CAMBRIDGE
CYBER ADVISERS

Cyber Red Teaming & Adversary Simulation

Service Definition Document. Version 1.0

14 January 2026

Cyber Red Teaming & Adversary Simulation

1. Introduction

This Service Definition Document describes the Cyber Red Teaming & Adversary Simulation service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides intelligence-led adversary simulation to test organisational resilience against realistic cyber threats.

Cyber threats don't follow a script, and neither should your security testing. Our Red Teaming service goes beyond traditional penetration testing, simulating real-world attacks by sophisticated adversaries to test your organisation's ability to detect, respond, and defend against a determined threat actor.

Using advanced tactics, techniques, and procedures, our expert operators conduct full-scale attack simulations, mirroring the behaviour of nation-state actors, cybercriminals, and insider threats. The objective isn't just to find vulnerabilities but also to test your entire security ecosystem, from technology and processes to human response and decision-making under pressure.

2. Service Overview

Cyber Red Teaming & Adversary Simulation delivers full-scope, covert attack simulations that replicate real-world threat actors. The service evaluates the effectiveness of people, processes, and technologies in preventing, detecting, and responding to advanced cyber-attacks.

This service delivers a realistic, end-to-end simulation of sophisticated cyber-attacks against an organisation’s cloud and on-premise environments. Using adversary tactics, techniques and procedures (TTPs), the service assesses the organisation’s ability to prevent, detect and respond to genuine threat scenarios.

Activities include:

- Threat intelligence analysis to identify relevant attack vectors
- Covert Red Team operations mirroring real-world threat actors
- Social engineering, phishing, network intrusion and lateral movement
- Testing SOC, SIEM, EDR and incident response capabilities
- Identification of vulnerabilities across people, process and technology
- Detailed reporting with prioritised remediation guidance
- Executive-level and technical debrief sessions

The service is conducted using formally agreed Rules of Engagement and ensures safe, controlled, compliant execution throughout.

Service Features

- Intelligence-led threat modelling based on sector and organisation risk
- Covert adversary simulation using advanced TTPs
- Physical, digital, and hybrid attack scenarios (optional)
- End-to-end attack pathway analysis
- Multi-vector Red Team operations (social, technical, cloud, identity)
- Detection and incident response evaluation
- CREST-aligned testing methodologies
- Comprehensive reporting with actionable recommendations
- Executive risk summary and technical remediation guidance
- Optional Purple Team follow-up exercises

Service Benefits

- Identifies unknown vulnerabilities exploited by real threat actors
- Improves organisational readiness and incident response capability
- Validates monitoring, alerting, SOC and detection controls
- Enhances employee awareness of social engineering and insider risks
- Provides evidence-based prioritisation for remediation
- Supports compliance with NCSC guidance, Cyber Essentials Plus and ISO 27001
- Informs strategic cyber investment decisions
- Improves cross-team collaboration between security, IT and leadership

3. Service Scope

The service includes but is not limited to threat intelligence analysis, attack scenario design, execution of red team operations, detection and response testing, and detailed reporting with remediation guidance. Activities may include social engineering, cloud compromise, identity attacks, lateral movement, and command-and-control simulation.

4. Delivery Methodology

All CCA engagements follow a phased approach using our standard methodology:

- Scoping and Rules of Engagement
- Threat Intelligence and Planning
- Red Team Execution
- Analysis and Reporting

- Executive and Technical Debrief

5. Deliverables

As part of the CCA Cyber Red Teaming & Adversary Simulation service, the following standard deliverables are provided:

- Executive Summary Report
- Technical Findings Report
- Attack Path Narrative
- MITRE ATT&CK Mapping
- Prioritised Remediation Roadmap
- Optional Purple Team Workshop Outputs

Additional deliverables can be agreed depending on requirements.

6. Service Levels

The standard CCA delivery SLAs are:

- Engagement commences within 10 working days of contract award
- Draft report within 10 working days of test completion
- Final report within 15 working days
- Weekly progress updates for longer engagements

Optional enhanced SLAs are available for accelerated engagements or continuous testing.

7. Governance and Assurance

All testing is conducted under agreed Rules of Engagement. Activities comply with legal, ethical, and safety requirements, and align with CREST and NCSC best practices.

Backup and Restore

Not applicable — this service does not handle customer production data or operate within customer systems in a way that requires backup/restore functionality.

Reporting & Analytics

Outputs include:

- Full attack narrative tracing each stage of compromise
- Detections observed (or missed) during the exercise

- Impact assessment mapped to assets and business functions
- MITRE ATT&CK mapping
- Executive summary with risk scoring
- Full remediation roadmap
- Evidence pack and IoCs (optional)

Incident Management

Controlled escalation paths defined in Rules of Engagement

- Clear stop/hold procedures
- Real-time escalation to customer security contacts if a genuine issue is detected
- Post-engagement incident response recommendations provided
- This service simulates attacks; it does not manage customer incidents.

Disaster Recovery

Not applicable — service is not hosted and does not rely on persistent operational infrastructure.

Availability

Service availability applies only to consultant scheduling. CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time with out-of-hours engagements available on request.

8. Security and Data Protection

Customer data is handled confidentially and securely. Data is retained only for the duration necessary to deliver the service and securely destroyed within 30 days of engagement completion. GDPR principles are applied throughout.

- All customer data handled under strict confidentiality
- UK-based testing team available
- Data stored and processed in secure environments
- Data retained for 30 days post-engagement then securely destroyed
- Compliance with GDPR, NCSC guidance, and ISO 27001-aligned practices
- No customer data transferred outside approved jurisdictions

GDPR & Data Privacy

- Personal data used only where strictly required (e.g., targeted phishing scenarios)
- Data minimisation applied
- DPIA support available where necessary
- All findings anonymised unless otherwise requested by customer

Accreditations

- CREST Registered Testers / Red Team Specialists
- ISO 27001-aligned internal management practices
- NCSC-aligned methodologies

Staff Security Clearance

SC cleared staff available on request. Baseline Personnel Security Standard (BPSS) checks conducted for all consultants.

9. Customer Responsibilities

Customers are responsible for providing accurate scoping information, nominating escalation contacts, supporting internal approvals, and implementing remediation actions.

Technical Requirements

- Defined scoping information (target systems, domains, cloud environments)
- Contact details for incident response and emergency halts
- Customer-supplied threat intelligence (optional)
- Access for briefing key stakeholders (security, IT, SOC)

No agent installation is required unless explicitly scoped.

Supported Browsers/Devices

Not applicable — this is a consultancy service, not a hosted software product.

Access Restrictions

Customer must designate authorised individuals for:

- Scope approval
- Rules of Engagement
- Emergency halt
- Receipt of confidential outputs

10. Service Constraints

Testing activities are limited to agreed scope and timeframes. Physical testing requires prior authorisation. Change freezes or restricted windows may apply.

- All activities require explicitly agreed Rules of Engagement
- Activities must comply with legal, ethical and safety constraints

- Customer must provide accurate escalation contacts and emergency halt procedures
- Physical testing requires property access permissions
- Testing may require change freezes or controlled windows in some environments

11. Pricing

Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:

- Scope and number of attack vectors
- Complexity of environments
- Duration of engagement
- Required stealth level
- Optional Purple Team follow-ups

Typical engagements range from 2–8 weeks.

Day-rate pricing is available on the pricing document and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering from clients is generally done via the presentation of a Purchase Order following confirmation of the purchase of a service. CCA will invoice at the end of every calendar month, giving a precise breakdown of the services purchased, including VAT/other expenses. CCA can provide consolidated invoices if required. Invoices can be issued electronically or via post.

12. Exit and Offboarding

At engagement end, all findings are delivered, knowledge transfer sessions completed, and customer data securely destroyed. Certificates of destruction can be provided.

Onboarding:

- Requirements workshop
- Definition of scope, assets, and Rules of Engagement
- Identification of critical assets, defensive technologies, and response processes
- Validation of communication protocols and escalation points

Offboarding:

- Full walkthrough of all findings
- Delivery of report, evidence and artefacts
- Remediation workshop (optional)
- Secure data destruction within 30 days post-engagement (certificate provided)

Training Provided

- Awareness session explaining Red Team methodology
- Incident response readiness briefing
- Optional tabletop exercises with leadership or IT teams
- Optional Blue Team uplift workshops (Purple Team mode)

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for continuous testing programmes.