Cisco

300-220
Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.0

Question: 1

Changes to a detection methodology to augment analytical and process gaps might include: (Choose two)
Response:

A. Decreasing the use of automation and machine learning
B. Integrating threat intelligence feeds
C. Implementing behavioral analysis techniques
D. Relying solely on signature-based detection

Answer: B,C

Question: 2

_____ involves proactively searching through networks to detect and isolate advanced threats that evade existing security solutions.
Response:

A. Compliance auditing
B. Network optimization
C. Threat hunting
D. Software development

Answer: C

Question: 3

Detection tools are limited in their effectiveness due to: (Choose two)
Response:

A. The dynamic nature of cyber threats
B. The physical security of the data center
C. Encryption used by network protocols
D. The evolving tactics of threat actors

Answer: A,D

Question: 4

When using the MITRE ATT&CK framework to model threats, changes in _____ are critical for understanding evolving attack strategies.
Response:

A. tactics, techniques, and procedures
B. encryption algorithms
C. software development methodologies
D. organizational policies

Answer: A

Question: 5

A comprehensive playbook addresses which phases of incident response?
(Choose two)
Response:

A. Detection
B. Budget planning
C. Recovery
D. Lunch break scheduling

Answer: A,C

Question: 6

The integration of which products would most enhance analytical capabilities for threat hunting?
Response:

A. Standalone antivirus solutions
B. Disconnected SIEM and endpoint detection and response (EDR) platforms
C. SIEM, EDR, and threat intelligence platforms
D. Uncoordinated firewall and intrusion prevention systems

Answer: C

Question: 7

Endpoint artifacts are crucial for uncovering undetected threats. Which of the following are considered endpoint artifacts?
(Choose two)
Response:

A. Router configuration files
B. Windows Registry keys
C. Bash history in Linux
D. DNS server logs

Answer: B,C

Question: 8

Which level of the Pyramid of Pain is most difficult for attackers to change and adapt to when detected?
Response:

A. Hash values
B. IP addresses
C. Domain names
D. TTPs (Tactics, Techniques, and Procedures)

Answer: D

Question: 9

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

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

Question: 10

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

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

For More Information – Visit link below:

https://www.certsgrade.com/

PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

16 USD Discount Coupon Code: NB4XKTMZ