VIRUS-OUTBREAK Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		28 April 2024	First draft
1.0	Devika Sivakumar	Joel Daniel	29 April 2024	Approved for Publishing
2.0	Devika Sivakumar		03 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.

Contents

1. Introduction

Virus outbreaks pose significant threats to data integrity, operational continuity, and organizational reputation. Timely detection, containment, and mitigation of virus incidents are crucial to minimizing damage and ensuring business resilience. This playbook provides a structured approach for managing virus outbreaks, detailing roles, responsibilities, and processes for an effective response.

1.1 Overview

There is a methodical structure available in the Virus Outbreak Incident Response Playbook for identifying, stopping, eliminating, and recovering from virus attacks. It seeks to expedite reaction efforts and lessen the impact of viral outbreaks on organisational assets and stakeholders by developing defined standards and communication channels.

1.2 Purpose

This playbook's goals are to:

- For viral outbreaks, create a standard operating protocol to guarantee uniformity and efficiency in incident response.
- Encourage the prompt discovery and containment of occurrences to limit damage and stop future spread.
- Minimise financial losses and the effect of viral outbreaks on organisational operations.
- During incident response efforts, encourage collaboration, coordination, and communication amongst response teams, stakeholders, and other pertinent parties.

1.3 Attack Definition

Malicious software that aims to damage, interfere with, or get unauthorised access to computer systems, networks, and data is known as a virus. They cover a wide range of dangers, such as spyware, ransomware, trojans, and worms. Numerous routes, including malicious websites, email attachments, infected files, and software flaws, can allow viruses to infiltrate a system.

1.4 Scope

This playbook describes events pertaining to virus outbreaks that affect the computers, networks, and endpoints of Redback Operations. It deals with internal and external viral problems that impact data assets, stakeholders, and organisational procedures. Regardless of the type of virus or how it spreads, a coordinated reaction is necessary.

2. Attack Types

There are several ways that virus outbreaks might appear, and each one poses different difficulties for incident response teams. The subsequent assault types are frequently linked to viral outbreaks:

2.1 File Infector Viruses

When executable files are opened, file infector viruses cling to them, multiply, and spread to other files, causing extensive harm.

<u>Signs of File Infector Virus Activity:</u>

- Unknown corruption or alteration of executable files.
- Unexpected variations in checksums or file sizes.
- Reports of malicious file alarms from antivirus software.
- Unexpected rise in system resource consumption brought on by viral propagation.
- Suspicious network traffic coming from machines that have been compromised.

Case Study: CIH Virus (1998)

- **Overview:** The destructive file infector virus known as the CIH virus, or Chernobyl, was specifically designed to attack executable files on Windows 95 and 98.
- **Signs of Activity:** Corruption of executable files, system crashes, and data loss.
- **Impact:** Infected thousands of computers worldwide, causing widespread data loss and hardware damage.
- **Response:** Antivirus updates and system restores were implemented to recover affected systems.

2.2 Macro Viruses

Macro viruses propagate by infecting spreadsheets and documents that include macros. The macros are subsequently performed when the file is accessed, potentially leading to data loss or system interruption.

<u>Signs of Macro Viruses Activity:</u>

- Unusual actions or error messages while attempting to open spreadsheets or documents.
- Emails with links to malicious documents or attachments that seem suspicious.
- Reports of unforeseen modifications to the layout or substance of documents.
- Infected papers are found and quarantined by antivirus software.
- Increased network traffic because of the transmission or sharing of infected documents.

Case Study: Melissa Virus (1999)

- **Overview:** The Melissa virus spread through infected Word documents sent via email.
- **Signs of Activity:** Mass emailing of infected documents, unauthorized access to email contacts.
- **Impact:** Disrupted email services and caused significant financial damage estimated at $80 million.
- **Response:** Vendors of antivirus software promptly produced updates to identify and eradicate the malware. Security protocols for emails were strengthened to prevent such assaults.

2.3 Boot Sector Viruses

The master boot record (MBR) or boot sector of storage devices can get infected with boot sector viruses, which impair the system's ability to start correctly and may result in data loss or system failure.

Signs of Boot Sector Viruses Activity:

- Anomalous errors during the boot process or the system's inability to boot up. Reports of system files being damaged or missing.
- Notifications from antivirus software that boot sector viruses are present.
- Adjustments to disc partitions or partition tables that are not explained.
- Suspicious behaviour on the network coming from devices that are infected and trying to propagate the infection.

Case Study: Michelangelo Virus (1992)

- **Overview:** On March 6th, a boot sector malware known as the Michelangelo virus became active and began damaging hard drives.
- **Signs of Activity:** System crashes and inability to boot.
- **Impact:** Infected thousands of computers, causing significant data loss.
- **Response:** Before March 6th, users were encouraged to do antivirus scans to identify and eliminate the infection. Protection measures for the boot area were put in place.

2.4 Polymorphic Viruses

With every infection, polymorphic viruses alter their look and coding structure, making antivirus software's job of detecting and eliminating them more difficult.

Signs of Polymorphic Viruses Activity:

- Files with often changing signatures are identified by antivirus software and placed in quarantine.
- Random crashes or problems on compromised devices that are not explained.

- Reports of unusual or unpredictable behaviour from files or apps.
- A rise in network traffic as the virus looks to infect other machines.
- System logs demonstrating many attempts to run malicious code with different characteristics.

Case Study: Storm Worm (2007)

- **Overview:** A polymorphic malware called Storm Worm propagated via hacked websites and email attachments.
- **Signs of Activity:** Rapidly changing code signatures, system slowdowns, and crashes.
- **Impact:** Infected millions of computers worldwide, creating a large botnet.
- **Response:** To detect and neutralise the virus, security researchers used sophisticated detection techniques. Campaigns for public awareness were started to inform people about secure email usage.

2.5 Resident Viruses

Because resident viruses lodge themselves in system memory, they can continue to function even after the system is restarted.

Signs of Resident Virus Activity:

- Unexpected system lag or deterioration in performance.
- Antivirus software that looks for infections in RAM.
- Persistence in task management or process monitor of processes linked to viruses.

Case Study: CodeRed Worm (2001)

- **Overview:** CodeRed was a resident virus that took use of an IIS buffer overflow vulnerability to attack Windows servers.
- **Signs of Activity:** Website defacements, system slowdowns, and memory consumption.
- **Impact:** Infected over 359,000 hosts, causing estimated damages of $2.6 billion.
- **Response:** Microsoft fixed the problem via updates. It was recommended that network administrators deploy fixes and keep an eye out for unusual activities.

2.6 Multipartite Viruses

Multipartite viruses combine the traits of boot sector and file infector viruses to infect executable files as well as boot sectors, hence increasing their effect and spread.

Signs of Multipartite Viruses Activity:

- Several antivirus notifications pointing to viruses in the boot sector and files.
- System instability or crashes that happen when apps are running, or the system is booting up.

- Reports pertaining to damaged or lost data in the impacted files and storage devices.
- Adjustments to system setups or settings that are not explained.
- Network behaviour suggestive of the spread of viruses via network drives or shared data.

Case Study: Tequila Virus (1991)

- **Overview:** Tequila was a multipartite virus that attacked DOS computers' executable files as well as boot sectors.
- **Signs of Activity:** Corrupted files, system crashes, and boot failures.
- **Impact:** Infected numerous systems, causing data loss and operational disruptions.
- **Response:** Updates for antivirus software were made available to help find and eradicate the malware. It was recommended that users not share contaminated discs and do routine virus scans.

2.7 Network Viruses

By exploiting holes in network protocols or services, network viruses propagate via network connections.

Signs of Network Viruses Activity:

- Abnormal trends in network traffic or sudden increases in network utilisation.
- Warnings from antivirus software that viruses are proliferating over network sharing.
- Identification of questionable behaviour on servers or network equipment.

Case Study: SQL Slammer (2003)

- **Overview:** A network virus known as SQL Slammer took advantage of a weakness in Microsoft SQL Server.
- **Signs of Activity:** Rapid network traffic spikes, causing widespread internet slowdowns.
- **Impact:** Infected over 75,000 systems within 10 minutes, causing network outages and significant financial damage.
- **Response:** Microsoft fixed the vulnerability with a patch. Patching and keeping an eye on network traffic were recommended for network administrators.

2.8 Stealth Viruses

To avoid being discovered by antivirus software, stealth viruses hide their existence and carry out their operations. They frequently use sophisticated strategies to stay undetected.

Signs of Stealth Viruses Activity:

- Abnormal trends in network traffic or sudden increases in network utilisation.
- Suspicious behaviour or symptoms, yet antivirus scans show no viruses.

- Unusual modifications to file properties or timestamps that suggest manipulation.
- Anomalies that point to possible illegal access or manipulation in system logs or event data.
- Unusual activity on the network coming from devices that are compromised.
- Reports of anomalous activity or decreased system performance on infected systems.

Case Study: Stuxnet (2010)

- **Overview:** Stuxnet was a sophisticated stealth virus designed to target industrial control systems.
- **Signs of Activity:** Unexplained system behavior, manipulation of industrial processes.
- **Impact:** Damaged Iran's nuclear centrifuges, causing significant disruption.
- **Response:** To comprehend the behaviour of the infection, forensic examination was carried out in detail. To safeguard vital infrastructure, security protocols have been strengthened.

3. Stakeholders

Collaboration between many Redback Operations stakeholders and external parties is necessary for an effective response to a viral epidemic.

3.1 IT Security Team

Lead: Daniel McAulay (Senior Project Leader)

The IT security team oversees defending the company's digital assets against virus attacks, spotting security issues, and putting preventative and remedial measures in place. Among their responsibilities and roles are:

- Evaluating the impact and reach of viral outbreaks through the analysis of security event data.
- Putting security measures in place to stop more illegal access and stop the spread of infections.
- Working together with the incident response team to control and reduce the effects of viral outbreaks.
- Carrying out forensic investigations to find the underlying cause of viral occurrences and stop them from happening again.
- Suggesting security improvements and offering incident response procedure advice to high management and other stakeholders.

3.2 Incident Response Team

Lead: Devika Sivakumar (Blue Team Leader)

The incident response team oversees managing the organization's response to viral outbreaks and organising cleaning activities. Among their responsibilities and roles are:

- Determining the extent and intensity of viral epidemics and carrying out the required corrective actions.
- Assembling staff and resources to lessen and mitigate the effects of viral assaults.
- Carrying out forensic investigations to ascertain the origin and scope of viral outbreaks and collect data for prospective legal actions.
- Notifying top management, outside contractors, and clients on crisis response strategies and recovery initiatives.
- Documenting best practices and lessons gained from viral occurrences will improve the organization's ability to respond to issues.

3.3 Communication Team

Lead: Kaleb Bowen (Company Lead)

Regarding viral outbreaks, the communication team oversees making sure that all internal and external stakeholders are informed in a clear and consistent manner. Among their responsibilities and roles are:

- Creating and carrying out communication strategies to alert relevant parties—such as staff members, clients, and outside suppliers—about viral outbreaks.
- Creating and distributing communication materials to answer queries and Concerns from stakeholders, including as statements, news releases, and FAQs.
- Taking part in public relations and media relations campaigns to safeguard the organization's image and lessen the damaging effects of viral outbreaks.
- Delivering frequent reports on stakeholder engagement and communication activities to the senior leadership and incident response team.

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 organisations who depend on the company's goods or services and might be impacted by viral pandemics. Among their responsibilities and roles are:

- Notifying the company of any unauthorised or questionable conduct pertaining to their accounts or transactions.
- Supplying pertinent data or proof to support the incident response team's viral outbreak investigation.
- Following the advice and directives of the organisation to safeguard personal data and lessen the effects of virus outbreaks.

3.5 Third-Party Vendors

Third-party vendors are outside companies that supply the company with products, services, or assistance; they may also have access to its networks, data, and systems. Among their responsibilities and roles are:

- Working along with the company's incident response team to find and fix security flaws or breaches pertaining to their goods or services.

- Giving the company help and support while it investigates and fixes any viruses that are damaging its networks or systems.
- Observing the duties imposed by law and contracts on data security and privacy, including the reporting of security breaches and assistance with incident response.

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)

RACI Chart for Virus Outbreak Incident Response

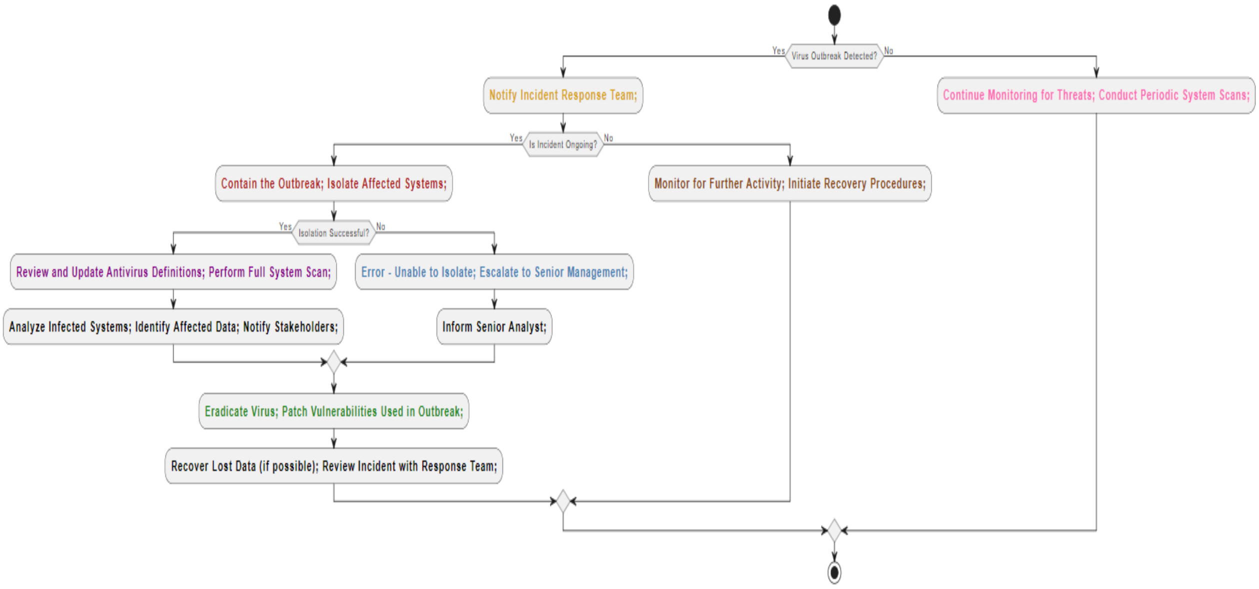
Task/Activity	**IT Security Team**	**Incident Response Team**	**Communication Team**	**Senior Management**	**Legal and Compliance**	**Customers**	**Third-Party Vendors**
Preparation							
Establish incident response team	R, C	A, R	I	I	C	I	I
Develop response procedures	A, R	R, C	I	C	C	I	I

Conduct training sessions	A, R	R	I	I	I	I	I
Implement surveillance systems	A, R	R	I	I	I	I	I
Detection							
Monitor system logs and traffic	A, R	R	I	I	I	I	I
Use IDS and SIEM tools	A, R	R	I	I	I	I	I
Analyse alerts	A, R	R	I	I	I	I	I
Analysis							
Collect forensic data	A, R	R	I	I	I	I	I
Identify attack methods	A, R	R	I	I	I	I	I
Determine impact	A, R	R	I	I	I	I	I
Containment							
Isolate compromised systems	A, R	R	I	I	I	I	I

Implement access restrictions	A, R	R	I	I	I	I	I
Block malicious traffic	A, R	R	I	I	I	I	I
Eradication							
Remove malicious software	A, R	R	I	I	I	I	I
Patch vulnerabilities	A, R	R	I	I	I	I	I
Update security policies	A, R	R	I	I	I	I	I
Recovery							
Restore backups	A, R	R	I	I	I	I	I
Rebuild systems	A, R	R	I	I	I	I	I
Conduct user training	A, R	R	I	I	I	I	I
Post-Incident Review							
Review incident response	A, R	R	I	I	I	I	I

Document lessons learned	A, R	R	I	I	I	I	I
Update response procedures	A, R	R	I	I	I	I	I
Communication							
Create communication plans	C	C	A, R	I	C	I	I
Draft communication materials	C	C	A, R	I	C	I	I
Manage media relations	C	C	A, R	I	C	I	I
Provide updates	C	C	A, R	I	C	I	I

4. Flow Diagram


Virus Outbreak Detected?
Yes
No
Notify Incident Response Team;
Continue Monitoring for Threats; Conduct Periodic System Scans;
Is Incident Ongoing?
Yes
No
Contain the Outbreak; Isolate Affected Systems;
Monitor for Further Activity; Initiate Recovery Procedures;
Isolation Successful?
Yes
No
Review and Update Antivirus Definitions; Perform Full System Scan;
Error - Unable to Isolate; Escalate to Senior Management;
Analyze Infected Systems; Identify Affected Data; Notify Stakeholders;
Inform Senior Analyst;
Eradicate Virus; Patch Vulnerabilities Used in Outbreak;
Recover Lost Data (if possible); Review Incident with Response Team;

1. Preparation (Prep): Yellow

    - Notify Incident Response Team: This phase is the first of getting ready to deal with a viral epidemic. As soon as a viral epidemic is detected, the incident response team is informed. We use the colour yellow to represent this stage of preparation.

2. Identification (Identify): Red

    - Contain the Outbreak; Isolate Affected Systems: This phase entails locating the viral outbreak and containing it right away. Measures are implemented to segregate compromised systems and restrict the virus's dissemination. Red is used to represent the vital and urgent nature of this stage.

3. Notification (Notif): Violet

    - Review and update antivirus definitions; perform full system scans: Notifying pertinent parties and putting initial mitigation measures in place are the main goals of this stage. Various measures are implemented to lessen the influence of the outbreak, including altering login passwords, and doing malware assessments. Malicious activity is also examined, and stakeholders are informed so they may organise a response. This notice and early reaction step are represented by the colour violet.

4. Containment (Contain): Sky Blue

    - Error-unable to isolate; Escalate to senior management: At this point, attempts are being done to stop the outbreak's spread. Senior management is informed so that the affected systems may be resolved if they cannot be effectively isolated. The containment measures meant to stop the virus's spread are symbolised by the colour sky blue.

5. Eradication (Erad): Light Green

    - Eradicate Virus; patch vulnerabilities used inn outbreak: The objectives of this step are to eradicate the infection and record incident information. Procedures for removing malware are followed, and incident details are recorded for later use. Light green is used to represent the process of getting rid of the infection and making sure the organization's systems are safe.

6. Recovery (Recover): Brown

    - Monitor for Further Activity; Initiate Recovery Procedures: At this point, attempts are being undertaken to recover from the viral outbreak and get everything back to normal. Recovery processes are started, and continual surveillance is done to find any new virus activity. The recovery phase, which aims to resume regular operations, is symbolised by the colour brown.

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

    - Continue Monitoring for Threats; Conduct Periodic system scans: In the last phase, post-event activities are carried out to assess the effectiveness of the reaction and pinpoint areas that require improvement. A post-event evaluation is carried out to evaluate the organization's reaction to the viral epidemic, and ongoing threat monitoring is maintained. The post-event steps intended to improve future response efforts and learn from the occurrence are indicated by the colour light pink.

5. Incident Response Stages

5.1 Preparation

- **Objective:** Putting in place the tools, processes, and regulations required to control virus outbreaks.
- **Activities:**
  - Putting up a team dedicated to incident response with specific duties.
  - Creating strategies and processes for crisis response, such as escalation routes and communication guidelines.
  - Ensuring preparedness via consistent training and event response practice.
  - Putting security measures and surveillance systems in place to identify and contain viral outbreaks.
- **Outcome:** A well-prepared company that can react to virus outbreaks fast and efficiently.

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 behaviour, such strange access patterns, or unauthorised file transfers.
  - Using security information and event management (SIEM) and intrusion detection systems (IDS) to find and stop threats.
  - Separating malicious from genuine activities by analysing anomalies and alarms.
- **Outcome:** Rapid reaction and mitigating actions are made possible by early virus outbreak identification.

5.3 Analysis

- **Objective:** Recognising the characteristics and extent of the virus an outbreak.
- **Activities:**
  - Gathering information and carrying out forensic investigation to determine the origin and severity of the virus infestation.
  - Examining networks and systems that have been infiltrated to identify attack strategies and the impact on compromised data.
  - Recognising the tactics, methods, and procedures (TTPs) of threat actors and indicators of compromise (IOCs).
- **Outcome:** A thorough comprehension of the virus outbreak, considering its origins, consequences, and sources.

5.4 Containment

- **Objective:** Help lessen the effect of the virus outbreak and prevent more illegal access or data leaks.
- **Activities:**
  - Dividing up susceptible machines and networks to stop intruders from moving laterally.
  - Putting access restrictions and protections in place to stop illegal access to sensitive information.
  - Limiting or preventing harmful data, software, or network flow to stop more damage.
- **Outcome:** Efficient handling of the virus outbreak, reducing harm to the company's information and infrastructure.

5.5 Eradication

- **Objective:** Removing all threats and vulnerabilities from the company's networks and IT systems, including those that still pose a threat.
- **Activities:**
  - Deleting dangerous files and software and putting hacked computers back in a safe configuration.
  - Upgrading or patching susceptible systems and software to stop further exploitation.
  - Examining and amending security guidelines and policies to fix any flaws or vulnerabilities found.
- **Outcome:** Eradication of all evidence of the virus breakout incident and mitigation of susceptibilities to avoid recurrence.

5.6 Recovery

- **Objective:** To restart company operations and return impacted systems and data to normal.
- **Activities:**
  - Restoring damaged systems and data backups to guarantee the integrity and accessibility of data.
  - Rebuilding or rearranging networks and systems to improve security and stop such incidents in the future.
  - Putting user awareness and education programmes into action to stop virus breakouts in the future.
- **Outcome:** Full restoration of operations and services, together with strengthened security measures to lessen the chance of recurrence.

5.7 Post- Incident Review

- **Objective:** Evaluating and pinpointing areas for improvement and lessons gained in the company's reaction to the virus outbreak issue.
- **Activities:**
  - Evaluating the incident response procedure in-depth to find its advantages, disadvantages, and potential areas for development.
  - Recording best practices and lessons discovered to improve incident response skills in the future.
  - Modifying security setups, rules, and incident response protocols considering review results.
- **Outcome:** Improved incident response capacities and preparedness against virus outbreaks in the future.

6. Steps for Monitoring Threats

6.1 Establish a Monitoring Strategy

Objective: Establish and implement a comprehensive strategy for continuous threat monitoring specifically targeting virus outbreaks.

Activities:

- **Objectives:** Clearly define the objectives for threat monitoring, such as detecting virus infections, identifying unauthorized access, and monitoring unusual network traffic indicative of virus activities.
- **Tools:** Select appropriate security tools such as IDS/IPS (Intrusion Detection/Prevention Systems), SIEM (Security Information and Event Management) systems, EDR (Endpoint Detection and Response) solutions, and antivirus software.
- **Baselines:** Establish baselines for normal user activity, system behavior, and network traffic patterns to identify deviations that may indicate virus presence.

Outcome: A well-defined monitoring strategy aligned with Redback Operations' goals, enhancing the ability to detect and respond to virus threats effectively.

6.2 Deploy Monitoring Solutions

Objective: Deploy and configure monitoring tools across the organization’s infrastructure to detect virus threats.

Activities:

- **Install and Configure Tools:** Deploy the selected monitoring tools across networks, systems, and endpoints. Ensure they are configured to detect virus-related activities and collect relevant data.
- **Integrate with Threat Intelligence:** Integrate monitoring tools with threat intelligence feeds to enhance the detection of known and emerging virus threats.
- **Enable Logging:** Ensure logging is enabled on critical systems, networks, and applications. Centralize log collection for efficient analysis and correlation.

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

6.3 Continuous Monitoring and Analysis

Objective: Maintain continuous monitoring and analysis to promptly detect and respond to virus threats.

Activities:

- **Real-Time Monitoring:** Implement real-time monitoring to continuously observe user activities, system behavior, and network traffic, facilitating the immediate detection of virus activities.
- **Anomaly Detection:** Utilize behavioral analytics and machine learning to identify anomalies and deviations from established baselines that may indicate virus presence.
- **Correlate Events:** Correlate events from various sources to identify patterns that may indicate coordinated virus attacks or persistent threats.

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

6.4 Alerting and Notification

Objective: Ensure timely and effective response to detected threats through a robust alerting system.

Activities:

- **Set Alert Thresholds:** Establish thresholds for different types of alerts based on severity and potential impact.
- **Automated Alerts:** Configure automated alerts to notify the security team of detected virus threats. Ensure alerts provide sufficient context for prompt assessment and action.
- **Prioritize Alerts:** Implement a system to prioritize alerts based on their severity and potential impact, focusing on the most critical threats first.

Outcome: Timely and effective response to detected virus threats, reducing the risk of significant damage.

6.5 Investigate and Respond

Objective: Conduct thorough investigations and implement appropriate actions to mitigate identified virus threats.

Activities:

- **Initial Triage:** Perform initial triage to verify the validity and potential impact of alerts. Determine the severity of the threat and whether the alert is a false positive.
- **Detailed Analysis:** Conduct in-depth analysis of confirmed alerts to understand the nature and extent of the virus threat. Use forensic tools and techniques to gather information and trace the source of the threat.
- **Containment and Eradication:** Initiate containment measures to prevent further damage if a threat is confirmed. Execute necessary eradication procedures to remove the virus from the environment.

Outcome: Effective investigation and mitigation of virus threats, ensuring minimal impact on the organization.

6.6 Post-Incident Review

Objective: Assess the effectiveness of the response and identify areas for improvement.

Activities:

- **Document Findings:** Record all details of the incident, including detection, analysis, and response actions taken.
- **Review and Improve:** Conduct a review of the monitoring and response processes post-incident to identify strengths, weaknesses, and lessons learned.
- **Update Monitoring Tools:** Update monitoring tools, configurations, and thresholds based on the findings to enhance future threat detection and response capabilities.

Outcome: Continuous improvement of incident response and threat monitoring processes, ensuring better preparedness for future virus outbreaks.

6.7 Continuous Improvement

Objective: Maintain and enhance the organization’s threat monitoring strategy and tools.

Activities:

- **Regular Audits:** Conduct regular audits to ensure monitoring tools and strategies remain effective and up to date with the latest threats.

- **Training and Awareness:** Provide ongoing training to security personnel on the latest threats and best practices for monitoring and response.
- **Adapt to New Threats:** Continuously adapt the monitoring strategy to address emerging threats. Stay informed about the latest threat intelligence and incorporate it into monitoring processes.

Outcome: A proactive and adaptive threat monitoring strategy that evolves with the changing threat landscape.

7. Terminology

- Virus Outbreak: A circumstance in which malicious software quickly spreads throughout the computers, networks, or devices of an organisation, usually with the goal of stealing, interfering with, or breaching data.
- Incident Response: A methodical and organised procedure designed to locate, contain, and lessen the harm a virus outbreak does to an organization's IT infrastructure to minimise interruption and get things back to normal.
- Forensic Analysis: The methodical analysis and assessment of digital data associated with the virus outbreak, such as malware samples, system artefacts, and network logs, to determine the source of the attack, estimate its extent, and supply proof for legal or investigative needs.
- Polymorphic Virus: A kind of virus that is challenging for antivirus software to identify and neutralise as it can alter its appearance or signature with every infection. During virus outbreaks, polymorphic viruses are renowned for their capacity to spread quickly and elude detection by conventional security measures.
- Endpoint Security: A thorough method for protecting mobile, laptop, and desktop computer systems—known as network endpoints—against online dangers including viruses. To prevent virus outbreaks, endpoint security solutions include host-based intrusion detection systems (HIDS), antivirus software, and endpoint detection and response (EDR) technologies.
- Infection Vector: The process or avenue via which a virus enters a network or organisation and infects systems. Email attachments, malicious websites, portable media (like USB drives), and software flaws are frequently used as entry points for virus outbreaks.
- Cyber Threat Hunting: Initiative-taking monitoring and scanning of networks and systems for indications of malicious behaviour or possible virus outbreaks. Cyber threat hunting is the process of identifying and eliminating threats before they become widespread viral outbreaks by examining network traffic, system behaviour, and records.