PEN TEST PARTNERS

G-Cloud 15

Lot 3 Cloud Support – Security Services Definition Document – Red Team Testing

Version 1.0

Contact: bidteam@pentestpartners.com

Commercial in Confidence

Table of Contents

Your Trusted Partner

Penetration Testing

- Regulated CHECK Testing
- Infrastructure Testing
- Web, API & Mobile App Testing
- Compiled App Testing
- Application Code Reviews
- Cloud Threat Actor Simulation
- DevOps & CI/CD
- Kubernetes & Containerisation

Bespoke Services

- Regulated Red Teaming (CBEST, GBEST, STAR-FS, TIBER)
- Purple Teaming
- Cyber & Physical Social Engineering
- OT & ICS Security Testing
- Attack Surface Management / Assessment
- IoT, IIoT & Hardware Testing
- Aerospace & Satellite
- Maritime, Rail & Automotive Cyber Security

Digital Forensics & Incident Response

- Incident Response (email compromise, data exfiltration & recovery, e-discovery, root cause & impact)
- Digital Forensics & Expert Witness
- IR Maturity Assessment
- Compromise Assessments
- First Responder Training
- Ransomware Assessments
- Identity Risk Assessments

GRC Consultancy

- Architecture & Secure Design
- Cloud Review & Support
- Gap Analysis & Maturity Assessment
- PCI Consultancy (SAQ Support & ASV Scanning)
- vCISO Services
- Business Continuity Planning & Disaster Recovery
- Tabletop Exercise & Simulation
- ISO27001 Gap Analysis & Implementation
- Cyber Essentials (Plus)
- CAA Assure / Gov Assure
- Vulnerability Management
- Security Awareness

About Us

Pen Test Partners (PTP) has been providing cyber security expertise to a huge variety of industries and businesses since 2010. We are the largest independent security testing and consultancy business in the UK with over 150 employees across the UK and US. PTP tests the security of all computer and internet connected devices, applications, software, hardware, operational technologies (OT / ICS) & cloud services. The security testing team is supported by experienced consultants specialising in ISO 27001, PCI, Cyber Essentials and vCISO amongst others. The PTP offering is completed by an NCSC CIR Standard Digital Forensic Incident response (DFIR) capability.

As one of the founding members of the CREST scheme in the UK and US and as a previous CVE board member, we have helped to shape cyber security standards and frameworks like CBEST. Through our CBEST accreditation we are regulated by the Bank of England (BoE) and Prudential Regulatory Authority (PRA) and through our CHECK accreditation we are closely aligned to the National Cyber Security Centre (NCSC) Framework.

We are one of just a few providers accredited with the coveted CBEST UK Threat Intelligence Led Penetration Testing standard which allows us to test on behalf of British Government (GBEST/GCASE) and the Bank of England/FCA (CBEST/STAR). We are also approved by the Civil Aviation Authority to provide ASSURE services.

Our applicable certificates to deliver our clients with best-in class cyber security services include CHECK, CREST, CBEST, STAR, TIBER, PCI QSA, Cyber Essentials Plus, ASSURE and NCSC CIR Standard. We are also ISO 27001 certified across our entire business operations.

Service Definition Overview

This document set out the range of Red Team Testing Services offered by the PTP Red Team. Services can be purchased individually or grouped based on our clients' specific needs.

Definitions

Full Chain vs. Phased

A full chain engagement is one in which follows all phases, from start to finish, of the Lockheed Martin Kill chain or Mitre ATT&CK framework. It is an indicator that the engagement is end-to-end.
A phased engagement is one in which has been split up into either multiple smaller engagements or select phases have been chosen from a typically larger assessment. This may be done for budgetary, availability or client scheduling requirements as well as other factors such as specific client requirements.
An example of each is a standard (unregulated) Red Team assessment, which is end-to-end. Beginning with OSINT, followed by external compromise, phishing onto endpoint compromise or internal network access followed by demonstrating access and achieving objectives. A client may only want to simulate an insider threat and therefore we can provide the phased engagement of a "malicious insider review/ assumed breach", which assumes compromise and therefore only assesses the internal and final phases of a typical Red Team assessment.

Chained

A chained engagement is one in which multiple services or service lines have been combined. This is most often seen with the combination of security awareness or a Phased Objective-Based Purple Team to the end of a Red Team. Other examples may be a Covert Intrusion Assessment, part of the Physical Social Engineering service, combined with a Red Team assessment or Cyber Social Engineering services like Phishing.
Guidance on what services can be chained can be found here.

Joint Services

A joint service is a service which is cross charged with the other PTP delivery pillars. This means that DFIR, Consultancy, Penetration Testing and PTP as a whole can collaborate within these engagements.

Red Team (RT)

Red Team operations are intelligence-led, objective-based, real-world simulations that emulate attacker tactics, techniques and procedures (TTPs) to give an organisation a holistic view of their security posture.

Red Team engagements are black box and performed covertly in coordination with a small team from the target organisation.
Red Team operations enable specific evaluation of an organisation's security awareness, security posture, external and internal technical security controls, endpoint and internal detection capability, telemetry efficacy, and incident response; amongst other, more idiosyncratic benefits per engagement.

Service Lines

- Regulated
  - CBEST, GBEST & TBEST
  - GCASE
  - STAR-FS
  - TIBER
  - AASE
  - iCAST
- Standard (Unregulated)
- Phased
  - External Breach (CybSE or PhySE+)
  - Internal Assumed Breach
  - Custom

Service Features

- Adheres to industry and regulatory standards.
- Simulates real-world threat scenarios.
- Incorporates intelligence-led tactics and TI providers.
- Offers both regulated and unregulated testing options.
- Longer, broader and more realistic than traditional penetration testing.
- Some services can be divided into specific, customisable phases.
- Includes a variety of testing methods (OSINT, social engineering, etc.).
- Overseen by experts and regulatory bodies when required.
- Focuses on both external and internal security vulnerabilities.
- Provides comprehensive security assessments and debriefings.

Service Benefits

- Ensures compliance with relevant regulations.
- Enhances overall security posture and resilience.
- Reveals vulnerabilities and attack paths across the organisation.
- Improves incident response and risk management capabilities.
- Boosts stakeholder confidence and industry reputation.
- Tailors to specific organisational needs and priorities.
- Provides actionable insights for security enhancements.
- Reduces the risk of security breaches and attacks.
- Encourages investment and a proactive security culture within the organisation.
- Supports continuous improvement and adaptation to new threats.

50 Words

Red Team operations are intelligence-led, objective-based, real-world simulations that emulate attacker tactics, techniques and procedures (TTPs) to give an organisation a holistic view of their security posture and readiness. Red Team engagements are black box and performed covertly in coordination with a small team from the target organisation.

Regulated

A Red Team Assessment that adheres to the specifications for a particular regulated framework. A typical Red Team Operation, often with varying requirements or scenarios. PTP are CREST accredited and are capable of running *BEST, STAR-FS, TIBER, AASE and iCAST. PTP work alongside Threat Intelligence providers and a regulator oversees the assessment. The assessments are aimed at identifying risks for the organisation and providing insight for the regulator.

Features

- Adheres to specific regulatory frameworks and ensures compliance.
- CREST-accredited operations including BEST, STAR-FS, TIBER, AASE, iCAST, DORA.
- Involves various real-world testing scenarios.
- Engages with Threat Intelligence providers.
- Overseen by regulatory bodies.
- Designed and tailored for regulated industries requiring strict adherence.
- Focuses on identifying critical risks and improving organisational resilience.
- Provides regulatory compliance insights.
- Enhances and evaluates organisational security posture.
- Aids in strategic security planning and continuous improvement.

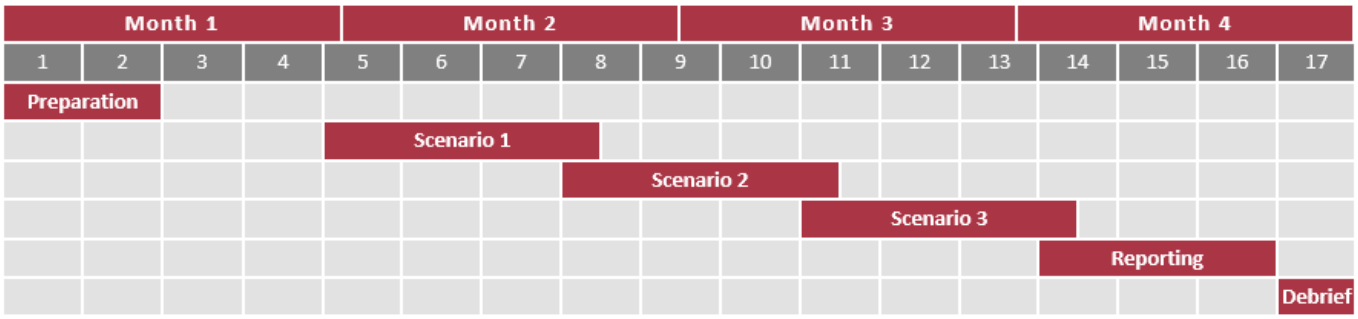
Benefits

- Ensures regulatory compliance and provides clear regulatory insights.
- Boosts stakeholder confidence.
- Offers targeted risk assessment.
- Enhances incident response capabilities.
- Drives continuous improvement.
- Supports compliance audits.
- Mitigates potential fines and penalties.
- Strengthens industry reputation.
- Sparks investment in security

Outcome

- A project plan and Red Team playbook prepared by the Red Team Manager including
  - An Intelligence scoping document, draft and final cyber threat intelligence document
  - Scenario discussion deck
- An end-to-end engagement with communication to the organisation control group including
  - Weekly update documents
- A comprehensive draft and final report detailing:
  - A full breakdown of all findings identified
  - Detailed remediation advice
  - High-level management summaries
  - ‘Attack flow diagrams’ showing a breakdown of the Red Teams actions
  - A detailed chronological attack narrative
  - Indicators of Compromise
- A 2 hour virtual executive debrief containing high-level overview and full technical breakdown.
- Alongside this the organisation and CTI provider will prepare reports that are aggregated into an executive summary report.

Pricing and Scoping



Regulated Red Team Assessment	Delivery Days
Project Preparation and management • Testing plan and risk management • Scenario / Playbook Generation	5
Scenario 1	30
Scenario 2	30
Scenario 3	30
Reporting	15
Debriefs and updates	10
TOTAL	**120**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Table Top Exercise	5
Physical Social Engineering	10
Phased Objective Based Purple Team Exercise	20

Regulatory adjustments:

- For GCASE and STAR-FS only one scenario is necessary.
- For *BEST, DORA and TIBER the minimum is three scenarios.

Standard (Unregulated)

Our standard Red Team offering is an intelligence-led end-to-end exercise aimed at demonstrating attacks that would be performed by real-world threats. It is designed to bring visibility to areas of risk within a business and to assess the ability to defend against a realistic threat.

Features

- Simulates realistic threat scenarios.
- Intelligence-led and comprehensive for a single attack path.
- Evaluates end-to-end security.
- Unrestricted by regulatory frameworks.
- Reveals vulnerabilities and risks.
- Tests against real-world threats.

- Flexible in approach and scope.
- Suitable for diverse organisations.
- Includes post-operation debriefing.
- Can be used before a regulated tests for preparation.

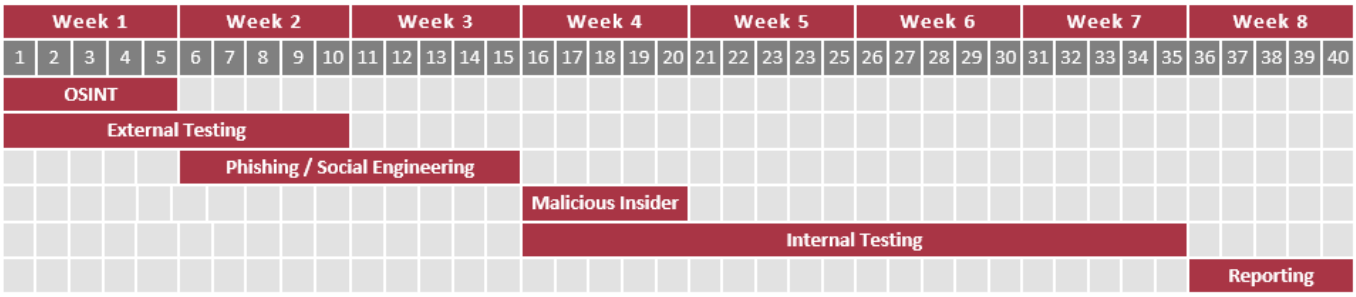
Benefits

- Reveals risks and vulnerabilities that may have been previously overlooked.
- Improves defensive strategies.
- Enhances cybersecurity awareness.
- Facilitates proactive security posture.
- Customisable to business needs.
- Provides actionable insights into risks.
- Encourages investment in security culture.
- Prepares for unknown threats.

Outcome

- An end-to-end engagement with communication to the organisation control group.
- A comprehensive report detailing:
    - A full breakdown of all findings identified
    - Detailed remediation advice
    - High-level management summaries
    - 'Attack flow diagrams' showing a breakdown of the Red Teams actions
    - A detailed chronological attack narrative
    - Indicators of Compromise
- A virtual debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



Red Team Assessment	Delivery Days
OSINT (Open Source Intelligence) / Reconnaissance	5
External Testing	5 – 10+
Phishing Campaigns	5 – 10+
Assisted Foothold	0 (included)
Internal Testing	10 – 35+
Malicious Insider Review	0 (included)
Reporting	5
Project management, debriefs and updates	4
TOTAL	**34 – 69+**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10
Phased Objective Based Purple Team Exercise	10 - 20
Project Preparation and management • Testing plan and risk management • Scenario / Playbook Generation	5

Phased

A Red Team exercise can be phased into typical or custom packages. Often organisations will want to address the risk of initial compromise and so OSINT, external testing, social engineering and endpoint testing will be combined into a single test. Another type of phased test is the insider threat/malicious insider or assumed breach.

Features

- Divisible into specific phases.
- Addresses initial compromise risks.
- Incorporates varied testing types.
- Targets insider threats effectively.
- Adaptable to organisational changes.
- Detailed at each security layer.
- Focuses on critical security controls.
- Identifies phase-specific vulnerabilities.
- Customisable to phase objectives.
- Strategic testing of key assets.

Benefits

- Allows focus on critical areas or most concerning.
- Supports iterative security enhancements.
- Provides deep dive into phase-specific vulnerabilities.
- Facilitates comprehensive risk management.
- Adapts to evolving threats.
- Adaptive for constrained budgets or schedules
- Sparks security investment.

Outcome

- A phased engagement with communication to the organisation control group.
- A comprehensive report detailing:
    - A full breakdown of all findings identified during that phase
    - Detailed remediation advice
    - High-level management summaries
    - ‘Attack flow diagrams’ showing a breakdown of the Red Teams actions
    - A detailed chronological attack narrative
    - Indicators of Compromise

- A virtual debrief containing high-level overview and full technical breakdown.

Pricing and Scoping

External Breach (CybSE or PhySE+)

External Breach (CybSE or PhySE+) Red Team Assessment	Delivery Days
OSINT	5
External Testing	5 – 20+
Physical SE	2
Phishing/Cyber SE	5
Internal Testing	4 – 10+
Reporting	5
Project management, debriefs and updates	2
TOTAL	**28 – 49+**

Additional Optional Test Elements:

Optional Test Element	Days
Security Awareness	2
Phased Objective Based Purple Team Exercise	10 - 20
Project Preparation and management • Testing plan and risk management • Scenario / Playbook Generation	5

Internal Assumed Breach

Assumed Breach Red Team Assessment	Delivery Days
Assumed Breach / Malicious Insider • Malicious Insider • Internal Testing	15 – 30+
Reporting	5 - 10
Project management, debriefs and updates	2
TOTAL	**22 – 42+**

Additional Optional Test Elements:

Optional Test Element	Days
Security Awareness	2
Phased Objective Based Purple Team Exercise	10 - 20
Project Preparation and management • Testing plan and risk management • Scenario / Playbook Generation	5

Custom

Or a combination of chronological phases from the following table:

Custom Red Team Assessment	Delivery Days
OSINT (Open Source Intelligence) / Reconnaissance	5
External Testing	5 – 20+
Physical SE • Covert or Overt • Optional Wireless Security Breach	2 - 10
Cyber SE (Phishing, Vishing, Smishing)	5 – 10+
Internal Testing • Assisted Foothold / Malicious Insider Review if separate	10 – 40+
Reporting	5
Project management, debriefs and updates	4

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Table Top Exercise	5
Domain Password Audit	3
Phased Objective Based Purple Team Exercise	10 - 20
Project Preparation and management • Testing plan and risk management • Scenario / Playbook Generation	5

Purple Team (PT)

Purple Team engagements are collaborative simulations of a variety of attack vectors. Using varied sophistication and TTPs, the Red Team consultants can identify which attacks bypass current technological, procedural and personnel controls, and which are prevented, detected and responded to.
Through daily workshops, the Blue Team and Red Team can establish the efficacy of the controls and provide metrics or risk insights around the attempted attack vectors. Ultimately allowing an organisation to map attack paths, identify gaps in controls and become aware of wider security issues.

Service Lines

- Standard (FLIP)
- Metric Based
- Objective Based
- Phased
    - Cloud
    - Development
    - Endpoint & EDR
    - AI / ML
    - Custom

Service Features

- Follows structured frameworks like FLIP for comprehensive assessments.
- Allows division into specific, focused engagements or phases.
- Includes diverse focus areas like cloud, endpoint, and AI/ML.
- Evaluates controls across technology, procedures, and personnel.
- Facilitates daily interactions between Red and Blue Teams.
- Captures all activities, outcomes, and recommendations in detailed documentation.
- Provides metrics on the efficacy of security controls.
- Offers both high-level summaries and detailed technical analysis.
- Generates and tests bespoke tactics, techniques, and procedures.
- Delivers actionable recommendations for improving security controls and responses.

Service Benefits

- Enhances overall security posture and resilience.
- Focuses on critical areas needing attention and enhancement.
- Raises organisational understanding of vulnerabilities and attack vectors.
- Assists in refining EDR/MDR, SOC capabilities, and other defences.
- Engages key personnel in security enhancement processes.
- Establishes baselines for ongoing assessments and improvements.
- Facilitates continuous learning and adaptation to real and emerging threats.
- Ensures security efforts align with organisational goals and risks.
- Provides specific recommendations based on attack paths for closing security gaps.
- Optimises resource allocation to high-risk areas.

50 Words

Purple Team engagements are collaborative simulations of various attack vectors. Using varied sophistication and TTPs bespoke to the environment, prevention, detection and response can be measured and plotted to show possible attack path maps. The efficacy of technological, procedural and personnel controls can be shown alongside gaps and risks.

Standard (FLIP)

The standard Purple Team offering follows the PTP Framework for Intelligence Led Purple Teaming (FLIP). The framework features an initial consultancy phase consisting of a controls audit, threat modelling, stakeholder meet & greets alongside derivation of the testing TTP set.
The Red Team will host daily workshops to evaluate prevention, detection, and response capabilities against simulated attacks for the deployed technological, procedural and personnel controls. This collaboration and resulting analysis and reporting provides guidance around security controls and response strategies, evaluates control effectiveness, and provides actionable recommendations. The assessment provides both high-level summaries and in-depth technical analysis, ensuring all stakeholders understand the security posture, attack paths that are possible, current gaps, and improvement strategies.
The standard offering is an expansion of the metric based purple team and includes elements of the objective based exercise. The assessment can be split into phases.

Features

- Follows PTP's bespoke Framework for Intelligence Led Purple Teaming (FLIP).
- Begins with a controls audit and threat modelling.
- Includes stakeholder interactions early in the process.
- Develops a set of bespoke TTPs for the engagement.
- Provides comprehensive engagement summaries and maturity metrics.
- Daily workshops evaluate technological, procedural, and personnel controls.
- Delivers actionable recommendations for security improvements.
- Offers comprehensive analysis of prevention, detection, and response.
- Documents both Red Team and Blue Team activities.
- Phased assessment option available for targeted focus.

Benefits

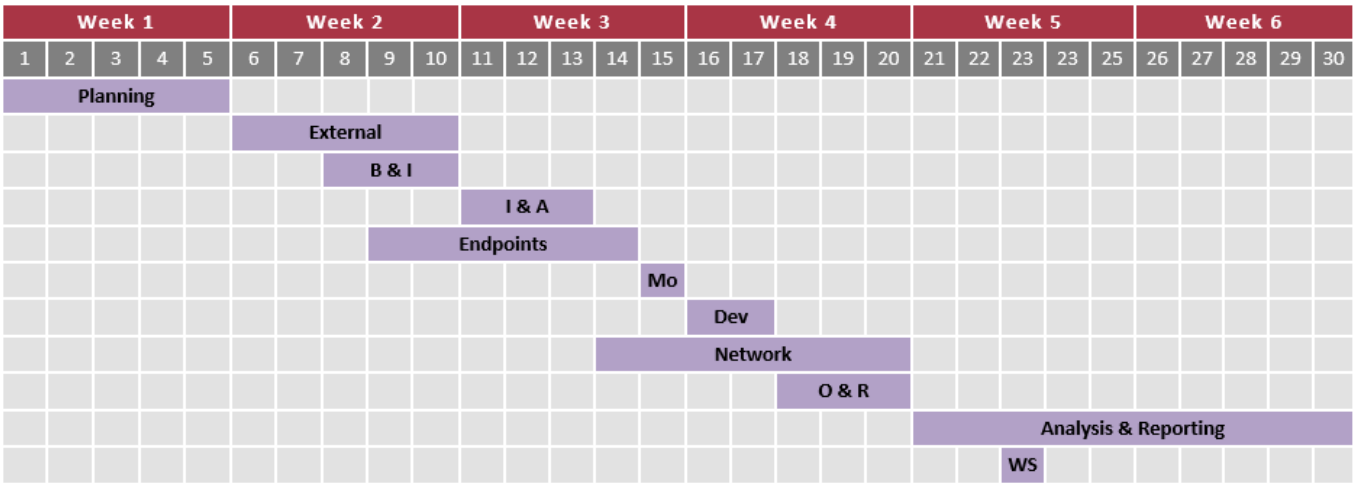
- Enhances overall security posture and awareness.
- Improves prevention, detection, and response capabilities.
- Facilitates stakeholder engagement and alignment.
- Provides actionable insights for security improvement.
- Identifies and addresses gaps in security controls.
- Offers detailed insights into potential attack paths.
- Encourages proactive improvement of security measures.
- Provides a benchmark for further testing.
- Strengthens technological and procedural defences.
- Supports continuous security enhancement and compliance.

Outcome

- A testing plan prepared by the Purple Team Manager
- An end-to-end engagement with communication to the involved stakeholders.
- Daily communication between the Red and Blue Team

- A comprehensive report detailing:
  - A full breakdown of all findings identified and TTPs assessed
  - Detailed metrics and matrix on detection, prevention, and response capability
  - Detailed recommendations, remediations and detection advice
  - High-level management summaries
  - 'Attack flow diagrams' showing a breakdown of the Red Teams actions
  - Root cause analysis and long-term strategy advice
  - Providing:
    - A comprehensive summary of the engagement
    - Metrics on the efficacy of controls and prevention, detection and response capabilities
    - Identification of as many attack paths as possible within an environment
    - Identification of gaps in the security controls and recommend improvements
    - Identification of security issues from multiple attack paths and provide recommendations
    - Documentation of conversations and actions of both the RT and the BT
    - Documentation of outcomes of collaboration such as improved detection rulesets
    - A benchmark for further testing and a framework to do that within
- A 2 hour virtual debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



- B & I = Boundary and Ingress
- I & A = Identity and Access
- Mo = Mobile
- Dev = Development
- O & R = Organisation & Response
- WS = Workshops with specific teams if needed

Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Reconnaissance • Test Plan Creation	7
Testing Phase – External • External • Boundary & Ingress • Identity & Access	10
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Laptops • Mobile	10
Testing Phase - Internal Network Testing • Networks & Servers • Development • Organisation and Response	20
Reporting	15
Project management, debriefs and updates	2
TOTAL	**64**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

Metric Based

A Metric Based Purple Team Exercise isolates the evaluation of the prevention, detection and response capability against a range of simulated attacks. By assessing what attacks were possible within an organisation against a baseline of TTPs, PTP is able to assess a level of maturity for an organisation, at the same time as providing insight into what attack paths are possible and if any risks were identified.

Features

- Isolates evaluation of prevention, detection, and response capabilities.
- Uses a baseline of TTPs for assessment.
- Focuses on assessing existing security maturity.
- Provides insights into possible attack paths.
- Identifies risks and potential security gaps.
- Measures effectiveness of current security controls.
- Offers objective measurement of security readiness.
- Prioritises metrics over subjective analysis.
- Documents outcomes of assessments and improvements.
- Provides a framework for subsequent testing.

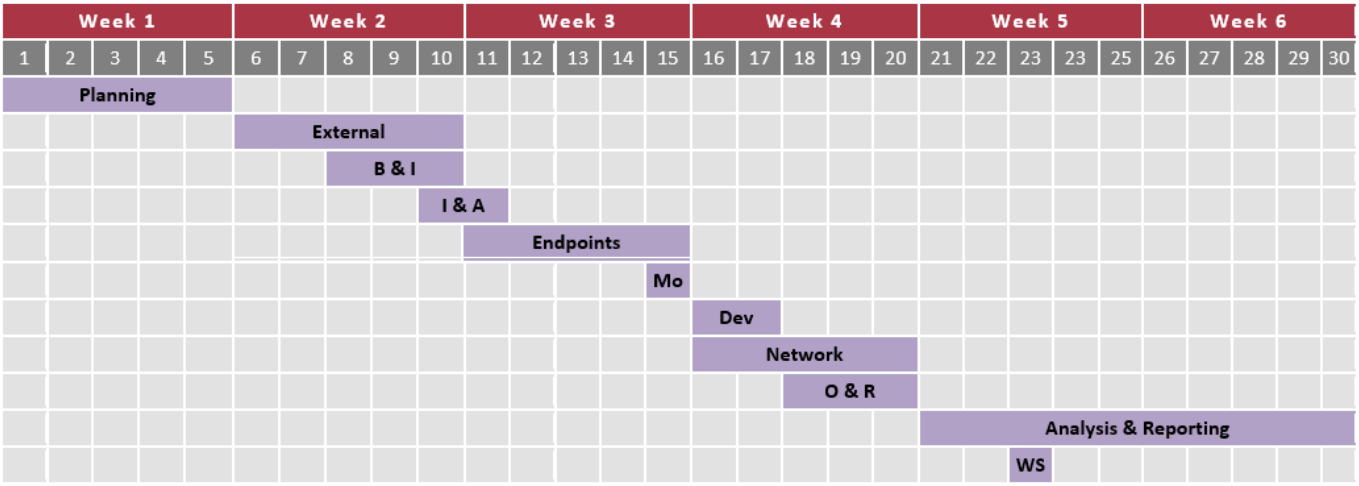
Benefits

- Delivers precise security metrics.
- Identifies areas needing immediate attention.
- Enhances specific security control mechanisms.
- Provides a baseline for future improvements.
- Increases organisational awareness of vulnerabilities.
- Encourages targeted security enhancements.
- Offers insights into effectiveness of responses.
- Assists in tuning existing security strategies.
- Helps quantify cyber maturity and security posture improvements.
- Supports strategic decision-making in cybersecurity.

Outcome

- Sequential testing of TTPs across predefined environments by the Purple Team Manager
- Constant and periodic communication with all teams about the attacks
- Comprehensive report on controls analysis, threat modelling, reconnaissance, and detailed TTP analysis
    - Focuses solely on TTP effectiveness, no narrative section
    - Includes root cause findings and IOC documentation
    - Identifies issues in technological, procedural, and personnel controls
    - Organisational Response Phase includes detailed metrics on prevention, detection, and response capabilities, along with timing assessments
- A virtual debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



- B & I = Boundary and Ingress
- I & A = Identity and Access
- Mo = Mobile
- Dev = Development
- O & R = Organisation & Response
- WS = Workshops with specific teams if needed

Metric Based Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Reconnaissance • Test Plan Creation	5
Testing Phase – External • External • Boundary & Ingress • Identity & Access	8
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Laptops • Mobile	7
Testing Phase - Internal Network Testing • Networks & Servers • Development • Organisation and Response	10
Reporting	9
Project management, debriefs and updates	1

TOTAL	**45**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

Objective Based

An Objective Based Purple Team Exercise will assess an organisations prevention, detection and response activity to a variety of attack scenarios whilst the Red Team also support the tuning of the EDR/MDR & SOC capabilities to improve.
A purple team assessment is generally highly collaborative and covers a selected number of tactics, techniques, and procedures (TTPs). Objectives will be defined during an initial consultancy phase when threat modelling and controls analysis will also be performed. In an Objective Based Purple Team, the Red Team perform a typical Red Team style engagement, performing attacks and moving towards objectives, whilst communicating the attacks and TTPs to the Blue Team in daily workshops.

Features

- Focuses on specific attack scenarios and objectives.
- Involves collaborative tuning of EDR/MDR & SOC capabilities.
- Includes detailed initial consultancy phase.
- Emphasises interaction between Red and Blue Teams.
- Utilises real-world attack simulations for assessment.
- Communicates ongoing attacks and TTPs in workshops.
- Assesses effectiveness across a variety of TTPs.
- Supports objective-driven security enhancements.
- Documents detailed narrative of engagement and collaboration outcomes.
- Provides comprehensive recommendations for improving detection rules.

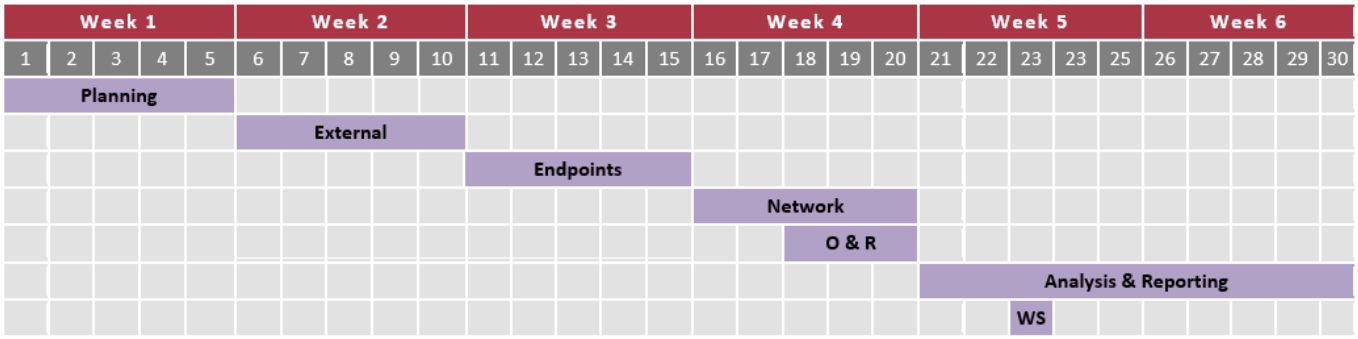
Benefits

- Improves specific detection and response operations.
- Facilitates deeper collaboration between security teams.
- Enhances understanding of advanced threat tactics.
- Directly addresses and improves SOC capabilities.
- Delivers focused and actionable insights.
- Strengthens overall security infrastructure.
- Encourages continuous learning and adaptation.
- Provides framework for ongoing security adjustments.
- Ensures alignment of security efforts and technologies with organisational goals.
- Optimises and refines security strategies and controls for future readiness.

Outcome

- Testing plan prepared by the Purple Team Manager
- Continuous interaction with stakeholders, informing them about ongoing attacks.
- Comprehensive report includes controls analysis, threat modelling, reconnaissance, narrative, and findings:
    - Findings associated with Mitre ATT&CK reference IDs
    - Documents preventions, detections, and responses
    - Full breakdown of the assessment narrative and IOC documentation provided
    - Organisational Response Phase measures prevention, detection, and response (PDR) effectiveness and timings
- A virtual debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



- O & R = Organisation & Response
- WS = Workshops with specific teams if needed

Objective Based Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Reconnaissance • Test Plan Creation	5
Testing Phase – External • External • Boundary & Ingress • Identity & Access	10
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Laptops • Mobile	10
Testing Phase - Internal Network Testing • Networks & Servers	10

• Development • Organisation and Response	
Reporting	9
Project management, debriefs and updates	1
TOTAL	**45**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

Phased

A phased Purple Team is an assessment that has been separated into multiple engagements or only a chosen phase is being carried out. There are variations of phased Purple Team such as Cloud, Development, Endpoint & EDR and AI/ML Stack. Each has a different focus and includes different technologies, processes and people within the security controls. Additional variations of Purple Teams may be compiled from the following standard phases:

- Controls Analysis, Threat Modelling, TTP Generation
- OSINT
- External
- Boundary & Ingress
- Endpoints
- Identity & Access
- Mobile
- Development
- Network
- Organisation & Response

Features

- Separates assessment into distinct, focused engagements.
- Offers specialised testing for various technology domains (e.g., Cloud, AI/ML).
- Includes phases for different security controls: OSINT, External, Mobile, etc.
- Tailors each phase to specific organisational needs and technologies.
- Can be configured to address specific areas like Endpoint & EDR.
- Involves a variety of security personnel and processes.
- Facilitates thorough controls analysis and threat modelling.
- Generates TTPs specific to each phase.
- Documents detailed findings and recommendations for each phase.
- Provides flexibility to focus on high-risk or critical areas first.

Benefits

- Allows for deep dives into specific security aspects.
- Enables targeted enhancements in critical security areas.
- Facilitates comprehensive understanding of attack surfaces.
- Supports incremental improvements in security posture.
- Provides detailed, actionable insights for each phase.

- Enhances specific controls and detection capabilities.
- Optimises scheduling, budget and resource allocation through focus.
- Helps build a robust framework for ongoing security efforts.
- Allows organisations to prioritise and address urgent risks.
- Provides a structured path for continuous security improvement.

Outcome

- Testing plan prepared by the Purple Team Manager
- Continuous interaction with stakeholders, informing them about ongoing attacks during the testing phase.
- Conducted over extended periods focusing on specific security aspects such as scoping, external, endpoint, and internal
- Reports and feedback tailored to the specific phase and focus area, providing targeted insights and recommendations
    - Each phase tailored to particular needs of the environment or security controls
    - Allows for thorough, focused analysis and gradual implementation of security measures and retesting
- Virtual debriefs containing high-level overview and full technical breakdown per phase.

Pricing and Scoping

Cloud

Cloud Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Reconnaissance • Test Plan Creation	7
Testing Phase – External • External • Boundary & Ingress • Identity & Access	10
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Laptops • Mobile	10
Testing Phase - Internal Network Testing • Cloud • Networks & Servers • Development • Organisation and Response	20
Reporting	15
Project management, debriefs and updates	2

TOTAL	**64**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2

Development

Development Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Reconnaissance • Test Plan Creation	7
Testing Phase – External • External • Boundary & Ingress • Identity & Access	10
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Development Endpoints • Mobile	10
Testing Phase - Internal Network Testing • Cloud • Networks & Servers • Development DevSecOps Stack • Organisation and Response	20
Reporting	15
Project management, debriefs and updates	2
TOTAL	**64**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

Endpoint & EDR

Endpoint & EDR Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Test Plan Creation	2
Testing Phase – External • Boundary & Ingress • Identity & Access	5
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Laptops	5
Testing Phase - Internal Network Testing • Organisation and Response	3
Reporting	7
Project management, debriefs and updates	2
TOTAL	**24**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

AI / ML

AI / ML Purple Team Assessment	Delivery Days
Consultancy and Scoping Phase • Controls & Gap Analysis • Threat Modelling • TTP Creation • Test Plan Creation	7
Testing Phase – External • Identity & Access	2
Testing Phase – Endpoint, Assisted Foothold & Malicious Insider Review • Developer Endpoints	5
Testing Phase - Internal Network Testing • Cloud • Networks & Servers • Development environment and DevSecOps Stack • ML Applications • Model Manipulation • Organisation and Response	25
Reporting	10
Project management, debriefs and updates	2
TOTAL	**51**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2

Custom

Or a combination of chronological phases from the following table:

Custom Purple Team Assessment	Delivery Days Guide
Controls & Gap Analysis	2
Threat Modelling	2
TTP Creation	1
Reconnaissance	5
Test Plan Creation	1
External	5
Boundary & Ingress	3
Identity & Access	3
Laptops and Endpoints	6
Developer Endpoints	6
Mobile	1
Cloud	5
Networks & Servers	5
Development environment and DevSecOps Stack	5
ML Applications	5
Model Manipulation	3
Organisation and Response	3
Reporting	15
Project management, debriefs and updates	2

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Physical Social Engineering	10

Open Source Intelligence (OSINT)

OSINT engagements provide organisations with insights into what attackers look for on the internet and using open-source methods and what can be found about them or their people. OSINT is the first stage in any intelligence-led service and assessing ones OPSEC is vital as a prerequisite to security. Our OSINT services provide organisation with ways to see what information is public, that they might not be aware of.

Service Lines

- Attack Surface Assessment (ASA)
- Executive Exposure Assessment (EEA)

Service Features

- Utilises open-source information to map attack surfaces.
- Identifies assets and potential real attacker targets.
- Begins with basic organisation or personal identifiers.
- Expands scope based on organisational needs.
- Provides foundation for targeted security assessments.
- Offers insights into combined or complex security threats.

Service Benefits

- Highlights systems, information or people vulnerable to attacks.
- Offers comprehensive view of public asset and information exposure.
- Understands organisation's appearance to attackers.
- Lays groundwork for further security enhancements and guides future testing.
- Educates executives on information, asset and personal exposure risks.
- Mitigates risks from publicly accessible information and enables protective measures.
- Increases security awareness among all levels of the organisation.
- Enhances overall organisational security posture.

50 Words

OSINT engagements provide insights into what attackers look and what can be found about an organisation, their people and their supply chain. Our OSINT services provide organisation with ways to see what information is public, that they might not be aware of.

Attack Surface Assessment (ASA)

An Attack Surface Assessment (ASA) uses open-source information to establish a list of assets that reflect the targets of a real attacker. This may help an organisation to find exposed systems that would typically be investigated by threat actors.

The outcome of the ASA and threat analysis elements help identify exposed systems that would typically be targeted by hackers or information that be used in targeted campaigns. Attackers can group several, seemingly minor, issues to form an overall, much more significant, threat to your organisation.

The assets found during the assessment do not necessarily indicate the existence of vulnerabilities but provide a path of exploration for future work. These assets, therefore, would need further testing to establish the risk faced by the organisation due to their exposure. The assessment also provides only a snapshot in time; thus, exposed assets may change.

An ASA has a wide scope and begins with only the organisation name and the main domain. In certain circumstances other organisational names and domains may be brought into the scope. Alongside the informational assets discovered the ASA will identify who are the likely threat actors to target the organisation. This combined with the identified assets will be used to provide custom threat scenarios demonstrating what could be used against the organisation.

Features

- Utilises open-source information to map the organisation's attack surface.
- Identifies assets reflecting potential real attacker targets.
- Begins with basic organisation identifiers like name and main domain.
- Identifies potential threat actors alongside discovered assets.

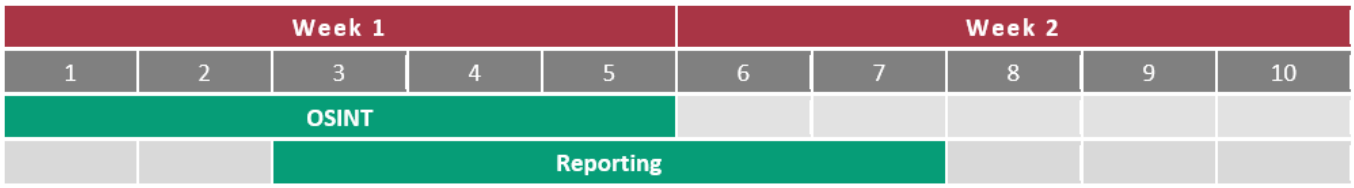
Benefits

- Highlights exposed systems and information that could be targeted by attackers.
- Provides a comprehensive view of publicly accessible assets and data.
- Helps organisations understand how they appear to potential attackers.
- Serves as a foundation for further targeted security assessments.
- Offers insights into combined minor issues creating significant threats.
- Can be used to increase operational security (OPSEC)

Outcome

- A comprehensive report that includes:
  - A detailed report of all exposed assets and information found.
  - Identification of potential threat actors.
  - Custom threat scenarios based on identified assets and information.
  - Analysis on how seemingly minor exposures can form significant threats.
  - Recommendations for further testing and security enhancements.

Pricing and Scoping



Attack Surface Assessment	Delivery Days

Attack Surface Assessment	7
Documentation and Analysis	0 (included)
Reporting & QA	0 (included)
TOTAL	**7**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Table Top Exercise	5

Executive Exposure Assessment (EEA)

An Executive Exposure Assessment (EEA) is designed to evaluate information publicly exposed to threat actors that directly concerns senior executives. Using publicly available information, such as home address, social contacts, spouse or partners, children and other information, intelligence can be inferred. This service is tightly controlled by various legal frameworks, including GDPR and Regulation of Investigatory Powers Act (RIPA), amongst others. Therefore, due the potentially sensitive of these assessments, direct executive subject approval for the assessment is required. The resulting report will be delivered to the executive subject only, with an anonymised summary report provided to the organisation. Following the investigation, a one-to-one workshop is carried out with the subject to help them understand the report, including what information can and cannot be expunged and what the impact of the information could be.

Features

- Evaluates publicly exposed information related to senior executives.
- Utilises publicly available data like addresses, social contacts, and family details.
- Conducted within strict legal frameworks such as GDPR and RIPA.
- Requires direct executive approval due to sensitive nature of information.

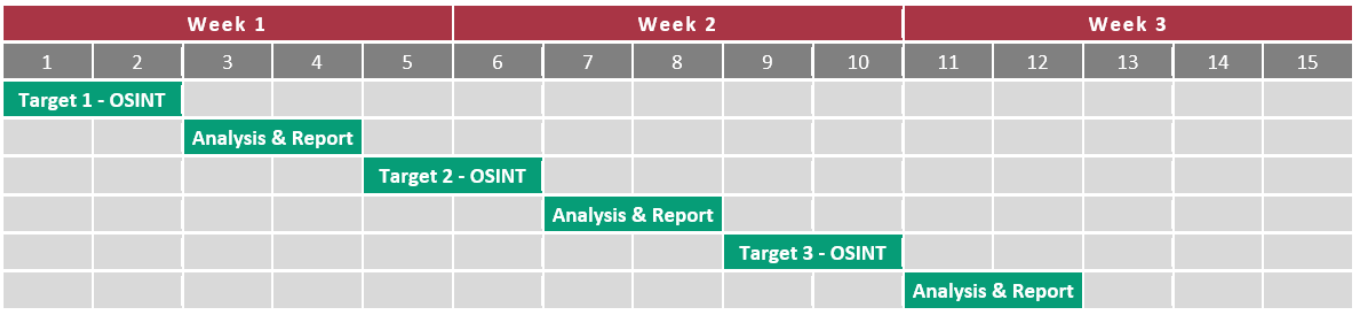
Benefits

- Provides executives with a clear understanding of their public exposure.
- Helps mitigate risks associated with publicly accessible personal information.
- Enables targeted protective measures for executives' personal data.
- Fosters heightened security awareness among senior leadership.

Outcome

- A detailed, confidential report delivered directly to the executive, covering:
  - Comprehensive analysis of publicly exposed personal information.
  - Insights into potential risks and impacts of exposed data.
  - Guidelines on what information can and cannot be expunged.
- An anonymised summary report provided to the organisation.
- A one-to-one workshop with the executive to discuss findings and protective measures.

Pricing and Scoping



Executive Exposure Assessment	Delivery Days
Executive 1 • OSINT • Analysis • Documentation	4
Executive 2 • OSINT • Analysis	4

• Documentation	
Executive 3 • OSINT • Analysis • Documentation	4
One-to-one Workshops	1
TOTAL	**13**

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Additional Executives	5
Security Awareness	2
Table Top Exercise	5

Cyber Social Engineering (CybSE)

Cyber Social Engineering operations use electronic means, such as email and telephony to contact and influence targets. Our services allow organisations to test technology, people and processes and establish if they can be persuaded to give out sensitive information, credentials or facilitate remote access into sensitive networks. Often multiple offerings are combined into a single engagement, or chained with other services.

Service Lines

- Email Phishing
- Phishing Susceptibility Audit
- SMS Phishing (Smishing)
- Voice Phishing (Vishing)
- Direct Message Phishing (DMishing)

Service Features

- Leverages OSINT for realistic threat simulation.
- Utilises electronic communication for targeted attacks.
- Engages multiple platforms: email, SMS, voice, direct messaging.
- Tests security across technology, people, and processes.
- Intelligence-led design tailored to specific organisational vulnerabilities.
- Flexible approach adaptable to varied organisational needs.
- Includes both broad and targeted phishing techniques.
- Controlled testing environment simulates real-world scenarios.
- Comprehensive evaluation of current security protocols.
- Combines several attack methods in single assessments.

Service Benefits

- Identifies potential vulnerabilities in electronic communication.
- Enhances defences against diverse phishing strategies.
- Increases organisational awareness of social engineering threats.
- Guides improvements in technological, procedural and personnel controls.
- Customisable to focus on specific organisational risks.
- Trains employees on recognising and mitigating threats.
- Encourages a robust security culture development and prepares for threats.

50 Words

Cyber Social Engineering uses electronic means, such as email (Phishing), telephony (Smishing & Vishing), or other methods to contact and influence targets. Our services allow organisations to test technology, people and processes and establish if they can be persuaded to disclose sensitive information, credentials or facilitate remote access into networks.

Email Phishing (Phishing)

Phishing may take the form of mass, spear or whaling depending on the targets identified. The assessment is a intelligence-led exercise where potential attack types are identified based on OSINT and pretexts are generated. The aim of the assessment is usually to test the technology, people or processes and identify the impact of the compromise on an organisation. This may range from stolen credentials, to access tokens, to stolen information, to remote access to the organisation's network.

Features

- Targets staff through mass, spear, or whaling phishing exercises.
- Uses OSINT to design intelligence-led attacks.
- Assesses technology, people, and processes.
- Replicates real world phishing and social engineering attacks.

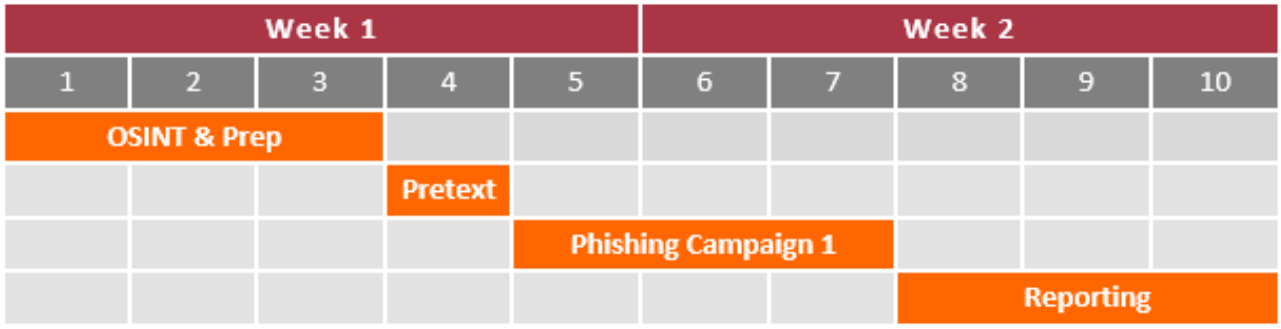
Benefits

- Identifies susceptibility to email-based threats.
- Tests effectiveness of organisational email filters and security protocols.
- Enhances awareness and preparedness against phishing.

Outcome

- Detailed report with findings from phishing attempts.
- Recommendations for improving mail security and user training.
- Exploration of attack paths and potential breaches.

Pricing and Scoping



This is for credentials, sessions or faux malware delivery. For delivery of Command & Control (C2) implant please add the optional testing element of Attack & Penetration Test (Assess Access).

Email Phishing Assessment	Delivery Days
OSINT	1 - 3
Pretext Generation (1 day per campaign) • Optional C2 implant development	1 – 10+
Single Phishing Campaign	2 - 3
Analysis and Reporting	1 - 3
TOTAL	**5 - 19**

Additional Optional Cyber Social Engineering:

Optional Test Element	Delivery Days

Phishing Susceptibility Audit	3
Single Smishing Campaign	2 - 3
Single Vishing Campaign	2 - 3
Single Dmishing Campaign	2 - 3

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Physical Social Engineering	10
Security Awareness	2
Attack & Penetration Test (Assess Access)	5
Optional C2 implant development	4 – 10+
Knowbe4 Subscription (Any template base phish or less than 4 days)	N/A

Phishing Susceptibility Audit

An assessment of which attack vectors are possible via email phishing to identify gaps in mail technologies and defensive layers. This is used to assess if the current controls can prevent or detect various attack vectors used in phishing campaigns. This includes differences in quantity such as mass vs. spear phishing as well as the following domain related delivery types:

- Spoofing employees and client domains
- Spoofing supply chain, contacts or 3rd parties
- Abusing mail infrastructure, relays and trusted headers
- Using trusted 3rd party email providers
- Using generic and free email providers
- Attempting typosquats of client domains, supply chain contacts or trusted 3rd party

These are assessed alongside testing the efficacy of any corporate proxies and the ability to prevent and detect malicious traffic and domains. Delivery of malicious content is also explored within this test which identifies gaps with attachments and links. Various types of each would be tested including a variety of filetypes attached, typical tracking links, but also looking at UNC paths, credential harvesting, OAuth applications and session token capture.

This should identify which types of attacks are currently possible, that would facilitate access to sensitive information. Relevant attack paths will be mapped and identified during the testing. Depending on the amount and sophistication of the controls in place, PTP can also explore bypasses and other techniques that could be exploited.

Features

- Comprehensively evaluates various email phishing attack vectors.
- Assesses effectiveness of mail technology and defensive layers.
- Analyses different domain-related delivery types and mail infrastructure.
- Only assesses technology and processes, not people.

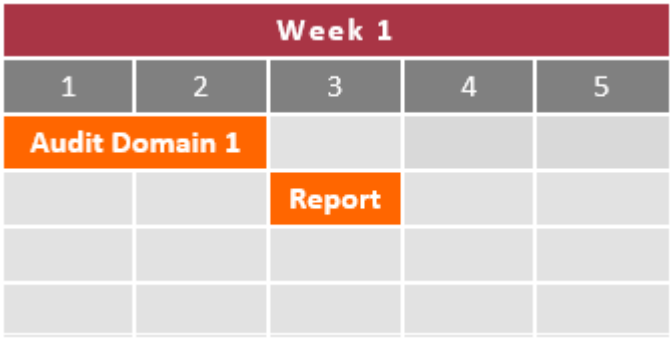
Benefits

- Maps susceptibility to different phishing strategies.
- Identifies gaps in mail security and proxy defences.
- Provides insights into the robustness of current email controls.
- Ensures a baseline of defences before relying on staff awareness.

Outcome

- Comprehensive report detailing gaps in mail security containing:
  - Documentation of tested attack types and their outcomes.
  - Specific remediation advice for enhancing detection and prevention.
- Virtual debriefs and ad hoc discussions for high-level overviews or full technical breakdowns.

Pricing and Scoping



Phishing Susceptibility Audit	Delivery Days
Phishing Susceptibility Audit per emailing domain	2
Analysis and Reporting	1
TOTAL	**3**

Additional Optional Cyber Social Engineering:

Optional Test Element	Delivery Days
Single Email Phishing Campaign	5 – 19
Single Smishing Campaign	5 – 19
Single Vishing Campaign	5 – 19
Single Dmishing Campaign	5 - 19

With further campaigns added as:

Optional Test Element	Delivery Days
Single Email Phishing Campaign	2 - 3
Single Smishing Campaign	2 - 3
Single Vishing Campaign	2 - 3
Single Dmishing Campaign	2 - 3

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Physical Social Engineering	10
Security Awareness	2
Attack & Penetration Test (Assess Access)	5
Optional C2 implant development	4 – 10+
Knowbe4 Subscription (Any template base phish or less than 4 days)	N/A

SMS Phishing (Smishing)

SMishing uses text messages to gather and extract sensitive information from a target. The assessment uses OSINT or information provided to form a pretext and target a pre-approved set of phone numbers.

Features

- Replicates real world social engineering attacks.
- Uses SMS for information extraction or deliver links and payloads.
- Designed pretexts based on OSINT or provided information.
- Targets a pre-approved set of phone numbers.

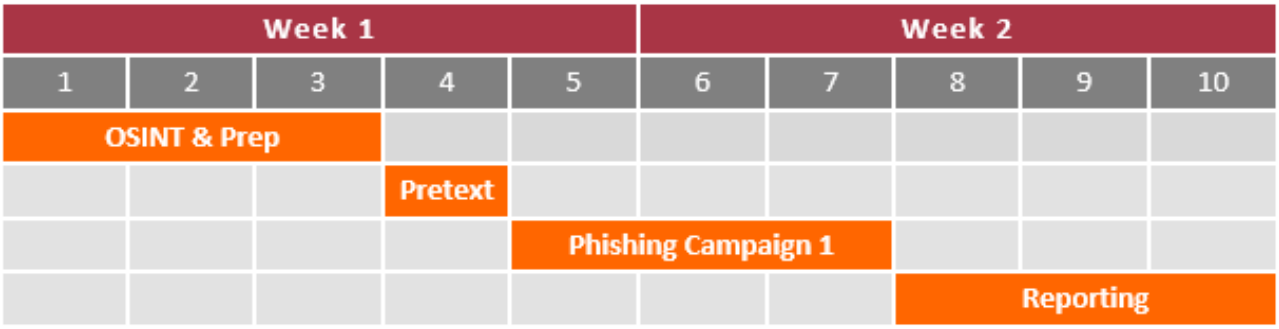
Benefits

- Tests vulnerability to SMS-based phishing attacks.
- Improves understanding of risks associated with text message interactions.
- Guides development of strategies to mitigate smishing threats.
- Provides insight into mobile vectors for attack.

Outcome

- Report on smishing campaign effectiveness and extracted data containing:
  - Detailed breakdown of SMS attack methodologies and results.
  - Strategic recommendations for protecting against SMS phishing.
- Virtual debriefs and ad hoc discussions for high-level overviews or full technical breakdowns.

Pricing and Scoping



This is for credentials, sessions or faux malware delivery. For delivery of Command & Control (C2) implant please add the optional testing element of Attack & Penetration Test (Assess Access).

Email Phishing Assessment	Delivery Days
OSINT	1 - 3
Pretext Generation (1 day per campaign) • Optional C2 implant development	1 – 10+
Single Smishing Campaign	2 - 3
Analysis and Reporting	1 - 3
TOTAL	**5 - 19**

Additional Optional Cyber Social Engineering:

Optional Test Element	Delivery Days
Phishing Susceptibility Audit	3
Single Phishing Campaign	2 - 3

Single Vishing Campaign	2 - 3
Single Dmishing Campaign	2 - 3

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Physical Social Engineering	10
Mobile Compromise Traffic Simulation	0.5
Security Awareness	2
Attack & Penetration Test (Assess Access)	5
Optional C2 implant development	4 – 10+

Physical Social Engineering (PhySE)

Physical Social Engineering operations use physical means, such as intrusion, bypassing physical controls and face-to-face manipulation to test an organisations physical controls, technology, processes and people. This is with the aim of proving access to restricted places, sensitive information or demonstrating the ability to place implants for further cyber operations. Often multiple offerings are combined into a single engagement or chained with other services.

Service Lines

- Covert Intrusion Assessment
- Overt Intrusion Assessment
- Physical Security Audit (Unregulated)

Service Features

- Restrictions with delivery outside of UK dependent on country and requirement.
- Simulates realistic physical security breach scenarios.
- Utilises both covert and overt assessment methods.
- Deploys advanced social engineering tactics.
- Targets sensitive or restricted organisational areas.
- Combines with broader cybersecurity assessments.
- Includes detailed pre-assessment reconnaissance.
- Provides "get out of jail free" safeguards.
- Assessments designed around specific organisational vulnerabilities.
- Tests both technological and human security controls.
- Flexible in approach, tailored to organisational needs.

Service Benefits

- Reveals gaps in physical and procedural security.
- Tests organisation's detection and response capabilities.
- Enhances preparedness against unauthorised access.

- Provides baseline for security under realistic conditions.
- Educates personnel on real-time threat detection.
- Identifies weaknesses in human and technological defences.
- Encourages improvements in security protocols and training.
- Prepares organisations for sophisticated physical threats.

50 Words

Physical Social Engineering uses physical means, such as intrusion, bypassing physical controls and face-to-face manipulation to test an organisations physical controls, technology, processes and people. This is with the aim of proving access to restricted places, sensitive information or demonstrating the ability to place implants for further cyber operations.

Covert Intrusion Assessment

An entirely covert operation against an organisation's physical, technological, procedural and personnel controls. The client will not be notified of arrival nor the pretexts or vectors to be attempted. The PTP consultant will be equipped with a "get out of jail free" letter signed by an authorised individual from the client organisation attesting the validity of the exercise. They will attempt to breach and gain entry to a client site, achieve goals or persistence and not get caught. This is often part of a wider, chained, engagement whereby physical access will provide initial access for a Red Team or data and devices extracted for further operations.

Features

- Completely covert operations test all organisational security layers.
- No notification of approach details or timing to the client.
- Equipped with a "get out of jail free" letter.
- Simulates advanced attacker tactics to breach facilities.
- Targets sensitive or restricted areas for access.
- Can be combined with broader Red Team engagements for full spectrum testing.
- Utilises realistic pretexts based on detailed OSINT.

Benefits

- Reveals gaps in physical and personnel security without prior alert.
- Tests real-world response to unauthorised access attempts.
- Measures effectiveness of physical, technological, procedural and personnel controls.
- Enhances preparedness against sophisticated breaches.
- Develops a baseline for security measures under stress.
- Provides critical insights into end-to-end security vulnerabilities.

Outcome

- Detailed report with:
  - Complete breakdown of entry methods, paths taken, and duration of stay.
  - Specific vulnerabilities exploited and potential for asset compromise.
  - Visual attack flow diagrams, blueprints, diagrams and narratives of intruder actions.
  - Strategic recommendations for tightening security postures.
  - High-level summaries for executive understanding and action.
- Aftercare for any staff interactions or controls breached.
- A virtual or in person debrief containing high-level overview and full technical breakdown.

Pricing and Scoping

Covert Intrusion Assessment	Delivery Days
OSINT and Remote Reconnaissance	3

Physical Reconnaissance	1
Covert Intrusion	2 - 4
Reporting	2
TOTAL	**8 - 10**

Additional Optional Physical Social Engineering:

Optional Test Element	Delivery Days
Overt Intrusion Assessment	2 - 3
Physical Security Audit	2

Additional Optional Cyber Social Engineering:

Optional Test Element	Delivery Days
Single Email Phishing Campaign	5 – 19
Single Smishing Campaign	5 – 19
Single Vishing Campaign	5 – 19
Single Dmishing Campaign	5 - 19

With further campaigns added as:

Optional Test Element	Delivery Days
Single Email Phishing Campaign	2 - 3
Single Smishing Campaign	2 - 3
Single Vishing Campaign	2 - 3
Single Dmishing Campaign	2 - 3

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Attack & Penetration Test (Assess Access)	5
Wireless Security Breach Assessment	1
Rouge Device and Bug Sweep (Third-Party Delivery)	1
Outside of UK	Tbc

Overt Intrusion Assessment

A review of physical, technological, procedural and personnel controls carried out in an overt manner. A predefined date of arrival will be arranged with a client and the consultant will perform common approach and opportunistic physical intrusion and social engineering vectors. This is an intelligence-led engagement where OSINT and in person reconnaissance allow for the generation of pretexts for common entry vectors and technical attacks. This engagement allows the consultant to be caught attempting a variety of vectors and provides a mechanism of "reset" so that many attack vectors can be demonstrated and many controls tested.

Features

- Simulate insider threat and external attackers.
- Simulates potential insider threats and external breaches.
- Test visitor, clear desk and fire evacuation policies.
- Identify vulnerable technologies such as cloneable cards or CCTV
- Short assessment providing a baseline for future testing.
- Allows for repeated testing of specific entry points.
- Known and scheduled testing of physical security measures.
- Uses straightforward and opportunistic intrusion methods.
- Engagement is transparent with client's security team.

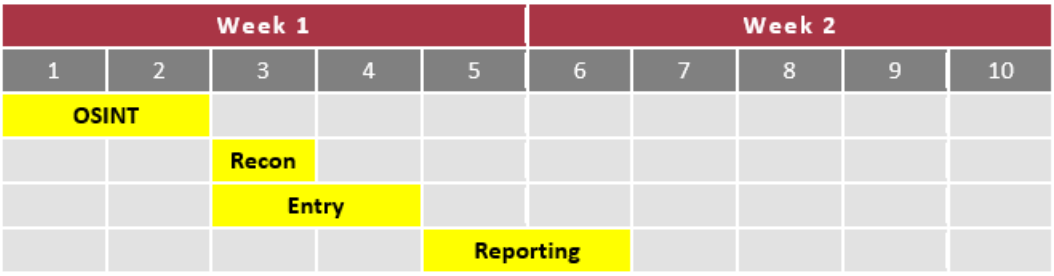
Benefits

- Adaptive for constrained budgets or schedules
- Directly assesses efficacy of known security procedures.
- Educates security personnel on real-time threat detection.
- Enhances training through live demonstration of breaches.
- Identifies weaknesses in both human and technological defences.
- Enables iterative testing and immediate feedback for improvements.
- Allows understanding of the most severe physical vulnerabilities.

Outcome

- Comprehensive report detailing:
    - Outcomes of each tested entry and security challenge.
    - Staff reactions and system alarms to each scenario.
    - Detailed recommendations for procedural and technological enhancements.
    - Chronological review of all actions taken during the assessment.
- A virtual or in person debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



Overt Intrusion Assessment	Delivery Days
OSINT	2
Physical Reconnaissance	1
Overt Intrusion	2 - 3
Reporting	2
TOTAL	**7 - 8**

Additional Optional Physical Social Engineering:

Optional Test Element	Delivery Days
Covert Intrusion Assessment	3 - 5
Physical Security Audit	2

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Wireless Security Breach Assessment	1
Rouge Device and Bug Sweep (Third-Party Delivery)	1
Outside of UK	Tbc

Physical Security Audit (Unregulated)

An open and sometimes escorted review of physical security. The open review will simulate "visitor attacks" where the consultant is signed in as a valid visitor and then seeks to wander around on their own performing the audit. The fully escorted audit is an in-depth risk identification exercise in collaboration with the client contact.

After a covert intrusion assessment has come to an end an assessment may convert to a physical security audit to ensure coverage. This allows the consultant to show the client the areas accessed as well as highlight unexploited, but potential, attack paths.

This audit does not need a typical get out jail free letter. But might require some form of authorisation letter if left to wander unattended (optional).

Features

- Not for organisations requiring DART or Top-Secret clearance.
- Open review of all organisational physical security measures.
- Includes both escorted and non-escorted assessments.
- Reviews access control systems, surveillance measures, and physical barriers.
- Conducted as either a direct walkthrough or post-covert assessment.
- Evaluates enforcement of policies like clear desk and secure storage.
- Checks compliance with physical security best practices.

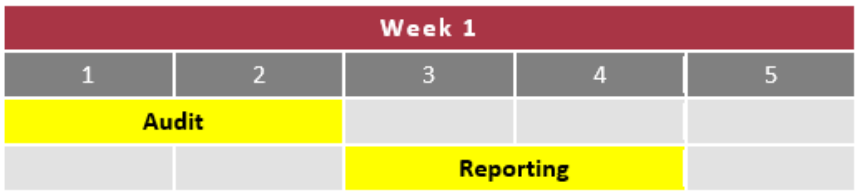
Benefits

- Provides a comprehensive overview of physical security protocols.
- Highlights compliance issues with internal security policies.
- Offers insight into daily security operations and potential oversights.
- Facilitates understanding of security from an external auditor's perspective.
- Improves security culture by demonstrating potential risk areas.

Outcome

- Detailed audit report including:
    - Specific vulnerabilities identified during the walk-through.
    - Potential security breaches and their implications.
    - Policy enforcement review and compliance assessment.
    - Recommendations for physical security improvements.
    - Documentation of findings with visual aids and descriptions.
- A virtual or in person debrief containing high-level overview and full technical breakdown.

Pricing and Scoping



Overt Intrusion Assessment	Delivery Days
Physical Security Audit	2
Reporting	2
TOTAL	**4**

Additional Optional Physical Social Engineering:

Optional Test Element	Delivery Days
Covert Intrusion Assessment	8 - 10
Overt Intrusion Assessment	7 - 8

Additional Optional Test Elements:

Optional Test Element	Delivery Days
Security Awareness	2
Outside of UK	Tbc