SAPPHIRE™

Threat-Led Penetration Testing Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

Threat-Led Penetration Testing (TLPT) is an enhanced and controlled security assessment to attempt to compromise the cyber resilience of a system or network by simulating the tactics, techniques and procedures (TTPs) of real-life threat actors.

Services features:

- Ensure safeguards are in place to respond to operational disruptions.
- Digital and physical attacks using data threat information reputable feeds.
- Create various scenarios from the data gathered to plan attack.
- Utilise OSINT techniques to gather external and internal infrastructure information.
- Adapt and evolve tactics based on real-time feedback and findings.
- Execute the attack phase across a defined period of time.
- Pre-Engagement Preparation, Reconnaissance, Threat Modelling, Planning, Execution and post-debrief.
- Diverse skill sets: offensive security experts, social engineers, technical specialists.
- TLPT is recommended as part of compliance for regulation such as DORA

Service benefits:

- Provide actionable recommendations to improve security posture.
- Use findings to enhance defences and refine security practices.
- Share insights and lessons learned across the organisation.
- Enhances defences by refining security practices based on real-world threats.
- Evaluates impact and likelihood of threats using risk-based insights.
- Tests operational resilience against advanced adversary tactics.
- Improves ability to resist, absorb, and recover from incidents.
- Validates safeguards for responding to operational disruptions.
- Strengthens readiness through intelligence-driven scenarios and real-time adaptation.
- Tests full attack surface including physical, human, and digital domains.

Functional and Non-Functional Detail

A Threat-Led Penetration Test (TLPT) is an intelligence-driven security assessment designed to emulate the tactics, techniques and procedures of real-world adversaries in order to evaluate an organisation's operational resilience. The process begins with detailed preparation and scoping, ensuring that testing focuses on systems supporting critical or important functions, including any in-scope third-party providers. This stage also establishes the necessary safeguards for conducting controlled activity on live production environments, as required under frameworks such as DORA and TIBER-EU.

Central to TLPT is the collection and analysis of high-quality Cyber Threat Intelligence (CTI). Intelligence teams identify likely threat actors, their motivations, capabilities, and historical behaviours, combining structured intelligence with external and internal OSINT gathering. This intelligence directly informs scenario development and threat modelling, enabling testers to design realistic attack paths rooted in genuine adversarial tradecraft. The result is a bespoke threat narrative that guides the test's execution.

Execution involves a multi-disciplinary Red Team simulating attacks across digital, human, and physical domains, adapting tactics dynamically as the engagement progresses. Testing typically runs over an extended period often involving a minimum period of active testing (e.g 12 weeks for DORA-aligned engagements), to fully explore the attack surface while avoiding operational disruption. Throughout, real-time risk management controls ensure that activity remains safe, measured, and appropriate for production environments.

Following execution, the TLPT a report with detailed analysis of findings, including the impact, likelihood, and exploitability of identified weaknesses. The report provides clear, actionable remediation guidance, enabling organisations to strengthen defences and enhance detection and response capabilities. Where required, outputs also form part of regulatory submissions, accompanied by summaries and remediation plans for relevant Competent Authorities. Beyond reporting, TLPT programmes often include validation and re-testing to confirm that remediation has been effective.

Underpinning the entire process are robust non-functional expectations: strong governance, regulatory alignment, skilled practitioners, and a commitment to operational resilience. TLPT demands rigorous quality assurance, secure handling of sensitive information, transparency with stakeholders, and the use of specialised teams with deep expertise in offensive security, CTI and engineering. These elements ensure that the engagement not only uncovers vulnerabilities but also provides meaningful, evidence-driven insight into the organisation's true resilience against sophisticated adversaries.

Adversarial Security Testing

As data breaches, ransomware incidents, phishing campaigns and broader security threats continue to rise, organisations increasingly require deeper, more comprehensive ways to assess their overall security posture. Human behaviour remains one of the most commonly exploited points in the attack chain, yet it is also the hardest element of the attack surface to measure or consistently control. The shift to widespread remote and hybrid working has further expanded this vulnerability, creating conditions that attackers can readily manipulate.

To address this, Sapphire has a number of adversarial security resting services that simulate real world threat actors, enabling us to evaluate an individual's susceptibility to manipulation and identify where human-centric weaknesses exist. These insights empower security leaders to shape strategies tailored to their organisation's specific risks whether that means targeted user education, the adoption of technical safeguards, or a combination of both.

Breach Attack Simulation

Our Breach Attack Simulation service is based on an assumed-breach approach, replicating the actions an attacker might take after successfully compromising a user—typically through social engineering techniques such as phishing. Because a real threat actor is likely to succeed at least once, the focus of this assessment is on how effectively your defensive controls can detect, contain, and eradicate malicious activity before significant impact occurs.

The exercise evaluates the strength of perimeter defences and supporting security technologies, with the expectation that certain stages of the attack lifecycle should be blocked. Testing is conducted under a grey-box model, enabling us to identify weaknesses arising from insecure configurations, flawed application logic, or architectural gaps. All activity is aligned to the MITRE ATT&CK Framework to provide clear mapping to recognised adversarial techniques.

During the simulation, Sapphire attempts to establish an initial foothold using common tools, tactics, and procedures, before exploring opportunities for lateral movement, privilege escalation, and—where feasible—execution of a controlled command-and-control payload. This approach highlights areas where additional controls, monitoring, or hardening may be required.

A key objective of the assessment is to test your organisation's resilience against data exfiltration attempts, as this remains a common tactic in ransomware and targeted intrusion scenarios. The scenario is split into two perspectives: first, an attacker operating on the network without credentials, and second, an attacker with user or administrative credentials (whether discovered or provided). This allows us to evaluate how easily sensitive data could be accessed or extracted,

and whether proxy enforcement, firewall egress filtering, and other security controls are functioning as expected or reveal exploitable gaps.

Physical Security Audit

Sapphire will conduct a comprehensive Physical Security Audit at the G-Cloud customer's premises to assess the organisation's resilience against non-technical threats. This engagement focuses on how effectively physical controls and human behaviours protect sensitive information, including the use of social engineering techniques designed to encourage employees to bypass established security procedures.

Human factors continue to represent one of the most challenging elements of any security programme. Many employees are unaware of the value of the information they handle, struggle to keep pace with technology-driven environments, or inadvertently adopt risky behaviours. As a result, sensitive data can be exposed through simple oversights such as the disposal of confidential documents, the selection of easily guessed passwords, or susceptibility to techniques like shoulder surfing and impersonation. Strengthening awareness and fostering a positive security culture are therefore essential to effective prevention.

During the audit, Sapphire conducts an on-site evaluation of physical security measures, staff practices, and the wider security culture. This may include reviewing access controls, observing how sensitive information is handled, assessing the effectiveness of existing physical safeguards, and identifying any gaps or weaknesses either within the customer's own environment or across recently acquired sites. The purpose of the assessment is to provide an informed snapshot of how well employees understand and uphold their security responsibilities, and to highlight areas where additional education, improved processes, or enhanced physical controls may be required.

Several of the following elements may be included within the Physical Security Audit:

- Physical access control vulnerabilities (Credential cloning, bypasses)
- Mechanical lock and door security (resistance to lock picking or door bypass techniques)
- Physical network related vulnerabilities (exposed RJ45 ports, unlocked workstations, etc)
- Staff security procedures (tailgating awareness, challenge culture)
- OSINT related risk (badge replication, internal building photos)
- CCTV coverage, weaknesses or blind spots.
- Audit of locked areas inside the building.
- Attempt breach of secure areas.
- Attempt removal of sensitive paperwork

- Observe/audit existing clear screen/clear desk policy.
- Desktop snooping and shoulder surfing exercises.
- Attempt to obtain confidential waste in bins situated in the office.

Sapphire will provide a report that summarises the findings as observed over the audit day and includes recommendations which the customer may wish to consider implementing because of the exercise.

The reconnaissance phase is key and ahead of the audit attempt, Sapphire will determine the best approach for a successful audit. This may be creating a fake badge to try and bypass reception or the form of a guise to gain unauthorised entry. The reconnaissance is in two parts, the planning stage in advance of the audit and the day prior to the audit to conduct a physical walkthrough of the perimeter.

A letter of authority will be created so the auditor will have proof that the exercises has been approved by G-Cloud customer. It is important that minimal people are aware of the exercise and one named point of contact is to be provided.

Open-Source Intelligence

The Open-Source Intelligence (OSINT) service involves the collection, collation, and analysis of information obtained entirely from publicly accessible sources to support intelligence-led decision-making. Every individual and organisation creates a digital footprint a trail of online activities, actions, and communications captured across the internet and digital devices. These footprints fall into two categories: passive, where information is gathered without the user's awareness, and active, where individuals intentionally publish personal data through websites, social media platforms, or online services.

Sapphire employs a range of specialist tools and techniques to gather and process this information securely. All research traffic is fully encrypted and anonymised to maintain operational confidentiality throughout the assessment. The resulting intelligence can be used to enhance user awareness initiatives or support corporate training by providing tailored recommendations and expert guidance.

Although the information identified is publicly available, the analysis may reveal sensitive insights about individuals or the organisation. As a result, access to the gathered intelligence is strictly limited to the authorised OSINT delivery team to ensure it is handled responsibly and securely.

For G-Cloud customer, we can complete a threat intelligence review to check for any corporate or executive information on the web and dark web. Sapphire will search third party companies for any data breaches, in particular we will complete a 'deep' search checking for:

- Search Configuration Documents
- User Credential Captures
- Social Media Review
- Domain Squatting

We will collect data and complete the review over an agreed period.

The OSINT report will typically include:

- Commercial Profile
- Social media footprint and exposure
- Company Reviews
- Company Search Engine Results
- Company Document Search Results
- Company in The News
- Company within other Documents
- URL Results
- Sub Domains and Mock Domains
- Company Business Records
- Email Breach Data
- Users Associated to Company and Social Media

Sapphire's Certifications and Associations