A cartoon of a lizard with headphones

Description automatically generated

**Incident Response Plan**

Contents

[Purpose 2](#_Toc152768254)

[Scope 2](#_Toc152768255)

[Maintenance 2](#_Toc152768256)

[Responsibilities of all staff 2](#_Toc152768257)

[Staff Roles and Responsibilities 3](#_Toc152768258)

[Dealing with security incidents 4](#_Toc152768259)

[Recognise a security incident 8](#_Toc152768260)

[Account Data Incidents 8](#_Toc152768261)

[Reporting 8](#_Toc152768262)

[Investigating 8](#_Toc152768263)

[Local Computer Technician Job in Investigating 9](#_Toc152768264)

[Dealing with Compromised Systems 10](#_Toc152768265)

[Communication Strategy 10](#_Toc152768266)

[Notification and Escalation Process 11](#_Toc152768267)

[Maintaining Business Continuity 12](#_Toc152768268)

[Recovering Objectives 13](#_Toc152768269)

[Preparing the Security of the System 14](#_Toc152768270)

[Phishing attack 14](#_Toc152768271)

[Phishing attack process 14](#_Toc152768272)

[Reconnaissance 14](#_Toc152768273)

[Delivery 14](#_Toc152768274)

[Command & Control 14](#_Toc152768275)

[Delivery 15](#_Toc152768276)

[WiFi Pineapple 15](#_Toc152768277)

[Reconnaissance 15](#_Toc152768278)

[Activation 15](#_Toc152768279)

[Data Audit 15](#_Toc152768280)

[Training Schedule 17](#_Toc152768281)

[Incidents Contact List: 17](#_Toc152768282)

[SEC. Hierarchy Chart 18](#_Toc152768283)

[Incident Response Forms # 19](#_Toc152768284)

[Definitions 32](#_Toc152768285)

# Purpose

The purpose of this response plan is to provide a plan, responding to security threats and attacks against Chameleon. Within this document it will define the roles of each individual of the response team and provide a large amount of information to help explain the process of how a response against an attack is handled.

# Scope

The Incident Response Plan applies to Chameleon security, networks, data and any user that has been granted permission to access their systems and data of the company.  
Contractual and sub-contractual members of the company, irrespective of scope, are subject to the same guidelines contained herein.

# Maintenance

This documentation is maintained on a regular basis and will be updated no less than annually but may be updated more frequently as needs and resources stipulate. Version information is appended at the end of the document.

# Responsibilities of all staff

It is expected that all existing staff, and future staff, will adhere to the policies stipulated in this document and utilise guidelines/framework where applicable.  
Please note that sub-sections and clauses may exist or be created by relevant departments (i.e. HR, OH&S etc.) and will be annotated accordingly.

# Staff Roles and Responsibilities

Staff members must adhere to both the global (read: company) policies and also policies stipulated by individual contracts and/or position information. Where policies that are role-neutral exist these apply to all staff members regardless of employment time or status.

Role: Incident Analyst

Team: Head of Red Team

Incident Analyst job is to successfully run attacks against the main server and computer systems for the documentation and reporting of exploits found within the system/ network devices by the company.

Role: Incident Responder

Team: Red Team Member

Incident Responder is basically a cyber first-responder. Provides a rapid initial response to any IT Security threats, incidents or cyber attacks on your organisation. They provide first-line response, IT security for day to day tasks and procedures.

Role: Incident Responder

Team: Red Team Member

Incident Responder is basically a cyber first-responder. Provides a rapid initial response to any IT Security threats, incidents or cyber attacks on your organisation. They provide first-line response, IT security for day to day tasks and procedures.

Role: Incident Responder

Team: Head of Blue Team

The role of the blue team is to assess network security and identify any possible vulnerabilities. Find ways to defend, change and re group defense mechanisms to make incident response much stronger for the network.

Role: Communication Liaisons

Team: Head of Purple Team

Purple team exits to maximize and ensure effectiveness of both the Red and Blue team. This is done by integrating defensive tactics and controls from the Blue team with the threats and vulnerabilities found by the Red team.

# Dealing with security incidents

Each and every security incident is to be dealt with and logged independently. Investigation (RE: forensics) will be conducted according to the baseline security and escalated where applicable; severity of security breach or infringement will determine level of escalation and tier of staff. Please see the individual policies governing breaches in associated support documentation.

|  |  |
| --- | --- |
| **Example Attack Types** | **Solutions for these attacks** |
| DDoS | * Buy more bandwidth * Build redundancy into your infrastructure * Configure network hardware against DDoS attack |
| Malware | * Install Antivirus/Malware Software * Keep Antivirus software up to date * Keep your operating system current |
| Phishing | * Check Emails * Apply spam filter * Have Antivirus installed |
| Ransomware | * Isolate the infection * Scareware * Screen Lockers * Encrypting Ransomware |

**DDoS Incident Response Flowchart**

A diagram of a flowchart

Description automatically generated

**Phishing Incident Response Flowchart**

A diagram of a flowchart

Description automatically generated

# Recognise a security incident

Baseline steps in classifying and recognising a security incident include:

* Logging all relevant details as accurately as possible (time/damage/involvement/resource cost)
* Advised mitigation strategies
* Implement SOC members as applicable
* Inform all staff strata as required (upper admin+)
* Adjust security resources if required and secure vulnerabilities
* Notify associated security firms or vulnerability specialists (if required)

# Account Data Incidents

* Notify stakeholders/data holders of incident
* Verify integrity of existing associated data
* Secure data repositories
* log incident and compare with existing security precautions and prior breaches
* IF appropriate extirpate data and relocate to safer endpoint/s.

# Reporting

Reporting, of all sorts, is to be to company standard. This includes usage of relevant company-wide terminology, correct reported information, verification of integrity, adequate logs and circulation through specific (company) channels. Reports should be kept to standard format with clear, concise information. Redacted information is to be reviewed prior to report release.

# Investigating

Investigation protocols exist for a.) internal and b.) external cases.  
In the event that an external (non-company) asset or individual is involved they are still bound by the same guidelines as internal staff regarding company policies, rules, and ethics. It is considered appropriate to bring in external assets in the event of a staff member or incident occurring where internal investigations could be compromised or biased.

# Local Computer Technician Job in Investigating

If there is an chance of an suspected security breach to the organisation, the onsite technicians will be asked to assist in certain ways like:

Check the backups:

By the technicians checking on the backup we can analyse the system to make sure that no files were affected, so that once the network system has been flushed and the computers have been reset they are able to upload the backup to the main network again.

Check anti-virus and firewall on endpoints:

Endpoint protects against various evolving security threats on a day to day basis. The technicians will reinstall antivirus on all fresh installations of windows to make sure that they are protected and enable the firewall to prevent unwanted traffic from the internet, while that is done they will also check all endpoints to make sure that the network is up and running with no issues.

Ensure the validity of Log Files:

By the technician checking the network logs, they will be able to understand how the system got infected and when so they can build a timeline. With this information they will be able to improve the security of the organization for any further attack.

Whoever is the individual who finds out about the breach should alert their supervising officer, once that is done the superior will be able to call up the technicians to act fast to prevent further damage to the network of the organization, once all is resolved an report of the attack is documented and given the organisation boss.

# Dealing with Compromised Systems

When an system has been compromised they are to be handled with care and contained, the procedures that should be followed are:

1. Disconnect the computer from the network- will help prevent any further untruest sources from taking further actions on the compromised computer.
2. Contact the Information Security Office
3. Notify users of the computer- by sending them an email or calling them so they do not continue to use the compromised system.
4. Preserve any log information on compromised computers- Any log files on a second computer or an external media device should be preserved immediately.
5. Wait for further instructions from Information Security Office

# Communication Strategy

* During a breach to the organization all communication needs to be on systems that are not compromised, so the workers can be aware of the situation.
* Some ways that communication can be secure in this situation is to contact the workers through their mobile phones or to communicate face to face.
* Once the security threat has been eliminated and the system resolved, all senior management workers of the organization need to get together to hold a meeting to reflect on the incident and improve overall security.

# Notification and Escalation Process

A diagram of a work flow

Description automatically generated

**Notification Process**

* Soc receives tickets from IT department
* Tickets reviewed by Alert Analyst (Tier 1)
* Alert Analyst investigates further
* Tickets get escalated to Incident Responders (Tier 2) if further analysis is required

**Escalation Process**

* Tickets unable to be resolved by Alert Analyst (Tier 1)
* Tickets escalate to Incident Responders (Tier 2)
* Tickets get escalated to Subject Matter Expert (Tier 3) if further resolution actions are required.

# Maintaining Business Continuity

The BCP (Business Continuity Plan) is initiated when a risk event occurs that has a key business interruption consequence. The business interruptions that are of concern from a continuity viewpoint are referred to as outages. These outage events will cause a significant disruption to, or unavailability of, key business processes. It follows that such events will have a high impact on and severe consequences. The nature of the business will indicate what high impact events influence company activity.

The first three phases relate to the initial development of the BCP. Business continuity management is an ongoing management responsibility; the BCP must be considered a ‘living document’. The fourth phase relates to the ongoing management of the plan. The plan should be actively managed: regularly tested, validated and updated. The BCP should remain current to fulfil its purpose in assisting management during times of major business disruptions.

BCP guidelines should be reviewed (preferably tested) at least every 3 years.  
Senior management should be made aware of BCP parameters and kept informed of significant changes.

A screenshot of a computer screen

Description automatically generated

# Recovering Objectives

Assets may need to be restored due to consequences of security compromise/s. Recovery may involve but are not exclusive to such actions as:

· Restoring systems from clean backups

· Rebuilding systems from original media

· Replacing compromised files with clean versions

· Installing patches

· Changing passwords

· Tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists)

# Preparing the Security of the System

Red team: (Attackers)

Are internal/external dedicated to testing the effectiveness of a security program by emulating the tools that are most likely attackers would use in realistic situations.

**Red Team methods are:**

# Phishing attack

The goal of the phishing attack is to breach the blue team’s network/data via phishing emails loaded with ransomware which encrypts said data, making it unaccessible to them unless they pay a price.

# Phishing attack process

## Reconnaissance

Collect as much data as possible on the organisation such as Infrastructure information, employee names, emails, phone numbers, IP addresses, login details, hardware specifications etc.

## Delivery

Posing as a corresponding third party with connections to the organisation. Send consistent malicious emails to the targeted employees of the organisation with false links or fake attachments which download the ransomware. Regularly change IP address to help avoid detection and bypass filters.

## Command & Control

After the payload is downloaded the code gets initiated, exploiting system vulnerabilities in order to encrypt the targets now accessible data. The goal of a DDoS attack is to effectively cripple a component of network infrastructure by ‘flooding’ that component with extraneous and useless network activity.  
  
DDoS Attack Process  
  
Reconnaissance

Examine the basic state of the network. Look for nodes/infrastructure that have minimal resistance or defence against randomised, non-essential web activity. Check for open ports, commonly used nodes and nodes linked to key network traffic.

## Delivery

Attack protocols are initiated. Incomplete, rapid-sent or incorrect (response) packets are sustainably sent at the vulnerable nodes via single or networked machines (see: zombie botnet etc.). Accessibility and function of attacked nodes are checked for resilience and/or failure of function. Attack process is maintained for a specified duration depending on attack method etc.

# WiFi Pineapple

A contemporary example of a MitM (Man In The Middle) attack. This involves using a specially crafted device to fool users into connecting to the WiFi Pineapple (which is disguised as a legitimate network connection point) instead of a typical network device, such as a router. In the context of a company environment this form of attack is useful to see if staff are practicing correct network hygiene and not connecting to unverified networks, using company network assets incorrectly etc.

## Reconnaissance

Red Team members survey a variety of physical locations (within and without company premises ideally) where staff are known to use WiFi network facilities. In the interests of ethical hacking processes if used OFF PREMISES they should notify the owner of a venue (i.e. a coffee shop) and notify them of the operation.

## Activation

WiFi Pineapple device is activated and concealed in location. The MitM Object is remotely contacted (physically is alternative) to parse data that passed through the network - activity is checked for company members’ access and credentials.

## Data Audit

Data collected via the Pineapple device is assessed in-depth via Red Team. Leaked data is tracked back to individual employees and both CyberSec and administration are notified of any activity indicative of poor network hygiene/data breaches that may render the organisation vulnerable to breaches.

Blue team: (Defenders)

Internal security team which defends against both real attackers and the Red team. They should be distinguished from the standard security team in most organizations.

The method that the Blue team will be using is SANS Incident Response Steps to prepare against Phishing Attacks:

1. **Preparation**

-All staff have been given training

-All desktop software is up to date

-The security policies have been put in place

-CIRT team is ready if needed

1. **Identification**

-Report phishing attack by submitting an ticket

-An manager will review the ticket, once confirmed there is an case of attack

-Notify management and law authorities

-Find the source of the attack

-Make sure that the attack has not spread to others systems

1. **Containment**

-All affected systems are isolated

-Deny access to affected accounts (Delete accounts if needed)

-Submit and containment request

1. **Eradication**

-Once request is approved, eradicate the infected system

1. **Recovery**

-Restore all data that was lost

-Notify all workers that the attack is over

1. **Lessons Learned**

-Collect all evidence of attack, document the incident

-Update all desktop software

-Teach those who don’t know about the attack so they know next time

Purple team: (Monitor both teams)

They exist to ensure and maximize effectiveness of the Red and Blue team. This is done by integrating defensive tactics and control from the Blue Team with threats and vulnerabilities found by the Red team. To monitor the cyberattack and defense of the Red and Blue team.

Example of this is SIEM system alerts and logs, as they will provide feedback to both teams by showing them their weaknesses so they can use this data to improve their attacks and defence for stronger security tests. Purple team will monitor both teams performance as follow:

* By checking SIEM system for alerts and affected systems
* Inspect Red teams by seeing how they will attack, potential detection and the impact to the system.
* Inspect Blue team by seeing their response time to the attack, their Incident Response Action Plan (Identification, Containment, Eradication, Recovery and Lesson Learnt).
* Inspect the types of tools that both team uses

To provide in depth feedback once the attack exercise is completed so both teams can improve.

# Training Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| **Training-** | **Date-** | **Time-** | **Staff-** |
| Incident Response | 17/9/20 - 18/9/20 | All Day | Red and Blue Team |
| Learn current tools and techniques | 24/9/20 - 30/9/20 | 9am - 1pm | Two individuals attend for the time, rest continue their job |
| Communication training | 2/10/20 - 9/10/20 | 9am - 1pm | Two individuals attend for the time, rest continue their job |
| Data Back-Up | 11/10/20 - 21/10/20 | 9am - 1pm | Two individuals attend for the time, rest continue their job |
| Engineering tools for cybersecurity | 23/10/20 - 30/10/2020 | 9am - 1pm | Two individuals attend for the time, rest continue their job |

# Incidents Contact List:

**Role**: Incident Analyst.

**Team**: Red Team

**Phone**:

**Email**:

**Role:** Incident Responders.

**Team:** Blue Team

**Phone:**

**Email:**

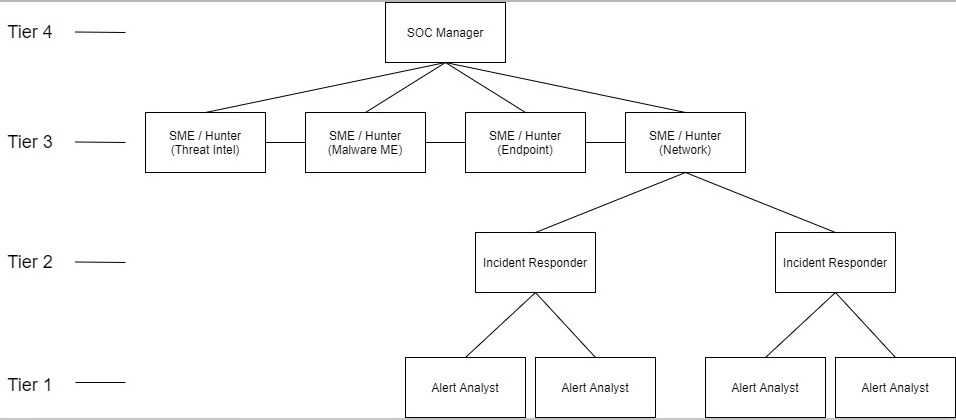
**Role:** Communication Liaisons.

**Team:** Purple Team

**Phone:**

**Email:**

# SEC. Hierarchy Chart



The diagram is a representation of the roles and team functioning.

SOC roles are as follows

* (Tier 1) Alert Analyst- Monitors SIEM alerts, manages and configures security monitoring tools.
* (Tier 2) Incident Responder- Receives incident and performs deep analysis, correlates with threat intelligence to identify threat actors.
* (Tier 3) Threat hunter- Day to day, conducts vulnerability assessments and penetration tests.
* (Tier 4) SOC Manager- Professionals who manage SOC and services and the main individual to contact for large organisations.

**Company Details**

Name: Chameleon

Business: Computer IT service and installation

**Member Responsibility**

Description:

Chameleon aims to utilise the Internet of Things (IoT), which is an ecosystem consisting of web-enabled smart devices such as phones, suburban traffic systems and domestic appliances, that all use embedded systems, such as processors, sensors, and communication hardware, to collect, send and act on data they acquire from their environments.

Internal:

Corporate Security Officer:

Corporate Legal Affairs:

CIO:

Corporate Public Affairs Officer:

Incident Responders:

Manager and reporting officer:

Corporate Incident Handling:

External:

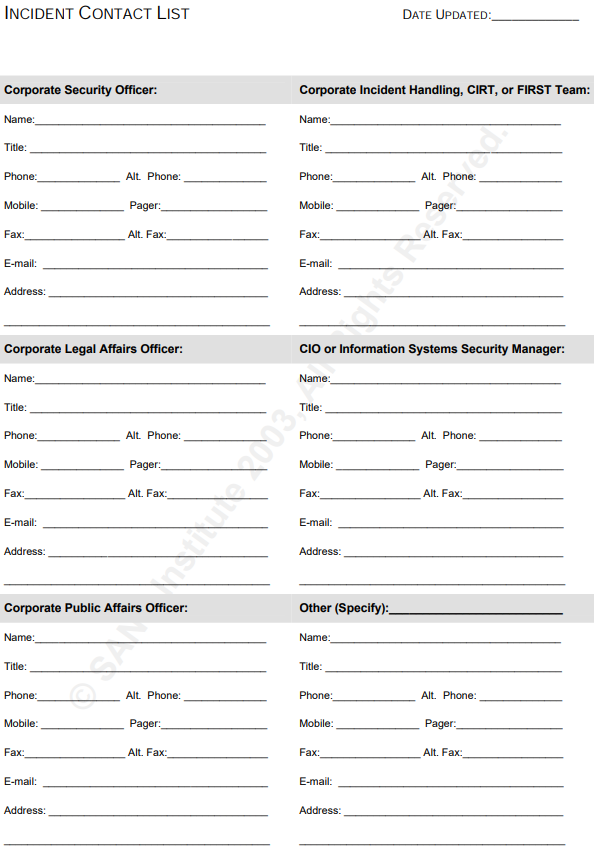
ISP- Internet Service Provider Technical Contact

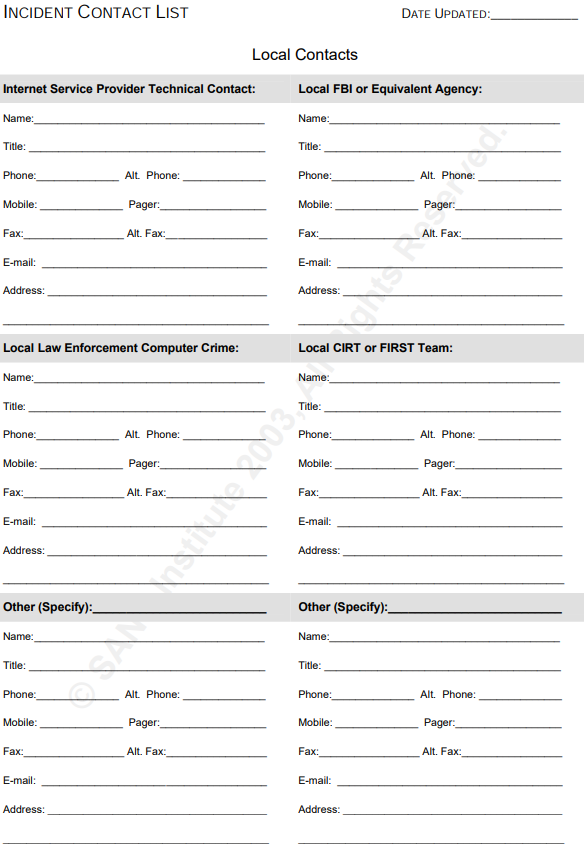
Federal Law Enforcement Agency

Local CIRT, CERT, CERT and Emergence Services

# Incident Response Forms #

**Incident Contacts List**

****

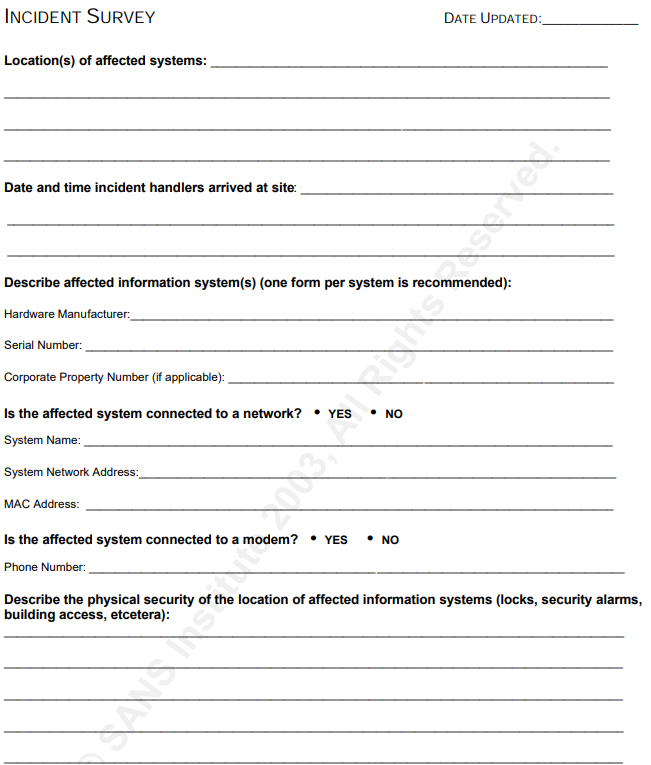
****

**Incident Communications Log**

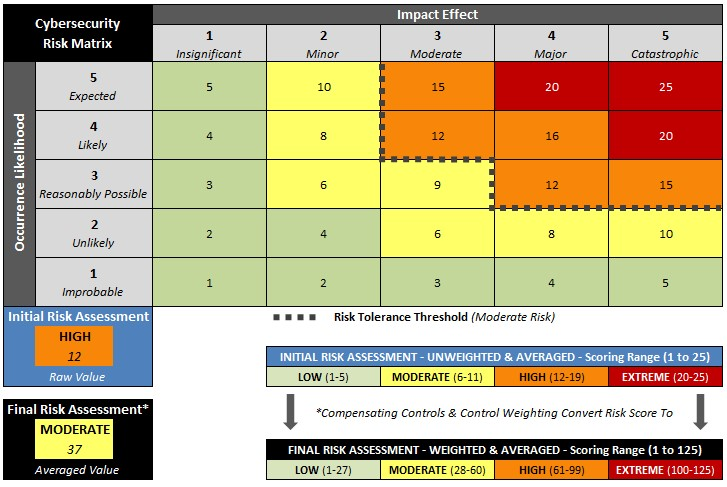
A close-up of a document

Description automatically generated

**Incident Survey**



**Threat Severity Assessment**

****

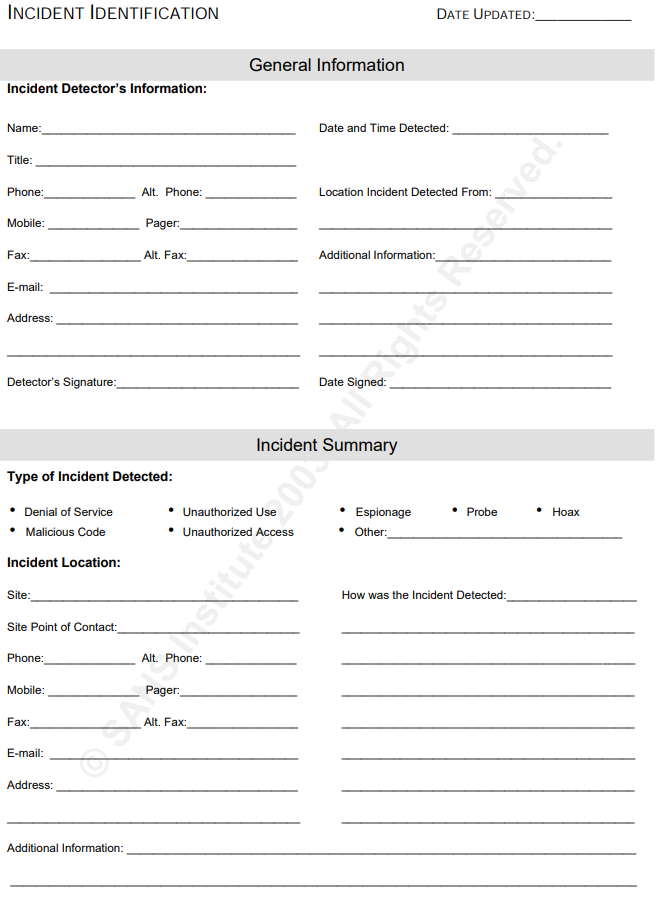
NIST-based Threat Matrix Criteria

Threats to organisational cybersecurity are assessed using the above matrix (as per NIST criteria state).

In general threats are broadly categorised; where necessary individual threats will be treated as a per-case basis for exceptional circumstances.

Note that threats can and will fall outside the parameters of the matrix as cybersecurity threats develop.   
  
Risk weighting is also dependent upon assets, size of business and organisational IP. External security assets should be made aware of company intricacies that do not violate NDA/IP limitations.

**Incident Identification**



**Chain of Custody**

A white sheet of paper with black text

Description automatically generated

A white sheet of paper with black text

Description automatically generated

**Incident Containment**

A document with text and images

Description automatically generated with medium confidence

**Incident Eradication**

A paper with lines on it

Description automatically generated

**Incident Handling Checklist**

A close-up of a checklist

Description automatically generated

# Definitions

**Event**

An event can be defined as a thing that happens or takes place.

**Incident**

An Incident is an event that is an instance of something happening.

**Red Team**

They are internal or external entities dedicated to testing the effectiveness of a security program by emulating tools and techniques.

**Blue Team**

They are an internal security team who defends against both real attacks as well as the Red Team.

**Purple Team**

Exist to ensure and maximize the effectiveness of the Red and Blue team.

**Threat actor**

Is a broad term for any individual or group of individuals that attempts to successfully conduct malicious activities against enterprises.

**Security Incident**

Is an event that may indicate that an organization's systems or data have been compromised or measures put in place to protect them have failed.

**Malware**

Collective name of a number of malicious software variants.

**Ransomware**

Is a type of malware that threatens to publish the victims data unless they are paid.

**Insecure attachment**

An attachment, usually of a common file type commonly used in businesses such as docx or pdf files, with malicious software built into it.

**Encrypted**

Convert into a code.

**ISO**

The ISO is the Information Security Office. They protect an organization's information technology programs from internal and external threats.

**Users**

User is a person who utilizes a computer or network service, like office workers using computers.

**Cloud storage**

The user uploads their files to the network for safe keeping.