A green chameleon logo

Description automatically generated

Incident Response Plan

By Harrison Tierney

​​

Contents

​

​ …

…..

….

…

# Document Control and Review

|  |  |
| --- | --- |
| **Document Control** | |
| Author | Harrison Tierney |
| Owner | Chameleon LTD |
| Date Created | 26/04/2024 |
| Last Reviewed By | Harrison Tierney |
| Last Date Reviewed | Publish Date |
| Endorsed by and date | Me, cause iM the best |
| Next Review Due Date | 26/04/2025 |

|  |  |
| --- | --- |
| **Role/Position** | **Name** |
| Chief Information Officer (CIO) | *Insert Name* |
| Chief Information Security Officer (CISO) | *Insert Name* |
| Chief Senior Student | *Insert Name* |
| Chief Senior Student | *Insert Name* |
|  | *Insert Name* |
|  | *Insert Name* |
|  | *Insert Name* |

The Incident Response Life Cycle

Preparation

* Prepare for incidents
* Compile IT Assets lists
* Setup monitoring for baseline
* Determine security events that should be investigated

Detection And Analysis

* Collecting data from IT systems, security tools, publicly available information from inside and outside the organization
* Identification of precursors and indicators of attacks
* Analyse baseline/normal activity in comparison to attacks
* Correlating related events

Containment, Eradication and Recovery

Post-Incident

# Purpose and Objectives:

This policy serves to be a guide on how to recover from a multitude of cyber security incidents including data theft and malware attacks amongst others.

Objectives of the CIRP:

1. Provide an overview of the technology stacks, hardware and frameworks utilised in each department of Chameleon.
2. Set standard procedure in the resolution of cybersecurity incidents in all departments of Chameleon.
3. Minimise impact of cyber security incidents that mya occur now and in the future, ensuring efficiency in recovery for all Chameleon team members.
4. Set roles, responsibilities, and communication guidelines for those within the Cyber Incident Response Team.

# Standards and Frameworks

* Chameleon MOP
  + React
  + Jupyter Notebook
  + HTML
  + CSS
  + JavaScript
  + Google Cloud Platform
* EVCFLO
  + HTML
  + Jupyter Notebook
* Evoleon
  + HTML
  + JavaScript
  + Jupyter Notebook
* Chameleon Security
  + Python
  + GCP Security Suite

# Common Security Incidents and Responses

This section of the report looks to detail common security incidents and the mitigation tactics that aid in the defence against them.

|  |  |
| --- | --- |
| Type/ Description | Response |
| **Distributed/ Denial of Service:**  To overwhelm a service/server through fake traffic | * Google Cloud Platform’s (GCP) in built security suite has been shown to mitigate DOS and DDOS attacks when hosted on new website infrastructure. * Chameleon looks to implement a WAF on the server hosting the web site but for now can be flooded by SYN attacks. |
| **Ransomware:**  Tool or malware that encrypts files and holds the decryption key for ransom, usually for crypto currency. | * Immediate isolation of the affected systems. * Look to “System priority guide” for taking certain systems offline. * Take snapshots of systems affected for forensic investigation later. * Look through current monitoring measures to catch intruders and where the ransomware originated |
| **Malware:**  Software or code that disrupts normal operations through data or resource theft. | Isolation of affected machine/s (Disconnect from internet and network)  Take a snapshot of the current affected machine state for forensic investigation later.   * Reset any credentials that may have been used to enact the malware. * Restore device using backup previously taken. * Monitor network traffic for data extraction, then determine further actions such as pursuit and further litigation if necessary. |
| **Phishing:**  Social engineering attempts to trick users into inputting credentials or downloading malicious software. | * Reset compromised account passwords, ensuring any other accounts using the same password also change/reset. * Review monitor and logging software to find the cause of the phishing attempt (Emails, websites, malicious software etc.) |
| **Data Breach:**  Unauthorised access and disclosure of information | * Review Monitoring software to determine what was taken or extracted from the network * Isolate affected machines (Isolation protocol) * Take snapshots of affected machines and network for forensic review |

# Roles and Responsibilities

This section details the roles and responsibilities of core members and the responsibilities of each member during incident response and further decision making. All members currently listed should be familiar with the current document, plan and responsibilities.

## Points of Contact

Primary and Secondary (Backup) Contact points for cyber incident reporting. 24/7 Support Roster.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Hours Of Operation** | **Contact Details** | **Role Title** | **Responsibilities** |
| Harrison Tierney | 9am – 5pm | Email: [htierney@deakin.edu.au](mailto:htierney@deakin.edu.au)  Phone: 5555 5516 | Senior, Chameleon Security | Document Control  Host Upkeep |

## Cyber Incident Response Team (CIRT)

CIRT members responsible in responding to and managing cyber incidents.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Organisation Role | Contact Details | CIRT Role |
| Harrison Tierney | Cyber Security – Junior | Email: [htierney@deakin.edu.au](mailto:htierney@deakin.edu.au) | Incident Manager |
| *Insert name Here* | *Insert Role Here* | *Insert Contact Details Here* | Communications Manager |
| *Insert name Here* | *Insert Role Here* | *Insert Contact Details Here* | Technology Leader |
| *Insert name Here* | *Insert Role Here* | *Insert Contact Details Here* | Customer Support Leader |
| *Insert name Here* | *Insert Role Here* | *Insert Contact Details Here* | Problem Manager |

## CIRT Team Roles and Responsibilities Definitions

### Incident Manager:

Leading authority over the incident, working with all roles to ensure progress in accordance to this document. Delegate additional roles to team members as seen fit or create additional roles for team members such as having more Customer Support Leads to if demand is necessitating more supply of that role. Anything else that is not assigned to a traditional role falls to the Incident Manager and becomes their responsibility.

### Communications Manager:

Manages internal and external communications regarding the incident as well as measures taken to progress solutions from the rest of the CIRT roles. This role looks to collect customer responses and feedback, meet with executives about the incident and response, and communicate changes and progress to a public status page for the resolution. This role works closely with the Customer Support Leader to ensure customer queries are efficient and utilise correct information at the given moment of incident response.

### Technology Leader:

Tech Lead needs to be a Senior Technical Responder, allowing them better knowledge of current topology such as networks, running frameworks and software in use. Tech Lead will need to develop theories regarding how the Incident happened, how it happened and why. This role needs to communicate analysis and actions taken to remedy the situation as well as document any theories for later review. Post incident, this role will participate in meetings regarding better safeguarding, what was done to remedy the Incident and perform technical documentation of the Incident. Tech Lead works closely with most roles, especially the Incident Manager, sharing updates consistently and new information as soon as it comes to light.

### Subject Matter Expert

This role requires a responder with sound technical knowledge or familiar experience with the software/hardware that is currently subject to the incident. Mostly responsible for implementing or suggesting technical fixes to remedy the Incident. This role also looks to liaise with other Subject Matter Experts to bring new information and angles to provide more sound judgement over the Incident and response.

### Customer Support Manager

This role looks to provide a ‘port-of-call’ to all customer and employee questions regarding the incident and subsequent resolutions that may disrupt their work/productivity. This person will primarily look after incoming tickets, phone calls and other communications regarding the Incident and ensure that they are answered in a timely manner. This role needs to work closely with eh Communications Manager to ensure that all information currently going out to answer questions is up to date and factually correct at the time of answering.

### Problem Manager

This role looks to go beyond the original incident to find the root cause of the incident and better mitigate future Incidents through thorough investigation and review of measures in place. The responsibility of coordinating, running, and documenting a post-mortem investigation of the Incident falls to this person. This role also needs to be in close contact with incident Manager, Technology Lead and Subject matter Experts to ensure correct information when undertaking the post-mortem.

# Communications

This section of the report details the communication guidelines that need to be used when dealing with different types of attacks/incidents. Tact needs to be used when communicating information about incidents which covers use cases, sharing of information and channels.

## Internal Communications

Depending on the severity and type of information, the CIRT Team needs to remain vigilant of bad actors having access to communication channels such as Microsoft Teams, email and other messaging services. If the incident scope provided by the Tech Lead includes compromise of company channels, steps to mitigate information getting to attackers must be considered.

Other Channels to Use:

* In person meetings
* Phone calls utilising phone numbers (Not Teams integrated)
* Personal emails and accounts that do not use company communication channels

This ensures that the CIRT can work effectively against the attack without notifying attackers of the solutions that are being worked on. This also includes channels used outside of the CIRT, which includes other employees, contractors and other parties that utilise and/or have access to company communications channels.

If internal communications are not deemed to be compromised, company channels can be used to inform and spread current knowledge of the situation between CIRT and other parties.

## External Communications

Customer Support Leader and Communications Manager will need to work closely regarding answering customer and employee concerns about the Incident, ensuring to respond efficiently and factually. Incoming tickets, phone calls and emails need to be answered but also archived for review later, as customers may be experiencing different effects from the Incident than what is originally observed by the CIRT.

Information is key to successfully answering and quelling customer concerns. Obtaining information from the Tech Lead and Incident Manager before putting out any communications needs to be completed, as this may change how customers interact with affected systems. Timelines also need to be discussed with the rest of the CIRT as timelines may not be feasible due to the severity or depth of the attack/Incident.

# Incident Response Process

## Incident Classification

|  |  |
| --- | --- |
| Incident Classification | Descriptions |
| Critical | Critical System compromise  Secret Data theft highly likely  Root access on device/s |
| High | Current running servers compromise  Network infiltration.  Data theft likely |
| Medium | Data access potential  Network compromise.  Data theft unlikely but possible |
| Low | Low level system compromised.  Does not affect employee workflow.  Unsuccessful overall attack. |

## Cyber Incident Response Team (CIRT) Activation

When learning of incidents that are in action or have happened, the CIRT needs to be actioned. Overall scope needs to be determined and will lead to what members of the CIRT will need to attend the Incident. For example, if the incident only covers a small phishing attempt that was not successful, the Customer Support manager and Communications Manager will not need to be actioned as it does not concern external customers or contractors.

Incident Manager will need to use judgment and scope to call upon needed members of the CIRT.

# Standard Operating Procedure and Playbooks

Supporting Standard Operating Procedures

* Network Defence Playbook (Appendix XX)
* Malware/Ransomware Playbook (Appendix XX)
* Server Protection Playbook (Appendix XX)

# Incident Notification and Reporting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Type/threshold** | **Organisation/Agency to receive notification or report** | **Contact Details for the notifying Organisation/Agency** | **Key Notifying/reporting requirements and link to organisation/agency information** | **Personnel Responisble** |
|  |  |  |  |  |
|  |  |  |  |  |

Legal and Regulatory Requirements

Insurance

# Conclusion

# References:

# 