CLOUDGUARD

ADVISORY

Red Teaming

Truly knowing your security effectiveness with a non-destructive assessment of cyber maturity & response

Service overview

CloudGuard's Red Team engagement provides a realistic, intelligence-led simulation of an advanced adversary, designed to test an organisation's ability to prevent, detect and respond to sophisticated attacks.

Unlike penetration testing, which focuses on vulnerabilities, Red Teaming measures resilience, detection capability, and response effectiveness across the entire kill chain.

A Red Team engagement answers the question: "Can an adversary achieve their objective against us, and how quickly would we know?"

It provides board-level assurance of real-world cyber resilience and gives the technical team detailed, actionable pathways to improve.

Key outcomes

•Realistic Adversary Simulation
•Emulates latest threat actor techniques
•Truly tests organisational defense performance
•Autonomous & Social Engineering attack paths
•Objective-driven scenarios to compromise

- **Readiness** – Test whether your controls and processes can withstand a genuine attack.
- **Responsiveness** – Learn how quickly your team would detect and react to attacker activity.
- **Resilience** – Evidenced route to reducing exposure over time.

Service value

Want to understand how your organisation would perform in the event of the real- world cyber event?

A Red Team event is an exceptionally powerful engagement which helps any business to understand and improve cyber defense performance by:

- Using the latest attack vectors & narrative to gain access, evade detection & defenses
- Escalated & enumerate privileges
- Move laterally
- Exfiltrate or distill identified data
- Test defense performance &responsiveness
- Help security teams to improve readiness, response & mitigations
- Repeat more frequently to continual improve security readiness

Why this matters now

Most security tests, such as Penetration testing, do not test or prove an organisations readiness or performance in the event of a real-world cyber event. Businesses face increasing challenges from AI adoption, user awareness and security team effectiveness to detect, protect & respond to minimise any business disruption.

CLOUDGUARD

Service outcomes

For the Organisation
Discovery & closure of critical vulnerabilities, weaknesses, misconfigurations and exploitation paths based on current & emerging Tactics, Techniques & Procedures (TTP's).

For the CISO or Security Officer
ATT&CK aligned maturity measurement with organisational security performance scoring, prioritised remedial action and improvement plans as well as Genuine testing or cyber resilience to help you sleep better at night!

For Security & IT Teams
Reproducible technical findings as well as improved detection and response recommendations, blue-team improvements and capability performance opportunities to enhance, audit based demonstrable evidence of testing.

For the C-Suite/Board
Real risk exposure and exploitation testing non-destructively to find any gaps, weaknesses or exposures BEFORE threat actors reducing business risks and impact. It is an independent validation of true cyber resilience.

For the Business
Engagement which simulates as close as possible real world TTP's and how an organisation performs and can improve. A platform which over team, when repeated can maximise an organisations performance under real world attacks.

Our approach

Delivered through a collaborative and supportive engagement:

- Executive Summary of Performance & Improvements
- Engagement Overview with Scope, Objectives, Constraints & customisations
- Full Attack Narrative including Attack Path mapping & learning
- Detection, Evasion & Response Assessment
- Strategic & Tactical improvement recommendations
- Continual improvement & Testing options to maximise response performance & learnings
- Option to Make it Purple where we Red Team alongside your Security & IT Teams
- Evidence mapping to detection engineering priorities, process & governance enhancements and further maturity steps.

Why CloudGuard

CloudGuard delivers enterprise-grade cybersecurity for growing businesses. Combining automation-led technology with UK-based experts, we provide 24/7 protection, without the complexity or cost of traditional platforms. Our fully managed approach simplifies detection, protection and improvement, so you can focus on growing with confidence.

Get in touch