

# IoT-based Brute-force Incident Response Playbook

<b>Title</b>	IoT-based Brute-force Security Incident Response Playbook
<b>Version</b>	V1.0
<b>Date issued</b>	DD-MM-YYYY
<b>Status</b>	In progress
<b>Document owner</b>	abc
<b>Creator name</b>	xyz
<b>Creator organization name</b>	ECC
<b>Subject category</b>	IoT Brute-force Attack
<b>Access constraints</b>	NA
<b>Review cycle</b>	Annually

## 1. Introduction

### 1.1 Incident Overview

The use of IoT devices has rapidly increased in the past decade owing to their multiple benefits for business operations. With the deployment of various IoT devices across organizations, it has become challenging for administrators to apply adequate security controls in each device and track their efficiency; in some cases, the default passwords of some devices are not even changed. This has created an opportunity for attackers to exploit potential vulnerabilities in the IoT network to disrupt business services, gain access to the organizational network, steal critical data, inject malware, and perform other malicious activities.

Assume that an administrator of organization X has reported an incident to the service desk based on an alert from a security solution. The security tool triggered an alert after it detected multiple login attempts on specific IoT devices in the organization. Now, the service desk must verify the report and raise appropriate ticket to assign the IH&R team for handling the incident.

### 1.2 Purpose of Playbook

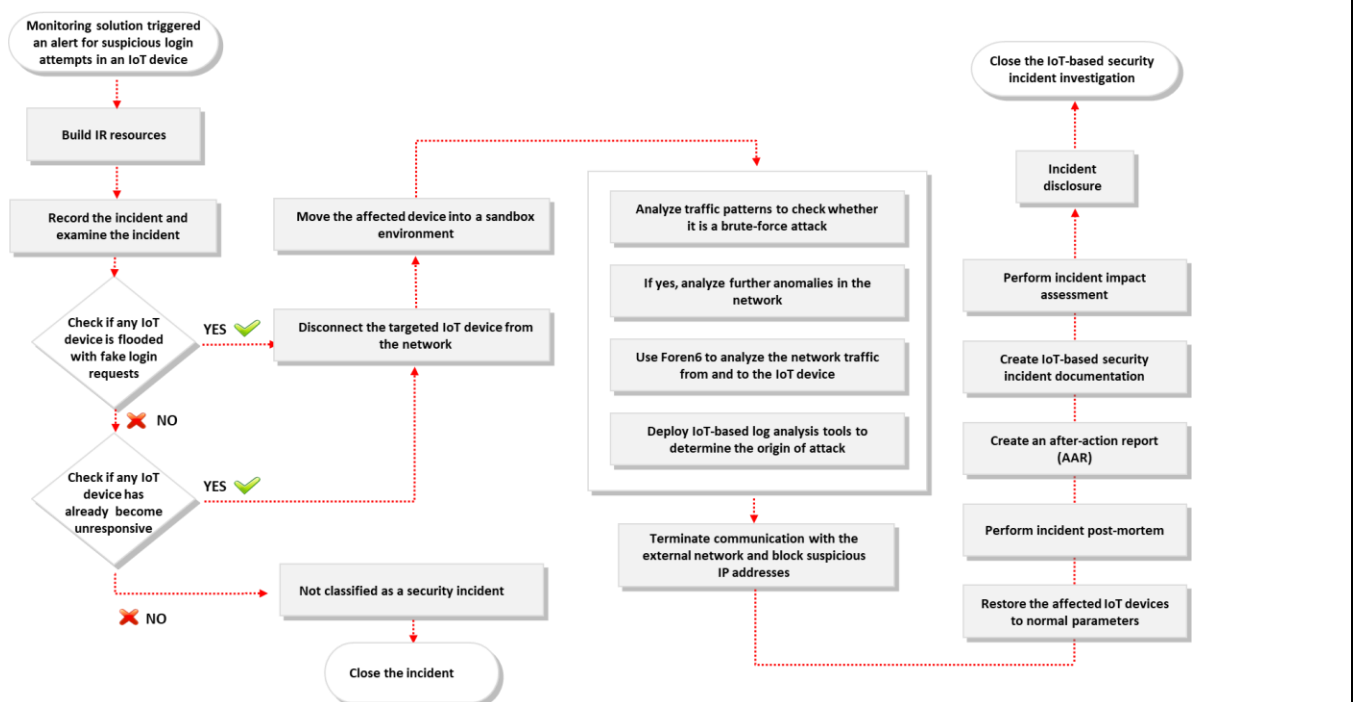
The main purpose of this playbook is to assist the IH&R team in the event of a security incident in the IoT environment of an organization. This playbook includes step-wise guidance and procedures for the IH&R teams to implement mitigative actions against brute-force attacks on IoT networks.

### 1.3 Scope

This playbook is developed for the use of incident responders to handle security incidents in the IoT environment of an organization. Additionally, this document must be used alongside the incident response plan of the organization. The scope of this document is listed below (not limited to):

- Determine the business impact due to the incident
- Determine the type of brute-force attack (for example, simple brute-force using an automated tool, dictionary attack, credential stuffing, etc.)
- Understand the motives behind the attack
- Determine the type of brute-forcing tool used by the attacker (for example, Aircrack-ng, John the Ripper, Rainbow Crack, etc.)
- Implement the incident response plan under the supervision of higher authorities of the organization
- Identify any related activities by checking the following:
  - Sudden surge in incoming traffic
  - Suspicious login attempts
  - Frequent connection loss
  - Multiple login requests within a specific period
  - Abnormal behavior of the IoT network
  - Frequent error reports
  - IoT device taking more time than usual to transfer data
  - Device crash while processing requests
  - Disabled security controls
  - Detect, contain, analyze, and eradicate the incident
  - Recover from the incident

## 1.4 Workflow Diagram



Workflow diagram of IoT-based brute-force security incident response

## 2. Preparation

### 2.1 Objectives

The main objective of the preparation phase is to prepare the organization to handle and respond to brute-force attempts in the IoT network. Another objective of this phase is to define the roles of personnel and their communication medium. This phase can also help in preparing organizational devices, network, and data for similar incident in future.

### 2.2 Activities Involved

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Prepare for incident response:
  - Validate the ticket/issue raised for the incident
  - Check the internal alarms/metrics indicating the issue based on the raised tickets
  - Maintain the contact information (such as vendor name, contact number, and product serial number) of IoT device vendors to promptly contact in the event of an attack
  - Deploy network sniffing tools such as Foren6 to identify IoT-related abnormal activities in the organizational network

- Define and assign roles to different IH&R team members
- Enable the concerned IH&R teams to access logs or other evidence to analyze the incident
- Accumulate industry best practices and guidelines before initiating the response process
- Deploy IoT incident management tools such as PagerDuty and OnPage to handle and resolve IoT-based security incidents
- Deploy IoT monitoring tools such as Domotz and Datadog IoT Monitoring to monitor and analyze IoT devices and infrastructure
- Create an outlook of the IoT network to be investigated
- Deploy IoT network traffic analysis tools such as Wireshark and IoT Inspector to analyze the network traffic of Internet-connected devices
- Perform continuous risk assessments and thoroughly review the possible risks associated with IoT devices
- Create an effective dashboard layout such that responders can quickly pinpoint any changes or issues emerging during the response process
- Incorporate threat intelligence into the existing security capabilities to feed them with the latest risks, vulnerabilities, and common patterns
- Implement network segmentation to separate the IT and IoT networks
- Deploy multi-layered security controls to protect IoT assets connected to the network
- Ensure that all IoT devices throughout the organization are provisioned and authenticated
- Create an inventory list of IoT devices in the organizational infrastructure to identify shadow IT devices that can become a threat
- Define business continuity plans and understand IoT network architectural designs
- Analyze the threat intelligence capabilities of the organization to obtain information related to the latest risks, vulnerabilities, and common patterns
- Provide access to the required documentation such as incident response plan and network architecture for responding to IoT-based security incidents. Links to important documents are given below:
  - Reference 1:
  - Reference 2:
  - Reference 3:

- Establish out-of-band communication channels between the IH&R team and customers/stakeholders
- Collaborate with the disaster recovery (DR) and business continuity planning (BCP) team for additional support
- Prepare a whitelist of protocols and IP addresses of systems to be accessed during the incident handling process
- Inform the employees:
  - Conduct regular training and awareness programs regarding the safe usage of IoT resources
  - Ensure that the IH&R team is aware of the latest IoT technologies and tools to handle IoT-based incidents
  - Create a proper format and mechanism for reporting and registering complaints
  - Provide proper contact information of personnel who can be contacted by users in case of a brute-force attack on IoT devices

### 2.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response ○ Create incident response processes and procedures ○ Define roles and responsibilities ○ Review recent incident reports ○ Incorporate threat intelligence ○ Maintain network architecture and data flow diagrams ○ Define IoT-based threat indicators and incorporate alerting solutions	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message

	Business Continuity Lead	Email, Phone, Text Message
Inform employees ○ Conduct training and awareness on how to identify and report IoT-based security incidents	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

## 2.4 Additional Information (if any)

**Note:** Refer to the following templates and checklists to fill the necessary details:

- a. Preparation to IoT-based Security Incidents Checklist.docx
- b. IH&R Plan Template.docx
- c. IH&R Plan Checklist.docx
- d. IH&R Policy and Procedure Template.docx

## 3. Detection and Notification

### 3.1 Objectives

The main objective of the detection phase is to perform initial investigation on the reported incident and determine whether it is an IoT-based threat. Additionally, the appropriate IH&R team members are assigned to handle the IoT-based security incident in this phase.

### 3.2 Activities Involved

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Detect and report the IoT-based security incident:
  - Check for login attempts with multiple usernames from the same IP address
  - Check for multiple login attempts within a short period
  - Check for multiple failed login attempts
  - Check if any reference URL was pulled from an employee's email or IRC
  - Check if any unauthorized modifications were applied to IoT devices
  - Check if any unknown communication paths were established to transfer data
  - Check if any IoT device became unresponsive

- Check if any IoT devices are consuming more Internet bandwidth to transfer data
- Check for unusual outbound DNS queries from IoT devices
- Check if any IoT device intercepted the traffic intended for another IoT device within the network
- Check for rogue devices and rogue access points across the organization
- Check if any port performed activities beyond its scope
- Check if any security monitoring solution was disabled
- Gather the following information from the initial investigation:
  - Type of IoT-based attack
  - Location of IoT devices affected
  - Who, how, and when was the incident reported
  - Users/employees/business operations/services affected by the incident
  - Reason behind the incident
  - Number of IoT devices affected by the incident
  - Amount of data exposed
  - Whether the attacker managed to gain access to the target IoT device(s)

### 3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting the incident <ul style="list-style-type: none"> <li>○ Monitor IoT security tools</li> <li>○ Respond to manual and automated alerts</li> <li>○ Escalate the incident via the ticketing system (if not escalated)</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initial investigation	Information Security Manager	Email, Phone, Text Message

<ul style="list-style-type: none"> <li>○ Collect initial evidence data</li> <li>○ Classify and prioritize the incident</li> </ul>	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Head of IT	Email, Phone, Text Message
Notification of the incident <ul style="list-style-type: none"> <li>○ Follow the defined IH&amp;R plan to notify the incident</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

### 3.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- e. IoT-based Security Incidents Detection and Analysis Template.docx
- f. Incident Notification Form-New.docx
- g. Incident Information Collection Form.docx
- h. Checklist for Preliminary Interviews.docx
- i. Incident Identification and Validation Template.docx
- j. Incident Priority Template.docx
- k. Incident Communication Logs Template.docx
- l. Incident Information Collection Form.docx
- m. Evidence Collection Template.docx

## 4. Containment

### 4.1 Objectives

The main objective of the containment phase is to minimize the damage caused by the IoT-based security incident and prevent further damage.



## 4.2 Containment Steps/Activities

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Activities to contain the IoT-based security incident are listed below:
  - Disconnect the infected IoT devices from the organizational network and isolate them for further investigation
  - Block unauthorized access to IoT devices
  - Disable IoT devices configured with remote access features
  - Block the origin IP address of the attack traffic
  - Disable ports and services not in use
  - Reset the password of the Wi-Fi network to disconnect suspicious wireless IoT devices from the organizational network
  - Use VLANs to separate specific sub-networks of compromised IoT devices
  - Disable features such as filesharing and universal plug and play on IoT devices
  - Implement IoT firewall to block unusual traffic from external networks
  - Block unnecessary communication of IoT devices with other networked devices
  - Block unauthorized data access, storage, and transmission from IoT ecosystems
  - Enforce the highest possible encryption rates (such as 256-bit encryption) for data storage
  - Segregate compromised IoT devices safely without exposure to data theft or business disruption
  - Move the affected devices into a sandbox environment without shutting or rebooting them
  - Block any outbound requests or commands to establish connections with IoT devices
  - Restrict the IP address range of IoT devices to the required connections and gateways
  - Identify and block vulnerable IoT network services from the active network
  - Disable auto-connections to open Wi-Fi networks
- Communicate the progress:
  - Regularly inform the respective stakeholders and authorities about the status of the incident handling process

### 4.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

### 4.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- n. Containment of IoT-based Security Incidents Checklist.docx
- o. Incident Containment Checklist.docx
- p. Incident Containment Template.docx

## 5. Analysis

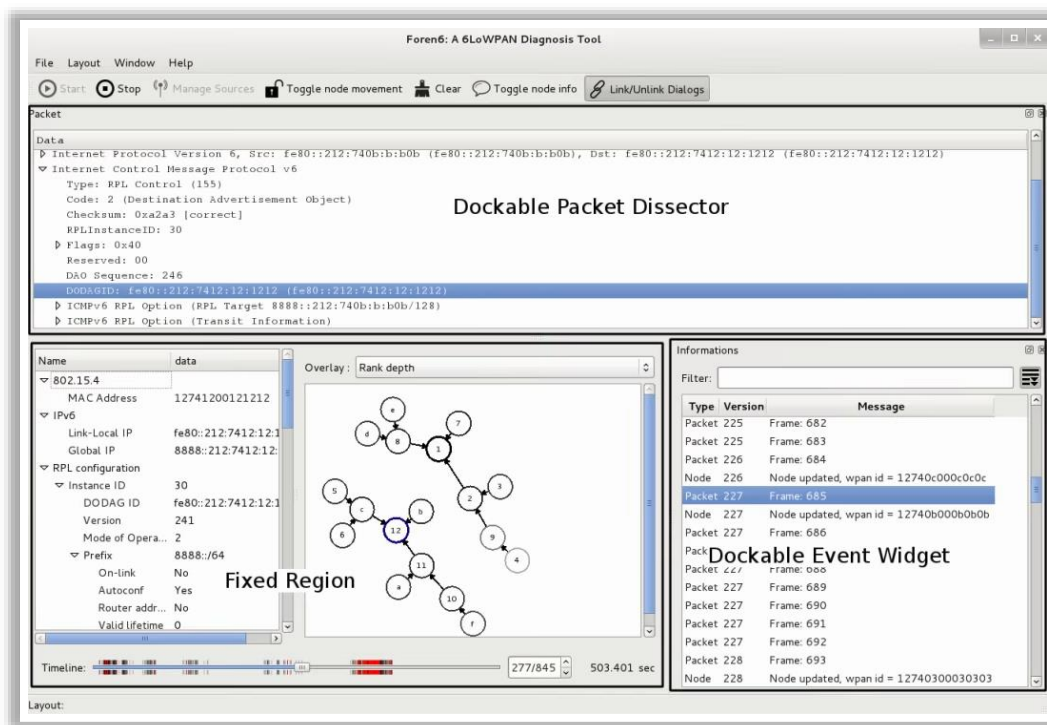
### 5.1 Objectives

The main objective of this phase is to analyze the security incident and its scope. Another objective of this phase is to detect and report the impact of the IoT-based security incident to establish forensic investigation requirements and develop an effective mitigation strategy based on analysis results.

### 5.2 Activities Involved

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Use tools such as Microsoft Sentinel to detect and respond to IoT-based security incidents
- Use tools such as Nmap and Masscan for IoT device discovery and analysis
- Perform network traffic analysis by capturing the network traffic from and to IoT devices using tools such as Foren6



Screenshot of Foren6 showing different result panes

- Analyze the firewall and other security solution logs
- Use tools such as Datadog and Sematext Logs to analyze IoT-based logs
- Use IoT Analytics and Wireshark to capture and analyze real-time traffic to the IoT network
- Analyze common adversary TTPs using the MITRE ATT&CK framework

### 5.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Analyze the scope of the IoT-based security incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the IoT-based security incident and	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

report potentially compromised data	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

#### 5.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- q. IoT-based Security Incident Handling Toolkit.docx
- r. IoT-based Security Incidents Detection and Analysis Template.docx
- s. Evidence Gathering and Forensic Analysis Form.docx

### 6. Eradication

#### 6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate the IoT-based security incident and prevent recurrence in future.

#### 6.2 Eradication Steps/Activities

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Perform the following activities to eradicate IoT-based threat incidents:
  - Perform factory reset on the affected IoT devices and reconfigure their device settings
  - Use the “Lock Out” feature to lock accounts for excessive invalid login attempts
  - Disable the “guest” and “demo” user accounts if enabled
  - Implement a zero-trust network
  - Enforce MFA to access critical IoT devices
  - Change the default or existing passwords and provide strong usernames and passwords to IoT devices
  - Update and patch the software of all compromised devices
  - Use password manager to track login activities
  - Use CAPTCHA and account lockout policy methods to avoid brute-force attacks
  - Enforce MFA in IoT devices to confirm user identity while accessing an IoT device

- Enforce the blockchain technology for IoT defense
- Limit the number of login attempts
- Implement a dedicated IoT manager on the IoT-based network for continuous monitoring, managing alerts, updating, and reporting incidents
- Install intrusion detection and intrusion prevention systems to defend against IoT-based attacks
- Implement end-to-end encryption and use public key infrastructure (PKI)
- Disable telnet (port 23)
- Disable the UPnP port on routers
- Deny access privileges in IoT devices for high-risk features such as location, camera, and microphone
- Limit unnecessary communications between IoT devices and the Internet
- Eliminate unusual data access privileges for IoT devices to prevent the risk of data exposure
- Prevent the disclosure of IP addresses by disabling WebRTC in the browser
- Map the network activity of IoT devices to completely eradicate the malware from the network, if required
- Verify the SSL certificates of websites that interacted with the IoT device
- Delete the registry file(s) of malware from the device firmware, if found
- Monitor the traffic on port 48101 because infected devices attempt to spread malicious files via this port
- Detect and remove network backdoors such as Telnet from the IoT device firmware
- Close unsecured and unused ports after performing port scan on IoT devices
- Update IoT devices with the latest application software and firmware to patch the identified vulnerabilities
- Implement automation to continuously discover new IoT devices connecting to the network; then, apply appropriate security controls
- Use Connectivity Management Platforms (CMPs) such as FirstPoint Secure CMP to avoid IoT connectivity mismanagement
- Monitor the booting source to prevent attackers from tampering with or glitching the hardware unit
- Enable a default entry-level logging mechanism
- Implement the Root-on-Trust mechanism
- Secure legacy units enabling modern gateway security features

### 6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan ○ Perform technical and business analyses and create a prioritized eradication plan ○ Establish a communication strategy based on the eradication plan	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Eradication activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

### 6.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- t. Eradication of IoT-based Security Incidents Checklist.docx
- u. Incident Eradication Template.docx
- v. Incident Eradication Checklist.docx

## 7. Recovery

### 7.1 Objectives

The main objective of this phase is to recover organizational resources from the impact of the IoT-based security incident and maintain business continuity.

### 7.2 Recovery Steps/Activities

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Activities to recover from the IoT-based security incident:
  - Change the privacy and security settings of IoT devices after recovering from the incident

- Install the latest patches to update outdated software and firmware in IoT devices
- Restore the affected business-critical IoT devices to normal parameters
- Restore devices based on business impact analysis
- Implement a new set of rules to reconfigure firewall solutions after recovery
- Enforce automatic failure recovery for IoT-edge applications
- Replace outdated IoT assets with modern devices configured with end-to-end security
- Follow proven data recovery methods and compliance guidelines to restore lost data
- Use remote and cloud-based replicas of IoT resources for immediate restoration
- Test the recovered IoT devices with different user scenarios in a recovered environment
- Continuously monitor the operations of IoT devices for abnormal behavior even after restoring them to the normal condition
- Strengthen the perimeter security by changing access control rules after restoring devices
- Use device failure recovery tools such as EmSPARK and InnoOSR
- Implement two-way authentication using cryptographic algorithms that employ symmetric keys using SHA with HMAC and asymmetric keys using ECDSA
- Safely secure the keys used for authenticating each device associated with a unique device ID crafted by the corresponding cloud service
- Enable VPN services while recovering backup data from the secondary zone
- Examine the entry point of the incident and enforce strict access controls on it after recovery
- File a complaint with the cybercrime department
- Perform complete vulnerability analysis and patch the identified vulnerabilities

### 7.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

### 7.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- w. Recovery from IoT-based Security Incidents Checklist.docx
- x. Incident Recovery Procedure Template.docx
- y. Incident Recovery Checklist.docx

## 8. Post-incident Activities

### 8.1 Objectives

The main objective of this phase is to create the necessary IoT-based security incident reports such as incident post-mortem, after-action report (AAR), incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close the investigation and disclose its details to the respective stakeholders through proper channels.

### 8.2 Activities

*[Activities may differ according to organizational policies, but they are not limited to the following.]*

- Perform IoT-based security incident post-mortem or incident review to understand the root causes
- Create an AAR that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar IoT-based security incidents
- Conduct a lessons learned meeting to document the details of the incident; moreover, ensure that the following questions are answered in this meeting:
  - When and who detected the incident?
  - What happened exactly?
  - What caused the IoT-based security incident?
  - To whom was the IoT-based security incident reported?



- Was the organization adequately prepared to handle the IoT-based security incident?
- How was the IoT-based security incident contained?
- What challenges were encountered during the response process?
- Which tools were effective during the response process?
- How were the impacted accounts sanitized?
- What procedures were followed during recovery?
- Were the documented procedures followed by the response team?
- How well did the incident response team and management perform in resolving the IoT-based security incident?
- How should the incident response team and management respond to mitigate similar IoT-based security incidents in future?
- Were there any gaps in communication during incident response?
- Was the right amount of information shared with the right personnel?
- What are the tools and resources required to detect, analyze, and prevent similar IoT-based security incidents?
- Create clean and concise IoT-based security incident documentation in a standard format and get it reviewed by an editor
- Create an incident impact assessment report to determine all types of losses caused by the IoT-based security incident; this report must address the following (if applicable):
  - Financial losses caused by the incident
  - Legal costs for investigating the case, lawyer's fees, etc.
  - Costs pertaining to analyzing the security incident as well as recovering and installing software and hardware
  - Implementation costs
  - Costs related to the damage of goodwill and loss of customer trust and reputation
- Officially close the IoT-based security incident investigation by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders through proper channels after consulting with the legal department of the organization

- Document the acquired results and preserve the evidence for further legal actions; if any lapses were observed in the implemented incident response plan, update the document according to latest incident handling procedures
- Conduct technical and operational training on how to handle corporate data
- Review the entire network after recovery and document areas of improvements to be managed by administrators (regularly changing passwords, updating software, etc.)
- Validate the lesson learned documentation with the help of subject matter experts (SMEs)
- Incorporate some best practices against IoT-based security incidents

### 8.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Create incident post-mortem report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create AAR	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Conduct lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Close the investigation officially	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Management	Email, Phone, Text Message

Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	IT Manager/ Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	HR Manager	Email, Phone, Text Message
	Media	Email, Phone, Text Message
	Vendors	Email, Phone, Text Message
	Customers & General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

#### 8.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- z. Incident Postmortem Template.docx
- aa. After Action Report Form Template.docx
- bb. Incident Documentation Template.docx
- cc. Incident Impact Assessment Report Template.docx
- dd. Incident Closure Letter.docx
- ee. Incident Disclosure Form.docx
- ff. Incident Reporting Template.docx

#### 9. Appendix (if any)