SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-9: Advanced persistent threat analytics tools

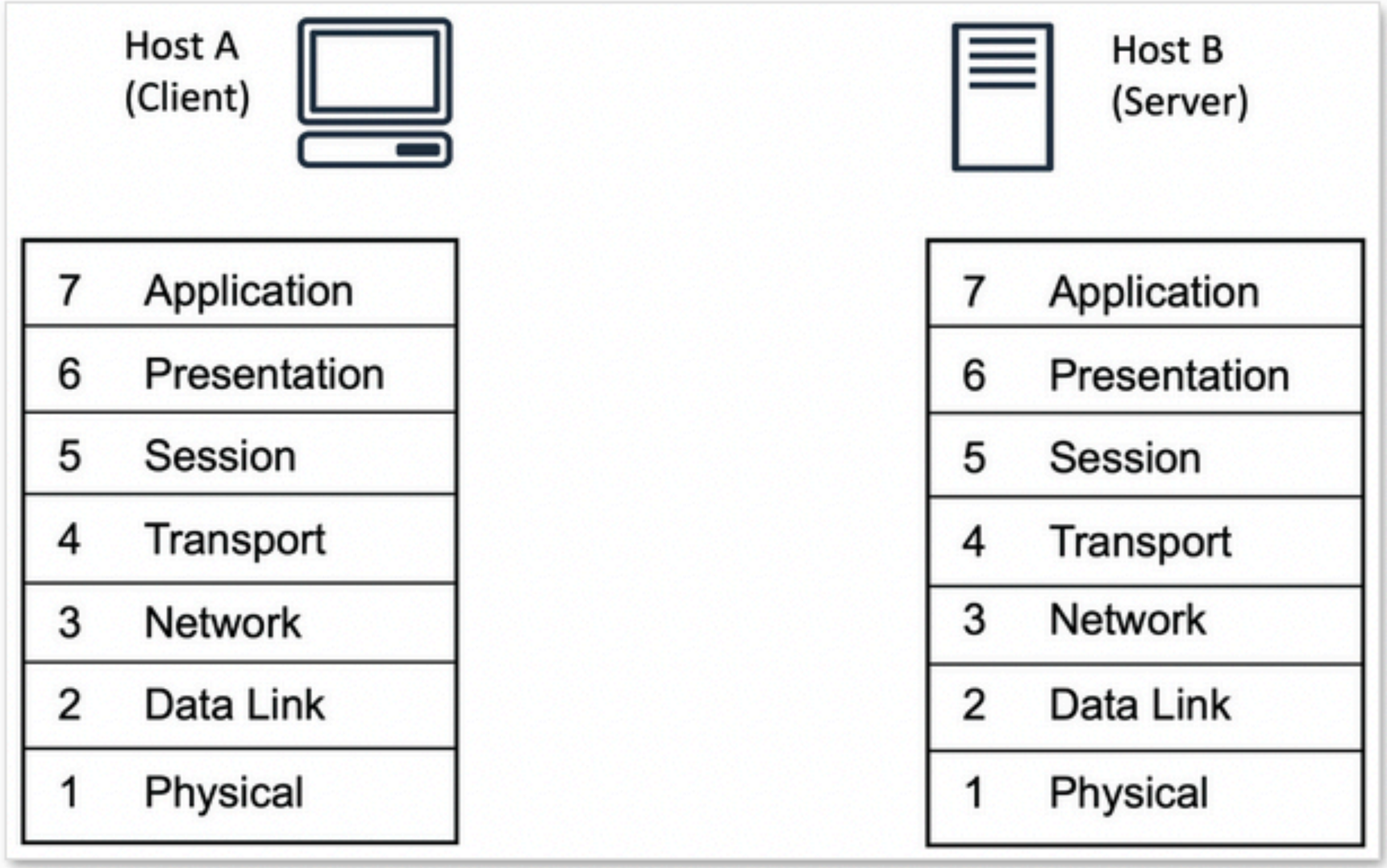
This lecture will shift our focus from traditional cyber-attacks to targeted attacks. We will learn about the following frameworks and simulators to reinforce our understanding.

- MITRE ATT&CK and Shield tools
- Kill chain and Diamond Model
- ATP Simulator and Caldera

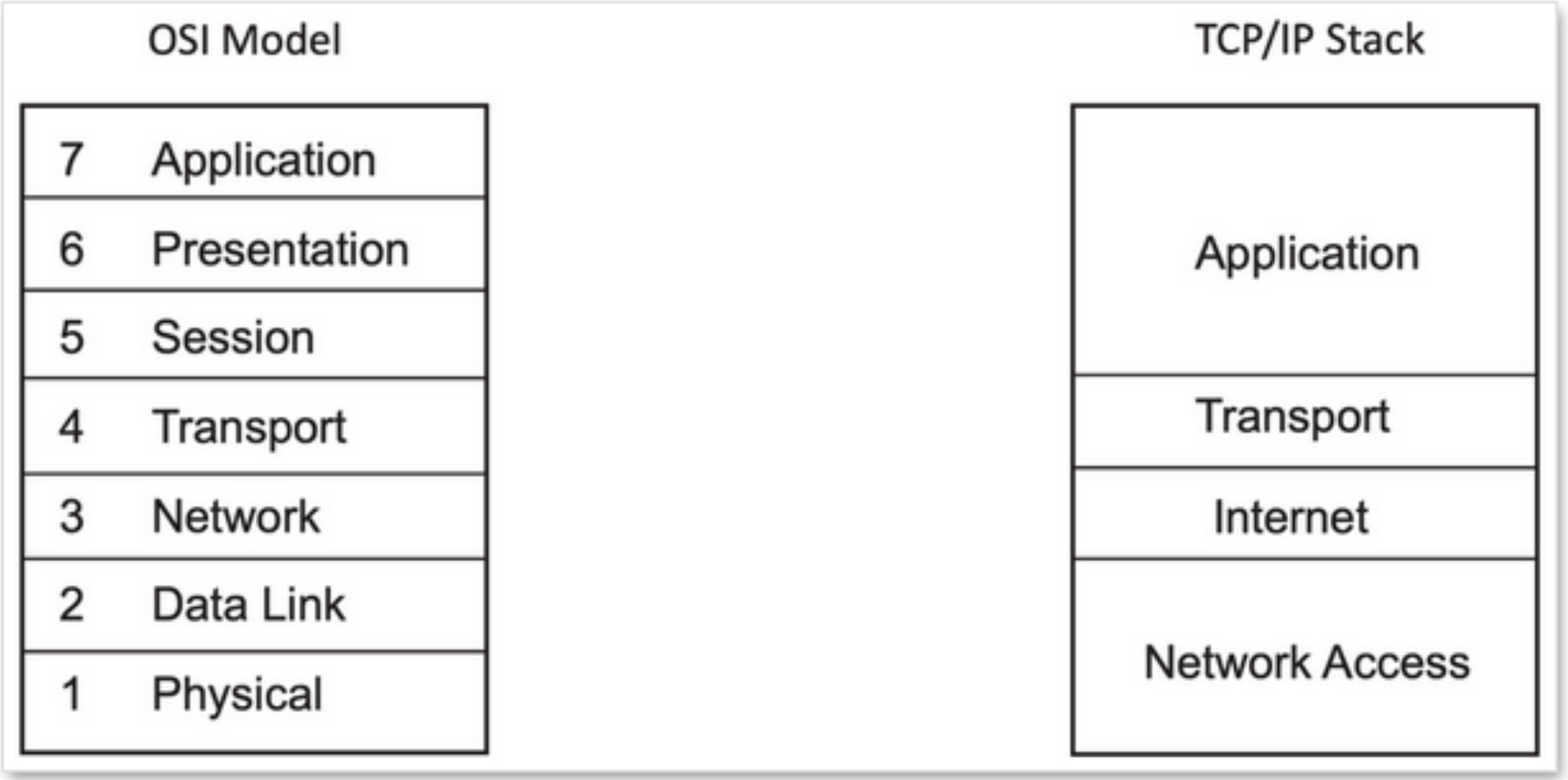
Goal of the Lecture

Today's lecture will part knowledge and skills required to understand AWS security tools. You will get access to ucertify.com website to perform lab exercises and prepare for AWS security certification.

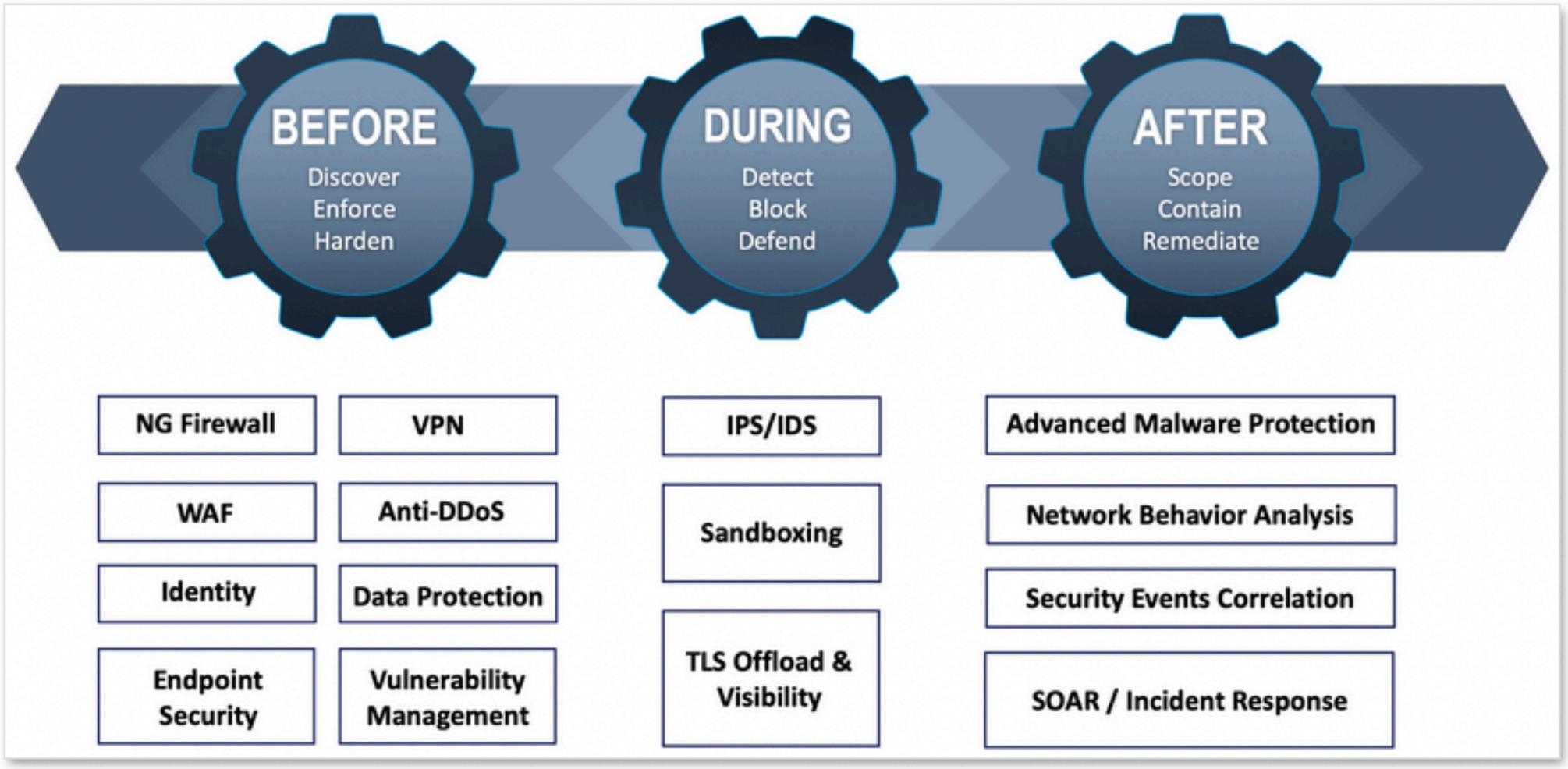
The OSI Model



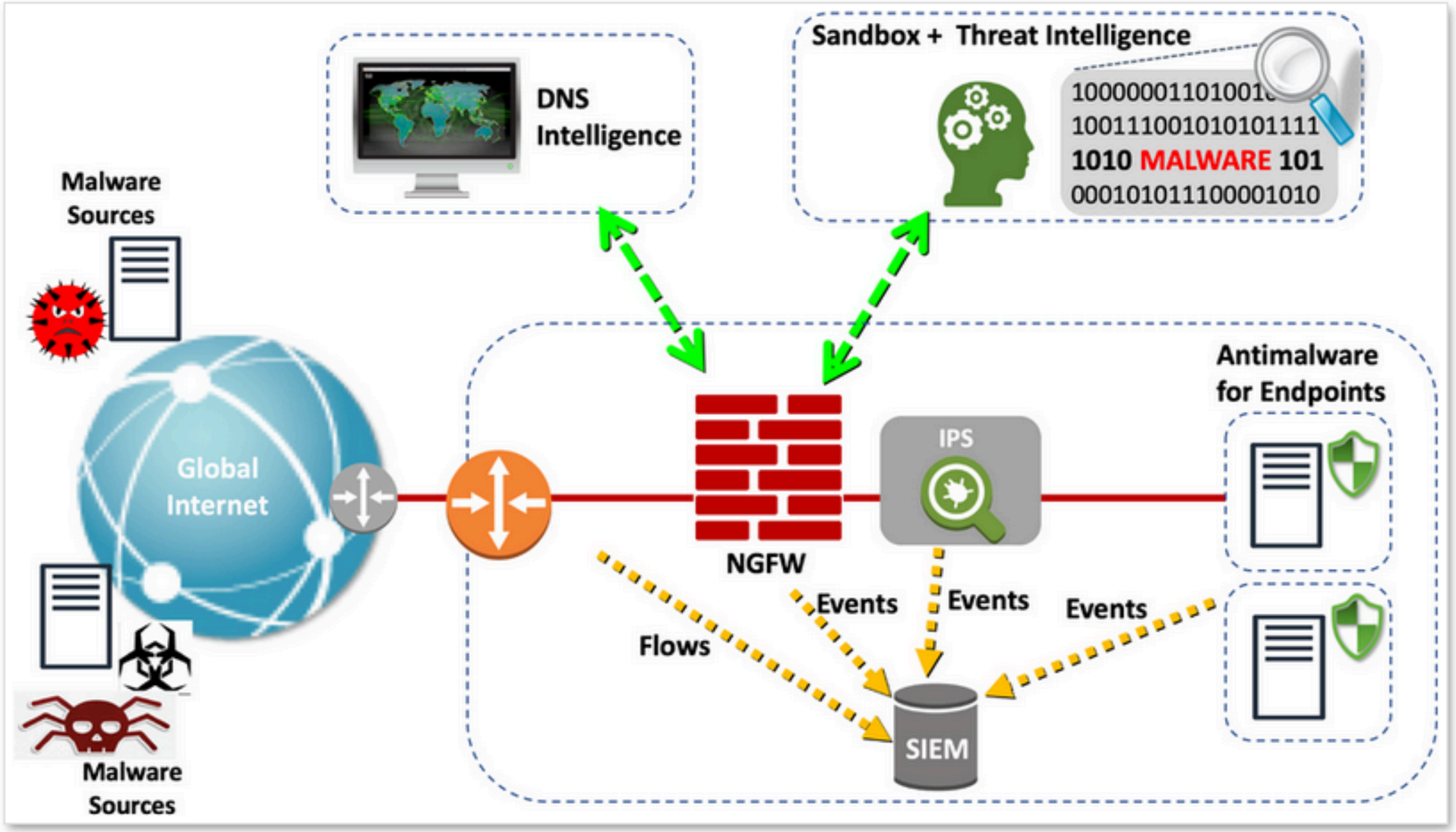
The OSI & TCP/IP Model



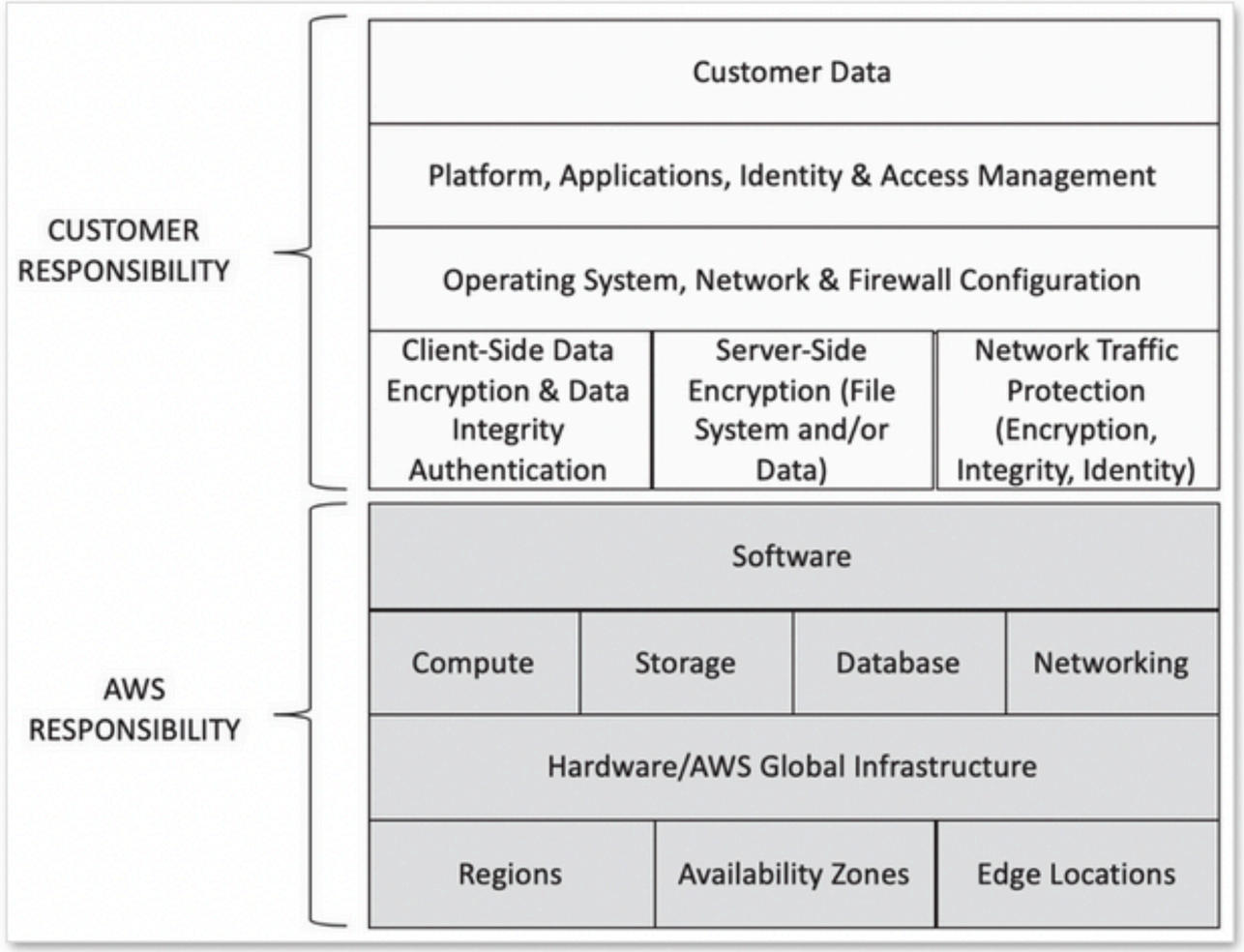
Attack Continnum Model (ACM)



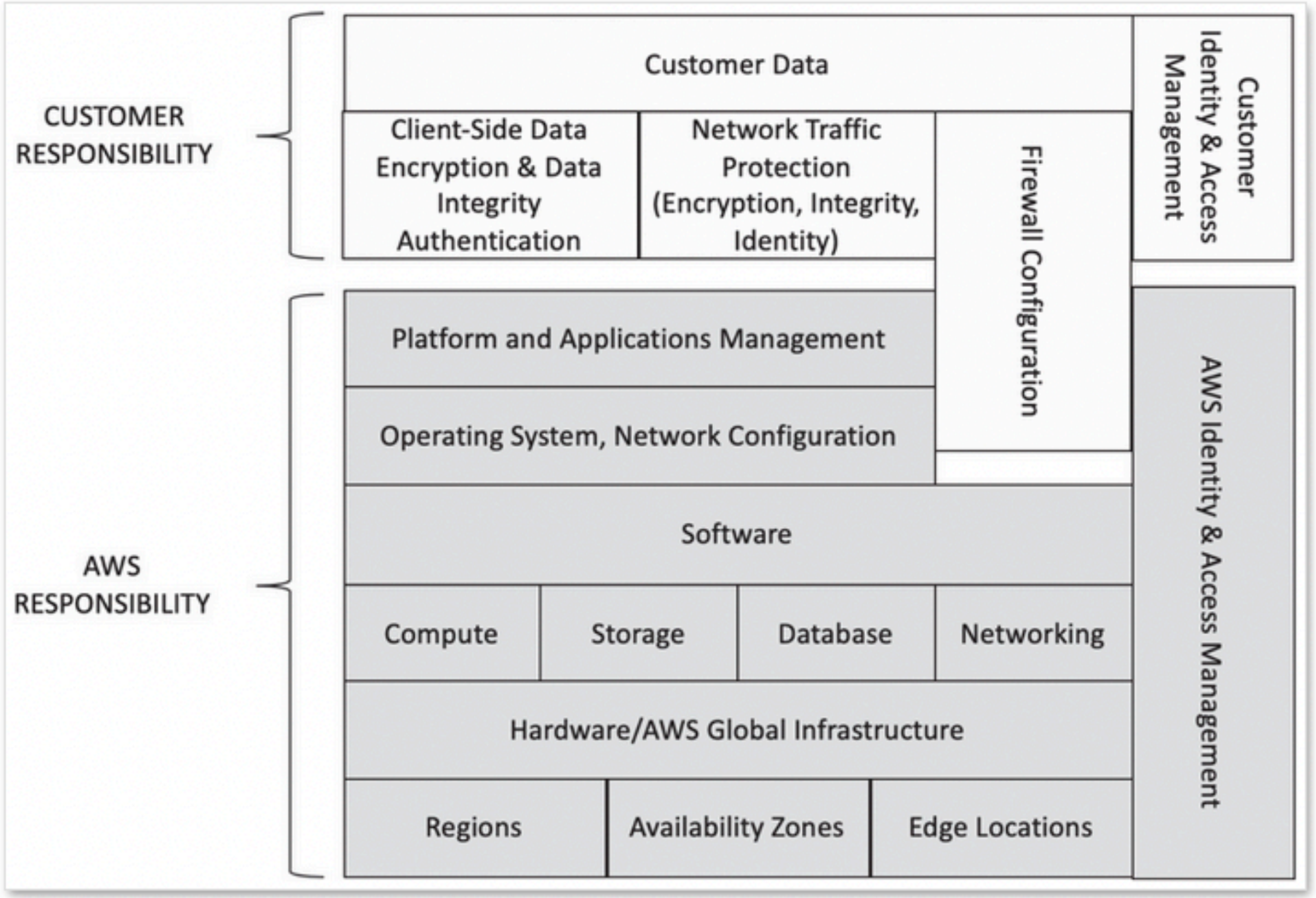
ACM for Malware Protection



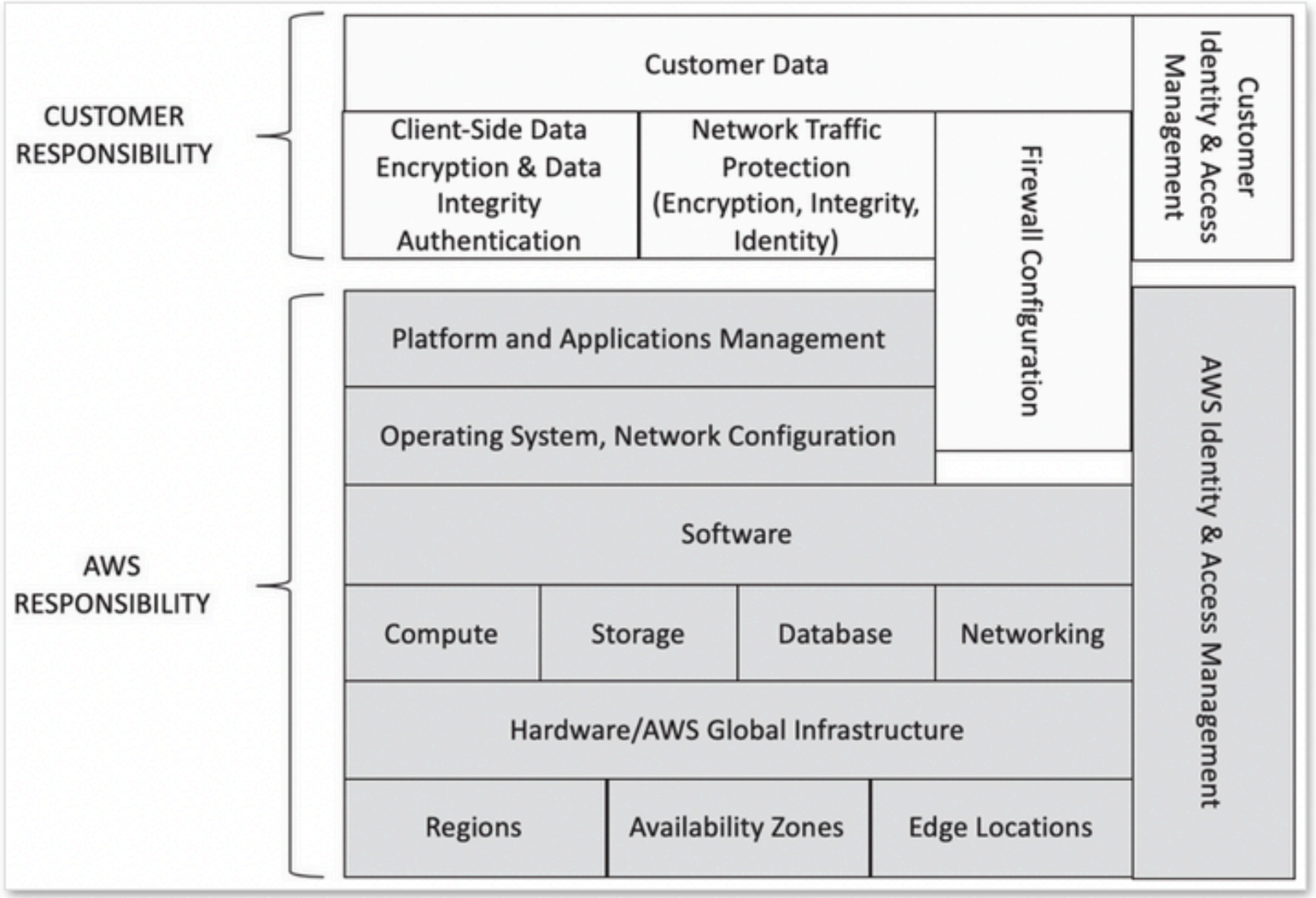
IaaS Shared Responsibility



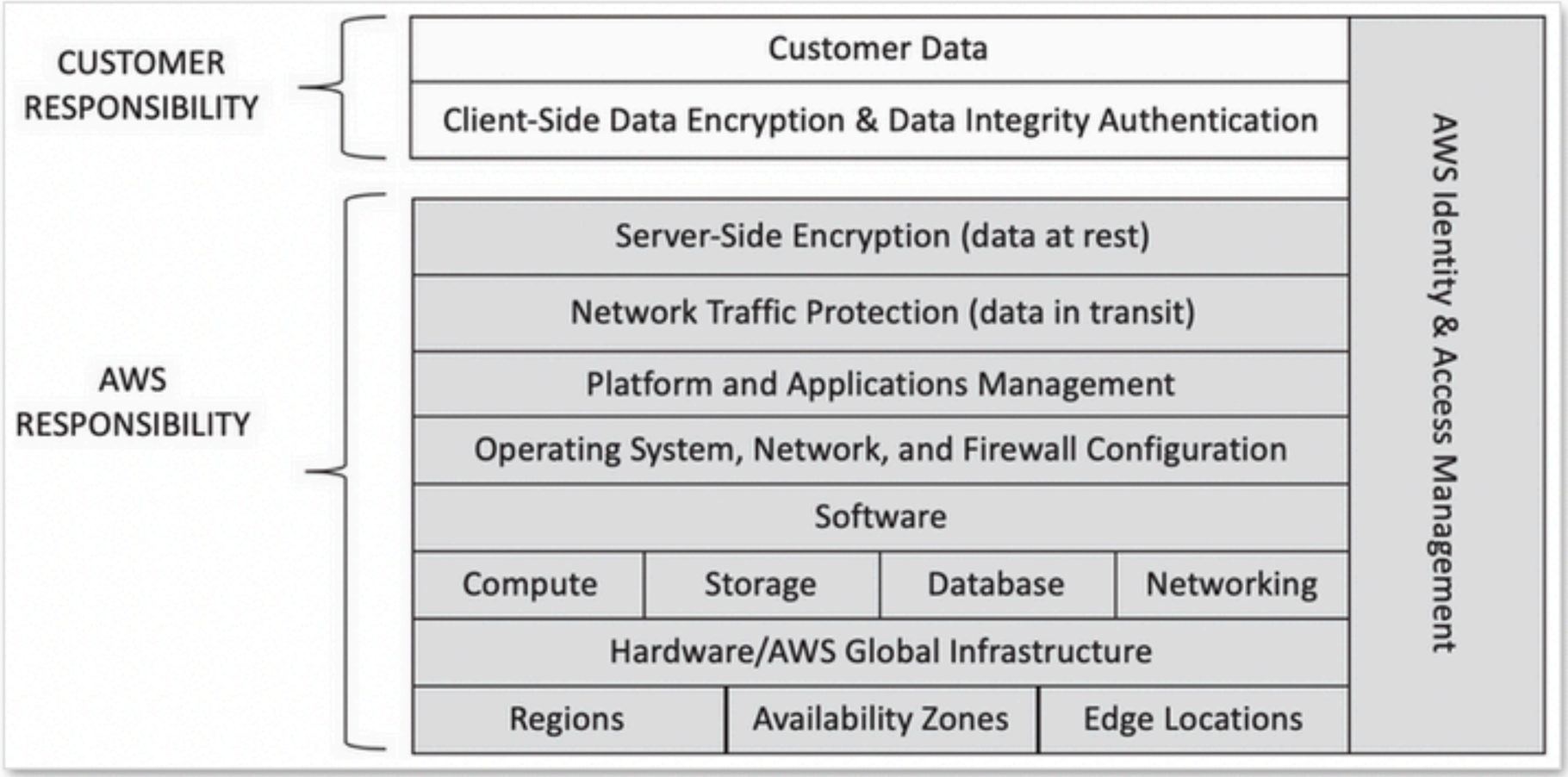
PaaS Shared Responsibility



PaaS Shared Responsibility



SaaS Shared Responsibility



https://docs.aws.amazon.com/security/
https://aws.amazon.com/artifact/
https://aws.amazon.com/architecture/well-architected

AWS Well-Architected Framework

- **Know how to use the Well-Architected Framework.** Understand that the AWS Well-Architected Framework has five pillars, one of which is security. In the security pillar, there are seven security design principles:

  1. Implement a strong identity foundation.
  2. Enable traceability.
  3. Apply security at all layers.
  4. Automate security best practices.
  5. Protect data in transit and at rest.
  6. Keep people away from data.
  7. Prepare for security events.

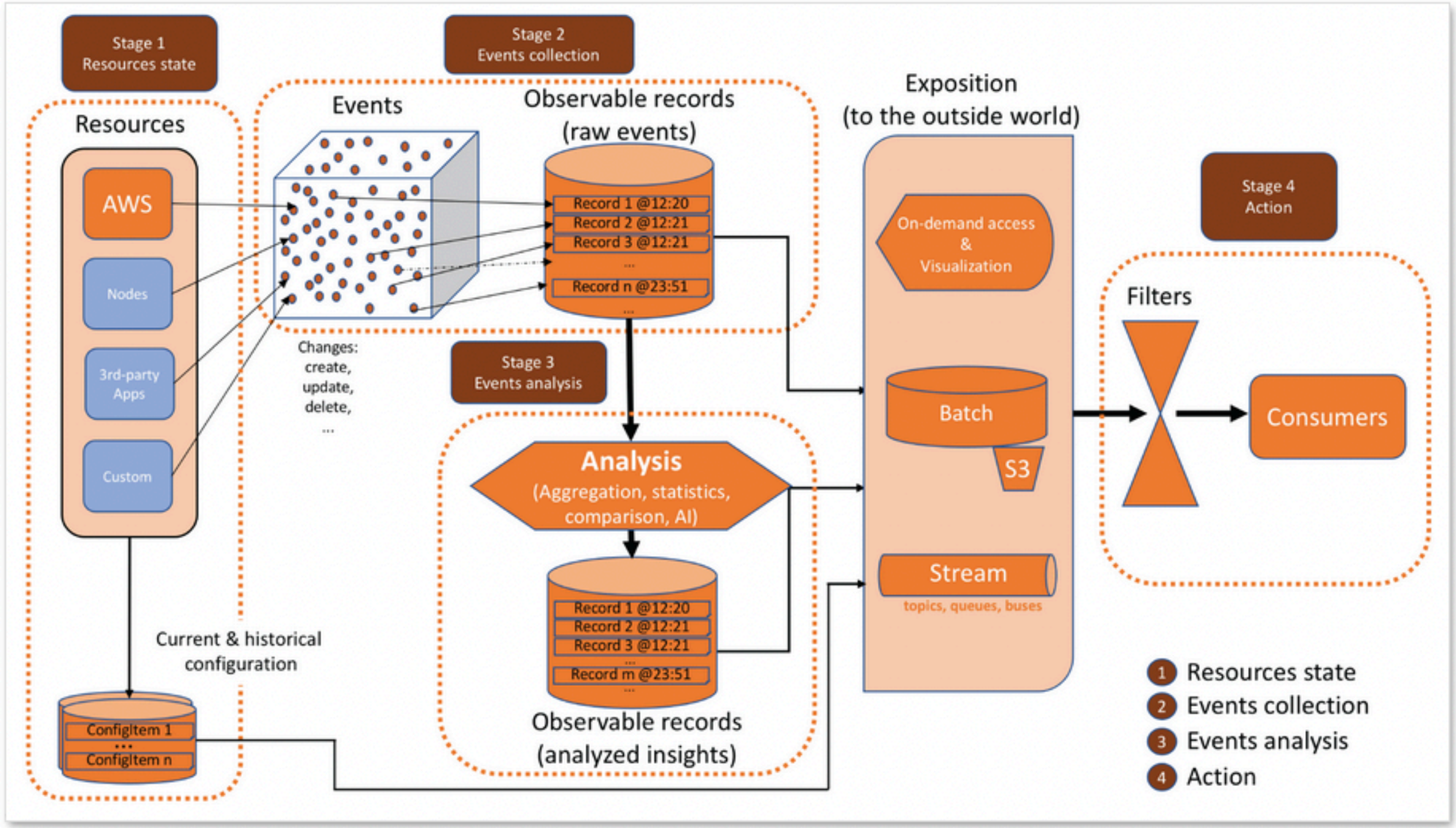
  Also defined as part of the Well-Architected security pillar are five security best practices areas:

  - Identity and access management
  - Detective controls
  - Infrastructure protection
  - Data protection
  - Incident response

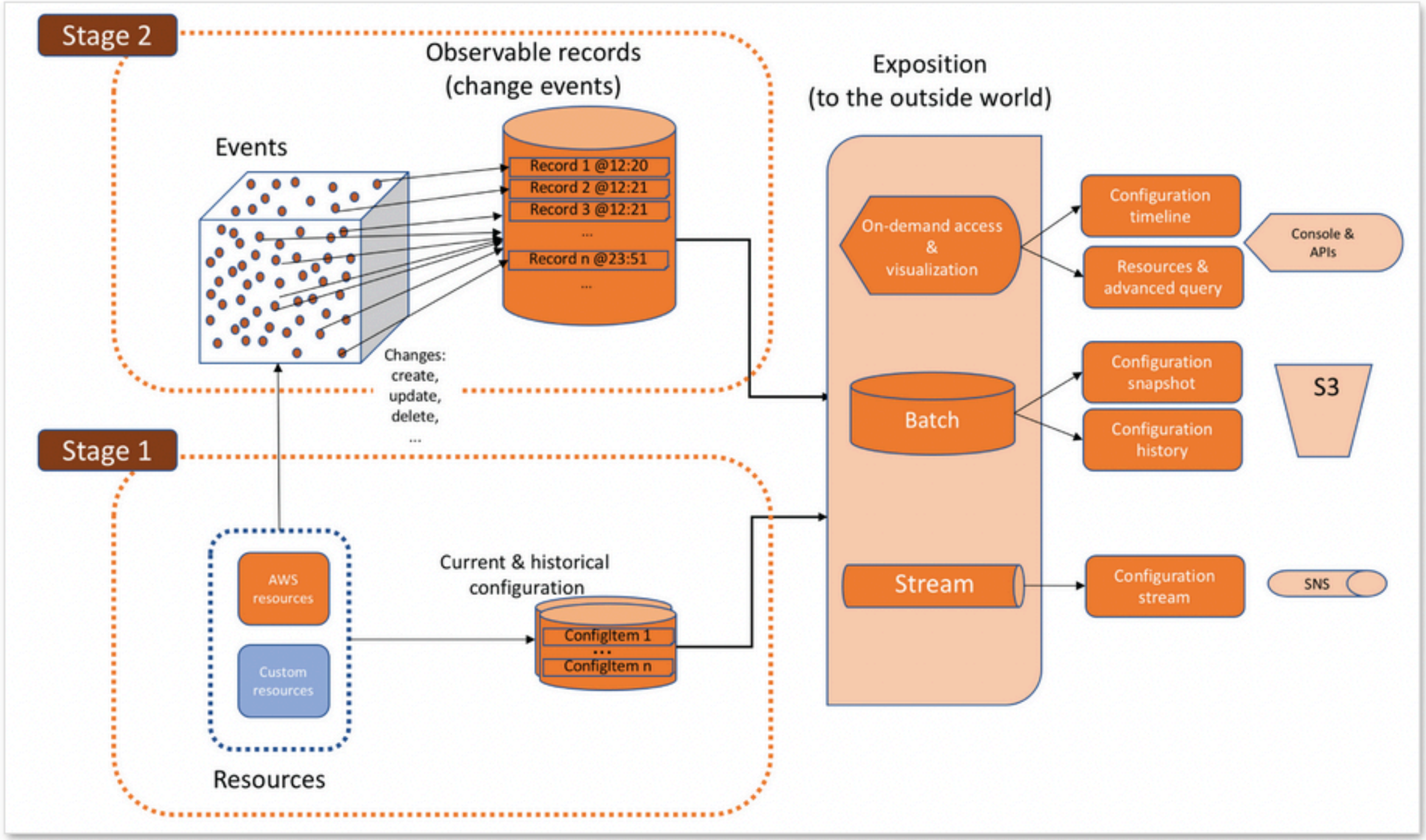
Q&A: Indicate if each of the given statements about AWS IAM is true or false.

Statement	True	False
It provides a set of TCPs that control access to the user's resources on the AWS Cloud.		
It gives the users the ability to define the nonrepudiation methods for using the resources in their accounts.		
It empowers the users to define strict access rules for individuals and other systems for manipulating resources in a specific account.		
It makes access to AWS resources possible for applications that are running on-premises or in the AWS Cloud.		

Detective Controls Flow Framework



AWS Configs & Detective Controls



Which of the following statements is true about GDPR?

A ○ It not only applies to transactions that occur within the EU members but also governs the transfer of personal data outside the EU.

B ○ It recognizes that the cybersecurity activities inside an organization should be guided by its business drivers.

C ○ It is a set of security standards for protecting certain health information that is transferred or held in electronic form.

D ○ It was created with the goal of increasing the level of protection for issuers of credit cards.

Explanation

Answer D is correct.

GDPR (General Data Protection Regulation) is a set of rules created by the EU (European Union) that requires businesses to protect the personal data and privacy of EU citizens. It not only applies to transactions that occur within the EU members but also governs the transfer of personal data outside the EU. This regulation states that foreign entities willing to conduct business with EU companies also need to demonstrate their compliance with GDPR. This fact motivated the creation of GDPR-like standards outside Europe.

Answer C is incorrect. NIST CSF (National Institute for Standards and Technology Cybersecurity Framework) is a publication that results from a collaborative work among industry, academia, and the U.S. government. The framework recognizes that the cybersecurity activities inside an organization should be guided by its business drivers. It also establishes that the overall risk management process should include the risks pertaining to the cybersecurity domain. The CSF assembles standards, guidelines, and practices that have proved effective and may be used by entities belonging to any market segment.

Answer A is incorrect. PCI DSS (Payment Card Industry Data Security Standard) was created with the goal of increasing the level of protection for issuers of credit cards by requiring that merchants meet minimum levels of security when they process, store, and transmit cardholder data.

Answer B is incorrect. HIPAA (Health Insurance Portability and Accountability Act) is a set of security standards for protecting certain health information that is transferred or held in electronic form.

Which of the following are the default master keys that protect S3 objects, Lambda functions, and Workspaces?

A ○ AWS-managed keys

B ○ AWS Certificate Manager

C ○ Customer-managed keys

D ○ Custom key stores

Explanation

Answer A is correct.

AWS-managed keys are the default master keys that protect S3 (Simple Storage Service) objects, Lambda functions, and Workspaces when no other keys (customer-managed keys) are defined for these services.

Answer C is incorrect. Customer-managed keys are CMKs (customer master keys) that the users can create and administer using JSON (JavaScript Object Notation) policies.

Answer B is incorrect. AWS Certificate Manager is a managed service that allows the users to quickly provision, manage, and deploy SSL/TLS (secure sockets layer/Transport Layer Security) certificates for use with both AWS Cloud-native services and their internal resources.

Answer D is incorrect. Custom key stores are used when the users want to manage their CMKs using a dedicated AWS CloudHSM cluster, giving them direct control to the HSMs (hardware security modules) that generate and manage the key material for the CMKs and perform cryptographic operations with them.

Which of the following provides a target in the VPC route tables for the Internet-routable traffic?

A ○ Network access control lists

B ○ Egress-only Internet gateways

C ○ Security groups

D ○ Internet gateways

Explanation

Answer D is correct.

Internet gateways provide a target in the VPC (virtual private cloud) route tables for the Internet-routable traffic (default route). They also perform NAT (network address translation) for instances that have been assigned the public IPv4 addresses and they support IPv6 traffic.

Answer B is incorrect. Egress-only Internet gateways are only used to enable outbound IPv6 traffic from the VPC.

Answer C is incorrect. Security groups are stateful, which means that the return traffic from an allowed inbound connection is automatically permitted to leave the instance and the users do not have to define a corresponding outbound rule to allow it.

Answer A is incorrect. Network access control lists are the network traffic control objects that act as firewalls when the traffic enters or leaves a subnet in the VPC. The users can add this extra layer of traffic filtering to avoid unexpected traffic between subnets regardless of what they have deployed on them.

What is the hash code size of SHA-1?

A	○	128
B	○	512
C	○	5256
D	○	160

Explanation

Answer D is correct.

The hash code size of SHA-1 (Secure Hash Algorithm) is 160. Here's the table showing the hash algorithms:

Name	Hash code size
MD5 (Message-Digest 5)	128
SHA-1	160
SHA-256	256
SHA-384	384
SHA-512	512

Table A: Hash algorithms

Which of the following AWS services uses machine learning and artificial intelligence technology to discover, classify, and protect the sensitive data in the AWS Cloud?

A ○ AWS Certificate Manager

B ○ Amazon S3

C ○ AWS CloudHSM

D ○ Amazon Macie

Explanation

Answer D is correct.

Amazon Macie is a security service that uses machine learning and artificial intelligence technology to discover, classify, and protect the sensitive data in the AWS Cloud, searching S3 (Simple Storage Service) buckets to create an inventory of the sensitive data, PII (personally identifiable information), or intellectual property while providing dashboards and alerts that show suspicious access and unusual data-related activity.

Answer B is incorrect. Amazon S3 is an object storage service that offers the ability to store large amounts of data for a variety of use cases, such as public site code that can be accessed by users, backing up and restoring files, images, business applications, and IoT devices. It is also a centerpiece for using big data and analytics in the AWS environment.

Answer A is incorrect. AWS Certificate Manager is a managed service that allows the users to quickly provision, manage, and deploy SSL/TLS (secure sockets layer/Transport Layer Security) certificates for use with both AWS Cloud-native services and their internal resources.

Answer C is incorrect. AWS CloudHSM is a managed service that automates administration tasks, such as hardware provisioning, software patching, high availability configurations, and key backups. AWS CloudHSM lets the users scale quickly by adding or removing on-demand HSM (hardware security module) capabilities in a pay-as-you-go model.

Which of the following activities of the IP routing function can be achieved by manual definition of static routes or by using dynamic routing protocols?

A ○ Searching for the longest prefix match

B ○ Building the routing table

C ○ Forwarding the packet on the outgoing interface

D ○ Gathering routing information

Explanation

Answer D is correct.

The IP routing function can be divided into four basic activities:

1. **Gathering routing information:** It can be achieved by manual definition of static routes or by using dynamic routing protocols, such as OSPF (Open Shortest Path First), RIP (Routing Information Protocol), or BGP (Border Gateway Protocol).
2. **Building the routing table:** Before installing a path in this table, a router sequentially performs two comparisons. First, if more than one equal-length network prefix is available to a destination, the router will prefer the one with the lowest administrative distance. The second comparison is for two equal-length prefixes that have the same value for the administrative distance parameter, a router will choose the one with the lowest cost under the perspective of the particular routing protocol.
3. **Searching for the longest prefix match:** When a packet arrives at the incoming interface, its destination IP address is extracted and compared with the available entries in the routing table. The comparison that results in the longest bitwise match for the network mask is selected. The last possibility of finding such a match is to use a default route if one is configured.
4. **Forwarding the packet on the outgoing interface:** When a match happens in step 3, it will point to an entry in the routing table that has a corresponding outgoing interface.

Why is the presentation layer sometimes referred to as the translation layer?

A ○ Because it is responsible for the physical connection between the devices

B ○ Because it concerns routing a unit of data from one given source to a destination

C ○ Because it is aimed at providing a reliable message delivery

D ○ Because it deals with the syntax and semantics of the data being transmitted

Explanation

Answer D is correct.

The presentation layer is sometimes referred to as the translation layer because it deals with the syntax and semantics of the data being transmitted. This layer is what makes it possible for devices that employ different data representations to communicate. The data structures being exchanged can be defined in an abstract way, along with a standard encoding to be used over the transmission media.

Answer C is incorrect. The transport layer is aimed at providing a reliable message delivery from the source to the destination host, irrespective of the types and the number of physical or logical networks traversed along the path. This layer is also able to confirm or acknowledge the successful data transmission and to trigger retransmission if errors are detected.

Answer B is incorrect. The main task of the network layer concerns routing a unit of data from one given source to a destination that resides on a different network that is potentially connected by means of a different data link layer technology.

Answer A is incorrect. The physical layer is responsible for the physical connection between the devices and is concerned with transmitting raw bits over a communication channel. The main design issues include dealing with mechanical, electrical, optical, and timing interfaces as well as with ensuring that when one side sends 1 bit, it is accurately received by the other side as 1 bit, and not as 0 bit.

You, as the head of the networking department, are asked to choose a path over which the datagrams, destined to a particular host, will be sent. Which of the following will help you in the given scenario?

A ○ IP routing

B ○ Sniffing

C ○ Network eavesdropping

D ○ IP spoofing

Explanation

Answer A is correct.

IP routing will help you in the given scenario. It deals with the choice of a path over which the IP packets or datagrams, destined to a particular host, will be sent. Even though some techniques employ additional attributes, the classic definition of routing considers the destination IP address as the only criterion for path selection.

Answer D is incorrect. IP spoofing is the act of copying or falsifying a trusted source IP address. It is frequently used as an accessory resource for performing innumerable types of attacks.

Answers B and C are incorrect. Network eavesdropping, also called sniffing, is an attack targeted at the confidentiality attribute of data. The goal is to obtain valid username and password combinations.

Which of the following is a client application that performs the authentication of the users against the IdPs?

A ○ Identity pool

B ○ Identity broker

C ○ User pool

D ○ SCP

Explanation

Answer B is correct.

An identity broker is a client application that performs the authentication of the users against the IdPs (identity providers). It then obtains the AWS temporary security credentials and provides the users with access to the AWS resources.

Answer C is incorrect. A user pool is a secure directory within Amazon Cognito that allows the users to manage the users of their web or mobile applications in one single place. Users in a user pool can sign in with their registered credentials or by using a social identity from web providers, such as Amazon, Google, Facebook, or Apple. Additionally, they can use SAML (Security Assertion Markup Language) 2.0 or OpenID Connect with the enabled identity providers.

Answer A is incorrect. Amazon Cognito identity pool allows the users to create unique identifiers for the guest users who access their application and authenticate these users with identity providers. The users can then exchange these identities with temporary, limited-privilege AWS credentials to access the other AWS services.

Answer D is incorrect. The users can use the SCP (service control policy) to centrally manage the availability of the service actions across the multiple AWS accounts within their AWS Organizations deployment. SCPs are similar to the IAM (Identity and Access Management) policies and have the same syntax.

Which of the following IP address blocks encompasses the addresses that are **not** valid on the Internet?

A ○ 192.178.0.0 to 192.178.255.255

B ○ 192.168.0.0 to 192.168.255.255

C ○ 192.168.0.0 to 192.168.255.256

D ○ 192.168.0.0 to 192.168.256.255

Explanation

Answer B is correct.

The three special IP address blocks which encompass the addresses that are not valid on the Internet are:

- 10.0.0.0 to 10.255.255.255 (10/8 prefix)
- 172.16.0.0 to 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Which of the following statements is true about the root user credentials?

A ○ It gives the users unrestricted access to all the AWS resources in the account.

B ○ It gives administrators the granularity required to control how users should interact with AWS resources.

C ○ It persists within the AWS accounts where they were created but may have cross-account permissions.

D ○ It allows administrators to manage users with similar permissions requirements.

Explanation

Answer A is correct.

The root user credentials give the users unrestricted access to all the AWS resources in the account. This access covers viewing the billing information, changing the root account password, and performing the complete termination of the account and deletion of its resources.

Answers B and C are incorrect. IAM (Identity and Access Management) users are people or applications in the organization. They persist within the AWS accounts where they were created but may have cross-account permissions if configured to do so. Each IAM user has its own username and password that give them access to the AWS Console. Additionally, it's also possible to create an access key to provide users with programmatic access to AWS resources. IAM user is a concept that gives administrators the granularity required to control how users should interact with AWS resources.

Answer D is incorrect. An IAM group is a good way to allow administrators to manage users with similar permissions requirements. Administrators can create groups that are related to job functions or teams, such as administrators, developers, FinOps, operations, and so on. They can then assign fine-grained permissions to these groups.

Your organization is experiencing performance degradation. On further investigation, it is found that the organization's website is attacked by a malicious bot and it collects the data for content reselling. Which of the following are a type of malicious bots that have attacked the organization?

A ○ HTTP floods

B ○ Scanners

C ○ Probes

D ○ Scrapers

Explanation

Answer D is correct.

Scrapers are a type of malicious bots that have attacked the organization. Malicious bots, also known as bad bots, are software applications that run automated tasks over the Internet that harm their victims in some way or cause an undesired result, such as performance degradation. Scrapers are a particular type of malicious bot that collects the data from the victim's website for malicious purposes, such as content reselling or price undercutting.

Answers A, C, and B are incorrect. You should use WAF (Web Application Firewall) Security Automation to protect your web application that is hosted in AWS from a malicious bot. AWS WAF offers AWS Managed Rules and allows the customers to leverage the signatures from the partners, such as Fortinet, Cyber Security Cloud, GeoGuard, F5, and Imperva. AWS Managed Rules protect against the common attacks on the applications, such as SQL (Structured Query Language) injection and cross-site scripting. To cover the other kinds of attacks, such as bad bots, scrapers, HTTP (Hypertext Transfer Protocol) floods, scanners, and probes, the implementation of other mechanisms, such as the WAF Security Automations solution, is needed.

Which of the following statements is true about security groups?

A ○ They are stateful, which means that the return traffic from an allowed inbound connection is manually permitted to leave the instance.

B ○ They are stateless, which means that the return traffic from an allowed inbound connection is automatically permitted to leave the instance.

C ○ They are stateless, which means that the return traffic from an allowed inbound connection is manually permitted to leave the instance

D ○ They are stateful, which means that the return traffic from an allowed inbound connection is automatically permitted to leave the instance.

Explanation

Answer D is correct.

Security groups are stateful, which means that the return traffic from an allowed inbound connection is automatically permitted to leave the instance and the users do not have to define a corresponding outbound rule to allow it.

Which of the following is an entity, which defines the resources that the service will evaluate when the evaluation will occur and what remediation action to take?

A ○ AWS Security Hub

B ○ Amazon Inspector

C ○ Amazon GuardDuty

D ○ AWS Config rule

Explanation

Answer D is correct.

An AWS Config rule is an entity, which defines the resources that the service will evaluate when the evaluation will occur and what remediation action to take. These rules can be configured to trigger in three ways:

- On a periodic basis
- When a configuration change is detected
- On-demand

Answer B is incorrect. Amazon Inspector focuses on evaluating the security status of an Amazon EC2 (Elastic Compute Cloud) instance. It provides insights into the security issues or vulnerabilities. The service gathers this information at the network level (network assessment) or directly from the instance operating system and applications, through an installed Amazon Inspector agent (host assessments).

Answer A is incorrect. AWS Security Hub is a service that consolidates security information about the AWS resources and presents it in a single pane. AWS Security Hub receives information from other AWS security services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Firewall Manager, and IAM (Identity and Access Management) Access Analyzer, as well as integrated third-party security products or from the custom security applications.

Answer C is incorrect. Amazon GuardDuty analyzes the selected logs to produce the observable records of suspicious activities, which are known as findings. The logs that the service uses come from Amazon VPC (Virtual Private Cloud) Flow Logs, AWS CloudTrail, and DNS (Domain Name System) queries.

Which of the following is a security countermeasure format?

A ○ Ensuring that someone cannot deny that they have performed an action

B ○ Verification of user identity before granting access to the critical data

C ○ Ensuring reliability and an acceptable level of performance for the legitimate users

D ○ Prevention of unauthorized disclosure of sensitive information

Explanation

Answer B is correct.

Within a computing environment, the mechanisms aimed at risk mitigation are called security countermeasures or security controls. They can come in multiple formats, including the following:

- Software patching
- Implementation of security capabilities that are specifically designed as defensive resources
- Verification of user identity before granting access to the critical data

Answer D is incorrect. Confidentiality is concerned with the prevention of unauthorized disclosure of sensitive information and ensuring that a suitable level of privacy is ensured at all stages of data processing. Encryption is an example of a technology designed with confidentiality in mind.

Answer A is incorrect. Nonrepudiation is the property of ensuring that someone cannot deny that they have performed an action in an effort to avoid being held accountable. In the IT security world, examples of nonrepudiation are someone denying that a certain system transaction has been carried out or a user denying the authenticity of its own signature.

Answer C is incorrect. Availability focuses on ensuring reliability and an acceptable level of performance for the legitimate users of computing resources. Provisions must be made against the eventual failures in the operating environment, which includes the existence of well-designed recovery plans at both the physical and logical levels.

Final Exam

Format

- 50 Questions
  - Multiple choice
  - True-False
  - Multiple Answers

Content

- Content from all 10 classes
- Review lecture recordings
- Lecture slides
- Questions AWS Security Study Guide