



212-82^{Q&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.pass4itsure.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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-speed data access, the administrator implemented a PAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. Which of the following RAID levels was implemented by the administrator in the above scenario?

- A. RAID Level 0
- B. RAID Level 3
- C. RAID Level 5
- D. RAID Level 1

Correct Answer: D

Explanation: RAID Level 0 is the RAID level that was implemented by the administrator in the above scenario. RAID Level 0 is also known as striping, which breaks data into sections and stores them across multiple drives. RAID Level 0 provides high-speed data access and increases performance, but it does not provide any redundancy or fault tolerance. The storage capacity of RAID Level 0 is equal to the sum of disk capacities in the set³. References: RAID Level 0

QUESTION 2

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 3

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat-hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat-hunting method employed by Mark in the above scenario.

- A. Entity-driven hunting
- B. TTP-driven hunting
- C. Data-driven hunting
- D. Hybrid hunting

Correct Answer: C

Explanation: A data-driven hunting method is a type of threat hunting method that employs existing data collected from various sources, such as DNS and proxy logs, to generate and test hypotheses about potential threats. This method relies on data analysis and machine learning techniques to identify patterns and anomalies that indicate malicious activity. A data-driven hunting method can help discover unknown or emerging threats that may evade traditional detection methods. An entity-driven hunting method is a type of threat hunting method that focuses on specific entities, such as users, devices, or domains, that are suspected or known to be involved in malicious activity. A TTP-driven hunting method is a type of threat hunting method that leverages threat intelligence and knowledge of adversary tactics, techniques, and procedures (TTPs) to formulate and test hypotheses about potential threats. A hybrid hunting method is a type of threat hunting method that combines different approaches, such as data-driven, entity-driven, and TTP-driven methods, to achieve more comprehensive and effective results.

QUESTION 4

Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.

Identify the role played by Walker in the above scenario.

- A. Cloud auditor
- B. Cloud provider
- C. Cloud carrier
- D. Cloud consumer

Correct Answer: A



Explanation: A cloud auditor is a role played by Walker in the above scenario. A cloud auditor is a third party who examines controls of cloud computing service providers. Cloud auditor performs an audit to verify compliance with the standards and expressed his opinion through a report⁸⁹. A cloud provider is an entity that provides cloud services, such as infrastructure, platform, or software, to cloud consumers¹⁰. A cloud carrier is an entity that provides connectivity and transport of cloud services between cloud providers and cloud consumers¹⁰. A cloud consumer is an entity that uses cloud services for its own purposes or on behalf of another entity

QUESTION 5

George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

- A. Permissive policy
- B. Paranoid policy
- C. Prudent policy
- D. Promiscuous policy

Correct Answer: A

Explanation: Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.

[212-82 PDF Dumps](#)

[212-82 VCE Dumps](#)

[212-82 Exam Questions](#)