CHECK POINT | CHECK POINT PROFESSIONAL SERVICES | CHECK POINT Cyber Resilience Team

Cybersecurity Resilience (Penetration) Test

Protect Your Critical Assets from Hackers

We live in an era in which companies are targeted for cyber-attacks on a daily basis. Cyber-crime is a worldwide phenomenon that causes millions of dollars in damages each year. The rapid development of new technologies makes it hard to keep track of your company's vulnerabilities and secure them. Check Point's Cybersecurity Resilience test (CRT) will evaluate the defensive capability of your business against the latest techniques used by malicious actors. Our security experts will perform a series of controlled real-world attacks and will make recommendations on how to improve your infrastructure's resilience.

Check Point's Cybersecurity Expert will:

- Work side-by-side with your response team to detect, react and mitigate your security vulnerabilities
- Help you to experience, assess, and remediate in advance a cyber-attack in a controlled/live environment
- Identify and protect your most critical assets and vulnerabilities at every level of your asset's hierarchy
- Reduce your response time to potential security events and service interruptions

Why Check Point?

- Worldwide leader in securing the Internet for 30 years.
- Protecting over 100,000 organizations of all sizes.
- The best penetration testers in the industry with vast experience in offensive and defensive security related activities.
- Collaboration with Check Point's Research and IRT teams, positioning the CRT service as the most advanced cyber resilience test in the world.

The 3 Ways to Perform a Pentest

Black Box Test

Penetrating the system with limited access and information, simulating an attack as a site user or a collaborator of the company.

Grey Box Test

Penetrating the system from the outside with a limited amount of information on the organization and its information system. Simulation of an attack as a site user or a collaborator of the company.

White Box Test

The penetration tester has all the information about the system, including the source code. He works and collaborates with the organization technical team in order to detect as many vulnerabilities as possible.

Types of CRT Offered by Check Point

- **External network** - designed to test the effectiveness of perimeter security controls and identify vulnerabilities in internet-accessible systems such as web, mail and FTP servers.
- **Internal network** - designed to identify what an attacker could achieve with initial access to a network. For example, insider threats, such as employees intentionally or unintentionally performing malicious actions.
- **Wifi** - assessment of wireless local area networks (WLANs) and the strength of their encryption, as well as use of associated wireless protocols and technologies to identify vulnerabilities that could lead to unauthorized network access and data leakage.
- **Mobile application** - testing the mobile apps and the services with which they communicate. Identifies the configuration and deployment flaws associated with integrating mobile solutions into your operating environment.
- **Web application** - assessment of your web applications' key components and supporting infrastructure, including how these components are deployed and how they communicate with users and server environments.
- **Social Engineering** - identifying whether your employees are vulnerable to phishing emails, allowing you to improve your company's cyber security awareness.

Penetration Test Process

1. Scoping
Preparation of a tailor made test for your security environment needs

2. Reconnaissance
After the test scope and goals are defined, out team will gather all the relevant intelligence about the assets

3. Scanning and Enumeration
Possible entry points are identified with manual testing and automated scanning

4. Exploitation
Web application attacks are executed, our penetration testers try to actively exploit security weaknesses

5. Documentation
Successful attacks are thoroughly documented and severity levels are determined

6. Mitigation & Support
Working closely with your organization's relevant teams, all security vulnerabilities will be mitigated according to the best possible practice

SKU and Description:

SKU	Description
CPTS-PRO-PENTEST-APP-1Y	Application Cyber Resilience Testing (one Web Application) OR Mobile Application Cyber Resilience Testing (one Mobile Application). Valid for 1 year.
CPTS-PRO-PENTEST-INFRS-1Y	Internal infrastructure Network Cyber Resilience Testing for 1 (One) Active directory domain OR External Network Cyber Resilience Testing, up to 32 IP addresses. Valid for 1 year.

To find out more, email us at ps@checkpoint.com

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com