

Incident Response and Recovery for SSCP®

Incident Life Cycle Management



Dr. Lyron H. Andrews

Cybersecurity Advisor - CISSP/CCSP/SSCP/CRISC/CISM/CCSK

<https://www.linkedin.com/in/drlyronhandrews/>



SSCP Certification Examination

Domains	Weights
Security Operations and Administration	16%
Access Controls	15%
Risk Identification, Monitoring and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communication Security	16%
Systems and Application Security	15%



Course Overview



Define and examine IR and review the incident handling process

Establish the forensic process and the technical and legal constraints

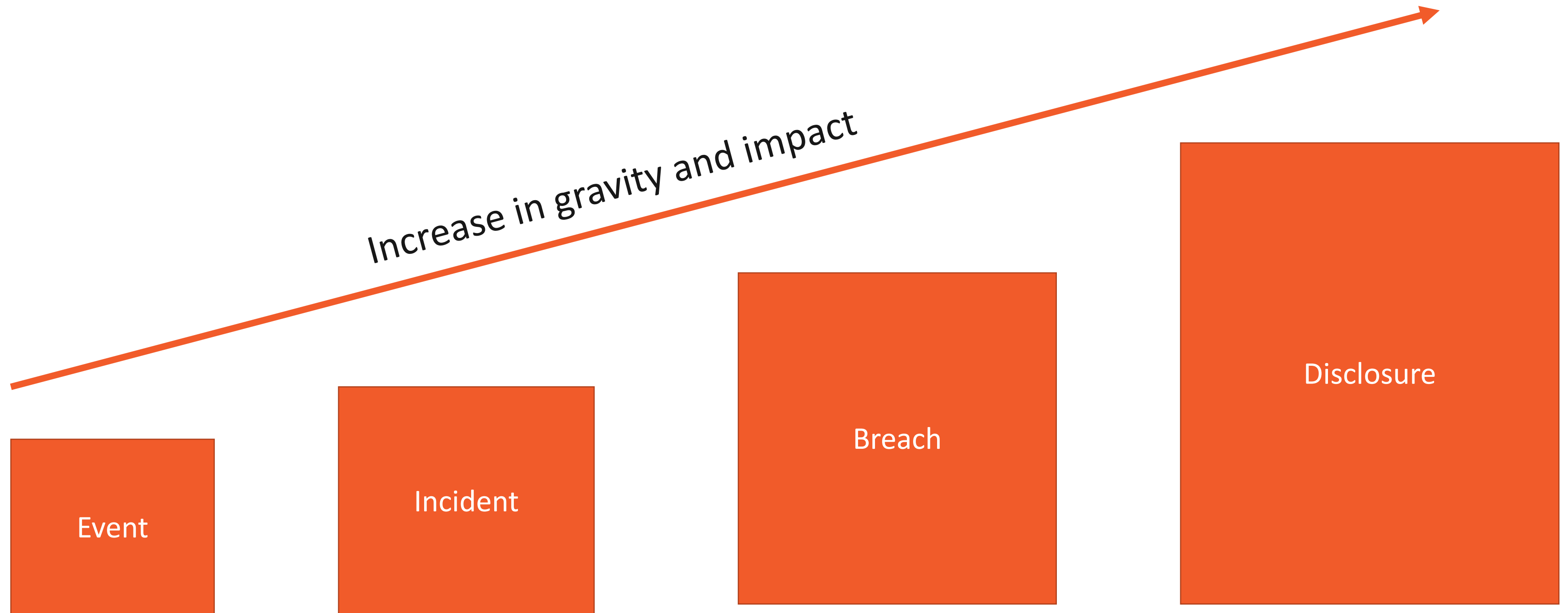
Review the process and underlying technology of BCDR



Defining Terms Related to Incident Response



Terms Related to Incidents



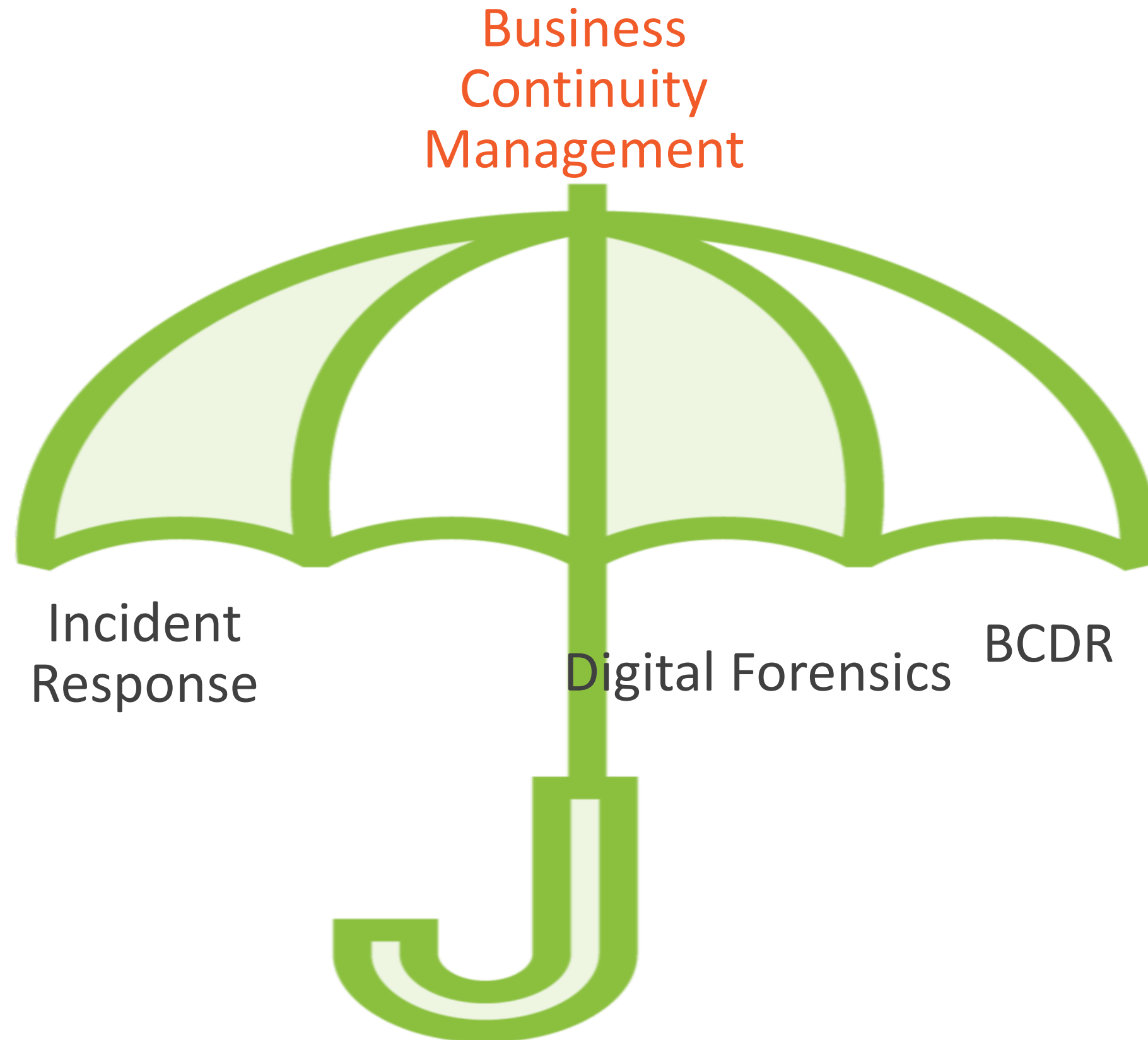
Terms Related to Incidents

A solid orange square with the text "Incident Response" centered inside it in white font.

Incident Response



BCM As Parent Of Incident Response



Overview of IR Frameworks



Examples of Incident Response Frameworks

NIST SP 800-61

ISO/IEC 27035

ENISA



NIST SP 800-61

Computer Security Incident Handling Guide

Preparation

Detection and analysis

Containment, eradication, and recovery

Post-incident activity



ENISA Incident Response

People safety first

Team makeup

Response plan procedures

External services



Information Security Incident Management ISO/IEC 27035

Plan

Detection

Assessment

Responses

Lessons



IR Framework Themes

People safety first

Pre-incident activities

Containment and recovery

Post-incident activities

NIST SP 800-61



Use business requirements to
determine the IR framework
selection.



Organizing Capability for IR



Organizations that complain
about technology woes often
have a lack of governance.



Foundation of Incident Response



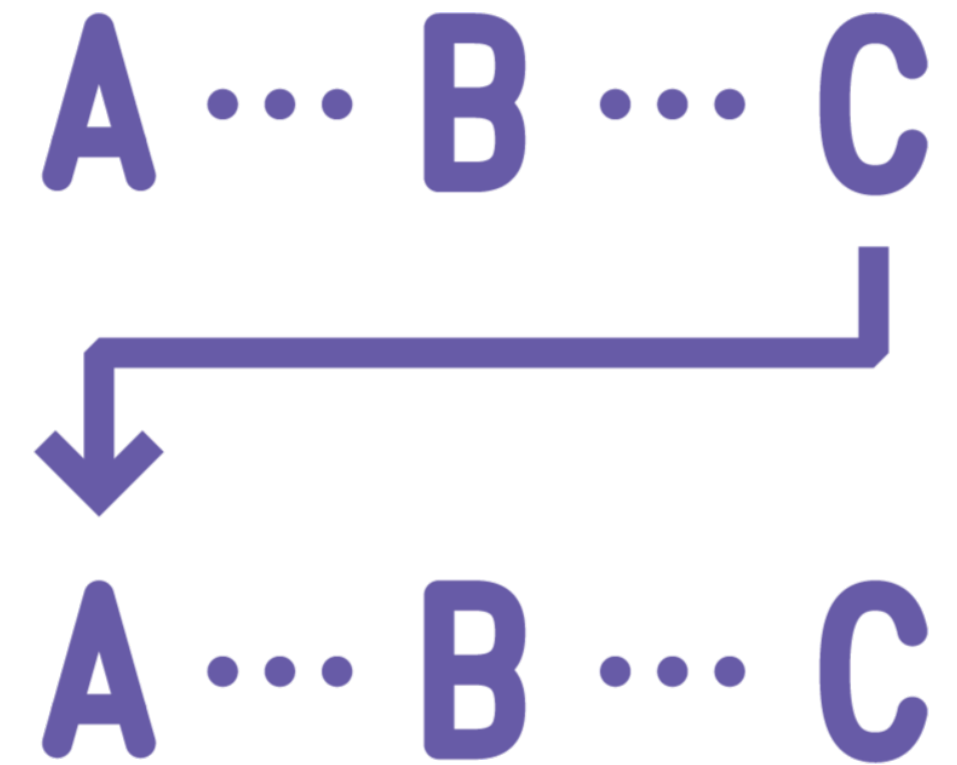
Policy

Overall governance of IR activities



Plan

Overall path of action that is taken



Procedure

Step-by-step instructions



IR Policy Elements

Statement of management commitment

Purpose and objectives

Scope of policy

Definition of incidents

Prioritization and severity ratings

Performance measures

Reporting obligations



IR Plan Elements

Mission, strategy and ,goals

Sr. management approval

Organizational approach

Communication paths

Metrics for measuring and maturing



IR Procedure Elements

Comprehensive and detailed

Priorities reflected in IR operations

Reduce errors through explicit steps

SOPs tested regularly



The Incident Response Team

Permanent

Full-time employees

Virtual

As needed

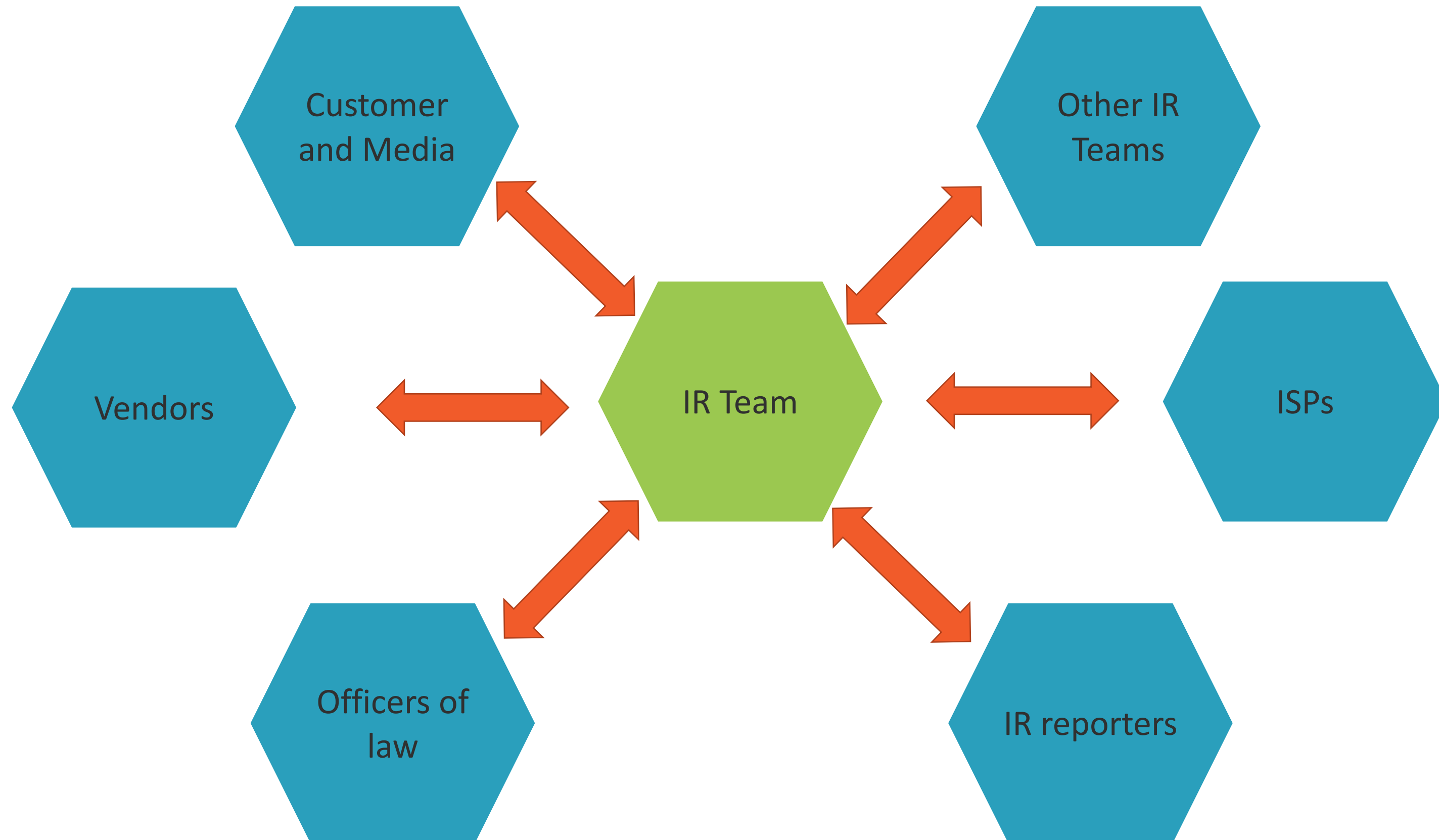
Hybrid

Combination of both

Policy drives the team design and makeup



Extended Incident Response Participants



IR Team Guidelines

Monitor morale

Continuously review competencies

Job rotation as a strategy

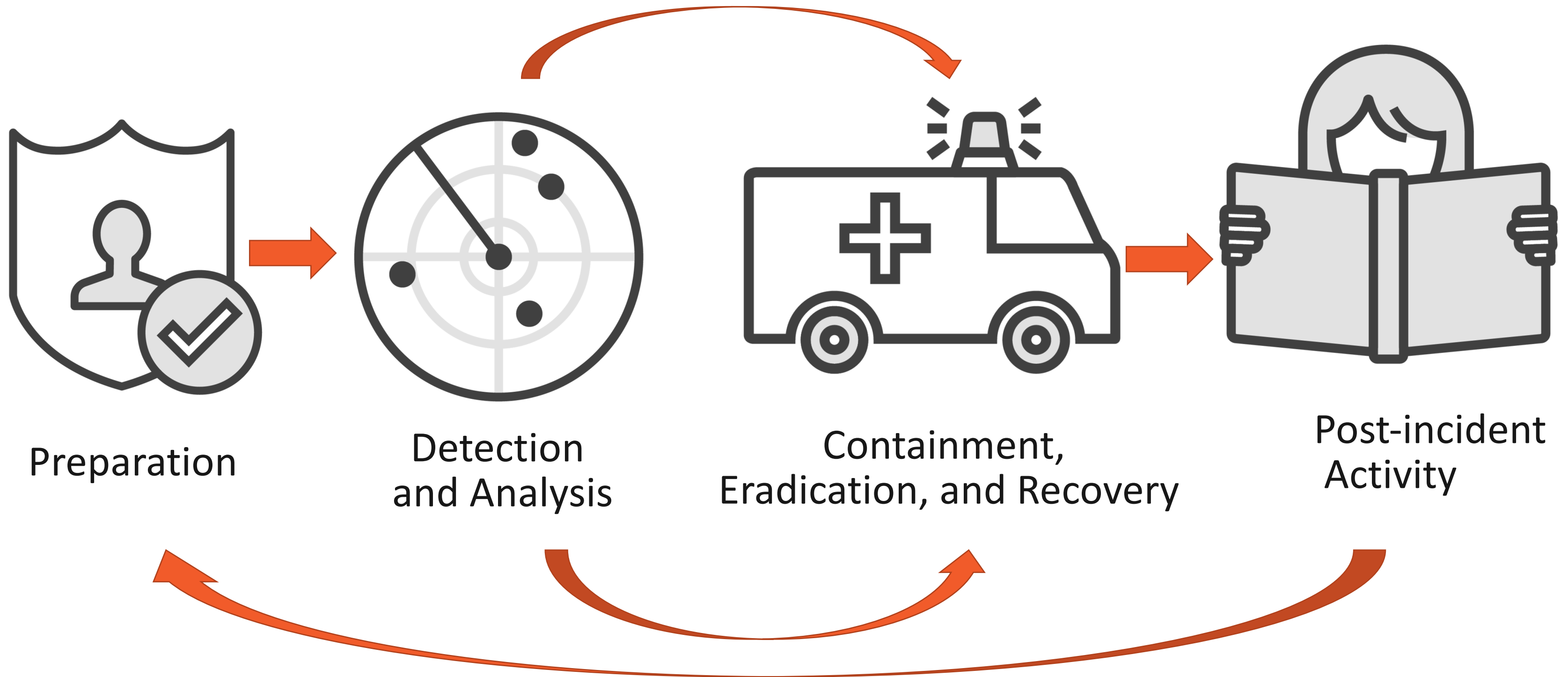
Develop service catalogue



IR Life Cycle - Preparation



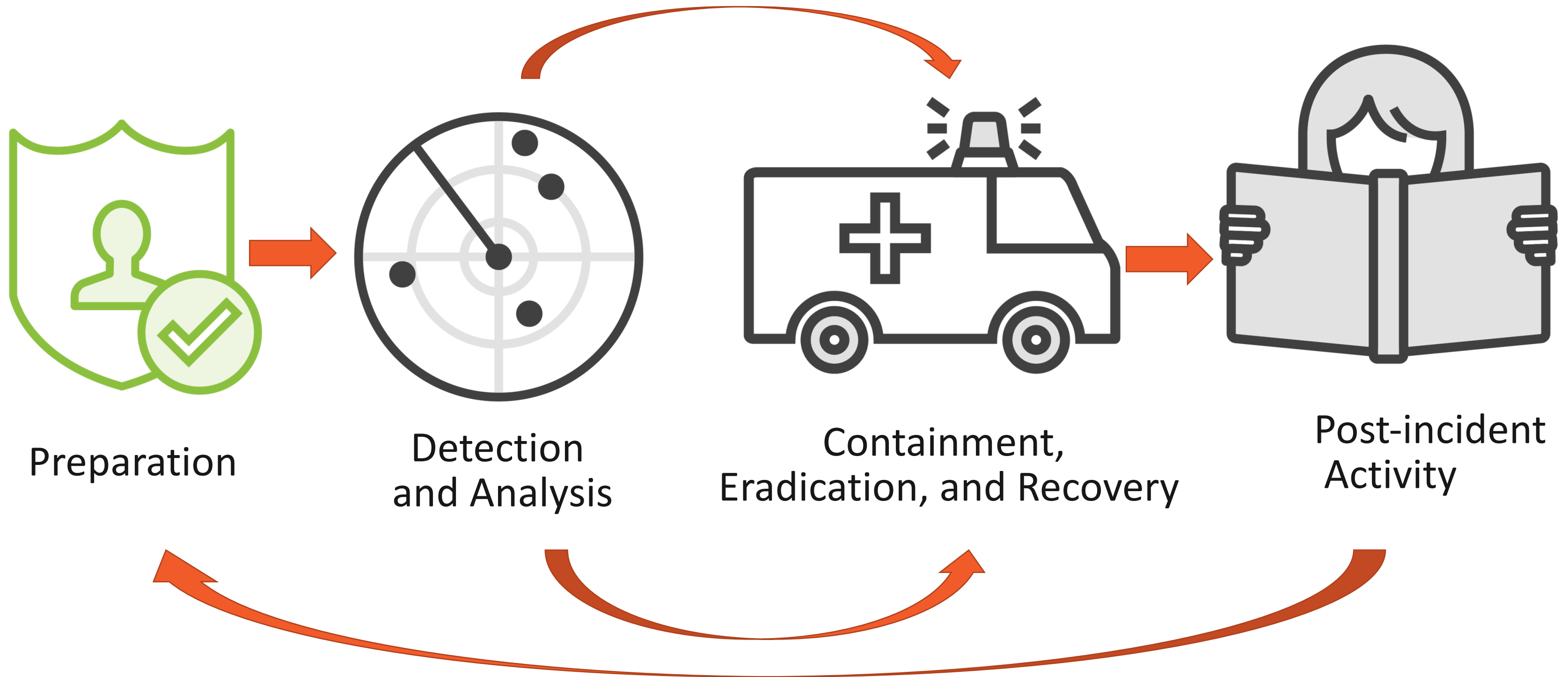
IR Life Cycle



Failing to plan is planning to fail.



IR Life Cycle





Incident mitigation

Incident prevention

Handler communications and facilities

Hardware and software analysis tools

Resource list

Preparation Phase – Communications and Facilities

Contact information

On-call information

Incident reporting mechanisms

Issue tracking

Encryption software

War room

Secure storage



Preparation Phase

– Hardware and Software Analysis

Digital forensics stations

Laptops and desktops

Blank media

Portable printer

Packet sniffers

Digital forensic tools



Preparation Phase – Analysis Resources

Port lists

Documentation

Network diagrams

Current baselines

Cryptographic hashes



Preparation Phase

– Mitigation Software and Prevention

Risk assessments

Host and network security

User awareness and training

Jump kit



IR Jump Kit



Jump Kit



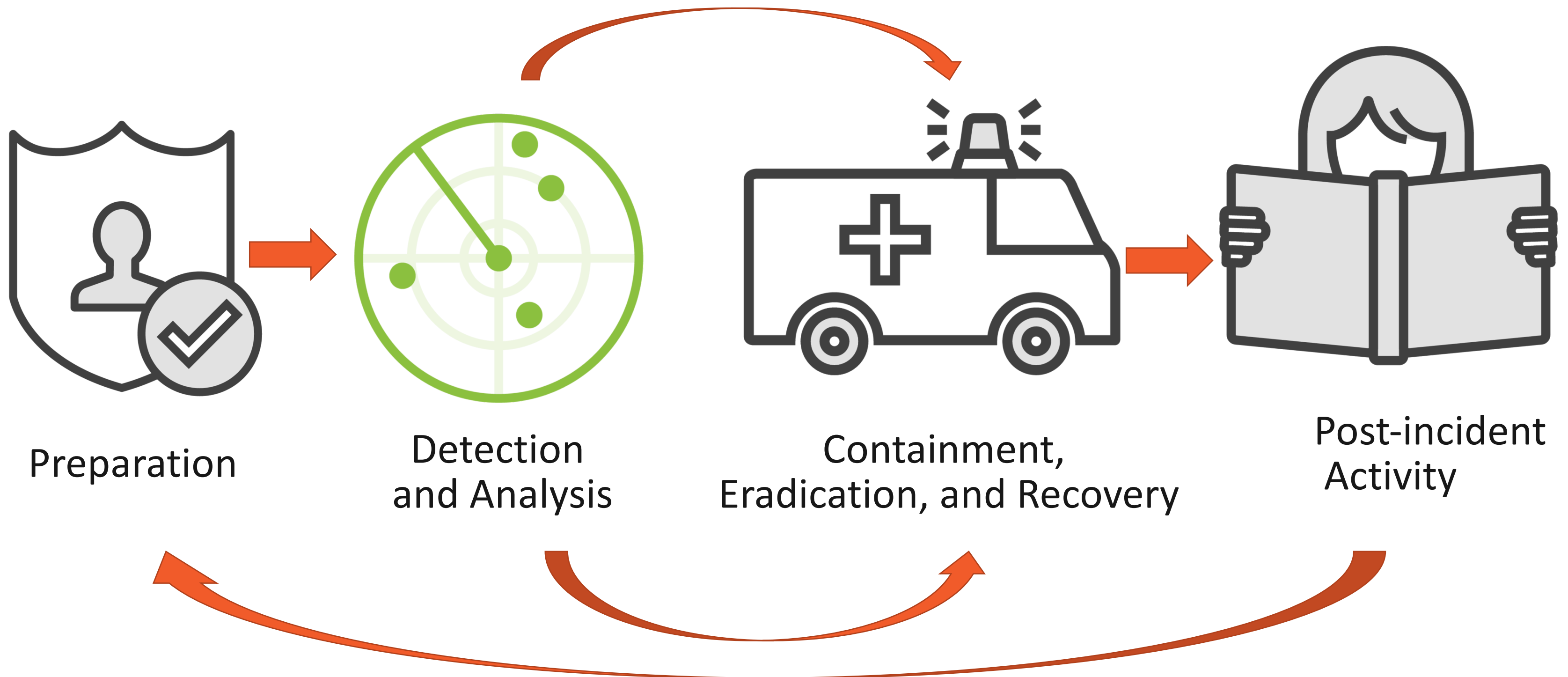
IR Jump Kit



IR Life Cycle – Detection and Analysis



IR Life Cycle





External and removable media

Attrition

Web

Email

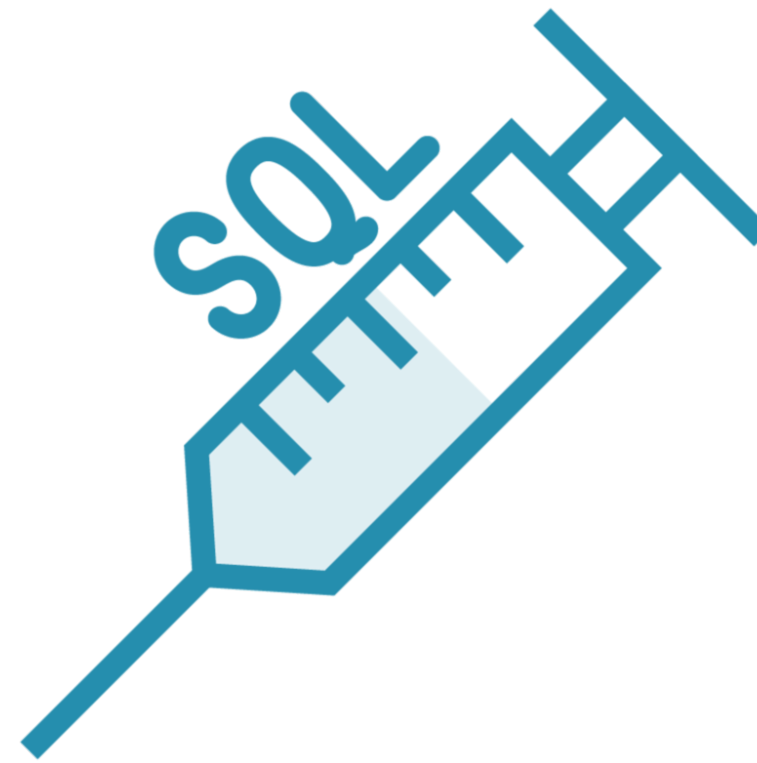
Spoofing

Improper usage

Two General Attack Vectors



Precursors



Indicators

While the preference is stopping
the attack before it begins the
reality is that rarely happens.



Common Sources of Percussors and Indicators

IDP

SIEM

Antivirus

File integrity check

3rd party monitoring

Detection then leads to analysis

Operating systems

Application logs

Network device logs

Network flow

New vulnerability lists

Internal people

External people



Groundwork For Analysis Validation

Search engine research
Filter data
Seek assistance

Event correlation
Host clocks synchronization
Maintain knowledge base

Network profiling
Understand baselines
Log retention



Incident Prioritization

Functional Impact

Business-related issues for users

Information Impact

CIA issues for organization

Recoverability

The time and resources tied to resolution

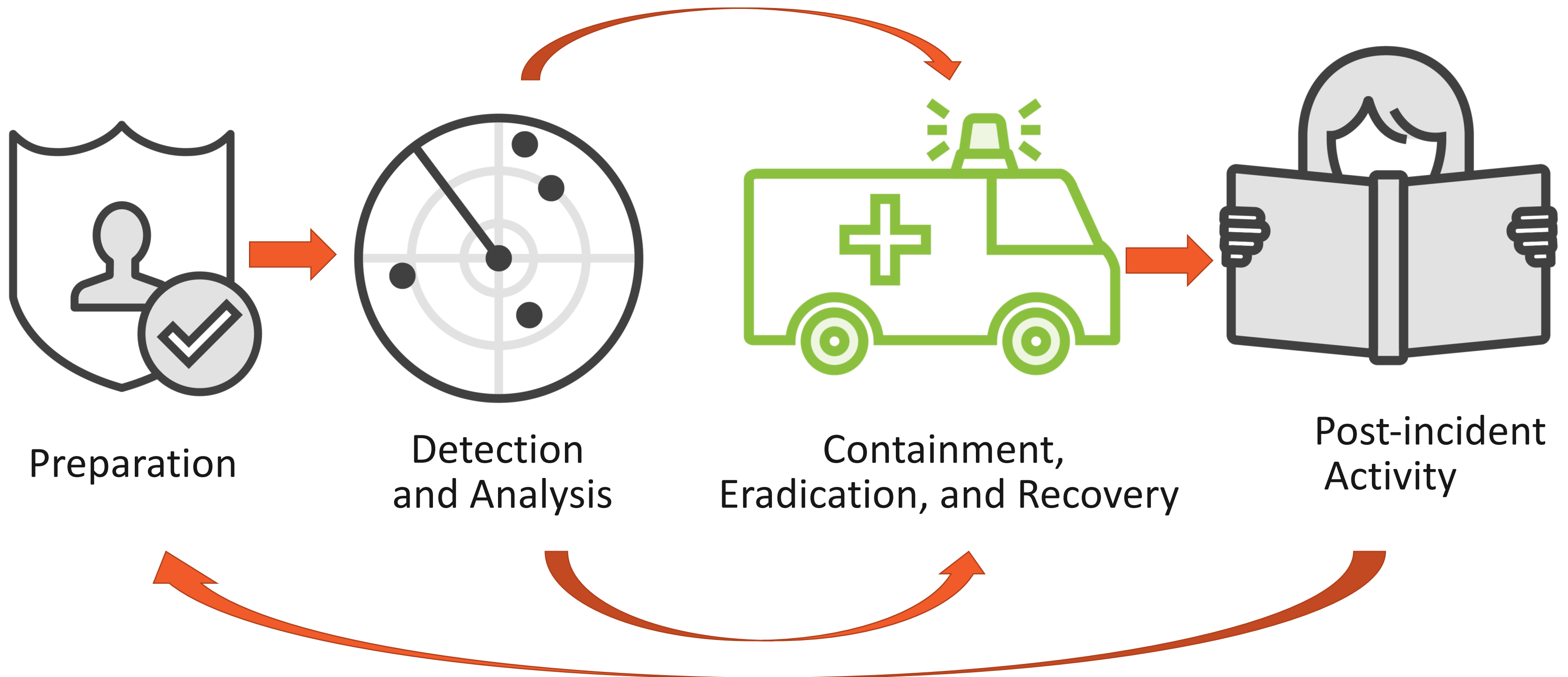
Severity level leads to notification determination



IR Life Cycle – Eradication, Containment, and Recovery



IR Life Cycle



Stopping the spread of the attack
is essential to recovery.





Potential damage and theft

Need for evidence preservation

Service availability

Time and resources

Duration of solution

Evidence Gathering and Identifying Attacker

Gathering

Snapshot

Validating

Researching

Databases

Monitoring



Eradication and Recovery

Delete destroy disable

Restore system to operational baseline

Clean version of system software

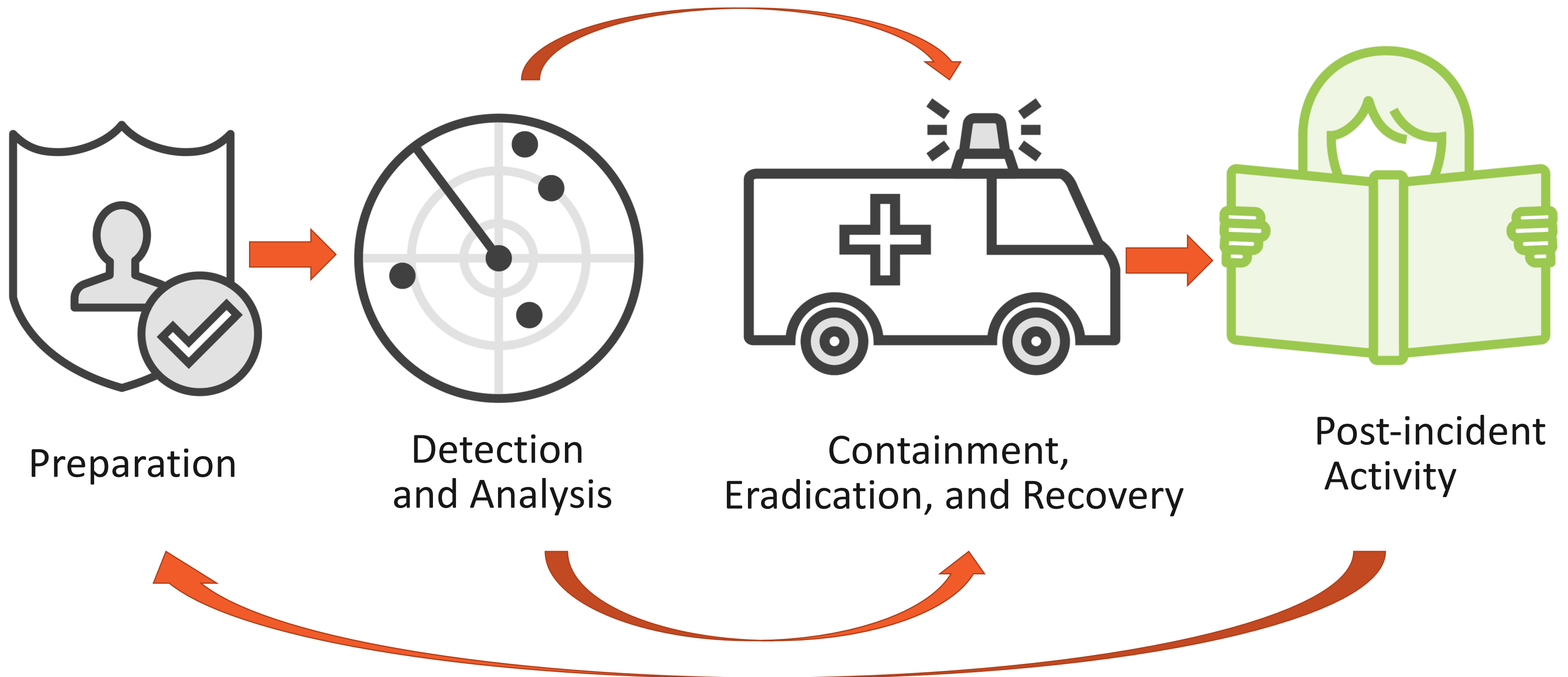
Lock down implicit access



IR Life Cycle – Post-incident Activity



IR Life Cycle



“One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned.”

NIST SP 800-61





The six question of existence must be asked

- What happened at what time
- Were documented procedures followed
- What information was needed
- How can information sharing improve
- When was the precursor noted
- Why was the system available

Summary



If IR is established in your organization, where can it improve

What competencies are adequate on the IR team and what are not

How effective is your IR for contemporary threats



Up Next:
Forensic Investigations

