|  |  |
| --- | --- |
| Service Catalogue | |
|  |  |
| Bramfitt Technology Labs | |
|  |  |
|  |  |
| Date: May 2025 |  |
| Reference: SCD-1468 |  |
| Version: 1.1 |  |



**Contents**

[1.0 Introduction 3](#_Toc198133756)

[**1.1** **Why Choose Bramfitt Technology Labs** 3](#_Toc198133757)

[**1.2** **Our Service Categories** 3](#_Toc198133758)

[2.0 Services Summary 4](#_Toc198133759)

[3.0 Service Descriptions 7](#_Toc198133760)

# **1.0 Introduction**

Bramfitt Technology Labs offers comprehensive cybersecurity solutions for diverse organisational needs, empowering businesses to proactively identify, prevent, and respond to evolving cyber threats. Our services span the entire cybersecurity spectrum, from threat assessment and vulnerability testing to strategic consulting and managed security services.

With our team of certified security professionals and cutting-edge technologies, you'll gain the expertise needed to protect your critical assets, ensure regulatory compliance, and maintain business continuity in today's complex threat landscape.

Our service portfolio combines proactive security assessments, strategic consulting, system integration, and ongoing managed services. Whether you need a one-time security assessment or continuous protection, we deliver tailored solutions that align with your business objectives and risk tolerance.

## **Why Choose Bramfitt Technology Labs**

• Comprehensive security solutions covering all aspects of modern cybersecurity

• Industry-certified professionals with extensive real-world experience

• Proven methodologies based on industry standards and best practices

• Customised approaches tailored to your specific industry and risk profile

• End-to-end support from initial assessment to ongoing management

• Advanced threat intelligence and cutting-edge security technologies

• Compliance expertise across multiple regulatory frameworks

## **Our Service Categories**

Cyber Assurance: Proactive security testing and assessment services to identify vulnerabilities before they can be exploited.

Cyber Consulting: Strategic advisory services to help design, implement, and optimise your security program.

Cyber Security System Integration: Implementation and integration of security solutions across your infrastructure.

Managed Security Services: Ongoing monitoring, management, and response services for continuous protection.

Custom Development: Tailored security solutions designed specifically for your unique requirements.

For comprehensive security solutions tailored to your organisation, contact a Bramfitt security advisor who will work with you to create a customised security strategy aligned with your business objectives and risk profile.

# **Services Summary**

| **Category** | **Service** | **Overview** |
| --- | --- | --- |
| **Cyber Assurance** | **Advanced Phishing Attack Simulations** | *Educate and empower your team to become your first line of defence against phishing attacks* |
| **Cyber Assurance** | **Cloud Infrastructure Attack Simulations** | *Identify vulnerabilities in your cloud environment - defend potential threats and protect your valuable data* |
| **Cyber Assurance** | **Infrastructure Attack Simulations** | *Test your network's defences against sophisticated cyber attacks - identify vulnerabilities before attackers do* |
| **Cyber Assurance** | **IoT, IIoT and OT Attack Simulations** | *Secure your connected devices against sophisticated threats* |
| **Cyber Assurance** | **Mobile Application Attack Simulations** | *Comprehensive dynamic, static, and interactive testing for mobile applications* |
| **Cyber Assurance** | **OSINT Assessment** | *Discover what your adversary knows about you - uncover exposed information before it's exploited* |
| **Cyber Assurance** | **Purple Team Program** | *Bridge offensive and defensive teams - enhance security through collaboration* |
| **Cyber Assurance** | **Red Team Assessments** | *Comprehensive adversarial simulation to test your security resilience* |
| **Cyber Assurance** | **Social Engineering Attack Simulations** | *Test your human firewall - identify vulnerabilities in your organisation's security awareness* |
| **Cyber Assurance** | **Vulnerability Assessments** | *Identify weaknesses before they become breaches - comprehensive vulnerability scanning and analysis* |
| **Cyber Assurance** | **Web Applications Attack Simulations** | *Secure your web presence - comprehensive testing of web applications and APIs* |
| **Cyber Assurance** | **Wireless Attack Simulations** | *Secure your wireless networks - test for vulnerabilities in your Wi-Fi and wireless infrastructure* |
| **Cyber Consulting** | **Application Security Consulting Service** | *Build security into your development process - establish secure coding practices* |
| **Cyber Consulting** | **Cyber Security Effectiveness Assessment** | *Measure and improve your security posture - comprehensive program evaluation* |
| **Cyber Consulting** | **IIoT / OT Security Architecture Review** | *Secure your industrial systems - comprehensive OT security architecture assessment* |
| **Cyber Consulting** | **Infrastructure and Cloud Security Architecture** | *Future-proof your security - comprehensive architecture review* |
| **Cyber Consulting** | **ISO 9001/27001 Consulting Service** | *Achieve certification with confidence - expert ISO compliance guidance* |
| **Cyber Consulting** | **PCI DSS Consulting Service** | *Protect payment card data - achieve and maintain PCI compliance* |
| **Cyber Consulting** | **Virtual CISO** | *Executive security leadership on demand - strategic guidance without the overhead* |
| **Cyber Security System Integration** | **Cloud Security Integration** | *Seamless cloud security - integrate protection across all cloud platforms* |
| **Cyber Security System Integration** | **Data Loss Prevention (DLP) Solutions Integration** | *Protect sensitive data - implement comprehensive DLP across your environment* |
| **Cyber Security System Integration** | **Endpoint Security Integration** | *Secure every device - comprehensive endpoint protection platform integration* |
| **Cyber Security System Integration** | **Identity and Access Management (IAM) Integration** | *Control access, protect identities - implement robust IAM solutions* |
| **Cyber Security System Integration** | **Incident Response Automation & Orchestration** | *Respond faster, reduce impact - automate your incident response* |
| **Cyber Security System Integration** | **Network Security Solutions Integration** | *Fortify your perimeter - integrate advanced network security solutions* |
| **Cyber Security System Integration** | **Secure DevOps (DevSecOps) Integration** | *Security at the speed of development - integrate security into your CI/CD pipeline* |
| **Cyber Security System Integration** | **Security Information and Event Management (SIEM) Integration** | *See everything, miss nothing - implement comprehensive security monitoring* |
| **Managed Security Services** | **Threat Intelligence Service** | *Stay ahead of emerging threats - proactive threat intelligence monitoring* |
| **Managed Security Services** | **Vulnerability Management Service** | *Continuous vulnerability monitoring and prioritised remediation guidance* |
| **Custom Development** | **Custom Secure Software Design and Development** | *Tailored security solutions - custom development with security built-in* |

# **Service Descriptions**

|  |  |
| --- | --- |
| **Category:** | Cyber Assurance |
| **Service:** | Advanced Phishing Attack Simulations |
| **Overview:** | Educate and empower your team to become your first line of defence against phishing attacks |
| **What We Offer** | |
| Phishing remains one of the most effective tactics in a cybercriminal’s toolkit, and today’s attackers, leveraging artificial intelligence, have become more sophisticated in their methods.  From spear-phishing to whaling, these targeted attacks can compromise even the most secure organisations by exploiting human vulnerabilities. Bramfitt Technology Labs offers advanced phishing attack simulations designed to test and strengthen your organisation’s resilience against these evolving threats.  Our simulations provide a realistic experience that helps your team recognise, respond to, and defend against sophisticated phishing attempts before they lead to security breaches.  Comprehensive Phishing Simulations Tailored to Modern Threats, BTL’s advanced phishing attack simulations are not just about sending a few generic emails to your staff; we design comprehensive campaigns that mimic the most cunning tactics used by attackers today.  Our service includes:   |  |  | | --- | --- | | **Simulation** | **Description** | | Spear-phishing simulations | Targeted attacks that impersonate trusted individuals or organisations to trick specific employees into revealing sensitive information or credentials. | | Whaling attacks | High-stakes simulations focused on senior executives and decision-makers, replicating scenarios that attackers use to gain access to privileged accounts or authorise fraudulent transactions. | | Smishing and vishing simulations | Testing your team’s response to text-based phishing (smishing) and voice-based phishing (vishing) attacks, which are increasingly common as attackers diversify their methods | | Clone phishing | Creating near-identical copies of legitimate emails with malicious links or attachments, challenging your staff to distinguish between real and fake communications. | | Customised training and awareness | Tailored educational resources and training sessions based on the results of the simulations, designed to boost your organisation’s phishing awareness and defensive capabilities | | |
| **Benefits** | |
| Our advanced phishing attack simulations go beyond basic security testing to create a security-aware culture within your organisation.  Key benefits include:   |  |  | | --- | --- | |  | | | Spear-phishing simulations | Targeted attacks that impersonate trusted individuals or organisations to trick specific employees into revealing sensitive information or credentials. | | Whaling attacks | High-stakes simulations focused on senior executives and decision-makers, replicating scenarios that attackers use to gain access to privileged accounts or authorise fraudulent transactions. | | Smishing and vishing simulations | Testing your team’s response to text-based phishing (smishing) and voice-based phishing (vishing) attacks, which are increasingly common as attackers diversify their methods | | Clone phishing | Creating near-identical copies of legitimate emails with malicious links or attachments, challenging your staff to distinguish between real and fake communications. | | Customised training and awareness | Tailored educational resources and training sessions based on the results of the simulations, designed to boost your organisation’s phishing awareness and defensive capabilities | | |