

Patrocinan



Validated ID



Plan de Respuesta a Incidentes de Seguridad Informática (CSIRP)

Ponente

Gonzalo Cuatrecasas

Head of Cybersecurity at Axel Johnson International (CISO)

Barcelona, 28 de mayo de 2024

Suport Institucional



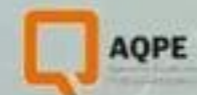
COL-LEGI OFICIAL
ENGINYERIA INFORMÀTICA
ILLES BALEARS



telecos.cat



Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1



Jornada conjunta



19/06/2024

Lloc

Seu de l'ICAB
Carrer Mallorca, 283
Barcelona

Agenda

10:00 – 11:30 Ponències
11:30 – 12:15 Pausa – Cafè
12:15 – 14:00 Ponències
14:00 – 15:30 Còctel i *networking*

Ponències

Programa pendent de tancar:
#Intel·ligència Artificial Responsable
#Novetats normatives: IA, NIS2, DORA...
#Digital Trust
#Auditoria de la IA
#Wallets d'identitat (eIDAS)

Gonzalo Cuatrecasas Freixas



Licenciado en Economía y con un MBA de la Universidad de Maryland;

Llevo 3 años como CISO en Axel Johnson International

Anteriormente 3 veces CIO con proyectos de Transformación Digital

15 años experiencia en Colgate Palmolive con varios cargos en sistemas, operaciones y 5 años como responsable de auditoría interna IT.

Certificaciones CISA, CISM y CGEIT

Colaborador con ISACA, OBS, Zigurat y ESADE



ISACA®

Barcelona Chapter



Una de las empresas de la familia Sueca Axel Johnson

Axel Johnson International es un conglomerado de empresas de componentes industriales con unas 200 PIMES en Europa y Asia Pacifico.

En España tenemos 4

AxFlow
Forankra
CYESA
ROYSE

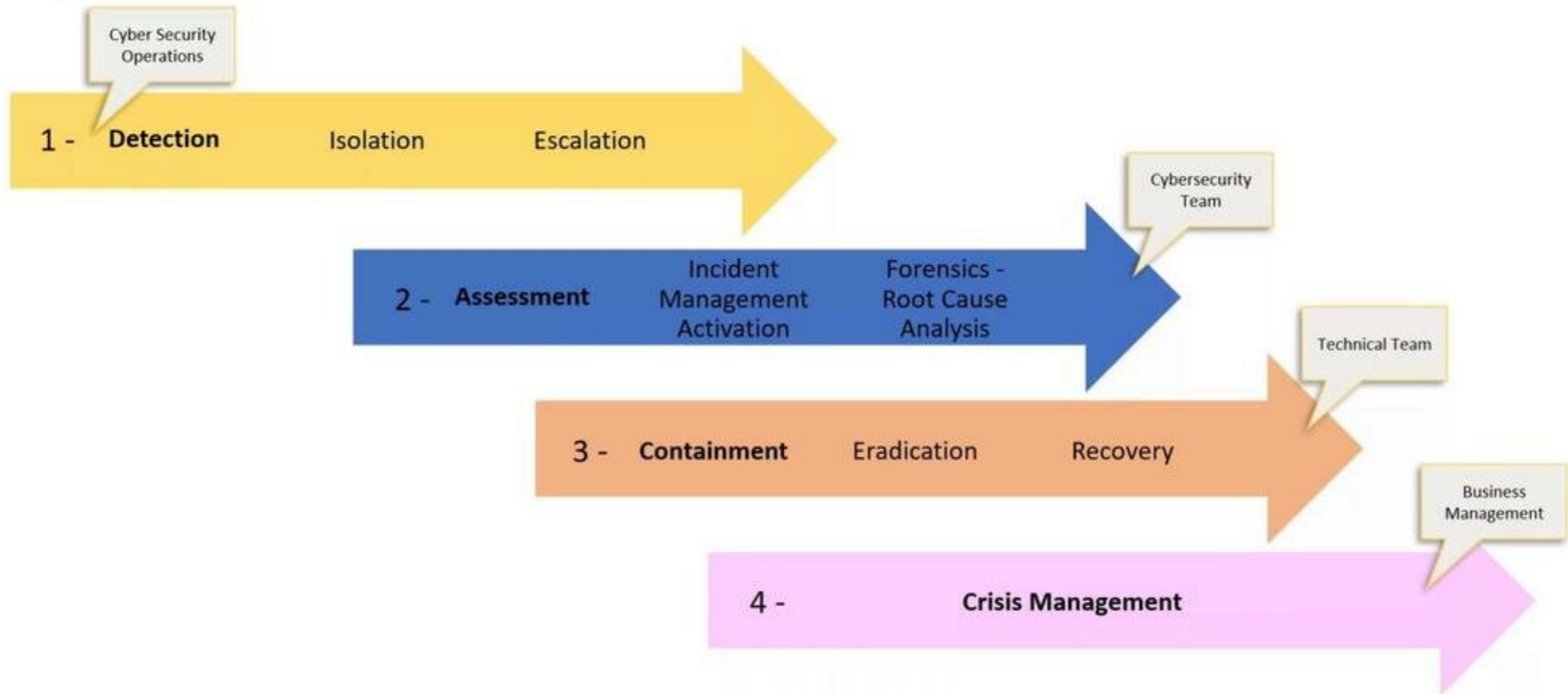
Las empresas que han planificado la respuesta a incidentes de seguridad cibernética (CSIRP) reaccionaran más rápidamente y de forma coordinada, facilitando la comunicación, limitando el alcance del ataque, acortando el tiempo de recuperación y asegurando que no haya recaídas.

Las organizaciones no pueden saber qué tipo de ciber-amenaza encontrarán, ni cuándo tendrá lugar. Por lo tanto, es vital elaborar un plan de acción, o una hoja de ruta flexible y adaptable, diseñada para usarla remotamente.

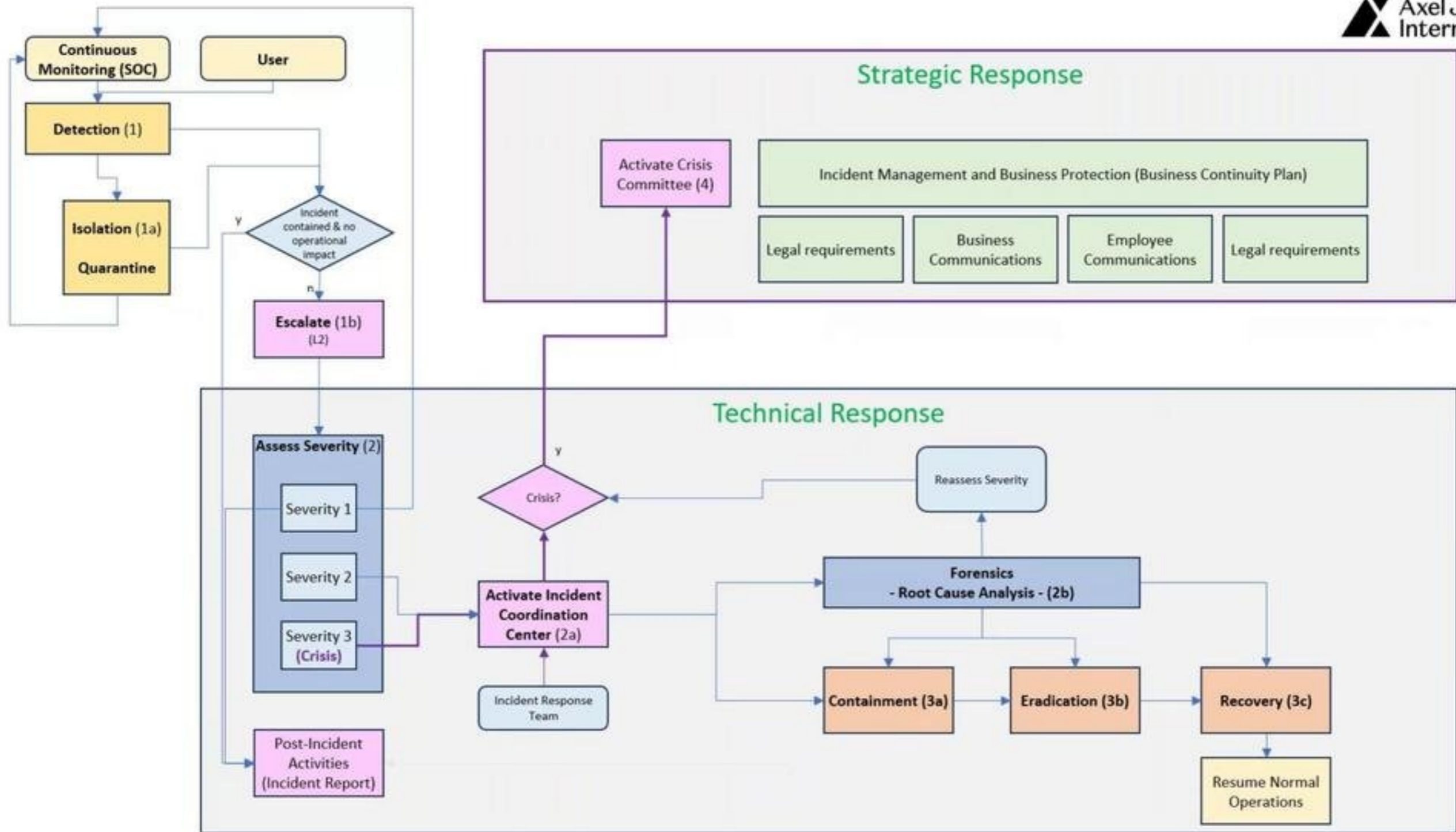
Aquí es donde entra en juego la planificación de respuesta a incidentes de seguridad cibernética.

“A breach is always an incident,
but not all incidents are breaches”.

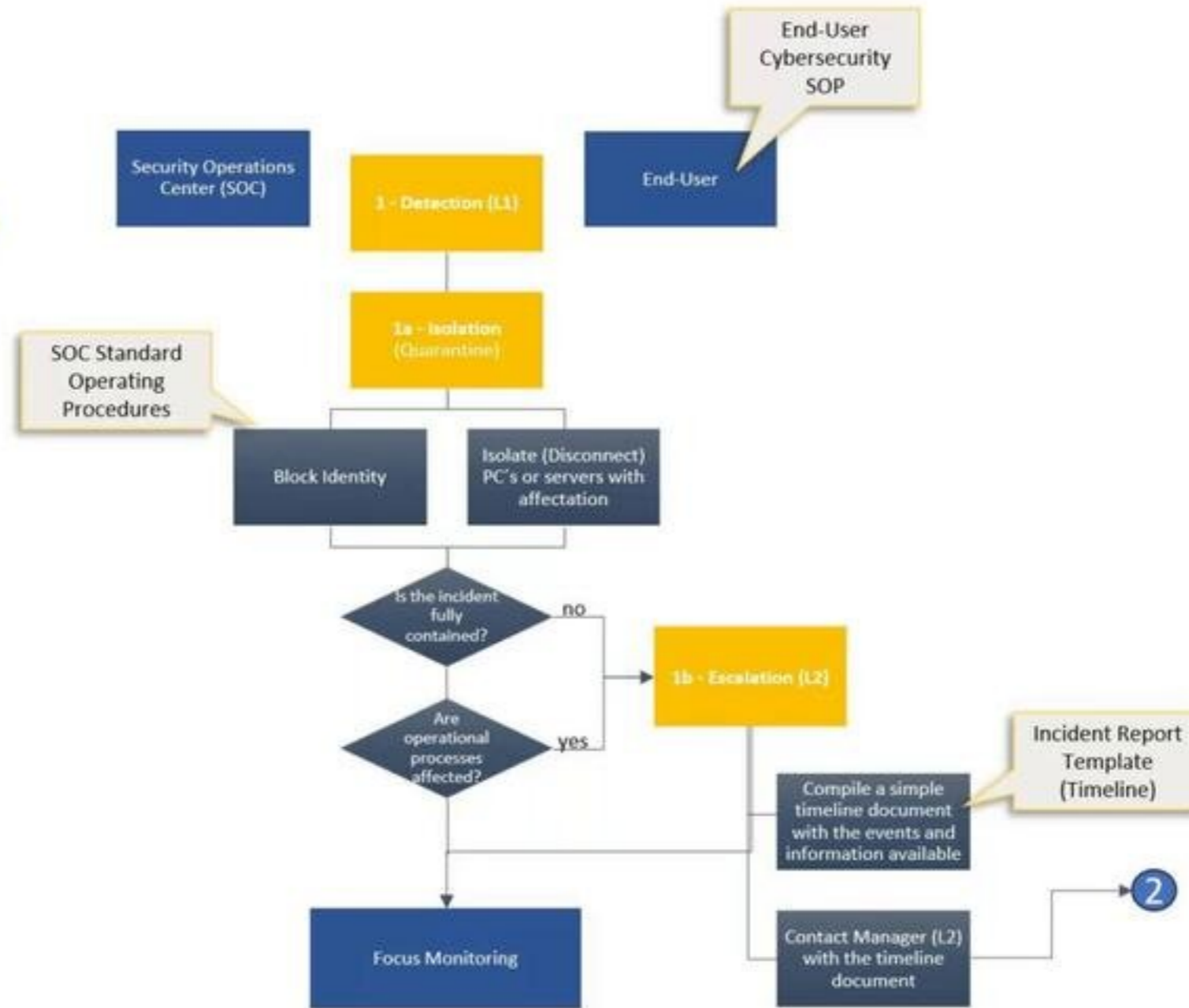
Cybersecurity Breach Response Process



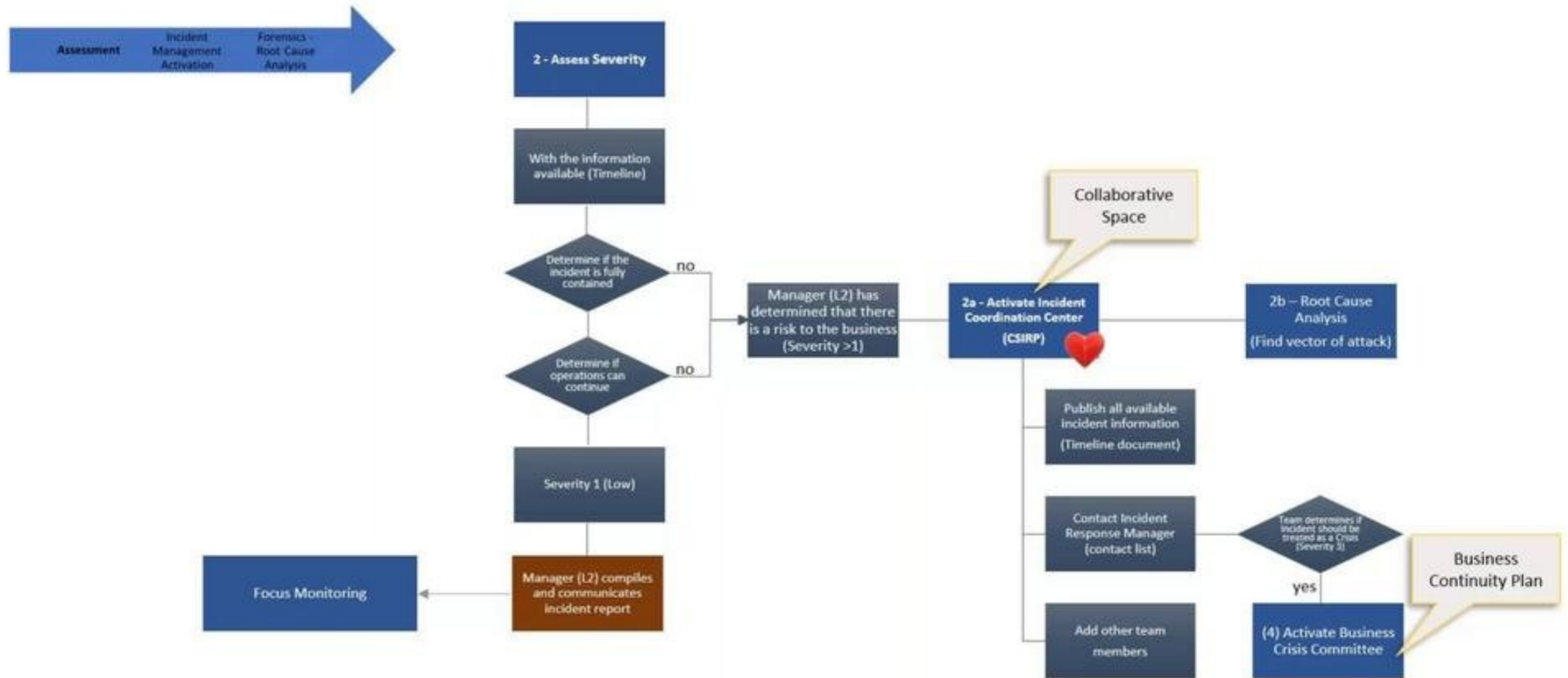




1- Detection



2 – Cybersecurity Assessment



Cybersecurity Incident Coordination Center

Collaborative
Space 

0- Classified Info

[Contact List](#)

[Network Map](#)

[Server Inventory](#)

1- Security
Operations

Monitoring

Logs

2- Forensics

Timeline

3- Technical &
Recovery

Laundry List

[Mass Password-Change procedure](#)

4- Business
Continuity

HR

Legal

Insurance

Communications

5- Report

Incident report

Learnings



▼ Your teams

-  Cyber Security
-  Cyber Security incident Coordination...

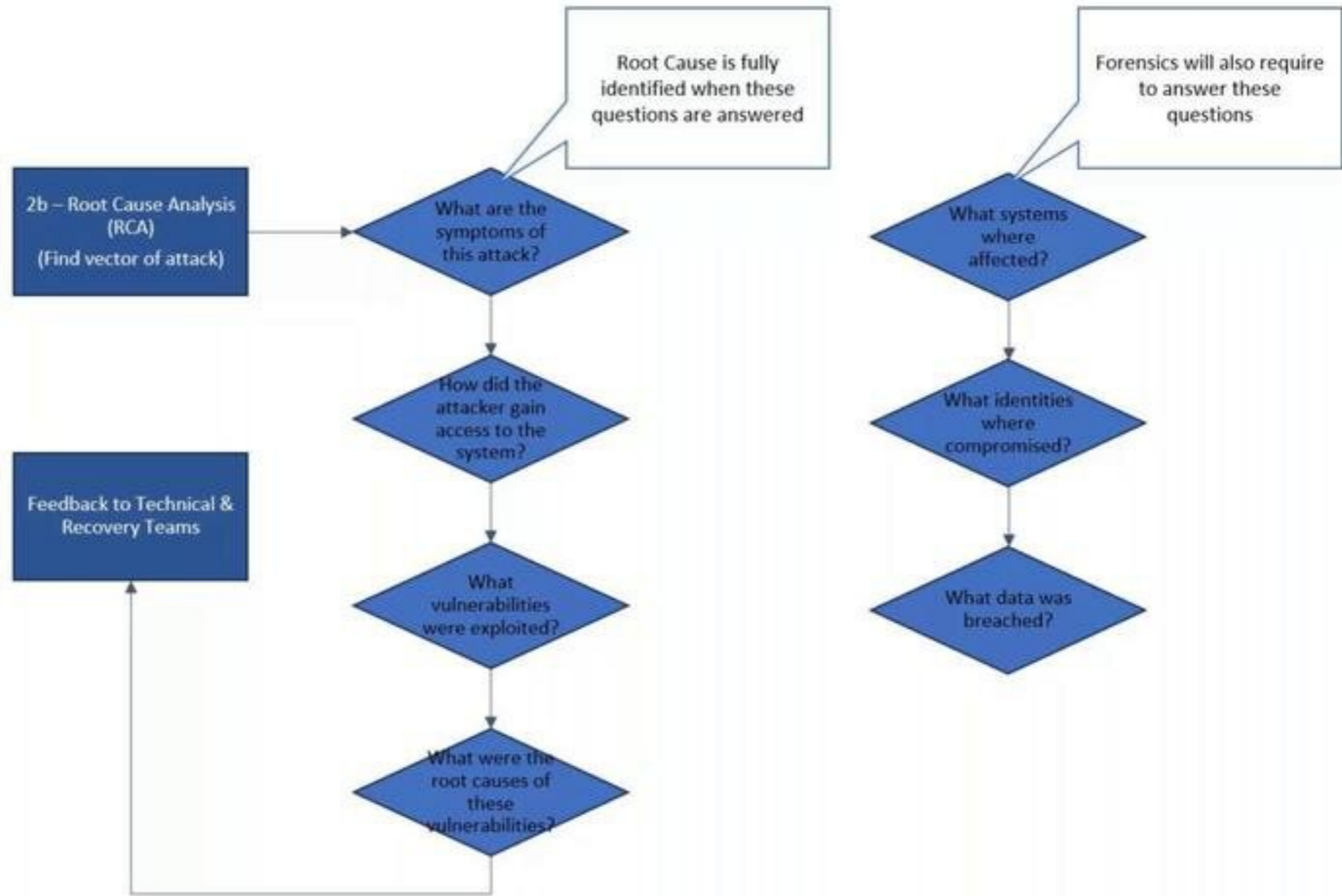
General

- 0- Classified Information 
- 1- Security Operations
- 2- Forensics 
- 3- Technical and Recovery
- 4- Business Continuity
- 5- Incident Report 

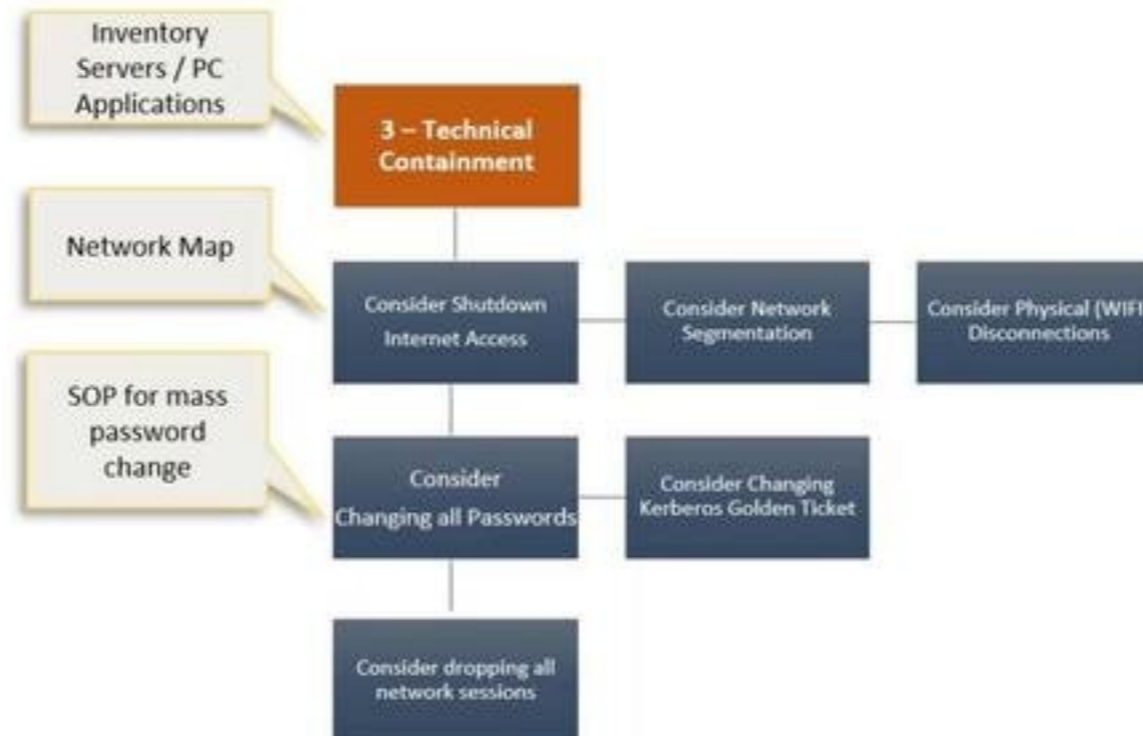
2b – Forensics



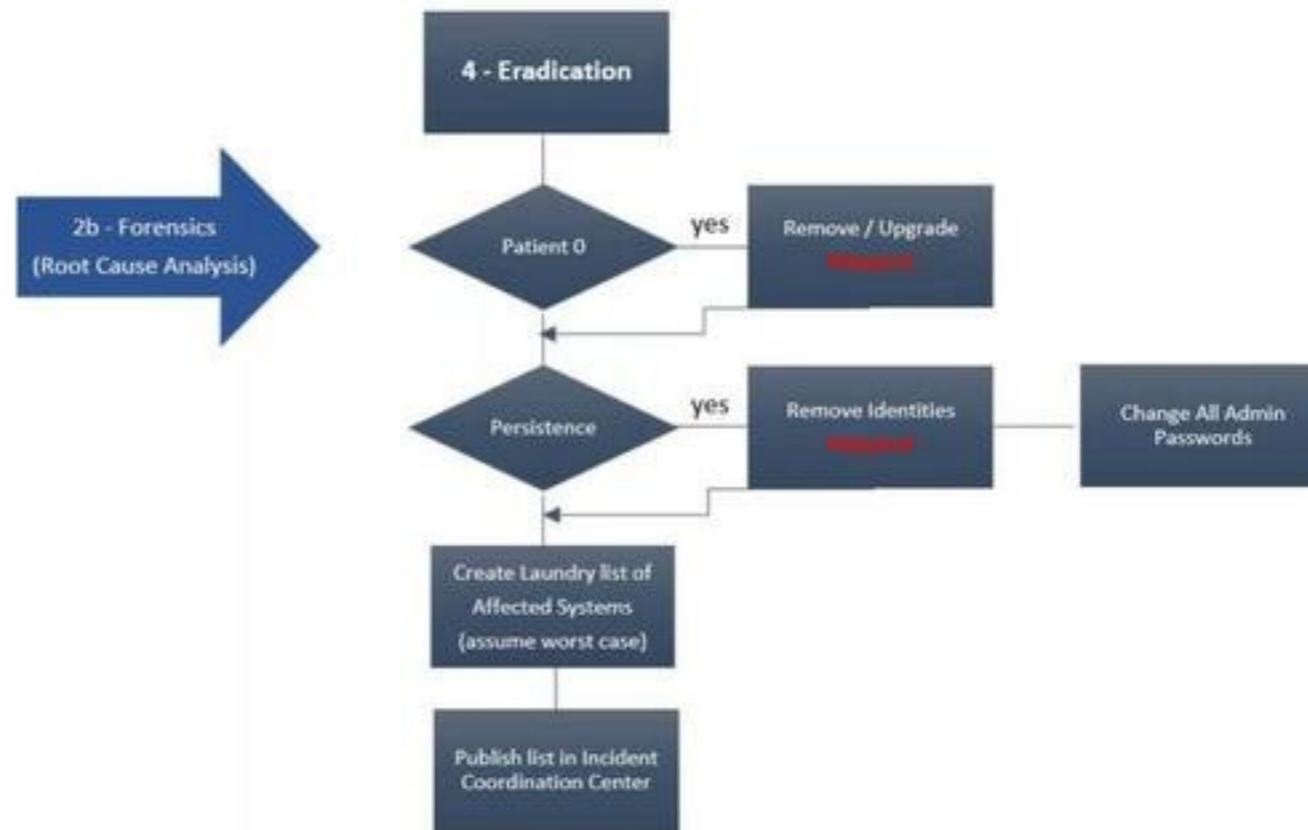
2b – Forensics



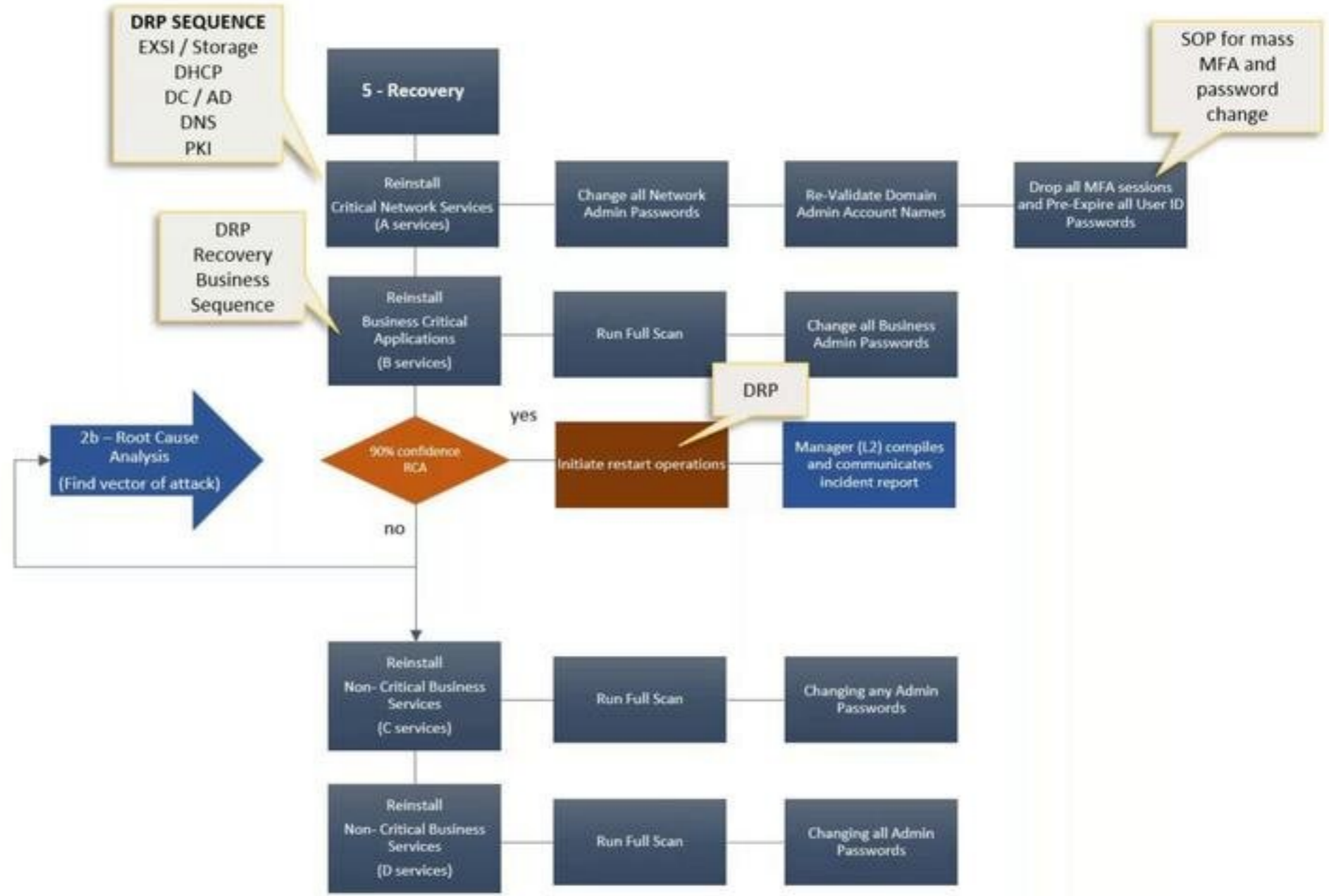
3 – Containment (Avoid spread or further damage)



4 – Eradication (Comfort that infection has been removed)



5 – Recovery



Q & A