PEN TEST PARTNERS

G-Cloud 15

Lot 3 Cloud Support – Security Services Definition Document – DFIR

Version 1.0

Contact: bidteam@pentestpartners.com

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 sets out the services and methodologies provided by the DFIR team at Pen Test Partners LLP. In a competitive market PTP are leading the way through their cutting-edge approach to DFIR. Through the use of a Cloud based DFIR lab PTP have a truly Global reach, able to respond to a client's needs in minutes through our remote threat hunting, acquisition and analysis capabilities.

Through the techniques and applications we employ, PTP are able to not only acquire data for analysis but conduct live analysis on impacted endpoints, including active containment actions to stop the attackers in their tracks. At PTP we take a holistic approach to any incident looking at the entire network or sub-net as a source of evidence, not just the now impacted systems.

PTP DFIR Services:

Services Type	Service	Services Type	Service
Reactive	Incident Response Retainer Service	Proactive	Compromise Assessments (CA)
	DFIR MDR Service		CA - Exposure Attack Surface Risk Assessment
	Incident Response (IR)		CA - Identity Risk Assessment
	IR - Digital Forensics		Security and Hygiene Assessment
	IR - Root Cause and Impact Assessment		Threat Hunting
	IR - Business Email Compromise		Dark Web Monitoring
	IR - Data Exfiltration Investigation		
	IR - Mobile Device Forensics		
	IR - Digital Forensics Expert Witness Service		

PTPs Approach to Working Together and Pricing

Every project we deliver is custom managed. From initial scoping through to debrief we will ensure the right approach and people are being utilised.

PTP's implementation plan typically follows an established workflow based on actions from PTP and our clients, although we can of course work around a client if they have a preferential implementation model.

PTP typical working model:

- **Dedicated Account Manager:**
  - PTP will allocate a dedicated account manager as a central point of contact for the duration of the relationship.
- **Initial Consultation:**
  - For each new engagement, PTP will initiate a conversation via email and/or call to understand your service requirements. This serves as the introduction call.
- **Scope of Works (SOW) Creation:**
  - A PTP technical consultant will review all relevant information and create a detailed Scope of Works (SOW). This document will include any necessary prerequisites.
- **Proposal and SOW Delivery:**
  - PTP will send a comprehensive Proposal/SOW, specifying:
    - Duration
    - Cost
    - Grade of consultant required
    - Proposed dates (if already discussed)
- **Pricing Calculation:**
  - Pricing will be determined based on the number of days required to deliver the services using the service day rates.
- **Acceptance of Proposal / SOW**
  - Upon acceptance of the SOW, delivery dates are agreed and scheduled.
- **Authorisation and pre-requisite information**
  - PTP will send a Authorisation form for signature and return.
- **Pre engagement Kick off Call**
  - PTP will host a pre-engagement call to discuss the engagement and introduce the team.
- **PTP undertakes the required services.**

Reactive Services – Post/Ongoing Breach

These services are ordinarily offered to respond to an immediate requirement and are not booked in advance due to their last-minute nature. They are often only associated with a customer who is suffering or has suffered a breach.

Incident Response Retainer

The PTP Response Retainer is your proactive shield against unexpected crises in the digital landscape.

Think of it as your emergency response team, standing by 24/7, ready to assist within pre agreed SLAs.

With an annual subscription, you can secure peace of mind knowing that you have a dedicated team of experts on standby as a priority client in the event of a global cyber outbreak. PTP are poised to mitigate and manage any cyber incidents that may arise. Whether it's a data breach, malware attack, or system compromise, our seasoned professionals are equipped with the tools and expertise to swiftly contain the situation and minimize its impact on your operations.

Moreover, our 'pre-authorised day' feature ensures expedited response times, allowing us to leap into action without delay. By streamlining the authorisation process in advance, we eliminate precious moments wasted on bureaucratic hurdles, enabling us to focus solely on resolving the issue at hand. As a client you are not charged for any unused pre-authorised days.

In essence, an Incident Response Retainer is your proactive insurance policy against unpredictable threats. By investing in this service, you not only safeguard your organisation's sensitive data and critical infrastructure but also fortify your resilience in the face of adversity.

Feature	Basic	Standard	Enhanced	Elite
Annual Retainer Fee	£0	£8,750	£12,800	£30,000
Day rate	£2,000 p.d.	£1,750 p.d.	£1,600 p.d.	£1,500 p.d.
				Includes Dark Web Monitoring
Free Onboarding	✅	✅	✅	✅
Enhanced Onboarding (1 day from retained days used for Maturity Assessment with report)	❌	❌	✅	✅
Full DFIR Support	✅	✅	✅	✅
Phone Availability	4 (Business Hours Only)	1 Hour	1 Hour	1 Hour
Hands-on Triage	4 (Business Hours Only)	4 Hours	2 Hours	2 Hours
24/7 Triage	✅	✅	✅	✅
Dark Web/OSINT Monitoring	❌	❌	❌	✅

Weekly Alerting	❌	❌	❌	✅
Included DFIR Days	0	5	8	12
Day Rate Reduction (Pre and Post-included Days)	0%	12.5%	20%	25%

Managed Detection & Response (MDR) Service

The Managed Detection and Response service, fortified by Falcon Complete and our elite PTP DFIR (Digital Forensics and Incident Response) team, offers unparalleled protection and rapid response capabilities in the ever-evolving landscape of cybersecurity threats.

Powered by Falcon Complete, the PTP MD&R service leverages cutting-edge technology and real-time threat intelligence to proactively detect and neutralize threats before they can inflict harm on your organisation. With Falcon Completes advanced endpoint detection and response capabilities, PTP provide round-the-clock monitoring of your digital assets, swiftly identifying suspicious activities and potential breaches.
However, the service doesn't stop at detection. It's complemented by our expert PTP DFIR team, comprised of seasoned professionals with extensive experience in digital forensics and incident response. When a threat is detected, the PTP DFIR experts are engaged through pre-agreed playbooks, conducting thorough investigations to determine the scope and severity of the incident. This service boasts rapid response capabilities and meticulous attention to detail, containing the threat, mitigate its impact, and restore the integrity of your systems.

In essence, the PTP Managed Detection and Response service, powered by Falcon Complete and our PTP DFIR team, offers comprehensive protection and rapid response capabilities to safeguard your organisation against the most sophisticated cyber threats.

Incident Response (IR) Services

An immediate response service to an active and potentially ongoing cyber security incident.

PTP has a team of DFIR experts with decades of experience responding to cyber security incidents to all enterprise environment types and scale, throughout the globe.

PTP can respond immediately to your incident using advanced remote incident response tooling.

Small agents can be deployed across your environment to allow our expert analysts to get right to the heart of the attack. PTP gather data within our cutting edge DFIR lab for analysis without the delays of waiting for analysts to deploy to your location. From our DFIR lab we can search for threats, gather vital data for further analysis, search for identified Indicators of the Compromise to uncover additional impacted systems, and in some cases can assist with containment of any active breach by neutralising malicious services and rouge processes.

Incident Response Service also include:

- Advanced targeted attacks
- Malware Attacks
- Ransomware Attacks

- Loss or compromise of data
- Unauthorized access to networks and/or data
- Improper usage of systems or information
- Network analysis
- End-point analysis
- Malware analysis
- Log file analysis
- Computer forensics including mobile device and preservation
- Expert witness services
- Crisis management
- Communications support such as Media/Legal
- Network recovery service
- Cyber threat and business intelligence
- Implementation of any technologies to remain on the network
- Personnel security review
- Physical security review
- Testing of any business partner systems
- Transmission security within any service provider's network
- Specific review of systems and internal controls
- Proactive scanning for APT activity
- Proactive scanning based on IOCs from threat intelligence

IR Digital Forensics

Detailed, in-depth forensic analysis of any device that has storage and/or memory to any capacity, either volatile or long-term.

Using skills honed over a decade of experience and the latest in forensic tools, PTP has the capability to provide you with the answers you seek. From intellectual property theft to placing a suspect behind a keyboard, PTP analysts are experts in the field of acquiring, analysing and presenting their findings. Whether you need a report to support an internal matter, an expert to present findings at a hearing, or just because you want to know what happened and why, the PTP team of experts are here to assist.

Following the best practices used by UK law-enforcement all our evidence and processes will stand-up to the greatest of scrutiny.

PTP DFIR analysts will work with you to agree the correct forensic strategy to achieve your aims before acquiring evidence from the device or item to analyse in our cutting edge DFIR laboratory. Where possible, evidence will be acquired remotely, however items can also be sent to PTP for acquisition. If required, arrangements can be made for acquisition to take place on-site, for example very sensitive matters, however this is not advisable due to the length of time often required and the limitation in tooling capacity.

IR Root Cause and Impact Assessment

Following a confirmed security breach, PTP will use detailed forensic analysis of compromised systems to aim to identify the root cause of the environment breach and the initial attack vector. Such analysis will assist any organisation to understand any security gaps or failings that led to the breach and steps to be taken to prevent such an attack taking place again.
It may be relevant for an organisation to understand the full impact that a breach has had. This could include analysis of malware deployed within the environment, calculating the window of compromise and the

window of data exfiltration, understanding the reach of the attack and the data they gained access to, confirmation of data access and exfiltration.
Unfortunately there are never any guarantees that these questions can be answered due to the availability of evidential artefacts however, PTP will use expert digital forensic techniques to recover and analyse the available evidence.
Key Points:

- Understand why and how the breach took place
- Assess the impact of the breach and risk of data disclosure
- Understand the full extent of a breach to support risk assessment and business recovery
- Support reporting to ICO and/or Cyber Insurance
- Requires detailed forensic analysis and malware analysis

IR Business Email Compromise

Business Email Compromise (BEC) is a type of scam targeting companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to make fraudulent transfers, resulting in hundreds of thousands of dollars in losses.
Also known as Man-in-the-Email scams, BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives. Often, they impersonate a CEO or any executive authorized to do wire transfers. In addition, fraudsters also carefully research and closely monitor their potential target victims and their organisations.
Following a confirmed security breach, PTP will use detailed forensic analysis of compromised systems to aim to identify the root cause of the BEC. This will involve requiring access to the clients Exchange and Domain Controller logs, be that (on-prem or hybrid), O365 and Azure tenants, the E-Discovery and explorer tools.

IR Data Exfiltration Investigation

Data exfiltration is the theft of data, often sensitive in nature, by an attacker during a security breach.
Once an attacker has established access to a victim's environment, data exfiltration is one of the common stages of an attack – the theft of sensitive data provides an attacker with leverage over the victim in order to extort financial gain (or any other goal). This is particularly prevalent in ransomware attacks.
Following a confirmed security breach, PTP will conduct an in-depth review of available logs and perform a comprehensive analysis of the data present to determine important factors such as:

- When the data was stolen
- How much data was stolen
- From which devices was the data stolen

Following the initial review of logging in relation to the above, PTP can then seek to conduct further review (in the event the devices on which the stolen data was stored can be identified) to determine exactly what data was accessed by the attackers during the breach.
A report detailing the findings of the above will be provided.

IR Mobile Phone Investigations

Mobile devices, including phones and tablets, are rapidly becoming a popular (and in some instances, more common) location for where individuals and organisations store their data and perform many of their day-to-day tasks.

It is therefore just as important to consider the value of data held on phones and tablets in tandem with the data held on computers, especially when investigating any matter related to digital evidence.

Using the latest DFIR tooling, PTP are able to analyse data from mobile device backups hosted in the cloud, circumventing the historic necessity for mobile devices to be analysed and their data extracted through physical possession of the device(s) in question.

Analysis can then be conducted on the extracted data, including the examination of data from third-party applications, to determine their relevance to an investigation and provide crucial findings related to an incident.

The PTP DFIR team has featured on the BBC – “Rip off Britain” which highlights our advanced capabilities in this specialist forensic field.

IR Expert Witness

Our PTP DFIR (Digital Forensics and Incident Response) expert witness service offers invaluable support for legal proceedings by providing authoritative testimony and insights derived from extensive experience and expertise in digital forensics and incident response.

When you engage our DFIR expert witness service, you benefit from the expertise of seasoned professionals who possess a deep understanding of digital evidence, cybersecurity, and the intricacies of modern technology. Our experts are adept at analysing complex technical data and presenting findings in a clear, concise manner that is accessible to judges, juries, and legal teams.

Key components of the PTP DFIR expert witness service include:

1. **Technical Expertise**: PTP experts possess a comprehensive understanding of digital forensics, cybersecurity principles, and incident response methodologies. They are proficient in analysing digital evidence from a variety of sources, including computers, mobile devices, and network logs.
2. **Case Assessment**: PTP experts conduct thorough assessments of the case at hand, identifying key issues, potential challenges, and areas of focus for the digital forensic analysis. They work closely with legal teams to develop strategies that leverage digital evidence to support the client's case.
3. **Evidence Collection and Preservation**: PTP experts are skilled in the proper collection, preservation, and chain of custody documentation of digital evidence to ensure its admissibility in court. PTP follow industry best practices and adhere to legal standards to maintain the integrity of the evidence throughout the forensic process.
4. **Expert Testimony**: PTP experts provide compelling testimony based on their findings and analysis of digital evidence. They are experienced in presenting complex technical information in a manner that is easily understood by non-technical audiences, helping to clarify key points and strengthen the client's case.
5. **Consultation and Support**: PTP experts offer ongoing consultation and support to legal teams throughout the litigation process. They assist with deposition preparation, trial strategy development, and other aspects of case management to ensure that digital evidence is effectively leveraged to support the client's legal objectives.

In summary, the PTP DFIR expert witness service offers invaluable expertise and support for legal proceedings involving digital evidence. With our experienced professionals at your side, you can confidently navigate the complexities of the courtroom and effectively leverage digital evidence to achieve a favourable outcome for your client.

Proactive Services – Non-Breach Dependant

These services aid in mitigating risk before it occurs and supports cyber maturity programs.

Compromise Assessment

There are times when the attackers have completely bypassed your defences and alerting. When someone outside your organisation informs you of a potential cyber security incident, or a new zero day is released that is already being actively exploited, or your IDS is reporting but you just can't find a confirmed breach.
For these instances PTP offers an assessment process to give you that definitive, initial, expert triage, and answer the question of, "have I been breached?"
This service is delivered by deploying agents for our Threat Hunting solution which will be placed on the endpoints within your environment. Scans will be run to look for common indicators of compromise or indicators specific to your potential breach.
A Digital Forensic Compromise Assessment is a meticulous examination of an organisation's digital environment to detect and respond to indicators of compromise (IOCs) and potential security breaches. This proactive service is essential for identifying and mitigating cyber threats before they escalate into significant incidents that could compromise sensitive data or disrupt business operations.
Key components of a Digital Forensic Compromise Assessment include:

1. **Threat Hunting and Detection**: Our expert digital forensics team employs advanced tools and methodologies to actively search for signs of malicious activity within your digital infrastructure. This includes analysing system logs, network traffic, and endpoint data to identify anomalous behaviour indicative of a compromise.
2. **Incident Response Readiness**: We assess your organisation's incident response capabilities to ensure readiness in the event of a security incident. This involves reviewing incident response plans, assessing communication protocols, and conducting tabletop exercises to validate response procedures and improve overall preparedness.
3. **Forensic Analysis**: Upon detection of potential compromises, our digital forensic experts conduct in-depth analysis to determine the scope and impact of the incident. This includes examining forensic artifacts, conducting memory and disk forensics, and reconstructing the timeline of events to understand the attacker's tactics, techniques, and procedures (TTPs).
4. **Attribution and Intelligence Gathering**: In cases where attribution is possible, our experts gather intelligence on threat actors and their motivations, tactics, and infrastructure. This helps inform response strategies and strengthens defences against future attacks.
5. **Remediation and Recommendations**: Based on our findings, we provide actionable recommendations for remediation to mitigate the impact of the compromise and prevent future incidents. This may include implementing security controls, applying patches and updates, enhancing employee awareness training, and refining incident response procedures.
6. **Post-Assessment Support**: We offer ongoing support and guidance to help implement recommended remediation measures and enhance your organisation's security posture. This includes aiding with incident response activities, conducting follow-up assessments to measure effectiveness, and staying vigilant against emerging threats.

In summary, the PTP Digital Forensic Compromise Assessment is a proactive and comprehensive approach to identifying and mitigating security breaches within your organisation's digital environment. By leveraging advanced digital forensics techniques and expertise, we help you strengthen your security defences, minimize risk, and safeguard your critical assets against cyber threats.

Exposure Attack Surface Risk Assessment (CA Bolt-on)

As a bolt on to the PTP Compromise Assessment, an Exposure Attack Surface Risk Assessment is a comprehensive evaluation designed to identify and mitigate potential vulnerabilities in an organisation's digital infrastructure, applications, and systems. This assessment provides valuable insights into the organisation's exposure to cyber threats by analysing its attack surface – the sum of all points in an organisation's digital presence where an attacker could gain unauthorized access.
Key components of an Exposure Attack Surface Risk Assessment include:

1. **Discovery Phase**: This initial phase involves identifying and cataloguing all digital assets, including hardware, software, networks, cloud services, and web applications. This step provides a holistic view of the organisation's attack surface and helps identify potential blind spots or overlooked assets.
2. **Enumeration of Attack Vectors**: Once the digital assets are catalogued, the assessment focuses on enumerating the various attack vectors that could be exploited by threat actors. This includes vulnerabilities in software and firmware, misconfigurations in network devices, weak authentication mechanisms, and other potential weaknesses that could be leveraged to compromise the organisation's security.
3. **Assessment of Risk Exposure**: Each identified attack vector is assessed for its potential impact on the organisation's operations, data integrity, and confidentiality. This involves evaluating the likelihood of exploitation, the severity of potential consequences, and the organisation's existing security controls and resilience measures.
4. **Prioritization of Remediation Efforts**: Based on the risk exposure assessment, identified vulnerabilities are prioritized according to their severity and potential impact on the organisation. This helps focus remediation efforts on addressing the most critical vulnerabilities first, reducing the organisation's overall risk exposure in a targeted and efficient manner.
5. **Recommendations and Mitigation Strategies**: Finally, the assessment provides actionable recommendations and mitigation strategies to address identified vulnerabilities and reduce the organisation's exposure to cyber threats. This may include implementing software patches and updates, reconfiguring network devices, strengthening authentication mechanisms, and enhancing security awareness training for personnel.

In summary, a PTP Exposure Attack Surface Risk Assessment is a proactive measure to identify and mitigate potential vulnerabilities in an organisation's digital infrastructure. By conducting a thorough evaluation of the attack surface and prioritizing remediation efforts, organisations can strengthen their security posture and reduce the risk of cyber-attacks and data breaches.

Identity Risk Assessment (CA Bolt-on)

As a bolt on to the PTP Compromise Assessment, an Identity Risk Assessment is a crucial process aimed at evaluating the security posture of an organisation's identity and access management (IAM) systems.
It involves analysing the effectiveness of mechanisms put in place to manage user identities, access permissions, and authentication methods across digital platforms. This assessment is essential for identifying vulnerabilities, gaps, and potential weaknesses that could expose the organisation to security risks and unauthorized access.
Key components of an Identity Risk Assessment include:

1. **User Identity Management Review**: This phase involves examining the processes and procedures for creating, managing, and deprovisioning user identities within the organisation's systems. It includes evaluating user provisioning workflows, role-based access controls (RBAC), and account lifecycle management practices to ensure proper governance and minimize the risk of unauthorized access.

2. **Access Controls Analysis**: The assessment scrutinizes the access controls implemented within the organisation's systems to determine their effectiveness in enforcing the principle of least privilege. This involves reviewing access permissions, privilege escalation mechanisms, and segregation of duties to identify potential misconfigurations or overprivileged accounts that could be exploited by attackers.
3. **Authentication Mechanisms Evaluation**: Authentication methods such as passwords, multi-factor authentication (MFA), and single sign-on (SSO) are examined to assess their strength and resilience against various attack vectors. This includes evaluating password policies, MFA implementation, and the security of authentication protocols to ensure robust protection against credential-based attacks.
4. **Risk Scoring and Prioritization**: Identified risks and vulnerabilities are scored and prioritized based on their severity, likelihood of exploitation, and potential impact on the organisation. This helps focus remediation efforts on addressing the most critical identity-related threats first, reducing overall risk exposure effectively.
5. **Recommendations and Remediation Strategies**: The assessment provides actionable recommendations and remediation strategies to mitigate identified risks and strengthen the organisation's identity and access management practices. This may include implementing stronger authentication measures, refining access controls, enhancing user training and awareness, and deploying identity governance solutions to automate and enforce policy compliance.
6. **Continuous Monitoring and Improvement**: Finally, an Identity Risk Assessment is not a one-time activity but rather an ongoing process. Continuous monitoring of identity-related risks, periodic reassessments, and adjustments to security controls are essential to adapt to evolving threats and maintain a robust security posture over time.

In summary, a PTP Identity Risk Assessment is a proactive measure to evaluate and enhance the security of an organisation's identity and access management practices. By identifying and addressing vulnerabilities and weaknesses in IAM systems, organisations can effectively mitigate identity-related risks and protect sensitive assets from unauthorized access and data breaches.

Security and Hygiene Assessment

Hygiene & Security Assessment is designed to identify systemic weaknesses in security fundamentals that are commonly exploited by threat actors.
This assessment focuses on asset visibility, vulnerability exposure, and identity hygiene to establish a clear and repeatable security baseline across the organisation.
Key components of the Hygiene & Security Assessment include:

1. **Comprehensive Asset Discovery**
   Identification of all managed and unmanaged assets across endpoints, applications, and connected systems, including legacy or shadow IT that unnecessarily expands the attack surface.

2. **Account Activity and Identity Hygiene Review**
   Analysis of account usage, administrative access, authentication activity, and suspicious behaviours such as failed logins, credential misuse, and privilege escalation attempts.

3. **Targeted Vulnerability Identification**
   Human-led vulnerability analysis focused on real-world exploitability rather than raw vulnerability volume. Findings are mapped to business impact and attacker techniques.

4. **Risk-Based Prioritisation**
   Vulnerabilities and misconfigurations are prioritised based on exposure, likelihood of exploitation, and potential business impact to support efficient remediation.

5. **Actionable Reporting**
   Delivery of a detailed hygiene and vulnerability report, including executive summary, prioritised remediation actions, and best-practice recommendations.

This assessment helps organisations reduce unnecessary exposure, improve cyber resilience, and address the foundational issues that underpin the majority of successful compromises.

Threat Hunting

The Threat Hunting service provides a proactive, intelligence-led investigation to identify malicious activity that may have bypassed traditional security controls.
Unlike reactive alert-based monitoring, threat hunting is driven by informed hypotheses, attacker tradecraft, and real-world threat intelligence. This service is designed to uncover stealthy behaviours such as persistence mechanisms, credential abuse, lateral movement, and living-off-the-land techniques that frequently evade detection tools.
Key components of the Threat Hunting service include:

1. **Hypothesis-Driven Hunting**
   Our analysts develop targeted hunting hypotheses based on current threat intelligence, recent campaigns, industry-specific risks, and indicators observed during the Compromise Assessment.
2. **Endpoint Data Collection and Analysis**
   Threat hunting agents are deployed to collect high-fidelity endpoint telemetry. This data is analysed using a combination of automated queries and manual investigative techniques to identify anomalous or suspicious behaviour.
3. **Deep-Dive Threat Investigation**
   Identified anomalies are investigated in depth to determine whether they represent malicious activity, misconfiguration, or gaps in detection coverage.
4. **Detection Validation and Improvement**
   The hunt validates whether existing security controls are effective and highlights blind spots where attacker behaviour is not currently detected.
5. **Reporting and Recommendations**
   Findings are documented in a detailed threat hunting report, including confirmed threats, investigative evidence, and actionable remediation guidance.

Where indicators of compromise are identified, PTP will immediately engage with the client to discuss escalation into Incident Response. This service significantly reduces attacker dwell time and provides assurance over the effectiveness of existing security controls.

Dark Web Monitoring

Dark Web Monitoring provides proactive visibility into criminal ecosystems where credentials, internal data, and targeting intelligence are commonly traded or discussed prior to an attack.
This service monitors open, deep, and dark web sources to identify early indicators of compromise, data leakage, or adversary interest in the organisation.
Key components of the Dark Web Monitoring service include:

1. **Comprehensive Intelligence Coverage**
   Monitoring of forums, marketplaces, file-sharing sites, ransomware group channels, and encrypted communication platforms such as Telegram.

2. **Historical Baseline Assessment**
   An initial assessment reviewing up to 12 months of historical activity to establish a baseline of leaked credentials, breaches, or malicious chatter relating to the organisation.
3. **Continuous Monitoring and Alerting**
   Ongoing monitoring with scheduled reporting (daily or weekly) and real-time alerts for high-risk findings requiring immediate action.
4. **Actionable Intelligence Reporting**
   Findings are enriched, contextualised, and delivered as actionable intelligence rather than raw data feeds, enabling rapid and informed decision-making.
5. **Early Threat Disruption**
   Early warning enables credential resets, access reviews, and defensive hardening before an incident escalates into a full compromise.

This service enhances situational awareness and provides an additional defensive layer outside the traditional perimeter.