All Services Brochure

Cyber-info@worknest.com

Penetration Testing

In the dynamic world of cyber security, innovation is key. Our penetration testing services are designed with this in mind. We offer an advanced, comprehensive solution to identify vulnerabilities in your systems and networks, using cutting-edge techniques and technologies.

CHECK Penetration Testing

Delivered by CHECK-certified consultants, ensuring compliance with NCSC and CREST standards.

Includes infrastructure, web application, and IT Health Check assessments, combining rigorous technical testing with regulatory assurance for high-security environments.

Application Security

Identifies vulnerabilities in web, mobile, desktop, and API-based applications through real-world attack simulations, static analysis, and targeted code reviews.

Covers common and complex threats, from insecure authentication and data exposure to unsafe input handling, across systems.

Social Engineering

Simulates real-world social engineering attacks to uncover human and physical security gaps.

Testing includes OSINT, phishing, vishing, and black team operations, delivering actionable insights to strengthen organisational resilience against manipulation and intrusion.

Network Infrastructure & Architecture Security

Uncovers vulnerabilities, misconfigurations, and privilege gaps across your network infrastructure and architecture.

From Active Directory to firewalls, VPNs, and Wi-Fi, our real-world attack simulations deliver clear risk ratings and actionable steps to strengthen your security.

Cloud & Container Security Services

Identifies and supports remediation of vulnerabilities and misconfigurations across AWS, Azure, Google Cloud, and containerised environments, including Docker and Kubernetes.

Reviews configurations in Google Workspace and Microsoft 365 to ensure alignment with best practices.

PSN IT Health Check (ITHC)

Ensure PSN compliance with comprehensive IT health checks.

Identifies vulnerabilities, streamlines audits, and delivers actionable guidance strengthening security across internal and external systems to protect public data and maintain robust assurance.

Attack Simulation

Uncover hidden risks and strengthen defences with CREST-accredited attack simulation that replicates realistic, sophisticated real-world attacks. By leveraging advanced tactics, techniques, and procedures (TTPs), we test your organisation's ability to detect and respond to evolving threats.

Red Team Engagement

A classic full end-to-end engagement to test and improve your defences.

Utilises evasion techniques and covert delivery to evaluate detection capabilities, identify security gaps and support blue teams in handling serious events.

Threat-Led Testing

Structured, intelligence-driven assessment that simulates realistic cyber-attacks based on current threat intelligence.

Simulates attacks from adversaries most likely to target your organisation and is tailored to your specific threat landscape, sector, and security posture.

Purple Team

A collaborative security testing approach where offensive (Red Team) and defensive (Blue Team) teams work together in real-time to test, detect, and improve your organisation’s ability to identify and respond to simulated cyber threats.

Assumed Breach Assessment

Simulates a scenario where an attacker already has internal access.

Starts from a point of compromise, such as domain user access, valid credentials, or network foothold, to evaluate how your organisation detects, responds to, and contains internal threats.

Continual Threat Service

Proactive, ongoing monitoring of your organisation's attack surface to ensure you stay ahead of potential adversaries.

Delivers persistent, targeted attacks using real-time intelligence to help safeguard your organisation while offering comprehensive, ongoing support.

EDR & XDR Evaluation

Evaluates the effectiveness of your endpoint detection and response systems against threats ranging from commodity malware to custom attacks, while providing insights into the configuration and maintenance of your security tools.

Incident Response

Respond swiftly and effectively to cyber incidents. Our array of bespoke retainers, immediate support, assessments and training services enables you to respond effectively, reducing the risk of escalation, minimising downtime, protecting critical assets, and preserving reputation.

Incident Response Retainers

Our retainer packages offer immediate access to our cyber defence experts to tackle any security incident.

Enhances preparation and incident response efficiency with features such as ongoing scanning, real-time monitoring, customer playbooks and rapid response.

Cyber Incident Helpline

Urgent support for any organisation experiencing a cyber incident and wanting instant, tailored advice and technical help from an expert.

Our team understands the threat landscape and can offer urgent support with innovative strategies to counter risks and keep your operations running.

Tabletop Exercises

Simulates specific cyber incident scenarios to test and strengthen your response capabilities.

Our experts guide your team through scenarios, showing how to handle incidents effectively. We help develop and refine your incident response strategy by integrating practical insights and actions.

Incident First Responder Training

This CREST-accredited hands-on training teaches early containment, evidence preservation, and effective handoff to specialist responders.

Tailored to your environment, we train your team to spot threats quickly, minimise impact, and maintain forensic integrity for faster resolution and stronger compliance.

Incident Response Gap Analysis

Identify and remediate weaknesses in your incident response readiness before issues arise.

By comparing your processes to standards such as NIST and ISO/IEC 27035, we provide tailored, prioritised roadmaps to improve your incident response, whether refining an existing plan or building one from scratch.

Ransomware Readiness Assessment

A nine-step assessment to strengthen your ransomware defences.

Our experts analyse your security posture, identify vulnerabilities, and provide tailored advice, hands-on consultations, and team training. We improve preventative measures and equip you with essential tools and knowledge.

Digital Forensics

Our Digital Forensics service helps uncover the root cause of security incidents with advanced analysis and strict evidence protocols.

From ransomware and IP breaches to payment fraud, we deliver actionable insights and litigation-ready reports to support compliance, remediation, and recovery.

Data Protection

From outsourced DPOs and detailed DPIAs to NHS toolkit support, records management, and breach response, we deliver practical, tailored solutions. We work alongside you to embed governance, achieve regulatory compliance, and protect the integrity of your sensitive information.

GDPR

Expert-led GDPR solutions to help you achieve, maintain, and demonstrate GDPR compliance.

From audits and gap analysis to tailored implementation and bespoke consultancy, we offer actionable guidance on how to safeguard personal data and avoid data breaches and penalties.

Outsourced DPO

Get access to one of our qualified Data Protection Officers to help manage GDPR compliance, provide expert guidance, and liaise with regulators, delivering flexible, cost-effective data privacy support without the costs of an in-house hire.

NHS Toolkit

Receive specialist consultancy to help your organisation achieve NHS DSP Toolkit compliance with ease.

We provide tailored guidance, practical policies, and expert support to meet mandatory data protection and cyber security standards quickly and cost-effectively.

Information Security

Protect your systems, data, and reputation. We offer practical, tailored support, including Virtual CISO services, PCI DSS compliance, SOC 2 consultancy, DORA support, and cyber maturity assessments, offering practical, tailored tactics designed to strengthen your security.

Cyber Essentials

Achieve Cyber Essentials or Cyber Essentials Plus with ease through our tailored guidance, expert consultants, and adaptable service options designed to match your organisation's size, goals, and security maturity.

Virtual CISO

Our vCISO services deliver flexible, cost-effective security leadership, providing strategic guidance, risk oversight, compliance support, staff training, and tool management to help your organisation improve governance, meet regulatory requirements, and strengthen resilience without a full-time CISO.

SOC 2 Compliance Service

Consultant-led SOC 2 support and AICPA-aligned audits to guide your organisation through implementation, control reviews, evidence preparation, and collaboration with CPA auditors for a smooth, efficient compliance journey.

DORA Consultancy Service

Expert-led DORA support to assess how DORA applies to your organisation, close compliance gaps, strengthen IT risk management, test resilience, oversee third parties, and streamline incident reporting, helping your organisation meet EU requirements with confidence.

PCI DSS Compliance Service

Get specialist guidance to achieve and sustain PCI DSS compliance, including expert assessments, remediation support, and essential testing services that strengthen security posture and reduce the risk of data breaches.

Cyber Security Maturity Assessment

Our Cyber Security Maturity Assessment reviews your organisation's systems, policies, and processes to uncover security gaps and provides a tailored report outlining clear actions to strengthen resilience and improve overall security posture.