**Task 2: Incident Response Simulation**

**Scenario:**   
This malware attack was detected when an employee clicked on an ad from a suspicious website via the organization's network.

**Context and Objective:**   
To gain unauthorized access to the company’s network to steal sensitive information (data, credentials, etc).

**Scope:**If successful, it could ruin not only the company’s reputation and financial aspect but could also lead to unauthorized access to personal data.

1. **Incident detection:**

**Detection:** The Security Operations Centre (SOC) of the Organization observed malware symptoms such as:

* Increase in CPU usage.
* Decrease in web browsing speed.
* Unexplainable network connections.
* Unknown processes running.

**Confirmation:** Use of Anti-virus and behavioral analysis software(e.g. **McAfee, Norton Security**) to determine and confirm malware attacks.

1. **Response Plan Execution Plan:**  
   **Actions taken:**

* Key stakeholders were informed.

**Identification and Detection:**

* Security analyst determined the extent of disruption to initiate a proper response plan.

**Containment and Eradication:**

* Infected computers were isolated from the organization’s network.
* Removal of malware-infected systems using reputable anti-malware software(e.g. **Malwarebytes, Avast Antivirus**).
* Manual removal of any malicious registry files or registry entries that may have been overlooked by automated tools.

1. **Forensic Analysis:**

* Creating a forensically sound environment to analyze affected systems without altering the original evidence
* Record chain of custody for all evidence to maintain integrity for potential legal proceedings.
* Identify the type and behavior of malware including entry point.
* Examine systems logs network traffic and file access time to reconstruct the timeline of malware attack.
* Thoroughly document all findings and evidence obtained during analysis.

1. **Post incident assessment:**

**Analysis:**

**Suggested analysis tools:   
1. Splunk  
2. Security Information and Event Management (SIEM) Toolss**

* Use findings from analysis to understand the impact of malware attacks, identify any vulnerabilities in defenses, and make recommendations for future mitigation.
* Determine whether communication and coordination among different terms, stakeholders, and external parties were effective and efficient.

**Accuracy of decision and actions:**

* Evaluate the accuracy and effectiveness made of decision-making during incident response, including incident identification, containment measures, and any remediation actions taken.
* Solicit feedback and lessons learned from the incident response team, relevant stakeholders, and external parties involved in the incident.
* Use findings from the review to update the incident response plan procedure and related documentation.

1. **Improvements:**

* Keep software and operation systems updated.
* Installing and regularly updating anti-malware software.
* Regular backups and secure data storage.
* Avoid questionable websites.