200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.leads4pass.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

How can TOR impact data visibility inside an organization?

A. no impact

B. increases security

C. increases data integrity

D. decreases visibility

Correct Answer: D

QUESTION 2

Which classification of cross-site scripting attack executes the payload without storing it for repeated use?

A. CSRF

B. reflective

C. DOM

D. stored

Correct Answer: B

QUESTION 3

Which type of data collection requires the largest amount of storage space?

A. alert data

B. transaction data

C. session data

D. full packet capture

Correct Answer: D

QUESTION 4

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context

B. session

C. laptop

D. firewall logs

E. threat actor

Correct Answer: CD

The following are some factors that are used during attribution in an investigation: Assets, Threat actor, Indicators of Compromise (IoCs), Indicators of Attack (IoAs), Chain of custody Asset: This factor identifies which assets were compromised by a threat actor or hacker. An example of an asset can be an organization\\'s domain controller (DC) that runs Active Directory Domain Services (AD DS). AD is a service that allows an administrator to manage user accounts, user groups, and policies across a Microsoft Windows environment. Keep in mind that an asset is anything that has value to an organization; it can be something physical, digital, or even people. Cisco Certified CyberOps Associate 200-201 Certification Guide

QUESTION 5

What is the impact of false positive alerts on business compared to true positive?

A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.

B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.

C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.

D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.

Correct Answer: C