

Malware Outbreak Playbook

**Authorised by** **:**

**Date issued or last reviewed/revised** **:**

**Date last exercised** **:**

# Table of Contents

[1. Table of Contents 2](#_Toc210210432)

[2. Document Control 3](#_Toc210210433)

[2.1 Document Revision 3](#_Toc210210434)

[3. Assumptions & Disclaimer 4](#_Toc210210435)

[3.1 Assumptions 4](#_Toc210210436)

[3.2 Disclaimer 4](#_Toc210210437)

[4. Background 5](#_Toc210210438)

[5. Objectives 9](#_Toc210210439)

[5.1 Proactive Response 9](#_Toc210210440)

[5.2 Quick Containment 9](#_Toc210210441)

[5.3 Effective Remediation 9](#_Toc210210442)

[6. Readiness 10](#_Toc210210443)

[6.1 General Readiness 10](#_Toc210210444)

[6.2 Prepare Phase Readiness 10](#_Toc210210445)

[6.3 Detect Phase Readiness 11](#_Toc210210446)

[6.4 Analyse Phase Readiness 11](#_Toc210210447)

[6.5 Contain Phase Readiness 11](#_Toc210210448)

[6.6 Eradicate Phase Readiness 11](#_Toc210210449)

[6.7 Recover Phase Readiness 12](#_Toc210210450)

[6.8 Post-Incident Handling Phase Readiness 12](#_Toc210210451)

[7. NIST Incident Handling Categories 13](#_Toc210210452)

[7.1 NIST Framework Incident Response Life Cycle 13](#_Toc210210453)

[7.2 Prepare 15](#_Toc210210454)

[7.3 Detect 17](#_Toc210210455)

[7.4 Analyse 21](#_Toc210210456)

[7.5 Contain 25](#_Toc210210457)

[7.6 Eradicate 29](#_Toc210210458)

[7.7 Recover 33](#_Toc210210459)

[7.8 Post-Incident 37](#_Toc210210460)

[8. Glossary 41](#_Toc210210461)

# Document Control

## Document Revision

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Issue Date | Changes |
| 0.1 | Name | XX/XX/2025 | Initial Draft |
| 0.2 |  | XX/XX/XXXX | Draft Review |
| 1.1 |  | XX/XX/XXXX | Final release |

# Assumptions & Disclaimer

## Assumptions

* This playbook must be followed by an experienced Incident Response Team
* This playbook is reviewed and updated as part of the post-incident review exercise at the end of each similar incident
* This playbook must be approved by the relevant stakeholders
* This playbook is accessible by the Incident Response Team
* Perform a continuous impact assessment during the incident treatment
* Additional logs collection might be required throughout the incident treatment

## Disclaimer

This playbook is to be followed by an experienced Incident Response Team. The steps defined in this document, in the different workflows available in the NIST incident handling categories section, are presumed to be validated and approved by the appropriate stakeholders in the organisation. In case of an incident falling under this playbook category, the Incident Response Team will follow the process described below and will presume that their actions are approved in applying the appropriate security control to reduce the threat identified.

Incident Response Teams must maintain their knowledge of products, processes, and systems and ensure access to systems is adequate and accessible in the event of an incident.

The organisation following this playbook must be aware of the applicable laws, regulations, and compliance obligations such as GDPR, PCI and NDB schemes etc.

# Background

Malware and virus are terms that are often confused to be the same. However, malware is a term that covers all types of malicious software without taking into account its purpose, dynamic, spread, and distribution, it can include viruses, spyware, adware, nagware, trojans, worms, and more.

A virus, on the other hand, is a specific type of malware that can self-replicate and spread. A virus self-replicates by inserting its code into other programs.

Viruses spread by attaching themselves to legitimate files and programs, then distributed through infected websites, flash drives, and emails. A victim activates a virus by opening the infected application or file. Once activated, a virus may delete or encrypt files, modify applications, or disable system functions.

There are many different types of viruses. These are the three most common examples:

* The file infector can burrow into executable files and spread through a network. A file infector can overwrite a computer's operating system or even reformat its drive.
* The macro virus takes advantage of programs that support macros. Macro viruses usually arrive as Word or Excel documents attached to a spam email, or as a zipped attachment. Fake file names tempt the recipients to open the files, activating the viruses. An old but still prominent type of malware, macro viruses, remain popular with hackers.
* Polymorphic viruses modify their code. The virus replicates and encrypts itself, changing its code just enough to evade detection by antivirus programs. Malware encompasses all types of malicious software, including viruses, and may have a variety of goals. A few of the common objectives of malware are:
  + Trick a victim into providing personal data for [identity theft](https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/new-mcafee-report-identity-theft/)
  + Steal consumer credit card data or other financial data
  + Assume control of multiple computers to [launch denial-of-service attacks](https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/zombie-iot-botnets/) against other networks
  + Infect computers and use them to mine bitcoin or other cryptocurrencies

Besides viruses, numerous other types of malware can infect not only desktops, laptops, and servers, but also smartphones. Malware categories include the following:

* Worms: A worm is a standalone program that can self-replicate and spread over a network. Unlike a virus, a worm spreads by exploiting a vulnerability in the infected system or through email as an attachment masquerading as a legitimate file.
* Ransomware: As the name implies, ransomware demands that users pay a ransom—usually in bitcoin or other cryptocurrency or normal bank currency to regain access to their computer.
* Scareware: Many desktop users have encountered scareware, which attempts to frighten the victim into buying unnecessary software or providing their financial data. Scareware pops up on a user's desktop with flashing images or loud alarms, announcing that the computer has been infected. It usually urges the victim to quickly enter their credit card data and download a fake antivirus program.
* Adware and spyware: Adware pushes unwanted advertisements at users and spyware secretly collects information about the user. Spyware may record the websites the user visits, information about the user's computer system and vulnerabilities for a future attack, or the user’s keystrokes. Spyware that records keystrokes is called a keylogger. Keyloggers steal credit card numbers, passwords, account numbers, and other sensitive data simply by logging what the user types.
* Fileless malware. Unlike traditional malware, file-less malware does not download code onto a computer, so there is no malware signature for a virus scanner to detect. Instead, file-less malware operates in the computer's memory and may evade detection by hiding in a trusted utility, productivity tool, or security application.

Malware attack follows a multiple steps process; the below section shows the modern web attack broken down into 5 stages:

Execution

Infection

Exploit

Distribution

Entry Point

A malware outbreak is defined as the spreading of the same virus to multiple computers in the same network of an organisation.

According to NIST Special Publication 800-61 rev 2, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Prepare** | **Detect & Analyse** | **Contain, Eradicate & Recover** | **Post-Incident Handling** |
| The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.  This should also include regular testing of playbooks to ensure they are robust, easy to follow and incorporate any recent learnings | The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes.  Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident. | The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organisation to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation. | Because the handling of Malware incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Malware incidents to prevent similar incidents from occurring. |

The Incident Response Plan (IRP) may contain references to the organisation-defined playbooks. The playbooks will define the steps to follow in case of a specific incident, in this playbook (Malware Outbreak). In case of an incident, it is recommended to refer to the IRP, if an incident response is covered in a playbook, the use of the playbook takes priority on the IRP.

This playbook will not cover the areas below that might already be available in the IRP.

The IRP may cover the areas below:

* Data Categories for Tracking Incidents
* Types of Incident Detection Channels
* Incident prioritisation matrix and triage process
* Incident Response Workflow
* Incident Root-cause Framework
* Incident Response Lifecycle
* Incident Response Checklist (During)
* Post-Incident checklist (After)
* Incident Response Performance Metrics
* Incident Response Process/Procedures/Playbook List
* Roles and Responsibilities
* Incident Response Team
* Incident Response Team Organisational Structures
* The communication process in case of an incident
* Checklist for Communicating with Media
* Incident Communication Memo to Employees - Template
* Sample Customer Notification Letter - Template
* Response Plan for Compromise of Personal Information - Template
* Incident evidence collection log

For any information related to the above, please refer to the Incident Response Plan.

# Objectives

## Proactive Response

A playbook helps security teams optimise their actions for efficiency and productivity. Your security team can plan and prioritise their actions in a methodical and repeatable fashion. Following a playbook, your team will have the best chance to respond and contain incidents when and where they occur.

## Quick Containment

Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organisation, and taking the proper steps to mitigate damage.

## Effective Remediation

Playbooks facilitate security processes, mitigation plans, and smooth communication between multiple departments. By working methodically through data collection, analysis, and communications, you improve the odds for effective eradication, recovery with integrity, and forensic-quality reporting.

# Readiness

Incident Response Teams function in a state of constant readiness. A security incident can occur at any time of day or night so Incident Response Teams should always be prepared to respond.

A state of readiness involves checking their processes, procedures, tools, and access in the downtime to ensure that when an incident occurs, they are familiar with the processes and tools involved to reduce wasted time and effort.

## General Readiness

* Ensure that the organisation has an Incident Response Plan (IRP) that is up to date, reviewed, approved by the appropriate stakeholders, authorised by the appropriate executive, and communicated to the appropriate teams (Incident Response Teams, IT Support Team, IT Team).
* Ensure that the required playbooks to support the IRP exists or are being developed.
* Ensure that the playbooks and all required processes and procedures in responding to an incident are referred to in the IRP.
* Ensure that the organisation has a functioning knowledge base tool.
* Ensure that the required users have access to the organisation’s knowledge base.
* Ensure that the organisation has a training plan in place to upskill the employees in the required area that will speed up their reaction in dealing with a threat.

## Prepare Phase Readiness

* Ensure access to the breached systems.
* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure access to the RACI matrix to identify the point of escalations.
* Ensure access to escalation paths.
* Ensure access to contact details (email, phone number) of the stakeholders designated as points of escalation.
* Ensure access to contact details (email, phone number) of the appropriate contact in the legal team.
* Ensure access to contact details (email, phone number) of the appropriate contact in the Governance and Compliance Team (GRC).
* Ensure access to contact details (email, phone number) of the appropriate contact in the marketing/communication team.
* Ensure access to contact details of vendors for the tools used and authority to engage vendor support teams where applicable and escalation contact details.

## Detect Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incidents are included in the knowledge base.
* Ensure that detection tuning learnings from previous incidents have been updated in the appropriate toolsets.
* Ensure toolsets are up to date.

## Analyse Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure toolsets are up to date.

## Contain Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure good functioning of firewalls and other network devices.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that firewall rules are documented.
* Ensure access to the organisation’s risk framework, process, and acceptance criteria.
* Ensure access (read and write) to the organisation’s asset register to update the status of the affected assets.

## Eradicate Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the Incident Response Team is aware of the communication plan in the event of incidents.

## Recover Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that cloud services and other data stores are synchronised.
* Ensure that any network changes are documented.
* Ensure any existing related risks are reviewed, reassessed, and updated.
* Create any risk items identified.

## Post-Incident Handling Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.

# NIST Incident Handling Categories

## NIST Framework Incident Response Life Cycle

[[1]](#footnote-1)Lifecycle diagram from NIST Computer Incident Handling Guide SP 800-61 Revision 2

**Preparation**[[2]](#footnote-2)

Incident response methodologies typically emphasise preparation—not only establishing an incidentresponse capability so that the organisation is ready to respond to incidents, but also preventing incidentsby ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.

**Detection & Analysis**[[3]](#footnote-3)

In the event of an incident, the Incident Response Team must detect and identify the type of incident occurring. In addition, it is necessary to collect the relevant data (logs, files, information) to be analysed. Once the above is completed, it is required to document the incident, prioritise it then communicate it to the appropriate authorities. The legal team of the organisation should be notified in the case of an event occurring that falls under the Notifiable Data Breaches (NDB) scheme.

**Containment, Eradication & Recovery**[[4]](#footnote-4)

Once the incident is identified, the Incident Response Team should be able to plan a strategy to stop the breach and reduce the risk of the threat spreading, therefore starting the recovery phase.

**Post Incident Activity**[[5]](#footnote-5)

Once an incident is resolved, the next step for the team is to go back to the beginning and prepare for the next incident; input from each new incident should help inform the preparation process, whether by adding new information about new threats or simply as a means of fine-tuning procedures that are part of the incident management process. Post-Incident Review is one of the main activities of this phase, and it includes the review and update of the incident playbook and the update of the knowledgebase.

Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organisation-specific threats. Each risk should be prioritised, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasise monitoring and response activities for those resources.[[6]](#footnote-6)

The objectives of using the NIST Framework are the following:

* A better understanding and management of cybersecurity risks
* A decrease in cybersecurity risks
* Prioritisation of cybersecurity activities
* Prioritisation in cybersecurity investments and maximisation of the impact of each dollar spent on cybersecurity
* Define a common language to communicate inside and outside an organisation
* Improvement of communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives
* Defined cybersecurity posture

## Prepare

The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they occur.

The organisation should have an Incident Response Plan (IRP) well documented, thoroughly explaining the roles and responsibilities of the employees/teams involved in the incident handling process. The plan must be tested to assure that your employees will perform as they were trained.

Additional procedures might be followed according to the organisation’s systems and service structure.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.2.1 | Determine Core Ops Team & Define Roles | Define roles and responsibilities in case of an incident and define the points of escalation | Incident Response Team and IT Team and Leadership team (CISO, CIO, CTO…etc) |
| 7.2.2 | Determine Extended Team & Define Roles | Define teams that are involved in the Malware outbreak Incident | Incident Response Team  IT Team |
| 7.2.3 | Define Escalation Path | Determine the list of stakeholders in case of escalation and define types of escalations | Incident Response Team |
| 7.2.4 | Request relevant logs and information | Collect the logs and relevant evidence related to the incident to identify its origin | Incident Response Team |

## Detect

The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes. Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| - | Define Threat Indicators | Decision box to illustrate the 2 paths possible (follow standard threat indicator or custom threat indicators) | Incident Response Team |
| 7.3.1 | Standard | An Indicator represents an atomic piece of information that has some intelligence value, there is a standard threat indicator that is predefined and makes the process smoother  Sub steps: 7.3.1.1 – 7.3.1.5 | Incident Response Team |
| 7.3.2 | Custom | An Indicator represents an atomic piece of information that has some intelligence value. There are custom threat indicators according to the type of incident/threat  Sub steps: 7.3.2.1 | Incident Response Team |
| - | Define Risk Factors | Decision box to illustrate the 2 paths possible (follow standard risk factors or custom risk factors) | Incident Response Team |
| 7.3.3 | Standard | A risk factor is any attribute or characteristic that increases the likelihood of a risk occurring  Sub steps: 7.3.3.1 – 7.3.3.8 | Risk Management Team (GRC) |
| 7.3.4 | Custom | A risk factor is any attribute or characteristic that increases the likelihood of a risk occurring  Sub steps: 7.3.4.1 | Risk Management Team (GRC) |
| 7.3.5 | Conduct Scans | Perform scans to detect vulnerabilities in the internal and external environment of the organisation | Incident Response Team |
| 7.3.6 | Deployment of EDR Tools | Consider the deployment of EDR tools | Incident Response Team |
| 7.3.7 | Request Logs | Request logs – DNS and Web Proxy | Incident Response Team |
| 7.3.8 | Request Packet Capture | Obtain packet capture to be used in the analyse phase | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Unknown or unexpected network traffic from a site | Detect any abnormal network traffic from the organisation’s sites, locations, stores, or headquarters | IT Team (Network Team)  Incident Response Team |
| 7.3.1.2 | Unknown or unexpected outgoing internet traffic | Detect any abnormal outgoing internet traffic | Incident Response Team  IT Team |
| 7.3.1.3 | Unknown or unexpected services and applications configured to launch automatically on system boot | Detect any abnormal services and applications programmed to launch on system boot | Incident Response Team  IT Team |
| 7.3.1.4 | Antivirus programs malfunctioning or becoming disabled for unknown reasons | Identify and list the antivirus installed that are not functioning properly or being disabled without the security team being notified | Incident Response Team  IT team |
| 7.3.1.5 | Degraded service | Check the CPU usage and other I/O operations for spikes or unavailability | Incident Response Team  IT team |
| 7.3.2.1 | Custom Indicators | An Indicator represents an atomic piece of information that has some intelligence value. There are custom threat indicators according to the type of incident or threat | Incident Response Team  IT Team |
| 7.3.3.1 | IP is at risk of being exposed | Determine if IP is at risk of exposure | Incident Response Team  IT Team |
| 7.3.3.2 | PII is at risk of being exposed | Determine if PII is at risk of exposure | IT Support Team  IT Team |
| 7.3.3.3 | This act could be exploited for criminal activity | Consider if the information exposed could be used for criminal activity | Incident Response Team  IT Team |
| 7.3.3.4 | Customers are affected by this incident | Identify if customers are affected | Incident Response Team  IT team |
| 7.3.3.5 | Public safety is affected | Identify if public safety is affected  e.g., affected systems impact safety controls | Incident Response Team  IT team |
| 7.3.3.6 | Brand impact | Document the incident, including risks and impacts, and communicate it to the appropriate stakeholder(s). Notify communication and legal teams | Incident Response Team  IT Team  Communication Team  Legal Team |
| 7.3.3.7 | Products/goods/services are affected by this outbreak | Detect and list the assets affected by the outbreak | Incident Response Team  IT Team |
| 7.3.3.8 | Personnel safety is affected | Identify if personnel safety is affected  e.g., affected systems impact safety controls | Incident Response Team  IT Team |
| 7.3.4.1 | Custom Factors | A risk factor is any attribute or characteristic that increases the likelihood risk of occurring | Incident Response Team  Risk Management Team (GRC) |

## Analyse

During this phase, collected data and information is analysed to confirm the incident scope and impact and determine possible containment and eradication techniques and tasks.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.1 | Gather metadata | Collect the metadata linked to the incident | Incident Response Team |
| 7.4.2 | Check knowledgebase | Use the organisation knowledgebase tool to gather information related to the incident | Incident Response Team |
| 7.4.3 | Analyse information | Analyse malicious or suspicious information | Incident Response Team |
| - | Identification of Malware by AV | Check how the malware was identified | Incident Response Team |
| 7.4.4 | Define Risk | Define the risk identified and categorise it | Incident Response Team |
| - | Define Risk Factors | Decision box to illustrate the 2 paths possible (follow standard risk factors or custom risk factors) | Risk Management Team (GRC)  Incident Response Team |
| 7.4.5 | Standard | Define standard risk factors according to the organisation’s risk management process and acceptance criteria that have a privacy impact, a business impact and technical impact  Sub steps: 7.4.5.1 – 7.4.5.8 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.6 | Custom | Define custom risk factor  Sub steps: 7.4.6.1 – 7.4.6.4 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.7 | Identification of AV signature | Define the type of virus in order to define the steps of resolution | Incident Response Team |
| 7.4.8 | Update and patch AV | Update and patch AV in order to include the vulnerability identified | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.5.1 | IP is at risk of being exposed | Determine if IP is at risk of exposure | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.5.2 | PII is at risk of being exposed | Determine if PII is at risk of exposure | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.5.3 | Customers are affected by this incident | Identify customers that are affected | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.5.4 | Public safety is affected | Identify if public safety is affected | Governance and Compliance team  Legal Team |
| 7.4.5.5 | Personnel safety is affected | Identify if personnel safety is affected | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.5.6 | This act could be exploited for criminal activity | Consider if the information exposed could be used for criminal activity | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.5.7 | This could harm the public brand | Document the incident, including risks and impacts, and communicate it to the appropriate stakeholder(s). Notify communication and legal teams | Legal Team  Communication Team  The leadership team (C level) |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4.5.8 | Products/goods/services are affected by this outbreak | Detect and list the assets affected by the outbreak | Legal Team  Governance and Compliance Team |
| 7.4.6.1 | Business | Define business impact due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.6.2 | Operational | Define operational impact due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.6.3 | Compliance | Define the impact on the governance and compliance team due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.6.4 | Industry | Define industry impact due to the incident | Risk Management Team (GRC)  Incident Response Team |

## Contain

The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. An organisation needs to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1 | Additional Information Gathering | Identify the systems that have been affected, the data compromised, the IT services being impacted, the means through which malware gained access, the vulnerability that is being exploited, and the ways the attack may spread  Sub steps: 7.5.1.1 – 7.5.1.19 | Incident Response Team  IT Team |
| - | Is the malware remotely controlled | Consider the possibility that the malware is controlled remotely | Incident Response Team  IT Team |
| 7.5.2 | Analyse accounts on systems that have been compromised | Identify and record all user and systems accounts on compromised systems | Incident Response Team  IT Team |
| 7.5.3 | Change the password of breached accounts | Change the password of the accounts that have been identified | Incident Response Team  IT Team |
| 7.5.4 | Consideration for containment | Consideration for containment of the following:  Network layer controls, host layer controls, application layer controls, EDR solution | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1.1 | Server | Check, isolate, and list servers that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.2 | Desktop | Check, isolate, and list desktops that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.3 | Laptop | Check, isolate, and list laptops that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.4 | Mobile | Check, isolate, and list mobiles that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.5 | VM | Check, isolate, and list virtual machines that have been corrupted | Incident Response Team  IT Team |
| 7.5.1.6 | LDAP Directory | Check, isolate, and list LDAP Directory that has been corrupted | Incident Response Team  IT Team |
| 7.5.1.7 | Select Database | Choose a database for observation | Incident Response Team |
| 7.5.1.8 | Query Database | Extract data from the chosen database | Incident Response Team |
| 7.5.1.9 | Generate Report | Generate the report to identify the abnormal activity | Incident Response Team |
| 7.5.1.10 | View Report | Generate a report on the compromised users and credentials | Incident Response Team |
| 7.5.1.11 | View Record Details | Check the details of the record | Incident Response Team |
| 7.5.1.12 | Layered controls | Containment steps can occur at the network, host, or application layer to obtain containment. E.g., firewall rules, host configuration changes or application of a patch | Incident Response Team and IT Teams |
| 7.5.1.13 | Select Records | Select records | Incident Response Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.5.1.14 | Copy Record Details | Copy records details | Incident Response Team |
| 7.5.1.15 | SIEM | Security information and event management systems are used to provide real-time analysis of security alerts generated by applications and network hardware. This tool should be used, monitored, and owned by the organisation’s security operation centre (SOC) | Incident Response Team |
| 7.5.1.16 | IDS | Use a monitoring system such as IDS | Incident Response Team |
| 7.5.1.17 | Firewall | It is necessary to have in place a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules | Incident Response Team  IT Team |
| 7.5.1.18 | Scanners | Implemented and updated | Incident Response Team  IT Team |
| 7.5.1.19 | Antivirus | Implemented and updated | Incident Response Team  IT Team |

## Eradicate

The fourth phase, eradicate, refers to the removal of the threat and its immediate recurrence.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1 | Prevent Spread | Implement the security controls in place to prevent the spread of the virus detected  Sub steps: 7.6.1.1 – 7.6.1.18 | Incident Response Team |
| 7.6.2 | Obtain an image of the machine or device | Capture an image of the corrupted machine’s hard drive(s) | Incident Response Team  IT Team |
| 7.6.3 | Wipe and rebuild or restore the device from a trusted source | Clean and rebuild the machine using a trusted source | Incident Response Team  IT Team |
| 7.6.4 | Forensic Investigation | Investigate the image taken from the corrupted device | Incident Response Team  IT Team |
| 7.6.5 | Conduct Scan | Conduct a scan after the steps above to check if the number of devices corrupted increased | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1.1 | Run in Sandbox | Execute the malware in a sandboxed environment to monitor for indicators of compromise and propagation | Incident Response Team  IT Team |
| 7.6.1.2 | Analyse forensics | Analyse incident logs, evidence …etc | Incident Response Team  IT Team |
| 7.6.1.3 | Request System Patch | Implement a patch management culture and schedule patch updates regularly | Incident Response Team  IT Team |
| 7.6.1.4 | Block with Antivirus | Use antivirus to stop malware and virus | Incident Response Team |
| 7.6.1.5 | Disable Services | Disable services | IT Team |
| 7.6.1.6 | Restrict Network and Site | Define the network and site to be restricted and action the restriction | Incident Response Team |
| 7.6.1.7 | Adjust Firewall Rules | Update firewall rules to make sure that they are up to date | IT Team |
| 7.6.1.8 | Apply SIEM Rules | Make sure that the rule defined in SIEM is applicable | Incident Response Team |
| 7.6.1.9 | Conference Call | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via conference call | Incident Response Team  IT Team |
| 7.6.1.10 | Intranet Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via Intranet Meeting | Incident Response Team  IT Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.6.1.11 | Internet Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via Internet Meeting | Incident Response Team  IT Team |
| 7.6.1.12 | Direct Phone Call | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via direct phone call | Incident Response Team  IT Team |
| 7.6.1.13 | In-Person Meeting | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach in-person meeting | Incident Response Team  IT Team |
| 7.6.1.14 | Mobile Messaging | Check if this communication channel is corrupted and if not, this channel can be used as Business as Usual. Inform the selected audience about the breach via mobile messaging | Incident Response Team  IT Team |
| 7.6.1.15 | Clean with Antivirus | Make sure to have a clean device and environment by using antivirus and cleaning the system with it | Incident Response Team |
| 7.6.1.16 | Quarantine with Antivirus | Enable the quarantine option within the Antivirus | IT Team |
| 7.6.1.17 | Malware Removal Tool | Use the malware removal tool | Incident Response Team |
| 7.6.1.18 | Manual Intervention | In case of failure of eradicating the malware with automated tools follow a manual process to remove traces of the malware. | IT Team |

## Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements;



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1 | Build the device from a trusted source | Rebuild the machine using a trusted source for download Sub steps: 7.7.1.1 – 7.7.1.11 | IT Team |
| 7.7.2 | Rollback or complete changes | Follow organisation processes for rolling back IT changes or complete change records for IT changes made during the incident | Incident Response Team |
| 7.7.3 | Documentation Update | Document all the changes made | Incident Response Team |
| 7.7.4 | Update ticket and Incident status | Update the ticketing system with the status of the incident (open, close, in progress, pending) to assure that the stakeholder is aware of where the incident is at | Incident Response Team |
| 7.7.5 | Validation & Assurance | The following assurance considerations should be considered during the recovery phase:   * Perform a baseline vulnerability scan * Perform penetration testing * Ensure configuration adheres to best practice * Perform a code review if relevant * Document the findings gathered from the assessment above   Update the risk and issue registers with the findings and prioritised them | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1.1 | Reimage | Reimage the device from a known good source of the corporate SOE or vendor-supplied restore media | IT Team  IT Support |
| 7.7.1.2 | IDS/IPS & firewall updates | Update the organisation’s monitoring and controls systems and keep these up to date | Incident Response Team  IT Team IT Support |
| 7.7.1.3 | Rebuild | Restore device to factory state and apply organisation changes to restore services. | Incident Response Team  IT Team |
| 7.7.1.4 | Remove Temporary Containment | Remove any temporary containment steps such as firewall rules or configuration changes | IT Support |
| 7.7.1.5 | Mitigate vulnerabilities | Identify and mitigate vulnerabilities. This has to be documented in vulnerability support and ensure regular vulnerability assessments are conducted | Incident Response Team  IT Support |
| 7.7.1.6 | Coordinate AV updates to be pushed upon release from the AV vendor | It is recommended to drive this activity to make sure that the updates are deployed effectively and in a timely manner | Incident Response Team  IT Support |
| 7.7.1.7 | Data Restore | Restore the data | Incident Response Team  IT Support |
| 7.7.1.8 | Cloud Synchronisation | Ensure to programme regular synchronisation | Incident Response Team  IT Support |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.7.1.9 | Baseline system | Before returning the device to the production environment conduct baseline checks to aid in the analysis of anomalies in future events. E.g., open network ports, running services etc. | Incident Response Team  IT Support |
| 7.7.1.10 | Scan host with updated signature | Performing scanning of the host(s) with an updated signature to identify any vulnerabilities or malware | Incident Response Team  IT Support |
| 7.7.1.11 | Scan file share with updated signature | Performing scanning on the file share with updated signature to identify vulnerabilities or malware | Incident Response Team  IT Support |

## Post-Incident

Because the handling of Malware Outbreak incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Malware Outbreak incidents to prevent similar incidents from occurring.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.1 | Incident review | It is necessary to include an incident review in the Incident management process  Sub steps: 7.8.1.1 – 7.8.1.2 | Incident Response Team (IRP) |
| 7.8.2 | Lessons uncovered | Identify the items that require improvements such as policy updates, new controls to implement, new standards or frameworks to implement etc.  Sub steps: 7.8.2.1 – 7.8.2.4 | Incident Response Team |
| 7.8.3 | Lessons applied | Determine what worked well in the organisation’s incident response plan, and opportunities for improvement. Lessons learned from both mock and real events will help strengthen systems against future attacks.  Sub steps: 7.8.3.1 – 7.8.3.3 | Incident Response Team |
| 7.8.4 | Response workflow updated | Check that the new configurations are in place via the performance of internal audits and following a continuous improvement process | IT Team  Incident Response Team |
| 7.8.5 | Update of the knowledgebase | Add the new processes or procedures used in this incident to the organisation knowledgebase | IT Team  Incident Response Team |
| 7.8.6 | Update Risk Register | Update the risk register to define the new level of the risk and define its new status | Incident Response Team  GRC Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.1.1 | Electronic Personal Health Information (ePHI) compromised? | Identify if Electronic Personal Health Information has been compromised as a consequence of this type of incident | Incident Response Team  IT Team |
| 7.8.1.2 | Sensitive information compromised? | Identify if sensitive information has been compromised as a consequence of this type of incident | Incident Response Team  IT Team |
| 7.8.2.1 | Discovery meeting | Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what was learned from the incident | Incident Response Team |
| 7.8.2.2 | Policy updates defined | Define the uplift required to improve the organisation’s security policies to embed them in the organisation | Incident Response Team  IT Team  Governance & Compliance Team  Leadership Team (C-Level) |
| 7.8.2.3 | Process updates | Update processes to ensure the inclusion of the new steps identified as missing to ensure an improved security posture | All organisation |
| 7.8.2.4 | Configuration updates defined | Implement the configuration updates as required to strengthen systems against future attacks | Incident Response Team  IT Team |
| 7.8.3.1 | Policies implemented | Once policies are updated, these have to be implemented and communicated within the organisation. Owners should be defined for each policy and the review date should be determined | Policy Owners |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.8.3.2 | Process changes implemented | Implementation of the uplifted or updated processes | Policy Owners  Organisational Change management Team  The project team in charge of the process update project |
| 7.8.3.3 | Configurations applied | Check that the updated configurations are in place and following a continuous improvement process | IT Team |

# Glossary

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CTO: Chief Technology Officer

GRC: Governance Risk & Compliance

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IR Team: Incident Response Team

IRP: Incident Response Plan

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

Malware: Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network

MB: Megabyte

NDB: Notifiable Data Breach

NIST: National Institute of Standards and Technology

Procedure: A document written to support a specific process

Process: A series of actions or steps taken to achieve a specific end state

SIEM: Security Information and Event Management

SOC: Security Operation Centre

VM: Virtual Machine

1. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-1)
2. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-2)
3. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-3)
4. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-4)
5. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-5)
6. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-6)