

Welcome to Security Lifecycle – Response.

What you will learn

At the core of the lesson

You will learn how to:

- List the typical steps in the incident investigation process
- Describe the purpose of a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP)
- Identify backup options
- Apply best practices for backups



Security lifecycle: Response




3

As a review, the phases of the security lifecycle consist of:

- **Prevention** – The first line of defense.
- **Detection** – Occurs when prevention fails.
- **Response** – Describes what you do when you detect a security threat.
- **Analysis** – Completes the cycle as you implement new measures to prevent the incident from occurring again in the future.

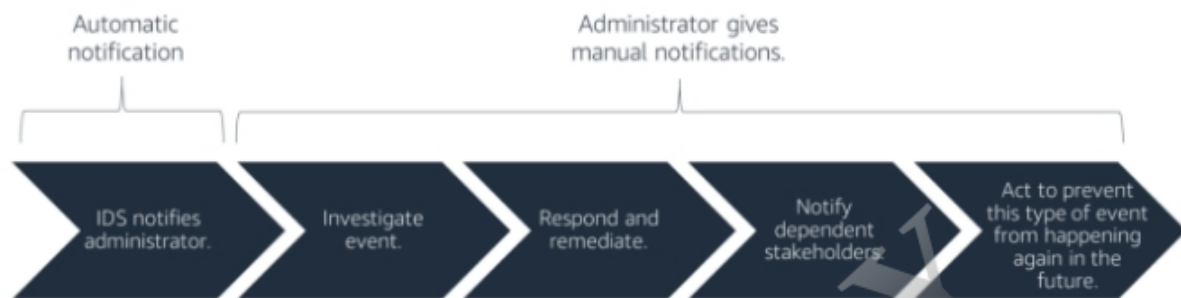
In this lesson, you will learn about the *Response* phase of the security lifecycle. Specifically, you will discover methods and techniques related to how to manage, respond, and remediate security events.



Process and planning for event response

Event investigation process

- Stages of a typical response to any malicious **event**



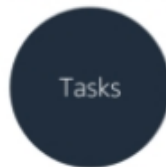
5

aws re/start

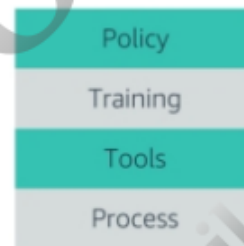
The figure shows the typical steps that are used to respond to and investigate a security event.

Event investigation: Preparation phase

Preparation is most the important step in dealing with any event.



Identify or detect
Escalate
Notify
Stop the event
Scrutinize
Eradicate
Recover



You cannot plan for every conceivable disaster. However, you can demonstrate due diligence by identifying and documenting the types of disasters that present a real threat to your business. The unexpected event can be a minor inconvenience or it could result in the end of your organization. If you fail to plan for these potentialities, you plan to fail.

Understanding Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

the next few slides will discuss the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

Business Continuity Plan and Disaster Recovery Plan

Business Continuity Plan (BCP)



Run business in reduced form

Disaster Recovery Plan (DRP)



Recover from an outage or loss

8

aws re/start

The purpose of these two plans is to do the following actions:

- Enable a business to continue supporting and offering critical services when there is a disruption.
- Survive a disastrous interruption to activities.

Planning business continuity

Business Continuity Plan



- Preventative and proactive management tool
 - Lists different disaster scenarios
 - Is not activated during an outage

9

aws re/start

A Business Continuity Plan (BCP) lists different disaster scenarios. It describes what the business will do to keep critical services and functions running when a disaster or disruption occurs, such as an interruption of service, or destruction of hardware.

The BCP accomplishes the following actions:

- Lists different disaster scenarios and what the business will do to keep business running as usual.
Example scenarios: Failed disk, failed server, failed database, bad communications line
- Keeps the business running in a reduced form over a period of time
For example, which minimum online systems, phones, servers, network connections, network drives, and other resources should continue to run?

The BCP is not activated during an outage.

Planning disaster recovery (DR)

- A strategy that helps the business recover from disasters and unplanned incidents.
 - **Recovery Time Objective (RTO):** How quickly do we need to be back up?
 - **Recovery Point Objective (RPO):** How much time and data can we afford to lose?

Disaster Recovery Plan



Recover from an outage or loss



10

A Disaster Recovery Plan (DRP) defines a strategy that helps the business recover from disasters and unplanned incidents, including cyber incidents. DRP uses two key parameters:

- **Recovery Time Objective (RTO):** How quickly do we need to be back up?
- **Recovery Point Objective (RPO):** How much time and data can we afford to lose?

As the value of these parameters becomes shorter, backup strategies and other recovery mechanisms become more expensive or complex. However, RTO and RPO have gotten shorter over time as technology has evolved.