

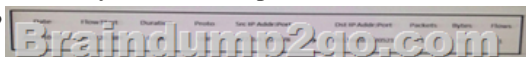
[2017-New-Exams!100% Success-Braindump2go 210-255(SECOPS) PDF and VCE 70q Instant Download[Q1-Q9

2017 New Cisco 210-255: Implementing Cisco Cybersecurity Operations Exam Questions Released by Braindump2go.com Today!

1. |NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download:<http://www.braindump2go.com/210-255.html> 2. |NEW 210-255

Exam Questions & Answers Download:<https://1drv.ms/f/s!AvI7wzKf6QBjgn5gut7hxGLZ6xws> QUESTION 1 Which option can be addressed when using retrospective security techniques? A. if the affected host needs a software update B. how the malware entered our network C. why the malware is still in our network D. if the affected system needs replacement Answer: A

QUESTION 2 Refer to the exhibit. Which type of log is this an example of?



A.

IDS

log B.

proxy log C. NetFlow log D. syslog Answer: A QUESTION 3 Which option is a misuse variety per VERIS enumerations? A.

snooping B. hacking C. theft D. assault Answer: B QUESTION 4 In the context of incident handling phases, which two activities

fall under scoping? (Choose two.) A. determining the number of attackers that are associated with a security incident B.

ascertaining the number and types of vulnerabilities on your network C. identifying the extent that a security incident is impacting

protected resources on the network D. determining what and how much data may have been affected E. identifying the attackers

that are associated with a security incident Answer: DE QUESTION 5 Which regular expression matches "color" and "colour"? A.

col[0-9]+our B. colo?ur C. colou?r D. [a-z]{7} Answer: C QUESTION 6 Which component of the NIST SP800-61 r2 incident

handling strategy reviews data? A. preparation B. detection and analysis C. containment, eradication, and recovery D.

post-incident analysis Answer: B QUESTION 7 Which option is generated when a file is run through an algorithm and generates a

string specific to the contents of that file? A. URL B. hash C. IP address D. destination port Answer: C QUESTION 8 Which

data type is protected under the PCI compliance framework? A. credit card type B. primary account number C. health conditions

D. provision of individual care Answer: C QUESTION 9 Which kind of evidence can be considered most reliable to arrive at an

analytical assertion? A. direct B. corroborative C. indirect D. circumstantial E. textual Answer: A !!!RECOMMEND!!!

1. |NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download:<http://www.braindump2go.com/210-255.html> 2. |NEW 210-255

Study Guide Video: YouTube Video: [YouTube.com/watch?v=3fI6ShLIZQo](https://www.youtube.com/watch?v=3fI6ShLIZQo)