BASE4 SECURITY

We help building a

more secure digital ecosystem!

Red team

DATA SHEET

Digital Footprint

Through OSINT's advanced techniques, we protect your organization against hidden risks on the Internet, carry out research, analysis and identification of possible attack vectors, reducing cyber risks.

Our Digital Footprint service provides a comprehensive and detailed analysis of open source information research to help your organization identify potential risks and opportunities, using advanced techniques and tools. Our specialized OSINT team has extensive experience in researching and analyzing information from various sources, such as websites, forums, social networks, code repositories, Deep and Dark Web. With this information, we can help your organization identify potential attack vectors, detect exposed sensitive information and assess reputational risk, as well as detect malicious activity on the Internet.

With our Digital Footprint ustded service you can improve your organization's cybersecurity and protect your digital ecosystem, while improving your ability to respond to incidents and threats, in order to ensure the protection of your digital assets and minimize cyber risks, please do not hesitate to contact us, we will be happy to help you.

Adversarial Emulation

We perform a comprehensive assessment of your organization's cyber risks using advanced techniques such as Attack Emulation and Open Source Information Research (OSINT). We identify and emulate potential attack vectors, helping your organization to detect and mitigate critical vulnerabilities in your systems.

Our Adversary Emulation is a comprehensive cyber security service that combines advanced attack techniques such as Adversary Simulation and OSINT to assess your organization's cyber risk. We emulate a realistic and in-depth attack against the technological infrastructure, identifying possible attack vectors specific to your organization. In addition, we indicate the Mitre ATT&CK Tactics, Techniques and Procedures (TTPs) that worked and evaded controls during the analysis, providing a detailed understanding of cyber risks and helping to improve incident detection and response in your SOC service. The benefits of our adversary emulation include assessing your organization's cyber risk, identifying your key attack vectors and evaluating your organization's resilience to potential real attacks.

Red Team

Our Red Team service is a specialized cybersecurity service that combines advanced attack techniques such as OSINT, Social Engineering and Adversary Emulation to assess your organization’s preparedness for realistic cyber attacks.

Our Red Team service is a highly specialized cyber security service that focuses on planning and executing strategic infiltration projects into an organization’s infrastructure with the objective of obtaining and extracting valuable information and accessing critical systems. Our security experts use and combine advanced attack techniques and simulations of potential attacker behavior to thoroughly evaluate your organization’s prevention, detection, recovery, response and resilience controls.

The goal is to find potential breaches, security flaws and critical vulnerabilities, and provide you with recommendations to improve your existing security plan. With our Red Team service, your organization can be better prepared to face real incidents and threats in the digital world.

Advanced Penetration Testing

Identify potential weaknesses and vulnerabilities in your Web, API and Mobile systems as well as in your Cyber Infrastructure through exhaustive and in-depth Pntesting techniques and tests in a controlled and secure manner.

Our Pentest projects are composed of advanced attack techniques, 70-80% of which are performed manually, controlled and in depth, the tests are exhaustive, trying to exploit the vulnerabilities identified with the aim of reproducing a real attack scenario carried out by a potential attacker.

We perform advanced Intrusion Tests on all types of systems, networks and platforms:

- Pentest Web
- Pentest API
- Pentest Android / iOs
- Pentest Wireless
- Pentest Cloud / Kubernetes
- Pentest ATM
- Pentest SCADA / OT / ICS

The methodology adopted by BASE4 Security divides the Pentest or Intrusion Test into phases and stages, which follow a standard and industry best practices such as OSSTMM, OWASP, PCI-DSS, NIST SP 800-115, which accompany the needs and expectations of the Client. In turn, the tasks performed and the specific actions taken and exploits pursued are chosen based on the perceived

opportunity and often augmented with additional approaches as the various tests are executed following the aforementioned standards.

This methodological alignment will enable effective administration and assertive management of results, action plans and risk management strategies associated with vulnerabilities that may be discovered in the client's systems, platforms and applications.

Benefits:

Based on the results obtained through Pentest projects, our clients will have a safer and more controlled technological environment against possible cyber attacks, thus avoiding information leakage and the unavailability of their services, while mitigating risks, fraud, economic damage and exposure of the company's brand and image.

Social Engineering

Our Social Engineering service consists of simulating Phishing, Smishing and Vishing attacks to evaluate your organization's preparedness and response to these threats and improve the security awareness of your employees.

BASE4 Security offers annual monitoring to provide indicators on the degree of maturity of the internal user and awareness campaigns and awareness of them through Social Engineering techniques such as:

- Phishing & Spear Phishing
- Smishing
- Vishing
- Tailgating
- Bating
- Dumpster Diving
- Hacking WiFi

We also provide support in the Awareness and Communication strategy through face-to-face and virtual talks and training.

Benefits:

Increase the cybersecurity maturity level of the company's employees to reduce the large-scale attack surface in a short time.

BASE4
SECURITY

www.base4sec.com