G-Cloud 15 Service Definition Document

Red Team (Penetration Testing)

Executive Summary

The Red Team Assessment service provides a controlled simulation of real-world attack techniques to test an organisation's ability to prevent, detect, and respond to targeted threats. The service assesses both logical (cyber) and physical security controls, reflecting how modern attackers combine digital and physical methods to achieve their objectives.
Red Team activities are designed to evaluate the effectiveness of people, processes, and technology rather than individual systems in isolation. Testing is conducted against agreed objectives and scope, focusing on realistic attack paths that could lead to unauthorised access, data compromise, or operational disruption. The service can be used to validate existing security controls, assess incident detection and response capability, or support assurance activities following security improvements or organisational change.

About Inductive Solutions

We are a specialist consultancy delivering Cyber Security, Red Teaming, Cloud FinOps, and Predictive Intelligence. Founded by a veteran, we bring a disciplined approach to complex government challenges.

Our team is built on three core pillars:

1. **Strategic Command:** We apply proven leadership principles to bring order to complex programmes.
2. **Cybersecurity:** We integrate security into the foundation of every service, not as an afterthought.
3. **Data Science & Insight:** We model outcomes using data and facts, providing certainty in decision making.

Social Value & Corporate Responsibility

We are committed to delivering value beyond the contract:

- **Veteran founded:** We bring the ethos of service and discipline to our engagements.

- **Disability Confident:** We are committed to recruiting diverse talent to ensure we have varied perspectives required to solve complex challenges.
- **Armed Forces Covenant Pledge:** We are in the process of submitting our Armed Forces Covenant Pledge to formalise our support to the Armed Forces community.
- **Women in STEM:** We actively promote gender diversity to close the skills gap in technical roles.
- **Net Zero:** We are on track to achieve Net Zero by 2030 through sustainable business architecture and remote-first working practices.

Service Overview

The Red Team Assessment service provides a controlled simulation of real-world attack techniques to test an organisation's ability to prevent, detect, and respond to targeted threats. The service assesses both logical (cyber) and physical security controls, reflecting how modern attackers combine digital and physical methods to achieve their objectives.

Features and Benefits

Service Features

- **Logical (Cyber) Testing:** Adversary-led testing of network, cloud, and identity controls.
- **Objective-Based Testing:** Testing aligned to real-world threat actor behaviour and recognised frameworks (e.g., MITRE ATT&CK, OWASP).
- **SOC Evaluation:** Evaluation of security monitoring, alerting, and SOC processes.
- **Attack Path Assessment:** Assessment of external, internal, and social attack paths, including credential exposure, privilege escalation, and lateral movement.
- **Physical Testing:** Assessment of physical access controls, subject to agreed scope (e.g., building entry controls, tailgating, access procedures).
- **Physical-to-Logical:** Evaluation of physical-to-logical attack paths where permitted.
- **Rules of Engagement:** Rules of engagement agreed in advance to ensure safety and control.
- **Reporting:** Evidence-based findings, attack path documentation, and clear articulation of business impact and risk.

Service Benefits

- **Realistic Assessment:** Realistic assessment of organisational resilience to targeted attacks.
- **Gap Identification:** Identification of gaps in detection, response, and escalation processes.

- **Combined Weakness Analysis:** Improved understanding of how physical and logical weaknesses can be combined.
- **Validation:** Validation of SOC and incident response effectiveness.
- **Assurance Support:** Supports assurance activities for senior leadership, GRC, risk and audit functions, and regulatory compliance.
- **Security Culture:** Strengthens security culture through realistic testing and learning outcomes.

Our Methodology

Testing is conducted against agreed objectives and scope, focusing on realistic attack paths that could lead to unauthorised access, data compromise, or operational disruption.

Planning & Authorisation

All Red Team activities are subject to detailed scope and rules of engagement agreed in advance to ensure safety and control. Written authorisation is required prior to testing.

Execution (Logical & Physical)

We conduct adversary-led testing of network, cloud, and identity controls using real-world threat actor behaviour. Where agreed, this includes physical testing limited to specific locations, times, and scenarios (e.g., testing tailgating and staff vigilance). We evaluate physical-to-logical attack paths where permitted.

Reporting & Debrief

We provide evidence-based findings and attack path documentation, including a clear articulation of business impact and risk. The engagement concludes with post-engagement reporting and debrief sessions.

Onboarding and Offboarding

Pre-boarding Process

To ensure compliance from the start of the engagement we follow a standard pre-boarding protocol in preparation for project delivery.

1. **Compliance & Contracting:** Exchange of Contracts, NDAs, and Statements of Work via secure digital signing to prevent administrative delays.
2. **Security Vetting:** Pre-submission of all consultant details to the Client Security Controller to ensure site and network access upon start of project.
3. **Technical Access:** We provide a prerequisite list of technical access requirements to allow the client to issue IT permissions.

Onboarding Process

Our Onboarding process is designed to ensure our team is operational and delivers value from Week 1, without administrative delays:

1. **Success Criteria & Scope:** A formal workshop to introduce the team, define specific outcomes, Key Performance Indicators (KPIs), and boundaries of the project.
2. **Communication Schedule:** We establish a clear routine for updates, agreeing on the exact format and timing of reports to ensure transparency.
3. **Stakeholder Mapping:** We identify key decision-makers and subject matter experts required for interviews and data gathering.
4. **Evidence Gathering:** We move immediately into discovery and access logs, billing data, or legacy documentation to establish a factual baseline.
5. **Early Value Delivery:** We aim to deliver an initial findings report within the first few weeks (if applicable to the project scope).

Offboarding & Knowledge Transfer

We plan for offboarding from the start of the engagement. Our goal is to leave the client capable of managing the service independently, ensuring sustainable long-term value.

1. **Knowledge Transfer:** We conduct structured handover sessions with permanent staff to explain strategies, operational processes, or maintenance requirements. We focus on upskilling your internal teams to ensure operational independence.
2. **Documentation & Deliverables:** We provide a full handover of all contractually agreed outputs.
3. **Intellectual Property:** While the Client owns the specific deliverables created for them and specified in the contract, Inductive Solutions retains ownership of its methodologies, models and all other Intellectual Property. We do not transfer our proprietary internal tools or code libraries unless explicitly agreed to in the contract prior to the start of the engagement.
4. **Secure Data Deletion & Asset Return:** Upon project closure, we execute a secure data destruction process. Client data is permanently deleted from our systems in compliance with GDPR and government security standards, with a confirmation certificate provided if required. Any assets belonging to the client are dutifully returned.
5. **Closure Report:** We submit a final engagement report summarising the outcomes achieved, lessons learned, and recommended next steps.

Service Constraints & Requirements

- **Authorisation:** Written authorisation is required prior to testing.
- **Scope & Rules:** All Red Team activities are subject to detailed scope and rules of engagement.

- **Physical Testing Limits:** Physical testing is limited to agreed locations, times, and scenarios.
- **Destructive Testing:** System stress testing does not form part of the service unless specifically requested in the Scope of Works (SoW); this includes denial-of-service or destructive activities.
- **Findings:** Findings are based on conditions present at the time of assessment.
- **Remediation:** Remediation activities are not included unless explicitly agreed.
- **Timescale Variables:** The overall timescale depends on the scope and objectives of the assessment, number of locations and systems in scope, level of physical testing required, and coordination with operational and safety stakeholders.

Service Levels & Support

During a scheduled engagement, the expected response time is within 1 hour. Direct telephone contact details for the test engineer are provided during the engagement.

Standard Support Hours

Our standard support hours are 9:00 - 17:00 GMT/BST, Monday to Friday (excluding UK Public Holidays).
Support is available via:

- **Email:** For general enquiries, reporting, and non-urgent issues.
- **Phone:** For urgent matters and immediate escalation.

Account Management

Every engagement is assigned a dedicated Account Manager to ensure quality and alignment with strategic goals. Clients also have a direct escalation route to the Company Directors if required.

Security & Business Continuity

Security Vetting & Personnel

- **Clearance:** All consultants hold a minimum of BPSS (Baseline Personnel Security Standard) clearance. We can submit staff for SC (Security Check) and DV (Developed Vetting) clearances for sensitive engagements upon request, if sponsorship is provided by the Client.
- **Training:** All staff undergo regular security awareness training and data handling instruction.

Data Security and Encryption

- **Data Residency:** Client data is processed and stored within the United Kingdom and the European Union (EU), in full compliance with UK GDPR and the Data Protection Act 2018.
- **Data Sovereignty:** Strict Data Sovereignty (guaranteed processing and storage solely within the UK) is available upon request, subject to a minimum contract size.
- **Encryption:** We enforce strict encryption policy. All data is encrypted in transit and at rest to ensure confidentiality and integrity.
- **Secure Communication:** Standard email communication is secured via TLS. Enhanced End-to-End Encryption is available upon request, subject to a minimum contract size.
- **Accreditation:** We are Cyber Essentials certified, demonstrating our commitment to fundamental cybersecurity controls.

Business Continuity & Resilience

- **Cloud Native Model:** We operate a secure, cloud-native business model. We do not rely on physical on-premise servers or single-site infrastructure. This ensures that our services are resilient to physical site failures.
- **Remote Working:** Our systems and security architecture support secure remote working. In the event of a physical office disruption, our team can continue to deliver services remotely without operational downtime.
- **Backup & Recovery:** All critical business data is backed up securely in the cloud with redundancy to ensure data availability and rapid recovery.

Pricing

Pricing is directly linked to the Project Scope and complexity of the requirement.

- We work with the Client to define the specific deliverables and timeline.
- We estimate the resource effort required to deliver that scope.
- We apply the corresponding daily rates from our SFIA Rate Card to calculate the total engagement cost.

All daily rates are listed in our separate SFIA Rate Card (Skills Framework for the Information Age).Our daily rates are fully inclusive of all consultant overheads, equipment, software tools (except client systems), and insurance. We do not charge administrative fees.

Discounts

To deliver maximum value to the public sector, we offer the following discounts:

- **Educational Discount:** We offer a standard discount to schools, colleges, and universities (institutions with .ac.uk domains).

- **Volume Discounts:** Volume discounts are available for long-term engagements or large team deployments. These are applied on a sliding scale based on the total number of days purchased.