Security Incident Response Plan

RightPoint

14 November 2021

Simon Jack Mitch

Elan Sithirasenan

**Table of Contents**

[1 Revision History 4](#_Toc138177705)

[2 Purpose and Scope 4](#_Toc138177706)

[3 Authority 5](#_Toc138177707)

[4 Definitions 6](#_Toc138177708)

[5 Roles & Responsibilities 6](#_Toc138177709)

[Internal Contacts\* 6](#_Toc138177710)

[External Contacts 8](#_Toc138177711)

[Other Stakeholders 8](#_Toc138177712)

[6 Team Structure 9](#_Toc138177713)

[7 Common Cyber Incidents and Responses 9](#_Toc138177714)

[8 Potential Threat Vectors 10](#_Toc138177715)

[9 Severity Matrix 10](#_Toc138177716)

[10 Incident Handling Process 12](#_Toc138177717)

[11 Incident Response Team Exercise (IRTx) 16](#_Toc138177718)

[11.1 Design Red and Blue Team Activities 16](#_Toc138177719)

[11.2 Create Red and Blue Team books 17](#_Toc138177720)

[11.3 Update Incident Response Plan based on feedback 25](#_Toc138177721)

[11.4 Evaluation revision table 26](#_Toc138177722)

[12 Approvals 27](#_Toc138177723)

[13 References 27](#_Toc138177724)

# Revision History

This Security Incident Response Plan has been modified as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| 01/08/2017 | 1.0 | Plan created |  |
| 14/11/2021 | 2.0 | Updated | Simon Jack Mitch |
| 16/02/2022 | 2.1 | Updated | Elan Sithirasenan |
| 20/06/2023 | 3.0 | Updated | Elan Sithirasenan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Review Cycle**This Security Incident Response Plan must be reviewed at least annually.

# Purpose and Scope

**Purpose**This Security Incident Response Plan exists to ensure RightPoint is prepared to manage cyber incidents in an effective and efficient manner. Security incidents are more frequent and sophisticated than ever. No organization globally is immune to attack. Organizations must ensure they are prepared to respond to incidents as well as prevent and detect. By having a plan, a team, and conducting exercises, organizations will be better prepared for inevitable incidents and will be able to contain the damage and mitigate further risk to the organization. Resources must be deployed in an organized fashion with exercised skills and communication strategies. This document describes the overall plan for responding to Security Incidents at RightPoint. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to preparing, identifying, containing, eradicating, recovering, and conducting lessons learned in order to minimize impact of security incidents.The goal of the Security Incident Response Plan is to ensure organizations are organized to respond to security incidents effectively and efficiently.

**Scope**This Security Incident Response Plan applies to all networks, systems, and data as well as members of the organization including employees and contractors as well as vendors that access the networks, systems, and data. Members of the organization who may be called upon to lead or participate as part of the Security Incident Response Team must familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impact to the organization.   
  
This document assists the organization with establishing incident handling and incident response capabilities and determining the appropriate response for common security incidents that will arise. This document is not intended to provide a detailed list of all activities that should be performed in combatting security incidents.

# Authority

Responsibility for the security of government information resides with the Incident Response Team Leader (often this is the Information Security Manager). During times when a high or critical security incident is underway this responsibility is entrusted to the Deputy Team Leader, which will be someone familiar with the organisation’s Information Security policy and procedure.

# 

# Definitions

Event an observable occurrence in a system or network. Events include a user connecting   
to a file share, a server receiving a request for a web page, or a user sending email.

Incident an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. An *incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It implies harm or the attempt to harm.

# Roles & Responsibilities

## Internal Contacts\*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Title | Phone | Email |
| Security Analyst (lead) | Jack Spence | Incident Handler Team Leader | 044 599 0088 | [js@RightPoint](mailto:js@mybank.com.au).com |
| Incident Handler | Mitchell Donovan | Incident Handler Deputy Team Leader | 0433112255 | [md@RightPoint](mailto:md@mybank.com.au).com |
| Incident Response (lead) | Simon Fleming | Incident Response Lead | 0445889977 | [sf@RightPoint](mailto:sf@mybank.com.au).com |
| Incident Response (backup) | Mitchell Donoval | Incident Response Deputy Lead | 0433112255 | [md@RightPoint](mailto:md@mybank.com.au).com |
| Note-taker | Janet Smith | Minute-taker | 0455556677 | [janets@RightPoint](mailto:janets@mybank.com.au).com |
| Commu- nications | David King | Communications Manager (PR & Media Relations) | 0466775576 | [dk@RightPoint](mailto:dk@mybank.com.au).com |
| Incident Management | Montanna Chisnall | Incident Manager | 0499889988 | [ms@RightPoint](mailto:ms@mybank.com.au).com |
| Security Manager | Kevin Ramezani | Security Technical Lead | 0433221122 | [kr@RightPoint](mailto:kr@RightPoint).com |
| Privacy | David King | Communications Manager (PR & Media Relations) | 0466775576 | [dk@RightPoint](mailto:dk@mybank.com.au).com |
| Network | Dylan Peters | Network Administrator | 0455556666 | [dp@RightPoint](mailto:dp@mybank.com.au).com |
| Desktop (Windows) | Peter House | IT Manager | 0411112222 | [ph@RightPoint](mailto:ph@mybank.com.au).com |
| Desktop (Other) | Peter House | IT Manager | 0411112222 | [ph@RightPoint](mailto:ph@mybank.com.au).com |
| Server (Windows) | Peter House | IT Manager | 0411112222 | [ph@RightPoint](mailto:ph@mybank.com.au).com |
| Server (Other) | Peter House | IT Manager | 0411112222 | [ph@RightPoint](mailto:ph@mybank.com.au).com |
| Datacentre | Peter House | IT Manager | 0411112222 | [ph@RightPoint](mailto:ph@mybank.com.au).com |
| Legal | John Cash | Inhouse Counsel | 0444334433 | [jc@RightPoint](mailto:jc@mybank.com.au).com |
| Law Enforcement (local) | QLD Police | Local Police | 0755554444 |  |
| Law Enforcement (federal) | Australian Federal Police | Federal Police | 132211 |  |
| Human Resources | Carmel Smith | Accounts Clerk | 0444333333 | [cs@RightPoint.com](mailto:cs@RightPoint.com) |
| Executive |  |  |  |  |
| Executive |  |  |  |  |
| CSO | Elan Sithirasenan | CSO | 0455667788 | [es@RightPoint.com](mailto:es@RightPoint.com) |
| CIO | Ian Brannigan | CIO | 0499997777 | [ib@RightPoint](mailto:ib@mybank.com.au).com |
|  |  |  |  |  |
|  |  |  |  |  |

\* every role should have a secondary and often a tertiary identified

## External Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Organization | Name | Title | Phone | Email |
| Vendor | IR on retainer | AusCERT |  | 0733332222 | [ir@auscert.org](mailto:ir@auscert.org) |
| Vendor | IR on retainer | Microsoft |  |  | [ir@microsoft.com](mailto:ir@microsoft.com) |
| Vendor | Service Provider |  |  |  |  |
| Vendor | Service Provider |  |  |  |  |
| Vendor | Service Provider |  |  |  |  |
| Vendor | Technology vendor |  |  |  |  |
| Vendor | Technology vendor |  |  |  |  |
| Vendor | Technology vendor |  |  |  |  |
| Connected organization | Peer |  |  |  |  |
| Connected organization | Peer |  |  |  |  |
| Connected organization | Peer |  |  |  |  |

## Other Stakeholders

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Organization | Name | Title | Phone | Email |
| Customers/ Clients | Refer company’s Xero database |  |  |  |  |
| Shareholders | c/- co accountant | Adrian |  | 0455555544 | [a@ac.com.au](mailto:a@ac.com.au) |
| Board of Directors |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Team Structure

# Common Cyber Incidents and Responses

|  |  |
| --- | --- |
| Type | Initial Response |
| Ransomware; a tool used to encrypt or lock victims’ data until a ransom is paid. | Immediately remove the infected device(s) from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined. |
| Malware Infections; a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. | Immediately remove the infected device(s) from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined. |
| Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks; overwhelming an ICT network with traffic that it cannot process, sometimes causing the network to fail. | Request gateway services provider to identify DOS/DDOS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and / or increase capacity. |
| Phishing and Social Engineering; deceptive communications designed to elicit users’ sensitive information (including network credentials). | Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took, and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorised access. |
| Data breach; unauthorised access to sensitive or personally identifiable information. | Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill. |
| Unauthorized Disclosure or Loss of Information | Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill. |
| Privacy Breach | Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill. |

# Potential Threat Vectors

|  |  |
| --- | --- |
| External/removable media | An attack executed from a USB containing malware. |
| Attrition | A DDoS attack on a critical network or system. |
| Web | The redirection of web traffic to a malicious URL that installs malware on a victim’s device. |
| Email | Phishing attacks that attempt to steal information and/or deploy malware to a victim’s device. |
| Impersonation usage | For example, a domain that is created to imitate yours in an attempt to deceive victims (typically associated with phishing attacks). |
| Improper usage | Human error resulting in a breach of information security policy; or attack from a malicious insider resulting in a cyber security incident. |

# Severity Matrix

The Incident Response team will determine the severity of the incident taking into consideration whether a single system is affected or multiple, the criticality of the system(s) affected, whether impacting a single person or multiple, whether impacting a single team or multiple, or impacting the entire organization. The Incident Response Team will consider whether a single business area or multiple and the impact of the incident. The Incident Handler must consider the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remediation.   
  
The Incident Response Team will consider the available information to determine the known magnitude of impact compared with the estimated size along with likelihood and rapidness of spread. The Incident Response Team will determine the potential impacts to the organization whether financial damage or brand and reputational damage or other harms.  
  
The incident may be the result of a sophisticated or unsophisticated threat, automated or manual attack, or may be nuisance/vandalism.   
  
The Incident Response Team will determine whether there is a vulnerability, whether there is an exploit, whether there is evidence of the vulnerability being exploited, and whether there is a known patch. Finally, the team will determine if this is a new threat (eg. zero day) or a known threat and the estimated effort to contain the problem.

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Indicators | Scope | Action |
| 1 – Critical | Data loss, Malware | Widespread and/or with critical servers or data exfiltration | Implement SIRT, Incident Response Plan, create Security Incident, Organization-wide |
| 2 – High | Theoretical threat becomes active | Widespread and/or with critical servers or data exfiltration | Implement SIRT, Incident Response Plan, create Security Incident, Organization-wide |
| 3 – Medium | Email phishing or active spreading infection | Widespread | Implement SIRT, Incident Response Plan, create Security Incident, Organization-wide |
| 4 - Low | Malware or phishing | Individual host or person | Notify SIRT, create Security Incident |

# Incident Handling Process

In the event of a Security Incident the Security Incident Response Team will adhere to the PICERL process as follows:

**Preparation**

* Build an incident response plan
  + Establish mandate, delegate authority decision making process and chain of command
  + Review/update annually
* Ensure you have an incident response team
  + Dedicated, virtual, or on-retainer
  + Provide training as necessary
* Document roles and responsibilities
  + Delegate authority
  + Provide training as necessary
* Conduct exercises, drills regularly
  + Consider that most incident types are known in advance
  + Prepare for the known so can focus on the unknown
  + Test the plan, team and tools
* Understand the environment
  + Diagrams, location of critical systems and data
  + Ensure adequate visibility into networks and systems to respond to an incident
  + Vendor environment
  + Understand dependencies
* Understand what controls are in place
  + Are they sufficient to mitigate risk to an acceptable level?
* Understand impacts
  + Determine Maximum Tolerable Downtime (MTD) and Acceptable Interruption Window (AIW)?
  + Prioritized list of assets and downtime
* Prepare war room and/or conference bridge(s)
  + Require a location physically or logically to convene
  + Ensure location is secure and appropriately equipped
* Establish communications plan in advance
* Establish agreements in advance
  + Eg. Incident Response on Retainer
  + Ensure annual plan review/update
  + Regular exercises
  + Familiarity with environment in advance
  + Preferred pricing
  + Established SLA, response times

**Notification**

* Ensure a central point of contact exists for employees to report real or suspected security incidents
* Ensure all employees are required to report security incidents
* Ensure all employees know they are required to report security incidents and how
* Ensure all employees do report security incidents in a timely fashion

**Convene**

* Bring together those who are aware of the incident
* Engage Incident Response Team members
* Remind all of responsibility to maintain need-to-know
  + Otherwise leads to managing misinformation
* Communicate effectively and efficiently
* Convene in war room or conference bridges
  + Ensure location is secure and appropriately equipped
* Often more than one location is required for different needs (eg. management and technical team)

**Identification**

* Determine whether an incident has occurred
  + Is it an event or an incident?
  + Search for correlating information to increase confidence there is a real incident
* Perform triage and ensure common understanding of how it was detected and who is aware
* Analyze the precursors and indicators
* Perform research (eg. search engines, knowledge base)
* Document investigation and evidence gathering
* Prioritize handling of incident based on relevant factors (functional impact, information impact, recoverability effort, etc)
* Determine severity, urgency and initial impact
* Review information and actions taken to date
* Report incident to appropriate internal personnel and external organizations

**Communication**

* Invoke communications plan respecting need-to-know
* Develop stakeholder relationship map, to determine the level of stakeholder involvement
* Ensure reported information is factual based on evidence available at the time
* Ensure a point of contact knows the current status at all times

**Containment**

* Implement incident response playbook
* Prevent further damage and problem from getting worse by containing the incident
* Determine the source, what vulnerability was exploited and plug the holes
* Continue impact/damage assessment and confirm the scope of the incident
* Determine what was changed (eg. files, connections, processes, accounts, access)
* Acquire, preserve, secure and document evidence and preserve chain of custody
* Continue taking notes, ensuring a detailed log about what was found and what you did about it

**Eradication**

* Eradicate the incident
* Remove all traces of the infection or other incident
  + Identify and mitigate all vulnerabilities that were exploited
  + Remove malware, inappropriate materials, and other components
* If more affected hosts are discovered (e.g., new malware infections), ensure to perform the identification steps on the newly identified examples, then contain
* Ensure the incident cannot re-occur
* Further understand the attack vector
* Continue taking notes, ensuring a detailed log
* Ensure any compromised machines are removed or formatted before placing back into service
  + Ensure necessary evidence has been collected

**Recovery**

* Return affected systems to an operationally ready state one by one
* Monitor closely to ensure incident does not re-occur or is not still ongoing
* Ensure systems are restored from a trusted source
* Confirm the affected systems are functioning normally
* Implement additional monitoring to look for future related activity if necessary

**Lessons Learned**

* Hold lessons learned meeting within 2 weeks
* Create a follow up report
* Walk through and review play-by-play of incident report
  + How was the incident detected, by whom, and when
  + Scope and severity of incident
  + Methods used in containment and eradication
* Identify opportunities for improvement to better prepare for next time
* Ensure accountability to follow up on identified opportunities

\* Multiple sources including NIST Special Publication 800-61 revision 2 and SANS

# Incident Response Team Exercise (IRTx)

# Rules of Engagement

Outline the rules of engagement in this section.

You will list all of the dos and don’t to successfully conduct the IRTx. The rules of engagement have to be strictly adhered by the team members to ensure consistency between teams and to enable the purple team to monitor the exercise without firefighting any unforeseen problems.

# Design Rean and Blue Team Activities

For the following section, you will need to plan and design your red team and blue team attack and defence activities.   
  
You are required to create 3 x Attack Runbooks & 3 x Defence Playbooks.

|  |  |
| --- | --- |
| **Attack** | **Description** |
| MitM | A man in the middle attack that redirects DNS queries to the attackers site. |
| Ransomware | A system has had files encrypted and held for ransom. |
| Phishing | A user has fallen victim to a phishing attack and may have given their credentials to the attacker. |
| Virus/Malware | A virus or malware has infected a system. |
| Data Exfiltration | A network monitor has detected an excessive amount of outbound bandwidth, indicating that data is being transferred out of the organizations network. |
| Compromised User Account | A user has had their user Account compromised and an attacker is likely to use it to gain access to unauthorized systems. |

List your attacks below and draft your Red & Blue team exercise  
  
Note: Your attack doesn’t need to be a legitimate attack, but you must demonstrate that you can execute the attack in a simulated environment such as Virtual Box using a virtual network.   
  
For example: If you select the DoS attack activity, you should setup at least 2 machines in a virtual network environment and demonstrate a basic denial of service attack. One of the machines might be a Kali or Parrot OS machine, and the other might be a windows server machine. You would simply demonstrate an attack from the Kali/Parrot machine to the Windows machine and take screenshots of the network traffic to prove that you have initiated the attack.   
  
It should be noted that with a DoS attack particularly, you won’t be able to put the windows machine offline because the denial of service is occurring over the same Network Adapter.   
  
Just a screenshot showing the traffic spike and the command you used for the attack would be enough evidence that the attack occurred.

|  |  |  |  |
| --- | --- | --- | --- |
| Attack | Red Exercise | Blue Exercise | Purple Exercise |
| [Attack chosen from above] | [How will you initiate the attack to practice your response plan?] | [How do you plan to defend from the attack if it happened in real life?] | [What will the purple team do during this exercise] |
| [Attack chosen from above] | [How will you initiate the attack to practice your response plan?] | [How do you plan to defend from the attack if it happened in real life?] | [What will the purple team do during this exercise] |

# Create Red and Blue Team books

During this task you will create the red team and blue team exercises which will form our incident response plan for the selected attacks. By the end of this activity, you should have 3 x Runbooks and 3 x Playbooks.   
  
**NOTE: Playbooks will be designed to follow the NIST Framework**[**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

What is a Runbook?

A runbook is a document used to create a simulated situation so that blue teams (Defence) can practice the response plan.  
  
When you create your Runbook, you must ensure that the following requirements are met:

* Use a computer and software to initiate an attack (Penetration Testing)
* Detailed instructions are provided, with screenshots.
* Don’t make the runbook too complicated, as another student will need to execute it.

What is a Playbook?

The Playbook is a document that is used to respond to the simulated exercise executed by the red team (Attack).   
  
When you create your Playbook, you must ensure the following requirements are met:

* Create a procedure that outlines who needs to be contacted or who you need to report the incident to.
* Create a process to collect and preserve evidence from the attack
* Create detailed steps to respond to the incident

Runbook 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the simulated attack] | | |  |
| Step 2 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task]  **[Copy and paste one of these step fields to create more steps]** | | |  |

The steps below have been named after each step in the NIST Incident Response Framework.  
You should have a good understanding of what is included in this framework so that you can complete this runbook effectively. You should provide very explicit and clear instructions on how to handle the attack which was written in the Runbook above. This guide will be used to defend against that exact attack.

Playbook 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| Preparation | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the response to the attack] | | |  |
| Step 2 | | Task | | | Complete |
| Detection & Analysis | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| Containment, Eradication & Recovery | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| Post Incident Activity | | [Provide details about what tasks to complete in this task] | | |  |

Complete the below runbook & playbook based on the second attack you chose.

Runbook 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the simulated attack] | | |  |
| Step 2 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task]  **[Copy and paste one of these step fields to create more steps]** | | |  |

Playbook 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| Preparation | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the simulated attack] | | |  |
| Step 2 | | Task | | | Complete |
| Detection & Analysis | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| Containment, Eradication & Recovery | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| Post Incident Activity | | [Provide details about what tasks to complete in this task] | | |  |

Complete the below runbook & playbook based on the third attack you chose.

Runbook 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the simulated attack] | | |  |
| Step 2 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| [Description of this step] | | [Provide details about what tasks to complete in this task]  **[Copy and paste one of these step fields to create more steps]** | | |  |

Playbook 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | [Document Name] | Version | [Version Number] | |
| Author | | [Author Name] | Date Created | [Created Date] | |
| Attack Type | | [Name of Attack] | Last Modified | [Last Modified Date] | |
| Staff Required | | [Number of Staff] | Skills Required | [Skills required by Staff] | |
| Document  Description | [Detail what is the purpose of this document? When would you use it and why?] | | | | |
| Step 1 | | Task | | | Complete |
| Preparation | | [Provide details about what tasks to complete in this task. This should be the first step to initiate the simulated attack] | | |  |
| Step 2 | | Task | | | Complete |
| Detection & Analysis | | [Provide details about what tasks to complete in this task] | | |  |
| Step 3 | | Task | | | Complete |
| Containment, Eradication & Recovery | | [Provide details about what tasks to complete in this task] | | |  |
| Step 4 | | Task | | | Complete |
| Post Incident Activity | | [Provide details about what tasks to complete in this task] | | |  |

# Update Incident Response Plan based on feedback

Swap your Incident Response Plan with another group and evaluate each other’s response plans.   
  
During your review, you must execute the Runbook and Playbooks and provide the required evidence from the attack and defence exercises.  
  
Once you have completed evaluating the other groups Incident Response Plan.   
  
Provide feedback in the form below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reviewer | | [Your Name] | | Review Date | [Today’s Date] |
| Author | | [Authors Name] | | | |
| **Feedback** | | | | | |
| Question | | | Response | | |
| Purpose of the document:  Is the purpose of document section clear? Could it be improved in any way? | | | [Provide feedback here] | | |
| Reporting Hierarchy:  Could the reporting hierarchy be improved in any way? | | | [Provide feedback here] | | |
| Can the Incident Response Team offer any other services other than what is currently listed? | | | [Provide feedback here] | | |
| How Can the Red Team Strategies be improved? | | | [Provide feedback here] | | |
| How can the Blue Team activities be improved to respond better to the incidents? | | | [Provide feedback here] | | |
| How can the communication between the IRT and Management be improved? | | | [Provide feedback here] | | |
| Feedback | [Based on the entire Incident Response Plan, including the Red Team and Blue Team activities, provide as much detail as possible to assist the improvement of this IRP] | | | | |

# 

# Evaluation revision table

After receiving feedback from a student, update this plan accordingly and provide very detailed information about the changes in the revision table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Modification** | **New revision number** | **Reviewer’s name** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Approvals

**Responsible Party**

Responsibility for the security of government information resides with the following responsible party:

|  |  |
| --- | --- |
| Responsible Party Name and Title | Responsible Party Signature |
| Kevin Ramezani  Security Manager |  |

The Responsible Party has reviewed the Security Incident Response Plan and delegates the responsibility for mitigating harm to the organization to the Incident Handler.

During times when a high or critical security incident is underway this responsibility is entrusted to the Security Analyst or their delegate.

**Incident Handler**

The Incident Handler has reviewed the Security Incident Response Plan and acknowledges that when a high or critical security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate.

The Incident Handler or their delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

|  |  |
| --- | --- |
| Incident Handler Name and Title | Incident Handler Signature |
| Mitchell Donovan  Incident Handler |  |

# References

National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revision 2, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident>

SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>