CLOUDGUARD

ADVISORY

Purple Teaming

Truly knowing your security effectiveness with non-destructive assessment of cyber maturity & response. A Collaborative, partnership-based approach to identifying & resolving security risks to prove detection & response effectiveness.

Service overview

CloudGuard's Purple Teaming Service 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, Purple Teaming measures **resilience**, **detection capability**, and **response effectiveness** across the entire kill chain.

A Purple 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.

- **Readiness** – collaboratively test how your controls and processes perform against realistic attack activity
- **Responsiveness** – discover how your team detects, investigates and responds as a scenario unfolds
- **Resilience** – help you build lasting capability through direct knowledge transfer

Service value

A Purple 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
- Collaboratively delivered with proven mitigations, knowledge transfer & real-world response testing with experts.

Why this matters now

Red Teaming testing does test and prove an organisations readiness and performance in the event of a real-world cyber event. A Purple Teaming event takes this to the next level working with each organisation to identify the risk, mitigate the risk, complete knowledge transfer whilst improving security team experience and confidence. It is the closest thing to improving real world attack performance.

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. Working with your security team, we explain the attack vector, mitigation, retest and transfer expert security knowledge as well as improving security incident confidence 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:

1. Collaborative, partnership-based approach to identifying, resolving & retesting security weaknesses in real world scenarios.
2. Executive Summary of Performance & Improvements
3. Engagement Overview with Scope, Objectives, Constraints & customisations
4. Full Attack Narrative including Attack Path mapping & learning
5. Strategic & Tactical improvement recommendations
6. Continual improvement & Testing options to maximise response performance & learnings
7. 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