# 212-82Q&As

Certified Cybersecurity Technician(C|CT)

## Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.passapply.com/212-82.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

**QUESTION 1**

Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIFM from a control room. The SIEM detected suspicious activity and sent an alert to the camera. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers.

Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

A. Application log monitoring

B. Log Retention

C. Dashboard

D. Data aggregation

Correct Answer: C

Explanation: Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

**QUESTION 2**

Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. Which of the following firefighting systems did Calvin use in this scenario?

A. Fire detection system

B. Sprinkler system

C. Smoke detectors

D. Fire extinguisher

Correct Answer: D

Explanation: Fire extinguisher is the firefighting system that Calvin used in this scenario. A firefighting system is a system that detects and suppresses fire in a physical location or environment. A firefighting system can consist of various components, such as sensors, alarms, sprinklers, extinguishers, etc. A firefighting system can use various agents or substances to suppress fire, such as water, foam, gas, powder, etc. A fire extinguisher is a portable device that contains an agent or substance that can be sprayed or discharged onto a fire to extinguish it . A fire extinguisher can be used to curb fire in the initial stage and prevent it from spreading over a large area . In the scenario, Calvin spotted blazing flames originating from a physical file storage location in his organization because of a short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. This means that he used a fire extinguisher for this purpose. A fire detection system is a system that detects the presence of fire by sensing its characteristics, such as smoke, heat, flame, etc., and alerts the occupants or authorities about it . A sprinkler system is a system that consists of pipes and sprinkler heads that release water onto a fire when activated by heat or smoke. A smoke detector is a device that senses smoke and emits an audible or visual signal to warn about fire.

**QUESTION 3**

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a

service-level down time is allowed a full backup is taken.

Identify the backup technique utilized by Ryleigh in the above scenario.

A. Nearline backup

B. Cold backup

C. Hot backup

D. Warm backup

Correct Answer: B

Explanation: Cold backup is the backup technique utilized by Ryleigh in the above scenario. Cold backup is a backup technique that involves taking a full backup of data when the system or database is offline or shut down. Cold backup ensures that the data is consistent and not corrupted by any ongoing transactions or operations. Cold backup is usually performed on a fixed date or time when the service-level downtime is allowed or scheduled . Nearline backup is a backup technique that involves storing data on a medium that is not immediately accessible, but can be retrieved within a short time. Hot backup is a backup technique that involves taking a backup of data while the system or database is online or running. Warm backup is a backup technique that involves taking a backup of data while the system or database is partially online or running.

**QUESTION 4**

Martin, a network administrator at an organization, received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. In which of the following threat-modeling steps did Martin evaluate the severity level of the threat?

A. Identify vulnerabilities

B. Application overview

C. Risk and impact analysis

D. Decompose the application

Correct Answer: C

Explanation: Risk and impact analysis is the threat-modeling step in which Martin evaluated the severity level of the threat in the above scenario. Threat modeling is a process that involves identifying, analyzing, and mitigating threats and risks to a system or network. Threat modeling can be used to improve the security and resilience of a system or network by applying various methods or techniques, such as STRIDE, DREAD, PASTA, etc. Threat modeling consists of various steps or phases that perform different tasks or roles. Risk and impact analysis is a threat-modeling step that involves assessing the likelihood and consequences of threats and risks to a system or network . Risk and impact analysis can be used to evaluate the severity level of threats and risks and prioritize them for mitigation . In the scenario, Martin received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. This means that he performed risk and impact analysis for this purpose. Identify vulnerabilities is a threat-modeling step that involves finding and documenting the weaknesses or flaws in a system or network that can be exploited by threats or risks . Application overview is a threat-modeling step that involves defining and understanding the scope, architecture, components, and functionality of a system or network . Decompose the application is a threat-modeling step that involves breaking down a system or network into smaller and simpler elements, such as data flows, processes, assets, etc.

**QUESTION 5**

Wilson, a security specialist in an organization, was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. Identity the method used by Wilson to achieve cloud network security in this scenario.

A. Virtual private cloud (VPC)

B. Public and private subnets

C. Transit gateways

D. VPC endpoint

Correct Answer: C

Explanation: Transit gateways are the method used by Wilson to achieve cloud network security in this scenario. Cloud network security is a branch of cybersecurity that focuses on protecting and securing the network infrastructure and traffic in a cloud environment. Cloud network security can involve various methods or techniques, such as encryption, firewall, VPN, IDS/IPS, etc. Transit gateways are a method of cloud network security that provide a network routing solution that establishes and manages communication between on-premises consumer networks and VPCs (Virtual Private Clouds) via a centralized unit . Transit gateways can be used to simplify and secure the connectivity between different networks or VPCs in a cloud environment . In the scenario, Wilson was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. This means that he used transit gateways for this purpose. A virtual private cloud (VPC) is not a method of cloud network security, but a term that describes an isolated and private section of a public cloud that provides exclusive access to cloud resources to a single organization or entity . A VPC can be used to create and configure virtual networks in a cloud environment . Public and private subnets are not methods of cloud network security, but terms that describe segments of a VPC that have different levels

of accessibility or visibility . A public subnet is a segment of a VPC that can be accessed from the internet or other networks . A private subnet is a segment of a VPC that cannot be accessed from the internet or other networks . A VPC endpoint is not a method of cloud network security, but a term that describes an interface that allows private connectivity between a VPC and other AWS (Amazon Web Services) services or resources .