Cybercrime Incident Handling and Response Strategies

by

Kenneth Okereafor, PhD

www.cyberken.ng
+234-802-314-8494
nitelken@yahoo.com

A Presentation at the Cybercrime Detection and Forensic Investigation Workshop, Organized by the Nigeria Computer Society (NCS), 26th – 28th May, 2021. Abuja, NIGERIA.

Outline

1. Agenda
2. Cybercrime Concept
3. Cybersecurity overview
4. The CIA
5. Access Control
6. Security Goals
7. Event vs Incident
8. Incident Response (IR), Handling and Management
9. IR Steps
10. IR Reporting
11. Practical Scenarios
12. Conclusions

CYBERCRIME CONCEPT

- Criminal activity in the cyber domain, involving:
- Targeting computer and data networks
- Using digital assets and online resources
- Aided by computing technology
- Security, financial, operational, health impacts.

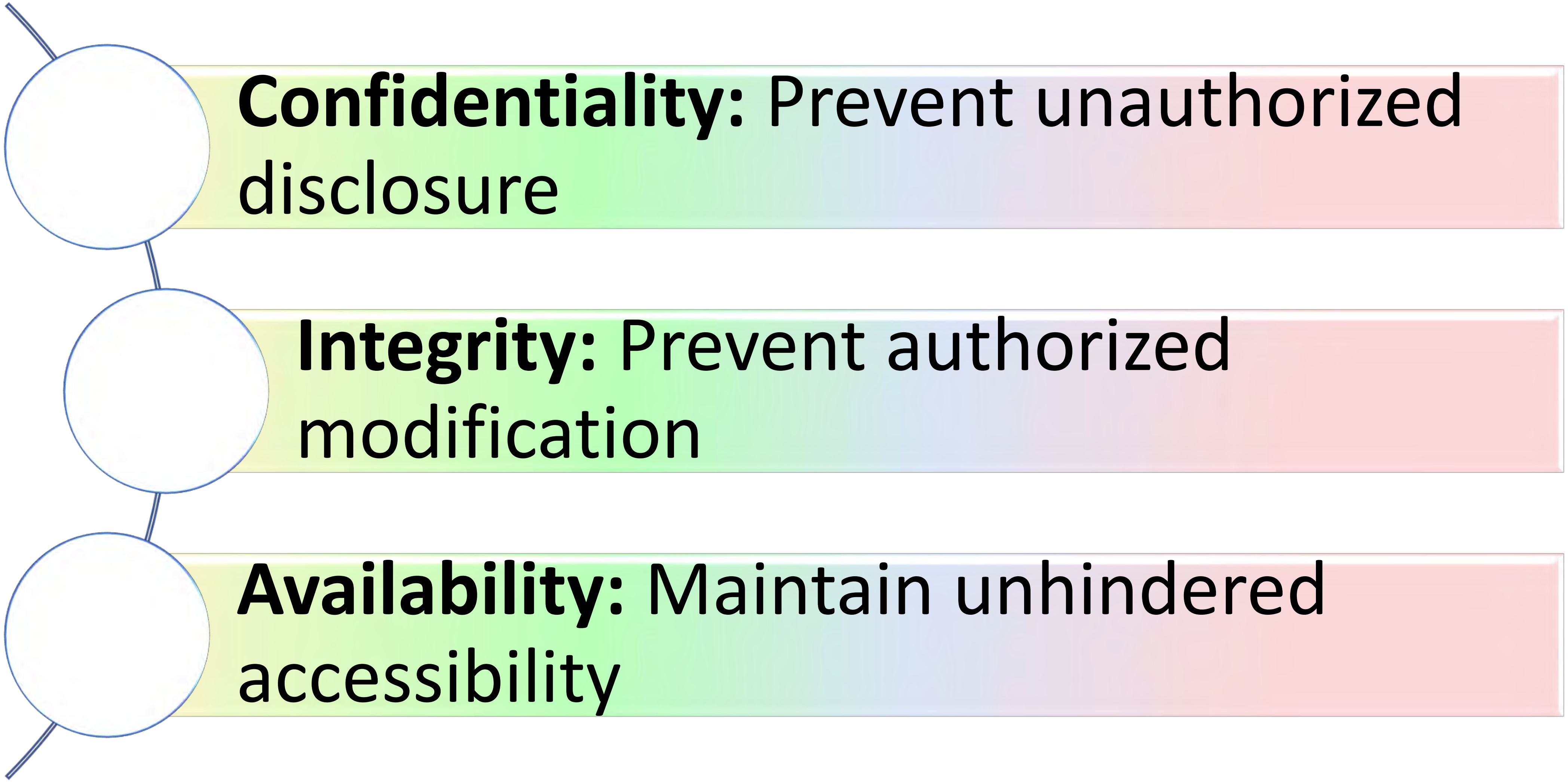
CYBERATTACK TYPES AND INCIDENTS

Malware: (Adware, Spyware, etc)	Ransomware	Computer virus	DDoS
Insider Attacks (Collusion)	Illegal data alteration	Credential racketeering	Email phishing
Man-in-the-middle	Cyber espionage	Cyber bullying	Social Engineering
Password attack	Website hijack	Site cloning	Click-jacking
Identity theft	Data Theft	Unauthorized information disclosure	Credential racketeering

CYBERSECURITY OVERVIEW

- Protection against misuse and abuse of computers
- Measures, policies to control cyberattacks
- Defence of digital assets and info systems
- Preventing unauthorised exploitation of systems
- Investigating abuse of computer systems
- Creating awareness on cyberspace safety and ethical computing

CYBERSECURITY FUNDAMENTALS (1)
THE CIA



Confidentiality: Prevent unauthorized disclosure

Integrity: Prevent authorized modification

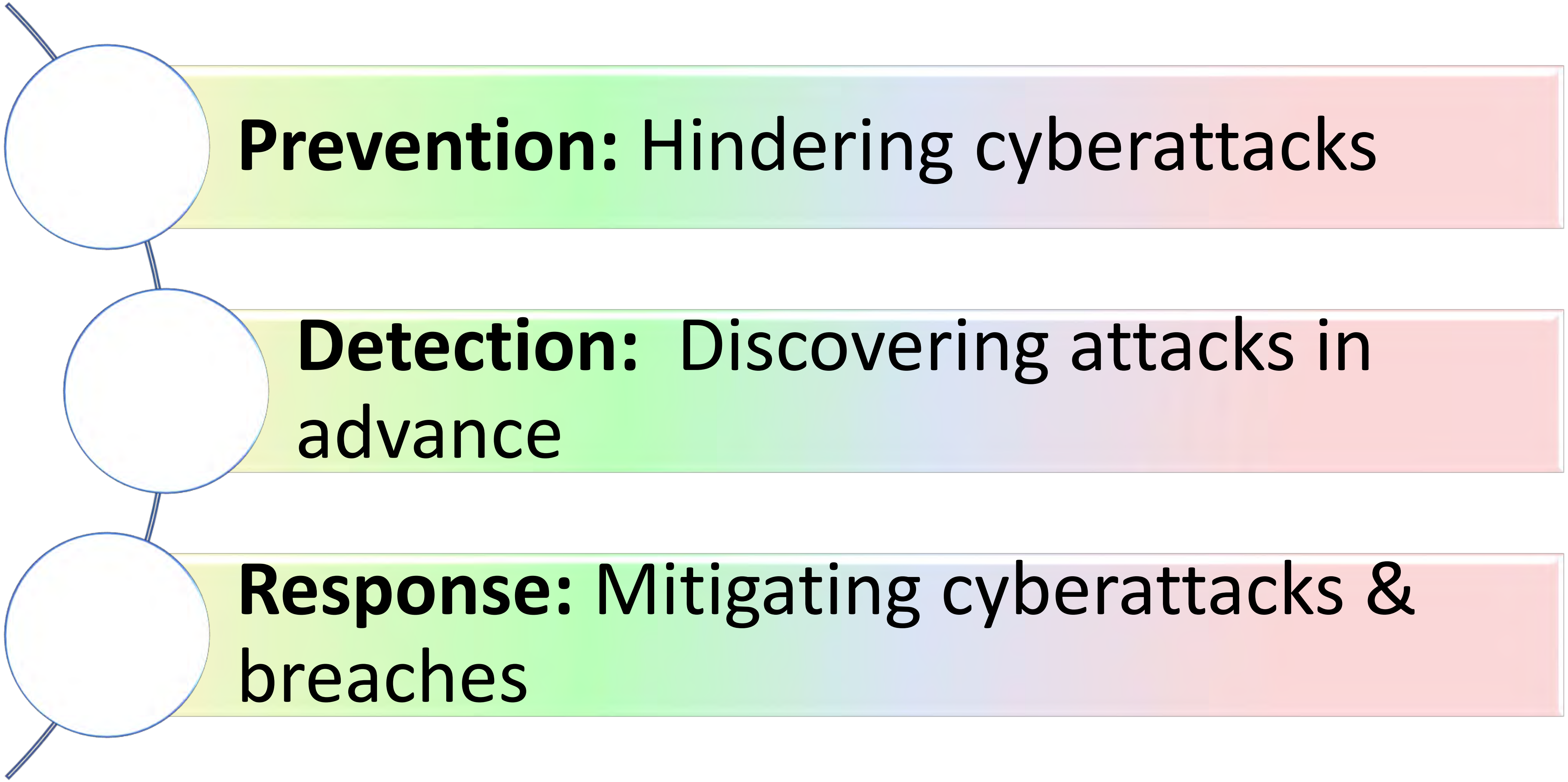
Availability: Maintain unhindered accessibility

CYBERSECURITY FUNDAMENTALS (2)

ACCESS CONTROL

- **Authentication:** Verifying user identities
- **Authorization:** Assigning roles to users
- **Accounting:** Tracking activities of users

CYBERSECURITY FUNDAMENTALS (3)
SECURITY GOALS

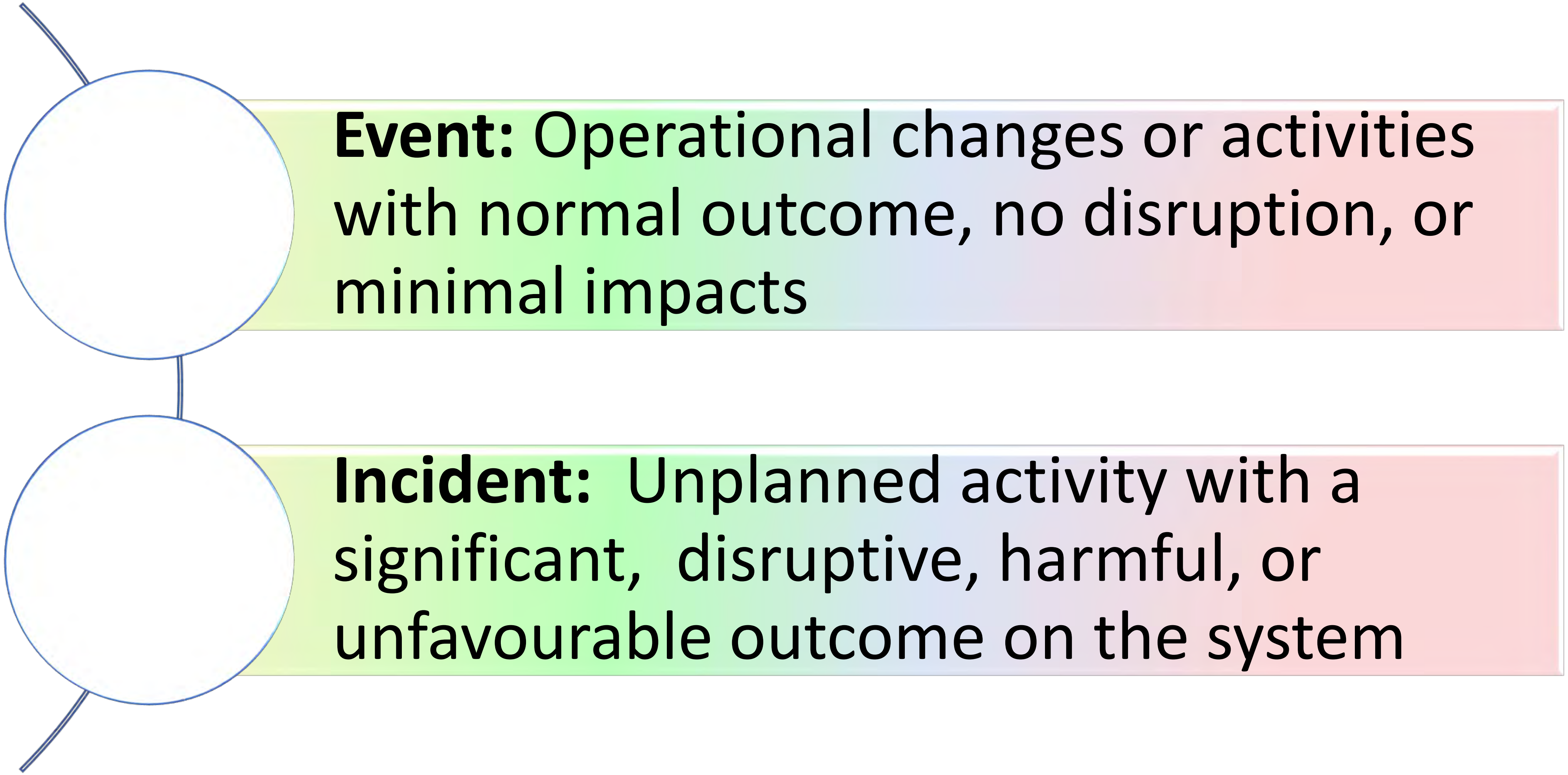


Prevention: Hindering cyberattacks

Detection: Discovering attacks in advance

Response: Mitigating cyberattacks & breaches

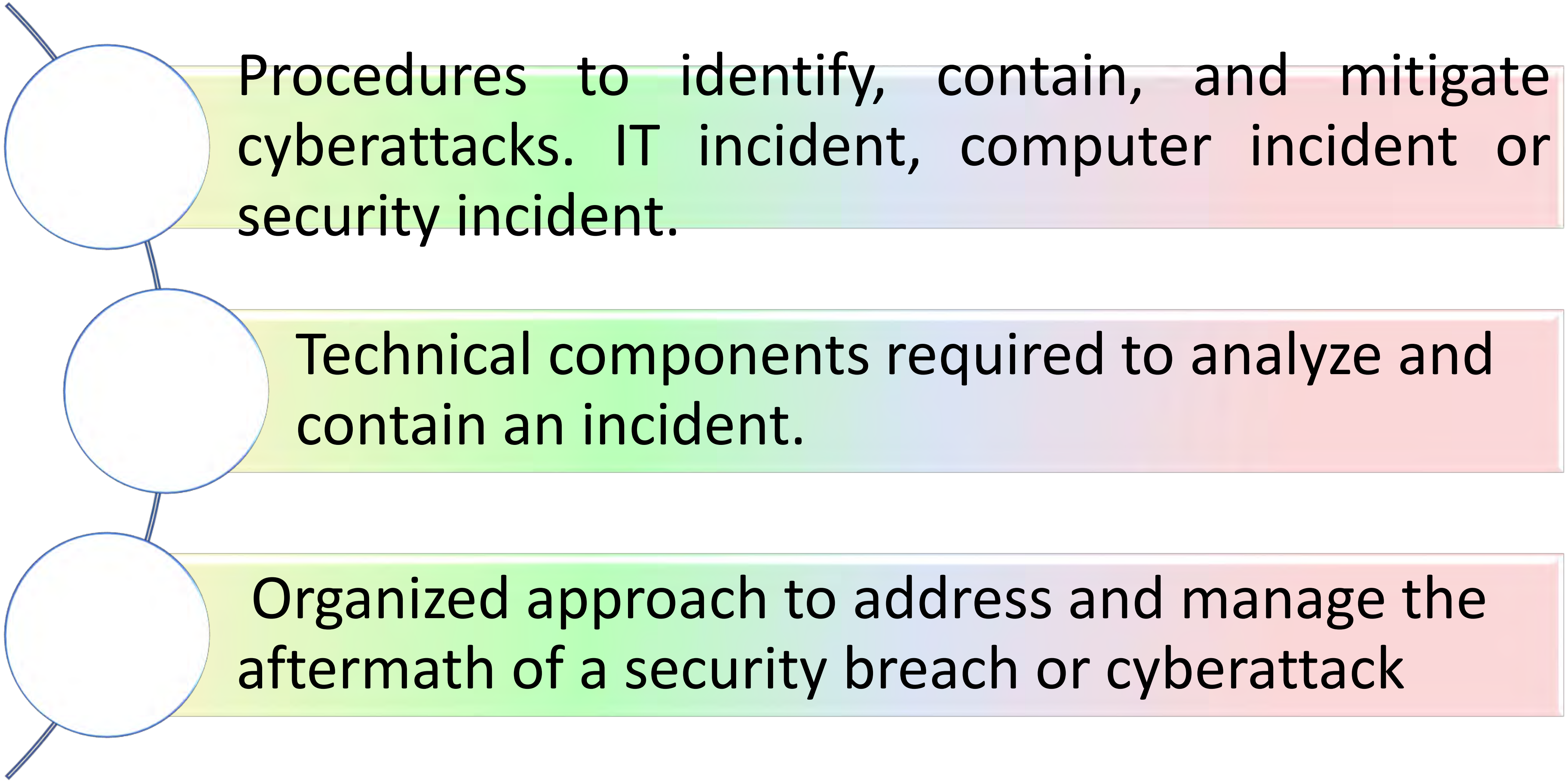
RESPONSE FUNDAMENTALS (1)
EVENT VS INCIDENT



Event: Operational changes or activities with normal outcome, no disruption, or minimal impacts

Incident: Unplanned activity with a significant, disruptive, harmful, or unfavourable outcome on the system

RESPONSE FUNDAMENTALS (2)
INCIDENT RESPONSE (IR)

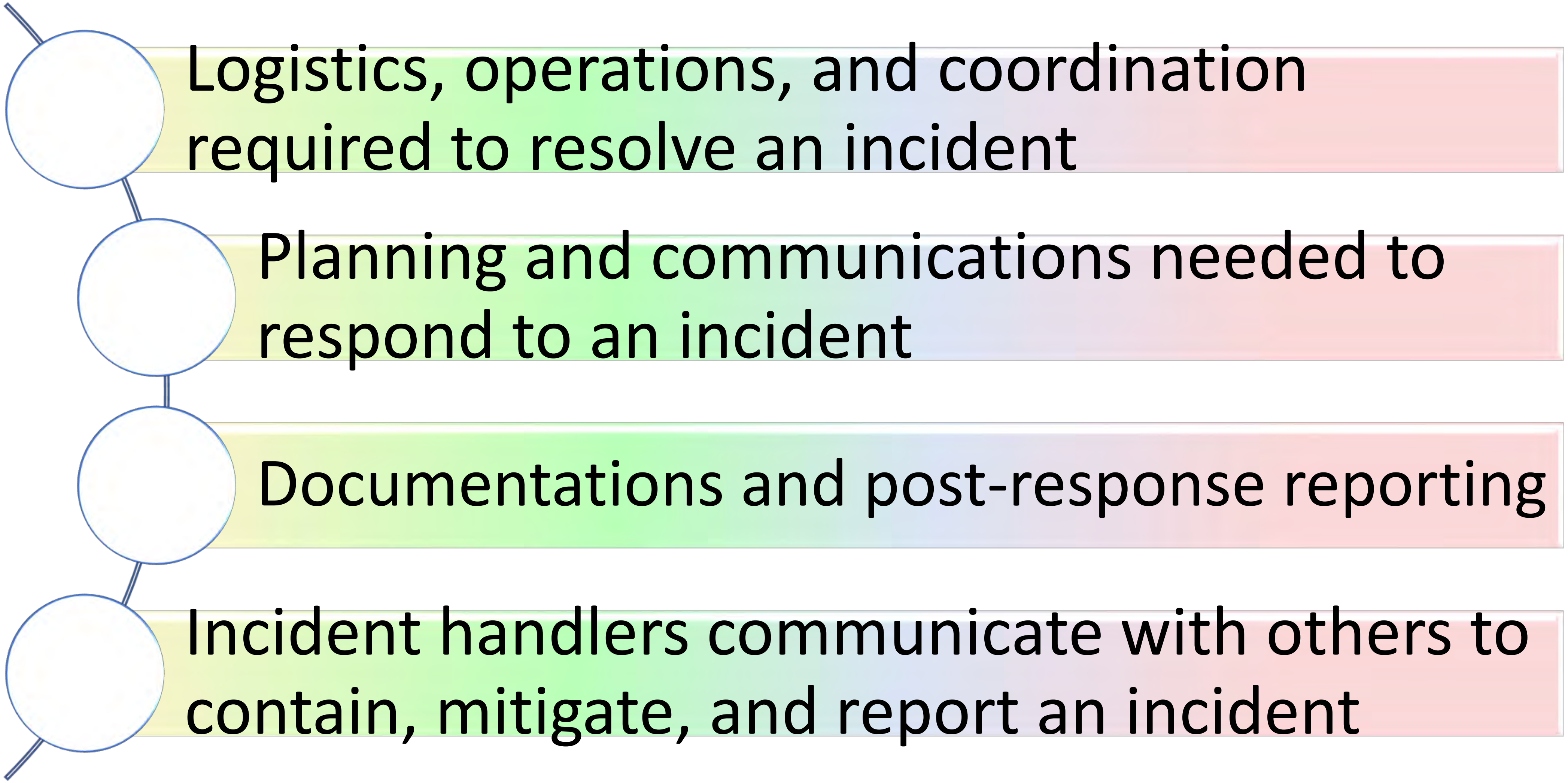


Procedures to identify, contain, and mitigate cyberattacks. IT incident, computer incident or security incident.

Technical components required to analyze and contain an incident.

Organized approach to address and manage the aftermath of a security breach or cyberattack

RESPONSE FUNDAMENTALS (3)
INCIDENT HANDLING (IH)

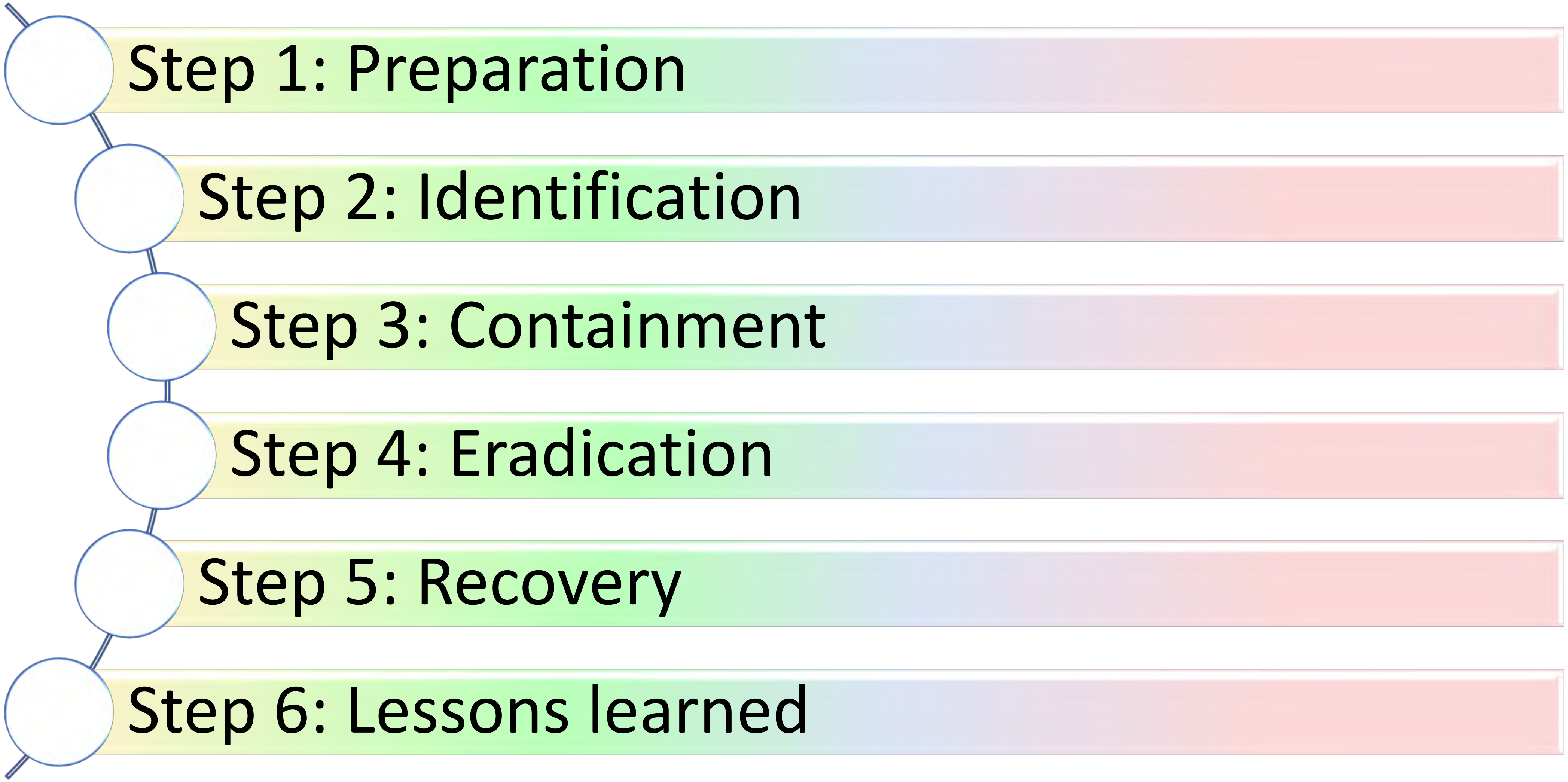


- Logistics, operations, and coordination required to resolve an incident
- Planning and communications needed to respond to an incident
- Documentations and post-response reporting
- Incident handlers communicate with others to contain, mitigate, and report an incident

RESPONSE FUNDAMENTALS (4)
INCIDENT MANAGEMENT (IM)

- Activities of an organization to identify, analyze, and mitigate cyberattacks
- Administrative policies to minimize impact of cyberattacks
- IM = IR + IH

INCIDENT RESPONSE STEPS



Step 1: Preparation

Step 2: Identification

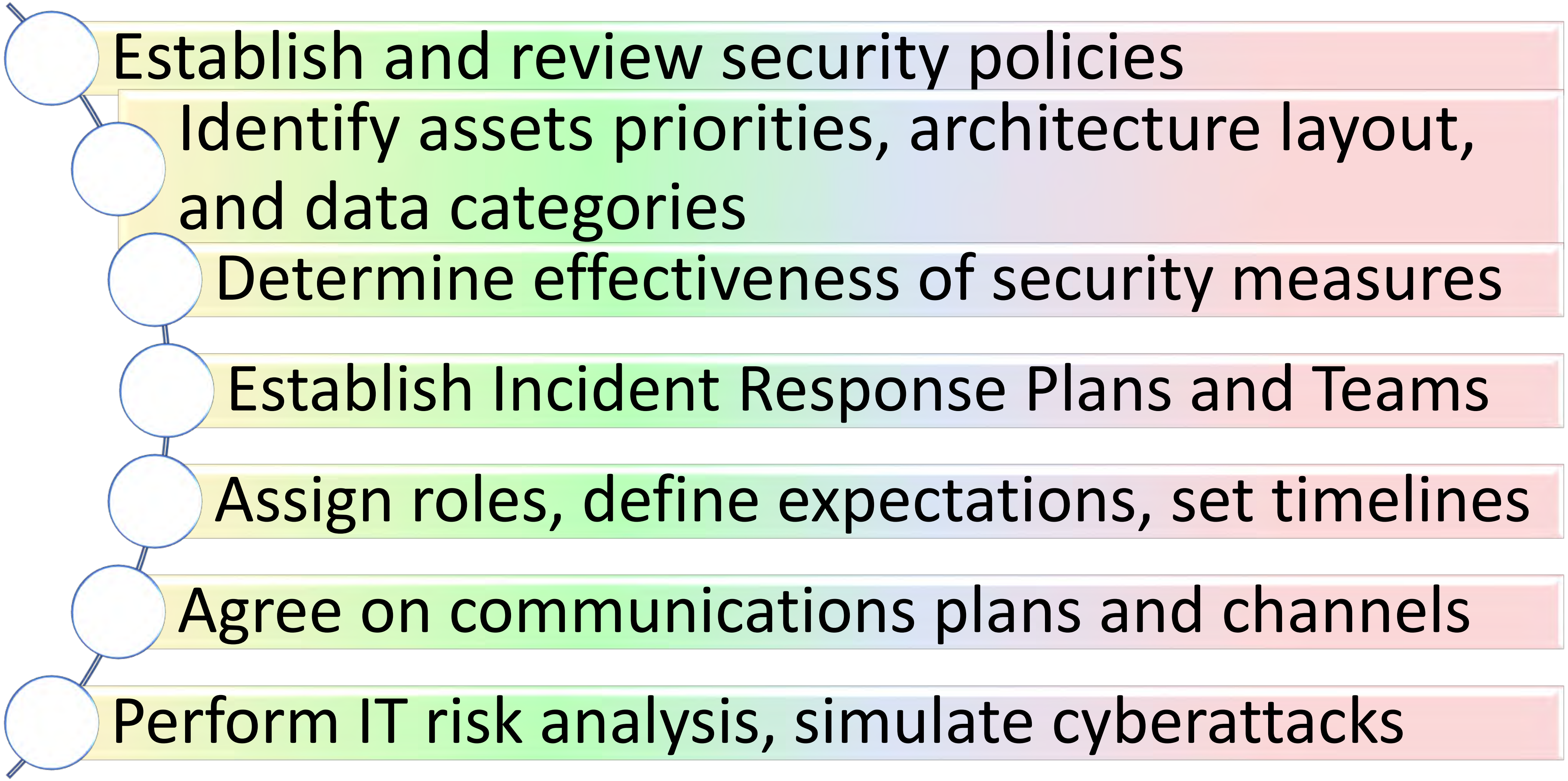
Step 3: Containment

Step 4: Eradication

Step 5: Recovery

Step 6: Lessons learned

INCIDENT RESPONSE STEP 1:
PREPARATION



- Establish and review security policies
- Identify assets priorities, architecture layout, and data categories
- Determine effectiveness of security measures
- Establish Incident Response Plans and Teams
- Assign roles, define expectations, set timelines
- Agree on communications plans and channels
- Perform IT risk analysis, simulate cyberattacks

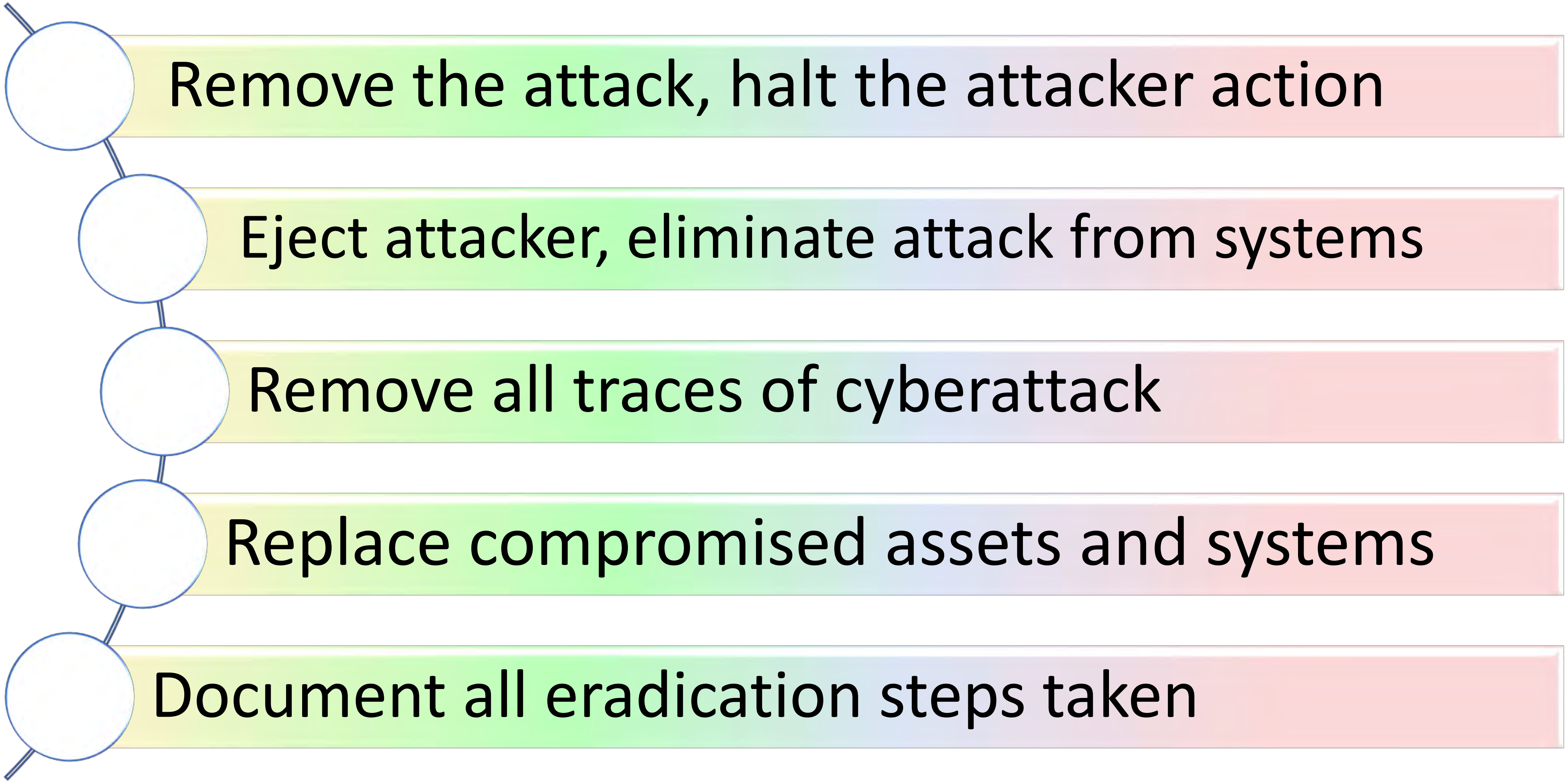
INCIDENT RESPONSE STEP 2:
IDENTIFICATION OR DETECTION

- Verify and confirm cyberattack incident status
- Identify nature, source, and goals of attack
- Detect suspicious activity, identify affected syst
- Collect, document, protect detailed evidence
- Activate communications plans
- Notify stakeholders, authorities, users, law enf.
- Activate situational management

INCIDENT RESPONSE STEP 3:
CONTAINMENT OR NEUTRALIZATION

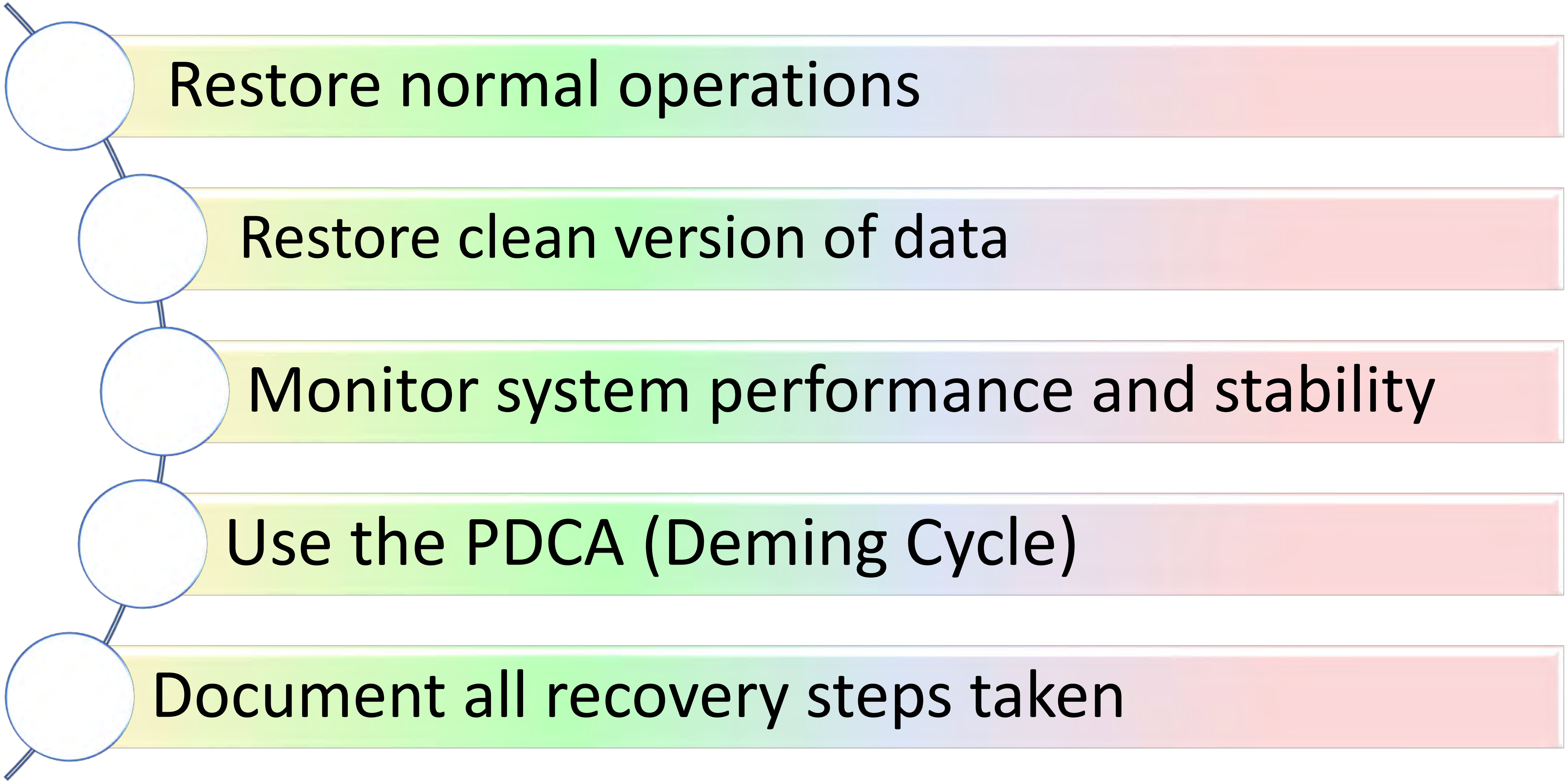
- Minimize impact, loss & amount of damage
- Isolate the object affected by the cyberattack
- Limit the spread of the attack
- Document all containment steps taken
- Keep track of all findings uncovered

INCIDENT RESPONSE STEP 4:
ERADICATION OR REMOVAL



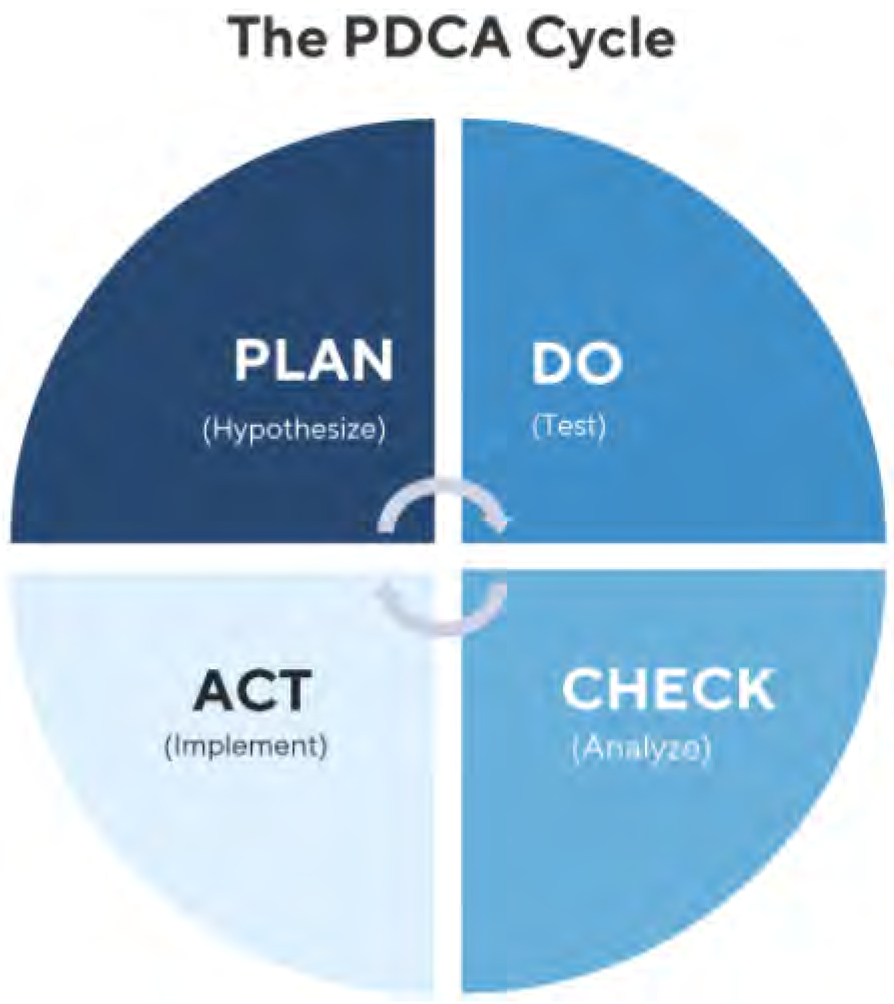
- Remove the attack, halt the attacker action
- Eject attacker, eliminate attack from systems
- Remove all traces of cyberattack
- Replace compromised assets and systems
- Document all eradication steps taken

INCIDENT RESPONSE STEP 5:
RECOVERY OR RESTORATION



- Restore normal operations
- Restore clean version of data
- Monitor system performance and stability
- Use the PDCA (Deming Cycle)
- Document all recovery steps taken

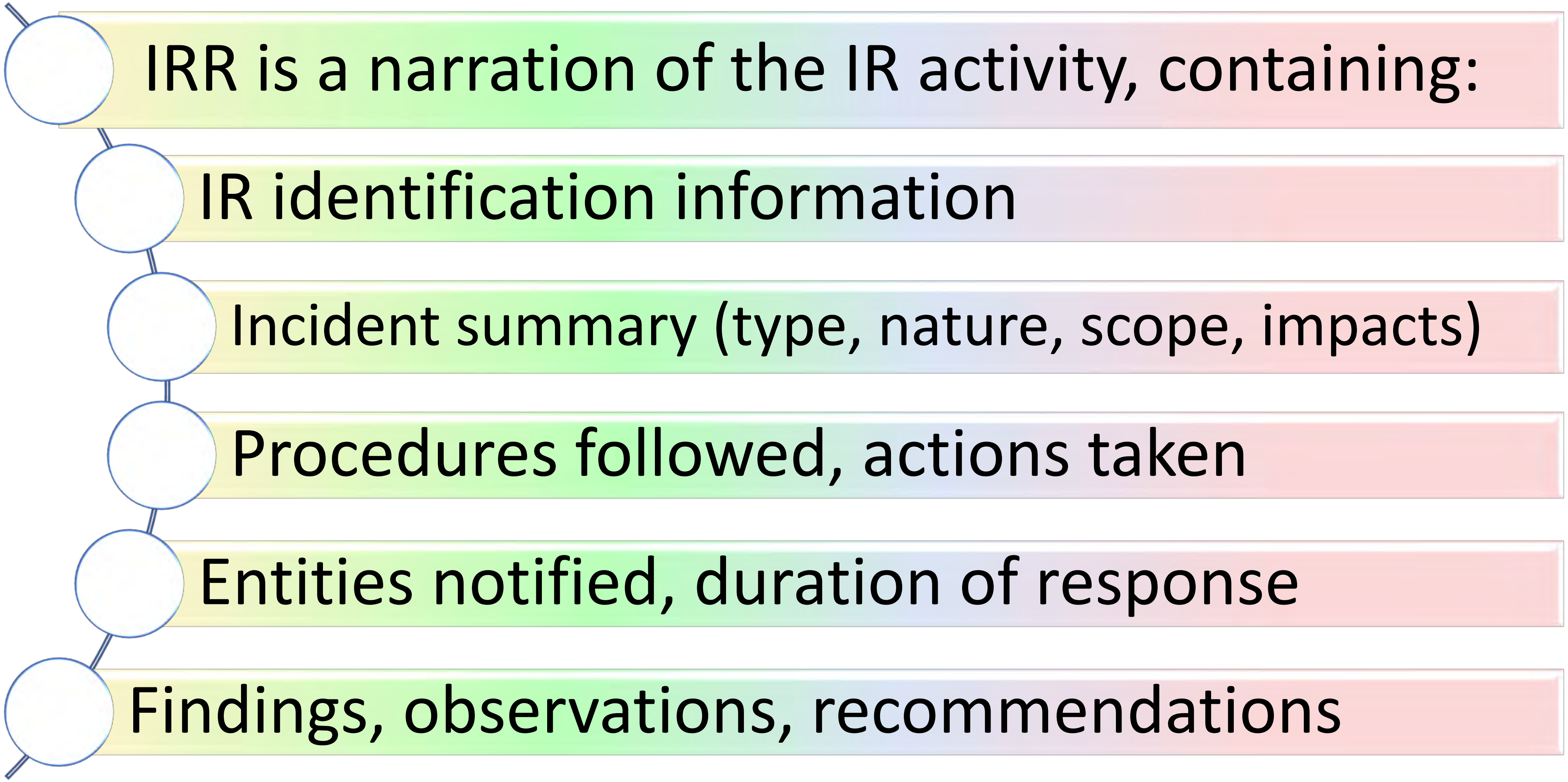
THE DEMING CYCLE
PLAN-DO-CHECK-ACT



INCIDENT RESPONSE STEP 6:
LESSONS LEARNED

- Review the steps taken during the response
- Identify successes and loopholes
- Itemize suggestions for future implementations
- Address all incomplete documentations
- Prepare & communicate comprehensive report
- Produce versions of report for specific audience

WRITING AN EFFECTIVE INCIDENT RESPONSE REPORT (IRR)



IRR is a narration of the IR activity, containing:

- IR identification information
- Incident summary (type, nature, scope, impacts)
- Procedures followed, actions taken
- Entities notified, duration of response
- Findings, observations, recommendations

PRACTICAL SESSION ON INCIDENT RESPONSE:
SCENARIO ANALYSIS

1: Three scenarios, three groups.

2: Study the scenario, and discuss how to carry out incident response following the standards steps.

3: Produce an incident response report.

SUMMARY AND CONCLUSIONS
WHY INCIDENT RESPONSE?

- Fix the immediate cyberattack
- Forestall future re-occurrence
- Limit the spread of the cyberattack
- Minimize impact, and cost of risk
- Ensure compliance with regulations
- Increase Cybersecurity awareness
- Document lessons on cyber threats

THANK
YOU
return