wavenet cyberguard

EXECUTIVE SUMMARY

CyberGuard

Attack Simulation

Understanding the importance of threat-led testing in today's security landscape

With cyber dangers growing in complexity and scale, all organisations need to stay ahead of the potential threats – particularly those in financial services and critical national infrastructure (CNI) organisations.

Key industry insights:

Threat-led attack simulation has become a standard expectation for UK financial services and CNI sectors, with CBEST and TIBER-EU now adopted across most major institutions – and good practice for all.

BoE/ECB Programme Adoption Report, 2023

74% of UK organisations now cite threat-led testing as the most valuable assurance activity for executive-level cyber risk understanding.

DCMS UK Cyber Security Breaches Survey, 2024

Only 21% of organisations detected CREST STAR red team activity within the first 48 hours. Just 7% triggered full IR protocols.

NCSC/CREST STAR Testing Trends, 2024

On a positive note, the Bank of England CBEST Programme Review shows that 83% of CBEST organisations altered their incident response or detection workflows following Red Team testing, demonstrating a commitment to continuous improvement in security measures.

Choosing the right service for your needs

When evaluating security services, it's essential to understand the differences between Penetration Testing, Red Teaming, and Purple Teaming. Each offers unique benefits tailored to specific organisational needs:

Feature/ Focus	Penetration Testing	Red Teaming	Purple Teaming
Objective	Identify vulnerabilities and misconfigurations	Simulate a real-world adversary	Improve detection and response through collaboration
Approach	Open or credentialed testing of systems/networks/apps	Covert, multi-stage attack simulation	Real-time engagement between red and blue teams
Visbility to defenders	Often fully visible or partially coordinated	Covert – defenders are unaware (unless scoped)	Fully visible and collaborative
Scope	Pre-defined, technical	Objective-based, full kill chain	Iterative, focuses on visibility and improvement
Output	Vulnerability report with remediation advice	Strategic + technical report with timelines and risk context	Detection gaps, response effectiveness, uplift plan
Ideal for	Compliance, regular testing, baseline assurance	Assessing real-world resilience, board-level risk, regulated sectors	Improving SOC performance, tooling validation, training defenders
Timeframe	1–2 weeks typically	4 - 8 weeks	2 – 4 weeks, can be iterative
Example Engagments	Web app test, internal infra test, cloud config review	Domain compromise, phishing + lateral movement, data exfil	Phishing simulation + EDR visibility check, IR playbook walkthrough

Take action today!

As the landscape of cyber threats evolves, investing in the right security assessments is vital. Ensure your company is prepared and resilient against future attacks by choosing the service that best fits your strategic goals. Wavenet can help you with that. Let's work together to enhance your security posture and build a more protected future!

Let's talk

0344 863 3000

enquiries@wavenet.co.uk

wavenet.co.uk

wavenet cyberguard