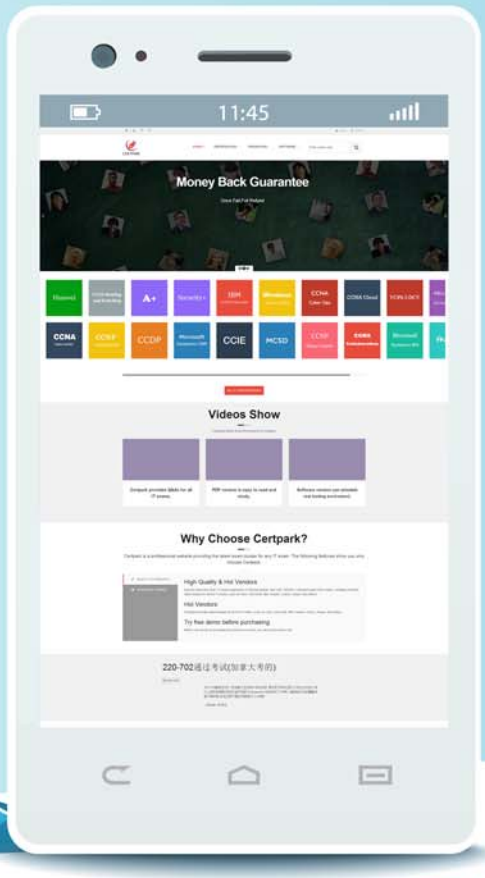
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **200-201**

Title : Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version : DEMO

1.Which event is user interaction?
A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file
Answer: D
Explanation:
User interaction is any event that requires the user to perform an action that enables or facilitates a cyberattack. Opening a malicious file is an example of user interaction, as it can trigger the execution of malicious code or malware that can compromise the system or network. Gaining root access, executing remote code, and reading and writing file permissions are not user interactions, but rather actions that can be performed by an attacker after exploiting a vulnerability or bypassing security controls.
Reference: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, More than 99% of cyberattacks rely on human interaction

2.Which security principle requires more than one person is required to perform a critical task?
A. least privilege
B. need to know
C. separation of duties
D. due diligence
Answer: C
Explanation:
Separation of duties is a security principle that requires more than one person to perform a critical task, such as authorizing a transaction, approving a budget, or granting access to sensitive data. Separation of duties reduces the risk of fraud, error, abuse, or conflict of interest by preventing any single person from having too much power or privilege. Least privilege, need to know, and due diligence are other security principles, but they do not require more than one person to perform a critical task.
Reference: Separation of Duty (SOD) - Glossary | CSRC - NIST Computer Security …, Separation of Duties | Imperva

3.How is attacking a vulnerability categorized?
A. action on objectives
B. delivery
C. exploitation
D. installation
Answer: C
Explanation:
Attacking a vulnerability is categorized as exploitation, which is the third phase of the cyberattack lifecycle. Exploitation is the process of taking advantage of a vulnerability in a system, application, or network to gain access, escalate privileges, or execute commands. Action on objectives, delivery, and installation are other phases of the cyberattack lifecycle, but they do not involve attacking a vulnerability. Action on objectives is the final phase, where the attacker achieves their goal, such as stealing data, disrupting services, or destroying assets. Delivery is the second phase, where the attacker delivers the malicious payload, such as malware, phishing email, or malicious link, to the target. Installation is the

fourth phase, where the attacker installs the malicious payload on the compromised system or network to maintain persistence or spread laterally.
Reference: What is a Cyberattack? | IBM, Recognizing the seven stages of a cyber-attack - DNV

4.What is a benefit of agent-based protection when compared to agentless protection?
A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously
Answer: C
Explanation:
Agent-based protection is a type of endpoint security that uses software agents installed on the devices to monitor and protect them. Agent-based protection can collect and detect all traffic locally, which means it can operate without relying on a network connection or a centralized server. Agent-based protection can also provide more granular and comprehensive visibility and control over the devices.
Reference: https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html (Module 2: Security Concepts, Lesson 2.3: Endpoint Security)

5.Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?
A. decision making
B. rapid response
C. data mining
D. due diligence
Answer: A
Explanation:
Decision making is a principle that guides an analyst to gather information relevant to a security incident to determine the appropriate course of action. Decision making involves identifying the problem, defining the criteria, analyzing the alternatives, and choosing the best solution. Decision making helps an analyst to respond to an incident effectively and efficiently, while minimizing the impact and risk to the organization.
Reference: https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html (Module 3: Security Monitoring, Lesson 3.1: Security Operations Center)