Attack Path Mapping

Service Definition Document
G-Could-15

2026-01-28

REVERSEC

28 January 2026

1 Attack Path Mapping (APM)

Attack Path Mapping gives you clear visibility into how adversaries can infiltrate your environment. By illuminating hidden pathways, prioritizing real risks, and strengthening critical controls, it empowers security teams to stay ahead of attackers. Turn complexity into clarity and transform your defensive strategy with actionable, threat-driven insights.

1.1 Service scope

This service analyses an organisation's digital environment to identify and map all feasible attacker pathways—from initial access to critical asset compromise. It includes assessment of configurations, identity relationships, network exposures, privilege escalation routes, and control gaps. Deliverables include a validated attack-path model, risk-prioritised findings, and actionable remediation guidance to reduce lateral-movement potential and strengthen overall cyber-resilience.

1.2 Service features and benefits

1.2.1 Service features

- Collaborative service, including interviews and workshops with key technical owners
- Understands and analyses an organisation's critical assets and processes
- Enumerates the likeliest paths attackers will take towards critical assets
- Assesses the effectiveness of security controls protecting critical assets

1.2.2 Service benefits

- Provides a complete picture of an environment's security posture
- Enables an organisation to prioritise security initiatives and investment accordingly
- Identify opportunities to build defense in depth
- Harden the network against likely attacker actions and high-risk objectives
- Facilitate holistic, risk-prioritised improvement initiatives

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 incur an additional charge (please see price list).

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

CLIENT CONFIDENTIAL