Penetration Testing



Offensive Security Capabilities

Independent. Evidence-Led. Business-Focused.

Cybernion

www.cybernion.com | info@cybernion.com

What is Penetration Testing?

A penetration test is an authorised, simulated attack against your systems, applications, or people, conducted by experienced testers to find and safely exploit vulnerabilities before an adversary does. It shows how real weaknesses chain together and what an attacker could actually achieve, mapped to business impact.

When Testing Is Required

Penetration testing is required by standards such as PCI DSS and ISO 27001, expected in enterprise supplier reviews, and prudent before any major release or significant change.

Testing should be repeated at least annually, and after significant changes to systems or applications.

1 Exploitation, Not Just Scanning

A test safely exploits and chains weaknesses to prove real impact, unlike an automated vulnerability scan.

2 Scope Defines the Test

Only the agreed targets are tested. A test covers what is in scope, not the whole estate by default.

3 A Point in Time

A test reflects security at the time of testing. Retesting confirms fixes and covers new changes.

Why Penetration Testing?

Compliance & Risk

Required by PCI DSS, ISO 27001, and many enterprise and regulator reviews

Real-World Assurance

Shows what an attacker could actually achieve, not just a list of theoretical flaws

Risk Reduction

Finds and prioritises the weaknesses that matter before they are exploited

Customer Confidence

Evidence of independent testing that unblocks enterprise security reviews

Credibility & Trust

Demonstrates a proactive, tested approach to protecting systems and data

Our Penetration Testing Services

A holistic service across Scoping, Testing, and Reporting, delivered by experienced, independent testers.

Scoping & Advisory

- Threat and scope definition
- Rules of engagement
- Test approach and methodology
- Environment and access planning
- Risk and priority guidance

Testing

- Web and API application testing
- Internal and external network testing
- Cloud configuration testing
- Social engineering and phishing
- Mobile and wireless testing

Reporting & Retest

- Prioritised findings and impact
- Remediation guidance & debrief
- Verification retesting
- Penetration Test Report
- Findings & Remediation Matrix

Penetration Testing Process

Four stages, repeated at least annually or after significant changes occur.

1 Plan & Prepare

- Define scope, targets & timeline
- Agree rules of engagement
- Establish communication process
- Confirm access & environment

2 Reconnaissance

- Map attack surface & data flows
- Identify entry points & assets
- Enumerate services & technologies
- Prioritise likely attack paths

3 Exploit

- In-depth manual testing
- Safe exploitation & chaining
- Impact analysis per finding
- Privilege escalation & pivoting

4 Report

- Penetration Test Report
- Findings & Remediation Matrix
- Detailed findings & recommendations
- Retest to verify remediation

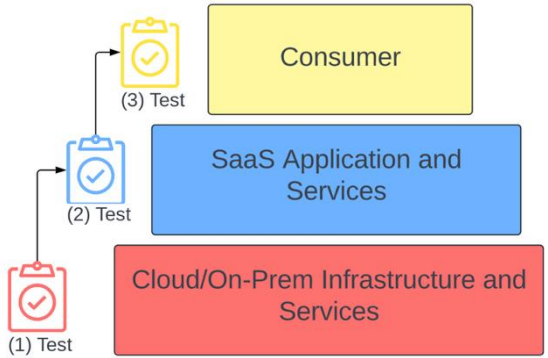
Case Study 1 - Web Application Test

An e-commerce company preparing for peak trading engaged us to conduct a penetration test of its customer-facing platform, covering its web application, payment APIs, and supporting cloud infrastructure.

Requirements

- Test the web application and payment APIs for vulnerabilities that could expose customer or payment data
- Assess the security of the supporting AWS cloud infrastructure and its configuration
- Provide prioritised, business-focused recommendations to remediate before peak trading

Our Solution



By manually testing and safely exploiting real weaknesses, we showed the e-commerce company exactly what an attacker could reach, and gave it a prioritised plan to remediate the highest-impact issues before peak trading.

Key Highlights

- **Plan & Prepare:** Define clear objectives, targets, rules of engagement, and comms process
- **Scope:** Scope the test to cover the web application, payment APIs, and cloud infrastructure
- **Test:** Conduct manual testing, safe exploitation, and impact analysis across each target
- **Report:** A detailed report and remediation matrix highlighting findings, impact, and a prioritised fix plan

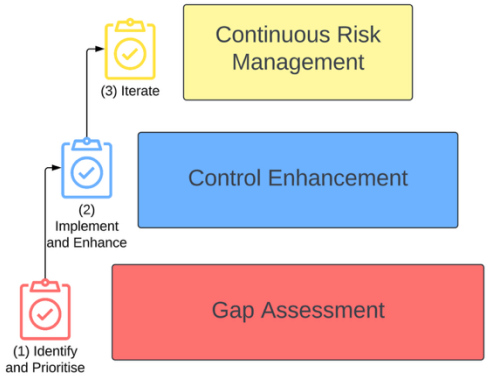
Case Study 1 - Internal Network Test

A professional services firm engaged us to conduct an internal network penetration test to understand what an attacker with a foothold, such as a phished employee, could achieve across its corporate environment.

Requirements

- Assess what an attacker with internal access could reach across the corporate network
- Test segmentation, privileged access, and lateral movement paths to critical systems
- Identify and prioritise the weaknesses that most increase the risk of compromise
- Verify remediation of high-impact findings through a follow-up retest

Our Solution



A structured internal test showed how a single foothold could lead to broad access, followed by clear remediation guidance and a retest that confirmed the firm had closed its highest-impact exposures.

Key Highlights

- **Reconnaissance:** A reconnaissance phase to map the internal attack surface and likely paths
- **Exploitation:** Manual exploitation of weaknesses across segmentation, access, and lateral movement
- **Analysis:** Impact analysis and prioritisation of findings by real business risk
- **Report & Retest:** Detailed reporting, a remediation debrief, and a retest to confirm fixes

Important Penetration Testing Artefacts

The inputs that shape the test, and what you receive in return.

Input: What You Provide

RoE	Rules of Engagement
SCP	Scope & Target List
ARC	Architecture & Data Flows
ACC	Test Accounts & Access
AUT	Written Authorisation
ENV	Environment Details
CON	Key Contacts & Escalation
WIN	Testing Windows
PRV	Prior Test Reports
CMP	Compliance Requirements

+ Other supporting information as agreed during scoping.

Output: What You Receive

1 Penetration Test Report

A comprehensive report of findings covering each vulnerability, how it was exploited, its business impact and severity, with clear, prioritised remediation guidance.

2 Findings & Remediation Matrix

A structured matrix of findings by severity and target, tracking remediation status and retest results, supporting clear ownership and closure.

Thank You

Ready to test your defences? Let's talk.



Web www.cybernion.com

FAQs www.cybernion.com/insights

Email info@cybernion.com

Phone 0404 760 923

A Trusted Cyber Companion