

# Penetration testing

Identify, assess and prioritise organisational vulnerabilities

CNS, part of the Flow group, have expert penetration testing capabilities and are CREST approved. The cybersecurity team will complete testing under real attack conditions replicating non-invasive hacker techniques and can advise on how to remediate any vulnerabilities identified.



 **security**

## CREST approved



CNS are CREST approved, meaning organisations can be assured that our penetration testing services are:

- Delivered using best practice policies and procedures
- Carried out by highly-qualified individuals
- Covered by rigorous and enforceable codes of conduct

## Main benefits of penetration testing:

- Evaluate your organisations security maturity
- Improve business awareness and understanding of your cybersecurity exposure to risk
- Detect and remediate security threats before they can be exploited by cyber criminals
- Provide independent technical security assurance of your security controls
- Prioritise security investments based on actionable intelligence
- Protect company reputation whilst displaying your continuous commitment to security

# Flow's adaptable approach to penetration testing

## Tier 1 - vulnerability scan



**Objective:** To highlight common problems.

The monthly "MOT" check of external/public interfaces. Common vulnerabilities are checked and then rated based on severity, using the Common Vulnerability Scoring System (CVSS).

## Tier 2 - vulnerability assessment



**Objective:** To highlight common and obscure problems and often conducted to reduce general costs over a penetration test.

A replication of the initial steps in a real-life attack, the point at which a malicious actor is thwarted and moves on to an easier target. The process is dependant on the engagement context, such as a web application and external infrastructure.

## Tier 3 - penetration test

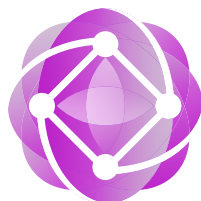


**Objective:** to highlight avenues to critical business systems and services to prevent future compromise from advanced vectors.

Similar to tier 2, with the inclusion of advanced techniques and methods in real-world attack chains. A penetration test is a go-to standard to identify risk and exposure.



 datacentre



 networks



 cloud



 security