

DDoS Playbook

**Authorised by** **:**

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

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

# Table of Contents

[1. Table of Contents 2](#_Toc210207166)

[2. Document Control 3](#_Toc210207167)

[2.1 Document Revision 3](#_Toc210207168)

[3. Assumptions & Disclaimer 4](#_Toc210207169)

[3.1 Assumptions 4](#_Toc210207170)

[3.2 Disclaimer 4](#_Toc210207171)

[4. Background 5](#_Toc210207172)

[5. Objectives 8](#_Toc210207173)

[5.1 Proactive Response 8](#_Toc210207174)

[5.2 Quick Containment 8](#_Toc210207175)

[5.3 Effective remediation 8](#_Toc210207176)

[6. Readiness 9](#_Toc210207177)

[6.1 General Readiness 9](#_Toc210207178)

[6.2 Prepare Phase Readiness 9](#_Toc210207179)

[6.3 Detect Phase Readiness 10](#_Toc210207180)

[6.4 Analyse Phase Readiness 10](#_Toc210207181)

[6.5 Contain Phase Readiness 10](#_Toc210207182)

[6.6 Eradicate Phase Readiness 10](#_Toc210207183)

[6.7 Recover Phase Readiness 11](#_Toc210207184)

[6.8 Post-Incident Handling Phase Readiness 11](#_Toc210207185)

[7. NIST Incident Handling Categories 12](#_Toc210207186)

[7.1 NIST Framework Incident Response Life Cycle 12](#_Toc210207187)

[7.2 Prepare 14](#_Toc210207188)

[7.3 Detect 16](#_Toc210207189)

[7.4 Analyse 19](#_Toc210207190)

[7.5 Contain 23](#_Toc210207191)

[7.6 Eradicate 27](#_Toc210207192)

[7.7 Recover 31](#_Toc210207193)

[7.8 Post-Incident 33](#_Toc210207194)

[8. Glossary 37](#_Toc210207195)

# 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

A Denial of Service (DoS) attack occurs when a service is degraded or stopped due to intentional unavailability of resources, intentional cause of system error(s), or other attempts to reduce the availability of a system.

A Distributed Denial of Service (DDoS) attack traditionally occurs when multiple compromised systems, which are often infected with a Trojan, are used to target a single system or network with the intent to overwhelm a target with a high volume of network traffic, system requests or attempts to exploit a vulnerability.

The common DoS and DDoS attacks are:

* Application layer attacks: this type of attack is to crash the web server. It can be measured by requests per second.
* Protocol attacks: this attack aims to consume server resources, and it can be measured in packets per second.
* Volume-based attacks: this type of attack is to saturate the site bandwidth. Its impact can be measured in bits per second.

Below are some samples of DDoS attacks, for more details, check the organisation's knowledge base and/or online:

* ICMP (ping) flood
* UDP flood
* SYN flood
* Ping of death
* NTP amplification
* HTTP flood

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 DDoS incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major DDoS 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 current playbook (DDoS). 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 if there is a regulation impact for degradation of service | Identify the list of regulations that have been broken as a result of the DDoS incident | Incident Response Team  Governance and Compliance Team (GRC) |
| 7.2.3 | Determine business & technical impacts due to Denial of Service | Define the organisation’s business and technical impact as a result of the DDoS incident | Incident Response Team |
| 7.2.4 | Conduct baseline activity & gather relevant information | Perform the defined steps to collect meaningful data | 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 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, and 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 |
| 7.3.3 | Categorise Incident | Define the category of the incident or order to define its priority and the escalation level | Incident Response Team |
| 7.3.4 | Traffic Analysis | Check the network traffic to identify any unusual activity | Incident Response Team |
| 7.3.5 | Gather telemetry data | Collection of the telemetry data required for the analysis | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Detection of unknown or unidentified packets from unknown senders | Identify packets that are not known and identify packets that are sent by anonymous or unknown senders | IT Team (Network Team)  Incident Response Team |
| 7.3.1.2 | Peaked amount of inbound data | Check the amount of inbound data to identify the period of peaks | Incident Response Team  IT Team |
| 7.3.1.3 | Unknown or unexpected incoming Internet traffic | Look for internet traffic and categorise it to identify unknown or unexpected traffic | Incident Response Team |
| 7.3.1.4 | Notification from outside organisations | Identify and list notifications coming from outside the organisation | Incident Response Team  IT Team |
| 7.3.1.5 | Alerting from firewall and intrusion detection systems | Monitor firewalls and IDS systems used by the organisation and alert required a team if a suspicious event is noticed | Incident Response Team  IT Team |
| 7.3.2.1 | Custom Indicators | Indicators of a threat or security incident that are predefined by an organisation according to the previous threats identified | 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) |
| 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 – 7.4.1.8 | Risk Management Team (GRC) |
| 7.4.2 | Custom | Define custom risk factor  Sub steps: 7.4.2.1 | Risk Team |
| 7.4.3 | Determine capacity & limitations | Choose the patch method to apply. E.g., Deploy vendor-supplied update or change of configuration to close the vulnerability | Incident Response Team  IT Support team  IT Team |
| 7.4.4 | Profile attack traffic | Collect the logs with a focus on the timeline of the incident recorded to identify any suspicious activity | Incident Response Team  IT Team  Support Team |
| 7.4.5 | Analyse device data | Collect all the evidence of the incident for investigation and post-incident learning purposes | Incident Response Team  IT Team |
| 7.4.6 | Define the type of denial of services attack | Capture data to gather key information linked to the incident using data capture tools | Incident Response Team  IT Team  Support Team |
| 7.4.7 | Re-assess business and technical impact | Analysis of the incident by analysing the log collection files, the data capture and all the evidence collected as a result of this incident | Incident Response Team |
| - | False-positive or Accepted risk? | Decision box | Incident Response Team |
| 7.4.8 | Move to the post-incident phase | If the incident is a false positive or if the risk is accepted, skip the contain, eradicate, and recover phase and move to the post-incident phase. | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.1.1 | Products, goods, or services are affected by this attack | Define the level of risk for this situation, the mitigation methods, and the level of escalation and communication of the incident | Risk Team  Incident Response Team  The leadership team (C level) |
| 7.4.1.2 | Customers are affected by this incident | Define the level of risk for this situation and the mitigation methods and level of escalation and communication of the incident to the relevant stakeholders | Legal Team  Communication Team  The leadership team (C level) |
| 7.4.1.3 | Public or personnel safety affected | Define the level of risk for this situation and the mitigation methods | Legal Team  Governance and Compliance Team (GRC) |
| 7.4.1.4 | This is being launched by known entities | Define entities involved in the incident | Incident Response Team |
| 7.4.1.5 | Ability to control, record, measure, and track any significant amounts of inventory, products, cash, or revenue lost | Monitor the systems and teams that can control, record, measure, and track any significant amounts of inventory, products, cash, or revenue loss | Incident Response Team  IT Team |
| 7.4.1.6 | Identify worst-case business impact if unable to mitigate this attack | Define simulation that will cover worst and best-case scenarios and evaluate the impact and therefore the mitigation method to reduce the risk of an attack | Risk Team  Incident Response Team |
| 7.4.1.7 | There is external knowledge of this incident | Identify the external channel aware of the incident occurring | Incident Response Team  Legal Team  Communication/PR Team |
| 7.4.1.8 | There is internal knowledge of this incident | Define the communication plan in case of an incident and define the communication channels and the audience | Communication Team  Change management team |
| 7.4.2.1 | Custom Factors | Identify the risk management process in specific scenarios unique to the organisation | Risk 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 or applications that have suffered an impact, outage, or degradation of services  Identify the network flow(s) or data flow(s) from the point of impact  Identify critical systems that are at risk from DoS/DDoS  Identify the type of packets being utilised or attack pattern  Identify critical choke points  Identify the source IP range(s) and examine if their network can be blackholed  Identify additional traffic routing  Identify the tools used to detect the attack  Sub steps: 7.5.1.1 – 7.5.1.5 | Incident Response Team  IT Team |
| 7.5.2 | Define DDoS type | Define and categorise the DDoS incident and check if it falls under the 4 DDoS types defined below  Sub steps: 7.5.2.1 – 7.5.2.4 | Incident Response Team  IT 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 impacted  Consider host-based IDS | Incident Response Team  IT Team |
| 7.5.1.2 | SIEM | Check the SIEM for any correlated events, early detection events, or other indicators of compromise  Consider the creation of a new alert for earlier detection | Incident Response Team |
| 7.5.1.3 | IDS | Check IDS for any correlated events, early detection events, or other indicators of compromise  Consider the creation of a new signature to detect or block the attack | Incident Response Team |
| 7.5.1.4 | Firewall | Check firewall logs for any correlated events, early detection events, or other indicators of compromise  Consider implementing firewall rules to block, allow, or re-route traffic | Incident Response Team  IT Team |
| 7.5.1.5 | Network Monitoring Tools | Check tools for any increase in downstream impact or changes  Consider the creation of a new alert for earlier detection | Incident Response Team  IT Team  Support Team |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.5.2.1 | Bandwidth exhaustion | Consider: firewall rules, geographical IP blocking, escalation to DDoS protection provider, IPS changes, Blackhole IP addresses and routing change, disaster recovery | Incident Response Team |
| 7.5.2.2 | Resource exhaustion | Consider: firewall rules at the host level, disabling impacted function or service, throttling, increased resources | Incident Response Team |
| 7.5.2.3 | Vulnerability related to denial of service | Consider: firewall rules at the host level, disabling impacted function or service, throttling, understanding, and patching the vulnerability | Incident Response Team |
| 7.5.2.4 | Identity management (malicious intent) | Consider: identifying how the accounts were locked, throttling the number of requests coming from one particular IP source, firewall rules, analysing logs to determine the source of the attack | Incident Response Team |

## Eradicate

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

A diagram of communication

AI-generated content may be incorrect.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1 | Confirm reduced impact | Check that the business and technical impacts on the service(s) have reduced to acceptable levels  Sub steps: 7.6.1.1 – 7.6.1.3 | Incident Response Team |
| 7.6.2 | Communications | Check if the communication channels have been impacted then communicate the identification of the incident using the right channels of communication and targeting the right audience (escalation point)  Sub steps: 7.6.2.1 – 7.6.2.6 | Incident Response Team  IT Team |
| 7.6.3 | Monitoring for a defined period on the attack factors | It is recommended to establish a monitoring period to ensure the service or function returns to normal operation  Consider heightened awareness for a suitable amount of time  Sub steps: 7.6.3.1 – 7.6.3.4 | 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 | Check for vulnerabilities in other systems  Consider deploying the patch to other systems in line with business and IT risk levels | Incident Response Team  IT Team |
| 7.6.1.2 | Request network segment or other configuration change | Request configuration update to patch the systems | Incident Response Team  IT Team  Dev Team |
| 7.6.1.3 | Add, change, or remove the affected system, site, or network | Update network as required by updating system or site network status | Incident Response Team  SOC Team  IT Team |
| 7.6.2.1 | 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 |
| 7.6.2.2 | 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 |
| 7.6.2.3 | 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 |
| 7.6.2.4 | 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 |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.6.2.5 | 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 through an in-person meeting | Incident Response Team  IT Team |
| 7.6.2.6 | 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 |
| 7.6.3.1 | Identify any alternate course for business operations that will be affected | List Business Ops that are affected | Incident Response Team |
| 7.6.3.2 | Create a whitelist of Source IPs & services that must be allowed into the network | List the services (IP whitelisting) that are required to be allowed to ensure BAU | Incident Response Team  IT Team |
| 7.6.3.3 | Coordinate with Business Continuity on rolling over services to any alternate sites | Coordination and communication with the BC team to ensure the rollover if required | Incident Response Team  IT Team |
| 7.6.3.4 | Coordinate with ISP (Internet Service Provider) to determine the best courses of action | Coordination and communication with ISP to define the steps to follow | Incident Response 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 | Consider rollback of containment steps | Recover systems that have been touched by the incident by making sure to have a backup process defined, a disaster recovery process and a backup policy and consider a rollback of systems modified during the containment phase  Sub steps: 7.7.1.1 – 7.7.1.3 | Incident Response Team |
| 7.7.2 | 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 | Perform a reimage to replace corrupted files and keep data intact | Incident Response Team |
| 7.7.1.2 | IDS/IPS, SIEM & firewall updates | Update the organisation’s monitoring and controls systems and keep these up to date | Incident Response Team |
| 7.7.1.3 | Determine alternate network ingress and egress solutions if malware-related DoS | Define network alternatives in case of malware-related DoS | Incident Response Team |

## Post-Incident

Because the handling of DDoS incidents can be extremely expensive, it is particularly important

for organisations to conduct a robust assessment of lessons learned after major DDoS 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 – 7.8.2.3 | 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 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 incident | Incident Response Team  IT Team |
| 7.8.2.1 | 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) |
| 7.8.2.2 | Process updates | Update processes to ensure the inclusion of the new steps identified as missing to ensure an improved security posture | All organisation |
| 7.8.2.3 | 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  The 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)