Introduction to the Cyber Security Services

"Empowering your business with proactive cybersecurity. We provide rigorous, real-world penetration testing to identify and remediate vulnerabilities before malicious actors can exploit them. Our comprehensive assessments give you the confidence and assurance needed to protect your critical assets, data, and reputation in an increasingly complex threat landscape."

Service 1: Internal and External Infrastructure Penetration Testing

Intro Blurb:

"Your network is the backbone of your operations. Our infrastructure penetration testing services delve deep into both your internal and external networks, simulating sophisticated attacks to uncover weaknesses that could lead to unauthorised access, data breaches, or operational disruption. We assess your perimeter defenses, internal segmentation, server configurations, and network devices to provide a holistic view of your security posture, ensuring your foundational IT infrastructure is fortified against both external threats and insider risks."

Key Benefits to Highlight:

- **Proactive Threat Mitigation:** Identify and fix vulnerabilities before attackers exploit them.
- **Compliance Adherence:** Meet regulatory requirements (e.g., GDPR, ISO 27001) for network security.
- **Business Continuity:** Prevent downtime and operational disruption from network attacks.
- **Reputation Protection:** Safeguard your brand by preventing data breaches.
- **Optimised Security Spend:** Focus remediation efforts on the most critical risks.

Service 2: Mobile Application (iOS and Android) Penetration Testing

Intro Blurb:

"In today's mobile-first world, your applications are often a direct gateway to your users and their data. Our mobile application penetration testing services for both iOS and Android platforms rigorously examine your apps for security flaws, insecure data storage, API vulnerabilities, and improper authentication mechanisms. We ensure your mobile presence is a secure and trusted extension of your business, protecting user privacy and maintaining brand integrity."

Key Benefits to Highlight:

- **User Trust and Data Protection:** Build confidence by demonstrating a commitment to mobile security.
- **Compliance with Mobile Standards:** Adhere to best practices for secure mobile development and being tested to OWASP Mobile Application Security Verification Standard (MASVS) standards
- **Prevention of Data Leakage:** Identify and fix flaws that could expose sensitive user data.
- **Enhanced App Reputation:** Avoid negative publicity and user churn due to security incidents.
- **Secure API Integration:** Ensure the secure interaction between your mobile app and backend systems.

Service 3: Web Applications and APIs Penetration Testing

Intro Blurb:

"Your web applications and APIs are frequently exposed to the internet, making them prime targets for cyberattacks. Our specialised web application and API penetration testing services go beyond automated scans, employing manual techniques to identify logic flaws, injection vulnerabilities, broken authentication, and insecure configurations. We ensure your ecommerce and critical data exchange points are resilient against the evolving threat landscape, safeguarding your customer data and business operations."

Key Benefits to Highlight:

- **Robust Data Protection:** Secure sensitive customer and business data transacted via web and APIs.
- **Prevent Financial Loss:** Mitigate risks of fraud and financial damage from web attacks.

- **Maintain Brand Credibility:** Avoid damaging security incidents that impact customer trust.
- **OWASP Top 10 Compliance:** Address the most critical web application security risks.
- **Secure Integration:** Ensure the integrity and confidentiality of data exchanged through APIs.

Service 4: Desktop Applications Penetration Testing

Intro Blurb:

"While often overlooked, desktop applications can harbour significant vulnerabilities that provide a foothold for attackers. Our desktop application penetration testing thoroughly assesses the security of your standalone or client-server applications, identifying weaknesses in areas such as local data storage, privilege escalation, insecure communications, and third-party library vulnerabilities. We help you secure these critical internal tools and protect the sensitive information they process."

Key Benefits to Highlight:

- **Internal Security Fortification:** Prevent lateral movement and privilege escalation within your network.
- **Protection of Sensitive Data:** Secure data processed and stored locally by desktop applications.
- **Compliance for Internal Systems:** Meet internal security policies and industry regulations.
- **Reduce Attack Surface:** Close potential entry points that could be exploited by malicious software.
- **Enhanced Software Integrity:** Ensure the reliability and trustworthiness of your desktop applications.

Service 5: Azure/AWS Cloud Security Reviews

Intro Blurb:

"Migrating to or operating in the cloud introduces a new set of unique security challenges. Our expert **Azure and AWS Cloud Security Reviews** provide a deep dive into your cloud configurations, identifying misconfigurations, insecure deployments, and non-compliance with best practices and regulatory frameworks. We assess your

Identity and Access Management (IAM), network security groups, storage configurations, logging, and other critical cloud services, ensuring your cloud environment is not only efficient but also robustly secured against evolving threats. With our review, you gain clarity on your shared responsibility model, enabling you to proactively strengthen your cloud posture and maximise the security benefits of these powerful platforms."

Key Benefits to Highlight:

- **Proactive Risk Identification:** Uncover misconfigurations and vulnerabilities unique to cloud environments.
- **Optimized Cloud Security Posture:** Ensure your cloud setup adheres to AWS/Azure best practices (e.g., AWS Well-Architected Framework, Azure Security Benchmark).
- **Compliance and Governance:** Help meet regulatory requirements (e.g., GDPR, ISO 27001, PCI DSS) within your cloud infrastructure.
- **Cost Efficiency:** Identify insecure over-provisioning or misconfigurations that could lead to unnecessary costs.
- **Enhanced Visibility and Control:** Gain a clear understanding of your cloud attack surface and shared responsibility model.
- **Reduced Attack Surface:** Limit potential entry points for attackers.

· **Basic Cloud Security Health Check (e.g., single account, limited services):**

- **Scope:** Review of core IAM, basic network security (VPCs/VNets, Security Groups/NSGs), logging (CloudTrail/Azure Activity Logs), and storage buckets/accounts against best practices (e.g., CIS Benchmarks).
- **Estimated Days:** 3-5 days
- **Estimated Price:** £3,000 - £9,000

· **Medium Cloud Security Review (e.g., multiple accounts, several applications/workloads, CI/CD pipeline review):**

- **Scope:** In-depth review of IAM policies, network segmentation, data encryption, container security, serverless functions, security monitoring tools, and potentially a review of Infrastructure as Code (IaC) templates.
- **Estimated Days:** 6-12 days
- **Estimated Price:** £6,000 - £21,000

· **Comprehensive Cloud Security Audit (e.g., large enterprise, multi-account, hybrid cloud, compliance-driven):**

- **Scope:** Covers all aspects of the medium review, plus deep dives into specific service configurations, compliance against specific frameworks (e.g., PCI DSS, HIPAA), incident response capabilities, and a review of DevSecOps practices. This might involve extensive stakeholder interviews and documentation review.
- **Estimated Days:** 15+ days
- **Estimated Price:** £15,000 - £30,000+

Pricing

Here are some ideas of prices, with data collected from market comparisons

External Network Penetration Test:

- **Small (1-5 IP addresses):** £550 - £1,500 (1-2 days)
- **Medium (5-20 IP addresses):** £1,100 - £3,000 (2-4 days)
- **Large (50+ IP addresses/complex):** £3,500 - £7,500+ (5+ days)

Internal Network Penetration Test:

- **Small (Up to 20 devices):** £1,800 - £3,000 (2-3 days)
- **Medium (21-100 devices/segmented VLAN):** £2,400 - £5,000 (3-5 days)
- **Large (100+ devices/multi-site/complex):** £4,250 - £10,000+ (5+ days)

· **Web Application Penetration Test:**

- **Small (Simple, less than 50 pages/basic authentication):** £3,000 - £6,000 (3-5 days)
- **Medium (E-commerce, multiple user roles, moderate API integration):** £6,000 - £12,000 (6-10 days)

- **Complex (Large enterprise app, extensive APIs, complex business logic):** £12,000 - £25,000+ (10+ days)

· **API Penetration Test:**

- **Small (Up to 10-25 endpoints):** £1,200 - £3,000 (2-3 days)
- **Medium (26-50 endpoints/multi-environment):** £2,600 - £5,000 (3-5 days)
- **Large (100+ endpoints/complex architecture):** £5,000 - £10,000+ (5+ days)

· **Mobile Application Penetration Test (iOS/Android):**

- **Typical Range:** £5,000 - £15,000 (depending on complexity, platform diversity, and API integration). This often translates to 4-10 days of effort.

· **Desktop Application Penetration Test:** Pricing for desktop applications can be less explicit online, but generally falls in line with the complexity of web/mobile apps. Expect it to be quoted based on an estimated day rate, similar to other application testing.

- **Small to Medium (Basic functionality):** £3,000 - £8,000 (3-7 days)
- **Complex (Extensive features, integrations, highly sensitive data):** £8,000 - £20,000+ (7+ days)

About the Consultants

Lastly, a nice intro into the consultants delivering the work

"Clients choosing our penetration testing services benefit from the assurance that all our consultants are **CHECK accredited** by the National Cyber Security Centre (NCSC), signifying their adherence to the highest standards for government and Critical National Infrastructure (CNI) systems. Furthermore, every consultant holds **NPPV Level 3 (Non-Police Personnel Vetting Level 3)** and **security clearance**, providing an unparalleled level of trust and enabling us to handle highly sensitive information and environments with the utmost discretion and integrity, including access to UK Secret and occasional Top Secret materials. We are unwavering in our commitment to **ethical penetration testing standards**, strictly operating within agreed-upon scopes, ensuring data confidentiality, and always obtaining explicit authorisation, guaranteeing responsible and professional engagement that prioritises your security and trust above all else."