This is a chargeable service

Proactive Protection, Professional Precision

Red Team Services

Bytes' Red Team Services simulate real-world attacks to test your organisation's defences against Advanced Persistent Threats (APTs).

Our approach ensures robust security, providing strategic insights to fortify defences. **CREST-certified experts** deliver cutting-edge analysis and actionable insights, customising engagements to meet specific needs, from insider threats to physical security assessments.

In today's **complex threat landscape**, Red Team services are essential for uncovering weaknesses traditional assessments might miss, ensuring preparedness for sophisticated attacks.

Bytes are here to help maintain compliance with industry standards, customer trust, and legal requirements, while **reducing the risk of costly breaches** and **improving resilience** and **incident response effectiveness.**

Find out more about how Bytes can help you with our Red Team Services by contacting us today.

Key Steps

Overview
- Start with a consultation to understand your security concerns and objectives.

Evaluate
- Develop a tailored attack plan using advanced techniques such as social engineering, physical security assessments, and technical exploitation.
- To identify vulnerabilities and test your detection and response capabilities.

Follow Up
- Post-engagement we provide a detailed report with findings, risk levels, and remediation steps, along with continuous support to enhance your security posture.

What These Services Cover

Insider Threat Assessments:
- Evaluates the risks posed by malicious or compromised insiders, including scenario-based testing of insider threats.
- Simulates scenarios where attackers gain access to stolen laptops, smartphones, or other devices to assess data and corporate resources.

Hackers Health Check:
- Provides a realistic evaluation of your security posture by simulating an external hacker's perspective.
- This proactive approach helps you identify and address weaknesses before they can be exploited, reducing the risk of costly security breaches.

Phishing and Vishing:
Conducts targeted phishing (email) and vishing (voice) campaigns to evaluate employee awareness and response to social engineering attacks.

Physical Security Assessments:
Assessing physical security controls through attempted unauthorised access to facilities and sensitive areas.

Open-Source Intelligence (OSINT):
Gathering publicly available information to identify potential vulnerabilities and exploitation opportunities.

Advanced Persistent Threat (APT) Simulations:
Emulating the tactics of sophisticated threat actors to test your defences against long-term, targeted attacks.

+44 1372 418500 www.bytes.co.uk tellmemore@bytes.co.uk