DATA SECURITY
A UBDS GROUP COMPANY

PENETRATION TESTING SERVICES

For G-Cloud 15

January 2026

Classification: Public

CONTENTS

1. INTRODUCTION

3B Data Security is one of the UK's only cyber security providers fully assured by the National Cyber Security Centre (NCSC) to deliver CHECK penetration testing, cyber incident response, cyber incident exercising, and cyber advisory services.

NCSC assured across the board, CREST accredited, and dual-approved by the PCI Security Standards Council as both a Qualified Security Assessor (QSA) and PCI Forensic Investigator (PFI), 3B Data Security is trusted by UK government, regulators, and critical national infrastructure organisations to deliver security assurance at the highest level.

Using the same reconnaissance techniques as threat actors and red teams, 3B Data Security's consultants uncover risks others miss, rigorously challenge assumptions, and deliver clear, action-oriented reporting that enables organisations to secure systems, data, and services that underpin the public sector. This approach is underpinned by **Check. Challenge. Secure.** 3B Data Security's proven method for ensuring defences hold under audit, attack, and public scrutiny.

Backed by over 20 years of real-world experience in digital forensics and incident response, 3B Data Security provides confidence that security controls operate effectively under real-world conditions - not just in theory.

CHECK

We uncover the risks others overlook, using deep expertise and the latest threat intelligence.

CHALLENGE

We rigorously test every control, critique every assumption, and simulate real attacker tactics so nothing is left to chance.

SECURE

We help you close every gap, validate every fix, and prove your defences hold under audit, attack, or public scrutiny.

CERTIFIED AT EVERY LEVEL THAT MATTERS.

You can get in touch with us via: 3bframeworks@3bdatasecurity.com

Website: www.3bdatasecurity.ccom

LinkedIn: https://www.linkedin.com/company/3b-data-security

2. PENETRATION TESTING – ACTIVE DIRECTORY SECURITY REVIEW.

Comprehensive Active Directory security reviews identifying misconfigurations, privilege escalation paths and weaknesses attackers exploit. The service assesses domain controllers, group policies and authentication mechanisms, delivering actionable recommendations to harden AD environments and reduce risk of compromise.

KEY FEATURES

- Assessment of domain controllers and AD infrastructure security posture
- Review of Group Policy Objects (GPO) for misconfigurations
- Privilege escalation path analysis and attack simulation
- Evaluation of password policies and authentication mechanisms
- Detection of orphaned accounts and excessive permissions
- Analysis of trust relationships and domain hierarchy risks
- Manual validation of findings for accuracy and relevance
- Detailed reporting with prioritised remediation recommendations
- Executive debrief translating AD risks into business impact
- Secure client portal with real-time findings and tracking

KEY BENEFITS

- Tailored testing specific to your organisation
- CREST and CHECK certified experts
- Accurate results using manual and automated techniques
- Real-time visibility supporting faster decision-making
- Reduced remediation cost through risk-based prioritisation
- Rapid retesting reduces exploitation risk
- Clear executive-level risk translation
- Non-technical reporting for senior stakeholders
- Faster identification and resolution of vulnerabilities
- Enhanced accuracy using threat intelligence

3. PENETRATION TESTING – API TESTING.

Expert API penetration testing across REST, GraphQL, SOAP and microservices. Identifies authentication flaws, authorisation gaps, injection risks and misconfigurations using manual and automated techniques to reduce attack surface and protect sensitive data.

KEY FEATURES

- Testing of REST, GraphQL and SOAP endpoints
- Authentication and session management assessment
- Authorisation checks for broken access control
- Injection testing including SQLi and NoSQLi
- Business logic abuse and workflow bypass testing
- Rate limiting and abuse resilience evaluation
- Schema validation and error handling review
- Sensitive data exposure verification
- Manual validation of automated findings
- Secure client portal with real-time findings

KEY BENEFITS

- Tailored API testing for your organisation
- CREST and CHECK certified experts
- Accurate results from manual and automated testing
- Faster remediation decisions via real-time visibility
- Reduced cost through prioritised recommendations
- Rapid retesting lowers exploitation risk
- Clear executive risk translation
- Non-technical reporting for stakeholders
- Reduced downtime through early identification
- Enhanced relevance using threat intelligence

4. PENETRATION TESTING – CLOUD SECURITY AUDIT (M365 / GCP / AZURE / AWS).

Expert cloud penetration testing for Microsoft 365, GCP, Azure and AWS. Combines manual and automated techniques with threat intelligence to identify misconfigurations and vulnerabilities, strengthening cloud security and protecting sensitive data.

KEY FEATURES

- Review of cloud configurations against security best practice
- Identity and access management assessment
- Testing for exposed storage and data leakage
- Privilege escalation and MFA evaluation
- Network security group and firewall analysis
- Encryption settings verification
- Manual validation of automated findings
- Threat intelligence-informed testing
- Secure portal with real-time vulnerability visibility
- Compliance checks against CIS, ISO and NIST

KEY BENEFITS

- Tailored cloud testing for your environment
- CREST and CHECK certified experts
- Accurate, comprehensive testing outcomes
- Faster decisions through real-time visibility
- Reduced remediation costs
- Rapid retesting reduces exploitation risk
- Executive debrief translating risk into impact
- Clear reporting for senior stakeholders
- Reduced downtime through early detection
- Improved relevance using threat intelligence

5. PENETRATION TESTING – FIREWALL RULES AND CONFIGURATION AUDIT.

Firewall rule base and configuration testing across Cisco, Palo Alto, Fortinet, Check Point, AWS and Azure. Identifies overly permissive rules, segmentation gaps and logging issues, providing actionable hardening guidance.

KEY FEATURES

- Firewall rule base review against best practices
- Identification of permissive and shadowed rules
- Inbound and outbound traffic analysis
- Network segmentation validation
- NAT and port forwarding assessment
- Logging and alerting configuration review
- VPN and remote access security evaluation
- Manual validation of findings
- Threat intelligence-informed testing
- Secure reporting portal with real-time visibility

KEY BENEFITS

- Organisation-specific testing
- CREST and CHECK certified experts
- Accurate manual and automated testing
- Faster remediation through real-time insight
- Reduced cost via prioritised recommendations
- Rapid retesting reduces exploitation risk
- Executive risk translation
- Clear reporting for non-technical stakeholders
- Reduced downtime through early identification
- Enhanced relevance via threat intelligence

6. PENETRATION TESTING – IOT AND SCADA.

Specialist penetration testing for IoT and SCADA/ICS environments. Assesses embedded devices, gateways and control networks using controlled techniques to identify vulnerabilities while protecting safety and availability.

KEY FEATURES

- Asset discovery across OT and IoT estates
- Risk-based scoping to protect safety-critical systems
- Firmware and configuration review
- Industrial protocol testing
- Gateway, PLC and HMI security assessment
- Credential and key management verification
- Network segmentation and lateral movement testing
- Supply chain integrity checks
- Detailed reporting with prioritised remediation
- Real-time notification via client portal

KEY BENEFITS

- Organisation-specific adversary simulation
- CREST and CHECK certified experts
- Accurate results using manual tradecraft
- Faster decisions via real-time visibility
- Reduced remediation cost
- Rapid retesting reduces exploitation risk
- Executive translation of findings
- Clear reporting for senior stakeholders
- Minimal operational disruption
- Enhanced accuracy using threat intelligence

7. PENETRATION TESTING – CHECK IT HEALTH CHECKS.

Penetration testing and IT Health Checks delivered under the NCSC CHECK scheme. Identifies vulnerabilities across networks, applications and infrastructure to reduce cyber risk and improve security posture.

KEY FEATURES

- External testing of internet-facing services and VPNs
- Internal configuration and patch management review
- Credentialed vulnerability scanning
- Representative sampling of large estates
- Firewall ruleset testing
- Secure build reviews
- Backup security validation
- Mobile device security assessment
- Manual validation of findings
- Secure client reporting portal

KEY BENEFITS

- Organisation-specific testing
- CREST and CHECK certified experts
- Accurate comprehensive results
- Faster remediation decisions
- Reduced cost through prioritisation
- Rapid retesting lowers exploitation risk
- Executive risk translation
- Clear reporting for stakeholders
- Reduced downtime
- Enhanced accuracy using threat intelligence

8. PENETRATION TESTING – OPEN-SOURCE INTELLIGENCE (OSINT).

Open-source intelligence gathering to identify publicly available information attackers exploit. Maps digital footprint, uncovers exposed assets and highlights credential leakage and social engineering risks.

KEY FEATURES

- Comprehensive OSINT reconnaissance
- Domain and subdomain enumeration
- Network range discovery
- Service fingerprinting
- Social media footprint analysis
- Leaked credential detection
- Threat modelling based on exposure
- Passive intelligence gathering
- Manual validation of findings
- Detailed remediation reporting

KEY BENEFITS

- Tailored OSINT aligned to attack surface
- CREST and CHECK certified experts
- Comprehensive manual and automated coverage
- Faster mitigation via real-time discovery
- Reduced remediation cost
- Repeatable exposure tracking
- Executive risk translation
- Clear reporting for all audiences
- Reduced risk before exploitation
- Identification of initial access paths

9. PENETRATION TESTING – PCI SEGMENTATION TESTING.

PCI segmentation testing validating isolation of the Cardholder Data Environment. Identifies segmentation weaknesses, tests firewall controls and confirms PCI DSS compliance.

KEY FEATURES

- Validation of PCI segmentation
- Firewall and access control testing
- VLAN and routing assessment
- CDE isolation verification
- Lateral movement risk identification
- Manual and automated testing
- Prioritised remediation reporting
- Executive segmentation risk debrief
- Retesting after remediation
- Secure client portal

KEY BENEFITS

- Organisation-specific testing
- CREST and CHECK certified experts
- Accurate segmentation validation
- Faster compliance decisions
- Reduced compliance delays
- Rapid retesting lowers risk
- Clear executive reporting
- Supports PCI accreditation
- Stronger CDE protection

10. PENETRATION TESTING – PHISHING.

Targeted phishing simulations assessing organisational resilience to social engineering. OSINT-driven campaigns measure user behaviour and provide actionable insight, with optional awareness training.

KEY FEATURES

- Custom phishing campaigns
- OSINT-driven scenario development
- Domain and asset cloning
- Realistic email templates
- Click and credential tracking
- Accurate landing pages
- Repeatable campaigns
- Detailed reporting and metrics
- Optional awareness training
- Optional professional security training

KEY BENEFITS

- Organisation-specific phishing testing
- CREST and CHECK certified experts
- Realistic scenarios
- Visibility of user behaviour
- Reduced risk through targeted training
- Measurable improvement over time
- Executive risk translation
- Clear reporting
- Stronger security culture
- Current threat research integration

11. PENETRATION TESTING – PHYSICAL SOCIAL ENGINEERING.

Physical social engineering assessments testing resilience to real-world intrusion. Uses tailgating, impersonation and pretexting to identify weaknesses in access controls and staff awareness.

KEY FEATURES

- Tailgating and piggybacking tests
- Impersonation scenarios
- Pretexting techniques
- Visitor management assessment
- Staff security awareness evaluation
- Restricted area testing
- Realistic, policy-aligned scenarios
- Prioritised remediation reporting
- Executive debriefs
- Optional awareness training

KEY BENEFITS

- Organisation-specific physical testing
- CREST and CHECK certified experts
- Realistic manual techniques
- Faster visibility of access risks
- Reduced physical security gaps
- Repeatable testing
- Executive risk translation
- Clear non-technical reporting
- Reduced risk of unauthorised access
- Enhanced scenario accuracy via intelligence

12. PENETRATION TESTING – RED TEAMING.

Advanced red teaming engagements emulating real-world attack scenarios to assess organisational resilience against sophisticated threats. The service combines OSINT, phishing, internal compromise and privilege escalation to identify weaknesses in technical controls and staff awareness, strengthening detection, response and overall security posture.

KEY FEATURES

- Realistic attack simulation based on adversary tactics and techniques
- OSINT reconnaissance mapping external footprint and exposed assets
- Targeted phishing campaigns testing user awareness
- Credential compromise and persistence testing
- Privilege escalation and lateral movement assessment
- Monitoring, alerting and incident response evaluation
- Custom scenarios aligned to critical assets
- Controlled exploitation to minimise operational impact
- Prioritised remediation and strategic recommendations
- Executive debrief translating findings into business risk

KEY BENEFITS

- Tailored attack simulations for your organisation
- Experienced operators emulating real-world adversaries
- Identification of hidden weaknesses
- Faster defensive decision-making through attack-path insights
- Validation of critical security controls
- Reduced exposure through early identification
- Executive-level risk translation
- Clear reporting for senior leaders
- Reduced operational risk
- Enhanced realism using threat intelligence

13. THREAT-LED PENETRATION TESTING.

Threat intelligence-led penetration testing identifying emerging risks and adversary tactics. Real-world threat data informs realistic attack scenarios, prioritising vulnerabilities based on active threat trends to strengthen security posture against evolving cyber threats.

KEY FEATURES

- Threat intelligence-driven testing
- Identification of vulnerabilities exploited by active threat actors
- OSINT and dark-web intelligence integration
- Sector-specific attack scenario development
- Risk prioritisation using real-world exploit likelihood
- Continuous monitoring of threat feeds
- Manual validation of findings
- Detailed reporting with threat context
- Executive debriefs
- Optional ongoing threat intelligence service

KEY BENEFITS

- Testing aligned to your threat landscape
- Intelligence-led attack scenarios
- Accurate results using manual and automated techniques
- Faster remediation through prioritised insights
- Reduced remediation cost
- Clear executive-level risk translation
- Non-technical reporting for stakeholders
- Reduced likelihood of attacker exploitation
- Enhanced accuracy via threat intelligence

14. PENETRATION TESTING – VULNERABILITY SCANNING (NESSUS).

Expert vulnerability scanning using Nessus to identify weaknesses across networks, servers and applications. The service provides detailed risk analysis, prioritised remediation guidance and compliance assurance to strengthen security posture.

KEY FEATURES

- Automated Nessus scanning
- Identification of known CVEs
- Credentialed vulnerability scans
- Patch and outdated software assessment
- Misconfiguration detection
- Risk-based prioritisation
- Compliance checks against standards
- Detailed remediation reporting
- Manual validation of results
- Secure portal with real-time tracking

KEY BENEFITS

- Organisation-specific scanning
- Accurate results through validation
- Faster decision-making with real-time visibility
- Reduced remediation cost
- Lower exploitation risk through retesting
- Clear executive reporting
- Reduced downtime
- Improved vulnerability management

15. PENETRATION TESTING – VULNERABILITY SCANNING / ASV (QUALYS).

Vulnerability scanning and PCI ASV services using Qualys to identify weaknesses across internet-facing assets and internal estates. Supports PCI DSS compliance with prioritised remediation guidance, attestation and retesting.

KEY FEATURES

- Qualys-powered vulnerability scanning
- PCI DSS Approved Scanning Vendor (ASV) service
- Asset discovery and inventory
- Quarterly compliance scans
- CVE and misconfiguration detection
- Risk-based remediation prioritisation
- False-positive validation
- ASV attestation and dispute support
- Executive and technical reporting
- Rescans to confirm remediation

KEY BENEFITS

- Meets PCI DSS external scanning requirements
- Supports ongoing compliance
- Accurate attacker-view testing
- Reduced remediation cost
- Faster compliance decisions
- Clear evidence for assessors
- Reduced downtime
- Improved visibility of exposed systems

16. PENETRATION TESTING – WIRELESS TESTING.

Wireless penetration testing identifying vulnerabilities in Wi-Fi networks and access points. Combines manual and automated techniques with threat intelligence to uncover misconfigurations, prevent unauthorised access and protect sensitive data.

KEY FEATURES

- Wi-Fi configuration assessment
- WPA2/WPA3 and EAP testing
- Rogue access point detection
- Guest network isolation validation
- Weak encryption identification
- Credential harvesting resilience testing
- Wireless signal leakage analysis
- Manual validation of findings
- Threat-informed testing
- Secure reporting portal

KEY BENEFITS

- Tailored wireless testing
- Accurate and comprehensive results
- Faster remediation decisions
- Reduced remediation cost
- Lower exploitation risk
- Executive risk translation
- Clear reporting for stakeholders
- Reduced downtime
- Enhanced accuracy via threat intelligence

17. PENETRATION TESTING – EXTERNAL INFRASTRUCTURE TESTING.

External infrastructure penetration testing identifying vulnerabilities in internet-facing networks and systems. Combines manual and automated techniques with risk analysis to strengthen external defences and prevent cyberattacks.

KEY FEATURES

- External network vulnerability assessment
- Threat-informed testing approach
- Real-time vulnerability visibility
- Manual and automated testing
- Firewall and remote access testing
- Misconfiguration identification
- Testing against current exploits
- Customised assessment scope
- Prioritised risk reporting
- Compliance-focused testing

KEY BENEFITS

- Organisation-specific testing
- Accurate vulnerability identification
- Faster remediation decisions
- Reduced remediation cost
- Lower exploitation risk
- Executive risk translation
- Clear stakeholder reporting
- Reduced downtime
- Improved external security posture

18. PENETRATION TESTING – INTERNAL INFRASTRUCTURE TESTING.

Internal infrastructure penetration testing uncovering vulnerabilities within organisational networks and systems. Identifies misconfigurations and privilege escalation risks to strengthen internal defences and protect sensitive data.

KEY FEATURES

- Internal network vulnerability assessment
- Threat-informed testing approach
- Real-time vulnerability visibility
- Manual and automated testing
- Server and workstation assessment
- Privilege escalation testing
- Internal threat scenario simulation
- Customised assessment scope
- Prioritised reporting
- Compliance-focused testing

KEY BENEFITS

- Organisation-specific testing
- Accurate assessment results
- Faster remediation decisions
- Reduced remediation cost
- Lower exploitation risk
- Executive risk translation
- Clear stakeholder reporting
- Reduced downtime
- Improved internal security

19. PENETRATION TESTING – WEB APPLICATION TESTING.

Web application penetration testing identifying vulnerabilities and preventing cyberattacks. Includes OWASP-aligned assessments, risk analysis and practical remediation guidance to ensure secure, reliable application delivery.

KEY FEATURES

- OWASP Top 10 testing
- SQL injection and XSS protection testing
- Authentication and session management assessment
- API and web service testing
- Real-world attack simulation
- Risk-based remediation guidance
- Real-time vulnerability notification
- Custom testing scope
- Compliance and audit reporting

KEY BENEFITS

- Organisation-specific testing
- Accurate vulnerability identification
- Faster remediation decisions
- Reduced remediation cost
- Lower exploitation risk
- Executive-level reporting
- Clear stakeholder communication
- Reduced downtime
- Improved application security

20. PENETRATION TESTING – MOBILE APPLICATION SECURITY TESTING.

Expert mobile application penetration testing to identify security vulnerabilities in iOS and Android applications. The service combines manual and automated techniques with real-world threat intelligence to uncover flaws in code, APIs and data handling, helping organisations protect users, data and brand reputation.

KEY FEATURES

- iOS and Android mobile application penetration testing
- Manual and automated mobile security testing techniques
- Testing of mobile APIs and backend integrations
- Secure storage and data leakage assessment
- Authentication and authorisation weakness identification
- Mobile encryption and certificate handling validation
- Testing aligned to OWASP Mobile Top 10 risks
- Runtime analysis and reverse engineering techniques
- Expert validation of automated findings
- Secure client portal with real-time vulnerability visibility

KEY BENEFITS

- Tailored testing for your organisation
- CREST and CHECK certified experts
- Reduced risk of mobile data breaches
- Protection of sensitive user and business data
- Identification of real-world mobile attack paths
- Reduced remediation costs through prioritised findings
- Improved customer trust and brand reputation
- Clear reporting for technical and non-technical stakeholders
- Testing aligned to current mobile threat landscape
- Faster remediation through actionable recommendations