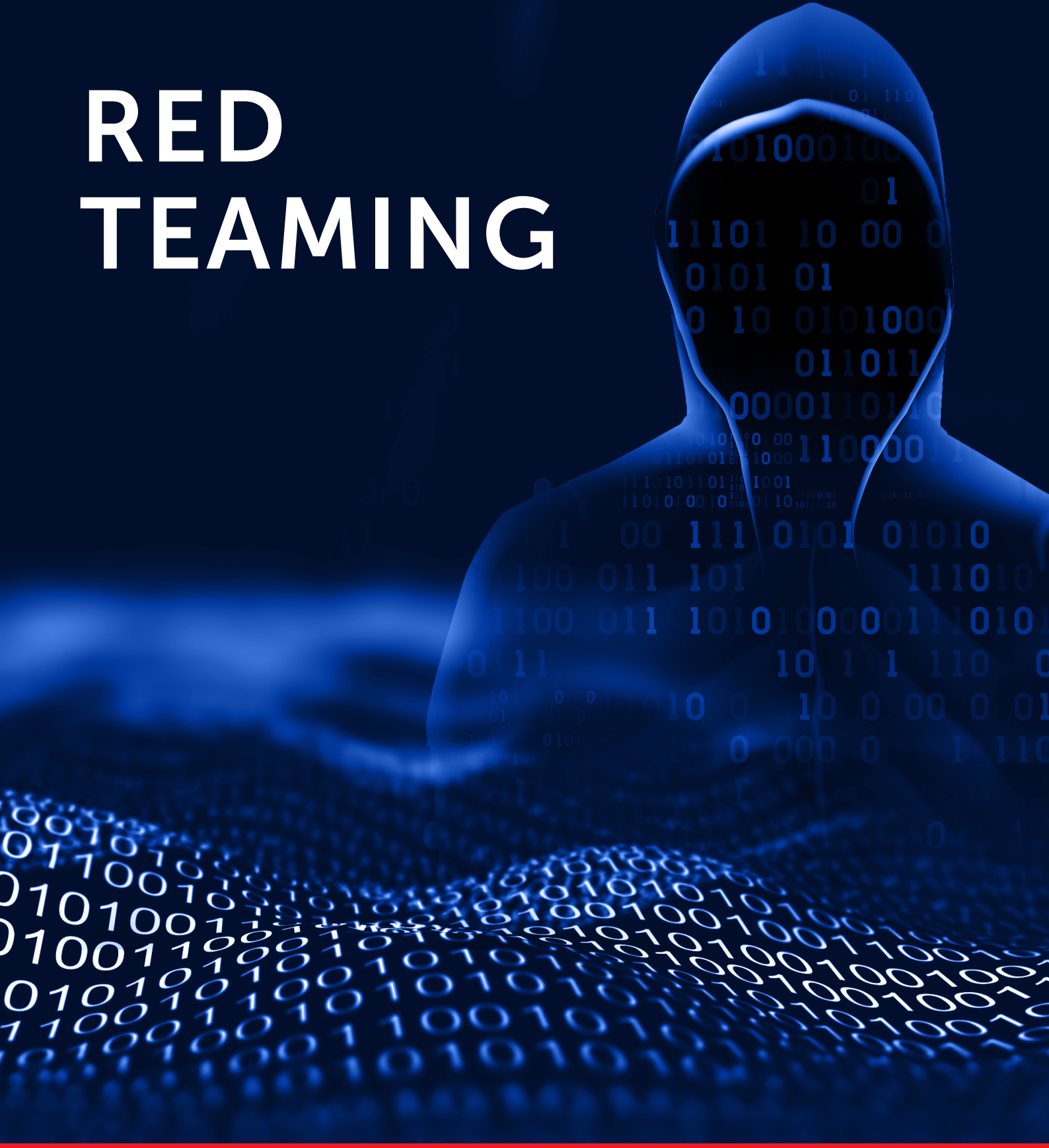
RED TEAMING



COMSEC

What is a Red-Team Exercise?

Red Teaming provides clients with a realistic understanding of the key cybersecurity threats and gaps they are facing, as well as the mitigation and response capabilities they possess. Rather than testing a single system and/or application, Red-Team activity tests the weakest paths into the organizational network. In most of the cases it is the most cost-efficient way to evaluate a company's resiliency to a real-life cyber-attack.

The Problem

Many organizations are taking action to secure their applications and networks as part of their security policy by conducting penetration tests., However, this might only provide a partial overview of their readiness for a real world attack. The reason for that, is that penetration tests are, most of the time, limited in scope and resources and therefore only demonstrating the impact against a certain application or system.

These clients may therefore be faced with several limitations that impact the overall security level of the organization:

1 | Limited insight into cybersecurity threats facing the organization

2 | Security solutions with unproven efficiency

3 | Untrained SOC team

4 | Lack of understanding of the exposure level of the organization

5 | Lack of insight into the security level of current infrastructure

6 | Weak business case for various goals such as SOC team improvement/ installation, IT maintenance, organizational-level upgrades, etc.

Comsec's premium red team service validate all of the above, alongside specific recommendations to mitigate the identified risks and vulnerabilities in order to improve the overall security level of the organization.

Comsec's Red Team Offering

Comsec's red team service offers a variety of customized cyber-attack scenarios against people (if needed), processes, and technologies. Throughout the course of the exercise, the Red Team performs controlled cyber-attacks against the client's corporate network to test the entire ecosystem and see how one security solution interacts with another and, depending on the goal of the test, to breach the perimeter, get control over predefined assets and exfiltrate them.

Red Team Exercise Goals

The Red Team attempts to breach the organization's perimeter in order to demonstrate how vulnerabilities in the organization's infrastructure, applications and processes – as well as the lack of awareness of its employees, or incomplete/inactive policies – could allow its assets to be compromised.

The Red Team's mission is defined as follows and is focused on successfully capturing three main objectives:

Breach the Perimeter

Attack from outside of the organization's facilities, getting inside.

Lateral Network Movement

Attack from within the organization's network and move laterally within the network to reach sensitive areas with elevated network rights.

Capture The Flag

Establishing access rights into servers, preferably with Domain Administrator rights.

COMSEC

Attack Levels

The research and exercises are being conducted on the basis of a predetermined attack profile. There are four levels of attack defined in which research and execution can take place with different resources. Each level has its own limitations and attack techniques:

1 | An attacker who only requests anonymity and needs the cheapest possible access attempts to access systems using open source software. The attacker will be looking for standard vulnerabilities that can be implemented quickly on many servers at once.

2 | A novice hacker where a limited budget is available to gain access to the networks of the party under consideration. The attacker will focus more on a specific target and has a focused goal.

3 | A professional hacker who works alone, but has professional resources and knowledge to deploy his own exploits against the organization. Specific attacks such as the use of proper written exploits of Social Engineering attacks are used to achieve the goal.

4 | The hacker-for-hire. Multiple hackers are hired by an organization and try to breach the external perimeter. The greater the value of the hack, the more resources are used during the attack.

Comsec's Value Proposition

Comsec offers a unique approach to Red Teaming services by combining proven domain expertise with a result-oriented mindset, supported by unique methodologies for intelligence gathering, infiltration, and attack techniques.

By tailoring the Red Team activity to the client, Comsec is able to accurately identify the most relevant cyber threats and provide the client with pragmatic insights into risk and feasibility. Moreover, this process demonstrates to the client their ability to detect and react to threats, and exposes gaps in mitigation techniques and security infrastructure.

While the traditional approach to Red Teaming only focuses on the technical aspects of cybersecurity, Comsec utilizes its renowned ability to analyze business and regulatory-level threats, risks, and perspectives in security in order to craft a unique and all-encompassing cybersecurity posture for clients.

Comsec UK

33rd floor, Euston Tower
286 Euston Road
London, NW1 3DP, England
Tel: +44 (0) 2034638727
info@comsecglobal.com

Comsec BV

Hogehilweg 4
1101 CC Amsterdam
The Netherlands
Tel: +31 (0) 102881010
info@comsecglobal.com

Comsec HQ

Yegia Kapayim St. 21D
P.O.Box 3474, Petach-Tikva
Israel 49130
Tel: +972 (0) 39234646
info@comsecglobal.com

COMSEC