**Cytomate**

**Incident Response**

**Service Offering for Lekhwiya**

Table of Contents

[Executive Summary 2](#_Toc207013601)

[Purpose 2](#_Toc207013602)

[The challenge 2](#_Toc207013603)

[Countering the Unknown 2](#_Toc207013604)

[Why Cytomate? 3](#_Toc207013605)

[Threat Hunting 3](#_Toc207013606)

[Preparation and Hypothesis Building 3](#_Toc207013607)

[Data Collection & Normalization 4](#_Toc207013608)

[Threat Hunting 4](#_Toc207013609)

[Analysis and Validation 4](#_Toc207013610)

[Documentation & Reporting 5](#_Toc207013611)

[Attack Surface Management 5](#_Toc207013612)

[DFIR Methodology 5](#_Toc207013613)

[Incident Response Life Cycle 5](#_Toc207013614)

[Preparation 6](#_Toc207013615)

[Detection and Analysis 6](#_Toc207013616)

[Containment, Eradication and Recovery 7](#_Toc207013617)

[Post-Incident Response 9](#_Toc207013618)

[Digital Forensics Areas 9](#_Toc207013619)

[Computer Forensics 10](#_Toc207013620)

[Live Forensics 10](#_Toc207013621)

[Network Forensics 10](#_Toc207013622)

[Forensic Methodology 11](#_Toc207013623)

[Assessment and Scenarios 11](#_Toc207013624)

[Evidence and Artifact Extraction 11](#_Toc207013625)

[Analysis 13](#_Toc207013626)

[Report 13](#_Toc207013627)

[Roles and Responsibilities 13](#_Toc207013628)

[Resource Communication Matrix 14](#_Toc207013629)

[On-Demand Delivery Timeline 15](#_Toc207013630)

# Executive Summary

## Purpose

This proposal outlines the scope of work, methodologies, industry standards, roles, and responsibilities for providing Incident Response (IR) services to Lekhwiya. Over the course of 40 hours annually, we will deliver top-tier incident response services, ensuring Lekhwiya readiness and resilience against cyber threats. Our approach emphasizes the seamless integration of our IR services within the existing cybersecurity framework, enhancing the ability to safeguard critical assets, maintain operational continuity, and meet regulatory compliance requirements. By leveraging industry-leading practices and cutting-edge tools, we aim to provide Lekhwiya with a robust and scalable defense mechanism against an ever-evolving threat landscape.

## The challenge

Many companies nowadays are faced with multiple types of cyber threats aimed at disrupting their productivity leading to financial losses and harming their reputation.

Cytomate Incident Response team helps **companies detect, contain and investigate** such threats motivated by one of the following:

## Countering the Unknown

Leveraging our expertise as well as our proven products, **Breach and Attack Simulation (Breach+) and Attack Surface Management (Racid)**, Cytomate IRR guarantees a fast engagement led by a team of professional expert responders who will intervene in case of breach alert, analyze the malicious activities, pinpoint their source and impact, then eradicate any persistent threats, and even reverse engineer malware to understand the way they operate, then come up with the appropriate Indicators of Compromise (IOC) for future prevention. Our team would thoroughly **study threat actors** and tackle their malicious attempts by identifying their intention, motivation, source, behavior, impact, then providing digital proof of the potential cybercrime while also extending recommendations for future prevention.

# Why Cytomate?

Nowadays attacks have become more sophisticated hence a traditional and time-sensitive DFIR approach, relying primarily on **manual intervention** techniques, **is no longer sufficient**. Time to Respond to an incident is precious and we continuously strive **to minimize the time spent on responding** to an incident before it leads to grave reputation, operational and financial losses. Cytomate has developed a comprehensive approach to respond to modern-day attacks leveraging the latest **AI powered Tactics, Techniques, and Procedures (TTPs)** setting the scene for an efficient IR process. This approach would lead to a high level of protection enabling customers to detect threats, investigate incidents, and remediate a breach in record times.

To respond to breaches effectively and efficiently against today’s sophisticated attacks, the below points are key components in our DFIR approach:

# Threat Hunting

## Preparation and Hypothesis Building

Before hunting, we define what we are looking for:

1. **Understand the environment:**
   * Network architecture (internal, external, cloud, hybrid).
   * Operating systems in use (Windows, Linux, macOS).
   * Security controls (EDR, NDR, SIEM, Firewall, etc.).
   * Logging sources (Sysmon, Windows Event Logs, Syslog, NetFlow, PCAP, DNS logs, etc.).
2. **Define threat model:**
   * Which adversaries or TTPs are most likely to target our organization?
   * Use threat intel (MITRE ATT&CK, advisories, ISACs, CTI feeds, Commercial Feeds).
3. **Formulate hunting hypotheses:**
   * Examples:
     + If an attacker deploys credential dumping tools (like Mimikatz), there should be unusual LSASS memory access events.
     + If an attacker is performing lateral movement with PsExec, there should be abnormal service creation events.

## Data Collection & Normalization

A hunt is only as good as the data we work with.

1. **Ensure visibility:**
   * Host-based: Sysmon, EDR telemetry, registry, file creation, process execution logs.
   * Network-based: PCAP, NetFlow, DNS queries, proxy logs.
   * Cloud: Audit logs, API activity.
2. **Centralize in a SIEM or Data Lake (e.g., Azure Sentinel, Splunk, ELK).**
3. **Normalize & enrich logs** with:
   * Time correlation.
   * Asset/user context (who owns the machine, AD group, business criticality).
   * Threat intelligence feeds (known IOCs, suspicious domains, hash reputation).

## Hunting

We are actively looking for anomalies and malicious behaviors in different types of logs:

1. **Hypothesis-driven hunting**

* Start from the hypothesis.
* Write queries (KQL, Splunk SPL, Sigma rules) to look for related activity.
* Example:
  + Hypothesis: “Adversaries might use PowerShell to download payloads.”
  + Query: Look for powershell.exe with command lines containing IEX, DownloadString, Invoke-WebRequest.

1. **Data-driven (Exploratory) hunting**

* Instead of starting with a hypothesis, look for **statistical anomalies**:
  + Rare process executions (e.g., rundll32.exe spawning cmd.exe).
  + Unusual logon hours.
  + Spikes in DNS requests to external domains.
  + Abnormal parent-child process relationships.
  + Use of Threat Intel feeds to hunt latest attacker behaviors.

1. **Technique-based hunting**

* Use frameworks like **MITRE ATT&CK** to pick TTPs (e.g., T1059: Command-Line Interface) and search for activity aligned with them.

## Analysis and Validation

1. **Separate noise from true positives:**
   * Investigate anomalies by pivoting across multiple datasets.
   * Correlate with threat intel (is the IP/domain malicious?).
   * Check baselines (is this process normal for this user/system?).
2. **Enrichment:**
   * Sandbox suspicious files.
   * Reverse engineer suspicious binaries or scripts.
   * Pivot on related hashes, registry keys, or network connections.

## Documentation & Reporting

1. Record findings clearly for SOC, IR, or management:
   * **What was found** (event, process, artifact).
   * **Why it is suspicious** (mapped to MITRE ATT&CK TTPs).
   * **Evidence** (screenshots, logs, queries).
   * **Next steps** (containment, deeper IR, rule creation).

# Attack Surface Management

Cytomate uses its own proprietary Attack surface management tool called **RACID** for active scanning, asset discovery, vulnerability management etc.

1. **Regular Scanning**: Continuously scan for exposed assets, vulnerabilities, and misconfigurations to keep visibility up to date.
2. **Risk Prioritization**: Score and rank findings based on asset criticality, exposure, and real-world threat activity.
3. **Remediation Guidance**: Provide actionable fixes, assign ownership, and validate through re-scans to ensure closure.

# DFIR Methodology

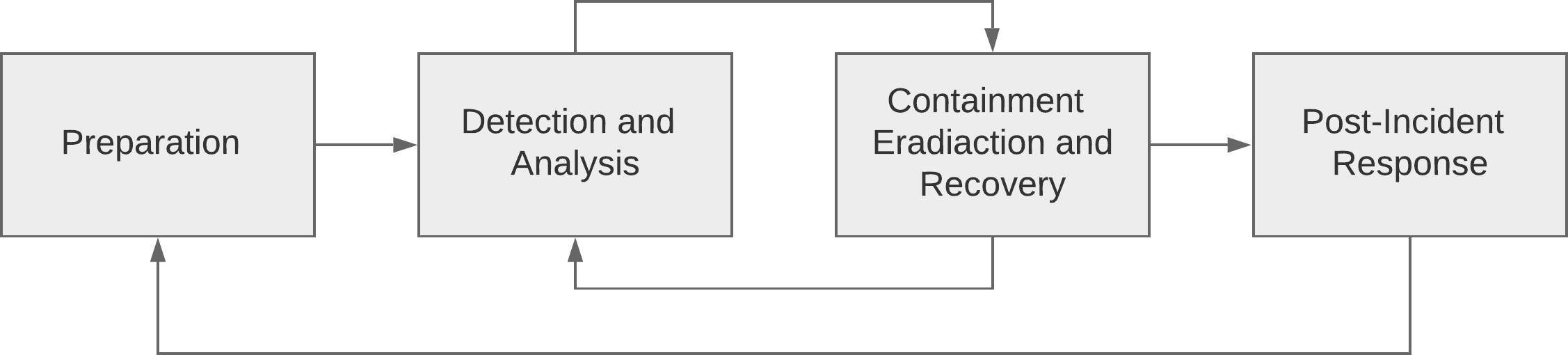
Cytomate is committed to providing comprehensive Digital Forensics and Incident Response (DFIR) services methodology designed to protect, detect, respond, and recover from security incidents. Our IR capabilities ensure that Lekhwiya is equipped with the expertise and processes necessary to manage and mitigate cybersecurity incidents effectively.

## Incident Response Life Cycle

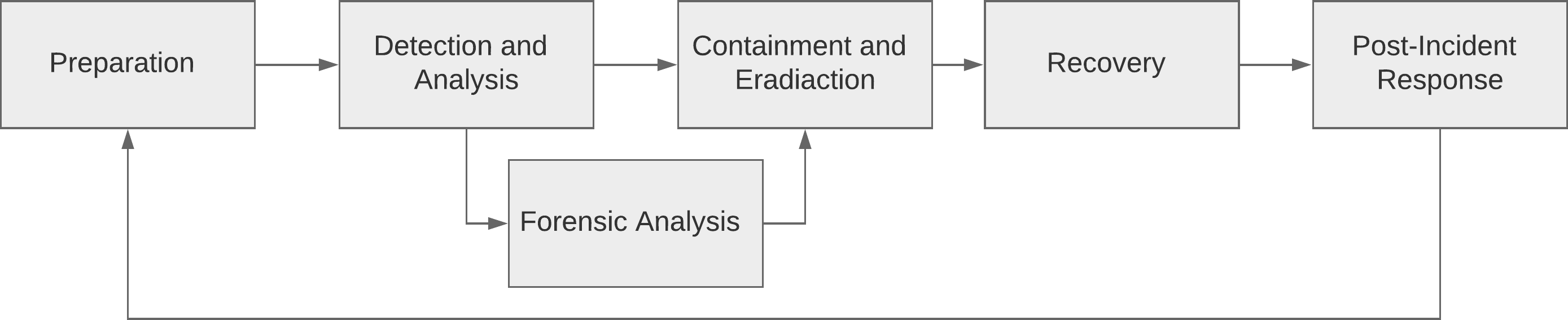
Prevention and reaction to the different security incidents create the incident response scope. This is one of the many security measures and cannot and should not be understood as an isolated proposal. Incident response is the final stage of defense, where, once a cybersecurity incident has occurred, it is necessary to intervene to contain, study, and eradicate it. This whole process serves, in the future, to prevent incidents of the same nature.

It is divided into different phases, their number varying according to the guides and sources consulted. However, for this scope, we divided our IR phases as follows:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned



Incident Response Life Cycle



Incident Response Life Cycle and Forensics

### Preparation

The Preparation Phase of Incident Response (IR) is essential for establishing the framework and readiness required to effectively manage security incidents. This phase involves developing a comprehensive Incident Response Plan (IRP), which defines procedures, communication protocols, and roles. Key activities include the deployment of security technologies (e.g., IDS, SIEM), regular training, and simulations to ensure the incident response team is proficient and ready to act decisively. Additionally, maintaining an up-to-date inventory of assets and implementing robust backup strategies are crucial to minimizing the impact of any potential security breach. Proper preparation ensures swift, efficient, and effective incident management, reducing downtime and ensuring operational continuity.

Detection and Analysis

The Detection and Analysis phase is a critical component of the Incident Response (IR) lifecycle, focusing on identifying, validating, and understanding security incidents to enable an effective and timely response. This phase begins with the continuous monitoring of network traffic, system logs, and endpoint activities using advanced security tools such as Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) platforms, and Endpoint Detection and Response (EDR) solutions. These tools are configured to detect anomalies, suspicious behavior, or patterns that could indicate a security breach, using techniques like signature-based detection, anomaly-based detection, and behavioral analysis.

When an alert is generated, it undergoes a triage process to determine its legitimacy, severity, and potential impact. This involves correlating the alert with other data sources, such as firewall logs, vulnerability scanners, and threat intelligence feeds, to validate the incident and assess its scope. Analysts will examine Indicators of Compromise (IOCs), such as unusual IP addresses, domain names, file hashes, or specific network traffic patterns, to determine if malicious activity is present. The analysis may involve examining memory dumps, disk images, and volatile data to identify artifacts left by the attacker, such as malware, rootkits, or evidence of lateral movement.

Detailed timeline reconstruction is crucial in this phase, as it helps analysts understand the sequence of events, from the initial compromise to the current state of the incident. This often involves analyzing logs from various sources (e.g., web servers, application servers, and authentication systems) to map out the attacker’s actions and identify any backdoors, persistence mechanisms, or data exfiltration attempts. Advanced techniques, such as reverse engineering malware or analyzing network traffic captures, may be employed to gain deeper insights into the attack's nature, objectives, and potential threat actors.

### Containment, Eradication and Recovery

The Containment, Eradication, and Recovery phase of Incident Response (IR) is where the organization takes decisive action to control the incident, eliminate the threat, and restore normal operations. Each of these steps is critical in mitigating the impact of a security breach, preserving forensic evidence, and ensuring that the incident does not recur.

**Containment**

Containment is the first step in this phase and aims to limit the spread and impact of the incident while a full response strategy is formulated. Containment strategies can be divided into two categories:

* **Short-Term Containment:** This is an immediate action taken to prevent further damage. Techniques include isolating affected systems from the network, disabling compromised accounts, or rerouting network traffic. These actions are typically quick and aim to stop the attack in its tracks without disrupting operations more than necessary.
* **Long-Term Containment:** Once the immediate threat is controlled, long-term containment strategies are implemented to maintain isolation while forensic analysis and system remediation are conducted. This may involve deploying patches, applying configuration changes, or setting up temporary security measures like enhanced monitoring or additional firewalls. In some cases, it might involve creating forensic images of compromised systems to preserve evidence before any changes are made.

Throughout the containment process, it’s crucial to monitor the affected systems for any signs of persistence mechanisms or secondary attacks. The incident response team should document all actions taken and maintain close communication with stakeholders to ensure they are informed of the situation and any potential impact on operations.

**Eradication**

Once containment is achieved, the eradication phase focuses on removing the root cause of the incident and any associated artifacts from the environment. This step is crucial to ensure that the threat actor no longer has access to the network and that no residual malware or vulnerabilities remain that could be exploited in the future.

**Key eradication activities include:**

* **Malware Removal:** Using specialized tools to scan and remove malicious code from infected systems. This may involve running antivirus software, specialized malware removal tools, or manual removal processes.
* **Patch Management:** Applying patches or updates to vulnerable systems that were exploited during the attack. This might include operating system patches, application updates, or firmware upgrades.
* **Credential Management:** Resetting passwords, updating authentication mechanisms, and revoking compromised certificates or keys to ensure that threat actors no longer have access to any compromised accounts.
* **System Hardening:** Implementing additional security measures, such as disabling unused services, enabling security configurations, or tightening access controls, to prevent re-exploitation of any vulnerabilities.
* **Log Analysis and Audit:** Reviewing logs and audit trails to ensure that all signs of the attacker’s presence have been identified and removed. This helps in verifying that no backdoors or persistence mechanisms remain in the environment.

Eradication should be thorough, as any missed artifacts or vulnerabilities could lead to a re-compromise of the system. Documentation during this phase is essential to record the steps taken and the findings, which will be useful for post-incident analysis and future prevention efforts.

**Recovery**

The recovery phase is focused on restoring affected systems and services to normal operation, ensuring that they are free of any compromise, and that business continuity is maintained. Recovery must be carefully planned to avoid reintroducing the threat into the environment.

**Key recovery activities include:**

* **System Restoration:** Restoring systems from clean backups, reimaging compromised machines, or rebuilding systems from the ground up, ensuring they are fully patched and secure before reintroduction to the production environment.
* **Data Recovery:** Restoring data from backups, verifying its integrity, and ensuring that no malicious data is reintroduced during the process. This may also involve recovering encrypted or corrupted data if the attack involved ransomware.
* **System Testing:** Conducting thorough testing of restored systems to ensure they are functioning correctly and securely. This includes vulnerability scanning, penetration testing, and verifying that all security controls are functioning as intended.
* **Enhanced Monitoring:** Implementing heightened monitoring on restored systems to detect any signs of residual threats or new attacks. This might involve more frequent log reviews, real-time alerts, or additional security controls.
* **Gradual Reintegration:** Reintroducing systems into the production environment in stages to minimize the impact on operations and to ensure that if any issues arise, they can be quickly isolated and addressed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident** | **Example** | **Response** | **Outcome** |
| DoS Attack | DDoS attack (A Popular Distributed Denial of Service Attack) | Reconfigure router to minimize effect of the flooding | Effects of attack mitigated by router countermeasures. Establishment of perpetrator’s identity may require too many resources to be worthwhile investment. |
| Unauthorized use | Using work computers to surf pornography sites | Possible forensic duplication and investigation. Interview with suspect. | Perpetrator identified, and evidence collected for disciplinary action. Action taken may depend on employee’s position, or past enforcement of company policy |
| Vandalism | Defaced web site | Monitor web site. Repair web site. Investigate web site while it is online. Implement web site “refresher” program. | Web site restored to operational status. Decision to identify perpetrator may involve law enforcement. |
| Theft of Information | Stolen credit card and customer information from company database | Make public affairs statement. Forensic duplication of relevant systems. Investigation of theft. Law enforcement contacted. | Detailed investigation initiated. Law enforcement participation possible. Civil complaint filed to recover potential damages. Systems potentially offline for some time. |
| Computer intrusion | Remote administrative access via attacks such as buffer overflow and Internet Information Services (IIS) attacks | Monitor activities of attacker. Isolate and contain scope of unauthorized access. Secure and recover systems. | Vulnerability leading to intrusion identified and corrected. Decision made whether to identify perpetrators. |

### Post-Incident Response

The final phase of any incident response process is, in itself, one of the most important. It is about learning and improvement. Highlighting what has happened and the intelligence that has been extracted from it is fundamental to the entire cybersecurity infrastructure, feeding back with each incident and threat. Helping to prevent future threats.

There are different ways to achieve this response. It is essential for good cybersecurity management that the knowledge and expertise gained from the threat is passed on to the lower levels of the SOC, facilitating the future work of all teams and improving their experience. It is also possible to share this knowledge with the community through the MITRE ATT&CK framework.

## Digital Forensics Areas

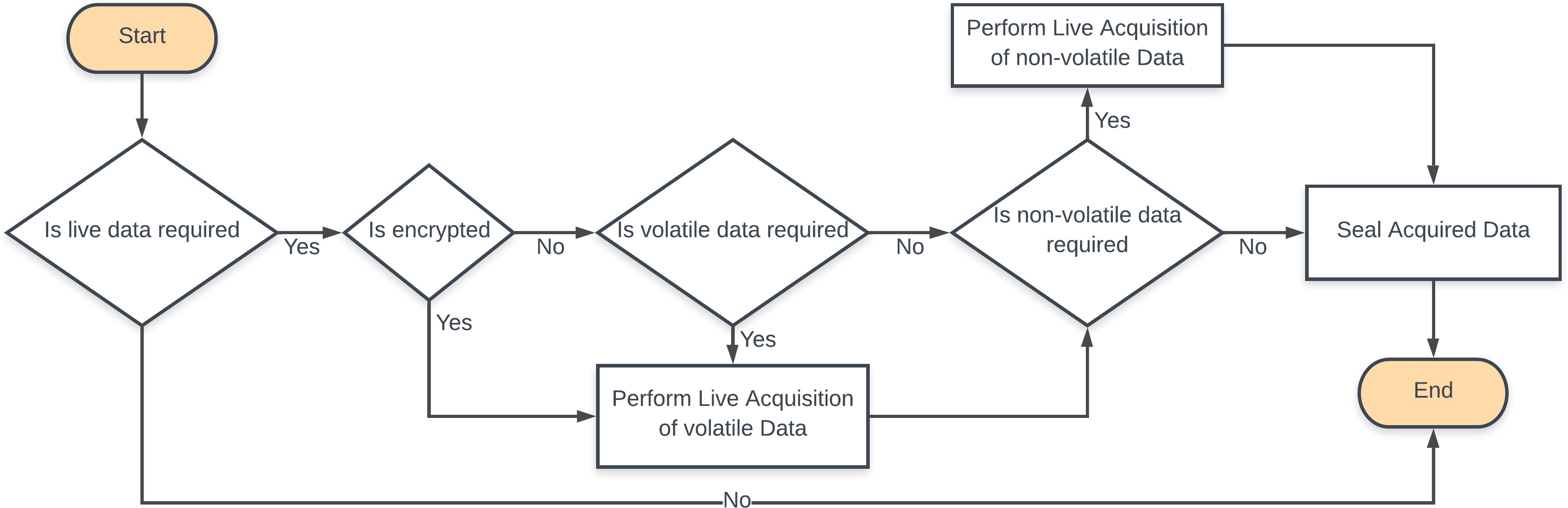
Digital forensics refers to a global idea, and although its original conception adhered to a single definition, it has now been partially fragmented by the great evolution that computer science has undergone. It is divided into the following areas: Computer Forensics, Live Forensics, Mobile Forensics, Network Forensics and Database Forensics. All these fields are of importance, however, due to the structure and approach of our methodology we will focus mostly on Computer and Live Forensics on Microsoft Windows environments.

Computer Forensics

Computer forensics, or digital forensics, involves the meticulous process of collecting, preserving, analyzing, and presenting digital evidence from electronic devices. It typically begins with forensic imaging, creating a bit-by-bit copy of the storage device to ensure data integrity. Analysts then recover and analyze deleted files, unallocated space, and file system structures to uncover relevant evidence. Advanced techniques like file carving allow for the recovery of data based on file signatures, even in the absence of file system metadata. Tools like FTK Imager, EnCase, and Scalpel are commonly used to perform these tasks, ensuring that the evidence is reliable and admissible in legal proceedings.

### Live Forensics

Live forensics involves the collection and analysis of data from a computer or digital device while it is still operational, as opposed to traditional forensics which typically involves working with static copies of data. This approach is crucial for capturing volatile data that may be lost if the system is shut down, such as active network connections, running processes, and system memory. Techniques include capturing live system memory using tools like FTK Imager or Volatility, extracting data from system registries and memory dumps, and monitoring real-time system activities. Live forensics often involves network analysis and the use of specialized tools to ensure data integrity while minimizing the impact on the live system.



### Network Forensics

Network Forensics is the capture, recording, and analysis of network events in order to be able to determine and discover the sources of attacks or incidents. This branch, unlike the rest of variants, has a different approach, not so much a post-mortem analysis but a proactive methodology. It bases its behavior on detecting and preventing cyberattacks and crime. For this purpose, different tools and techniques present in other fields of cybersecurity (defensive stance) are used.

* **Anomaly detection:** patterns of the normal behavior of the network are created so any disturbance and mismatch are evaluated and monitored.
* **Signature scan:** signatures and hashes of malicious activity are periodically checked within network traffic and, in case of matches, alerted.
* **Intrusion Detection System (IDS):** Monitoring tool deployed in strategic nodes of the network, analyzing all traffic in it and comparing with a preloaded set of rules.
* **Access Control List (ACL):** Prevent traffic with certain headers matching preloaded rules.
* **Honeypots:** Fake networks to deceive attackers. Emulating a real environment so that intruders are monitored and studied, revealing their tactics and techniques without jeopardizing real infrastructure and as- sets.

## Forensic Methodology

At Cytomate, our digital forensics methodology adheres to the highest standards of industry best practices and procedures. We employ a comprehensive, multi-phase approach to ensure thorough and accurate investigations. Our methodology begins with securing the physical crime scene to preserve the integrity of potential digital evidence. We then meticulously identify, document, and acquire relevant digital devices and data using state-of-the-art forensic tools and techniques. The analysis phase involves a detailed examination of the acquired data to uncover critical evidence and insights. Finally, we prepare a detailed and professional report that clearly communicates our findings, methodologies, and conclusions. This rigorous approach ensures that our investigations are reliable, reproducible, and aligned with legal and industry standards.

The phases to be addressed during an investigation are as follows:

**• Physical Crime Scene Securing**

**• Identification**

**• Collection and Acquisition**

**• Analysis**

**• Reporting**

### Assessment and Scenarios

The first phase of the forensic investigation itself. It consists of searching, identifying potential sources of information and cataloguing them. To this end, all devices that may contain evidence must be identified.

In addition, according to RFC-3227, it is necessary to take into consideration the order of volatility (from more volatile to less volatile) when identifying and collecting, thus determining the urgency at the time of treatment and avoiding the loss of information. These levels of urgency are, in order:

1. Registers, cache
2. Routing table, ARP cache, process table, kernel statistics, memory
3. Temporary file systems
4. Disk
5. Remote logging and monitoring data that is relevant to the system in question
6. Physical configuration, network topology
7. Archival media

Evidence and Artifact Extraction

The extraction process is critical and fundamental during a forensic investigation, since the entire investigation is based on this and its results. It is necessary that the procedure followed is documented in detail and in a transparent manner, so that the process is as standardized as possible and guided (minimizing errors during extraction).

#### 1. Evidence Identification

Objective: Determine which types of evidence are pertinent to the investigation.

**Steps:**

* **Define the Scope:** Establish the types of data and artifacts relevant to the investigation, such as files, emails, logs, or system configurations. This depends on the nature of the crime and the specific objectives of the investigation.
* **Identify Relevant Artifacts:** Based on the scope, identify potential sources of evidence on the device. Common artifacts include:
* **File Systems:** Files, directories, and metadata.
* **Registry Entries (Windows):** Configuration settings and user activity.
* **System Logs:** Activity logs, error reports, and system events.
* **Application Data:** Logs and cached data from applications.
* **Network Artifacts:** Network connections, history, and configuration files.
* **Memory Dumps:** Active processes and volatile data.
* **Document Evidence Locations:** Record the locations and types of artifacts identified for extraction, including specific file paths, registry keys, and log files.

#### 2. Evidence Acquisition

Objective: Create a forensic image or copy of the identified evidence to prevent alteration and maintain integrity.

**Steps:**

* **Use Forensic Tools:** Employ specialized forensic tools to acquire a bit-for-bit copy of the storage media or specific data segments. Tools such as FTK Imager, EnCase, or X1 can be used to capture images or files.
* **Implement Write Protection:** Utilize write blockers or similar technology to prevent any modifications to the source device during the acquisition process.
* **Verify Integrity:** Generate hash values (e.g., MD5, SHA-1) of both the original evidence and the acquired copy to ensure data integrity. Compare hash values to confirm that the acquisition is accurate and complete.
* **Document the Process:** Record details of the acquisition process, including the tools used, hash values, and any issues encountered. Maintain a log of all actions taken to ensure a clear chain of custody.

#### 3. Artifact Extraction

Objective: Extract and interpret specific artifacts from the acquired evidence.

**Steps:**

* **Analyze File Systems:** Examine file systems to extract files and metadata. Use forensic tools to recover deleted files, examine file properties, and analyze file structures.
* **Parse System and Application Logs:** Extract and analyze system and application logs to identify relevant events and activities. This can include reviewing event logs, security logs, and application-specific logs.
* **Extract Registry Data (Windows):** Analyze Windows registry hives to extract key entries related to user activity, system configurations, and installed applications. Use tools like RegRipper or Registry Explorer for parsing.
* **Examine Network Artifacts:** Extract and analyze network-related artifacts, such as connection logs, IP addresses, and network configurations. Tools like Wireshark or Network Miner can aid in this process.
* **Analyze Memory Dumps:** If a memory dump is available, use forensic tools to analyze active processes, open files, and network connections. This can provide insights into volatile data and ongoing activities at the time of capture.

#### 4. Validation and Documentation

Objective: Ensure the accuracy and completeness of the extracted evidence and document the process.

**Steps:**

* **Cross-Verify Data:** Validate extracted data against the original evidence to ensure that no critical information was missed or altered during extraction.
* **Create Detailed Reports:** Document the extraction process, including methodologies, tools used, and findings. Include detailed descriptions of artifacts and their significance to the investigation.
* **Preserve Evidence:** Store extracted evidence securely, ensuring that it remains protected and accessible for future analysis or legal proceedings.
* **Maintain Chain of Custody:** Ensure that all evidence handling and extraction activities are recorded in a chain of custody log, maintaining accountability and transparency.

Analysis

In the analysis phase of digital forensics, the focus shifts to examining the acquired evidence to uncover critical information and insights. This phase involves a thorough investigation of the digital artifacts extracted from the forensic images, utilizing advanced tools and techniques to interpret data such as file contents, system logs, and registry entries. Analysts meticulously search for patterns, recover deleted files, and piece together timelines of events to reconstruct activities and identify any evidence of malicious behavior or unauthorized access. The goal is to correlate data points, validate findings, and build a coherent narrative that supports the investigation's objectives. Accurate documentation and validation of the analysis process are essential to ensure that the findings are reliable and can withstand scrutiny in legal or organizational contexts.

Report

Finally, once the conclusions have been drawn, it is necessary to explain them as well as all the procedures and methodologies followed. This report must, without exception, be written in a plain and accessible format and language, avoiding technical terminology. In such a manner that people outside this field can easily understand it. If necessary to include technical terms, they should be referenced and annotated separately. Many forensic tools come with a built-in reporting feature that typically follows predefined templates and may allow customization of the report structure. However, depending on the data and type of information handled, it may not be compatible with a fixed report.

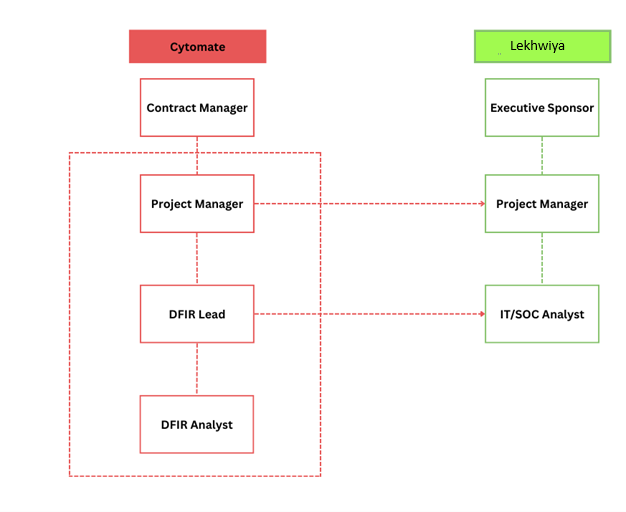
* Identity of the reporting agency
* Case investigator
* Identity of the submitter
* Date of evidence receipt
* Date of report

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| DFIR Lead | * Oversee DFIR activities and ensure alignment with organizational goals. * Provide strategic guidance and coordination as needed. |
| Incident Responder | * Respond to and manage security incidents on an as-needed basis. * Conduct initial triage and investigation when incidents occur. * Implement containment, eradication, and recovery measures as required. |
| Forensic Analyst | * Perform digital forensic analysis on affected systems as incidents occur. * Collect, preserve, and analyze digital evidence. |
| Threat Hunter | * Perform threat hunting over multiple log sources utilizing both commercial and open-source threat intelligence |
| Technical Specialist | * Offer technical expertise on tools and technologies as needed. * Assist with the configuration and troubleshooting of forensic tools on demand. |
| Training Coordinator | * Develop and conduct awareness sessions as needed. |

## Resource Communication Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No** | **Organization Name** | **Contact Person** | **Role** | **Email** |
| 1 | Cytomate | Hamad Saleh Hadeed | Contract Manager | hamad@cytomate.net |
| 2 | Cytomate | Dr. Masoom Alam | Project Manager | mmalam@cytomate.net |
| 3 | Cytomate | Osama Ellahi | DFIR Analyst | osama@cytomate.net |
| 4 | Cytomate | Anand Kumar | DFIR Analyst | [anand@cytomate.net](mailto:anand@cytomate.net) |
| 5 | Cytomate | Muzammil Hassan | Threat Hunter | muzammil@cytomate.net |



# On-Demand Delivery Timeline

Detailed timeline plan for an IR engagement, broken down into phases according to industry standards. This plan assumes a total of 40 hours of work per year and is based on a standard IR approach. The proposed timeline for the Digital Forensics and Incident Response (IR) services is outlined with estimated hours allocated to each task. However, please note that the hours assigned to each step are flexible and can be adjusted based on the specific needs and priorities. This flexibility allows for the efficient reallocation of hours between tasks to address the evolving demands of the incident response process, ensuring that each phase receives the appropriate attention and resources as required.

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **Activity** | **Hours** | **Total Hours** |
| Preparing and Planning |  | ***5*** |  |
|  | Initial Consultation | 2 |  |
|  | |  | | --- | | Establishing the Incident Response Plan |  |  | | --- | |  | | 1 |  |
|  | Tools and Resources Preparation | 2 |  |
| Identification and Detection |  | ***10*** |  |
|  | Incident Identification | 4 |  |
|  | Incident Triage | 4 |  |
|  | Initial Reporting | 2 |  |
| Containment, Eradication, and Recovery |  | ***15*** |  |
|  | Containment | 5 |  |
|  | Eradication | 7 |  |
|  | Recovery | 3 |  |
| Post-Incident Analysis |  | |  | | --- | |  |  |  | | --- | | ***6*** | |  |
|  | Forensic Analysis | 3 |  |
|  | Root Cause Analysis | 2 |  |
|  | Reporting and Documentation | 1 |  |
| Review and Improvement |  | ***4*** |  |
|  | Post-Incident Review | 3 |  |
|  | Process Improvement | 1 |  |
| **Total** | | | **40** |