

# AWS-based DDoS Incident Response Playbook

<b>Title</b>	AWS-based DDoS Incident Response Playbook
<b>Version</b>	V1
<b>Date issued</b>	DD-MM-YYYY
<b>Status</b>	In progress
<b>Document owner</b>	Full Name
<b>Creator name</b>	Full Name
<b>Creator organization name</b>	<Organization Name>
<b>Subject category</b>	AWS DDoS Incident Response
<b>Access constraints</b>	NA
<b>Review cycle</b>	Annually

## 1. Introduction

### 1.1. Incident Overview

Attackers often use sophisticated techniques/technologies to compromise or disrupt targeted cloud networks. With greater exposure to the Internet, cloud services have become the easiest target for attackers. Therefore, the incident handling and response (IH&R) team must establish appropriate plans and procedures to hunt down such cloud threats before they disrupt the entire cloud environment.

Assume that the AWS platform opted by an organization encountered an unexpected DDoS incident that made its services unavailable to some customers. This playbook provides different activities related to various stages of incident response for better implementation of incident response procedures and handling of DDoS incidents in AWS environments.

### 1.2 Purpose of Playbook

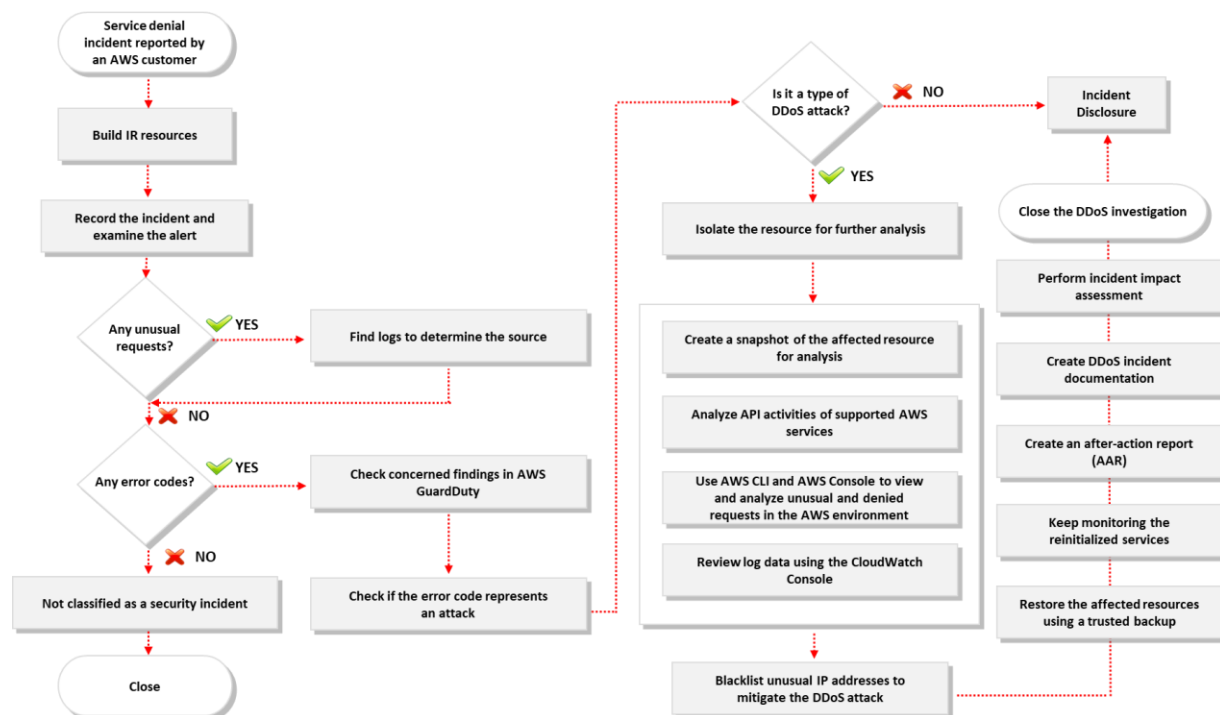
The main purpose of this playbook is to provide guidance to detect and respond to DDoS incidents in AWS environments. This playbook includes step-by-step procedures that can help the IH&R team to implement mitigative actions against DDoS attacks on AWS services.

### 1.3 Scope

This playbook is developed for IH&R teams to enable them to handle and respond to DDoS incidents in AWS environments. Additionally, this document must be used alongside the incident response plan of an organization. The scope of this document is as follows (not limited to):

- Determine the total number of resources affected by a DDoS incident
- Understand and document various actions associated with a DDoS attack; for example:
  - User 1: Unable to access AWS resources
  - User 2: High bandwidth consumption
- Identify any related activities by checking the following:
  - Sudden increase in traffic owing to an unusual event
  - Many requests within a short period
  - Incessant requests from unknown IP addresses
  - Unknown URLs in the request section
  - Unusual queries that are incompatible with the application
  - Any non-deliverable services
- Analyze suspicious traffic
- Recover from incidents

## 1.4 Workflow Diagram



Workflow diagram for AWS-based DDoS incident response

## 2. Preparation

### 2.1 Objectives

The main objective of the preparation phase involves:

- Preparing the organization to respond to AWS-based DDoS incidents
- Defining the roles and communication medium for the entire DDoS incident response process
- Preparing tools and resources required for handling AWS-based DDoS incidents
- Preparing users of their roles and reporting procedures

### 2.2 Activities Involved

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

- Prepare for incident response:
  - Validate the incident ticket/issue raised by customers
  - Check the resources involved in providing AWS services
  - Prepare, review, and practice the incident response procedures in accordance with the incident response plan

- Identify the team's AWS account numbers, IP ranges of virtual private clouds (VPCs), corresponding network diagrams, logs, data locations, and data classifications
- Identify external AWS security APN partners to provide expertise and different insights to improve response capabilities
- Provide access to the required documentation such as incident response plan and network architecture to respond to DDoS incidents. The links of important documents are given below:
  - Reference 1:
  - Reference 2:
  - Reference 3:
- Train cloud security experts in your team or enlist the support of expert partners to monitor your AWS environment during the response process
- Subscribe to a global continuous feed of current and relevant threats, risks, and indicators for threat intelligence
- Utilize machine learning functionalities to identify complex anomalies and unusual behaviors in the AWS environment
- Create AWS IAM roles for incident responders to use during a security incident
- Use a new, purpose-built AWS account so that incident responders can work from a separate secure network
- Configure AWS Systems Manager Agent (SSM Agent) to remotely and securely operate Amazon EC2 instances
- Create a decision tree with other teams and stakeholders to enable them to assist you in the creation and documentation of decisions
- Allow incident responders to access logs or other evidence to analyze and provide the ability to view or copy data
- Utilize Amazon Elastic Block Store (Amazon EBS) snapshots to investigate security incidents
- Utilize AWS Key Management Service (AWS KMS) and Customer Managed Keys (CMKs) to encrypt snapshots.
- Subscribe to CloudWatch Logs to share Amazon VPC flow logs with your centralized security account
- Consider moving data from Amazon S3 to Amazon S3 Glacier using object lifecycle policies to securely store data for long-term usage
- Utilize immutable storage to ensure data integrity at the source

- Launch forensic workstations such as the base Amazon Machine Image (AMI) for analyzing incident artifacts
- Inform customers:
  - Provide a manual with guidelines describing how to deal with service outage events
  - Create a proper format for reporting and registering complaints
  - Provide proper contact information of personnel who can be contacted by users in case of a DDoS incident

### 2.3 Stakeholders Involved/Communication

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

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response	CISO	Email, Phone, Text Message
○ Create incident response processes and procedures	Information Security Manager	Email, Phone, Text Message
○ Define response mechanisms for incident response	IT Manager/Director	Email, Phone, Text Message
○ Define security assertions	Service Desk	Email, Phone, Text Message
○ Incorporate threat intelligence	Service Delivery Manager	Email, Phone, Text Message
○ Subscribe to a continuous feed of current and relevant threats	IH&R Team	Email, Phone, Text Message
○ Prepare related processes required for investigation	Administrators	Email, Phone, Text Message
○ Generate notification alerts for unusual, malicious, or expensive activities	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

Inform customers <ul style="list-style-type: none"><li>○ Provide proper guidelines on how to deal with service outage issues</li></ul>	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager/Director	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:

- Preparation to Handle Cloud Security Incident.docx
- Cloud Security Incident Handling Toolkit.docx
- IH&R Plan Template.docx

## 3. Detection and Notification

### 3.1 Objectives

The main objective of the detection phase is to perform initial investigation on the suspected network and determine whether it is a DDoS attack.

### 3.2 Activities Involved

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

- Detect DDoS attack:
  - Check for internal alarms/metrics indicating the issue based on the raised ticket
  - Check for sudden increase in traffic in the network
  - Check for unusual update requests for any resource
  - Check for major variation in data transferred over HTTP and HTTPS
  - Check for major variation in HTTPCode\_ELB\_4xx\_Count
  - Check for major variation in HTTPCode\_ELB\_2xx\_Count
  - Check for major variation in ActiveConnectionCount
  - Check for major variation in ClientTLSNegotiationErrorCount
  - Check for major variation in RequestCount

- Check for major variation in HTTPCode\_Target\_5XX\_Count
- Check for major variation in TargetResponseTime
- Check for major variation in ELBAuthFailure
- Check for excessive CPU utilization
- Check for unusual disk performance
- Check for excessive memory utilization
- Check for sample findings such as Backdoor:EC2/DenialOfService.Dns, Discovery:S3/AnomalousBehavior, and Backdoor:EC2/C&Cactivity.B in Guard Duty
- Gather information from initial investigation:
  - Find logs related to the incident (for example, web server access logs, load balancer logs, and CloudFront distribution logs)
  - Based on these logs, determine the type of incident (for example, SYN flood, HTTP flood, amplification attacks, or reflection attacks)
  - Note down who, how, and when the incident was reported
  - Make a list of customers affected by the outage
  - Make a list of resources being targeted
  - List the number of resources affected
  - Determine the impact on business operations

### 3.3 Stakeholders Involved/Communication

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

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting incident <ul style="list-style-type: none"><li>○ Monitor security solutions</li><li>○ Respond to both 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 <ul style="list-style-type: none"> <li>○ Collect initial evidence data</li> <li>○ Classify and prioritize the incident</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Head of IT	Email, Phone, Text Message
Notification of 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:

- d. Cloud Security Incident Handling Toolkit.docx
- e. Incident Priority Template.docx
- f. Incident Communication Logs Template.docx
- g. Point-of-Contact Template.docx
- h. Incident Identification and Validation Template.docx



## 4. Containment

### 4.1 Objectives

The main objective of the containment phase is to identify the resources affected by the DDoS attack and isolate them from the network while maintaining business operations.

### 4.2 Containment Steps/Activities

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

- Activities to contain DDoS incident:
  - Isolate the affected resources and implement a sandbox environment to examine them
  - Define a single rule of 0.0.0.0/0 (0-65535) for all inbound and outbound traffic
  - Implement a dedicated “Isolation” security group rule for applications
  - If a single instance is providing services, consider resource autoscaling
  - Develop multiple availability zones to run services after blocking the existing instance
  - Contact the AWS application developer to check whether a new instance can be created from the existing one
  - Use load balancers to distribute the traffic
  - Implement CloudFront distribution beyond the load balancer
  - Keep additional instances behind the load balancers
  - Store the resources in multiple availability zones
  - Deploy firewalls to block abnormal traffic
  - Implement a zero-trust model to identify and block spoofed queries
  - Use AWS Lambda and AWS-provided IP ranges to configure security groups for load balancers
  - Ensure that load balancer security groups are properly configured
- Communicate the progress:
  - Regularly inform the customers and stakeholders about the status of the incident handling process

### 4.3 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:

- i. Containment of Cloud Security Incidents Checklist.docx
- j. Incident Containment Checklist.docx
- k. Incident Containment Template.docx

## 5. Analysis

### 5.1 Objectives

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

### 5.2 Activities Involved

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

- Analyze the scope of DDoS incident:
  - Analyze DDoS condition and impacted resources
  - Create a snapshot of affected resources for analysis
  - Analyze API activities of supported AWS services
  - Use AWS Management Console to view and analyze requests originating from specific IP addresses

- Use AWS CLI and AWS Console to view and analyze unusual and denied requests in the AWS environment
- Analyze Backdoor:EC2/DenialOfService.Dns findings in GuardDuty
- Search and review log data using CloudWatch Console
- Analyze AWS applications through log data
- Set notification alerts for specific API activities for further investigation and troubleshoot the issues
- Use GuardDuty to analyze different findings

### 5.3 Stakeholders Involved

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

Activities	Stakeholders Involved	Communication Mode/Channel
Analyze the scope of AWS-based DDoS 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 origin of requests and report potentially compromised resources	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
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:

- l. Cloud Security Incident Report Template.docx
- m. Evidence Gathering and Forensic Analysis Form.docx
- n. Checklist for Handling the Forensic Evidence Properly.docx

## 6. Eradication

### 6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate incidents and prevent their 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 an AWS DoS/DDoS incident:
  - Deploy AWS Shield Advance
  - Create your own AWS WAF rules on your web ACL to mitigate the attack
  - Block or rate-limit traffic port 389 from the Internet
  - Blacklist unusual IP addresses
  - Use AWS Support to reduce the risk and enable the handling of requests, patches, backups, etc.
  - Build automated incident response mechanisms using ThreatResponse Suite such as AWS\_IR CLI for common security incidents
  - Implement Security Incident Response Simulations (SIRS) to practice incident response plans on internal events, and create runbooks that provide guidance during incident eradication
  - Enforce “Deny Policy” to deny all actions
  - Deactivate the original access keys and modify secret/access keys and CLI commands
  - Use AWS WAF WebACL to protect CloudFront and load balancer
  - Block the attack signatures to further mitigate the DDoS attack

### 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 analysis and create 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:

- o. Eradication of Cloud Security Checklist.docx
- p. Incident Eradication Template.docx
- q. Incident Eradication Checklist.docx

## 7. Recovery

### 7.1 Objectives

The main objective of this phase is to recover the affected systems, network, and other resources from the incident impact 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 AWS DDoS incident
  - Implement suitable backup approaches such as backup and restore, pilot light, warm standby, or multi-site active/active to recover resources

- Restore resources based on business impact analysis
- Restore the affected resources using a trusted backup
- File a complaint with the cybercrime department
- Contact law enforcement and brief them about the incident
- Take complete backups and update the software
- Recover the impacted resources using recovery tools such as CloudEndure Disaster Recovery
- Perform complete vulnerability analysis and patch the identified vulnerabilities
- Restart any suspended services
- Compare the current baseline levels with pre-incident metrics and logs
- Confirm that the service is reinitialized to pre-incident state
- Keep monitoring the reinitialized services to identify potential attack signatures

### 7.3 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:

- r. Recovery of Cloud Security Incidents Checklist.docx
- s. Incident Recovery Procedure Template.docx
- t. Incident Recovery Checklist.docx

## 8. Post-incident Activities

### 8.1 Objectives

The main objective of this phase is to create the necessary AWS-based DDoS incident reports such as incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close the AWS-based DDoS investigation and disclose it to the respective stakeholders.

## 8.2 Activities Involved

- Create a report on the implementation of the incident response process (along with attacker vectors and their mitigation steps)
- Create concise and clear incident documentation in a standard format
- Review the document along with the concerned teams
- Store the artifacts along with application information under CMDB entry for future DDoS incident response
- Update the existing response process document with newly identified threats and their response activities
- If a network or infrastructure requires frequent updates, include guidelines for administrators to configure the resources with appropriate measures
- Create an after-action report (AAR) that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar incidents
- Review the document along with the concerned teams and subject matter experts
- Conduct meetings discussing the lessons learned to document the details of the AWS-based DDoS incident. Moreover, ensure that the following questions are answered in these meetings:
  - When and how was the DDoS incident detected?
  - What happened exactly?
  - What were the motives behind the DDoS incident?
  - Who was contacted first about the incident?
  - Did the team face any additional challenges during the response process?
  - Was the organization prepared adequately for the incident?
  - How was the incident contained?
  - How were the impacted resources 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 incident?
  - Is the incident response team capable enough to mitigate similar incidents in future?
  - Were there any gaps in communicating the incident?
  - Was the right amount of information shared with the right personnel?

- What tools and resources are required to detect, analyze, and prevent such incidents in future?
- Which tools were effective during the response process?
- Create an incident impact assessment report to determine all types of losses caused by the AWS-based DDoS incident. Incident impact assessment must address the following, if required:
  - Financial losses incurred owing to service disruption
  - Legal costs for investigating the case, lawyer's fees, etc.
  - Costs pertaining to analyzing the AWS-based DDoS incident, recovering from it, and installing resources.
  - Implementation costs
  - Costs related to the damage of goodwill as well as loss of customer trust and reputation
- Close the AWS-based DDoS investigation officially by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization

### 8.3 Stakeholders Involved/Communication Established

Activities	Stakeholders Involved	Communication Mode/Channel
Conduct lessons learned meetings	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
	Senior Management	Email, Phone, Text Message



Disclose incident details with the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	Manager - Information Governance	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Human Resource	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:

- u. Incident Postmortem Template.docx
- v. After Action Report Form Template.docx
- w. Incident Documentation Template.docx
- x. Incident Impact Assessment Report Template.docx
- y. Incident Closure Letter.docx
- z. Incident Disclosure Form.docx
- aa. Incident Reporting Template.docx