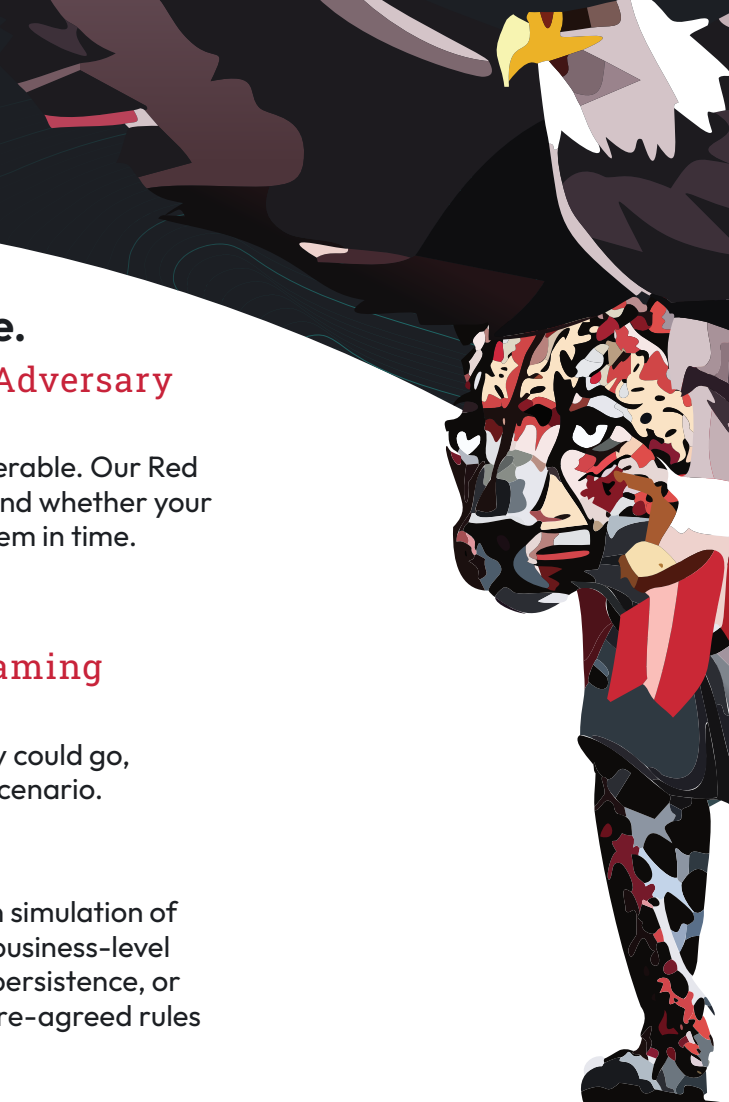


Red Teaming

See Your Organisation
Through an Attacker's Eyes





Moves in silence. Strikes with purpose.

Strengthen Your Defences with Realistic Adversary Simulation

Traditional vulnerability assessments tell you what is vulnerable. Our Red Team exercises show you what an attacker can achieve; and whether your people, processes and technology can detect and stop them in time.

Why Red Teaming

Traditional tests list weaknesses. Red Teaming shows impact

Know what a real attacker could accomplish, how far they could go, and how effectively your defences respond in real event scenario.

What Is a Red Teaming

A Red Team engagement is a controlled, objective-driven simulation of a real-world attacker. The exercise focuses on achieving business-level objectives - like accessing sensitive data, demonstrating persistence, or exfiltrating critical information - while remaining within pre-agreed rules of engagement.

Key characteristics

Objective-focused:

Realistic end goals rather than just finding vulnerabilities.

Multi-stage & stealthy:

Emulates an attacker's full kill-chain across time.

Detection & response testing:

Validates SOC monitoring, alerting and incident response playbooks.

Operational realism:

Uses tactics, techniques and procedures (TTPs) that adversaries use in the wild.

Red Teaming vs Penetration Testing

Outcome-driven

Exploits weaknesses to achieve attacker objectives.

Broader & adaptive

Evolves over time like a real adversary.

Defender-focused

Tests detection and response capabilities.

Actionable insights

Delivers evidence, detection gaps & priority fixes.

Checklist-driven

Identifies weaknesses and reports vulnerabilities.

Narrower scope, shorter timeline

Runs within a fixed, limited scope.

Focus on systems

Measures technical exposures.

Technical findings

Provides vulnerability lists.

Our Methodology

Scoping & Planning

Execution / Adversary Simulation

Reporting & Remediation

Follow-ups



1. Scoping & Planning

- Business objective alignment
- Risk appetite and exclusion list
- Rules of Engagement and safety controls

2. Execution / Adversary Simulation

- Multi-vector, multi-stage adversary simulation (technical, operational and approved social engineering)
- Controlled, reversible actions to avoid business disruption
- Continuous risk monitoring during the exercise

3. Reporting & Remediation

- Evidence-backed attack narrative and timeline
- Detection gap analysis with sample alerts and log excerpts (where permitted)
- Prioritized remediation roadmap & recommended playbook updates
- Executive summary and technical annex for engineering teams

4. Follow-ups

- Tabletop exercises for senior stakeholders
- SOC tune-up sessions and playbook workshops
- Targeted retests after remediation

Timeline & Engagement

4 weeks

Full-scope emulation, multi-goal objectives and progressive lateral movement.



Contact us

info@cybersift.io

+356 7949 8471 (MT)

+44 20 8638 0550 (UK)

Safety & Compliance

We prioritise business continuity, data protection and legal compliance.

Every engagement includes:

- Pre-agreed Rules of Engagement and exclusion lists
- Point-of-contact and escalation procedure
- Minimal-impact techniques where necessary and immediate stop mechanisms
- Secure handling and redaction of any sensitive evidence

Deliverables

- Pre-engagement scoping pack and RoE
- Real-time updates or controlled disclosure model, as per agreement
- **Final report:** executive summary, attack timeline, evidence appendix, prioritized remediation plan
- **Optional:** tabletop workshop, SOC tuning session, retest report

Pricing & Next Steps

Pricing is quoted per engagement based on scope, timeline and objectives.

Get started

- A short discovery call to confirm objectives, constraints and risk appetite
- Approval of Rules of Engagement and an exclusions list
- A concise proposal and statement of work

Protection Through Collective Intelligence

At Cybersift, we believe cybersecurity should be intelligent, accessible, and built to empower everyone.

Born from a fusion of research and real-world expertise, we transform advanced AI into clear, strategic protection - enabling every organization to stay secure and resilient.

Guided by our vision to make cybersecurity accessible to everyone and to serve as a protector for the unprepared, we stand as a trusted partner in a world where digital threats evolve faster than awareness.

We don't just protect systems - we protect confidence, continuity, and growth.

Protection, at its core, is not about standing alone - it's about standing together. Like in nature, where every instinct contributes to survival, our technology learns, adapts, and protects as one.

