Incident Response Playbook Template

Redback Operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified By** | **Approver** | **Date** | **Changes made** |
| 1.0 | Pari |  |  | Initial Draft |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 Introduction 4](#_Toc166781235)

[1.1 Overview 4](#_Toc166781236)

[1.2 Purpose 4](#_Toc166781237)

[1.3 Attack definition 4](#_Toc166781238)

[1.4 Scope 4](#_Toc166781239)

[2 Attack Types 4](#_Toc166781240)

[2.1 Type 1 4](#_Toc166781241)

[2.2 Type 2 4](#_Toc166781242)

[2.3 …... 4](#_Toc166781243)

[3 Stakeholders 4](#_Toc166781244)

[4 Flow Diagram 4](#_Toc166781245)

[5 Incident Response Stages 4](#_Toc166781246)

[5.1 Preparation 4](#_Toc166781247)

[5.2 Detection 4](#_Toc166781248)

[5.3 Analysis 4](#_Toc166781249)

[5.4 Containment 4](#_Toc166781250)

[5.5 Eradication 4](#_Toc166781251)

[5.6 Recovery 4](#_Toc166781252)

[5.7 Post Incident Review 4](#_Toc166781253)

[6 Terminology 4](#_Toc166781254)

# 1 Introduction

## 1.1 Overview

## 1.2 Purpose

## 1.3 Attack definition

## 1.4 Scope

# 2 Attack Types

## 2.1 Type 1

## 2.2 Type 2

## 2.3 …...

# 3 Stakeholders

# 4 Flow Diagram

# 5 Incident Response Stages

## 5.1 Preparation

## 5.2 Detection

## 5.3 Analysis

## 5.4 Containment

## 5.5 Eradication

## 5.6 Recovery

## 5.7 Post Incident Review

# 6 Terminology