A cartoon of a lizard with headphones

Description automatically generated

**Attack Scenario Playbook Template**

Contents

[SCENARIO 2](#_Toc153221126)

[Teams 3](#_Toc153221127)

[Introduction 4](#_Toc153221128)

[Attack Scenario 1: (DDoS Attack) 4](#_Toc153221129)

[Red Team: Playbook 4](#_Toc153221130)

[Blue Team: Playbook 6](#_Toc153221131)

[Purple Team: Playbook 9](#_Toc153221132)

[Attack Scenario 2: (Spear Phishing) 14](#_Toc153221133)

[Red Team: Playbook 14](#_Toc153221134)

[Blue Team: Playbook 16](#_Toc153221135)

[Purple Team: Playbook 20](#_Toc153221136)

[Definitions 27](#_Toc153221137)

# SCENARIO

Chameleon is in the process of expanding their business and implementing security controls. However, before this is can be completed, your team has been tasked with running **your Incident Response Plan to properly table test containment and mitigation of an incident, and to restore services as quickly as possible.**

TEST TOPOLOGY

The company has a firewall protecting various services; however, it may have been not been configured properly with the services left unhardened and therefore be vulnerable to various attacks.

The basic topology below shows the environment that the Table exercise will use for both Red and Blue in the simulation.

|  |  |  |
| --- | --- | --- |
| **Red Team** | **Blue Team’s monitoring SIEM** | **Chameleon’s Web Server** |
| **A black background with a black square  Description automatically generated with medium confidence** | **A black background with a black square  Description automatically generated with medium confidence** | **A white box with a blue cup and a blue globe  Description automatically generated** |
|  |
|  | **Chameleon’s Firewall** |  |

# Teams

**RED TEAM**

The Red Team may choose their own attack mechanism against the servers of Chameleon. You may consider attack vectors such as denial of service, virus introduction, data exfiltration or others.

Activities:

1. Discuss attack vectors, and launch mechanisms involved
2. Create a Red Team Play book
3. Execute the Red Team Playbook
4. Evaluate effectiveness of attack, and note lessons learned

**BLUE TEAM**

The Blue Team must follow their Incident Response Plan, including completing all necessary forms – such as a communications log, chain of custody, threat severity assessment, incident recovery checklist, etc. This will show how the Blue Team has responded and recorded relevant events.

Once the incident has been contained, services restored, and communication strategies enacted, then the Blue Team will need to debrief and consider lessons learned and record any improvements to their process that may have been discovered.

Note that the blue team’s response must follow the team’s Incident Response Plan, including the following critical steps:

1. Follow your Incident Response Plan that you developed
2. Receive (and make record of) the incident alert
3. Complete a chain of custody report for all stages of the incident
4. Complete and follow all relevant documentation and forms
5. Invoke strategies on how to react to the incident
6. Reaction to the incident
7. Follow communication protocols as listed including escalations and notifications
8. Evaluate the Incident Response Plan for effectiveness
9. Evaluate communication protocols from IRT to management
10. Make note of improvements to the IRP, and implement these changes
11. Evaluate effectiveness of defenses, and note lessons learned

# Introduction

We are tasked with running our Incident Response Plan to properly take test containment and mitigation of an incident, and to restore services as quickly as possible. So we will be in charge of using the Red team, Blue team and Purple teams to examine how efficient each group is. The training scenario will be carried out for the organisation to help improve the overall security of their network but also deepen their understanding to give them more options to adapt to new threats by using the data collected and then analysed. With this the organization system will be challenged in order to uncover weaknesses before real adversaries do.

# Attack Scenario 1: (DDoS Attack)

## Red Team: Playbook

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

The procedure that red team will follow is SANS Kill Chain process model which consists of:

1. ***Reconnaissance - (To gather information on the target pre-attack):***

Network is probed for vulnerabilities/nodes that can be overwhelmed in a DDoS attack. Focus is on web servers, ports, and other network contact points where security is weak or easily over-run with excess activity.

1. ***Weaponisation - (Preparing a ‘payload’ which will exploit a weakness of the target system and a method of entry):***

Software/network resources are pooled for the DDoS attack. This primarily involves configuring or ‘zombifying’ bot-nets, hiring bot-nets (usually illegal) or co-opting other networked machines on the same target network to participate. Counter-defense systems may also be investigated or employed if there is plausibility of stubborn defense parameters.

1. ***Deliver Exploitation - (Utilising a network vulnerability/human error/malicious action to unleash payload or malware onto system):***

All bot-net devices and other supporting elements are unleashed, flooding the targeted nodes with extraneous (pointless) traffic - usually acting on SYN/ACK principles - for a specified duration. This duration is normally limited by the extent of bot-net/s and ‘zombie’ clients.

1. ***Installation - (Deploying malicious elements onto target system):***

Unlike most other mechanisms of attack, DDoS ventures generally don’t have lingering presence/s on affected systems. Influence over targets is normally only as long as the surge of unwanted traffic is continued. Some more advanced methods may employ piggybacked code that allows placement of ‘back door’ components but this is uncommon (in which case there is an installation aspect: this normally assisting with future DDoS endeavours/circumventing defenses).

1. ***Command & Control - (Gaining either partial or full control of target asset/s via deployed malware or exploits. At this point the aggressor is in charge of network resources as targeted):***

The C&C (Command and control) aspect of this attack is crippling of network infrastructure - there is no traditional control of resources in the classical sense. Control here is purely preventing network traffic from continuing at healthy baseline levels.

***Lessons Learned***

* There are numerous DDoS-vulnerable elements on the Chameleon’s network (external and internal).
* Long-term suppression of network activity means a net loss of business for Chameleon and a worsening customer service level.
* Current network settings must be altered and secured against excess traffic and/or simulated excess traffic. Advised to re-examine data pipeline or minimise potential attack vectors.
* Network filters advised to be implemented (suggestions include screening traffic by region, times accessing servers etc.)

## Blue Team: Playbook

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

***Preparation***

* All staff have been given training
* Contact your ISP to understand the paid and free DDoS mitigation it offers and what process you should follow.
* Create a whitelist of the source IPs and protocols you must allow if prioritizing traffic during an attack
* Confirm DNS time‐to‐live (TTL) settings for the systems that might be attacked. Lower the TTLs, if necessary, to facilitate DNS redirection if the original IPs get attacked All desktop software is up to date
* Establish contacts for your ISP, law enforcement, IDS, firewall, systems, and network teams
* Document your IT infrastructure details, including business owners, IP addresses and circuit IDs; prepare a network topology diagram and an asset inventory
* Understand business implications (e.g., money lost) of likely DDoS attack scenarios
* If the risk of a DDoS attack is high, consider purchasing specialized DDoS mitigation products or services
* Collaborate with your BCP/DR planning team, to understand their perspective on DDoS incidents
* Harden the configuration of network, OS, and application components that may be targeted by DDoS
* Baseline your current infrastructure’s performance, so you can identify the attack faster and more accurately
* The security policies have been put in place
* CIRT team is ready if needed

***Identification***

* Report phishing attack by submitting an ticket
* Manager will review the ticket, once confirmed there is an case of attack
* Understand the logical flow of the DDoS attack and identify the infrastructure components affected by it
* Review the load and logs of servers, routers, firewalls, applications, and other affected infrastructure
* Identify what aspects of the DDoS traffic differentiate it from benign traffic
* If possible, use a network analyzer (e.g. tcpdump, ntop, Aguri, MRTG, a NetFlow tool) to review the traffic.
* Contact your ISP and internal teams to learn about their visibility into the attack, and to ask for help.
* If contacting the ISP, be specific about the traffic you’d like to control
* Find out whether the company received an extortion demand as a precursor to the attack
* If possible, create a NIDS signature to focus to differentiate between benign and malicious traffic
* Notify your company’s executive and legal teams; upon their direction, consider involving law enforcement

***Containment***

* Attempt to throttle or block DDoS traffic as close to the network’s “cloud” as possible via a router, firewall, load balancer, specialized device
* Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings
* Deny access to affected accounts (Delete accounts if needed)
* Submit and containment request

***Eradication***

* Once request is approved, eradicate the infected system
* If possible, switch to alternate sites or networks using DNS or another mechanism. Blackhole DDoS traffic targeting the original IPs
* If the bottleneck is a particular a feature of an application, temporarily disable that feature
* If possible, add servers or network bandwidth to handle the DDoS load
* If possible, route traffic through a traffic‐scrubbing service or product via DNS or routing changes
* If adjusting defenses, make one change at a time, so you know the cause of the changes you may observe
* Configure egress filters to block the traffic your systems may send in response to DDoS traffic, to avoid adding unnecessary packets to the network

***Recovery***

* Restore all data that was lost
* Notify all workers that the attack is over
* Collect all evidence of attack, document the incident

***Lessons Learned***

* Consider what preparation steps you could have taken to respond to the incident faster or more effectively
* If necessary, adjust assumptions that affected the decisions made during DDoS incident preparation
* Assess the effectiveness of your DDoS response process, involving people and communications
* Consider what relationships inside and outside your organizations could help you with future incidents
* Update all desktop software
* Teach those who don’t know about the attack so they know next time
* Summarise evidence and documents for preparation update

## Purple Team: Playbook

**Lessons learned:**

* When an attack is identified, the appropriate response teams must dedicate resources to dealing with the oncoming wave. That is essentially costing valuable hours and money, but it’s also taking those teams away from more important tasks. A particularly nasty attack could cause crews to pause or delay certain activities simply to cooperate with an investigation. That could then result in a provider losing efficiency, capabilities, or worse. At the very least, providers that incur significant costs would need to recuperate the money somehow, and that will most likely roll back into pricing. It’s hard to imagine a minor cyberattack having such an impact on the market, but it’s a definite possibility.
* Sophisticated cyberattacks can cause a lot of damage, but many of them can be easily prevented with the right security in place. Just as important to stopping attacks is building a strong and proactive security foundation. The latter requires vigilant maintenance for the systems and devices in question, which would include updating the tech and applying security patches for known exploits.
* DDoS attacks are different seeing as they are more vicious, pointed, and capable. Originally, launching a DDoS attack meant sending a huge bulk of requests to an IP address that overload the related systems and lock out legitimate requests. Generally, while these attacks do come from a few different computers and sources, they use less complex request methods. A massive distributed-denial-of-service attack can take down company websites, entire networks or nearly the entire Internet. For utility providers this kind of attack could prove disastrous to operations, inundating network servers and equipment with requests and blocking out official communications. DDoS attacks should be taken more seriously, and today’s enterprise world should be focused on preventing and protecting from them as much as any other threat. Most cloud service providers already do a great job protecting against these attacks. It becomes a real issue when hackers can take advantage of existing vulnerabilities.
* Even if there is a solution that can handle any threat, known and previously unknown, you still need a solution that can inspect the traffic deep enough into the payload to be able to form a distinctive pattern in spite of the randomization employed to the TCP/IP packet header.

**Incident Response Forms**

**Appendix A. Situation update**

|  |  |  |
| --- | --- | --- |
| **DATE OF ENTRY:** | **TIME OF ENTRY:** | **AUTHOR:** |
| **DATE AND TIME INCIDENT DETECTED** |  | |
| **CURRENT STATUS** | New / In Progress / Resolved | |
| **INCIDENT TYPE** | DDoS (Denial of service) | |
| **INCIDENT CLASSIFICATION** | Incident / Significant Incident / Emergency | |
| **SCOPE –** list the affected networks, systems and/or applications; highlight any change to scope since the previous log entry |  | |
| **IMPACT –** list the affected stakeholder(s); highlight any change in impact since the previous log entry |  | |
| **SEVERITY –** outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry |  | |
| **NOTIFICATIONS ACTIONED/PENDING** |  | |
| **ADDITIONAL NOTES** |  | |
| **CONTACT DETAILS FOR INCIDENT MANAGER** | **Name:**  **Email:**  **Phone Number:** | |
| **DATE AND TIME OF NEXT UPDATE** |  | |

**Appendix B. Incident Log**

|  |  |
| --- | --- |
| **DATE / TIME** | **NOTES (log, Record facts, decisions and rationale)** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Appendix C. Resolution action plan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATE AND TIME** | **CATEGORY**  (Contain / Eradicate / Recover / Communications) | **ACTION** | **ACTION OWNER** | **STATUS** (Unallocated / In Progress / Closed) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**FIREWALL & SECURITY**

|  |  |
| --- | --- |
| **FIREWALL SOFTWARE / HARDWARE** |  |
| **WIRED NETWORK** |  |
| **WIRELESS NETWORK** |  |
| **SINGLE POINT OF FAILURE – FIREWALL INFRASTRUCTURE** |  |

**ADMINISTRATION SYSTEMS (Supporting ICT systems)**

|  |  |
| --- | --- |
| **WEB PROXY SERVER DETAILS / LOGS & LOCATIONS** |  |
| **DOMAIN CONTROLLER DETAILS / LOGS & LOCATIONS** |  |
| **WEB SERVER DETAILS / LOGS & LOCATIONS** |  |
| **SERVER ENVIRONMENT OPERATING SYSTEM DETAILS / LOGS & LOCATIONS** |  |
| **VIRTUAL SERVER HOST ENVIRONMENT DETAILS / LOGS & LOCATIONS** |  |

**EMAIL SYSTEMS**

|  |  |
| --- | --- |
| **EMAIL SERVER DETAILS / LOGS & LOCATIONS** |  |

**STAFF DESKTOP / LAPTOP / TABLET SYSTEMS**

|  |  |
| --- | --- |
| **CLIENT ENVIRONMENT OS / LOGS & LOCATIONS** |  |
| **CLIENT HARDWARE MANUFACTURER / MODEL** |  |

## Attack Scenario 2: (Spear Phishing)

## Red Team: Playbook

Spear phishing attacks are the practice of sending fraudulent communication that appears to come from a reputable source and is usually done through email. Spear phishing targets specific people & organisations which can contain information relevant to the target to make it appear more legitimate with the goal being to steal sensitive data like credit card and login information, or to install malware on the victim’s machine.

1. ***Reconnaissance - (To gather information on the target before attack begins)***

Using multiple information sources in order to build up background knowledge of a target or organisation, this process is known as Reconnaissance. Collecting information across the internet via various social media or public websites, this information can be posted by themselves or by a third party. The goal of this stage is to acquire as much information relating to the target as possible as this will shape how the phishing email is put together correlating to the target, increasing the chance that the phishing email will be seen as legitimate.

Reconnaissance on Chameleon’s online information would highlight information which will be used in the following stages, this information could include employee names and contact details, technical information (IP addresses), job descriptions, the names of projects and other information.

1. ***Weaponization- (Preparing a ‘payload’ which will exploit a weakness of the target system and a method of entry)***

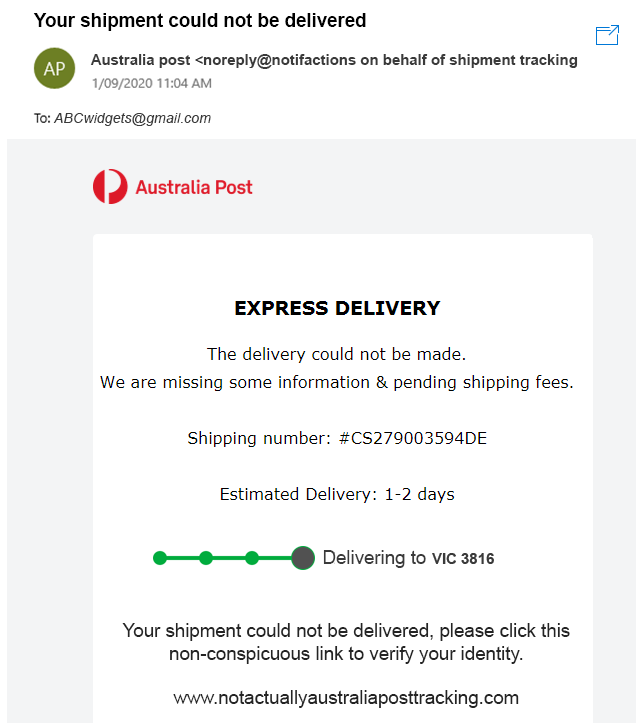
After the reconnaissance stage is complete and enough information has been collected to create the phishing email and the targets it will be sent to have been identified, it’s time to construct the email. This email will include information gathered from previous stages and will contain an attachment or website link which the target would have interest in. Attachments within the phishing email will appear as common file types such as .pdf, with the name relating to the target ie: “Chameleon\_Report.pdf”. When the attachment is opened malicious software is executed. Phishing emails can also contain links which when accessed executes malicious code or takes them to a fake website which appears legitimate.

The phishing email will then be made to appear as if it was sent from a trusted source in relation to the target, doing this will increase the chance of a compromise. ie: Chameleon regularly gets shipments from Australia post so an email from them would seem authentic.

1. ***Deliver Exploitation- (Utilising a network vulnerability/human error/malicious action to unleash payload or malware onto system)***

Sending the phishing emails to the specified targets while utilizing a VPN to avoid detection and IP filters.

Phishing email example to Chameleon with a malicious link:



1. ***Installation- (Deploying malicious elements onto target system)***

Activating the malicious payload after the target has clicked the malicious link or attachment. Their machine becomes infected with the malware/virus allowing control of the machine and the data on it.

1. ***Command & Control- (Gaining either partial or full control of target asset/s via deployed malware or exploits. At this point the aggressor is in charge of network resources as targeted).***

Retrieving the sensitive information/data on the targets now infected machine. Could be recurring depending if "back-door" access is configured allowing continued control and access to data.

## Blue Team: Playbook

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

***Preparation***

* Review and rehearse cyber incident response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary
* Review recent cyber incidents and the outputs
* Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities
* Ensure appropriate access to any necessary documentation and information including out-of-hours access
* Identify and obtain the services of a 3rd party Cyber Forensic provider
* Identify and secure the services of a 3rd party Cyber Responder Service
* Conduct regular awareness campaigns to highlight information security risks faced by employees
* Ensure regular security training is mandated for those employees managing personal, confidential or high risk data and systems
* All desktop software is up to date
* The security policies have been put in place
* CIRT team is ready if needed

***Identification***

* Monitor detection channels, both automatic and manual, customer and staff channels and social media for indications of a data breach or compromise such as spoofed emails and linked unknown URLs
* Report phishing attack by submitting an ticket
* Manager will review the ticket, once confirmed there is an case of attack
* Consider whether data loss or data breach has occurred
* Classify the cyber incident, based upon available information related to the Phishing attack and the incident types
* Where appropriate consider reporting requirements to law enforcement & authorities
* CIRT to begin initial investigation of the cyber incident
* Identify spoofed email
* Collate initial incident data
* Secure artefacts, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis
* Check escalation procedures and escalate in accordance with the CIRP
* Determine patch methods
* Review affected infrastructure for indicators of compromise derived from the Phishing analysis to identify any additional compromised system(s)
* Preserve all evidence to support attribution or anticipated legal action
* Examine threat intelligence feeds to determine if the Phishing attack is bespoke and targeted at specific individuals/senior stakeholders
* Verify all infected assets are in the process of being recalled and quarantined
* Identify any data or systems that have been affected
* Identify user credentials compromised or at risk
* Identify IT services being impacted
* Identify business impacts of the attack
* Identify how widespread the attack is across the organisation
* Identify the tools used to detect the attack
* Update senior stakeholders on any suspected or confirmed data breach
* Report any suspected or confirmed data breach including any personal data breach to the appropriate parties

***Containment***

* Identify systems being impacted or at risk of impact such as mobile devices, desktops, servers
* Reduce any further malicious activity by preventing the Phishing activity, quarantining affected systems and removing them from the network, or applying access controls to isolate from production networks
* Block access to any identified Remote Access Tools (RATs) to prevent communication with command and control servers, websites and exploited applications
* Identify compromised or at risk user credentials

***Eradication***

* Identify removal methods from the results of the attack
* Complete an automated or manual removal process to eradicate Phishing attack using appropriate tools
* Conduct a restoration of affected networked systems from a trusted back up
* Re-install any standalone systems from a clean OS back-up before updating with trusted data back-ups
* Change any compromised account details
* Confirm policy compliance across the organisation

***Recovery***

* Recover systems based on business impact analysis and business criticality
* Complete vulnerability scanning of all systems, across the organisation
* Re-set the credentials of all involved system(s) and users account details
* Reintegrate previously compromised systems
* Restore any corrupted or destroyed data
* Restore any suspended services
* Establish monitoring to detect further suspicious activity
* Co-ordinate the implementation of any necessary patches or vulnerability remediation activities

***Lessons Learned***

* Draft a post-incident report including the following
* Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users
* Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed
* Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process
* Complete the formal lessons identified process to feedback into future preparation activities
* Consider sharing lessons identified with the wider stakeholders
* Conduct root cause analysis to identify and remediate underlying vulnerabilities
* Publish internal communications in line with the communications strategy to inform and educate employees on Phishing attacks and security awareness

## Purple Team: Playbook

**lessons learned:**

* The lack of training and testing left employees unaware of how to recognize sophisticated malicious behaviour or report suspicious emails.
* Improved cyber awareness training with clear processes on how to report unusual emails or behaviours as well as regular testing to heighten employees’ vigilance can change the “click-first” mentality. In addition, implementing a tool that identifies emails from an external source can help employees take the time to stop and evaluate whether it’s from a trusted source.
* Hackers can leverage email conventions, titles, and company branding from public sources to build highly customized campaigns that make it extremely difficult for employees to detect suspicious behavior. Testing employees is very important, so they are aware of the evolving tactics attackers are using, and then building robust training on how to recognize and report these attacks. This training should include best practices for social media.
* Phishers are constantly changing tactics and developing new scams to fool people and technological anti-phishing solutions. The key to phishing attack prevention is to implement a range of defenses to block attacks. Any one of those measures may fail to detect a phishing email on occasion, but others will be in place to provide protection. This defense-in depth approach is essential given the sophistication of phishing attacks and the volume of messages now being sent.
* In addition to regular end user training and phishing simulation emails to harden the human element of defenses, the company needs an advanced spam filter. By using Office 365 company will already have a basic level of protection provided through Microsoft’s basic spam filter, Exchange Online Protection (EOP), but this should be augmented with a third-party solution such as SpamTitan to block more threats. EOP blocks spam, known malware, and many phishing emails, but SpamTitan will greatly improve protection against more sophisticated phishing attacks and zero-day malware.
* Company should also consider implementing a web filter to block the web-based component of phishing attacks. When an employee attempts to visit a malicious website that is used to steal credentials and other sensitive information, a web filter can prevent that website from being accessed.

**Incident Response Forms**

**Appendix A. Situation update**

|  |  |  |
| --- | --- | --- |
| **DATE OF ENTRY:** | **TIME OF ENTRY:** | **AUTHOR:** |
| **DATE AND TIME INCIDENT DETECTED** |  | |
| **CURRENT STATUS** | New / In Progress / Resolved | |
| **INCIDENT TYPE** | Spear Phishing Attack | |
| **INCIDENT CLASSIFICATION** | Incident / Significant Incident / Emergency | |
| **SCOPE –** list the affected networks, systems and/or applications; highlight any change to scope since the previous log entry |  | |
| **IMPACT –** list the affected stakeholder(s); highlight any change in impact since the previous log entry |  | |
| **SEVERITY –** outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry |  | |
| **NOTIFICATIONS ACTIONED/PENDING** |  | |
| **ADDITIONAL NOTES** |  | |
| **CONTACT DETAILS FOR INCIDENT MANAGER** | **Name:**  **Email:**  **Phone Number:** | |
| **DATE AND TIME OF NEXT UPDATE** |  | |

**Appendix B. Incident Log**

|  |  |
| --- | --- |
| **DATE / TIME** | **NOTES (log, Record facts, decisions and rationale)** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Appendix C. Resolution action plan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATE AND TIME** | **CATEGORY**  (Contain / Eradicate / Recover / Communications) | **ACTION** | **ACTION OWNER** | **STATUS** (Unallocated / In Progress / Closed) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Appendix D. Evidence register**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATE, TIME AND LOCATION OF COLLECTION** | **COLLECTED BY** (name, title, contact and phone number) | **ITEM DETAILS** (quantity, serial number, model number, hostname, media access control (mac) address, and ip addresses) | **STORAGE LOCATION AND LABEL NUMBER** | **ACCESS –** date, time, person and rationale for access after collection |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**FIREWALL & SECURITY**

|  |  |
| --- | --- |
| **FIREWALL SOFTWARE / HARDWARE** |  |
| **WIRED NETWORK** |  |
| **WIRELESS NETWORK** |  |
| **SINGLE POINT OF FAILURE – FIREWALL INFRASTRUCTURE** |  |

**DATA BACKUP**

|  |  |
| --- | --- |
| **BACKUP SOFTWARE** |  |
| **BACKUP LOCATION & RESTORATION TIMEFRAMES** |  |
| **DATA RETENTION REQUIREMENTS** |  |

**ADMINISTRATION SYSTEMS (Supporting ICT systems)**

|  |  |
| --- | --- |
| **WEB PROXY SERVER DETAILS / LOGS & LOCATIONS** |  |
| **DOMAIN CONTROLLER DETAILS / LOGS & LOCATIONS** |  |
| **WEB SERVER DETAILS / LOGS & LOCATIONS** |  |
| **SERVER ENVIRONMENT OPERATING SYSTEM DETAILS / LOGS & LOCATIONS** |  |
| **VIRTUAL SERVER HOST ENVIRONMENT DETAILS / LOGS & LOCATIONS** |  |

**EMAIL SYSTEMS**

|  |  |
| --- | --- |
| **EMAIL SERVER DETAILS / LOGS & LOCATIONS** |  |

**DATABASE SYSTEMS**

|  |  |
| --- | --- |
| **SERVER DETAILS / LOGS & LOCATIONS** |  |
| **PRODUCTION DATABASE DETAILS / LOGS & LOCATIONS** |  |
| **TEST DATABASE DETAILS / LOGS & LOCATIONS** |  |

**CLOUD SERVICE PROVIDERS**

|  |  |
| --- | --- |
| **HOSTED SERVICE PROVIDERS & SLAs** |  |

**STAFF DESKTOP / LAPTOP / TABLET SYSTEMS**

|  |  |
| --- | --- |
| **CLIENT ENVIRONMENT OS / LOGS & LOCATIONS** |  |
| **CLIENT HARDWARE MANUFACTURER / MODEL** |  |

# Definitions

**Red Team**

This team offers a wide variety of benefits, including a better understanding of the potential data exploitations on the company and ways in which the breaches can be prevented. The objective of the team is to detect, prevent and eliminate vulnerabilities. They are hired to uncover weaknesses in the companies network and exploit them, so then they can improve the companies overall security. By Red Team simulating a cyber-attack on the companies network, they can make sure that their security system is up to par with current standards.

Blue Team

A blue team consists of security professionals who have an inside out view of the organisation. Their task is to protect the organization’s critical assets against any kind of threat. They are well aware of the business objectives and the organization’s security strategy. Therefore, their task is to strengthen the ‘castle walls’ so no intruder can compromise the defenses.The blue team first gathers data, documents exactly what needs to be protected and carries out a risk assessment. They then tighten up access to the system in many ways, including introducing stronger password policies and educating staff to ensure they understand and conform to security procedures.

Purple Team

Purple teams exist to ensure and maximize the effectiveness of the Red and Blue teams. They do this by integrating the defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team into a single narrative that maximizes both. Purple team can help security teams to improve the effectiveness of vulnerability detection, threat hunting and network monitoring by accurately simulating common threat scenarios and facilitating the creation of new techniques designed to prevent and detect new types of threats.