Penetration Testing from Nexon

Protect your organisation and its assets with assurance from front-line experts in ethical hacking. Nexon Penetration Testing provides the insights, measures and structures to manage and mitigate cyber risk and future proof your business.

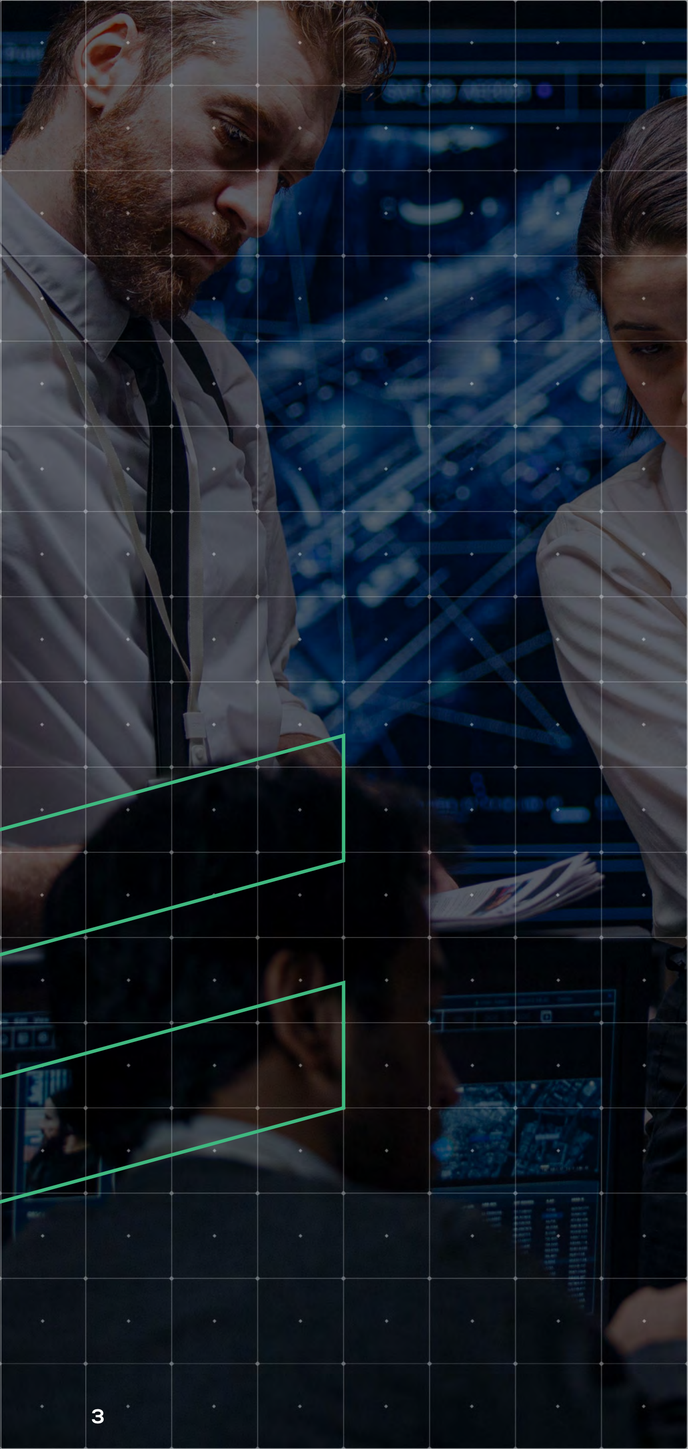
The issue

The vast escalation in the volume and complexity of threats is raising the profile of cybersecurity at Board level. Understanding the security maturity of your organisation, its infrastructure and assets is a critical next step. Penetration Testing is a measurable and high impact exercise to identify and target weaknesses to ensure organisations are both forewarned and forearmed.

Using ethical hackers to evaluate your security posture through real life adversary simulations, Penetration Testing helps to face vulnerabilities head on – and provides the re-assurance, structure and control your organisation needs to take preventative action, avoiding down time, financial loss or reputational damage that can result from a breach or attack.

Insurance for peace of mind

Cyber insurance has emerged as a critical aspect of risk management for organisations navigating the digital landscape. As these businesses face heightened vulnerability to data breaches and losses, many insurance providers now mandate organisations to implement robust security measures to safeguard their digital assets. One such measure, regular pen testing, can significantly lower cyber insurance premiums and fulfill the stipulations of certain insurance policies. By proactively identifying and addressing potential vulnerabilities, organisations can not only protect themselves from cyber threats but also demonstrate a commitment to risk mitigation, which is increasingly valued by insurance providers.



The right time to do a Penetration test

It’s probably the right time if:

Your last penetration test was more than 12 months ago

Your insurances require a penetration test

You have compliance or audit requirements that mandate a security assessment

Vulnerabilities have been identified as an issue and require validation / action

Unauthorised access to perimeter services, users or applications is suspected

Best practice security benchmarking of deployment practices / implementations is needed

You need assurance that systems have been deployed securely and your IT team are operating effectively.

If boards are requesting due diligence around data assets, they must ensure these assets are stored and protected appropriately, applying the same oversight used for financial reporting and governance.

A third party can provide a fresh perspective and expertise to uncover security holes that internal teams might miss, keeping you a step ahead.

The Service

Penetration Testing (Pentest) is where we perform an assessment of an organisation's security, from the position of a malicious attacker using the same tools and techniques as real threat actors in the wild. This includes an assessment of your risks, threats, vulnerabilities and overall security posture, in a safe and structured manner.

There are three types of Penetration Testing offered – White Box, Grey Box and Black Box.

White Box

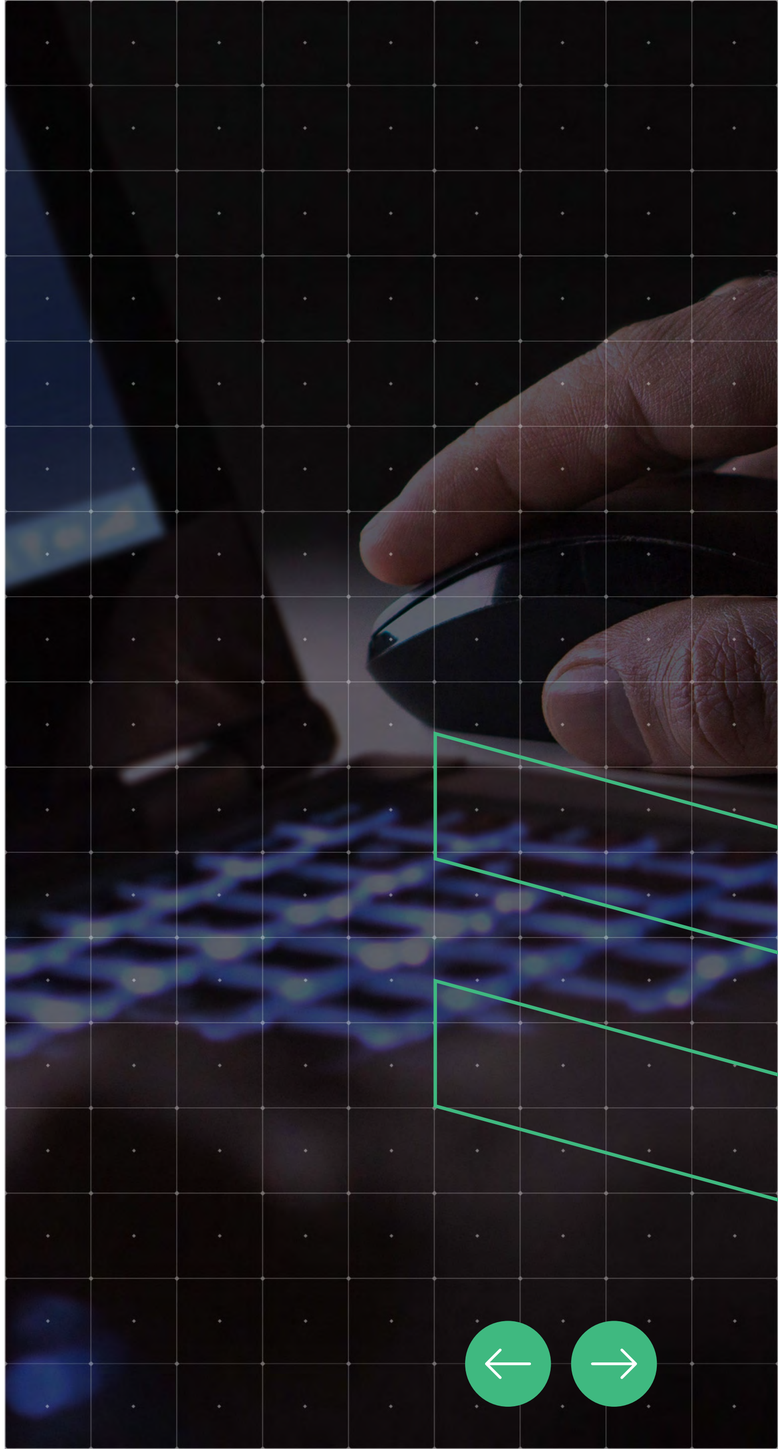
Penetration testers are given full access to source code and architecture, providing a full assessment of internal and external vulnerabilities from an informed source.

Grey Box

Penetration Testers perform an assessment with some information or access provided by the organisation, such as IP addresses or user credentials to focus efforts on high-risk areas.

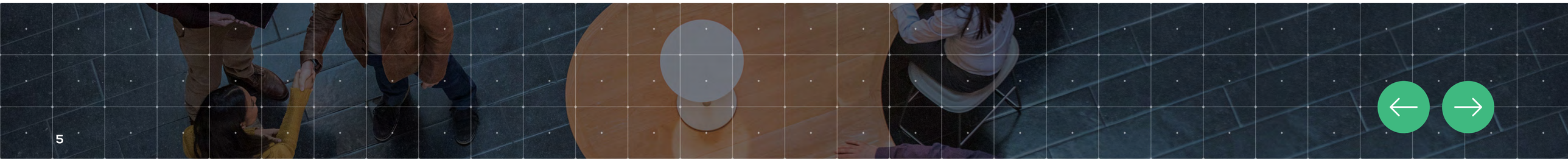
Black Box

Penetration Testers perform an assessment of the organisation with no information except the company name, to investigate and target vulnerabilities exploitable from outside of the network.



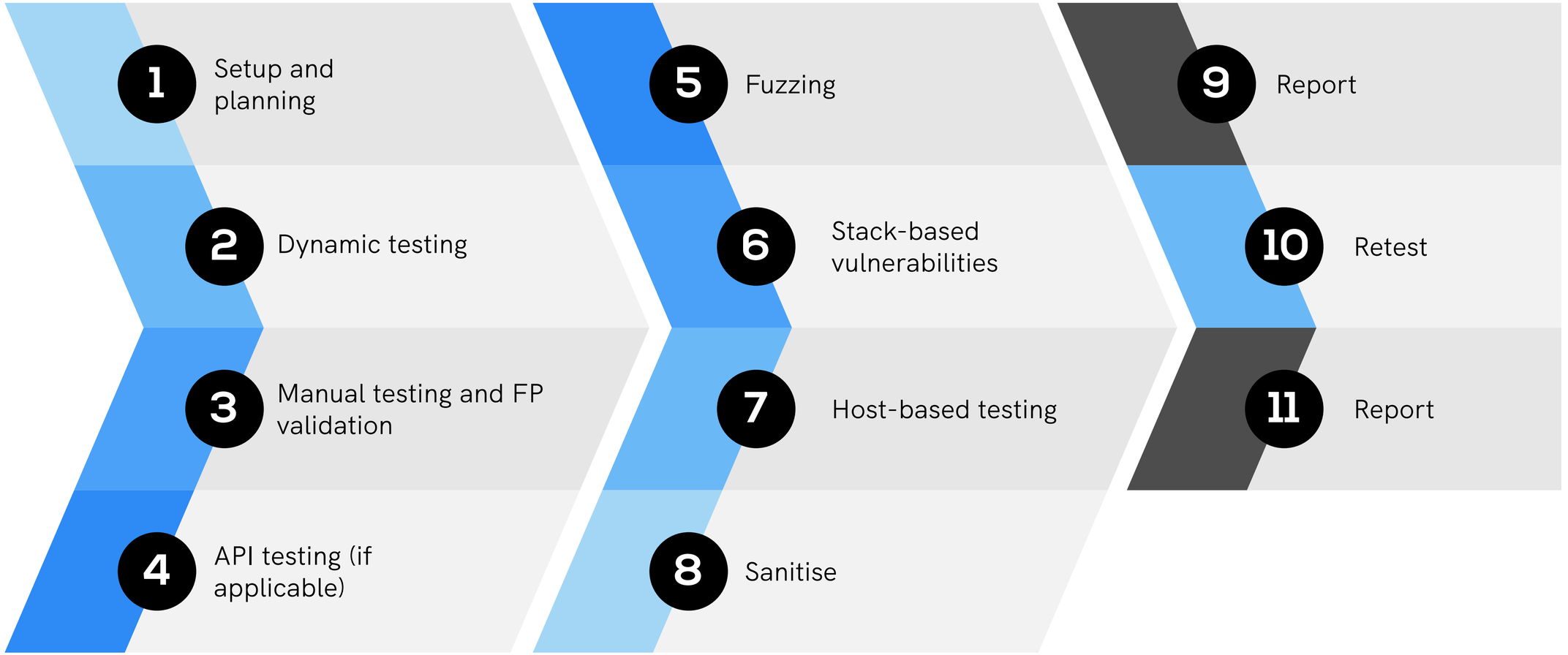
Services

- Network/Cloud
- Webapps and APIs
- WiFi
- Password audits
- Jack-in assessment (Disgruntled employee, cleaner)
- Social engineering (Phishing, Vishing etc.)
- Physical access testing
- Mobile apps
- Breach simulation exercises
- Adversary simulation and testing, Red/Blue Team Ops
- IoT/ICS/PCS/SCADA testing
- Vulnerability assessments
- Bespoke testing, for example, cars, charging stations, hardware platforms, etc



Methodology

Webapps methodology



The deliverable

Our engagement starts by crafting a Network Attack Blueprint to ensure we target all of the key areas to obtain access to your corporate network, web applications, wireless networks, end users and perimeter services in a structured and safe way.

Your Penetration Test includes:

- Comprehensive Penetration Test Report with all evidentiary information, screenshots, repeatable steps and recommended remediation activities
- Executive Level Summary Insights
- Access to our next generation reporting platform to track, manage and remediate all of the findings
- Pentest certificate to satisfy auditor and insurance requirements
- Supplemental Documents such as; Raw Data, Phishing Site, Password Audit, Jack-in Assessment and and files from particular testing components
- Presentation to Stakeholders

Our engagement process

By working to first map and evaluate security maturity, we reduce and mitigate risk by remediating vulnerabilities and reducing security incidents, to ensure your organisation has the necessary foundations and tools to be both forewarned and forearmed.

1

Pre-engagement

Identify and understand outcomes from the penetration test.

2

Proposal

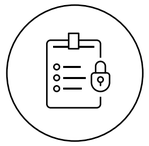
We identify the type of testing and the elements within the scope in a detailed proposal.

3

Engagement

An official engagement has been signed, timelines and deliverables defined.

4



Reconnaissance

We commence our engagement and footprint the organisation from the internet to determine the attack strategy (Network Attack Blueprint)

5

Exploitation

Our team of ethical hackers start testing against your systems for weaknesses, vulnerabilities and potential entry points.

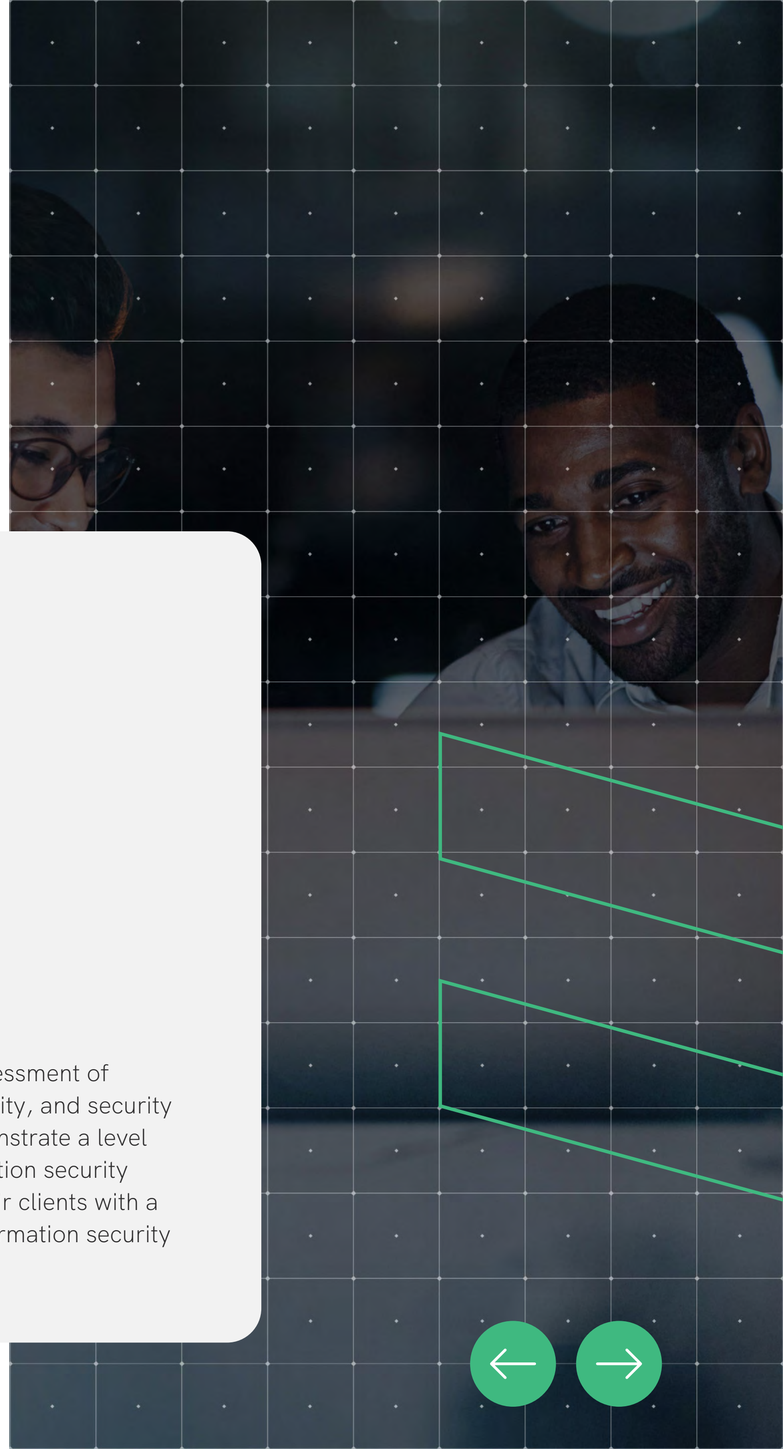
6

Report

We conclude our engagement by delivering a comprehensive report of our findings, impacts, criticality, and suggested remediation strategies.

Why Nexon?

Our Security Assurance services undertake independent testing and incident simulations to ensure networks and applications are secured and teams are equipped and able to respond with minimal disruption in the fastest timeframe; mitigating risk and providing assurance at every level.



Expertise + experience

We're an award-winning organisation, founded over 20 years ago. We've been at the forefront of Cybersecurity and Penetration Testing for over 19 years, bringing expertise and experience across all industries, sectors and verticals.

Confident and assured

We use real world tools, tactics and techniques to provide an authentic adversary simulation. By partnering with you to tackle the big issues - and the detail, we face vulnerabilities together and provide support beyond the report.

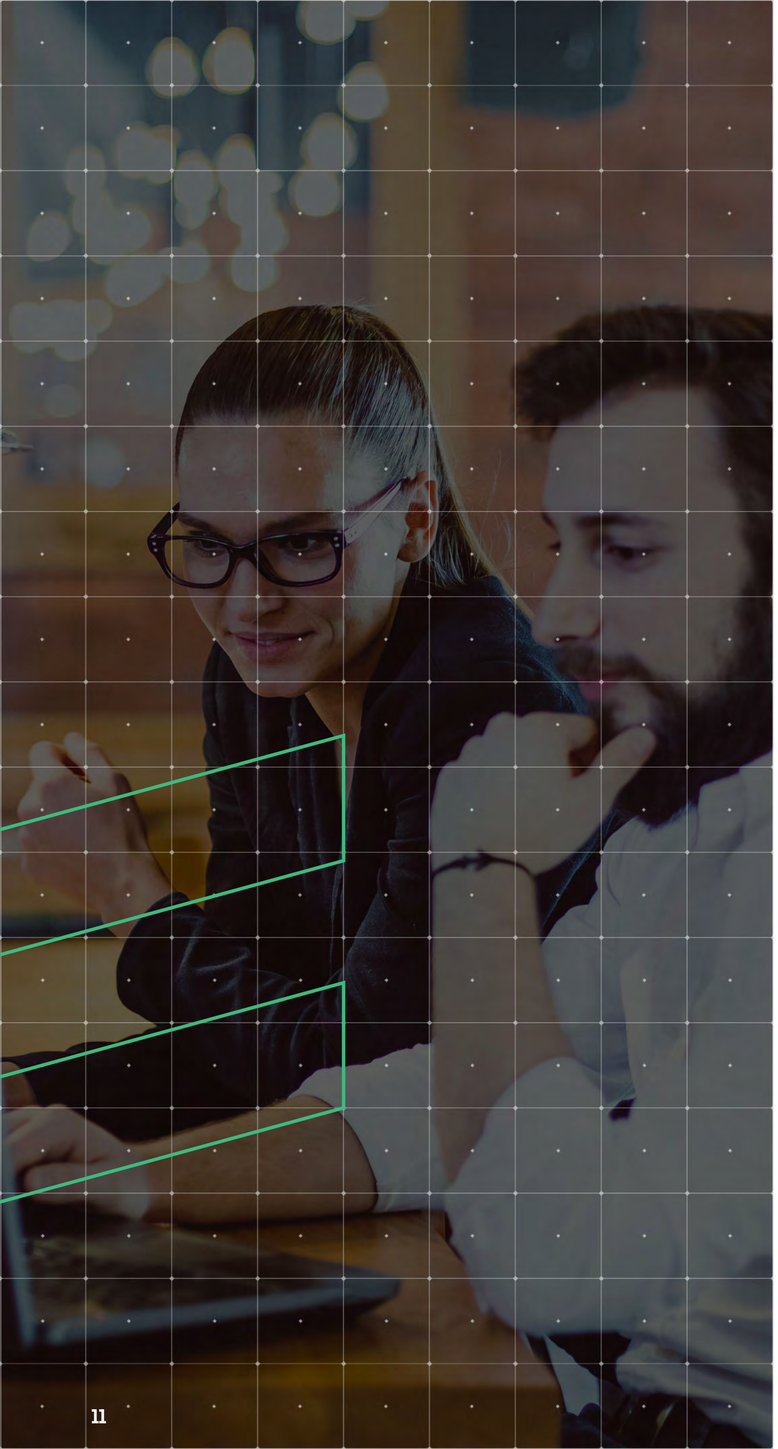
Local resources. Global service.

We're an Australian-based team of certified ethical hackers and testers; security vetted, police checked and ready to protect your business. Our team offer vast expertise in businesses of all sizes and sectors with attributed bug bounties and zero-day vulnerabilities.

CREST certified

The CREST certification is an independent verification and assessment, conducted by the not-for-profit cybersecurity body on Nexon's Cyber Security capabilities, systems and processes which provide a level of confidence and assurance that clients are working with an approved provider and highly skilled experts in the industry.

CREST requires a rigorous assessment of business processes, data security, and security testing methodologies to demonstrate a level of assurance that their information security methodologies can provide their clients with a robust assessment of their information security posture.



Certified and accredited

We're a CREST Certified organisation, ensuring you receive independence and a premium standard of testing and deliverables. As an ISO27001 and ISO9001 Accredited organisation, you'll have absolute peace of mind and re-assured delivery.

Certified System Quality ISO 9001 SAI GLOBAL
Certified System Information Security ISO 27001 SAI GLOBAL
Certified System Environment ISO 14001 SAI GLOBAL
Certified System OHS ISO 45001 SAI GLOBAL

Our team hold vast qualifications and accreditations from leading vendors and industry bodies:

CREST PEN TEST
CREST CPSA PRACTITIONER
CREST CRT REGISTERED
OFFENSIVE OSCP
OFFENSIVE OSWP
TCM SECURITY CERTIFIED Practical Network Penetration Tester PNPT
CISSP Certified Information Systems Security Professional
CERTIFIED AI RED TEAM PROFESSIONAL
Certified Enterprise Security Professional (CESP-AD CS)
CEH Certified Ethical Hacker
ECSA EC-Council Certified Security Analyst
LPT Licensed Penetration Tester
CISA Certified Information Systems Auditor. An ISACA Certification
CompTIA Security+
CompTIA Network+
CompTIA Linux+
CompTIA CTT+
aws certified Cloud Practitioner
eCPPT
eWPT

Look to the future, with Nexon

Interested in finding out more about how you can protect your business with a Pentest? Contact a Nexon expert today.

1300 800 000
pentestenquiries@corp.nexon.com.au
pentest.nexon.com.au

Follow **nexonap**