CLOUDGUARD

ADVISORY

# Red Teaming – BEC & AiTM

Truly understanding your resilience against modern phishing, Business Email Compromise & MFA bypass attacks

## Service Overview

Business Email Compromise & Adversary-in-the-Middle phishing attacks are among the most effective techniques used by modern threat actors to gain unauthorised access to corporate environments. By targeting authenticated user sessions rather than passwords, these attacks can bypass traditional MFA controls and enable rapid account compromise.

CloudGuard's Red Teaming BEC & AiTM engagement is designed to provide that assurance through a controlled, intelligence-led simulation of a modern phishing attack. By replicating the tactics, techniques and toolsets used by real-world threat actors.

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.

- **Readiness** – Know if your defences can stop a modern BEC compromise.
- **Responsiveness** – Test how effectively your teams detect and respond under pressure.
- **Resilience** – Build confidence that your organisation can withstand and recover from attack.

## Service Value

The Value the Red Teaming BEC AiTM Service Delivers:

- Validate resilience against real-world BEC and AiTM attack techniques.
- Identify weaknesses in user awareness, email security and identity controls
- Measure the effectiveness of security monitoring and detection capabilities.
- Assess incident response readiness during a live attack simulation.
- Gain evidence-based insight into actual organisational exposure and risk.
- Prioritise remediation activities to strengthen cyber resilience and reduce business risk.

## Why this matters now

As attackers increasingly target users and identities rather than infrastructure, organisations require greater assurance that security controls, monitoring capabilities and response processes can withstand modern phishing and account compromise techniques. Testing resilience against real-world attack scenarios is now a critical component of cyber defence.

CLOUDGUARD

# Red Teaming BEC AiTM Service Scope

Our Red Teaming engagement aligns to these six service components:

**Threat Intelligence & Reconnaissance**
Identify publicly available information, target users and attack paths that may be exploited by an attacker.

**Adversary Infrastructure & Campaign Preparation**
Deploy toolsets & prepare domain configuration. Develop realistic phishing scenarios and supporting infrastructure aligned to the agreed engagement scope

**Phishing-Led Attack Simulation**
Execute a controlled BEC and AiTM phishing campaign to assess organisational exposure and user susceptibility.

**Identity & Access Control Validation**
Evaluate MFA, Conditional Access and identity controls against modern account compromise techniques.

**Detection & Response Assessment**
Measure the effectiveness of security monitoring, alerting and incident response capabilities.

**Reporting & Remediation Guidance**
Deliver actionable findings, campaign metrics and prioritised recommendations to strengthen resilience.

# Our Approach

Delivered through a collaborative and supportive engagement:

**Engagement Initiation** - Confirm scope, objectives, target user groups and rules of engagement, register domain.

**Reconnaissance & Planning** - Identify target users, develop attack scenarios and prepare the engagement approach.

**Campaign Preparation** - Execute a controlled BEC and AiTM phishing campaign against user populations.

**Detection Assessment** – Assess monitoring, alerting and incident response effectiveness throughout the engagement.

**Report & Recommend** - Deliver findings, campaign metrics and prioritised recommendations to improve resilience.

**Data & Infrastructure Purge** – Digitally destroy all assets used during engagement.

## 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