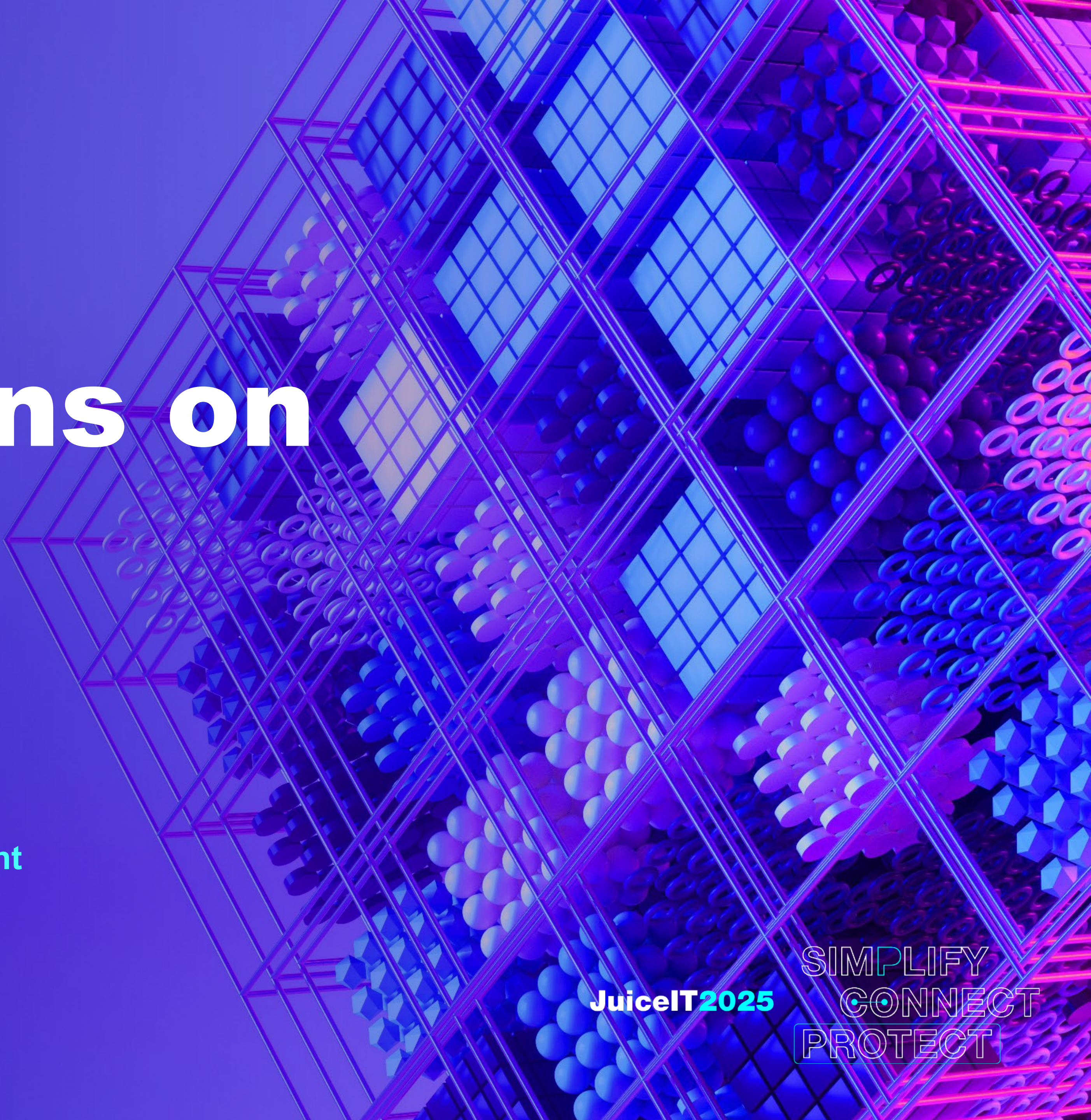
Data#3

What Happens on Day 2

Richard Dornhart

National Practice Manager – Security, Data#3

Confidential – Do not share without prior consent

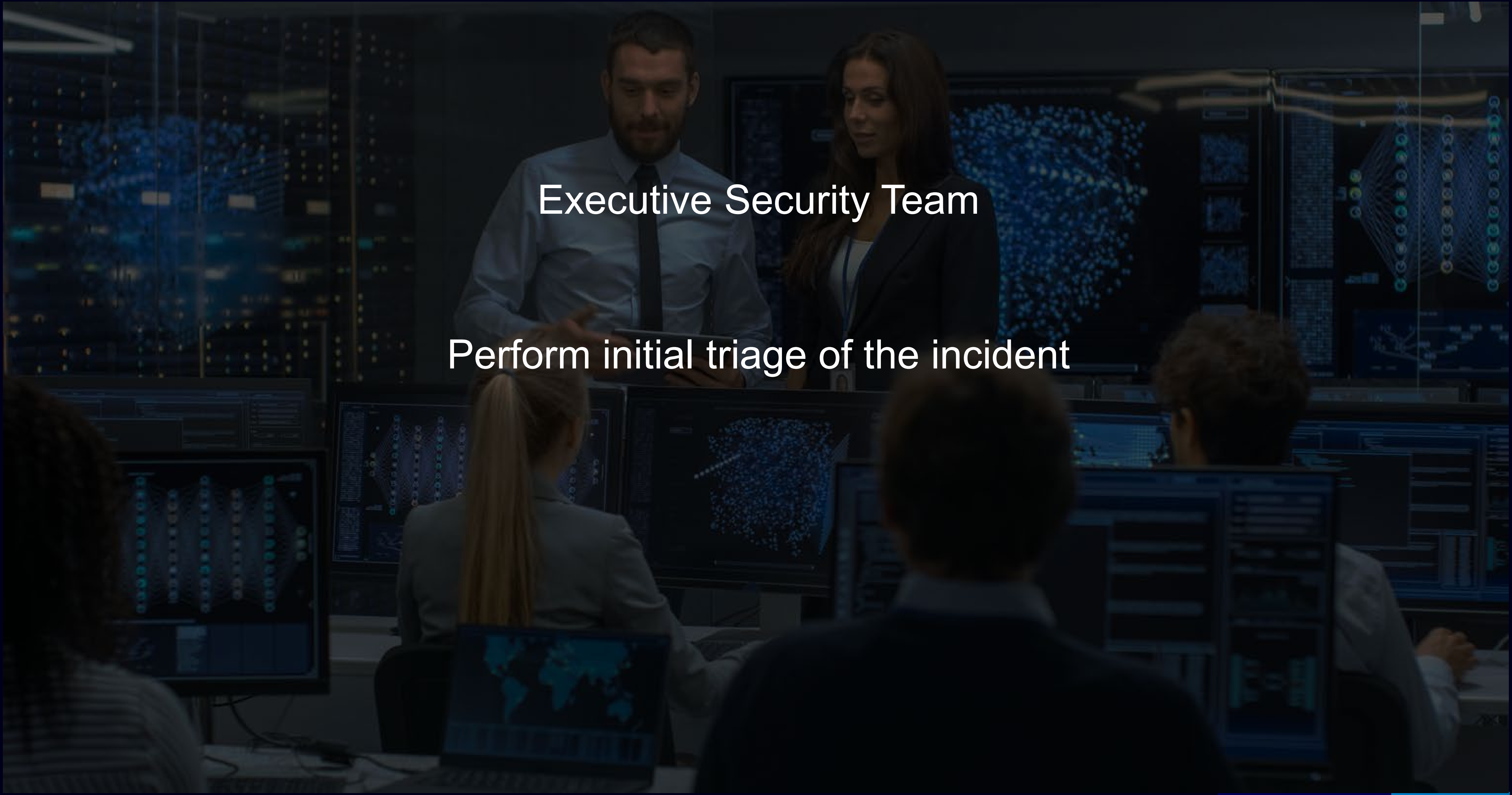


JuiceIT2025

SIMPLIFY
CONNECT
PROTECT

In Our World...

RANSOMWARE



Executive Security Team

Perform initial triage of the incident

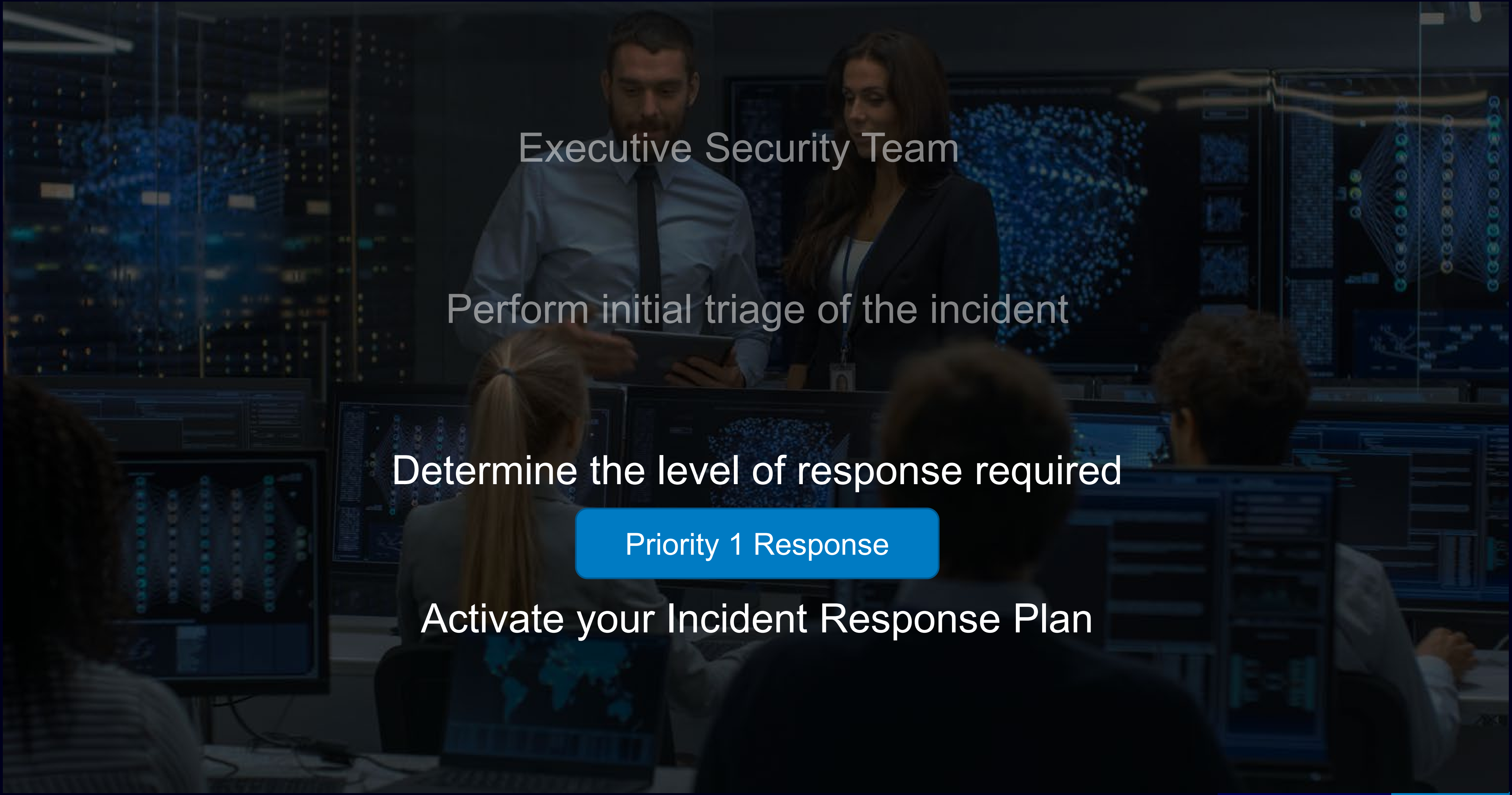
Perform initial triage of the incident

Compromised Credentials

Unauthorised Access and Lateral Movement

Data Exfiltration

Active Web Shells



Executive Security Team

Perform initial triage of the incident

Determine the level of response required

Priority 1 Response

Activate your Incident Response Plan

KEEP
CALM

What happens on day two?

People

Containment

Get Organised

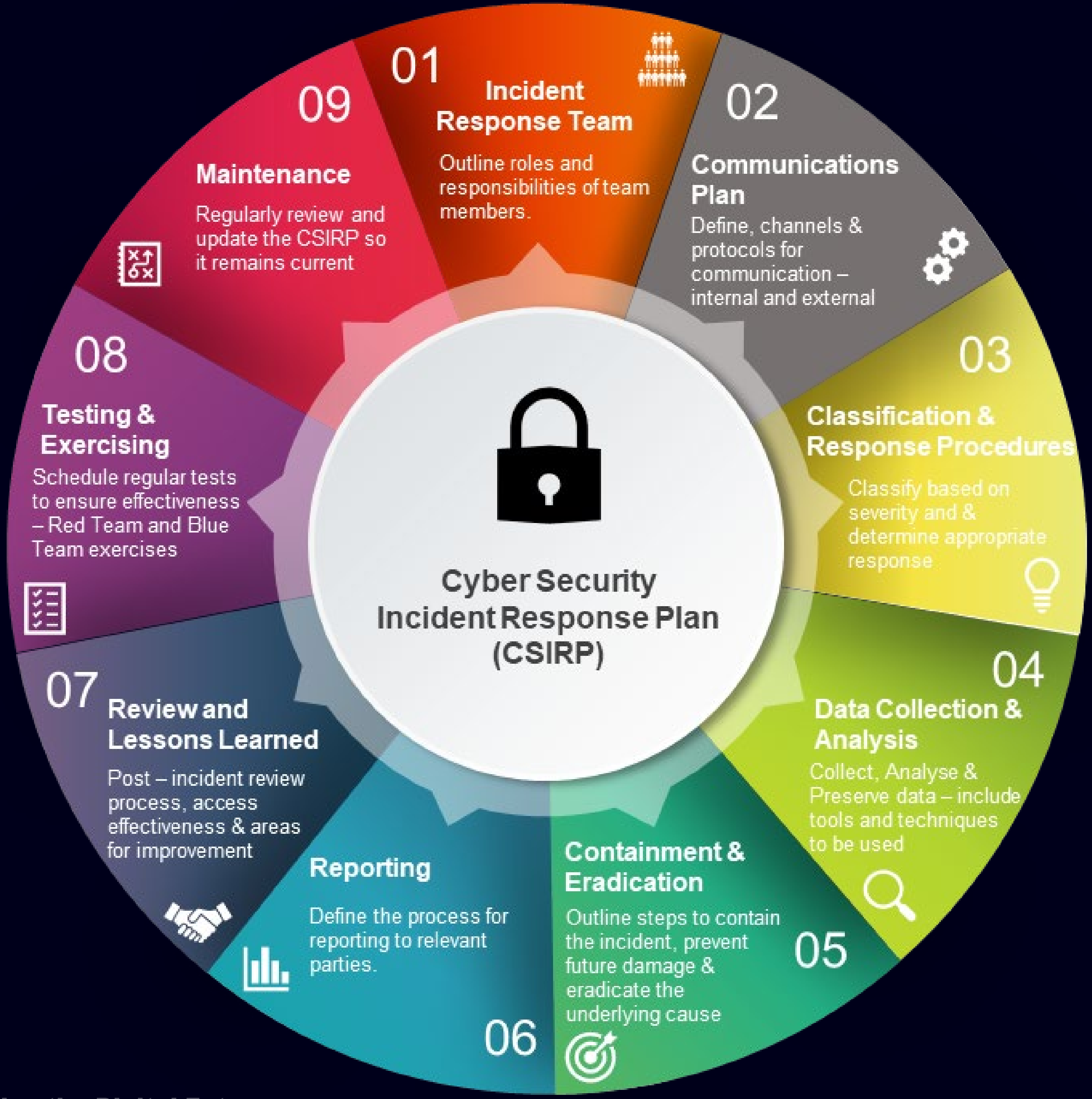
3rd Parties

Communication

Logging

The Plan

The Plan
Is to have a
Plan
Before you need a
Plan



Cyber Security Incident Response Plan (CSIRP)

01 **Incident Response Team**
Outline roles and responsibilities of team members.

02 **Communications Plan**
Define, channels & protocols for communication – internal and external

03 **Classification & Response Procedures**
Classify based on severity and & determine appropriate response

04 **Data Collection & Analysis**
Collect, Analyse & Preserve data – include tools and techniques to be used

05 **Containment & Eradication**
Outline steps to contain the incident, prevent future damage & eradicate the underlying cause

06 **Reporting**
Define the process for reporting to relevant parties.

07 **Review and Lessons Learned**
Post – incident review process, access effectiveness & areas for improvement

08 **Testing & Exercising**
Schedule regular tests to ensure effectiveness – Red Team and Blue Team exercises

09 **Maintenance**
Regularly review and update the CSIRP so it remains current

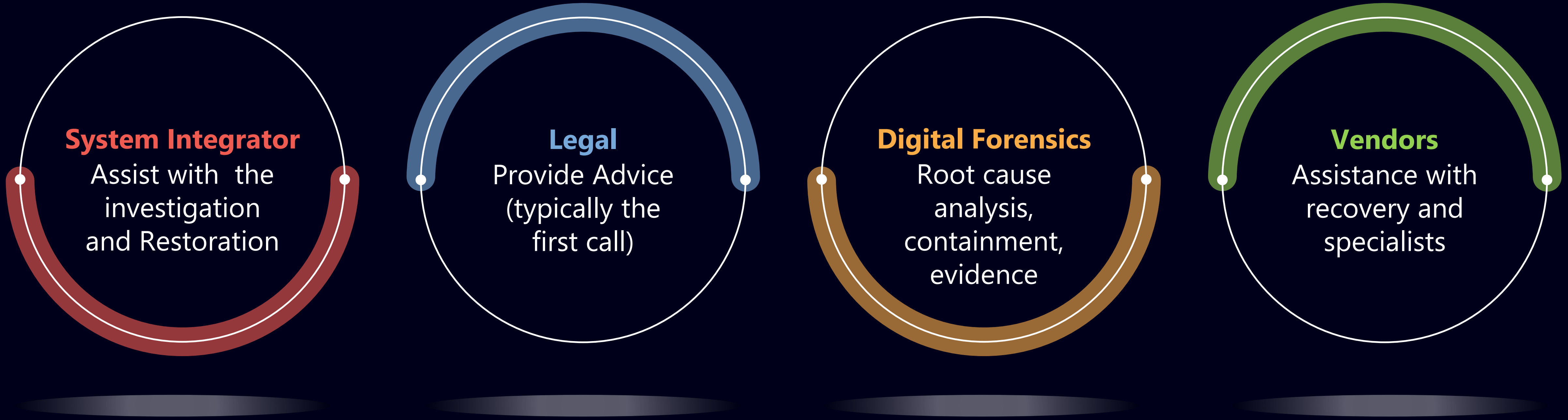
People

Process

Technology

3rd Parties & Partners

3rd Parties and Partners



System Integrator
Assist with the investigation and Restoration

Legal
Provide Advice (typically the first call)

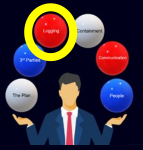
Digital Forensics
Root cause analysis, containment, evidence

Vendors
Assistance with recovery and specialists

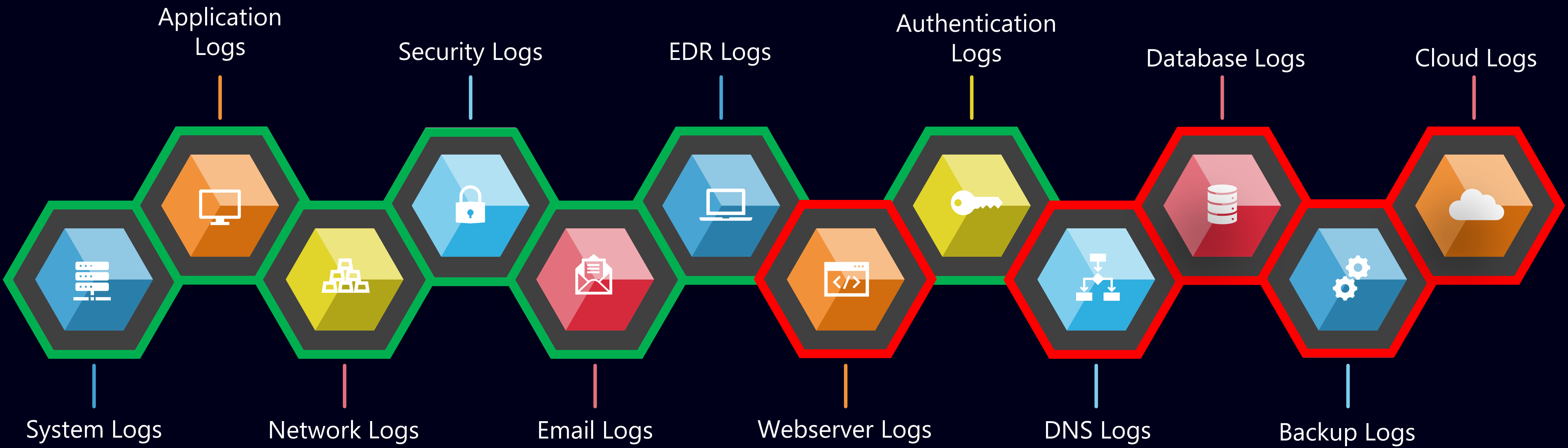
Questions to be prepared for from your partners

What is the nature of the incident?	This includes the type of attack, the data or systems that are affected, and any known impacts to your organisation.
When did the incident occur?	Establishing a timeline of the incident can help the DFIR team determine the scope of the incident and identify key events that took place.
Have you taken any actions already? If so what?	The DFIR team needs to know if any remediation steps have already been taken to prevent further damage or loss of data.
Who has access to the affected systems?	Understanding who has access to the systems that are affected by the incident can help the DFIR team determine the potential scope of the breach.
Have any backups been made?	Knowing if backups have been made can help the DFIR team determine if there is an opportunity to recover data that was lost or impacted during the incident.
Have you notified any regulatory or legal authorities?	Have you notified any regulatory or legal authorities? Depending on the nature and severity of the incident, there may be legal or regulatory requirements to report the incident.
What systems and networks are affected?	The DFIR team will need to know what systems, networks, and applications are involved in the incident in order to determine the extent of the compromise.
Have any files been deleted or encrypted?	If files or data have been deleted or encrypted, the DFIR team may need to recover the data in order to investigate the incident further.
Have any changes been made to systems or configs?	Knowing if any changes have been made to the systems or configurations can help the DFIR team determine if the attacker has altered the environment in any way.
Have any new accounts or devices been added?	Understanding if new accounts or devices have been added to the network can help the DFIR team determine if the attacker has established a foothold within the environment.
Have any logs or monitoring systems been tamper with?	Knowing if logs or monitoring systems have been tampered with can help the DFIR team determine if the attacker has attempted to conceal their activities.
Have you identified any indicators of compromise (IOC)?	If you have identified any indicators of compromise (IOCs), such as suspicious IP addresses or file hashes, the DFIR team may use this information to help track down the source of the attack.

Logs



A Plan for Logging



Application Logs

Security Logs

EDR Logs

Authentication Logs

Database Logs

Cloud Logs

System Logs

Network Logs

Email Logs

Webserver Logs

DNS Logs

Backup Logs

01 Incident Response Team
02 Communications Plan
03 Classification & Response Procedures
04 Data Collection & Analysis
05
06 Containment & Eradication
Reporting
07 Review and Lessons Learned
08 Testing & Exercising
09 Maintenance
Cyber Security Incident Response Plan (CSIRP)

A Plan for Logging

Audit File and Folder Access for Sensitive Data

Keep your logs for as long as possible – Minimum 12 months

Investigate Investing in a SOC Service

Cyber Security Incident Response Plan (CSIRP)
01 Incident Response Team
02 Communications Plan
03 Classification & Response Procedures
04 Data Collection & Analysis
05 Containment & Eradication
06 Reporting
07 Review and Lessons Learned
08 Testing & Exercising
09 Maintenance

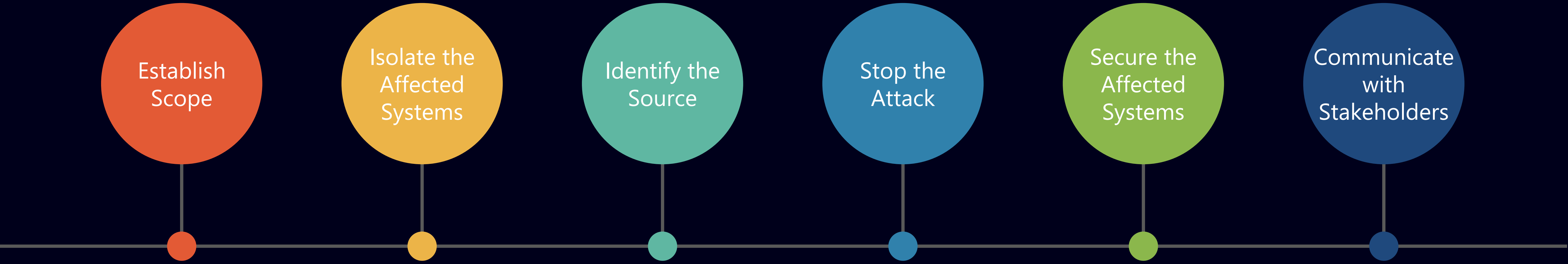
System logs need to be protected to preserve their integrity

Should be accessible only by security staff

Should be backed up to allow forensic analysis if there is an incident

Containment

A Plan for Containment



Establish Scope

Isolate the Affected Systems

Identify the Source

Stop the Attack

Secure the Affected Systems

Communicate with Stakeholders

Cyber Security Incident Response Plan (CSIRP)
01 Incident Response Team
02 Communications Plan
03 Classification & Response Procedures
04 Data Collection & Analysis
05 Containment & Eradication
06 Reporting
07 Review and Lessons Learned
08 Testing & Exercising
09 Maintenance

A Plan for Containment

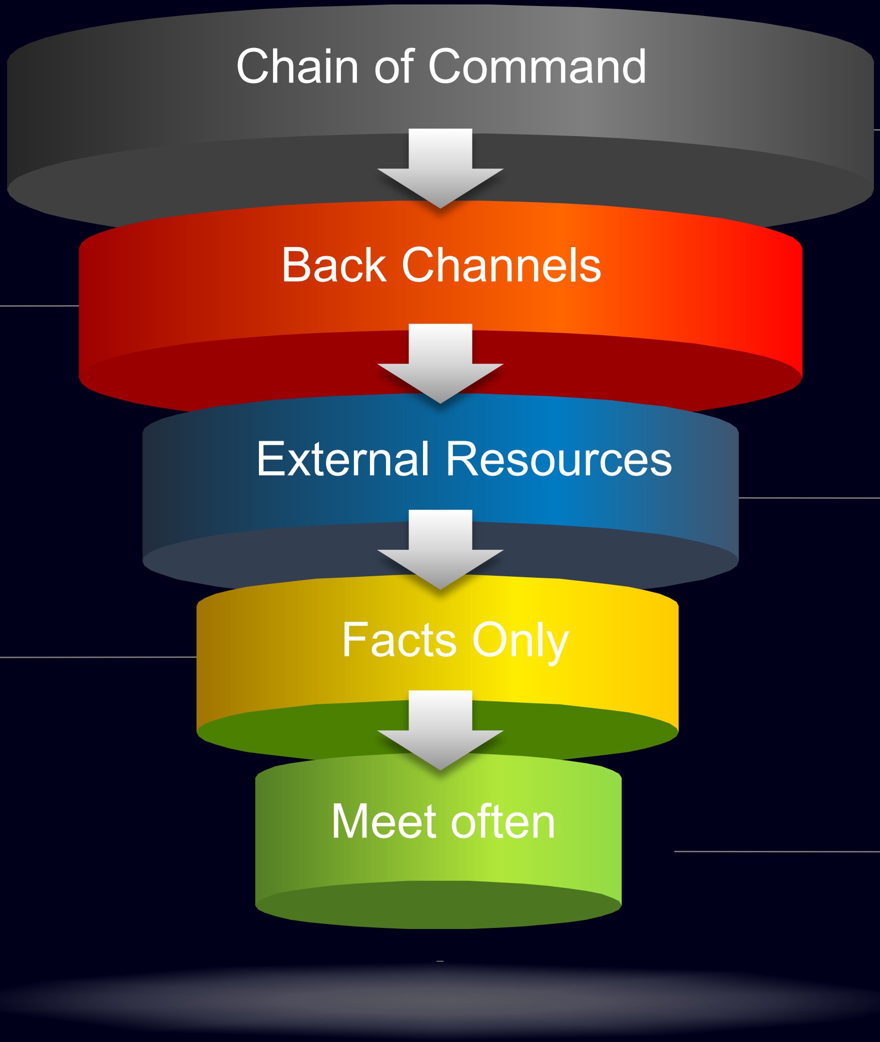
- Enterprise Detection and Response (EDR)
- Security Operations Centre (SOC)
- Education and Training

Communication

01
Incident Response Team
02
Communications Plan
03
Classification & Response Procedure
04
Data Collection & Analysis
05
Containment & Eradication
06
Reporting
07
Review and Lessons Learned
08
Testing & Exercising
09
Maintenance
Cyber Security Incident Response Plan (CSIRP)

Logging
Containment
3rd Parties
Communication
The Plan
People

Structured Communication is Essential



All communications should be funneled through a central point of contact.

Have communication back channels ready No communication silos

WhatsApp

Signal

Messenger

Engage your DFIR or external legal advisory about how and when to communicate

Stick to the facts. It is ok to say, “I do not have any evidence”. People will push you.

Through out the incident meet with key stakeholders often to update them on the communication strategy

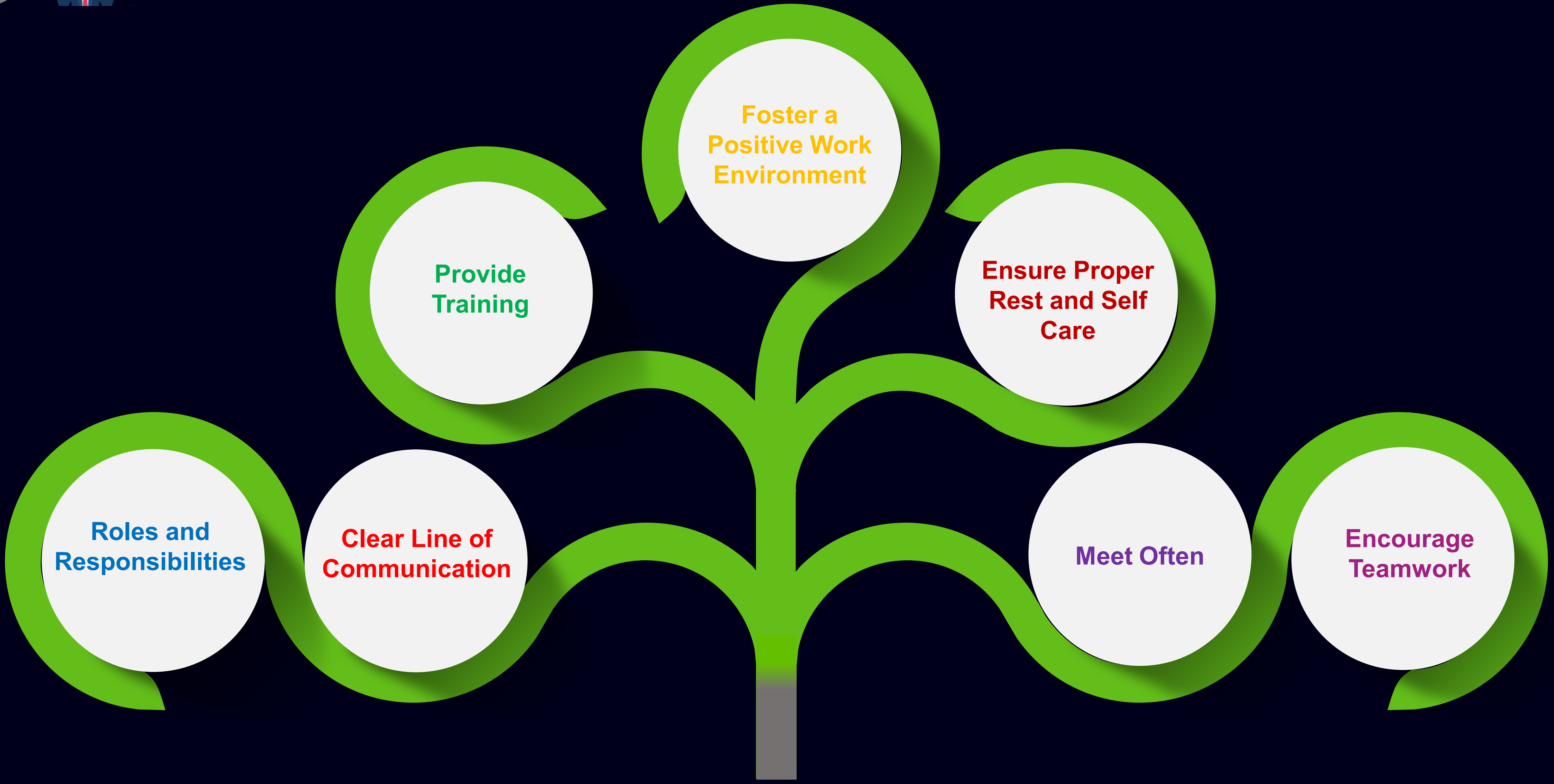
People

No one can whistle a symphony.

It takes a whole orchestra to play it.

H.E. Luccock

Staff Management and Morale



Roles and Responsibilities

Clear Line of Communication

Provide Training

Foster a Positive Work Environment

Ensure Proper Rest and Self Care

Meet Often

Encourage Teamwork

The Plan

Is to have a

Plan

Before you need a

Plan

People

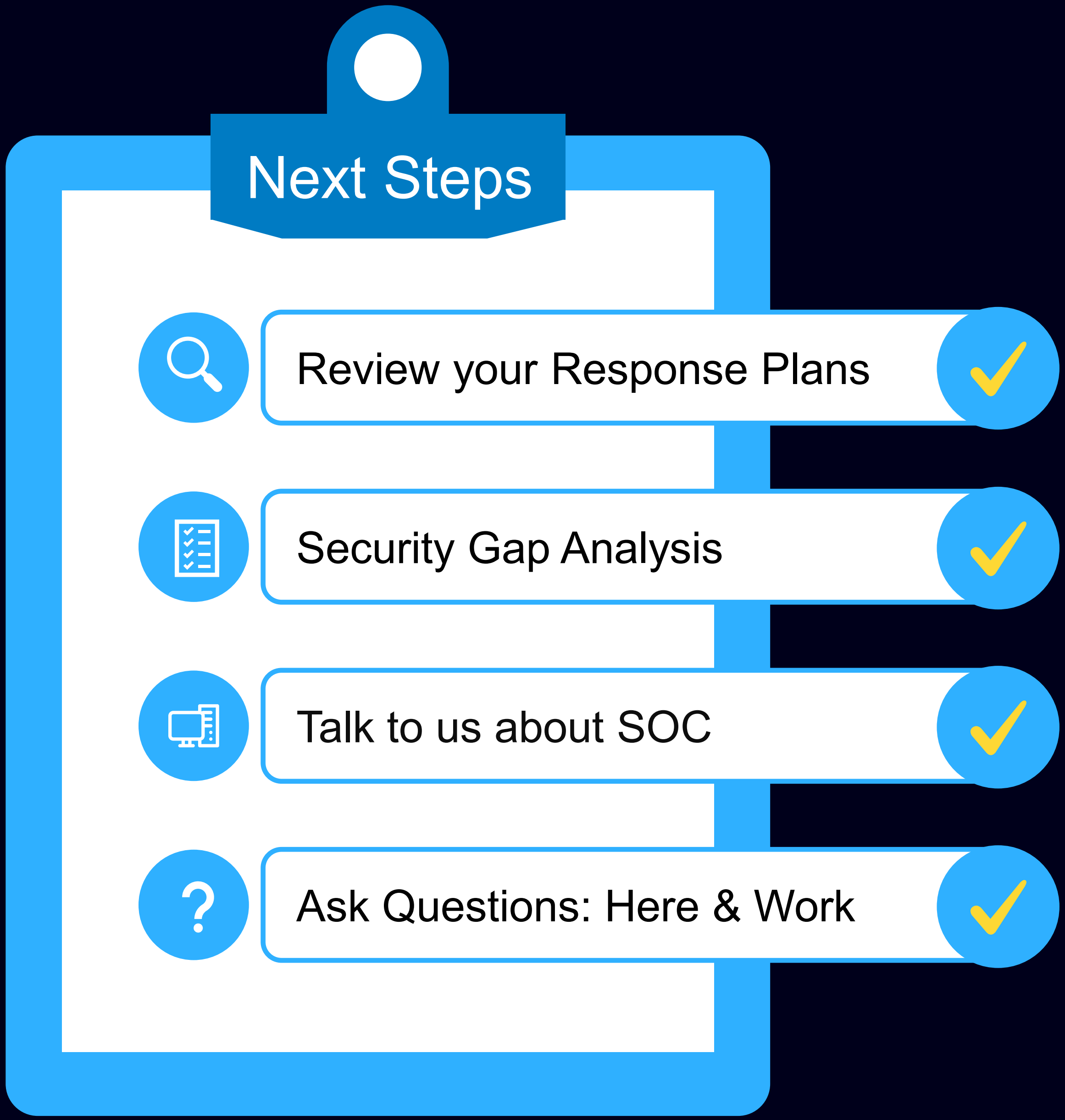
Containment

Get Organised

3rd Parties

Communication

Logging



Next Steps

- Review your Response Plans ✓
- Security Gap Analysis ✓
- Talk to us about SOC ✓
- Ask Questions: Here & Work ✓

Thank You

Data#3

www.data3.com.au

1300 23 28 23

Linkedin.com/company/data3

Twitter.com/data3limited

Facebook.com/data3limited

YouTube.com/data3limited