HAWKTESTERS

Everyone should ***feel secure*** online.

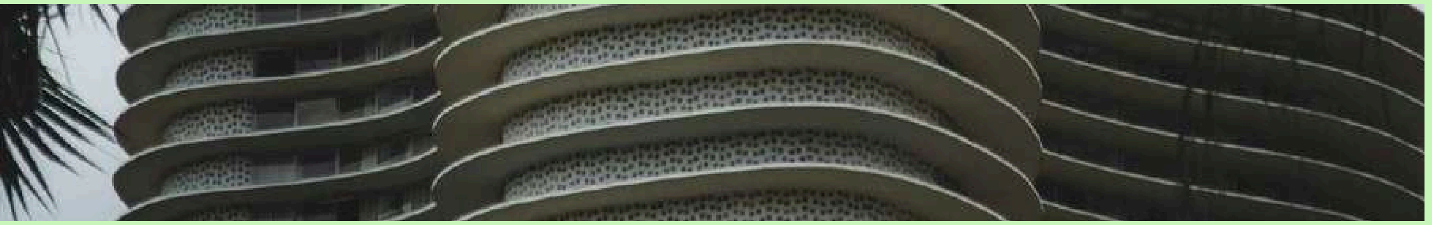
We emulate threat *adversaries.*

By conducting simulations of real attacks, organizations have the opportunity to discover and address vulnerabilities in their systems before cybercriminals act.

This preventive strategy is not only crucial for safeguarding confidential information and intellectual assets, but also constitutes an essential defense against financial risks and the deterioration of the corporate image.

Penetration testing is vital for complying with regulatory and compliance standards, as it provides concrete evidence of an organization's commitment to security.

By regularly performing these tests, organizations can continuously assess their security posture, refine their defense strategies, and maintain a resilient stance against constantly evolving cyber threats.



Our **Focus.**

HAWKTESTERS is a company specialized in cybersecurity, business networks, and IT risk management, with extensive expertise in penetration testing for businesses of all sizes.

Our tests can cover every aspect of your network and systems, including security and assurance testing for customized applications. We identify and report vulnerabilities and risks in a clear and prioritized format, with recommendations.

HAWKTESTERS' penetration testing approach is closely aligned with the guidelines of the Open Web Application Security Project (OWASP). To provide a consistent, repeatable, and high-quality outcome, we use a series of methodologies depending on the organization and objectives. These include well-defined standards such as:

OWASP Top 10 (Web, Mobile, y API)

OSSTMM

NIST

MITRE ATT&CK

Key *Benefits.*

1.

Validate your cybersecurity across your entire attack surface and align vulnerability management with key business objectives.

2.

Prioritized and actionable reports to guide vulnerability remediation and risk management.

3.

Gain an understanding of the strengths and weaknesses in your systems management to guide the continuous improvement of your security processes.

4.

Revalidating tests ensures that remediations are applied and security gaps are closed.

5.

Comply with regulations, including data privacy and security, to build customer trust and protect your organization from penalties.

1. Web Applications Audit.

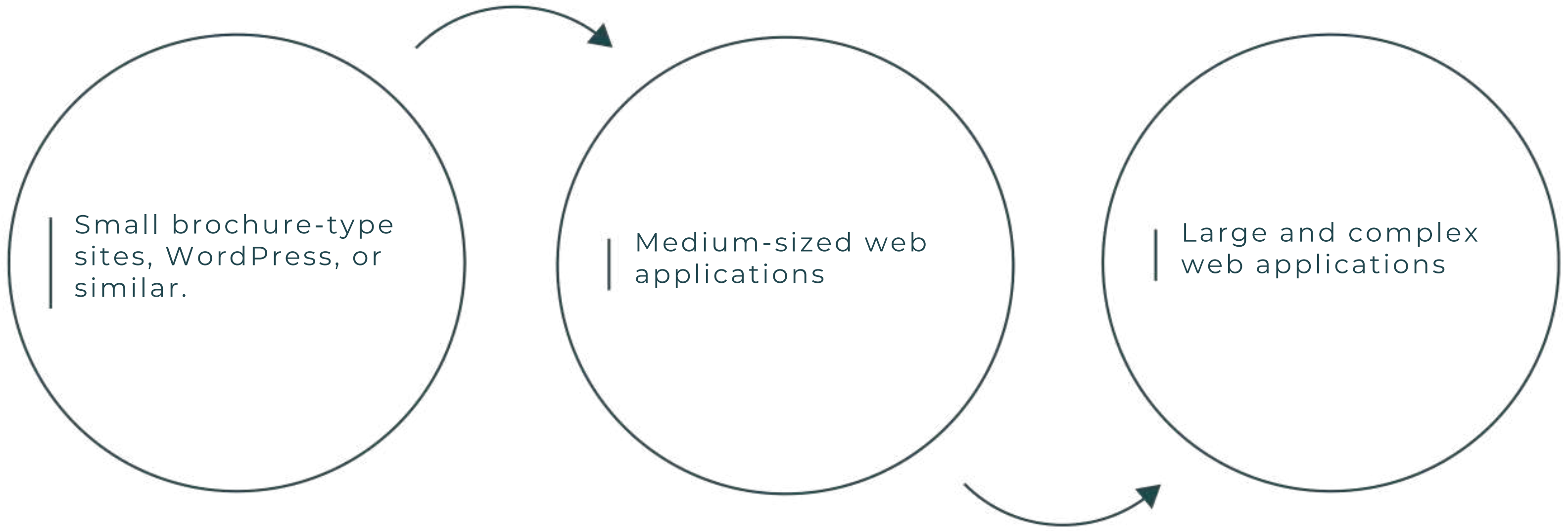
Web testing is based on the industry methodologies of the Open Web Application Security Project (OWASP) as well as the Common Weakness Enumeration (CWE) Top 25.

The results of application testing are valuable indicators of the skills and gaps in internal application development, providing opportunities for training and improving tools to address future issues.

With each test using the same workflow and practices, including an extensive quality control process conducted by a senior tester, you can be confident in obtaining thorough and consistent results.

Inclusions

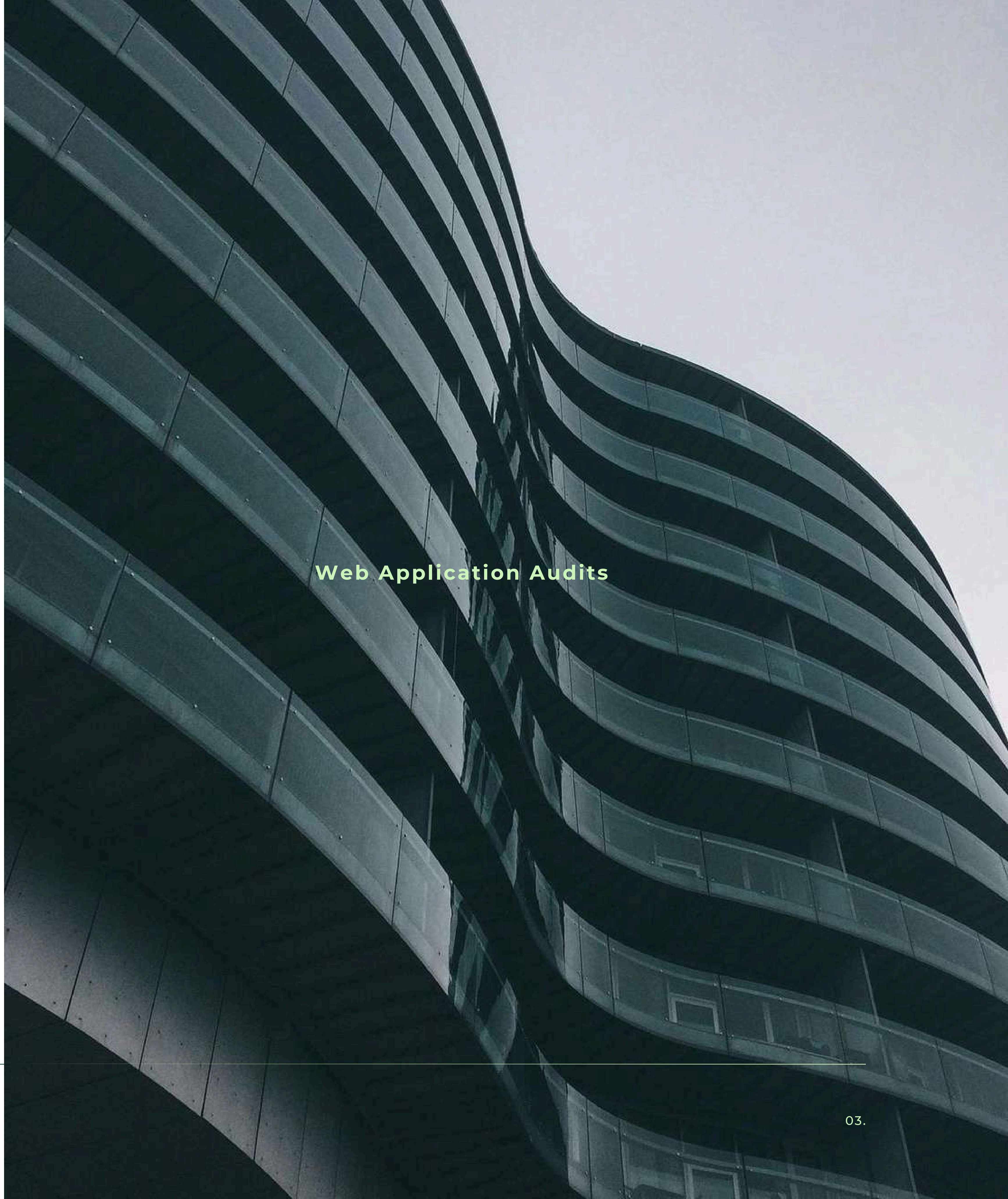
Hawktesters can test all your web applications, whether they are:



Small brochure-type sites, WordPress, or similar.

Medium-sized web applications

Large and complex web applications



Web Application Audits

2. ***Wireless Security*** *Assessment*

Wireless networks can provide an attack surface that extends far beyond the physical boundaries of an organization's premises. This makes them an attractive target for a determined attacker.

Inclusions

Wireless security audits focus on the following components:

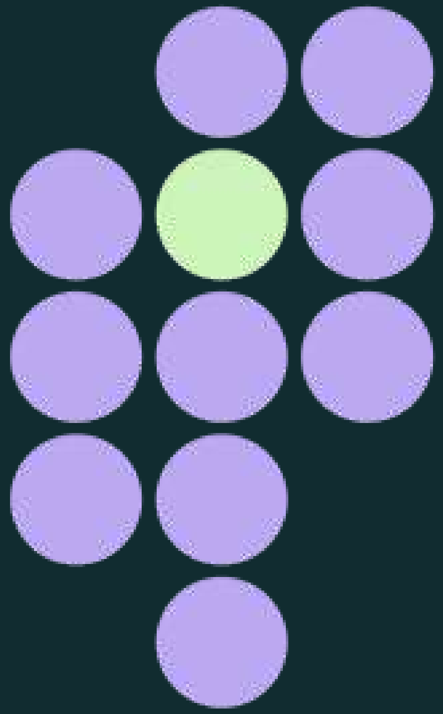
Wireless Environment: *Scanning and discovery.*

Wireless Infrastructure: *Device configuration review.*

Wireless Infrastructure: *Evaluation of implementation and operations.*

Validation of Network Segregation: Ensuring separation between wireless networks, such as guest and corporate networks.

After completing the initial review and addressing any issues, this will establish a security baseline.

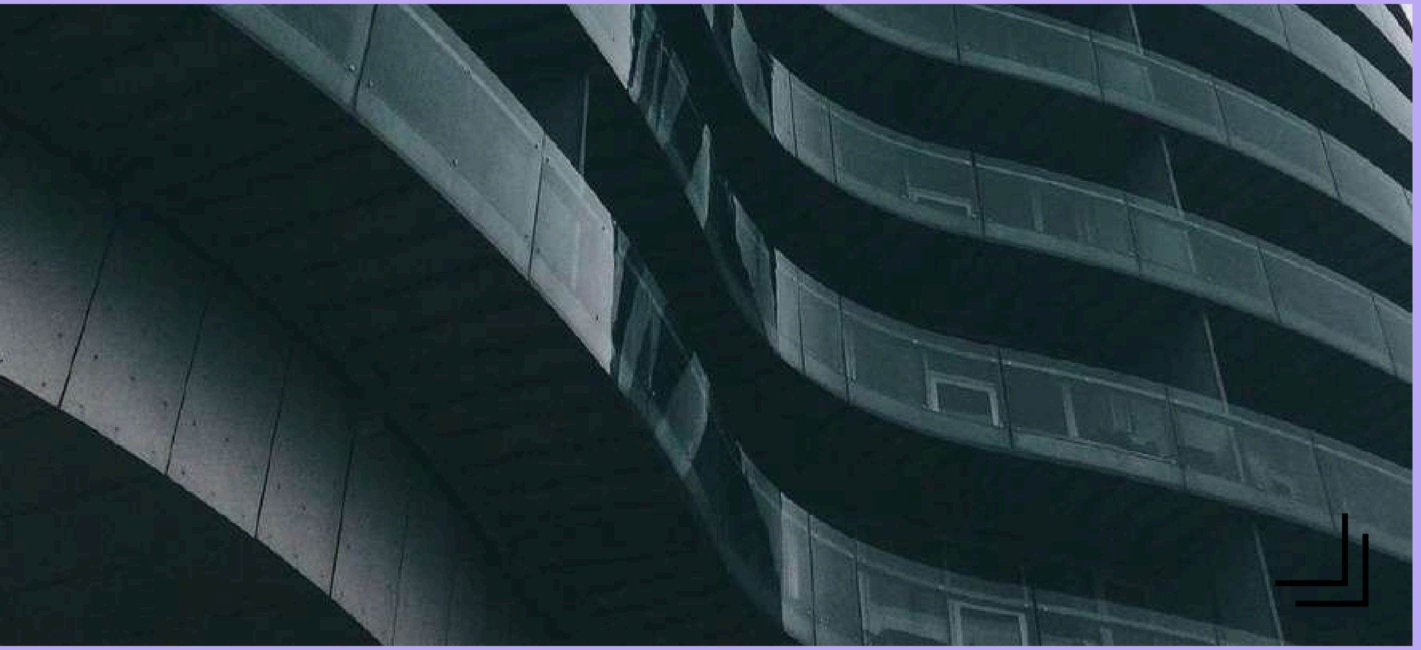


3. API Security *Audit*

Our approach is based on the industry guidelines of the Open Web Application Security Project (OWASP) for API testing.

Inclusions

Tests can be performed independently (using a Postman or Open API specification) or as part of a broader test that includes the web application or another API client. All tests are conducted according to industry best practices, and findings are mapped to the latest OWASP API Top 10.



4. Host Configuration *Audit*

Host configuration assessment considers the configuration of specific server devices (and supporting applications) or other devices.

Inclusions

The focus areas and review during this activity may include:

- **Operating system updates and patches (or equivalent)**
- **File system permissions**
- **Default configurations**
- **Minimized attack surface (no unnecessary services running)**
- **Misconfigurations and known vulnerabilities with installed services**
- **Comparison against a provided baseline/documented configurations**
- **Access to sensitive data, such as configuration files containing credentials**

5. **Mobile Security** *Assessment*

Inclusions

Since many applications are currently delivered through mobile devices, we meet your security testing requirements, whether they are native, web, or hybrid.

All tests are conducted according to industry best practices, and findings are mapped to the latest OWASP Mobile Top 10.

6. *Internal Penetration Test*

Inclusions

This is typically carried out under one of the following three approaches:

- **Living off the Land (LoL)**: The tester is provided access to the internal network and then uses standard tools and techniques to access systems, exploring identified vulnerabilities and opportunities for lateral movement.
- T**arget-Based Testing**: The tester is provided with a standard user account within the network and aims to gain access to an agreed-upon target (such as Active Directory, Financial Data, or Customer Data).
- **Vulnerability Assessment**: All targets within scope are scanned using industry-leading tools, and all findings are manually reviewed and categorized to help assess overall risk.

7. External Penetration Test

External Network Penetration Testing evaluates the overall security posture of infrastructure exposed to the Internet.

Inclusions

This is carried out in two broad categories:

- Automated Scanning: Scans all exposed services for misconfigurations or known vulnerabilities.
- Manual Testing: Applies manual testing techniques and expertise to review exposed hosts and services. Identified assets are analyzed using a variety of tools to identify open ports, services, and vulnerabilities.

Focus Areas and Review include:

- Incorrect infrastructure configurations
- Known vulnerabilities related to exposed services
- SSL certificate configurations
- Analysis of results from network security assessment tools such as Nessus and Nmap
- Manual analysis of reported vulnerabilities to assess exploitability and criticality

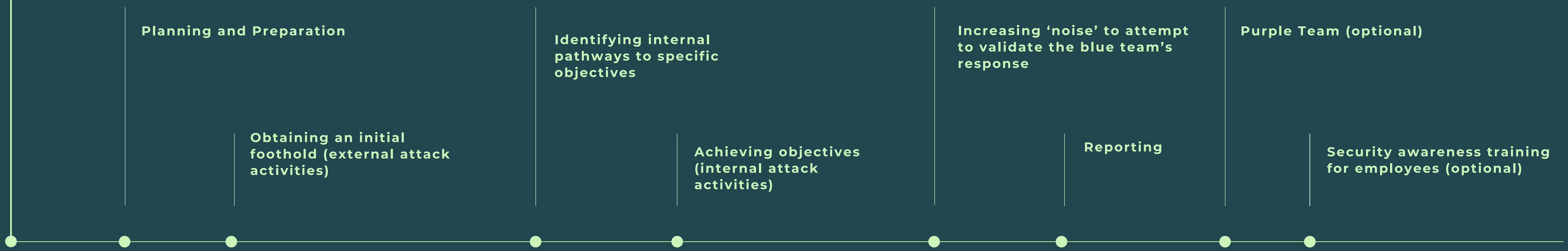
8. *Adversary Simulation -* Red Team

Planning, coordination, execution, evaluation, analysis, and reporting of simulated real-world attacks using red team techniques, TTPs, and the TIBER-EU methodology.
We employ attack and penetration tools to covertly assess the organization’s technological controls and processes against threats such as phishing, malware, and attacks on applications or infrastructure, ensuring a comprehensive evaluation aligned with European cybersecurity standards.

Inclusions

By conducting a red team exercise, we simulate a real attack targeting critical objectives for your current and future operations. This process allows you to assess your organization’s preparedness against advanced threats, improve your security posture, and provide recommendations and learning opportunities to optimize your security incident response.

This engagement is expected to follow a phased approach:



Planning and Preparation

Obtaining an initial foothold (external attack activities)

Identifying internal pathways to specific objectives

Achieving objectives (internal attack activities)

Increasing ‘noise’ to attempt to validate the blue team’s response

Reporting

Purple Team (optional)

Security awareness training for employees (optional)

9. Source Code Review

Hawktesters can perform security-focused reviews of applications developed using a wide variety of languages and platforms, applying the OWASP ASVS and NIST-SSIF methodologies.

Inclusions

- ↘ High-Level Manual Review: Searching the code for common security issues and weaknesses.
- ↘ Code Scanning Evaluations: Using SAST or DAST tools to assess the code.
- ↘ Identification of Security Weaknesses and Vulnerabilities: Detecting issues at the source code level and demonstrating how they result in security defects.
- ↘ Additional Code Review: For applications running on legacy codebases and frameworks to identify new and emerging classes of coding vulnerabilities.

10. Cloud Services Security Review

Cloud-Based Service Security Assessment (SaaS/PaaS/IaaS) for AWS, Azure, and O365 Based on Configuration and Deployment Review

Inclusions

- ↘ Review Configurations and Options: Assess configurations and settings against the provider's and industry best practices.
- ↘ Examine User and Group Management: Evaluate the practices and effectiveness of user and group administration.
- ↘ Analyze Data Protection Measures: Inspect the measures in place to protect data.
- ↘ Evaluate Service Policies: Review the policies governing the services.
- ↘ Documentation and Reporting: Provide detailed reports of the findings with actionable recommendations.

11. Phishing Campaigns

We offer a comprehensive phishing campaign service designed to assess and enhance the security awareness of employees within your organization.

The goal of these campaigns is to provide a realistic measurement of the security awareness level among employees, identify areas for improvement, and strengthen the organization's defenses against deceptive tactics.

Inclusions

Phishing: We conduct simulated email campaigns to measure employees' responses to phishing attempts, providing a clear insight into the organization's vulnerability to this type of attack.

Vishing: We implement phone-based social engineering tests to evaluate how employees respond to verbal requests for sensitive information or actions that could compromise security.

Smishing: We send text messages that mimic tactics used by cybercriminals to determine employees' susceptibility to SMS phishing attacks.

12. Secure Development Trainings

Hawktesters can perform security-focused reviews of applications developed using a wide variety of languages and platforms.

Inclusions

Secure Development Training According to ASVS

We adopt the OWASP ASVS standard to provide a solid foundation in security practices during application development, ensuring that teams understand and can implement the necessary security requirements.

Interactive and Hands-On Sessions

The training sessions are designed to be dynamic, with practical exercises and real case analyses that allow the application of knowledge in concrete scenarios.

Updated and Relevant Content

We ensure that the training content reflects the latest trends and threats in the field of cybersecurity, preparing teams to face current challenges.

Learning Assessment and Continuous Improvement

We measure the progress and understanding of the topics covered, providing detailed feedback and suggestions to strengthen skills and knowledge.

13. Hardware Hacking

Physical devices, such as routers, IoT devices, SCADAs, and PLCs, are often overlooked but are as vulnerable as any other asset.

Inclusions

This is carried out in three broad categories:

- **Physical Assessment:** We evaluate your hardware's resilience against physical attacks using techniques such as side-channel attacks, reverse engineering, and tampering tests.
- **Communication Interface Assessment:** We analyze wireless and wired communication channels to detect vulnerabilities, evaluating protocols, identifying attack vectors, and proposing solutions.
- **Firmware and Software Assessment:** We perform static and dynamic analysis, search for vulnerabilities, conduct reverse engineering, and evaluate the overall security of your system.

The focus areas and review include:

- Detect information leaks through power variations and electromagnetic emissions.
- Assess the hardware's ability to resist physical openings and alterations.
- Inspect the security of Bluetooth, Wi-Fi, Ethernet, and other protocols.
- Decompile and analyze firmware to identify backdoors and assess its integrity.
- Detect and mitigate risks of unauthorized execution and exploitation of vulnerabilities.

Reports and Analysis ↘

Our standard report includes an **executive and technical** summary of the findings, along with:

- ↘ A detailed description of each result
- ↘ Associated risk classifications
- ↘ Recommendations to resolve the vulnerability.

Additionally, we organize a virtual session to share and discuss the findings with the company's technical team, thereby fostering a collaborative approach to risk mitigation.

Our Penetration Testing Credentials ↘

Hawktesters stands out for its high specialization and its **25 years of accumulated experience** in penetration testing and Ethical Hacking.

Our team holds a wide range of industry-recognized certifications, including **OSCE, OSWE, OSCP, OSEP, OSWA, eWPTXv2, PNPT**, and more.

Everyone should ***feel secure*** online.