# Cisco

# 300-220

## Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

# Latest Version: 6.0

## Question: 1

To identify unknown gaps in detection, one should:

A. Only trust verified threats
B. Conduct regular security assessments
C. Assume all configurations are secure
D. Rely solely on automated alerts

**Answer: B**

## Question: 2

A tactic that indicates a sophisticated threat actor rather than a commodity malware campaign is:

A. Use of widely available exploit kits
B. Targeted spear-phishing emails
C. Scanning the internet for vulnerable servers
D. Posting threats on social media

**Answer: B**

## Question: 3

In cloud-native threat hunting, which AWS service's logs are essential for analysis?

A. Amazon EC2
B. AWS CloudTrail
C. Amazon Simple Storage Service (S3)
D. AWS Lambda

**Answer: B**

## Question: 4

What indicates a successful C2 communication detection using endpoint logs? (Choose two)

A. Increased outbound traffic to unknown IPs
B. Frequent system reboots
C. Unusual process tree formations
D. High volume of encrypted data sent to known ports

**Answer: A,C**

## Question: 5

Artifacts at which level of the Pyramid of Pain provide the most context about an attack but are also the most challenging to use for attribution?

A. IP addresses
B. Domain names
C. File hashes
D. TTPs

**Answer: D**

## Question: 6

To attribute a cyber attack to a specific threat actor, analysts primarily look for:

A. The language of comments in the malware code
B. The sophistication of the attack vector
C. Unique identifiers in the malware payload
D. Consistencies in TTPs with previous attacks

**Answer: D**

## Question: 7

Advancing in the Threat Hunting Maturity Model involves:

A. Lowering the bar for what constitutes a successful hunt
B. Increasing reliance on manual processes
C. Integrating threat hunting findings into broader security practices
D. Keeping threat hunting findings within the team to maintain knowledge exclusivity

**Answer: C**

## Question: 8

What aspect of a threat intelligence report is critical in drawing conclusions about threat actor tactics?

A. The geographic location of the attacker
B. The industry targeted by the attacker
C. The specific vulnerabilities exploited
D. The malware delivery method

**Answer: C**

## Question: 9

To determine C2 communications from infected hosts, analysts should examine:

A. Application version updates
B. Encrypted traffic patterns
C. CPU temperature logs
D. Email content filters

**Answer: B**

## Question: 10

How can logs help in identifying the tactics, techniques, and procedures of a threat actor?

A. By showing the time of day attacks are most likely to occur
B. By revealing patterns and anomalies that indicate malicious activity
C. By indicating the level of user satisfaction with IT services
D. By tracking the number of successful phishing attempts

**Answer: B**

# Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

**15 USD Discount Coupon Code:**

**G74JA8UF**

# FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer