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.passapply.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which description is a defense-in-depth principal strategy?

A. isolating employees with access to critical data

B. implementing VLANs to segment network traffic

C. developing approval flow for new hires

D. designing Active Directory groups

Correct Answer: B

QUESTION 2

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

A. syslog messages

B. full packet capture

C. NetFlow

D. firewall event logs

Correct Answer: C

QUESTION 3

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

A. Biba

B. Object-capability

C. Take-Grant

D. Zero Trust

Correct Answer: D

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

QUESTION 4

According to CVSS, which metric group does user interaction belong to?

A. temporal

B. temporary

C. base

D. environmental

Correct Answer: C

QUESTION 5

A company plans to implement network segmentations and use IP address inventory management best practices. Servers and end-user devices are using the same VLANs and IP subnets with manual address assignment. What are the first two steps the engineers must take to meet these requirements? (Choose two.)

A. Configure packet captures to perform deep packet inspection for further traffic analysis and implementation of access rules.

B. Implement deep network traffic analysis using NetFlow v5 from routers and switches.

C. Deploy an Active Directory server and add all assets to the created domain for better visibility.

D. Assign separate hard-coded IP address spaces for critical assets, according to their role and functions.

E. Create IP address inventory database and deploy separate role-based IP subnetting for users using centralized DHCP server.

Correct Answer: DE