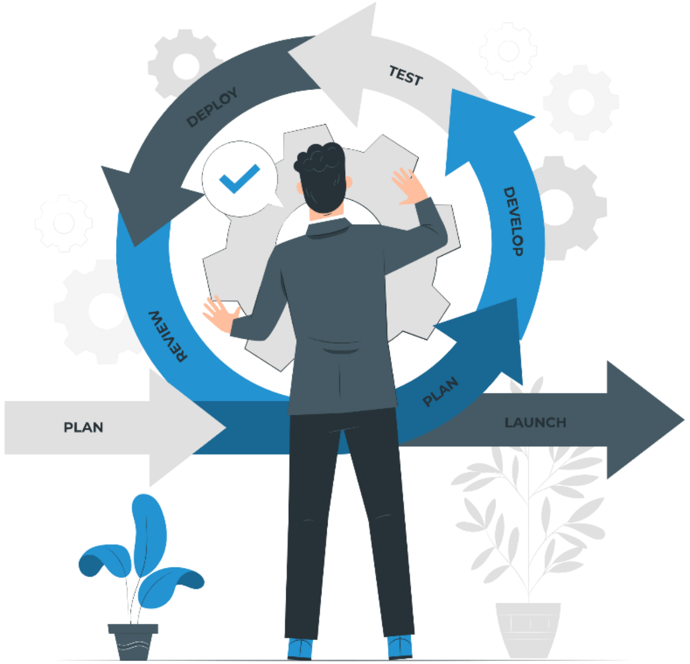
Your company will sign an agreement with us as well as an NDA. The project scope will be outlined in the contract in order to ensure that we do not violate the scope of scans. The start and continuity of the assignment is also determined and noted in the contract.

3. Performing the vulnerability assessment

Our team will begin performing the vulnerability assessment and will notify you if there are any performance or connectivity issues while scanning.

4. Final report delivery

The final product is a report from an automated scanner that has been reviewed and approved by experts. It includes a summary and classification of vulnerabilities, image content as well as recommendations for mitigation of risks, references and fixes.



CYBER ONE

Contact us:

www.cyberone.bg
office@cyberone.bg

+359 88 260 0493

51D “Cherni Vrah” blvd.
Sofia, Bulgaria