

Root Access Playbook

**Authorised by** **:**

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

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

# Table of Contents

[1. Table of Contents 2](#_Toc210223463)

[2. Document Control 3](#_Toc210223464)

[2.1 Document Revision 3](#_Toc210223465)

[3. Assumptions & Disclaimer 4](#_Toc210223466)

[3.1 Assumptions 4](#_Toc210223467)

[3.2 Disclaimer 4](#_Toc210223468)

[4. Background 5](#_Toc210223469)

[5. Objectives 7](#_Toc210223470)

[5.1 Proactive Response 7](#_Toc210223471)

[5.2 Quick Containment 7](#_Toc210223472)

[5.3 Effective Remediation 7](#_Toc210223473)

[6. Readiness 8](#_Toc210223474)

[6.1 General Readiness 8](#_Toc210223475)

[6.2 Prepare Phase Readiness 8](#_Toc210223476)

[6.3 Detect Phase Readiness 9](#_Toc210223477)

[6.4 Analyse Phase Readiness 9](#_Toc210223478)

[6.5 Contain Phase Readiness 9](#_Toc210223479)

[6.6 Eradicate Phase Readiness 9](#_Toc210223480)

[6.7 Recover Phase Readiness 10](#_Toc210223481)

[6.8 Post-Incident Handling Phase Readiness 10](#_Toc210223482)

[7. NIST Incident Handling Categories 11](#_Toc210223483)

[7.1 NIST Framework Incident Response Life Cycle 11](#_Toc210223484)

[7.2 Prepare 13](#_Toc210223485)

[7.3 Detect 15](#_Toc210223486)

[7.4 Analyse 19](#_Toc210223487)

[7.5 Contain 23](#_Toc210223488)

[7.6 Eradicate 27](#_Toc210223489)

[7.7 Recover 30](#_Toc210223490)

[7.8 Post-Incident 32](#_Toc210223491)

[8. Glossary 36](#_Toc210223492)

# 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

Obtaining root access is to execute any command and access any system resource on a device using the ‘root’ or local administrator account on a system or device. Root access is specific to Linux and Unix and also to some similar systems such as Android or Mac OSX. Root access is typically not required as the ‘sudo’ function permits users to execute commands in an elevated manner. Any activity of the root account should be reviewed.

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 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. 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. | Because the handling of Root Access incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Root Access 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 (Root Access). 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 when they are uncovered.

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 this type of Incident | Incident Response Team  IT Team |
| 7.2.3 | Define Escalation Path if different from IRP | Determine the list of stakeholders in case of escalation and define types of escalations that are not documented in IRP | Incident Response Team  IT Team |
| 7.2.4 | Collect and store logs and information | Collect the logs and relevant evidence related to the incident to identify its origin | Incident Response Team  IT 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 two 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 – 7.3.1.17 | 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 or threat  Sub steps: 7.3.2.1 | Incident Response Team |
| 7.3.3 | Categorise incident | Define the type of incident, its level, its degree of priority…etc. | Incident Response Team |
| 7.3.4 | Request logs as required | Request logs of DNS, Proxy, local…etc | Incident Response Team |
| 7.3.5 | Conduct content Scans | Perform scans to detect vulnerabilities in the internal and external environment of the organisation | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Installation or configuration of unauthorised software or services | Investigate usual software installation and unusual changes to system configuration | Incident Response Team  IT Team |
| 7.3.1.2 | Logins to multiple systems with the same administrative user credentials | Identify the credentials used to login into multiple systems | Incident Response Team  IT Team |
| 7.3.1.3 | Increased administrator or root logins to a computer system | Monitor administrator and root logins to identify any increase in the use of these types of credentials | Incident Response Team  IT Team |
| 7.3.1.4 | Exfiltration of data off of a computer system | Check if there was any data exfiltration | Incident Response Team  IT team |
| 7.3.1.5 | Administrative or root access to systems outside of normal business hours | Monitor to detect administrator or root access done out of agreed business hours | Incident Response Team  IT team |
| 7.3.1.6 | Access to a computer system through abnormal ports or protocols | Detect any access done via usual ports or protocols | Incident Response Team  IT Team |
| 7.3.1.7 | The user is unable to log into an account | Identify any account that has difficulties logging in | Incident Response Team  IT Team |
| 7.3.1.8 | Suspicious network traffic is initiated from the internal network | Monitor the network traffic to identify suspicious traffic | IT Support Team  IT Team |
| 7.3.1.9 | Unexplained system failures or restarts | Detect system failures | Incident Response Team  IT Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.3.1.10 | Unexplained escalation of privileges of user accounts | Identify accounts that have usual access to systems | Incident Response Team  IT team |
| 7.3.1.11 | Unexplained use of disabled or dormant user accounts | Detect dormant accounts that are suddenly in use again | Incident Response Team  IT team |
| 7.3.1.12 | Unexplained modification or destruction of user files | Identify any unusual deleting or destruction of documents or files | Incident Response Team  IT team |
| 7.3.1.13 | Unexplained modifications to system settings | Monitor and identify unusual changes to system settings and parameters | Incident Response Team  IT team |
| 7.3.1.14 | Unexplained emails from user accounts | Identify and quarantine unusual or suspicious emails | Incident Response Team  IT team |
| 7.3.1.15 | Notification from outside organizations (ISP, business partners, 3rd party) | Ensure to review notifications from third parties regarding root access incidents | Incident Response Team  IT team |
| 7.3.1.16 | Alerting from Firewall and Intrusion Detection Systems | Analyse firewall and AV reports to detect intrusions | Incident Response Team  IT team |
| 7.3.1.17 | Unauthorized creation of new user accounts | Monitor account creation to avoid the unusual user account creation | 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 |

## 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** |
| - | Define risk factors | Decision box to illustrate the two paths possible (follow standard risk factors or custom risk factors) | Risk Management Team (GRC)  Incident Response Team |
| 7.4.1 | 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: 7.4.1.1 – 7.4.1.13 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2 | Custom | Define custom risk factor | Risk Management Team (GRC)  Incident Response Team |
| 7.4.3 | Determine patch methods | Define the patching methods that will be used in these circumstances | Incident Response Team |
| 7.4.4 | Additional log collection | Collection of logs is required by the security analyst to determine the incident spread and the next steps for containment and eradication | Incident Response Team |
| 7.4.5 | Evidence collection | It is required to gather the evidence related to the incident happening to be used for analysis | Incident Response Team |
| 7.4.6 | Data capture | Perform a data capture | Incident Response Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4.7 | Analysis | Analyse malicious or suspicious information. It is recommended to identify the following:   * The systems that have been accessed or are at risk * Systems to be taken offline due to compromise * Systems locked out due to repeated login attempts * Systems with outage or degradation of services * User accounts compromised or modified * IT services impacted * Unauthorised tools used to access systems or user accounts * Any source attribution collected * The tools used to detect the attack | Incident Response Team |
| 7.4.8 | Identify root cause | It is required to investigate the root cause of the root access incident by analysing the evidence and logs collected | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.1.1 | Employees are affected by this compromise | Identify and list internal accounts that have been affected | Incident Response Team |
| 7.4.1.2 | Customers are affected by this compromise | Identify and list the customer accounts that have been affected | Incident Response Team |
| 7.4.1.3 | Public or personnel safety affected | Identify if personnel or public data has been affected | Incident Response Team |
| 7.4.1.4 | Ability to control, record, measure, or track any significant amounts of inventory, products, cash, or revenue lost | Track revenue loss due to the incident | Incident Response Team |
| 7.4.1.5 | Products, goods, or services are affected by this compromise | Identify the products, goods, or services that have been compromised | Incident Response Team |
| 7.4.1.6 | There is internal knowledge of this incident | Ensure the communication around the incident to make sure that the right stakeholders and team are aware of it | Incident Response Team |
| 7.4.1.7 | This act is being launched by known entities | Identify the source of the incident | Incident Response Team |
| 7.4.1.8 | Worst-case business impact if unable to mitigate the attack | Define worst-case business impact | Incident Response Team |
| 7.4.1.9 | Data has been compromised | Identify the data that has been compromised if it Is the case | Incident Response Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.4.1.10 | There is external knowledge of this incident | Ensure that the incident has been communicated to third parties and customers to ensure their control of the breach | Incident Response Team |
| 7.4.1.11 | Vulnerability or services have been exploited | Identify the vulnerabilities | Incident Response Team |
| 7.4.1.12 | IT services are impacted | Identify the IT services affected and impacted | Incident Response Team |
| 7.4.1.13 | System(s) have been affected | Identify the systems that have been affected | 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 | Quarantine of affected boxes | It is required to isolate the impacted boxes to contain the spread of the incident  Subtasks: 7.5.1.1 – 7.5.1.19 | Incident Response Team |
| 7.5.2 | Change root password | It is required to update the root password that has been compromised  Subtasks: 7.5.2.1 – 7.5.2.7 | Incident Response Team |
| 7.5.3 | Change credentials of affected accounts | Update credentials of compromised accounts | 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 |
| 7.5.2.1 | Run in Sandbox | Execute the malware in a sandboxed environment to monitor for indicators of compromise and propagation | Incident Response Team  IT Team |
| 7.5.2.2 | Analyse forensics | Analyse incident logs, evidence etc | Incident Response Team  IT Team |
| 7.5.2.3 | Request System Patch | Implement a patch management culture and schedule patch updates regularly | Incident Response Team  IT Team |
| 7.5.2.4 | Block with Antivirus | Use antivirus to stop malware and virus | Incident Response Team |
| 7.5.2.5 | Disable Services | Disable services | IT Team |
| 7.5.2.6 | Restrict Network and Site | Define the network and site to be restricted and action the restriction | Incident Response Team |
| 7.5.2.7 | Adjust Firewall Rules | Update firewall rules to make sure that they are up to date | 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 | Rebuild of systems | Implement the security controls in place to prevent the spread of the virus detected  Sub steps: 7.6.1.1 – 7.6.1.11 | Incident Response Team |
| 7.6.2 | Rollback | Follow rollback steps | Incident Response Team |
| 7.6.3 | Monitoring for a defined period | Monitor systems for an approved period to ensure that the systems are back to normal and detect any new suspicious activity | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1.1 | Request System Patch | Request recommended system patching | Incident Response Team  IT Team |
| 7.6.1.2 | 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 |
| 7.6.1.3 | 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 |
| 7.6.1.4 | 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 |
| 7.6.1.5 | 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 |
| 7.6.1.6 | 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 in-person breach meeting | Incident Response Team  IT Team |
| 7.6.1.7 | 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 |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.6.1.8 | Add, change, or remove affected systems, sites, or networks | Affected systems configuration as required | IT Team |
| 7.6.1.9 | Perform Data Forensics | Perform data forensics | Incident Response Team |
| 7.6.1.11 | Identify lateral movement or compromised user throughout the enterprise | Follow the spreading of the attack to identify the compromised user across the whole organisation | Incident Response Team |
| 7.6.1.1 | Request System Patch | Request recommended system patching | Incident Response Team  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 | Recover system | Rebuild the machine using a trusted source for download Sub steps: 7.7.1.1 – 7.7.1.5 | IT Team |
| 7.7.2 | Incident remediation | Ensure the education of staff on this type of incident to avoid repetition and quick reaction if there is the same incident in the future | Incident Response Team |
| 7.7.3 | 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 | Rebuild | Restore device to factory state and apply organisation changes to restore services. | Incident Response Team  IT Team |
| 7.7.1.3 | Remove Temporary Containment | Remove any temporary containment steps such as firewall rules or configuration changes | IT Support |
| 7.7.1.4 | Data Restore | Restore the data | Incident Response Team  IT Support |
| 7.7.1.5 | Cloud Synchronisation | Ensure to programme regular synchronisation | Incident Response Team  IT Support |

## Post-Incident

Because the handling of Root Access incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Root Access 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 is 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 by embedding 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

BC: Business Continuity

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CTO: Chief Technology Officer

DDOS: Distributed Denial Of Service (attack)

DOS: Denial Of Service (attack)

DR: Disaster Recovery

GRC: Governance Risk & Compliance

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IR Team: Incident Response Team

IRP: Incident Response Plan

ISP: Internet Source Provider

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

Procedure: A document written to support a specific process

Process: A series of actions or steps taken to achieve a particular 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)