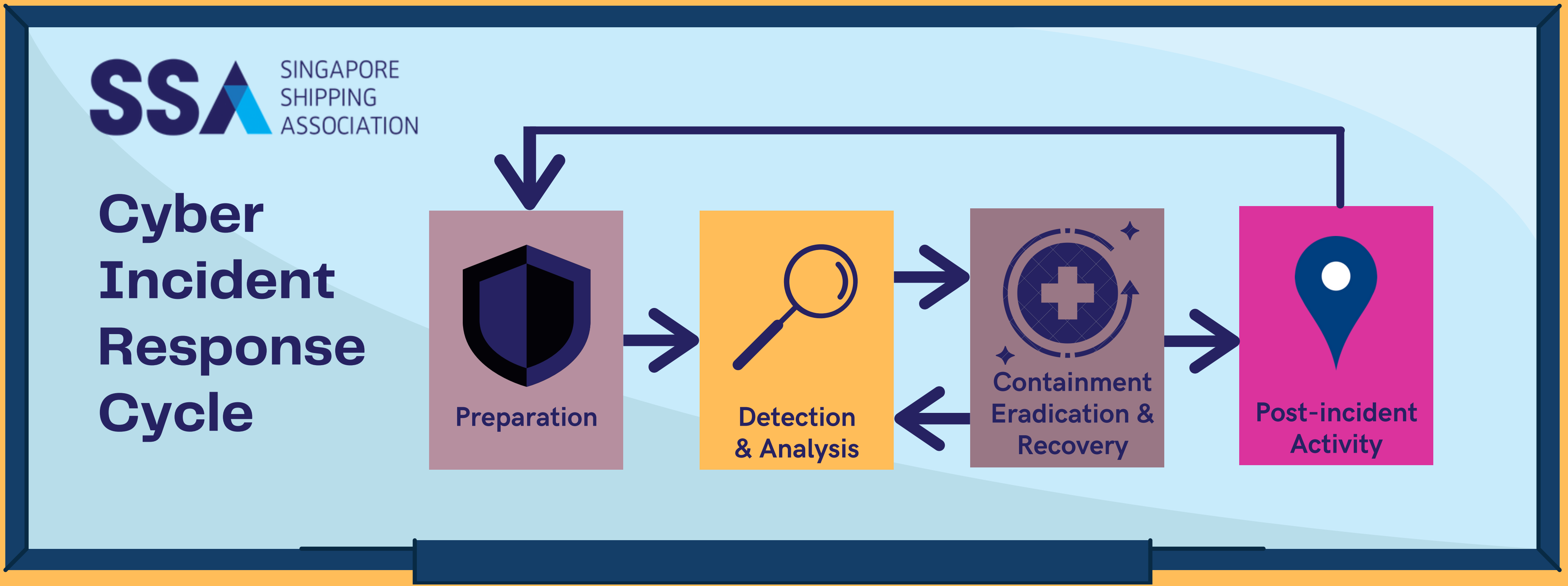
Cyber Incident Response PLAYBOOK

The purpose of the Cyber Incident Response Playbook (IT) is to define activities that should be considered when detecting, analysing and remediating cyber incidents.

The playbook also identifies the key stakeholders that may be required to undertake these specific activities.



SSA SINGAPORE SHIPPING ASSOCIATION

Cyber Incident Response Cycle

Preparation

Detection & Analysis

Containment Eradication & Recovery

Post-incident Activity

AN INITIATIVE BY THE SSA CYBERSECURITY SUB-COMMITTEE

About this Cyber Incident Response PLAYBOOK (IT)

> “*We look forward to having our members benefits from the Incidents Response Playbook. With this reference, we can be better prepared on our response procedures, conduct frequent drills and training for internal staff. Organisations will be able to respond swiftly, systematically contain/eradicate the incident and maintain strong communications with key stakeholders. Effective response and recovery is as important as protection and detection.*”
>
> ***Leslie Yee,*** **SSA Cybersecurity Sub-Committee Chairman,** ***2019/2021***

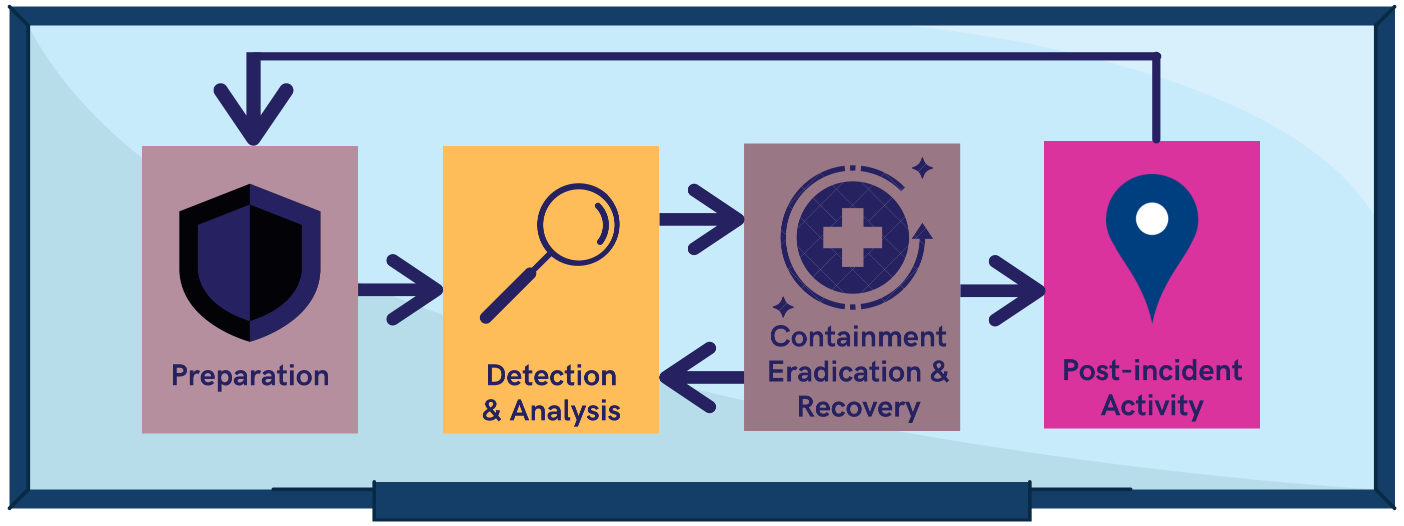
THIS PLAYBOOK CONTAINS THE FOLLOWING SECTIONS:

- Handling Ransomware/ CryptoLocker
- Handling Malware Infection
- Handling Phishing Attack
- Handling Data Breach
- Handling DoS Attack

Cyber Incident RESPONSE CYCLE

Establishing an appropriate cyber security incident response capability helps in assessing the state of readiness so that an organisation can prepare for a cybersecurity incident, respond to a cyber security incident and follow up and review a cyber security incident.

The Cyber Incident Response Cycle consists of 4 stages:



1. **Preparation involves utilising anti-malware software and firewalls.**
2. **The Detection & Analysis phase uses technical or administrative security controls to detect malicious activity in the environment,**
3. **which then flows into the next stage containment, eradication, and recovery, with the implication that each may be repeated multiple times during a given incident.**
4. **In the post-incident activity, this stage looks at understanding the cause of the incident, reviewing how the program can be improved, with the proceeding to start to implement improvements.**

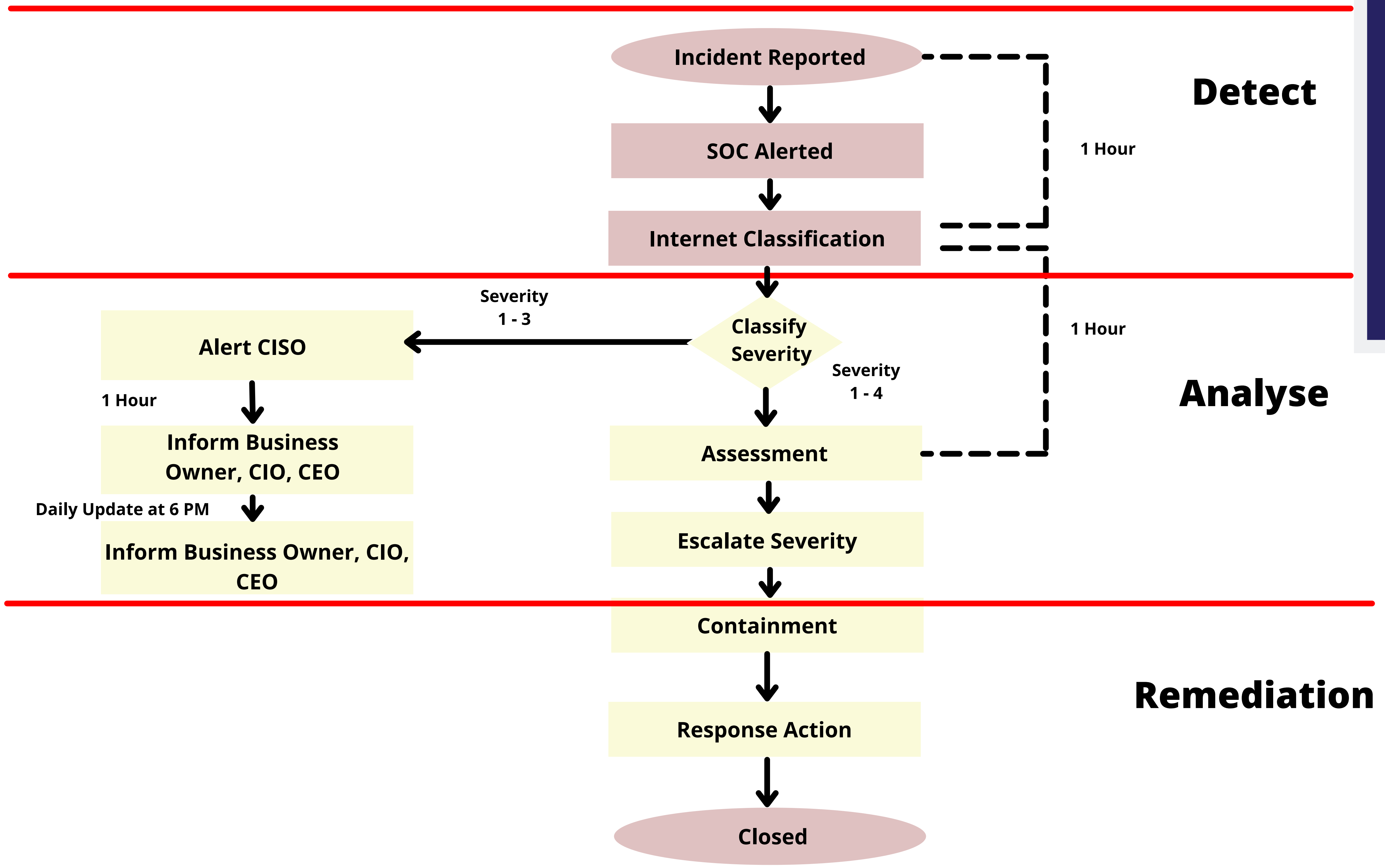
Defining the ORGANISATION SECURITY LEVEL

Risk Level Evaluation

Severity Level	Timeframe Escalation	Next Level	What is the impact?
1	Within 1 hour	Deputy GM/CIO	Security Level 1: • Affected more than 50% of the IT system • The overall Company business affected • Business data integrity affected
2	Within 4 hours	Deputy GM/CIO	Security Level 2: • At least 1 business function/operation affected • Material financial impact
3	Within 6 hours	Deputy GM/CIO	Security Level 3: • Minor system failure has occured • Service Degradation has occured
4	Within 2 days	Deputy GM	Security Level 4: • Suspicious security issues detected by SIEM • Issues already prevented by existing security controls • Issues can be prevented by existing security controls

Depending on their complexity & risk appetite, these levels can be established with the assistance of a company's IT department or a cybersecurity services provider.

Defining the INCIDENT FLOW RESPONSE



Incident Reported

SOC Alerted

Internet Classification

1 Hour

Detect

Classify Severity

Severity 1 - 3

Alert CISO

1 Hour

Inform Business Owner, CIO, CEO

Daily Update at 6 PM

Inform Business Owner, CIO, CEO

Severity 1 - 4

Assessment

1 Hour

Analyse

Escalate Severity

Containment

Response Action

Closed

Remediation

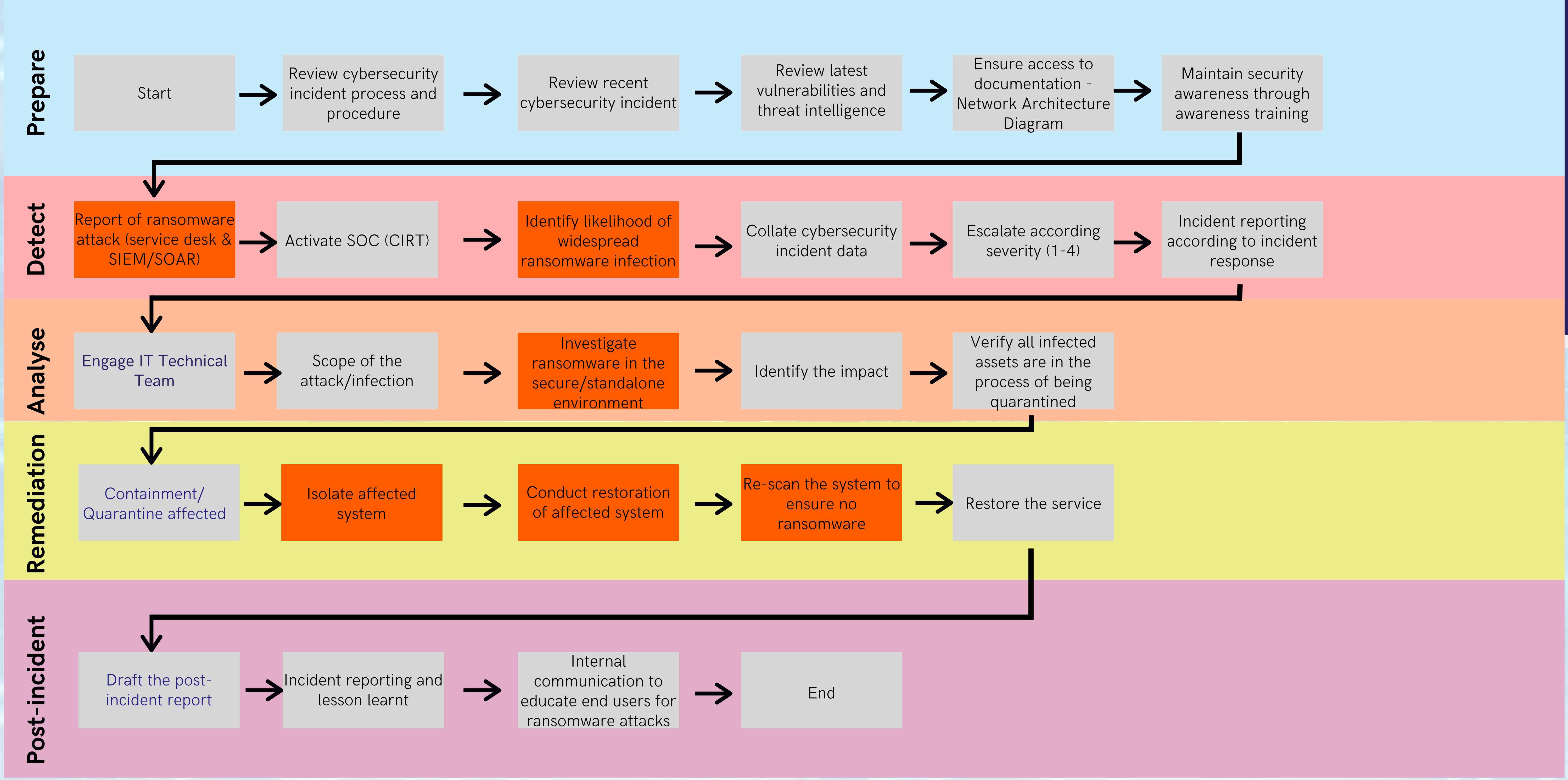
The need to prepare people and organizations for cyberattacks is very important.

The recommended structure will be to have a team that looks at Remediation, Analyze and Detect.

How do you HANDLE RANSOMWARE/CRYPTOLOCKER?

Infections can be devastating to an individual or organization.

Also, recovery can be a difficult process that may require the services of a reputable data recovery specialist.



Prepare

- Start
- Review cybersecurity incident process and procedure
- Review recent cybersecurity incident
- Review latest vulnerabilities and threat intelligence
- Ensure access to documentation - Network Architecture Diagram
- Maintain security awareness through awareness training

Detect

- Report of ransomware attack (service desk & SIEM/SOAR)
- Activate SOC (CIRT)
- Identify likelihood of widespread ransomware infection
- Collate cybersecurity incident data
- Escalate according severity (1-4)
- Incident reporting according to incident response

Analyse

- Engage IT Technical Team
- Scope of the attack/infection
- Investigate ransomware in the secure/standalone environment
- Identify the impact
- Verify all infected assets are in the process of being quarantined

Remediation

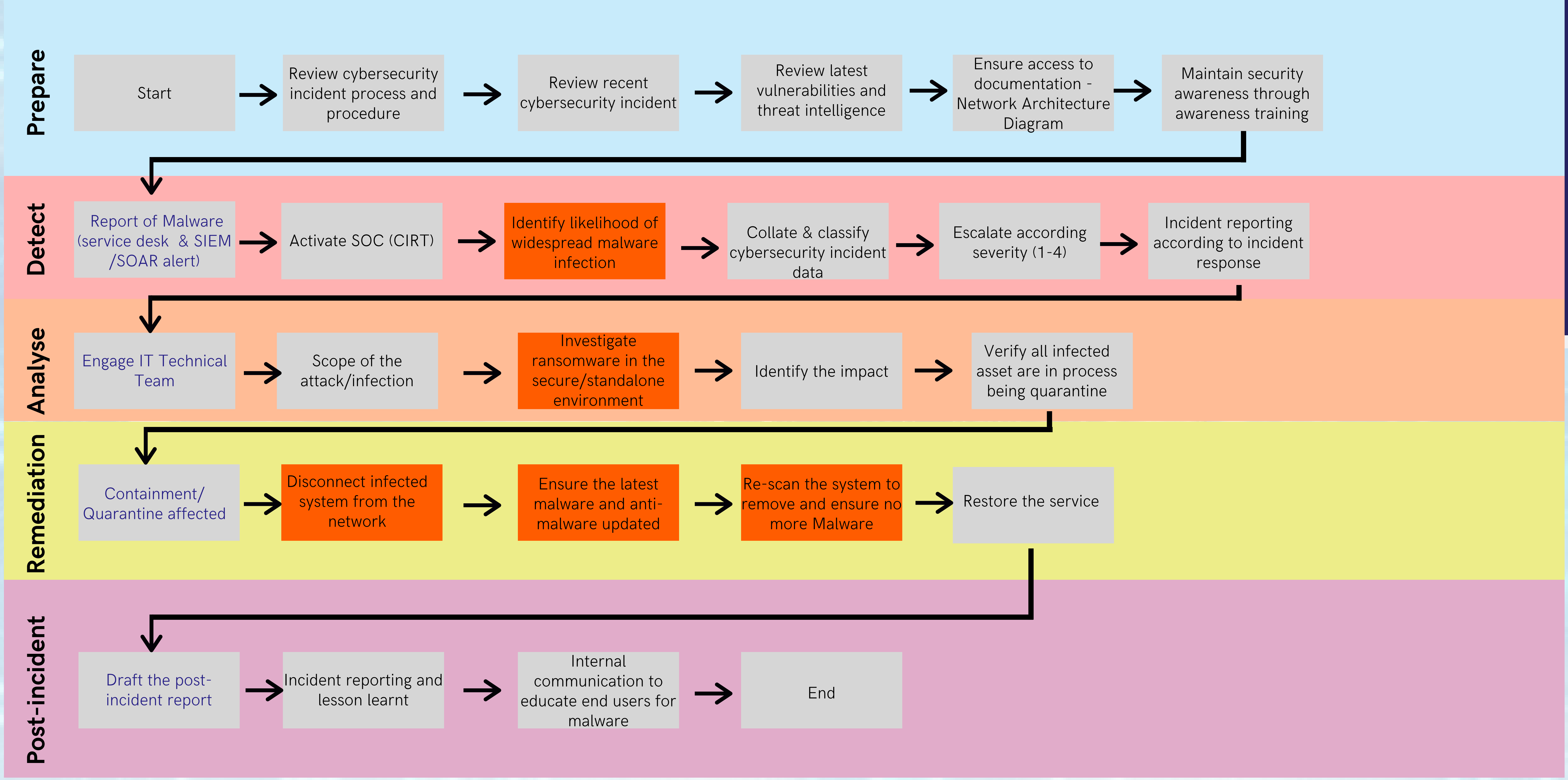
- Containment/ Quarantine affected
- Isolate affected system
- Conduct restoration of affected system
- Re-scan the system to ensure no ransomware
- Restore the service

Post-incident

- Draft the post-incident report
- Incident reporting and lesson learnt
- Internal communication to educate end users for ransomware attacks
- End

How do you HANDLE MALWARE INFECTION?

Organizations should have a robust incident response process capability that addresses malware incident handling.



Prepare

Start → Review cybersecurity incident process and procedure → Review recent cybersecurity incident → Review latest vulnerabilities and threat intelligence → Ensure access to documentation - Network Architecture Diagram → Maintain security awareness through awareness training

Detect

Report of Malware (service desk & SIEM /SOAR alert) → Activate SOC (CIRT) → Identify likelihood of widespread malware infection → Collate & classify cybersecurity incident data → Escalate according severity (1-4) → Incident reporting according to incident response

Analyse

Engage IT Technical Team → Scope of the attack/infection → Investigate ransomware in the secure/standalone environment → Identify the impact → Verify all infected asset are in process being quarantine

Remediation

Containment/ Quarantine affected → Disconnect infected system from the network → Ensure the latest malware and anti-malware updated → Re-scan the system to remove and ensure no more Malware → Restore the service

Post-incident

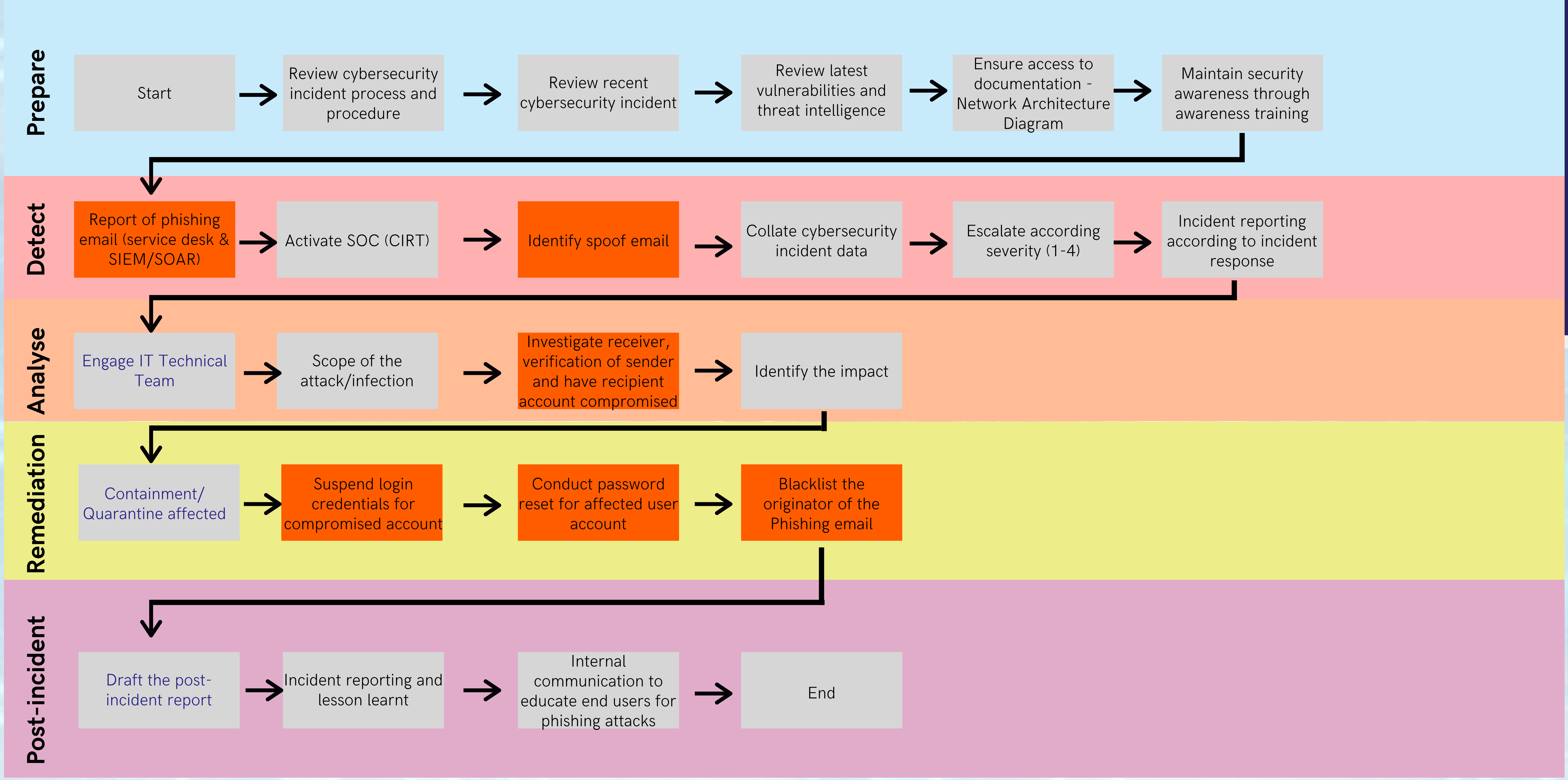
Draft the post-incident report → Incident reporting and lesson learnt → Internal communication to educate end users for malware → End

The first step is to detect whether or not your system truly has been infected.

How do you HANDLE PHISHING ATTACK?

There are several human and technological factors that companies should consider to avoid falling victim to phishing attacks.

It's also important to educate your employees about the tactics of phishers. Employees awareness is key.



Prepare

Start → Review cybersecurity incident process and procedure → Review recent cybersecurity incident → Review latest vulnerabilities and threat intelligence → Ensure access to documentation - Network Architecture Diagram → Maintain security awareness through awareness training

Detect

Report of phishing email (service desk & SIEM/SOAR) → Activate SOC (CIRT) → Identify spoof email → Collate cybersecurity incident data → Escalate according severity (1-4) → Incident reporting according to incident response

Analyse

Engage IT Technical Team → Scope of the attack/infection → Investigate receiver, verification of sender and have recipient account compromised → Identify the impact

Remediation

Containment/ Quarantine affected → Suspend login credentials for compromised account → Conduct password reset for affected user account → Blacklist the originator of the Phishing email

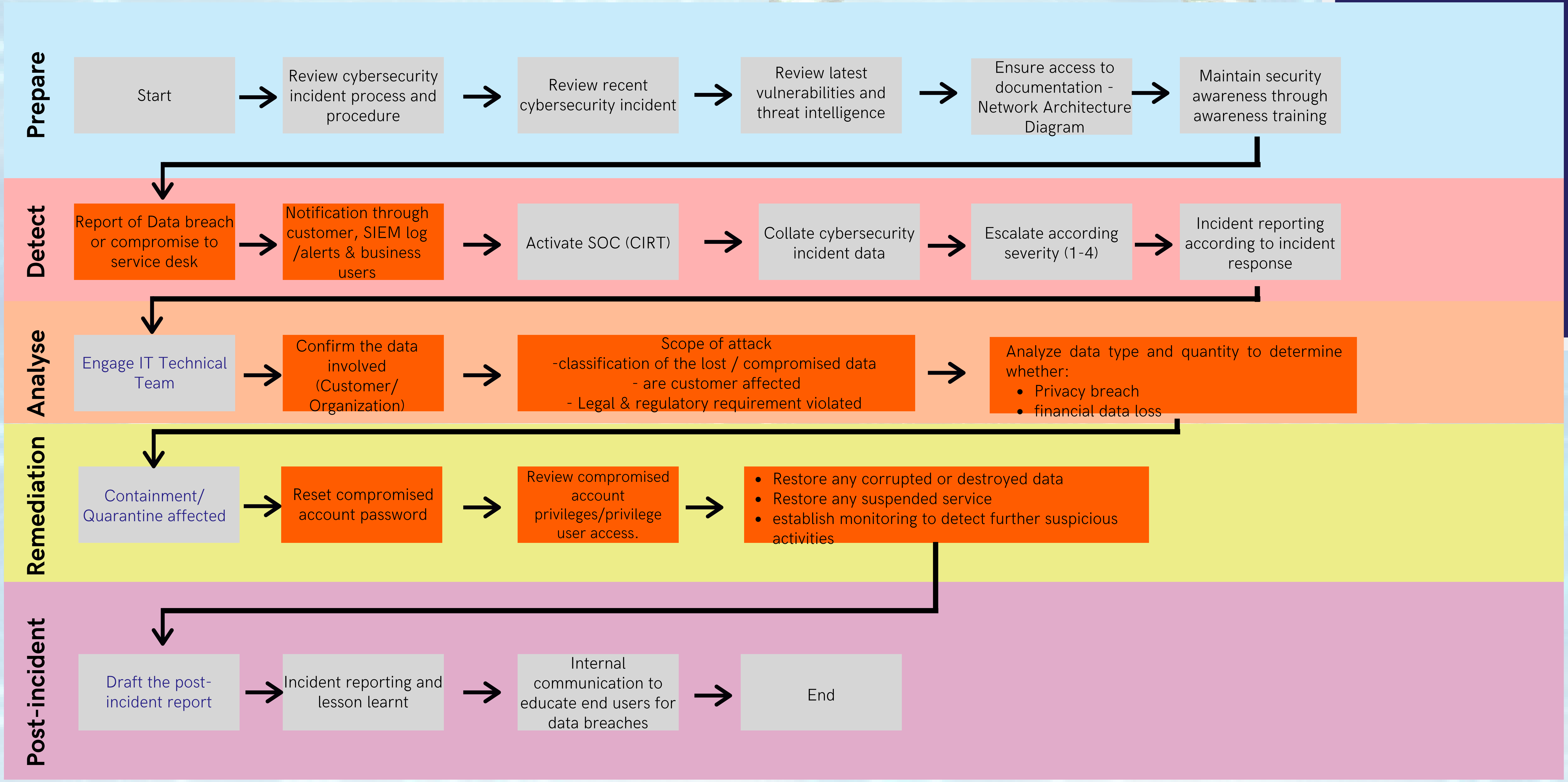
Post-incident

Draft the post-incident report → Incident reporting and lesson learnt → Internal communication to educate end users for phishing attacks → End

How do you HANDLE DATA BREACH?

The most important step to take after a data breach is to understand the root of the issue.

Then, it's important to begin notifying your employees and your customers of the breach. Problems such as these are best presented upfront and honestly.



Prepare

Start → Review cybersecurity incident process and procedure → Review recent cybersecurity incident → Review latest vulnerabilities and threat intelligence → Ensure access to documentation - Network Architecture Diagram → Maintain security awareness through awareness training

Detect

Report of Data breach or compromise to service desk → Notification through customer, SIEM log /alerts & business users → Activate SOC (CIRT) → Collate cybersecurity incident data → Escalate according severity (1-4) → Incident reporting according to incident response

Analyse

Engage IT Technical Team → Confirm the data involved (Customer/ Organization) → Scope of attack -classification of the lost / compromised data - are customer affected - Legal & regulatory requirement violated → Analyze data type and quantity to determine whether:

- Privacy breach
- financial data loss

Remediation

Containment/ Quarantine affected → Reset compromised account password → Review compromised account privileges/privilege user access. →

- Restore any corrupted or destroyed data
- Restore any suspended service
- establish monitoring to detect further suspicious activities

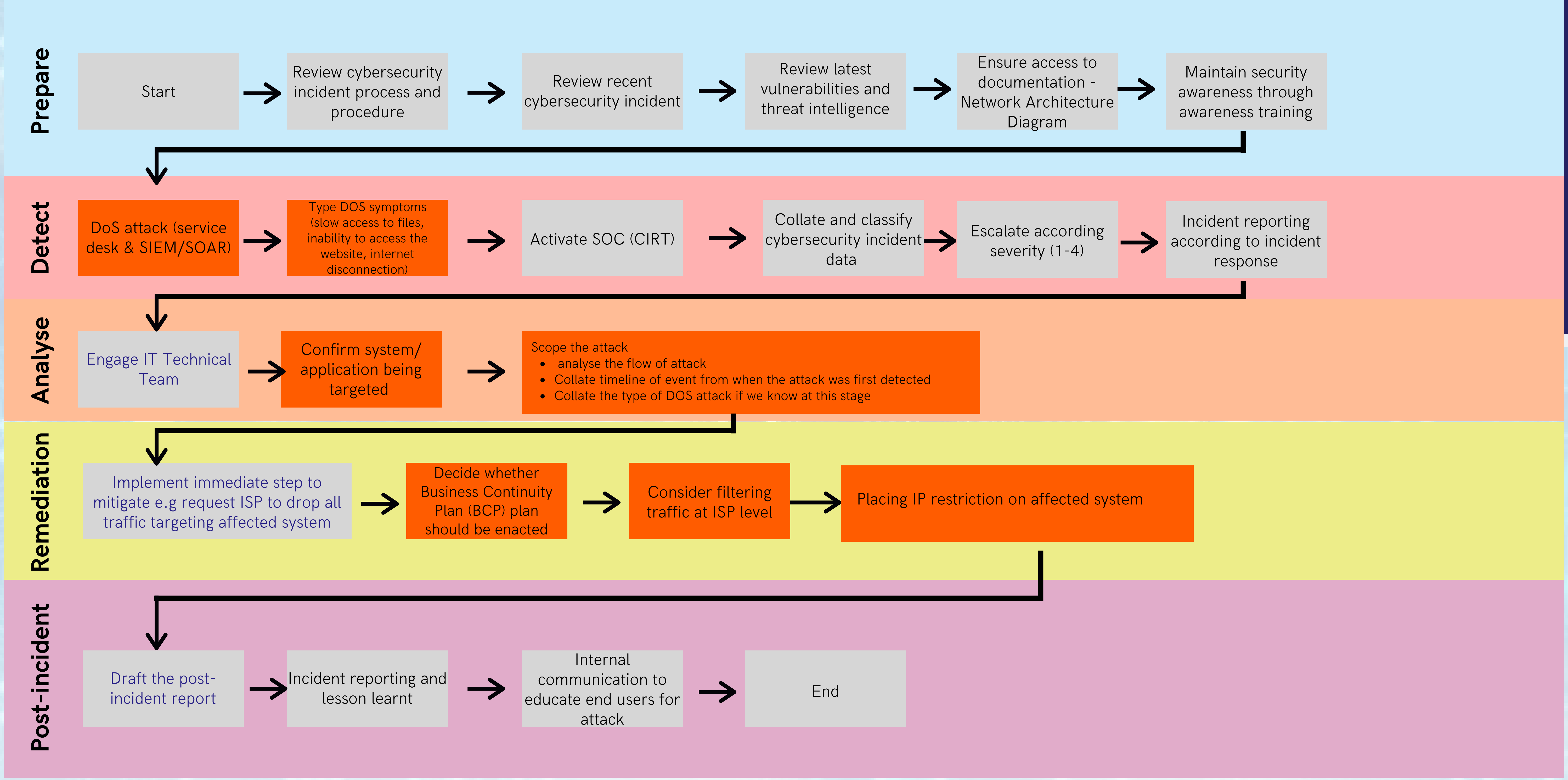
Post-incident

Draft the post-incident report → Incident reporting and lesson learnt → Internal communication to educate end users for data breaches → End

How do you HANDLE DoS ATTACK?

Recovering from a DDoS attack is no simple matter, but once an attack is over, it is important to do a thorough inventory of your systems and data.

Many times, DDoS attacks are used as a smokescreen for another, more sophisticated attack.



Prepare

Start → Review cybersecurity incident process and procedure → Review recent cybersecurity incident → Review latest vulnerabilities and threat intelligence → Ensure access to documentation - Network Architecture Diagram → Maintain security awareness through awareness training

Detect

DoS attack (service desk & SIEM/SOAR) → Type DOS symptoms (slow access to files, inability to access the website, internet disconnection) → Activate SOC (CIRT) → Collate and classify cybersecurity incident data → Escalate according severity (1-4) → Incident reporting according to incident response

Analyse

Engage IT Technical Team → Confirm system/ application being targeted → Scope the attack

- analyse the flow of attack
- Collate timeline of event from when the attack was first detected
- Collate the type of DOS attack if we know at this stage

Remediation

Implement immediate step to mitigate e.g request ISP to drop all traffic targeting affected system → Decide whether Business Continuity Plan (BCP) plan should be enacted → Consider filtering traffic at ISP level → Placing IP restriction on affected system

Post-incident

Draft the post-incident report → Incident reporting and lesson learnt → Internal communication to educate end users for attack → End

Prepared by:

Chairman of Cyber-Security Sub-Committee - Mr Leslie Yee, PIL

Vice-Chairman of Cyber Security Sub-Committee - Mr David Aw, PIL

Members Review:

Naveen Selvam, ABS Group

Duncan Ng, MSC

References:

1. NIST Cybersecurity Framework
2. BIMCO - The Guidelines on Cyber Security Onboard Ships
3. The Singapore Computer Emergency Response Team (SingCERT) - Report a Cyber-Incident to SingCERT
   To report an incident, please call the SingCERT hotline at 6323 5052. Alternatively, please email SingCERT at singcert@csa.gov.sg

Revision Date: June 2021

For any queries, please contact haniza@ssa.org.sg