SENCODE

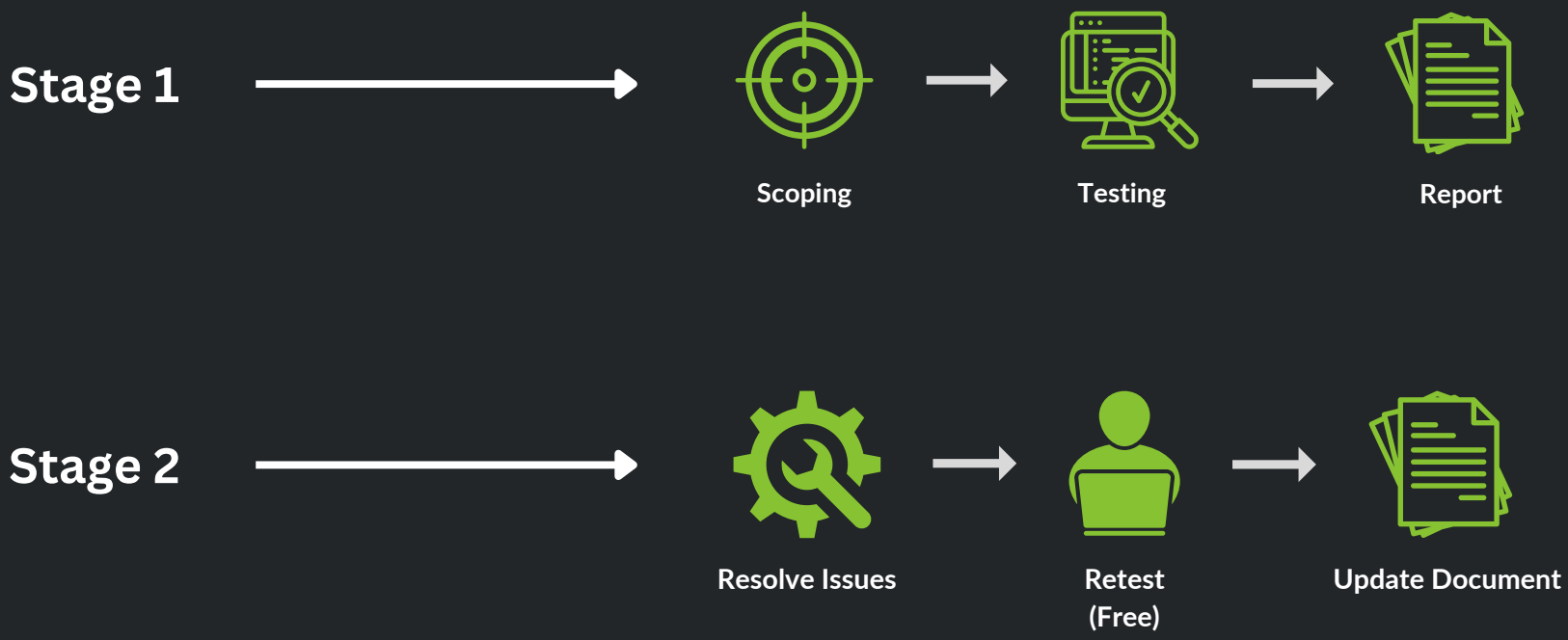
Service Definition Document

Email: office@sencode.co.uk

Tel: 01642716680

2024/2025

Penetration Testing
Process



Web Application
Penetration Testing Service

Our Web Application Penetration Testing service is designed to identify and address security vulnerabilities in your web applications. We simulate real-world attacks to identify weak points, providing you with a comprehensive report and actionable recommendations.

By adhering to the Open Web Application Security Project (OWASP) Testing Guide, a globally recognised framework, we ensure a thorough and effective approach to securing your digital assets.

References:

- https://owasp.org/www-project-web-security-testing-guide/
- https://sencode.co.uk/penetration-testing/web-application-penetration-testing/
- https://sencode.co.uk/web-penetration-testing-planning-guide/

Methodology Overview

- Pre-engagement Interactions
- Information Gathering
- Config and Deployment
- Identity Management
- Authentication
- Authorisation
- Session Management
- Input Validation
- Error Handling and Logging
- Business Logic
- Client-Side
- Reporting - Drafting and Review
- Reporting - Finalisation

Network Infrastructure (External, Internal)
Penetration Testing Service

Our Network Penetration Testing service identifies vulnerabilities in your network infrastructure that could be exploited by cybercriminals. Using advanced techniques, we simulate cyber-attacks to assess your network's resilience, providing you with a roadmap for remediation.

Our testing team adheres to the PTES methodology. The Penetration Testing Execution Standard (PTES) provides a comprehensive methodology for conducting infrastructure penetration testing. The PTES framework breaks down the process into several distinct phases.

References:

- http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- https://sencode.co.uk/penetration-testing/network-penetration-testing/

Methodology Overview

- Pre-engagement Interactions
- Intelligence Gathering - Passive
- Intelligence Gathering - Active
- Threat Modeling
- Vulnerability Analysis - Automated
- Vulnerability Analysis - Manual
- Exploitation
- Post-Exploitation and Analysis
- Reporting - Drafting and Review
- Reporting - Finalisation

Application Programming Interface (API)
Penetration Testing Service

Our API Penetration Testing service is aimed at uncovering and mitigating security vulnerabilities in your APIs. Leveraging industry-standard methodologies (With guidance from OWASP), our approach ensures a comprehensive assessment of your API security posture. This service is essential for protecting the integrity of your APIs and the data they handle, thereby safeguarding your digital infrastructure.

References:

- https://owasp.org/www-project-api-security/
- https://sencode.co.uk/penetration-testing/api-penetration-testing/

Methodology Overview

- Pre-engagement Interactions
- Information Gathering
- Config and Deployment
- Authentication & Authorisation
- Parameter and Input Validation
- Business Logic
- Data Validation
- Session Management
- Rate Limiting
- Error Handling
- Dependency Testing
- Reporting - Drafting and Review
- Reporting - Finalisation

Mobile Application (IOS, Android)
Penetration Testing Service

Our Mobile Application Penetration Testing service is expertly designed to identify and mitigate security vulnerabilities in mobile applications.

Utilising the OWASP Mobile Application Security Verification Standard (MASVS), a globally recognised framework, we provide a comprehensive and effective approach for securing your mobile apps against a range of digital threats.

References:

- https://owasp.org/www-project-mobile-app-security/
- https://sencode.co.uk/penetration-testing/mobile-application-penetration-testing/

Methodology Overview

- Pre-engagement Interactions
- Architecture and Data Security
- Authentication and Session Management
- Network Communication Security
- Platform Interaction Assessment
- Cryptography
- Data Validation
- Build Configuration
- Reverse Engineering
- Client-Side Injection
- Reporting - Drafting and Review
- Reporting - Finalisation

Social Engineering
Penetration Testing Service

Even the most secure systems can be compromised through human error. Our Social Engineering Penetration Testing service evaluates your organisation's susceptibility to social engineering tactics like phishing, pretexting, and tailgating.

We test your employees' awareness and response to simulated attacks, helping you to fortify your human firewall and reduce insider risks.

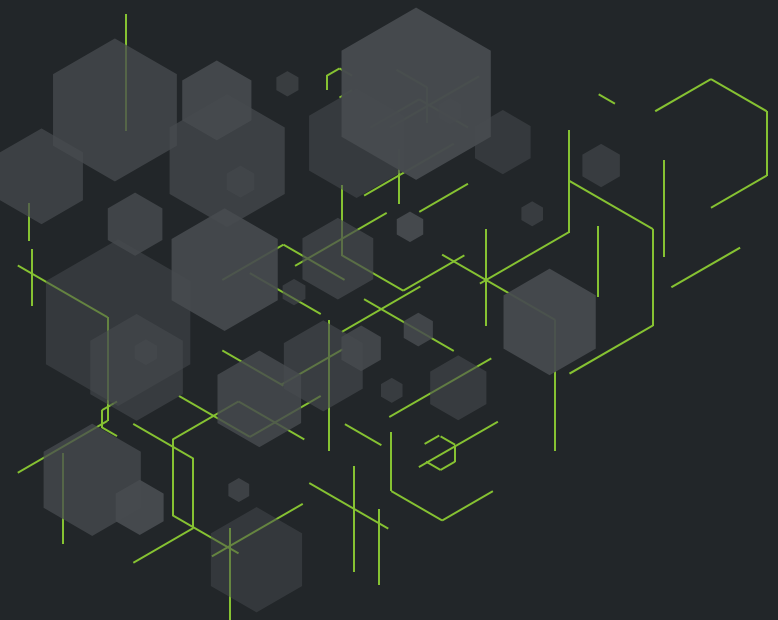
References:

- https://sencode.co.uk/penetration-testing/social-engineering-penetration-testing/
- https://sencode.co.uk/what-is-a-social-engineering-attack/

Methodology Overview

- Pre-engagement Interactions
- Reconnaissance
- Information Gathering
- Target Selection
- Pretexting and Planning
- Attack Execution
- Exploitation and Access
- Reporting - Drafting and Review
- Reporting - Finalisation

Security Assessments



2024/2025

AWS
Security Review

Is your AWS environment as secure as it could be? Our AWS Security Review service provides a comprehensive audit of your AWS configurations, from S3 buckets to EC2 instances.

Receive actionable recommendations to fortify your cloud infrastructure and ensure you're in compliance with best practices and industry regulations. Secure your AWS assets and maintain peace of mind with our expert review.

AZURE
Security Review

Cloud environments are not immune to security risks. Our Azure Security Review service provides a thorough examination of your Azure configurations and implementations.

We identify misconfigurations, insecure data storage, and other vulnerabilities that could jeopardise your cloud assets. Secure your Azure environment with our expert guidance and ensure compliance with industry standards.

Red Team Assessment

Looking for a comprehensive evaluation of your organisation's security posture? Our Red Team Assessment simulates a full-scale, real-world attack on your systems to test your defenses across multiple vectors.

This multi-layered approach provides a holistic view of your security landscape, allowing you to understand your weaknesses and improve your resilience against sophisticated attacks.

Stolen Device Assessment

Lost or stolen devices pose a significant risk to your organisation's data. Our Stolen Device Assessment service evaluates the potential impact and risks associated with a compromised device.

We provide you with a detailed analysis of data exposure and offer recommendations for immediate action and future prevention. Mitigate the risks associated with device loss and protect your sensitive data with our specialised assessment.