200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative

B. true positive

C. true negative

D. false positive

Correct Answer: D

QUESTION 2

What is threat hunting?

A. Managing a vulnerability assessment report to mitigate potential threats.

B. Focusing on proactively detecting possible signs of intrusion and compromise.

C. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.

D. Attempting to deliberately disrupt servers by altering their availability

Correct Answer: B

QUESTION 3

What is vulnerability management?

A. A security practice focused on clarifying and narrowing intrusion points.

B. A security practice of performing actions rather than acknowledging the threats.

C. A process to identify and remediate existing weaknesses.

D. A process to recover from service interruptions and restore business-critical applications

Correct Answer: C

Reference: https://www.brinqa.com/vulnerability-management-primer-part-2-challenges/

Vulnerability management is the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities.[1] Vulnerability management is integral to computer security and network security, and must not be confused with Vulnerability assessment" source: https://en.wikipedia.org/wiki/Vulnerability_management

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

During a quarterly vulnerability scan, a security analyst discovered unused uncommon ports open and in a listening state. Further investigation showed that the unknown application was communicating with an external IP address on an encrypted channel. A deeper analysis revealed a command and control communication on an infected server. At which step of the Cyber Kill Chain was the attack detected?

A. Exploitation

B. Actions on Objectives

C. Weaponization

D. Delivery

Correct Answer: B

Latest 200-201 Dumps 200-201 Study Guide 200-201 Exam Questions