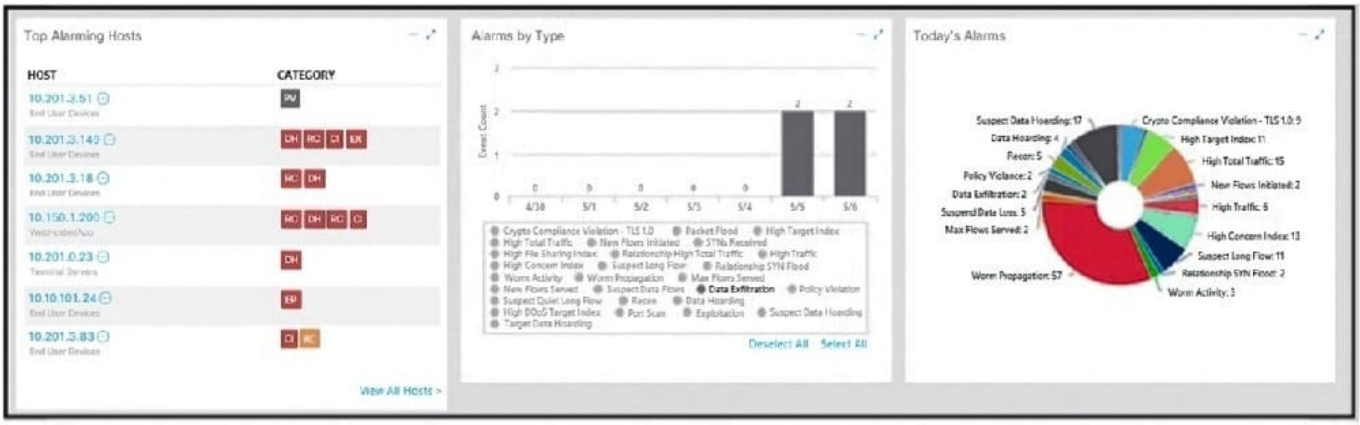
200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

QUESTION 1

Refer to the exhibit.



Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 [illegible]	RC DH RC CI
10.201.0.23 Terminal Servers	DH
10.10.101.24 End User Devices	EP
10.201.3.83 End User Devices	CI RC

View All Hosts >

What is the potential threat identified in this Stealthwatch dashboard?

A. A policy violation is active for host 10.10.101.24.

B. A host on the network is sending a DDoS attack to another inside host.

C. There are two active data exfiltration alerts.

D. A policy violation is active for host 10.201.3.149.

Correct Answer: C

QUESTION 2

An information security analyst inspects the .pcap file and observes encrypted unusual SSH traffic flow over nonstandard ports. Which technology makes this behavior feasible?

A. NAT

B. tunneling

C. P2P

D. TOR

Correct Answer: B

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

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

A. nmap --top-ports 192.168.1.0/24

B. nmap P 192.168.1.0/24

C. nmap -sL 192.168.1.0/24

D. nmap -sV 192.168.1.0/24

Correct Answer: B

https://explainshell.com/explain?cmd=nmap+-sP

QUESTION 5

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

C. DHCP snooping

D. command and control

Correct Answer: B

An ARP-based MITM attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of the attacker\\'s network interface card (NIC). Once the ARP caches have been successfully poisoned, each victim device sends all its packets to the attacker when communicating to the other device and puts the attacker in the middle of the communications path between the two victim devices. It allows an attacker to easily monitor all communication between victim devices. The intent is to intercept and view the information being passed between the two victim devices and potentially introduce sessions and traffic between the two victim devices