Purple Teaming

GG-Could-15

Service Definition Document

2026-01-16

REVERSEC

16 January 2026

1 Purple Teaming

Reversec provides Purple Teaming services that actively simulate real-world cyberattacks to evaluate and strengthen your organisation's detection and response capabilities. Our proprietary tooling replicates up to 1,000 attacker techniques across the kill chain, delivering a holistic assessment of people, processes, and technology.

1.1 Service scope

This service validates an organisation's ability to prevent, detect, and respond to real-world threats by fusing offensive (red) and defensive (blue) practices in collaborative, intelligence-led exercises. It defines mission-relevant objectives, selects adversary TTPs (e.g., MITRE ATT&CK), and runs iterative scenarios across kill-chain stages: initial access, persistence, privilege escalation, lateral movement, and exfiltration. Controls, logging, detections, and response playbooks are tested and tuned in real time, with gaps triaged into quick wins and strategic fixes. Deliverables include a risk-prioritised report, mapped ATT&CK coverage, improved detections (Sigma/KQL examples where applicable), updated response procedures, and a retest window to verify remediation and uplift.

1.2 Service features and benefits

1.2.1 Service features

- Simulates targeted cyberattacks across multiple stages of the kill chain
- Proprietary tooling replicates up to 1,000 attacker techniques
- Assesses detection and response capabilities end-to-end
- Provides actionable recommendations for people, process, and technology
- Customisable engagements aligned to organisational threat profiles

1.2.2 Service benefits

- Accelerate risk reduction by identifying and remediating weaknesses
- Improves detection and response timeliness to minimise breach impact
- Strengthens overall security posture through defense-in-depth assessment
- Reduces long-term security costs via proactive improvements
- Supports compliance with industry standards and frameworks

1.3 Support

Standard project support is provided via email, phone, and optional secure chat—each available Monday to Friday, 9am–5pm (UK time). Additional Support provision can be agreed per project which may additional charge (please see price list).

CLIENT CONFIDENTIAL

1.4 Staff security

Staff are screened to BS7858:2019 standards, with personnel eligible for UK Government security clearances up to Developed Vetting (DV)

1.5 Project Management

Contracting with Reversec provides our client with a fully managed project planning and delivery process. To oversee the successful delivery of each engagement, Reversec shall assign an Engagement Lead for the duration of the engagement. Reversec Engagement Managers have various qualifications including PMP, AGILE, PRINCE2 and/or ITIL and follow industry best practices that can be aligned to match Our client preferred internal project management practices. The allocated Engagement Lead will also have relevant experience of delivering similar projects to global organizations across different industries and be able to proactively advise on delivery execution options.

1.6 Communication

Reversec provides a dedicated engagement manager as the primary contact during business hours, with immediate alerts for critical vulnerabilities. Clear, secure communication channels support real-time collaboration, while a structured communication plan ensures stakeholders receive timely, accurate, and actionable updates throughout the engagement

1.7 Quality Assurance

Reversec has been successfully assessed against the Council of Registered Ethical Security Testers (CREST) criteria for the ethical practice and supply of advanced cyber services; CREST regulations form a critical part of Reversec's own quality management processes and have informed the internal governance process.

1.8 Information Security

Our organization is committed to maintaining the highest standards of information security, in line with industry's best practices and regulatory requirements. As an ISO/IEC 27001:2022 certified company, we operate a comprehensive Information Security Management System (ISMS) that governs how we protect sensitive data throughout its lifecycle.