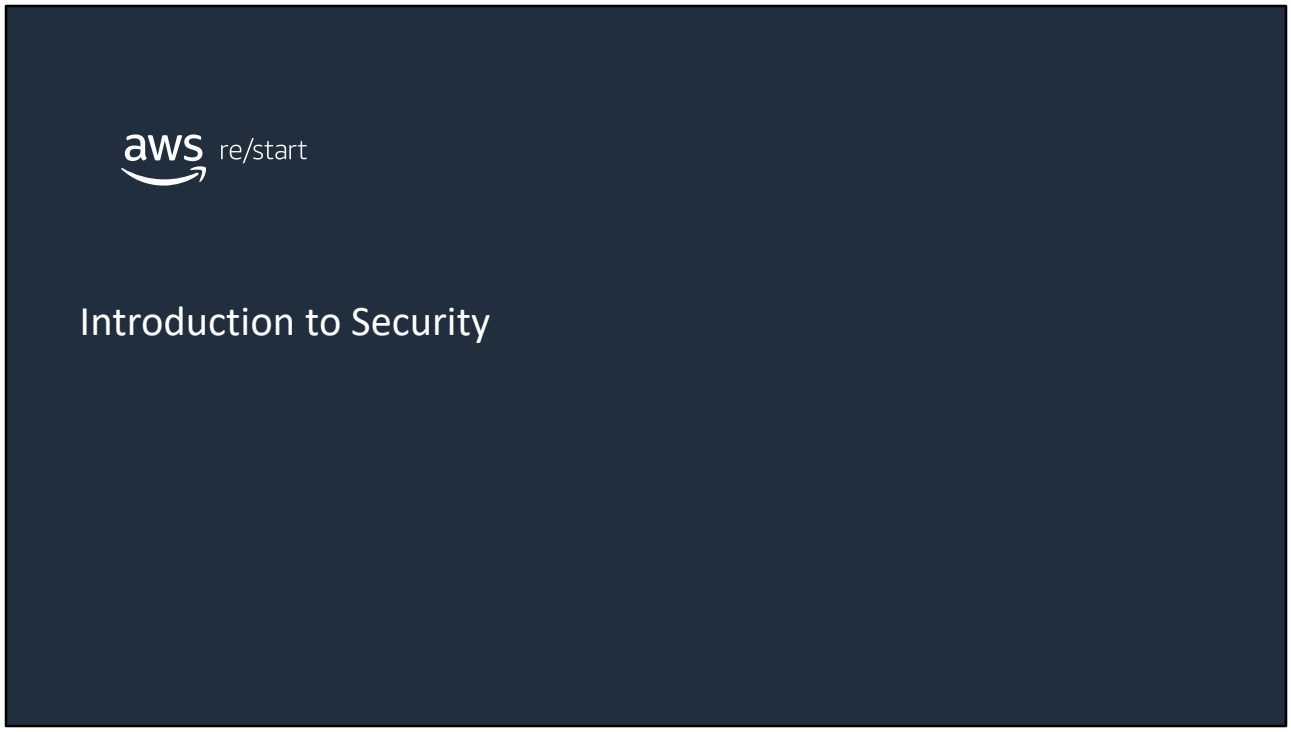


Welcome to Introduction to Security.

Third-party links are for educational purposes only. AWS takes no responsibility and assumes no liability for the accuracy or accessibility of the linked content.

What you will learn

At the core of the lesson

You will learn how to:

- Define key security terms
- Identify different types of security threats
- Identify the components that comprise a security strategy
- List the types of security controls
- Name the stages of the security lifecycle

aws re/start

In this lesson, you will learn how to:

- Define key security terms
- Identify different types of security threats
- Identify the components that comprise a security strategy
- List the types of security controls
- Name the stages of the security lifecycle

Security basics

Let’s begin with some security basics.

Discussion: Security introduction

1) What would be the impact on your life if you could not access the internet for a few days?
2) What would be the impact if your personal information were stolen?
3) What are some ways that you can think of to prevent any of this from happening?

aws re/start

To get you started thinking about the topic of security, answer the following questions:

1) What would be the impact on your life if you could not access the internet for a few days?
2) What would be the impact if your personal information were stolen?
3) What are some ways that you can think of to prevent any of this from happening?

What is security?

Security is the practice of protecting valuable assets.

- Assets can be physical or digital and include people, buildings, computers, software applications, and data.
- **Cybersecurity** is concerned with protecting networks, devices, systems, and digital information from the following:
  - Unauthorized access
  - Malicious modification, theft, or destruction
  - Disruption of intended use
- The primary goal of cybersecurity is to ensure the confidentiality, integrity, and availability of digital information.

aws re/start

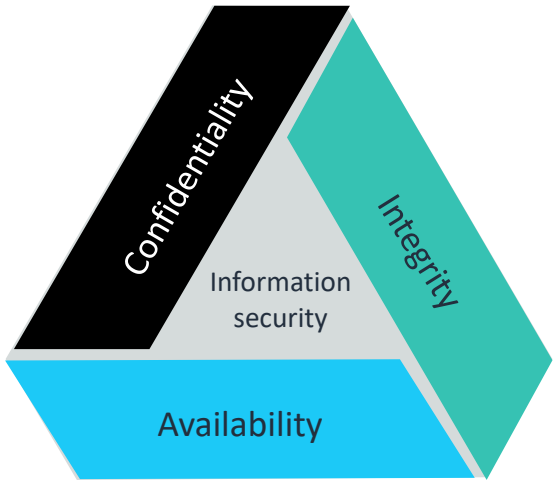
Security can be generally defined as the practice of protecting valuable assets. These assets can be physical, such as people, computers, and buildings, or digital, such as software applications and user data. Security attempts to ensure that only authorized personnel are allowed access to these assets and protects these assets from malicious modification, theft, or destruction so that they can be used according to their intended purpose.

Cybersecurity is particularly concerned with the protection of networks, computers, and systems to ensure the confidentiality, integrity, and availability (CIA) of the digital information that they contain.

Confidentiality, integrity, and availability (CIA)

Information needs to be protected to ensure its confidentiality, integrity, and availability.

- **Confidentiality**: Is private data protected to prevent unauthorized access?
- **Integrity**: Are measures in place to ensure that data has not been tampered with and is correct and authentic?
- **Availability**: Are authorized users able to access the data when they need it?



aws re/start

The confidentiality, integrity, and availability (CIA) triad represents three important security aspects that must be considered when protecting information. They are defined as follows:

- Confidentiality protects the privacy of the information by preventing unauthorized access to it. A common method to ensure confidentiality, for example, is to first asks users to identify themselves before they are allowed to use a system. This process is known as authentication.

- Integrity ensures that the information is always accurate and correct where it is stored and whenever it is moved. The data cannot be altered by unauthorized users as it moves inside and outside its containing system or when it reaches its final storage location. Hashing is an example of a technique that can be used to ensure that data has not been tampered with during transit.

- Availability ensures that the information is accessible to users when they need it. Businesses typically address availability requirements by creating plans such as a business continuity plan (BCP) and a disaster recovery plan (DRP). These plans define processes and procedures to maintain or quickly restore the availability of the systems containing the information in the event of failure or disruption.

You will learn more about the methods for ensuring the confidentiality, integrity, and availability of information in the upcoming modules.

Basic security terms

Attacker	A person or entity with malicious intent to compromise a system
Vulnerability	A weakness in a system that an attacker can exploit
Threat	An event that has the potential to negatively impact a system
Breach	An attack that compromises a system
Control	A mechanism to reduce or eliminate a vulnerability

aws re/start

The following scenario explains the basic security terms that this slide lists:

1) An attacker is an entity that wants to maliciously affect a system.
2) The attacker searches for a vulnerability in the system that they can exploit. A vulnerability is a weakness that exists usually due to an oversight, flaw, or error in the system.
3) When the attacker finds a vulnerability, they create an event that is capable of causing a negative impact on the system through the vulnerability. This is called a threat.
4) If the threat is successful and the system is compromised, a breach or incident has occurred.
5) When the breach is detected, the owner of the system implements a control to eliminate the vulnerability that attackers used to carry out the breach.

Why is security important? (1 of 2)

Security threats are real.

- Reports of breaches in the government, financial, healthcare, and internet commerce areas are commonplace in the news.
- The types and number of threats continue to rise.

13,256

data breach incidents recorded in North America (in 2020)*

aws re/start

Security has become crucial for everyone because computers and related technologies are integrated into our work environments and personal lives more each day. As more valued information is put on systems, the types and number of threats continue to increase. It is commonplace today to hear reports in the news of government agencies, financial companies, and other businesses with an internet presence being hacked (that is, breached). To quantify the magnitude of the problem, a study conducted by Verizon estimates that 13,256 data breach incidents were recorded in North America alone in 2020.*

Source: *Verizon. 2021. 2021 Data Breach Investigations Report (DBIR). Accessed November 23, 2021. https://enterprise.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx.

Why is security important? (2 of 2)

Security breaches have consequences.

- Identity theft
- Data theft
- Loss of online services and resources
- Damaged business reputation
- Loss of customers

38%
of data breach costs is from lost business (in 2020)*

Security breaches are costly.

- It often takes many days to identify and resolve a breach.
- The longer it takes to resolve a breach, the costlier it becomes.
- The cost of remediating a breach continues to rise.

$4.24 million
is the global average total cost of a data breach (in 2020)*

aws re/start

The consequences of a breach can affect both individuals and businesses. For example, identity theft is an event that targets an individual's personally identifiable information (PII), such as their name, data of birth, and passwords. It can result in the individual losing control of their bank and credit card accounts.

Similarly, an attacker might steal confidential company data or intellectual property. The attacker may then try to sell the data or exact a ransom to give it back to the company. In addition, a business may experience damage to its reputation as a result of a security breach. Customers may lose confidence in the company's ability to protect information, leading to more monetary loss for the company.

In summary, security breaches are costly. Consider the following additional research data statistics:

- The average time it takes to identify and contain a data breach is 287 days.*
- The cost of recovering from the loss of one PII record is $180.*
- The total cost of a data breach has increased by 10 percent from 2020 to 2021.*

Sources: *Ponemon Institute. 2021. Cost of a Data Breach Report 2021. Accessed November 23, 2021. https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915.

Security breach example

In December 2020, the US government suffered its worst data breach to date.*

- Attackers gained access to highly sensitive data for more than 8 months.
- Attackers exploited vulnerabilities in software and security credentials from at least three American companies.
- The attack affected other international organizations, including the UK government and the European parliament.
- The attack was widely considered to be the most costly cyberattack to date at the time.

aws re/start

The impact and reach of this data breach example emphasizes the importance of security in today's connected digital world.

Source: *Reuters. 2020. U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack. Accessed November 23, 2021. https://www.reuters.com/article/global-cyber-idUSKBN28O1Z3.

Types of threats (1 of 2)

Threat type	Description	CIA attribute affected
Malware	• Malicious software designed to disrupt the operation of a computer system, gain unauthorized access to it, or collect sensitive information from it • Examples: Virus, spyware, worm, remote access Trojan (RAT)	• Confidentiality (virus, spyware, or RAT) • Integrity (virus or RAT) • Availability (virus, worm, or RAT)
Ransomware	• Malicious code that restricts access to a computer or its data until a ransom is paid	• Availability
Denial of service (DoS)	• Attack that prevents authorized users from accessing a system	• Availability

This table lists common types of threats and identifies the areas of the CIA triad that they affect. The types of threats listed in the first part of the table are malware, ransomware, and denial of service (DoS) attack.

Some examples of malware include the following:

- **Virus**: A program that can corrupt or delete data and propagate itself from one system to another.
- **Spyware**: Code that secretly gathers information on a system and reports it to the attacker.
- **Worm**: A program that spreads itself and consumes resources destructively on a computer.
- **Remote access Trojan (RAT)**: A software tool used to gain unauthorized access to a computer in order to control it.

Note that a distributed denial of service (DDoS) is a variation of a DoS threat. A DDoS attack uses multiple machines to flood a target system with multiple requests to prevent the system's normal use.

Types of threats (2 of 2)

Threat type	Description	CIA attribute affected
Man-in-the-middle (MitM)	• Attack in which the attacker intercepts the communication between two parties and impersonates one of the parties or modifies the communication between them	• Confidentiality • Integrity
Phishing	• Technique in which the attacker masquerades as a legitimate person or business and uses email or a website to get personal information, such as passwords or credit card numbers	• Confidentiality
Social engineering	• Technique in which the attacker uses human interaction to manipulate a person into revealing sensitive information or breaking security procedures to gain access to systems or information	• Confidentiality

aws re/start

The types of threats listed in the second part of the table are man-in-the-middle (MitM) attack, phishing, and social engineering.

According to a Verizon study,* social engineering was among the top techniques used in data breaches in 2021 and accounted for over 30 percent of attacks. In a social engineering attack, an attacker uses psychological manipulation to convince an individual to take an action that compromises security.

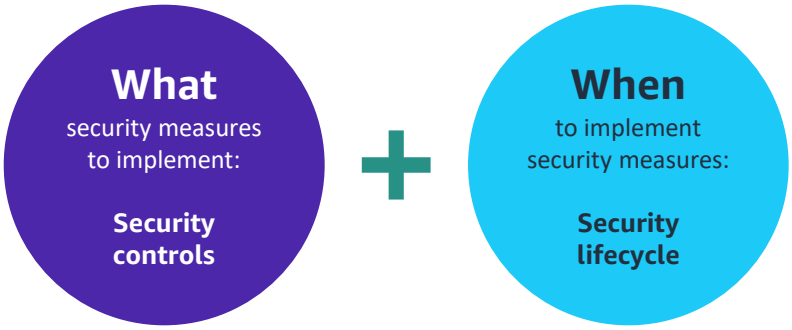
Source: *Verizon. 2021. 2021 Data Breach Investigations Report (DBIR). Accessed November 23, 2021. https://enterprise.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx.

Security strategy

Now, let’s turn to security strategy.

What is a security strategy?

A security strategy defines:



aws re/start

Businesses need a security strategy to prevent threats, eliminate vulnerabilities, and recover from breaches. At a minimum, a security strategy defines the following:

- What security measures to implement: This is achieved through security controls.
- When to implement security measures: This is defined in a security lifecycle.

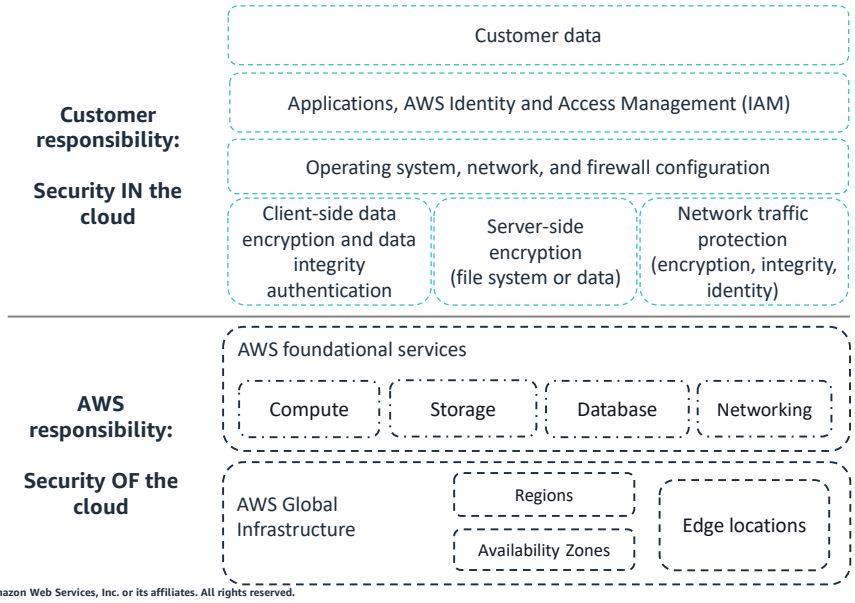
Security strategy for the cloud

A cloud security strategy defines:

aws re/start

For a cloud environment, the security strategy should also define who is responsible for implementing the different security measures.

AWS Cloud security shared responsibility model



aws re/start

In the AWS Cloud, the shared responsibility model indicates who is responsible for implementing security measures. In this model, AWS is responsible for security OF the cloud, and the customer is responsible for the security IN the cloud.

AWS handles the security of the physical infrastructure that hosts your resources, which includes the following:

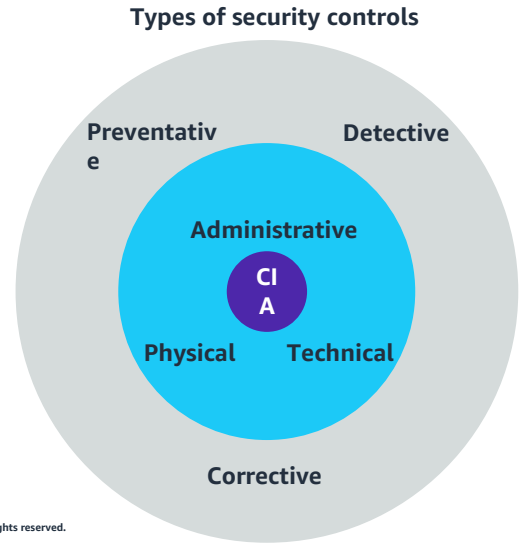
- **Data centers:** These centers are secured with controlled, need-based access and are located in nondescript facilities. In addition, security guards protect them 24 hours a day, 7 days a week.
- **Network infrastructure:** This infrastructure includes routers, switches, load balancers, firewalls, and cabling. It is protected with nearly continuous network monitoring at external boundaries, secure access points, redundant infrastructure, and intrusion detection.
- **Virtualization infrastructure**: Each compute instance is isolated from other instances.

Customers are responsible for the security of everything they put in the cloud. In particular, the customer is responsible for managing the security of their data, including the following:

- Which country that data is stored in
- Whether or not the data is encrypted
- Who has access to the data, and how those access rights are granted, managed, and revoked

What are security controls?

Security controls are measures that protect against threats and eliminate vulnerabilities.



aws re/start

Security controls are measures that protect against threats and eliminate vulnerabilities. There are three types of security controls: preventive, detective, and corrective. For each type of control, you can implement physical, technical, and administrative security measures to ensure information confidentiality, integrity, and availability.

A preventative security control protects a system from security threats before they can happen. A detective security control helps find a vulnerability early or quickly alert when a breach has happened. A corrective security control remediates a security breach.

Each type of control provides protection in three different security areas: physical, administrative, and technical. A physical control is a device or object, such as a security camera. An administrative control is usually a policy or a procedure that must be followed. Finally, a technical control is usually some software that provides security functions.

Note that each type of security control represents three stages of a security lifecycle. In the next lessons, you will learn about specific security controls that you can implement in each phase of the security lifecycle.

Security control type examples

Control type	Physical	Administrative	Technical
Preventative	Card reader devices to allow access to a building	Corporate policy stating that all employees must swipe their individual cards to access the building	Software to collect data from card readers and monitor building access traffic
Detective	Metal detector at an airport to detect weapons	Control procedures that require a report when a system is changed	Antivirus software that runs scans on regular basis
Corrective	Backup generator in a data center that turns on automatically if the power is interrupted	Business continuity plan that details how to keep the business running if a system is compromised	Antivirus software that removes malware when it is detected

This table provides some examples of preventative, detective, and corrective security controls. Each example is further categorized as a physical, administrative, or technical control.

For the preventative security control type, a card reader device that allows access to a building is an example of a physical control. To complement this control, a corporate policy should exist requiring that all persons who access the building swipe their individual cards to enter and exit. This is an example of a administrative preventative control. Finally, a software application that collects and monitors the data from the card readers is as an example of a technical preventative security control.

Typically, when implementing a security control, start by controlling the physical access to the resource if possible and applicable. Then, establish policies and procedures that describe how to define, set up, and manage the security of the resource. Finally, use a technical control to enforce secure access and usage of the resource.

Activity: Reviewing an Acceptable Use Policy (AUP)

In this activity, you will review an example Acceptable Use Policy (AUP) and answer questions regarding its administrative security content.

Activity instructions:

1) Open the file named **Acceptable Use Policy Example.pdf**.
2) Review the security-related information in the document, and then answer the questions below.
3) Be prepared to report and compare your answers with those that the instructor provides.

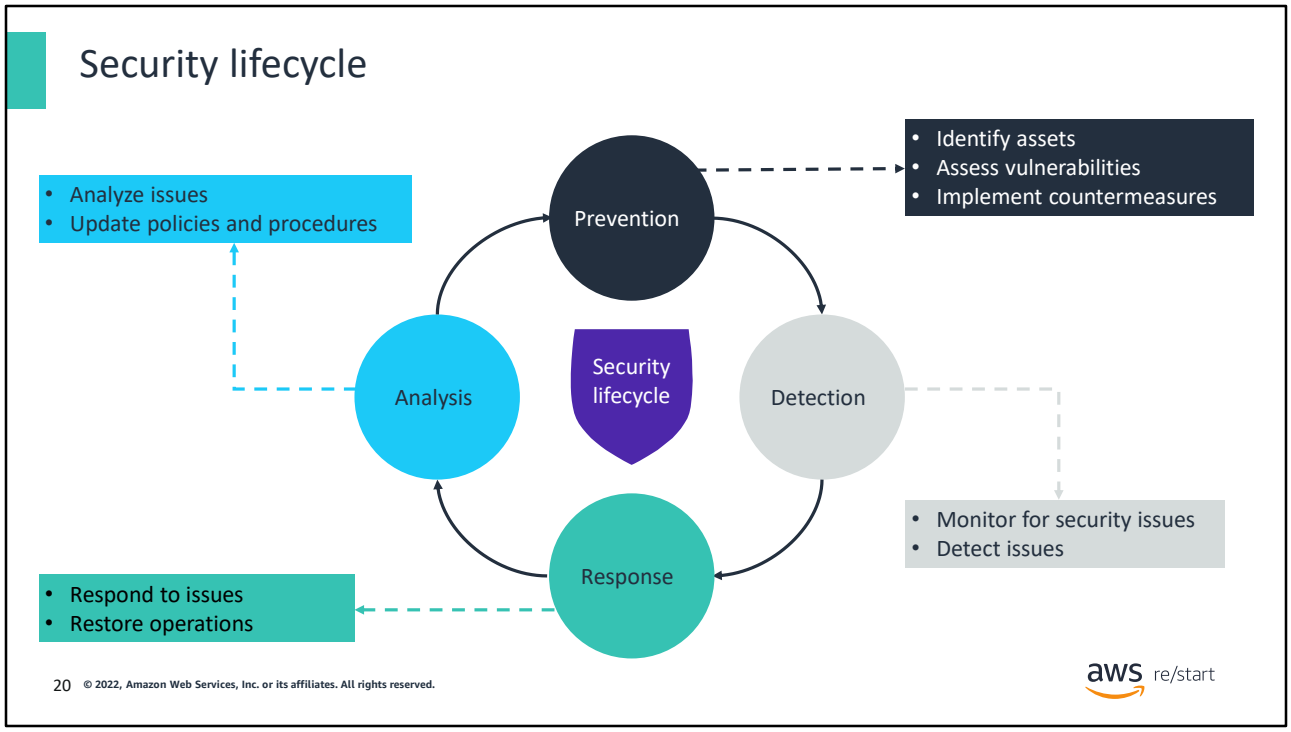
Activity questions:

1) What are three types of computing resources that are protected by this policy?
2) What are two security-related violations that are prohibited?
3) What are the consequences of violating the terms of this policy document?

aws re/start

During this activity, you look at an example of a policy document that serves as an administrative security control for using the services of a fictitious company. Follow the instructions that this slide describes to perform the activity.

In the end, the instructor will provide the answers to the questions.



An effective security strategy addresses security in stages of a lifecycle. These stages consist of prevention, detection, response, and analysis. Note that the first three stages correspond to the three types of security controls.

In the prevention stage, you identify the assets to be protected, assess their vulnerabilities, and implement measures to remove any discovered vulnerability.

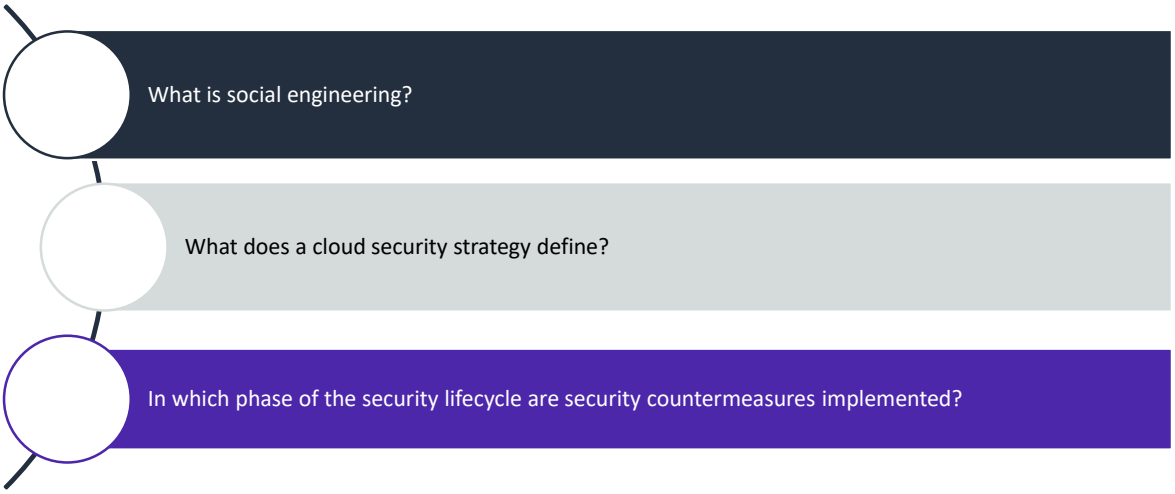
In the detection stage, you implement monitoring solutions to quickly identify and generate alerts if a breach is detected.

In the response (or corrective) stage, you perform the corrective tasks to eliminate the breach and restore normal operations.

Finally, in the analysis stage, you review the steps used to resolve the issue and identify any lessons learned. If necessary, you update your security policies and procedures to make adjustments based on the result of the analysis.

In the next lessons, you will examine the details of each phase of the security lifecycle, including the security controls that each one uses.

Checkpoint questions



aws re/start

1. Social engineering is a type of security threat where an attacker uses human interaction to manipulate a person into revealing sensitive information.

2. A cloud security strategy defines:
    - What security measures to implement (security controls)
    - When to implement security measures (security lifecycle)
    - Who is responsible to implement security measures (security responsibility)

3. Security countermeasures are implemented in the Prevention phase of the security lifecycle.

Key takeaways

- Security is the practice of protecting valuable assets.
- **Confidentiality**, **integrity**, and **availability** are three important perspectives when addressing information security.
- Common types of security issues include **malware**, **phishing**, and **social engineering**.
- An effective security strategy implements **security controls** throughout a **security lifecycle**. A cloud security strategy also defines **security responsibilities**.
- Security controls can be **physical**, **administrative**, or **technical**.
- The phases of the security lifecycle are **prevention**, **detection**, **response**, and **analysis**.

aws re/start

Key takeaways from this lesson include the following:

- Security is the practice of protecting valuable assets.
- Confidentiality, integrity, and availability are three important perspectives when addressing information security.
- Common types of security issues include malware, phishing, and social engineering.
- An effective security strategy implements security controls throughout a security lifecycle. A cloud security strategy also defines security responsibilities.
- Security controls can be physical, administrative, or technical.
- The phases of the security lifecycle are prevention, detection, response, and analysis.

Thank you

aws re/start