MALWARE-OUTBREAK Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		21 April 2024	First draft
1.0	Devika Sivakumar	Joel Daniel	29 April 2024	Approved for Publishing
2.0	Devika Sivakumar		02 August 2024	Comprehensive updates and refinements have been made to the introduction and scope sections. Case studies have been added to the attack types, stakeholders have been updated, and changes have been made throughout. A RACI chart has been included, steps for monitoring threats have been added, and terminology has been updated.

Contents

1. Introduction

Data integrity, reputation, and company operations are all seriously at danger from malware outbreaks. To reducing harm and guaranteeing business continuity, timely malware incident identification, containment, and mitigation are essential. This playbook offers a systematic approach for managing malware outbreaks, defining roles, duties, and procedures to enable a successful response.

1.1 Overview

The incident response playbook for malware outbreaks provides a structured approach to locating, stopping, eliminating, and recovering from attacks by malware. It seeks to expedite reaction efforts and lessen the effect of malware breakouts on organisational assets and stakeholders by creating defined protocols and communication channels.

1.2 Purpose

This playbook's goals are to:

- Provide a uniform procedure for tackling malware outbreaks to guarantee consistency and effectiveness in incident management.
- Enable prompt detection and incident containment to stop malware from spreading further and reduce damage.
- Reduce the impact of malware outbreaks on company operations and lower the financial losses they cause.
- During incident response activities, encourage cooperation, coordination, and communication amongst response teams, stakeholders, and other relevant parties.

1.3 Attack Definition

Malware is software that is intentionally created to cause harm, interfere with operations, or obtain unauthorised access to data, networks, and computer systems. It includes a wide range of dangers, including as trojans, worms, viruses, ransomware, and spyware. Multiple routes, including portable media, malicious websites, email attachments, and software flaws, can lead to malware epidemics.

1.4 Scope

This playbook covers incidents related to malware outbreaks on Redback Operations computers, networks, and endpoints. It addresses both external and internal malware issues that impact stakeholders, data assets, and company processes, requiring an integrated response effort regardless of the type of malware or transmission technique.

2. Attack Types

Malware outbreaks may take many different shapes, and responding to each one presents different difficulties for incident response teams. Malware outbreaks are often linked to the following attack types:

2.1 Worms

Worms are self-replicating viruses that spread across networks, exploiting security holes to quickly infect connected computers.

Signs of Worm Activity:

- Unusual network traffic increases.
- High bandwidth usage due to worm replication.
- Increased memory or CPU consumption on compromised computers.
- Unknown files or processes in system logs.
- Random system restarts or crashes.

Case Study: The Morris Worm (1988)

- **Overview:** One of the earliest worms to spread across the internet was the Morris Worm. Robert Tappan Morris was the creator, and it was made available on November 2, 1988.
- **Signs of Activity:** Spreading quickly across networked computers, resulting in resource exhaustion-related system slowdown or crashes.
- **Impact:** Affected around 6,000 significant Unix computers, or 10% of the internet at the time. It was projected that the worm would cost between $100,000 and $10 million to eradicate.
- **Response:** Network security awareness has grown, and CERT (Computer Emergency Response Team) was established to deal with these kinds of situations.

2.2 Trojans

Trojans pose as trustworthy programmes to fool users into downloading and running malicious code, giving hackers access to compromised systems without authorisation.

Signs of Trojan Infection:

- Suspicious applications or processes running in the background.
- Unauthorized changes to files or system settings.
- Remote attackers accessing sensitive information or system resources.
- Unexpected toolbar or application installations.
- System sluggishness or frequent crashes.

Case Study: Zeus Trojan (2007)

- **Overview:** Zeus, sometimes referred to as Zbot, is a Trojan horse malware bundle that operates on Microsoft Windows versions. It was initially discovered in July 2007.
- **Signs of Activity:** Unauthorised access to banking information, unauthorised transactions, and keylogging.
- **Impact:** Zeus compromised millions of dollars' worth of fraudulent transactions by infecting thousands of machines throughout the globe with malware and stole banking passwords.
- **Response:** Law enforcement and security firms worked together to knock down Zeus command-and-control servers and make many arrests.

2.3 Ransomware

Ransomware encrypts user files or locks them out of their computers, then demands money to free it or grant access again.

Signs of Ransomware Activity:

- Files that are inaccessible and have a.locky or.crypt file extension are encrypted.
- Appearance of warning messages or ransom notes requesting money to unlock files.
- Alteration of file dates or properties through the encryption procedures of ransomware.
- Unusual patterns of network traffic as the ransomware talks to the servers that govern it.
- Existence on compromised systems of ransomware-related artefacts, such as executables or registry entries.

Case Study: WannaCry Ransomware Attack (2017)

- **Overview:** WannaCry was a ransomware cryptoworm that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin.
- **Signs of Activity:** Files became inaccessible with ".wncry" extensions, and users saw ransom notes demanding payment.
- **Impact:** The incident impacted more than 230,000 computers across 150 nations, seriously disrupting businesses like the National Health Service (NHS) in the United Kingdom. There were billions to hundreds of millions of dollars in financial losses.
- **Response:** The ransomware's propagation was slowed down when a security researcher found a kill switch in its code. Affected companies strengthened their security protocols and put strategies in place for data recovery.

2.4 Botnets

Botnets are networks of infected devices under the control of hackers, frequently employed to carry out coordinated assaults or disseminate malware payloads.

Signs of Botnet Infection:

- Strange outgoing network connections to command-and-control sites made by compromised devices.
- Large amounts of harmful or spam emails coming from infected computers.
- Botnet activity on compromised devices is causing high CPU or bandwidth utilisation.
- The existence of backdoor trojans or remote access programmes that facilitate botnet communication.
- Unexpected alterations in system behaviour or performance brought on by botnet activity.

Case Study: Mirai Botnet (2016)

- **Overview:** A software known as the Mirai botnet transforms Linux-powered networked devices into remotely controlled bots that may be deployed as components of a larger botnet in extensive network attacks.
- **Signs of Activity:** Unusual network traffic patterns, particularly to command-and-control servers, and involvement in large-scale DDoS attacks.
- **Impact:** One of the worst DDoS assaults ever launched against DNS provider Dyn was brought on by the Mirai botnet and resulted in extensive disruptions to the internet.
- **Response:** Police departments located and detained Mirai's founders. ISPs and security companies collaborated to increase device security and lessen the botnet's effects.

2.5 Spyware

Without user agreement, spyware secretly records private user data, gathers it, and sends it to hostile parties.

Signs of Spyware Presence:

- Unexpected adjustments to the homepage or default search engine in a browser.

- Display of inappropriate pop-up advertisements or browser reroutes to unsafe websites.
- Existence of toolbars or unusual browser extensions that have been installed without permission.
- Spyware activity might cause a slow internet connection or poor browser performance.
- Criminals gaining illegal access to passwords, surfing history, or sensitive information.

Case Study: FinFisher/FinSpy (2011)

- **Overview:** Gamma Group sells the surveillance spyware suite FinFisher, also referred to as FinSpy. Several nations have employed it for monitoring reasons.
- **Signs of Activity:** Unauthorized access to sensitive data, keystroke logging, and remote surveillance capabilities.
- **Impact:** Human rights advocates, journalists, and political dissidents have all been the targets of FinFisher. Devices in more than 30 nations have been found to contain the malware.
- **Response:** Human rights groups have brought attention to the use of FinFisher, and cybersecurity companies have created instruments for identifying and eliminating the malware.

2.6 Adware

Without the user's permission, adware gathers user data for targeted advertising, displays invasive adverts, and reroutes web traffic.

Signs of Adware Infection:

- Sudden emergence of unwelcome pop-up advertising or banners when browsing the internet.
- Redirects users who click on links or search results to dubious or harmful websites.
- Adware processes causing slow browser speed or frequent crashes.
- Altering the main page or preferred search engine in a browser without permission.
- Data, database entries, or browser extensions connected to adware being present on compromised machines.

Case Study: Fireball Adware (2017)

- **Overview:** Check Point found an adware called Fireball that takes over browsers and transforms them into zombies.
- **Signs of Activity:** Browser hijacking, changes to default search engine, and installation of additional adware or potentially unwanted programs.

- **Impact:** Over 250 million machines were infected by Fireball globally, mostly because of it being bundled with other free software. It gathered user data and made false advertising money.
- **Response:** To identify and get rid of Fireball, security researchers and antivirus software providers developed updates and removal tools. Campaigns were started to inform people about the dangers of bundled software.

3. Stakeholders

Effective malware outbreak response requires collaboration among various stakeholders within and outside Redback Operations.

3.1 IT Security Team

Lead: Daniel McAulay (Senior Project Leader)

The IT security team oversees protecting the company's digital assets, identifying security risks, and putting preventative and corrective measures in place for data breaches.

Responsibilities:

- Analyzing security events to assess malware outbreak impact.
- Implementing security measures to prevent further unauthorized access.
- Collaborating with the incident response team to contain malware outbreaks.
- Conducting forensic investigations to identify root causes.
- Advising on incident response protocols and security improvements.

3.2 Incident Response Team

Lead: Devika Sivakumar (Blue Team Leader)

The incident response team is responsible for organising cleanup activities and overseeing the organization's reaction to malware outbreaks.

Responsibilities:

- Assessing the extent of malware outbreaks.
- Assembling resources to mitigate the effects of malware attacks.
- Conducting forensic investigations for root cause analysis.
- Communicating response protocols and recovery efforts to stakeholders.
- Enhancing incident response capabilities based on lessons learned.

3.3 Communication Team

Lead: Kaleb Bowen (Company Lead)

The communication team oversees overseeing and guaranteeing clear and consistent message for both internal and external communications about malware outbreaks.

Responsibilities:

- Creating communication plans to inform stakeholders about malware outbreaks.
- Drafting and distributing communication materials.
- Managing media relations to protect the organization's image.

- Providing regular updates on stakeholder engagement.

Collaboration Matrix:

- IT Security Team: Response implementation and technical analysis.
- Incident Response Team: Coordination and execution of response actions.
- Communication Team: Information dissemination and media management.
- Senior Management: Decision-making and oversight.
- Legal and Compliance: Regulatory adherence and legal guidance.

3.4 Customers

Clients are people or groups that have a stake in the goods or services that the company provides and who could be impacted by malware outbreaks. Among their duties and functions are:

- Notifying the company of any unauthorised or questionable conduct pertaining to their accounts or transactions.
- Supplying the incident response team with pertinent data or proof to aid in the investigation of malware outbreaks.
- Following the advice and directives of the organisation on safeguarding their personal information and lessening the effects of virus outbreaks.

3.5 Third-Party Vendors

Third-party vendors are outside businesses that supply the company with goods, services, or support; they may also have access to its systems, networks, or data. Among their duties and functions are:

- Working along with the company's incident response team to find and fix security flaws or breaches pertaining to their goods or services.
- Providing help and backing to the company as it investigates and resolves malware problems impacting its systems or networks.
- Meeting legal and contractual standards for data security and privacy, including reporting security breaches, and supporting incident response activities.

Communication Plan Template:

- Internal: Immediate notification to IT Security and Incident Response Teams.
- External: Timely updates to customers and third-party vendors.
- Media: Press releases and statements to manage public relations.

RACI Chart:

- **R:** Responsible (who does the work)
- **A:** Accountable (ultimate ownership)
- **C:** Consulted (provides input)
- **I:** Informed (kept up to date)

Key Definitions:

- **Responsible (R):** The individual(s) who perform the work to achieve the task.
- **Accountable (A):** The individual who is ultimately answerable for the correct and thorough completion of the task.
- **Consulted (C):** The individual(s) whose opinions are sought.
- **Informed (I):** The individual(s) who are kept up to date on progress and outcomes.

RACI Chart

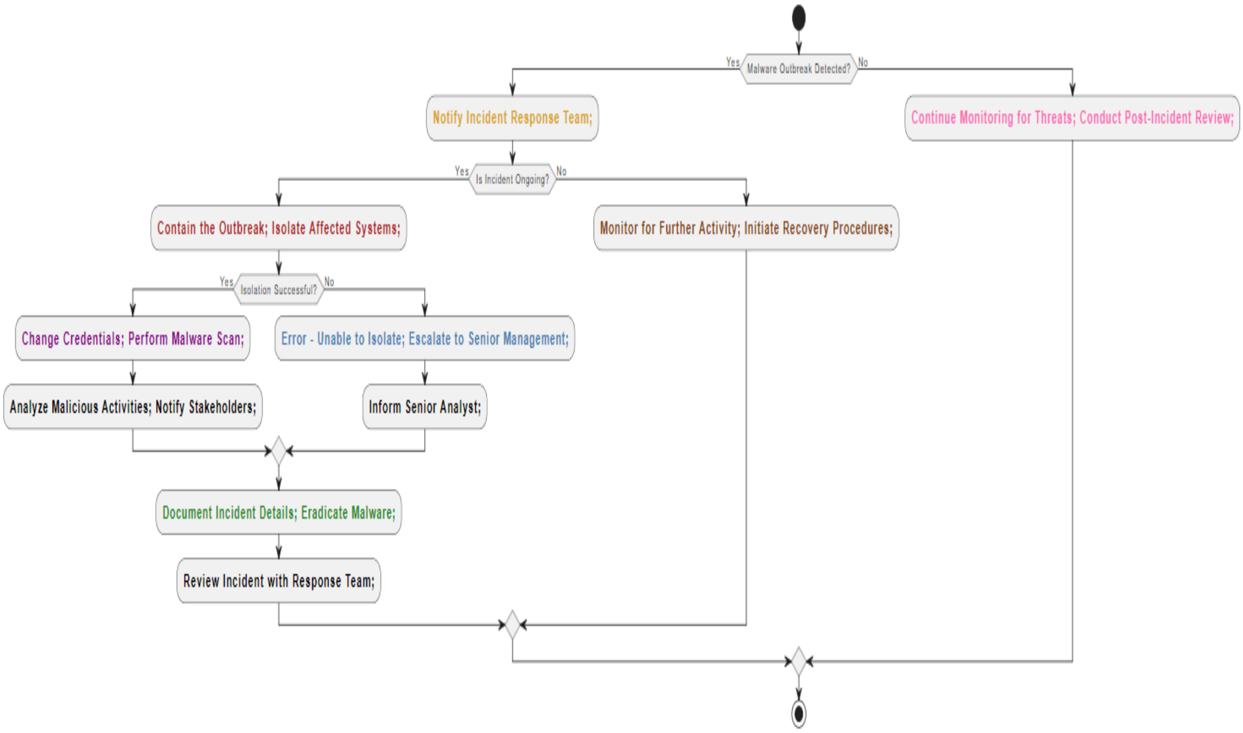
Task/Activity	IT Security Team	Incident Response Team	Communication Team	Senior Management	Legal and Compliance	Customers	Third-Party Vendors
Preparation	R, C	A, R	I	I	C	I	I
Establishing incident response team	A	R	I	I	C	I	I
Developing malware response procedures	A, R	R, C	I	C	C	I	I

Conducting training and practice sessions	A, R	R	I	I	I	I	I
Implementing malware detection systems	A, R	R	I	I	I	I	I
Detection	A, R	R	I	I	I	I	I
Monitoring system logs and network traffic	R	A, R	I	I	I	I	I
Using IDS and SIEM tools	A, R	R	I	I	I	I	I
Analyzing alerts	A, R	R	I	I	I	I	I
Analysis	A, R	R	I	I	I	I	I
Collecting data for forensic analysis	A, R	R	I	I	I	I	I
Identifying attack methods	A, R	R	I	I	I	I	I
Determining impact	A, R	R	I	I	I	I	I

Containment	A, R	R	I	I	I	I	I
Isolating compromised systems	A, R	R	I	I	I	I	I
Implementing safeguards	A, R	R	I	I	I	I	I
Blocking malicious software	A, R	R	I	I	I	I	I
Eradication	A, R	R	I	I	I	I	I
Removing malicious software	A, R	R	I	I	I	I	I
Patching vulnerabilities	A, R	R	I	I	I	I	I
Updating security policies	A, R	R	I	I	I	I	I
Recovery	A, R	R	I	I	I	I	I
Restoring backups	A, R	R	I	I	I	I	I
Rebuilding systems	A, R	R	I	I	I	I	I
Conducting user	A, R	R	I	I	I	I	I

awareness training							
Post-Incident Review	A, R	R	I	I	I	I	I
Reviewing incident response process	A, R	R	I	I	I	I	I
Documenting best practices	A, R	R	I	I	I	I	I
Updating response procedures	A, R	R	I	I	I	I	I
Communication Plan	C	C	A, R	I	C	I	I
Creating communication plans	C	C	A, R	I	C	I	I
Drafting communication materials	C	C	A, R	I	C	I	I
Managing media relations	C	C	A, R	I	C	I	I
Providing updates	C	C	A, R	I	C	I	I

4. Flow Diagram


Malware Outbreak Detected?
Yes
No
Notify Incident Response Team;
Continue Monitoring for Threats; Conduct Post-Incident Review;
Is Incident Ongoing?
Yes
No
Contain the Outbreak; Isolate Affected Systems;
Monitor for Further Activity; Initiate Recovery Procedures;
Isolation Successful?
Yes
No
Change Credentials; Perform Malware Scan;
Error - Unable to Isolate; Escalate to Senior Management;
Analyze Malicious Activities; Notify Stakeholders;
Inform Senior Analyst;
Document Incident Details; Eradicate Malware;
Review Incident with Response Team;

1. Preparation (Prep): Yellow

   - Notify Incident Response Team: To begin incident response preparations, the incident response team is notified as soon as a malware outbreak is discovered.

2. Identification (Identify): Red

   - Contain the Outbreak; Isolate Affected Systems: To stop more unauthorised access, steps are made to isolate compromised systems and limit the outbreak.

3. Notification (Notif): Violet

   - Change Credentials; Perform Malware Scan: To mitigate the effect of the outbreak, malware scans and password changes are made.

- Analyse Malicious Activities; Notify Stakeholders: Malicious activity is found through additional analysis, and stakeholders are informed to plan reaction actions.

4. Containment (Contain): Sky Blue

- Error - Unable to Isolate; Escalate to Senior Management: Senior management is notified of the issue for resolution if the impacted systems cannot be isolated.

5. Eradication (Erad): Light Green

- Document Incident Details; Eradicate Malware: To remove the danger, malware removal processes are carried out and incident facts are logged.

6. Recovery (Recover): Brown

- Monitor for Further Activity; Initiate Recovery Procedures: To restore regular operations, recovery steps are started, and ongoing monitoring is carried out for any new malware activity.

7. Post-Incident Actions (Post): Light pink

- Continue Monitoring for Threats; Conduct Post-Incident Review: In addition to ongoing threat detection, a post-event evaluation is carried out to assess the response's efficacy and pinpoint areas in need of development.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Establishing the policies, procedures, and assets necessary to effectively manage malware outbreaks is the primary objective of the preparation stage.
- **Activities:**
  - Assembling an incident response team with distinct responsibilities.
  - Developing crisis response procedures and plans that incorporate communication protocols and escalation pathways.
  - Ensuring readiness by regularly training and practicing incident responses.
  - Putting in place surveillance systems and security measures to find and stop malware outbreaks.
- **Outcome:** A fully prepared business with the ability to respond quickly and effectively to malware outbreaks.

5.2 Detection

- **Objective:** The goal of the detection stage is to look for indications of malware outbreaks or illegal access to the networks and systems of the company.
- **Activities:**
  - Keeping an eye out for questionable activity, such strange access patterns, or illegal file transfers, by examining system records and network traffic.
  - Using intrusion detection systems (IDS) and security information and event management (SIEM) tools to find any assaults.
  - Examining anomalies and alerts to distinguish between dangerous and acceptable activity.
- **Outcome:** Early malware outbreak identification enables rapid reaction and mitigation measures.

5.3 Analysis

- **Objective:** Finding out and understanding the nature and scope of the malware epidemic occurrence are the main goals of the analysis stage.
- **Activities:**
  - Collecting data and using forensic analysis to identify the source and extent of the malware infestation.
  - Analysing systems and networks that have been compromised to determine attack tactics and the effects on compromised data.
  - Identifying the indications of compromise (IOCs) and strategies, methods, and procedures (TTPs) of threat actors.

- **Outcome:** A comprehensive comprehension of the malware outbreak, considering the causes, effects, and attribution of the outbreak.

5.4 Containment

- **Objective:** The containment stage stops future unauthorised access or leakage of information to mitigate the effect and spread of the event.
- **Activities:**
  - Dividing vulnerable computers and networks to stop attackers from spreading laterally.
  - Putting in place safeguards and access limits to stop illegal access to private data.
  - Containing or obstructing dangerous software, data, or network traffic to stop more harm.
- **Outcome:** Effective handling of the malware breakout incident, minimising the harm done to the organization's data and systems.

5.5 Eradication

- **Objective:** The goal of the eradication phase is to eliminate the attackers from the company's networks and IT infrastructure, along with any hazards or vulnerabilities that may still exist.
- **Activities:**
  - Eradicating bad software and data and returning hacked machines to a safe configuration.
  - Repairing or updating software and systems that are susceptible to attack to stop future exploitation.
  - Examining and amending security procedures and policies to fix any vulnerabilities or faults found.
- **Outcome:** Removing all traces of the malware breakout event and cutting down on vulnerabilities to stop future occurrences of this kind.

5.6 Recovery

- **Objective:** The goal of the recovery stage is to get the affected systems and data back to normal and to start doing business as usual.
- **Activities:**
  - Restoring corrupted systems as well as information backups to guarantee information accessibility and integrity.
  - Rebuilding or rearranging systems and networks to improve security and stop such incidents in the future.

  - Putting in place initiatives for user awareness and education to stop malware outbreaks in the future.
- **Outcome:** Complete recovery of services and operations, along with stronger safety protocols to reduce the probability of a repeat.

5.7 Post- Incident Review

- **Objective:** The company assesses its reaction to the malware outbreak issue during the post-incident assessment phase, looking for areas for improvements and lessons learnt.
- **Activities:**
  - Completing a thorough analysis of the incident response procedure, considering its advantages, disadvantages, and potential areas of development.
  - Recording best practices and lessons discovered to improve future incident response capabilities.
  - Modifying incident response procedures, policies, and security setups considering the review's conclusions.
- **Outcome:** Enhancing incident response skills and preparing for any malware outbreaks in the future.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

Objective: Create and put into action a thorough plan for ongoing threat surveillance that focuses on malware outbreaks.

Activities:

- **Objectives:** Clearly state the goals of threat monitoring, including spotting malware infections, seeing illegal access, and keeping an eye on strange network activity that could be a sign of malicious activity.
- **Tools:** Choose the right security technologies, such as anti-malware software, SIEM (Security Information and Event Management) systems, EDR (Endpoint Detection and Response) solutions, and IDS/IPS (Intrusion Detection/Prevention Systems).
- **Baselines:** Create baselines for typical system behaviour, user activity, and network traffic patterns to spot any variations that could point to the existence of malware.

Outcome: A clear monitoring plan that supports Redback Operations objectives and improves the capacity to identify and address malware threats.

6.2 Deploy Monitoring Solutions

Objective: Install and set up monitoring technologies throughout the infrastructure of the company to identify any malware threats.

Activities:

- **Install and Configure Tools:** Distribute the chosen monitoring tools to endpoints, systems, and networks. Make sure they are set up to identify actions connected to malware and gather relevant data.
- **Integrate with Threat Intelligence:** Combine threat information feeds with monitoring technologies to improve the identification of both established and new malware threats.
- **Enable Logging:** Verify that logging is turned on for all important networks, systems, and applications. Log collecting should be centralised for effective analysis and correlation.

Outcome: Comprehensive deployment and integration of monitoring solutions providing detailed insights into potential malware threats.

6.3 Continuous Monitoring and Analysis

Objective: Continue investigation and monitoring to quickly identify and address malware risks.

Activities:

- **Real-Time Monitoring:** IIn order to enable the prompt identification of malware activity, utilise real-time monitoring to continually examine user actions, system behaviour, and network traffic.

- **Anomaly Detection:** Make use of machine learning and behavioural analytics to spot abnormalities and departures from predetermined baselines that could point to the existence of malware.
- **Correlate Events:** Connect events from different sources to find trends that could point to well-planned malware assaults or enduring dangers.

Outcome: Enhanced capability to detect malware threats promptly, enabling swift response to mitigate potential impacts.

6.4 Alerting and Notification

Objective: Use a strong alerting system to guarantee prompt and efficient reaction to risks that are identified.

Activities:

- **Set Alert Thresholds:** Determine thresholds according to probable effect and severity for various alert kinds.
- **Automated Alerts:** Set up automatic alerts to inform the security team of any malware dangers found. Make sure warnings have enough context to allow for quick assessment and response.
- **Prioritize Alerts:** Establish a method to rank warnings according to their seriousness and possible consequences, concentrating on the most urgent dangers first.

Outcome: Prompt and efficient handling of malware threats identified, lowering the possibility of serious harm.

6.5 Investigate and Respond

Objective: To reduce the threat of detected malware, carry out in-depth investigations and put the necessary measures into place.

Activities:

- **Initial Triage:** To confirm the veracity and possible significance of warnings, carry out preliminary triage. Assess the threat's seriousness and determine if the warning is a false positive.
- **Detailed Analysis:** To determine the kind and scope of the malware threat, thoroughly examine verified warnings. To get data and locate the threat's origin, employ forensic instruments and methods.
- **Containment and Eradication:** If a danger is confirmed, start containment procedures to stop more harm. To get rid of the virus from the environment, carry out the required eradication processes.

Outcome: Efficient examination and reduction of malware hazards, guaranteeing little influence on the establishment.

6.6 Post-Incident Review

Objective: Evaluate the response's efficacy and pinpoint areas in need of development.

Activities:

- **Document Findings:** Keep a record of the whole occurrence, including the steps taken for identification, analysis, and reaction.
- **Review and Improve:** Examine the monitoring and reaction procedures after the event to find areas of improvement and lessons discovered.
- **Update Monitoring Tools:** To improve threat detection and response capabilities in the future, update monitoring tools, setups, and thresholds in light of the findings.
- **Outcome:** Processes for incident response and threat monitoring are continuously improved, guaranteeing increased readiness for malware outbreaks in the future.

6.7 Continuous Improvement

Objective: Preserve and improve the tools and approach used by the organisation for threat monitoring.

Activities:

- **Regular Audits:** To make sure monitoring techniques and technologies are still relevant and effective in light of emerging dangers, conduct audits on a regular basis.
- **Training and Awareness:** Continually train security staff on the newest risks and optimal techniques for observation and reaction.
- **Adapt to New Threats:** Make constant adjustments to the monitoring plan to handle new risks. Keep up with the most recent threat intelligence and apply it to your monitoring procedures.

Outcome: A proactive, flexible approach to threat monitoring those changes as the environment around threats does.

7. Terminology

- Malware Outbreak: A circumstance in which malicious software quickly spreads throughout the computers, networks, or devices of a company, usually with the goal of stealing, disrupting, or infiltrating data.
- Indicators of Compromise (IOCs): Indications of potentially harmful activity that may be seen in an organization's IT infrastructure and that point to the existence of malware, or a security breech connected to the outbreak.
- Incident Response: A methodical and structured process for locating, controlling, and lessening the damage that a malware outbreak does to an organization's IT infrastructure to reduce interruption and get things back to normal.
- Forensic Analysis: The careful inspection and evaluation of digital evidence associated with the malware outbreak, including system artefacts, malware samples, and network logs, to determine the origin of the attack, gauge its scope, and provide proof for legal or investigative needs.
- Security Controls: Defensive measures and protections, including as firewalls, antivirus software, intrusion detection systems (IDS), and endpoint protection solutions, put in place to identify, stop, and reduce the impact of a malware outbreak.
- Vulnerability: Vulnerabilities or holes in a company's networks, apps, or IT systems that might be used by malware to propagate, get improper access, or do damage. Preventing and managing malware outbreaks requires the identification and patching of vulnerabilities.
- Phishing: A popular attack vector that hackers employ to fool people into disclosing private information, including passwords, usernames, and financial information. This is frequently done through fake emails, websites, or texts. Phishing assaults have the potential to spread malware and start an outbreak of the infection inside a company.
- TTPs: Tactics, Techniques, and Procedures used by threat actors.
- SIEM: Security Information and Event Management tools.
- IDS: Intrusion Detection Systems.
- Zero-Day Exploit: An attack that targets a previously unknown vulnerability.