BLACKBOX PENTESTERS

Services

BLACKBOX
PENTESTERS

AI Penetration Testing

We assess the security of your AI systems to ensure they cannot be manipulated, misused, or exploited.

This includes testing how AI models respond to malicious inputs, whether sensitive data can be extracted, and if outputs can be influenced in unintended ways.

In simple terms:
We test whether your AI can be tricked into doing something it shouldn’t.

BLACKBOX
PENTESTERS

Adversary Simulation & Red Teaming

We simulate real-world cyber attacks to test how well your organisation can detect and respond.

This combines technical attacks, social engineering, and physical access attempts to replicate how a determined attacker would operate.

In simple terms:
We act like a real attacker to see how far we can get and how well you can stop us.

BLACKBOX
PENTESTERS

Free Vulnerability Assessments

We identify security weaknesses across your systems and provide clear, actionable advice to fix them.

Unlike automated scans, we manually validate findings to ensure accuracy and remove false positives.

In simple terms:
We find the real security gaps in your environment and show you how to fix them.

BLACKBOX
PENTESTERS

Social Engineering Assessments

We test how vulnerable your organisation is to manipulation tactics such as phishing, impersonation, and pretexting.

This helps assess how attackers might exploit human behaviour rather than technical weaknesses.

In simple terms:
We test whether someone could trick your staff into giving access or sensitive information.

BLACKBOX
PENTESTERS

Network Infrastructure Penetration Testing

We assess your internal and external networks to identify weaknesses that could allow unauthorised access.

This includes servers, devices, firewalls, and network configurations.

In simple terms:
We test whether someone could break into your network and move around inside it.

BLACKBOX
PENTESTERS

Web & API Application Penetration Testing

We test your websites and APIs for vulnerabilities that could expose data or allow unauthorised actions.

This includes authentication, data handling, and business logic flaws.

In simple terms:
We test whether your applications can be exploited to access or manipulate data.

BLACKBOX
PENTESTERS

Physical Intrusion Penetration Testing

We assess how easily an attacker could physically access your buildings and sensitive areas.

This includes entry points, staff behaviour, and internal movement.

In simple terms:
We test whether someone could walk into your building and access restricted areas.

BLACKBOX
PENTESTERS

Cyber Essentials Certification Support

We guide your organisation through the Cyber Essentials certification process.

This includes identifying gaps, providing remediation advice, and preparing you for assessment.

In simple terms:
We help you meet the requirements to achieve Cyber Essentials certification.

BLACKBOX
PENTESTERS

Configuration Review & Security Posture Assessment

We review how your systems and technologies are configured to identify weaknesses and misconfigurations.

This ensures your environment is aligned with security best practices.

In simple terms:
We check whether your systems are set up securely, not just whether they exist.

BLACKBOX
PENTESTERS

Rogue Device & Covert Camera Sweep

We search for unauthorised devices such as hidden cameras, listening devices, or rogue network equipment.

This helps protect sensitive environments from surveillance and data leakage.

In simple terms:
We check whether anything has been secretly installed to spy on you.

BLACKBOX
PENTESTERS

Cyber Risk Advisory

We provide strategic guidance to help you understand and manage cyber risk.

This includes prioritising investments, improving security maturity, and aligning with business objectives.

In simple terms:
We help you make smarter decisions about where to focus your security efforts.

BLACKBOX
PENTESTERS

Scoping Assessment

We define the right approach for your security testing based on your environment, risks, and objectives.

This ensures testing is targeted, effective, and aligned with business priorities.

In simple terms:
We make sure you're testing the right things in the right way.

BLACKBOX
PENTESTERS

Cloud Security Assessment

We assess the security of your cloud environments (e.g. AWS, Azure, GCP).

This includes configurations, access controls, and potential exposure risks.

In simple terms:
We check whether your cloud systems are securely set up and protected.

BLACKBOX
PENTESTERS

PCI DSS Penetration Testing Services

We perform testing aligned with PCI DSS requirements to support compliance.

This includes identifying vulnerabilities that could impact cardholder data security.

In simple terms:
We help ensure your systems meet the security standards required for handling payment data.

BLACKBOX
PENTESTERS

IoT Penetration Testing

We assess connected devices for vulnerabilities that could be exploited.

This includes hardware, firmware, communication protocols, and integrations.

In simple terms:
We test whether your smart devices can be hacked.

BLACKBOX
PENTESTERS

Cyber Threat Intelligence: Dark Web Monitoring Service

We monitor dark web and underground sources for signs of compromised data, credentials, or threats related to your organisation.

This enables early detection and proactive response.

In simple terms:
We check whether your data or access details are being shared or sold online.

BLACKBOX
PENTESTERS

Source Code Review

We review your application source code to identify security vulnerabilities before deployment.

This helps prevent issues from reaching production environments.

In simple terms:
We check your code for security flaws before attackers can find them.

BLACKBOX
PENTESTERS

SOC Breach Simulation & Detection Training

We simulate realistic attacks to test and improve your Security Operations Centre (SOC) detection and response capabilities.

This includes identifying gaps in monitoring, alerting, and response processes.

In simple terms:
We test whether your security team can spot and respond to an attack in real time.

BLACKBOX
PENTESTERS

Post-Remediation Validation Testing

We verify that previously identified vulnerabilities have been properly fixed.

This ensures that remediation efforts are effective and risks are genuinely reduced.

In simple terms:
We confirm that the fixes you've made actually work.

BLACKBOX
PENTESTERS

Access Control Audit (Physical Security Review)

We assess how effectively your buildings and restricted areas are protected against unauthorised access.

This includes entry systems, staff behaviour, and movement within facilities.

In simple terms:
We test whether someone could get into your building and go where they shouldn’t.