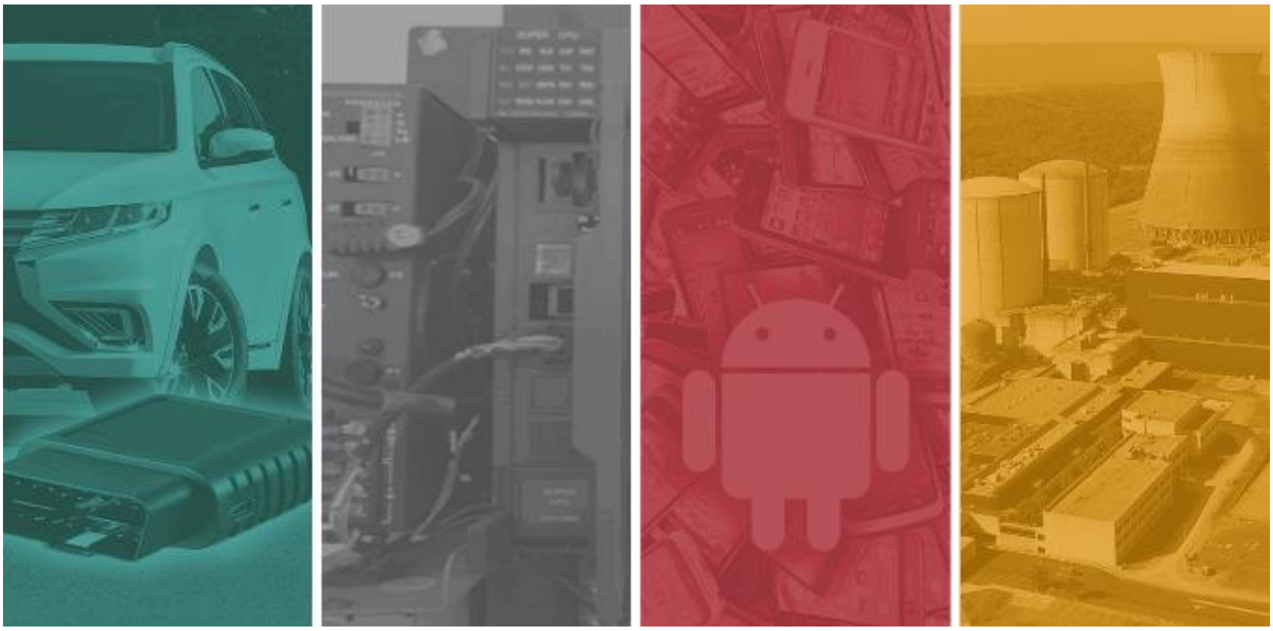
PTP Digital Forensic Incident Response Service Definition Document

G-Cloud – 14 (RM1557.14), Lot3 Cloud Support, Security Services



Version 1.0

Wednesday, 01 May 2024

Prepared by: PTP DFIR

DFIR Services and Methodology

1. 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.

1.1. PTP DFIR Services:

Services Type	Service	Services Type	Service
Reactive	Incident Response Retainer Service	Proactive	IR Maturity Assessment
	DFIR MDR Service		Compromise Assessments (CA)
	Incident Response (IR)		CA - Exposure Attack Surface Risk Assessment
	IR - Digital Forensics		CA - Identify Risk Assessment
	IR - eDiscovery		First Responder Training level 1
	IR - Root Cause and Impact Assessment		First Responder Training level 2
	IR - Business Email Compromise		Defender Compromise Assessment
	IR - Data Exfiltration Investigation		Ransomware Readiness Assessment
	IR - Mobile Device Forensics		DFIR vCISO
	IR - Data Recovery Service		Compromise Assessment - off Network
	IR - Digital Forensics Expert Witness Service		

1.2. 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.**

2. 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.

2.1. 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 <u>not</u> charged for any unused pre-authorised days.

In essence, an Incident Response Retainer is your proactive insurance policy against the 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.

2.2. 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.

2.3. Incident Response

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

2.4. 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.

2.5. DFIR eDiscovery

PTP DFIR eDiscovery offering provides a comprehensive solution for organisations navigating the complexities of digital forensics and electronic discovery. Designed to streamline the process of identifying, collecting, and analysing electronic data for legal and investigative purposes, our eDiscovery service ensures efficiency, accuracy, and compliance every step of the way.

At its core, DFIR eDiscovery combines the expertise of our Digital Forensics and Incident Response (DFIR) team with advanced technology and best practices in electronic discovery. Whether you're facing litigation, regulatory inquiries, or internal investigations, our seasoned professionals are equipped to handle the intricacies of digital evidence collection and analysis with precision and discretion.

From identifying relevant data sources to preserving and extracting electronic evidence, the PTP DFIR experts employ industry-leading tools and methodologies to ensure a defensible and efficient eDiscovery process. We will work closely with your legal team to understand the specific requirements of your case and tailor our approach, accordingly, minimising risk and maximising results.

Furthermore, PTP DFIR eDiscovery offering goes beyond mere data collection and analysis. PTP provide comprehensive reporting and documentation to support your legal strategy, empowering you with the insights and evidence needed to make informed decisions and navigate the legal landscape with confidence.

In essence, PTP DFIR eDiscovery offering is your trusted partner in navigating the intersection of technology, law, and investigation. With our expertise and dedication to excellence, we help you unlock the full potential of electronic evidence, enabling you to achieve your legal objectives efficiently and effectively.

2.6. 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

2.7. 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.

2.8. 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.

2.9. 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.

2.10. Data Recovery Service

The loss of data, whether through intentional or accidental actions, can be devastating to an individual or organisation, regardless of the circumstances.

Using a comprehensive toolset, PTP can attempt recover data deleted from physical drives regardless of the nature of its loss. In some instances, it may even be possible to decrypt data that has been subjected to encryption.

2.11. 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.

3. Proactive Services – Non-Breach Dependant

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

3.1. IR Maturity Assessment

The PTP Incident Response (IR) Maturity Assessment service offers a comprehensive evaluation of your organisation's readiness to effectively respond to cyber incidents. Over two days, our expert-led workshops delve into your current IR processes, procedures, and technologies. Following this, a dedicated one-day reporting session provides a detailed assessment report, including findings, recommendations, and a roadmap for enhancing your IR maturity level. With our tailored insights and strategic guidance, you can strengthen your incident response capabilities and better prepare for cyber threats.

1. **Evaluation of Current Processes**: Assess the effectiveness of existing incident response processes, including incident detection, analysis, containment, eradication, and recovery.
2. **Examination of Procedures**: Review documented procedures and protocols for incident response, including communication plans, escalation procedures, and post-incident analysis.
3. **Analysis of Technologies**: Evaluate the efficacy of incident response technologies, such as SIEM (Security Information and Event Management) solutions, endpoint detection and response (EDR) tools, and forensic capabilities.
4. **Assessment of Personnel Training**: Review the training and awareness programs for incident response personnel, ensuring they are equipped with the necessary skills and knowledge to respond to cyber incidents effectively.
5. **Identification of Gaps and Weaknesses**: Identify gaps, weaknesses, and areas for improvement in current incident response capabilities, including process inefficiencies, technology limitations, and skills shortages.
6. **Development of Improvement Roadmap**: Provide recommendations and a roadmap for enhancing IR maturity, outlining actionable steps to address identified gaps, improve processes, and strengthen incident response capabilities.
7. **Alignment with Best Practices and Standar**ds: Ensure alignment with industry best practices and standards for incident response, such as the NIST Cybersecurity Framework, ISO/IEC 27035, and SANS Incident Response.
8. **Continuous Improvement Planning**: Establish a framework for ongoing monitoring, evaluation, and enhancement of incident response capabilities, enabling continuous improvement and adaptation to evolving cyber threats.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. First Responder Training Level 1 & 2

Training for those responsible for the initial response to an enterprise cyber security incident.

Training will equip attendees with:

- How to detect abnormalities or threats - Attack kill chain
- How to identify a cyber incident - different types of threats (internal and external) and HR related policy breaches.
- How to identify and preserve evidence for further analysis - Processes and services, Network traffic, Malware, and Memory.
- Use of tools such as ProcessMonitor, TCPDump, and Memory capture.
- How to use the Observe, Orient, Decide, and Act model.

Training is aimed at those likely to provide the initial response, such as IT staff, SOC staff, Network administrators, Information security staff.

Level 1 training focuses on the Windows operating system and utilises many tools from the Sysinternals suite.

Level 2 includes some Linux threat hunting and is more advanced, aimed at SOC and internal incident response teams.

3.6. Ransomware Readiness Assessment

A PTP Ransomware Readiness Assessment is a proactive measure aimed at evaluating an organisation's resilience to ransomware attacks and strengthening its defences against this increasingly prevalent threat. This comprehensive assessment, delivered through workshops, provides valuable insights into the organisation's preparedness, identifies potential vulnerabilities, and offers actionable recommendations to enhance its ability to prevent, detect, and respond to ransomware incidents.

Key components of a Ransomware Readiness Assessment utilizing workshops include:

1. **Workshop Sessions**: The assessment kicks off with interactive workshop sessions facilitated by PTP cybersecurity experts. These workshops engage key stakeholders across the organisation, including IT personnel, security teams, executives, and other relevant stakeholders. Through collaborative discussions and exercises, participants gain a deeper understanding of ransomware threats, attack vectors, and best practices for mitigation.

2. **Risk Identification and Assessment**: During the workshops, participants work together to identify and assess potential ransomware risks and vulnerabilities within the organisation's IT infrastructure, systems, and processes. This may include evaluating security controls, user awareness, backup and recovery procedures, network segmentation, and incident response capabilities.
3. **Scenario-Based Exercises**: Optionally, the assessment may include scenario-based exercises to simulate ransomware attacks and test the organisation's response capabilities. These exercises provide valuable insights into the effectiveness of existing security measures, incident response procedures, and employee awareness training. Participants have the opportunity to practice their response in a controlled environment and identify areas for improvement.
4. **Gap Analysis and Recommendations**: Following the workshop sessions, the PTP assessment team conducts a comprehensive gap analysis to identify areas where the organisation may be susceptible to ransomware attacks. Based on the findings, actionable recommendations are developed to strengthen security controls, enhance incident response procedures, and improve overall resilience to ransomware threats.
5. **Customised Roadmap**: The PTP assessment culminates in the development of a customized roadmap that outlines prioritized actions and milestones for enhancing ransomware readiness. This roadmap is tailored to the organisation's specific needs, budget constraints, and risk tolerance, providing a clear path forward for implementing recommended improvements.
6. **Optional Testing and Evidence Gathering**: Depending on the organisation's requirements and scoping, the assessment may include optional testing and evidence gathering to validate the effectiveness of security controls and response procedures. This may involve penetration testing, vulnerability assessments, or tabletop exercises to further assess the organisation's readiness and validate the effectiveness of proposed solutions.

In summary, a PTP Ransomware Readiness Assessment delivered through workshops offers organisations a proactive approach to evaluating and enhancing their resilience to ransomware attacks. By engaging key stakeholders, identifying risks, and providing actionable recommendations, organisations can strengthen their defences and mitigate the impact of ransomware incidents on their operations and reputation.

3.7. Defender Compromise Assessment

A PTP Compromise Assessment leveraging Defender for Endpoint and Sentinel is a comprehensive service designed to proactively detect and respond to potential security breaches and compromises within an organisation's digital environment. By harnessing the power of Microsoft's advanced threat protection solutions, this assessment offers unparalleled visibility, threat intelligence, and response capabilities to safeguard against sophisticated cyber threats.

Key components of a PTP Compromise Assessment utilizing Defender for Endpoint and Sentinel include:

1. **Endpoint Detection and Response (EDR)**: Defender for Endpoint provides real-time visibility into endpoint activities, allowing for the detection of suspicious behaviour and potential indicators of compromise (IOCs) across the organisation's devices. Through advanced behavioural analytics and machine learning algorithms, Defender for Endpoint identifies and prioritizes security alerts, enabling swift response to potential threats.
2. **Threat Intelligence Integration**: Sentinel leverages Microsoft's vast threat intelligence network to correlate security events and identify emerging threats across the organisation's digital ecosystem. By aggregating and analysing data from multiple sources, including Defender for Endpoint, Sentinel provides actionable insights into potential security incidents, enabling proactive threat hunting and response.
3. **Incident Investigation and Forensics**: In the event of a suspected compromise, the Compromise Assessment utilizes Defender for Endpoint and Sentinel to conduct detailed investigations and forensic analysis to determine the scope and impact of the incident. This includes analysing endpoint telemetry data, network traffic, and other digital artifacts to reconstruct the attack chain and identify the root cause of the compromise.
4. **Response and Remediation**: Leveraging the capabilities of Defender for Endpoint and Sentinel, the assessment facilitates rapid response and remediation efforts to contain and mitigate security incidents. This may include isolating compromised endpoints, blocking malicious activities, applying security updates and patches, and implementing security controls to prevent future incidents.
5. **Continuous Monitoring and Threat Hunting**: Beyond incident response, the Compromise Assessment provides continuous monitoring and proactive threat hunting to identify and mitigate potential security risks before they escalate. By leveraging Defender for Endpoint's behavioural analytics and Sentinel's threat intelligence, the assessment helps organisations stay ahead of evolving threats and maintain a strong security posture over time.

In summary, the PTP Compromise Assessment utilizing Defender for Endpoint and Sentinel offers organisations a comprehensive solution for detecting, investigating, and responding to potential security compromises. By leveraging Microsoft's advanced threat protection capabilities, organisations can effectively safeguard their digital assets and mitigate the impact of cyber threats on their operations.

3.8. DFIR vCISO

PTP DFIR (Digital Forensics and Incident Response) vCISO (virtual Chief Information Security Officer) is a strategic cybersecurity service that combines the expertise of digital forensics and incident response with the leadership and guidance of a seasoned CISO. This service provides organisations with access to a dedicated virtual CISO who specializes in leading and managing cybersecurity initiatives, particularly in the areas of incident response and forensic investigations.

Key components of a DFIR vCISO service include:

1. **Strategic Leadership**: The PTP DFIR vCISO serves as a trusted advisor to the organisation's executive leadership, providing strategic guidance and direction on cybersecurity matters. Drawing upon extensive experience in cybersecurity and incident response, the vCISO helps align cybersecurity initiatives with the organisation's business goals and objectives.
2. **Incident Response Planning and Management**: The vCISO leads the development and implementation of comprehensive incident response plans tailored to the organisation's unique risk profile and compliance requirements. In the event of a security incident, the vCISO orchestrates the organisation's response efforts, coordinating with internal teams, external stakeholders, and regulatory authorities to mitigate the impact of the incident and restore normal operations.
3. **Forensic Investigations**: Leveraging expertise in digital forensics and incident response, the vCISO oversees forensic investigations into security incidents, such as data breaches, malware infections, and insider threats. Working closely with the organisation's internal teams or external forensic specialists, the vCISO conducts thorough examinations of digital evidence to determine the root cause of the incident and identify potential remediation measures.
4. **Security Program Development**: The vCISO assists in the development, implementation, and enhancement of the organisation's cybersecurity program, ensuring that it aligns with industry best practices, regulatory requirements, and emerging threats. This includes evaluating existing security controls, identifying gaps and weaknesses, and recommending improvements to strengthen the organisation's security posture.
5. **Vendor and Third-Party Management**: The vCISO provides oversight and guidance on vendor and third-party risk management, helping the organisation assess the security posture of its suppliers, partners, and service providers. This includes evaluating vendor contracts, conducting security assessments, and implementing risk mitigation measures to protect the organisation's sensitive data and assets.
6. **Training and Awareness**: The vCISO develops and delivers cybersecurity training and awareness programs for employees at all levels of the organisation, fostering a culture of security awareness and accountability. This includes providing education on cybersecurity best practices, conducting simulated phishing exercises, and promoting vigilance in identifying and reporting security threats.

In summary, the PTP DFIR vCISO service offers organisations access to experienced cybersecurity leadership and expertise, particularly in the areas of incident response and digital forensics. By partnering with a virtual CISO, organisations can enhance their cybersecurity capabilities, mitigate risks, and protect against the ever-evolving threat landscape.

3.9. Off-Network Compromise Assessment

The PTP Off-Network Compromise Assessment is a specialised cybersecurity service tailored to assess and enhance the security posture of Internet of Things (IoT) and Industrial Control Systems (ICS) networks and infrastructure. This assessment is particularly crucial for organisations operating critical infrastructure or relying heavily on interconnected IoT devices, where traditional security measures may be insufficient to protect against sophisticated cyber threats.

Key components of an Off-Network Compromise Assessment utilizing Velociraptor and conducted in person on site include:

1. **On-Site Assessment**: Our cybersecurity experts conduct the assessment in person, on-site, to gain firsthand insight into the organisation's IoT and ICS networks and infrastructure. This allows for a comprehensive examination of devices, systems, and protocols, ensuring that no potential vulnerabilities or compromises are overlooked.
2. **Velociraptor Deployment**: Velociraptor, an open-source endpoint visibility and forensics tool, is deployed within the organisation's environment to collect and analyse telemetry data from endpoints and networked devices. Velociraptor enables real-time monitoring and forensic analysis, providing valuable insights into potential security threats and suspicious activities.
3. **Network and Endpoint Visibility**: Velociraptor facilitates deep visibility into the organisation's network and endpoints, allowing for the detection of anomalous behaviour, unauthorized access attempts, and potential indicators of compromise (IOCs). By analysing telemetry data from endpoints and network traffic, Velociraptor helps identify security risks and vulnerabilities that may be lurking within the organisation's infrastructure.
4. **Threat Hunting and Investigation**: Our cybersecurity experts leverage Velociraptor's powerful capabilities to conduct proactive threat hunting and forensic investigations within the organisation's environment. This involves analysing endpoint telemetry data, examining system artifacts, and reconstructing the timeline of events to identify and mitigate potential compromises or security incidents.
5. **Recommendations and Remediation**: Based on the findings of the assessment, our cybersecurity experts provide actionable recommendations and remediation strategies to strengthen the organisation's security posture. This may include implementing security controls, updating configurations, patching vulnerabilities, and enhancing incident response procedures to mitigate identified risks and vulnerabilities.

6. **Customized Reporting and Documentation**: The assessment concludes with the delivery of a comprehensive report detailing the findings, analysis, and recommendations derived from the assessment. The report is tailored to the organisation's specific needs and requirements, providing clear and actionable insights to support informed decision-making and risk management efforts.

In summary, the PTP Off-Network Compromise Assessment conducted in person, on site, utilizing Velociraptor offers organisations operating IoT and ICS networks and infrastructure a proactive approach to identifying and mitigating potential security risks and vulnerabilities. By leveraging advanced endpoint visibility and forensics capabilities, organisations can strengthen their security defences and safeguard critical assets against cyber threats.

4. Introduction to PTP

Pen Test Partners LLP is focussed on delivering innovative and meaningful penetration testing. It's a simple mandate, and one that we have built our business and reputation with.

Why choose Pen Test Partners?

Established in June 2010, we've got consultants with a vast range of skills and experience, some with extremely niche skills.

As an entire company we know our stuff and we'll work at your pace.

We research, test, and assure a lot of interesting and complex things!

We've provided testing and assurance for all sorts of things; ships at sea, international finance infrastructure, mobile apps for smart toys, airplane systems and avionics, power stations and critical national infrastructure, automotive and telematics, mobile banking apps, physical security, cloud services to rail infrastructure.

Our Credentials

PTP are a CREST, CBEST, ASSURE, STAR, CSIR, NCSC CIR L2, CHECK, Tigerscheme, PCI QSA, ISO27001, Cyber Essentials/+ accredited ; this ensures the highest quality of testing.

All PTP staff are vetted prior to commencement of employment in line with British Standard 7858 Clearance Service and through the Disclosure and Barring Service (DBS). National Vetting Solutions. All our security consultants are a minimum of SC cleared.

What we provide

Responsiveness

We are recognised as being extremely responsive. We can begin an engagement with as little as 24 hours' notice.

Follow-up

One of the reasons we have such loyal clients is the availability our consultants have for follow-up work.

Ongoing guidance

Once an engagement is over… It's never truly over, there will always be questions, queries, and advice needed, so we make a point of always being available post engagement.

Our Reputation

The BBC and other news agencies often contact us to comment on the latest cyber news.

We are frequently called upon to provide keynotes at events such as BSides, TED talks, InfoSecurity Europe and the US Chamber of commerce.

We can't name names, but our clients come from a wide range of verticals and sizes including:

Automotive, Banking, Education, Engineering, Energy, Oil & Gas, FinTech, Government, Healthcare, Manufacturing, Retail, Telco’s, Insurance, Legal, Transport and Finance.