Red Teaming

AEC

With the development of new types of attacks, and with the increase in their sophistication, penetration testing ceases to serve its purpose satisfactorily. Therefore, it is necessary to start testing applications and infrastructure in a more comprehensive way. Standard testing methods reveal various types of vulnerabilities, but do not check the ability to detect, respond to and recover from a cyber-attack.

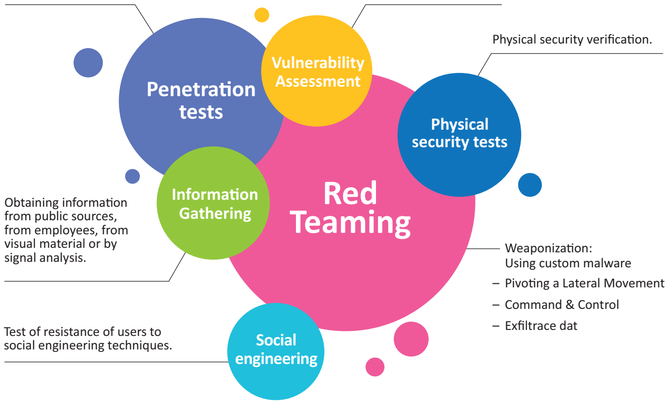
The Red Teaming service faithfully simulates the threat of attacks using state-of-the-art technology, tactics and provides information on the company's readiness to detect and eliminate these attacks and take corrective action.

www.aec.cz

What is the Red Team?

In the framework of cyber security, we label the Red Team as a group of experienced and organized ethical hackers whose task is to carry out a simulated attack on a given entity. The attack tests cyber and physical security as well as internal processes and communications in the framework of the technical and other teams in charge of cyber security. The whole exercise is carried out as a covert operation, about which only a very small group of people are informed - usually the company's top management.

The Red Team faithfully simulates the tactics, techniques and procedures of real attackers. By suitably defining the goals, we verify the effectiveness of the people, processes and technologies used to defend a company. During the Red Teaming exercise, your employees will be indirectly trained by real situations in a controlled manner, without the threat of real damage.



Exploiting vulnerability

Identifying vulnerability

Physical security verification.

Obtaining information from public sources, from employees, from visual material or by signal analysis.

Weaponization:
Using custom malware
- Pivoting a Lateral Movement
- Command & Control
- Exfiltrace dat

Test of resistance of users to social engineering techniques.

Red Teaming

AEC

Definition of roles

RED TEAM

Our specialists who simulate the tactics, techniques and procedures of attackers.

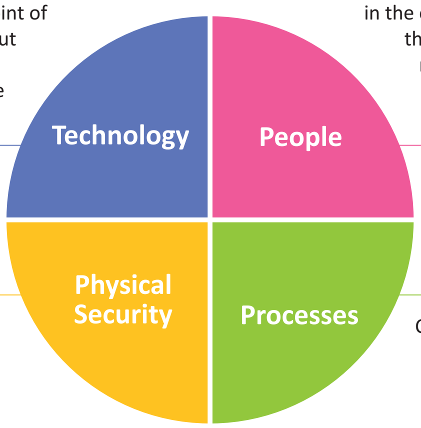
WHITE TEAM

A selected team from the company's management that oversees the exercise as it unfolds.

BLUE TEAM

A team of the company's internal security specialists, which detects the attack and takes the necessary countermeasures.

Red Teaming



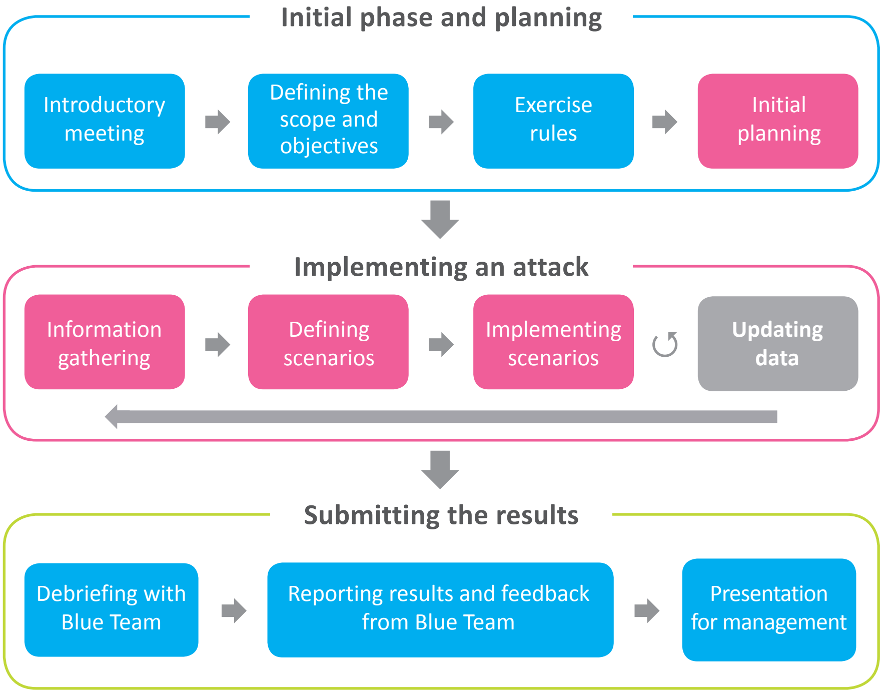
Red Team checks the technology not just from the standpoint of possible vulnerabilities, but also from the standpoint of the effectiveness of the defensive tools deployed.

Checks people's ability to react in the event of a real attack and the management decisions made in a crisis situation.

Tests the organisation's physical security.

Checks the process setting within the company.

Course of the RT project / phase



Initial phase and planning

Introductory meeting → Defining the scope and objectives → Exercise rules → Initial planning

Implementing an attack

Information gathering → Defining scenarios → Implementing scenarios ↺ Updating data

Submitting the results

Debriefing with Blue Team → Reporting results and feedback from Blue Team → Presentation for management

🟦 – necessary cooperation 🟥 – without cooperation

Testing is divided into four groups:

Technology

Internal infrastructure, cloud, applications (web, mobile), servers, end devices, etc.

People

Internal and external staff (employees, contractors, suppliers, business partners, etc.).

Processes

Internal processes (existence, formality, integrity and compliance), communication between members of the defence team.

Physical security

Testing the physical security of buildings, warehouses, data centres, manufacturing plants, etc.

I carry out penetration tests, do I need Red Teaming?

Penetration testing and vulnerability scanning are an integral part of security and it is necessary to maintain, adhere to and develop these activities. However, such a methodological approach is not able to test real readiness and thus face cyber threats. Red Teaming, as a simulation of a real attack, really verifies the readiness and ability to react.

Penetration tests

- Short duration (1-3 weeks)
- Administrators and application owners know testing is going on
- Aims to find vulnerabilities in a given application or infrastructure
- Strictly defined, limited range
- Additional protection layers (WAF, IPS, etc.) may be deactivated for testing purposes
- Often carried out in a non-production environment

Red Teaming

- Longer duration (average 1-3 months)
- Carried out covertly, only White Team members know about the activity
- Unlimited testing for all layers of protection as a whole (technology, people, processes, physical security)
- Encroaches on the production environment