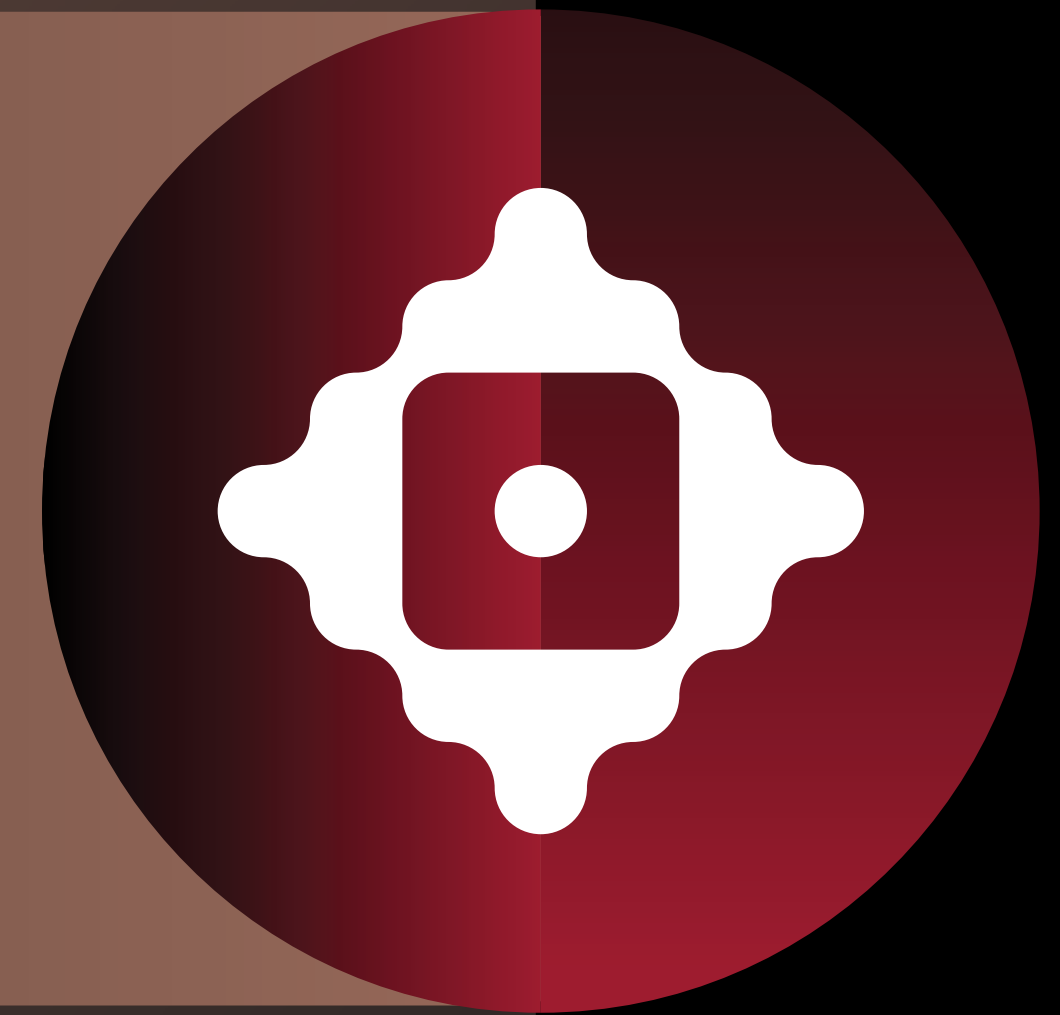
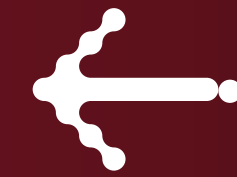


REDTEAM



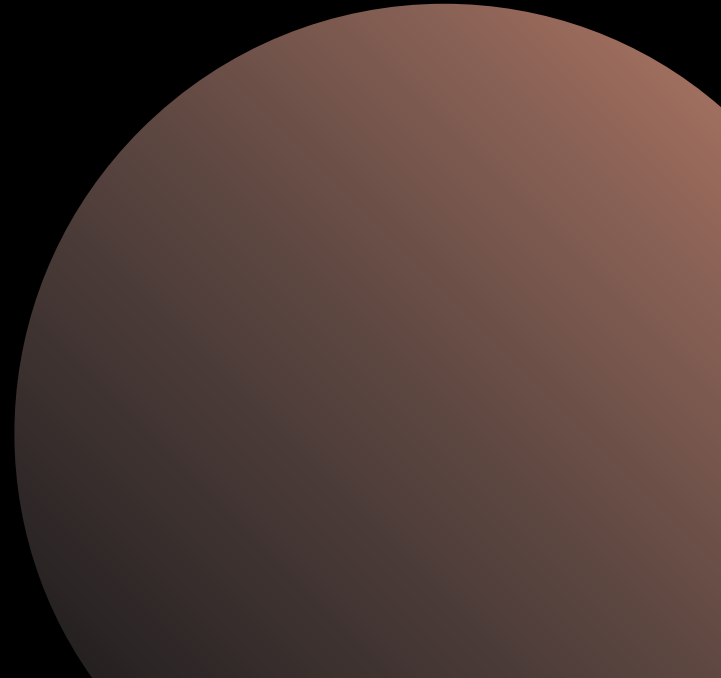
Red Team

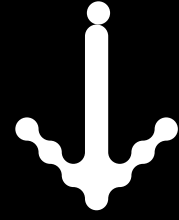
By implementing simulated attacks, the Red Team service helps organizations assess their readiness against advanced attacks, identify points of penetration, and fix them.



However, using up-to-date security tools can prevent some attacks, but having a high-security level requires constant control and monitoring. Each new tool or technology, in addition to the benefits it creates, can be new gateways to penetrate and access the layers of an organization and cause irreparable damage. Using the latest attack methods, penetration, and implementation of advanced persistent threat (APT), attackers first identify vulnerabilities in the infrastructure and then use these vulnerabilities to penetrate the organization and cause irreparable damage, such as data theft or loss of access. Because these vulnerabilities exist at various levels, such as network infrastructure, physical devices, and human resources, identifying and limiting their penetration requires as much knowledge, experience, and expertise as possible. Relying on its knowledge and expertise in cybersecurity and implementing simulated attacks, Spara's Red Team helps organizations assess their readiness against advanced attacks, identify penetration points, fix them, and eventually create a high level of security for your organization.

What are the characteristics of Spara's Red Team?

- Simulation of the most advanced attacks and threats (APT) suited to the infrastructure and characteristics of each organization
 - Development of various attacks based on a comprehensive database of threats (Threat Intelligence)
 - Using the most up-to-date tools and developing dedicated tools if necessary
 - Provide a complete report, including access methods to the attack target
- 



Benefits of working with the Red Team

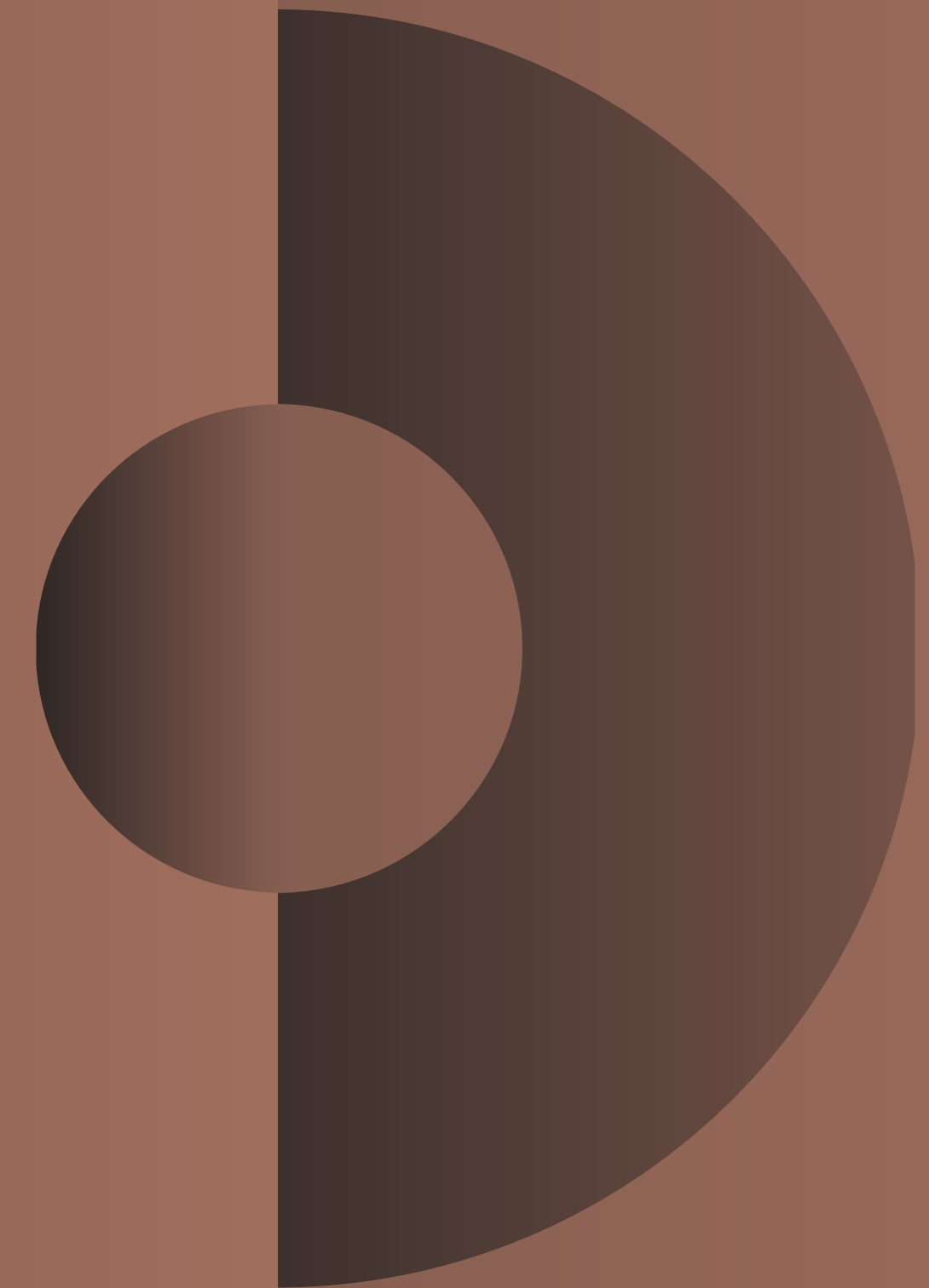
- Performance of attacks in a simulated environment without the damage of actual attacks
- Evaluating the readiness of organizations to deal with attacks and threats at different levels (including equipment, network, and human resources)
- Identification of vulnerabilities in the organization's infrastructure and providing solutions
- Increasing people's awareness of security after identifying and introducing ways of penetration
- Continuous growth and learning of the blue team (security team within the organization)



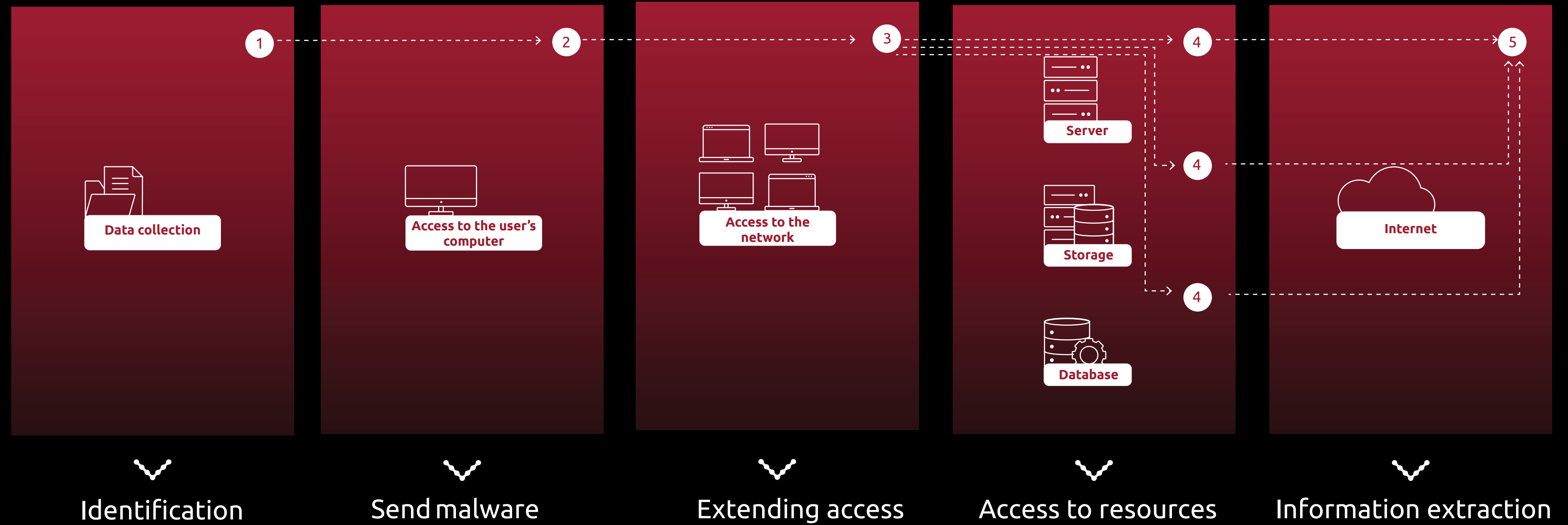
How does the Red Team work?

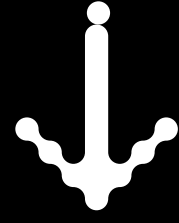
After determining the target of the attack by organization, the red team first collects information about the organization, including its infrastructure and personnel, which will help to establish and expand access in the following stages of the attack. In the next step, attempts are made to gain access to the network through penetration, perform penetration tests, or use people's access using social engineering. Although entering the internal network is an essential part of an attack, given the simultaneous activities of the blue team (the organization's internal security team) to identify and eliminate the attacker, part of the red team's efforts is devoted to maintaining access.

Then, the red team tries to expand its access using different methods and moves toward the plan set by the organization. At the end and after reaching the goal, the team prepares a complete report on the development process of the attack and the successful and unsuccessful methods used and delivers it to the organization. Studying this report, along with the presence of the blue team in all these stages and red team activities at the same time, will increase the possibility of identifying attackers in the network, and the security policies of the organization will be reviewed and amended if necessary.



Executive phases





Red Team Advantages

- Providing comprehensive solutions, including security and EDR, after identifying penetration points
- Development of penetration tools specific to each organization's infrastructure
- A team of security experts with more than eight years of experience in cybersecurity

Difference between Red Team and Penetration Test services

The red team simulates one or more realistic attack scenarios on your organization to measure the effectiveness of your defense solutions (including human resources, equipment, architecture, and various defense processes). But, penetration testing focuses on finding many technical vulnerabilities that exist by default in your IT or cellular infrastructure that may leave your organization vulnerable to a cyberattack. Also, to access a system, the penetration test team requires that you provide them with the information needed to complete the project, such as IP addresses or authentication information. Once a vulnerability is discovered in this process, the attacker of the Pentest team often tries to investigate it more deeply or exploit it to expand access to better understand the potential dangers of this vulnerability. The important thing is that the process of the penetration test is often carried out in an isolated and controlled environment. as a result, due to the high benefits it brings, it is not able to create a comprehensive view of the bigger risks.

But in the red team process, unlike the penetration test, a series of tests are performed on the entire organization's defense system. In other words, the red team comprehensively examines the organization's security processes and looks for weak points. This method has a detailed and deeper view of the defense boundaries, the level of human resources preparation, and which solutions are more effective in dealing with the real cyberattack scenario. This method evaluates an organization's capabilities in detecting and responding to attacks. The red team starts like real-world hackers with no information or knowledge about the organization.

Penetration test skills and tools are also needed to perform red team simulations. Both red team and penetration test are complementary and have a vital role in keeping an organization secure against complex cyber threats.

Red Team is suitable for which businesses?

One way to increase security in the organization is its constant monitoring, which can be improved by implementing a simulated attack. In this regard, using the services of Spara's Red Team can be effective for all companies, public and private departments, and organizations that pursue the following goals:

- Assessing and improving security in all hardware, software, or human resources layers
- Ensuring that previously detected vulnerabilities have been resolved
- Keeping people and infrastructure up-to-date on safety
- Identification of blind spots of network infrastructure





About Spara

Today cyber risks are a critical threat to all organizations worldwide. In the past, organizations tried to provide their cyber security only by using the security equipment and software available in the market. But today, cyberattacks have a very complex structure, so it is no longer possible to deal with them using traditional methods. Therefore, to deal with advanced cyber threats, organizations need to use advanced detection and prevention systems to identify them in the shortest possible time in case of cyber penetration.

In this regard, “Spara” company and a group of the best cyber security experts in the country have produced new products, diverse services, and comprehensive cyber security solutions. “PAM”, “EMS” and “EDR” are the most important products of Spara. Spara’s security services and solutions also include a wide range of security services such as “Security Operations Center”, “Penetration Test”, “Threat Hunting”, “Red Team”, “Governance, Risk Management, and Compliance”, “Incident Response”, “Consulting” and “Training”.



We have been trusted by:



بانک پاساگاد



بانک تجارت



فنا
زیرساخت



فناپ تلکام
FARNAP TELECOM



فناپ تک
FANAP TECH



بانک آینده
AYANDEH BANK



ریاست جمهوری
معاونت علمی و فناوری



ساییا



MIDHCO



پست بانک ایران



هاده اول



شاتل
SHATEL



شرکت سپرده‌گذاری مرکز
اوراق بهادار و تسویه وجوه (سپد)



شوکا



شرکت فناوری اطلاعات فناپ



پایگاه اطلاع رسانی پشتیبانی پاد



شرکت نرم‌افزاری دانش آراین قشم



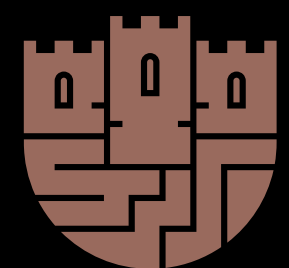
سازمان فناوری اطلاعات ایران



نماوا
NAMAVA



ایرانسل
MTN



سپارا
SPARA



+98(0)21-22275003



info@spara.ir



www.spara.ir