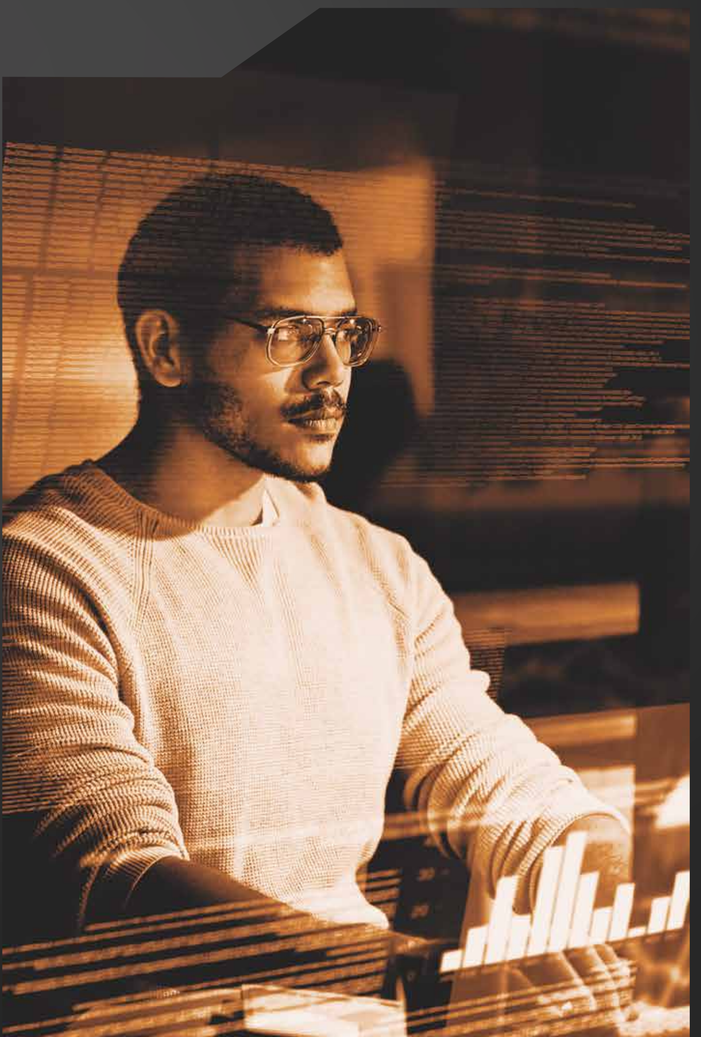
BASE4
SECURITY

Your cyber ally



OFFENSIVE

A secure investment with advanced methodologies and creative approaches

DIFFERENTIALS

OSCP OSCE OSWP

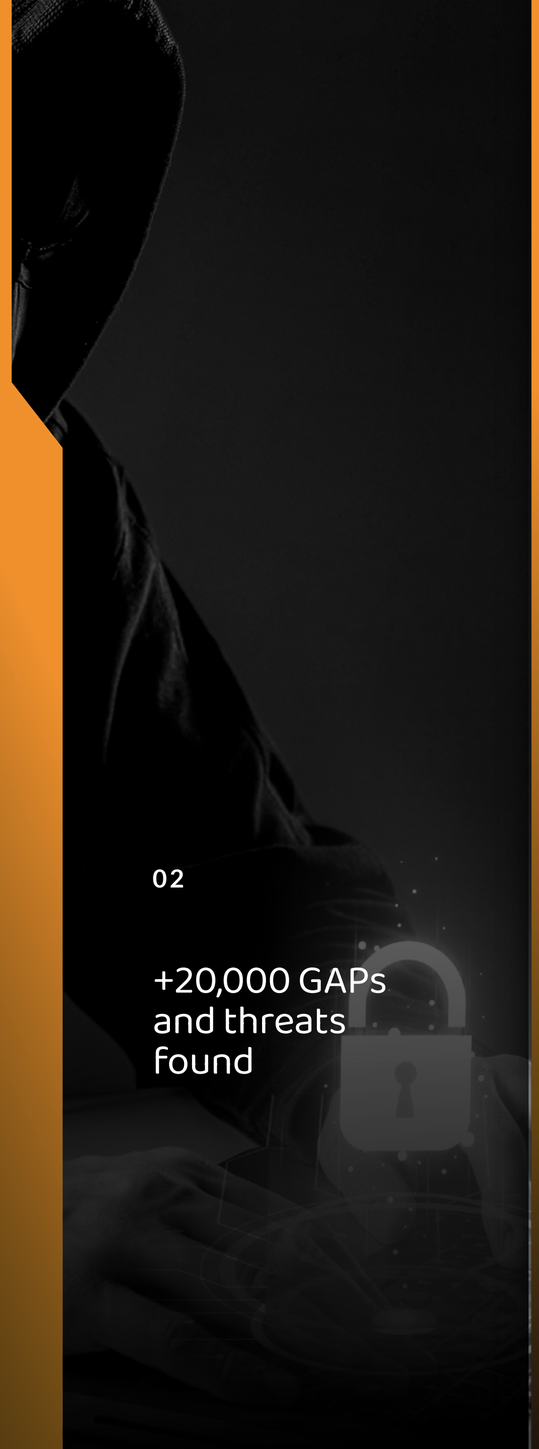
OSWE OSED

eCPPT V2 eWPTX V2 eMAPT

C|EH Certified Ethical Hacker

01

+1,000 projects executed manually



02

+20,000 GAPs and threats found

03

+500 satisfied customers

04

Knowledge of industrial and IoT networks, and frameworks- MITRE/OWASP

Continuous Pentesting

Constant security, continuous adaptation. We implement a dynamic and proactive approach that differs from traditional pentesting. This service performs tests continuously and systematically, adapting quickly to changes in the environment and emerging threats

PROCESS

- Initial evaluation and setup: We define scope and objectives
- Automated and manual pentesting: Continuous testing of applications and systems
- Delivery of periodic reports: Security status, risks and action plans

OUTSTANDING FEATURES

Constant monitoring through advanced technologies and automated techniques

Combined experience: In-depth and strategic analysis performed by security experts

Regular, real-time reports with vulnerabilities detected and mitigation recommendations

Why choose our service?

- Real-time identification and remediation: We detect vulnerabilities before they are exploited by attackers
- Continuous integration in the development cycle: We improve security throughout the development of software and infrastructure
- Compliance with regulations: Adaptation to the most demanding standards and regulations

Contact Us

Purple Team

Defense and attack in perfect synchrony. Purple Team is a collaborative service that simulates cyber-attacks in a controlled environment, combining offensive and defensive techniques to assess your organization's preparedness and response capability in real time

PROCESS

- Exercise planning: We define the scope and objectives of the simulations
- Controlled attacks: Red Team emulates opponents, while Blue Team responds
- Strategic feedback: Results are shared and processes are adjusted collaboratively

OUTSTANDING FEATURES

- Controlled simulations led by our Red Team, imitating real cyber-attacks
- Active response by the Blue Team, identifying and mitigating attacks in real time
- Post-exercise analysis, where findings and lessons learned are shared and improvement strategies are designed

Why choose our service?

- Identification of security breaches: We detect weak points and necessary improvements in your defenses
- Realistic assessment: We simulate real tactics and procedures (TTP) for a practical diagnosis
- Continuous improvement and mutual learning: We foster a proactive safety culture with every exercise

Contact Us

Adversarial Emulation

Confront threats like a real attacker would. Our Adversarial Emulation service allows you to evaluate your organization's ability to withstand specific and known cyber-attacks. Through controlled offensive operations, we simulate the techniques, tactics and procedures (TTP) used by real threat actors, helping to strengthen your security posture and anticipate potential risks.

PROCESO

- Assessment of the environment: Identification of the most likely and relevant adversaries
- Attack simulation: Reproduction of TTPs used by real actors to test defense
- Report and recommendations: Report with vulnerabilities detected and suggested improvements.

OUTSTANDING FEATURES

Analysis based on the most relevant threat actors for your sector

Detailed report with specific findings and recommendations

Safe and controlled offensive operations, minimizing the impact on production.

Why choose our service?

- Preventive detection: We identify and correct vulnerabilities before they are exploited
- Realistic simulation: We recreate the most likely attacks for your organization based on industry-specific threats
- Proactive fortification: We offer actionable recommendations to improve defense against potential adversaries

Contact Us

Digital Footprint

Map and Protect your Digital Footprint. Our Digital Footprint service offers a comprehensive view of your organization's digital presence through advanced OSINT (Open Source Intelligence) techniques. This offensive security solution allows you to identify hidden risks and possible attack vectors, assessing both the exposure of sensitive information and the reputational impact

PROCESS

- Collection and analysis: Exploration in public web, Deep and Dark Web, and other relevant sources
- Risk identification: Detection of attack vectors and leaked information
- Report of results: Delivery of a report with risks found and mitigation measures

OUTSTANDING FEATURES

- Advanced research conducted by experienced OSINT experts
- Early detection of exposed information to prevent attacks
- Detailed reports with key findings and actionable recommendations

Why choose our service?

- Exhaustive analysis of open sources (web, forums, social networks, repositories, Deep and Dark Web)
- Identification of attack vectors and exposed sensitive data
- Reputational risk assessment and detection of opportunities to mitigate threats

Contact Us

Malware Emulation

Advanced threat simulation. Malware Emulation is a specialized service that allows you to assess your systems' ability to withstand advanced malware attacks, such as ransomware and spyware, in a controlled and secure environment

PROCESS

- Custom malware design: Tailored to the threats most relevant to your organization
- Simulations in secure environments: We evaluate how your systems respond to real attacks
- Results report: Includes detailed analysis and recommendations to strengthen your security.

OUTSTANDING FEATURES

Controlled malware simulation: We emulate real attacks to evaluate protection levels

Detailed analysis of the effectiveness of the implemented security controls

Comprehensive technical report, including results, techniques used and suggestions for improvement

Why choose our service?

- Identification of critical vulnerabilities: We discover weak points that could be exploited by real malware
- Exhaustive evaluation of defenses: We test the effectiveness of solutions such as antivirus, firewalls, EDRs and intrusion detection systems
- Continuous safety improvement: We offer customized recommendations to optimize controls and processes

Contact Us

Manual Application Pentesting

Securing your critical applications. We thoroughly evaluate the security of your web, mobile and APIs applications, using advanced penetration testing techniques. We simulate real attacks in controlled environments to detect vulnerabilities and critical errors that could compromise your business

PROCESS

- Planning and scope definition: Identification of critical applications
- Test execution: Simulation of controlled cyber-attacks
- Report and recommendations: Risk analysis and detailed mitigation plan

OUTSTANDING FEATURES

- Complete coverage: Manual evaluations of web, APIs and mobile applications
- Simulation of controlled attacks to understand real threat behavior
- Report with a prioritized mitigation roadmap, facilitating strategic decisions

Why choose our service?

- Discovery of hidden vulnerabilities: We detect flaws that could go undetected in traditional assessments
- Detailed and prioritized analysis: We deliver reports with critical findings and practical recommendations
- Comprehensive protection: We test from code and configurations to security practices to secure every layer of your application

Contact Us

Red Team Exercise

Test your resilience with realistic simulations. Our Red Team Exercise service focuses on strategic infiltration of your organization's infrastructure to simulate advanced attacks. Through a combination of attack techniques, social engineering and adversary emulation, we evaluate the ability of your systems to withstand real cyber-attacks

PROCESS

- Planning: Definition of scenarios and strategic objectives
- Attack execution: Controlled infiltration of critical systems and assets
- Results report: Vulnerability analysis and clear recommendations for mitigation

OUTSTANDING FEATURES

- Realistic simulations aligned with real adversary tactics
- Exhaustive analysis of technical and operational controls
- Detailed report with critical findings and a prioritized improvement roadmap

Why choose our service?

- Identification of critical gaps: We discover vulnerabilities and flaws that could be exploited
- Actionable recommendations: We provide prioritized suggestions to strengthen your security plan
- Comprehensive controls testing: We evaluate your organization's prevention, detection, recovery and response

Contact Us

Social Engineering

Strengthening your first line of defense. We assess your organization's preparedness for Phishing, Smishing and Vishing attacks through controlled simulation of these scenarios. Our goal is to identify human vulnerabilities and improve staff cybersecurity awareness through realistic tests that reflect current tactics used by cybercriminals.

PROCESS

- Scenario design: Creation of simulated attacks aligned with current threats
- Execution of the attack: Launching of controlled campaigns to evaluate the response
- Report and training: Personalized recommendations and, optionally, talks to close the detected gaps.

OUTSTANDING FEATURES

- Analysis of personnel behavior with maturity indicators
- Detailed reports with strengths, weaknesses and specific recommendations
- Realistic simulations of Phishing, Smishing and Vishing

Why choose our service?

- Detection of cultural vulnerabilities: We identify areas for improvement in the response of employees
- Customized scenarios: We adapt the simulated attacks according to the most relevant threats for your sector
- Active awareness: Optional accompaniment in the training strategy through virtual and face-to-face talks

Contact Us

Pentest Cloud | IT OT Infrastructure

Evaluación integral de vulnerabilidades. Identifica y evalúa vulnerabilidades en la infraestructura tecnológica de tu organización, cubriendo entornos de información tecnológica (IT), tecnología operativa (OT) y nube, con un enfoque proactivo y exhaustivo

PROCESO

- Simulación de ataques reales: Emulación de tácticas que los atacantes emplearían en entornos IT, OT y Cloud
- Análisis de infraestructura crítica: Evaluamos componentes clave, como servidores, redes y aplicaciones
- Informe exhaustivo y priorizado: Detalle de hallazgos y recomendaciones de mitigación

CARACTERÍSTICAS DESTACADAS

- Recopilación de datos y planificación: Identificamos el alcance y definimos los objetivos de la prueba
- Pruebas de penetración avanzada: Simulamos ataques reales en los diferentes componentes
- Análisis de riesgos: Evaluamos el impacto y la probabilidad de cada vulnerabilidad encontrada
- Informe y recomendaciones: Generamos un análisis detallado con pasos prioritarios para mejorar la seguridad.

Why choose our service?

- Descubrimiento de fallos de seguridad: Identificamos y evaluamos configuraciones incorrectas y vulnerabilidades explotables
- Visión integral de la postura de seguridad: Proporcionamos una evaluación completa de la infraestructura
- Prevención proactiva de amenazas: Ayudamos a mitigar riesgos antes de que se conviertan en incidentes

Contact Us

Why choose BASE4 Security?

- **Service guarantee**
  We provide a measure of security and confidence in the quality of our cybersecurity services.

- **Backed by globally renowned talent**
  Our certified and award-winning company culture is chosen by people of high caliber and technical recognition.

- **Consultative service**
  We offer customized solutions to address specific cybersecurity challenges or needs.

BASE4
SECURITY

www.base4sec.com