KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **300-220**

Title : Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Version : DEMO

1.Which of the following best describes an advanced persistent threat (APT)?
A. A short-term financial fraud scheme
B. A quickly evolving malware variant
C. A long-term, targeted attack campaign
D. An opportunistic ransomware attack
Answer: C

2.Blocking C2 traffic effectively requires:
A. Ignoring encrypted traffic as it's secure by default
B. Focusing on inbound traffic only
C. Analyzing network traffic for anomalies
D. Assuming all internal network traffic is safe
Answer: C

3.When selecting indicators for attribution, which of the following is considered a weak indicator on its own?
A. A unique tool or piece of malware
B. Time of attack
C. Specificity of the target
D. Language of the attack code
Answer: B

4.Analytical gaps in threat hunting methodologies can result in:
A. An overreliance on automated alerting systems
B. Perfect detection with no false negatives
C. Improved threat actor attribution
D. Missed detection opportunities
Answer: D

5.Diagnosing analytical gaps is crucial for:
A. Justifying the reduction of the cybersecurity budget
B. Identifying underutilized resources
C. Ignoring emerging threat vectors
D. Complying with outdated regulations
Answer: B