350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company\\'s confidential document management folder using a company-owned asset al039-ice4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

A. Measure confidentiality level of downloaded documents.

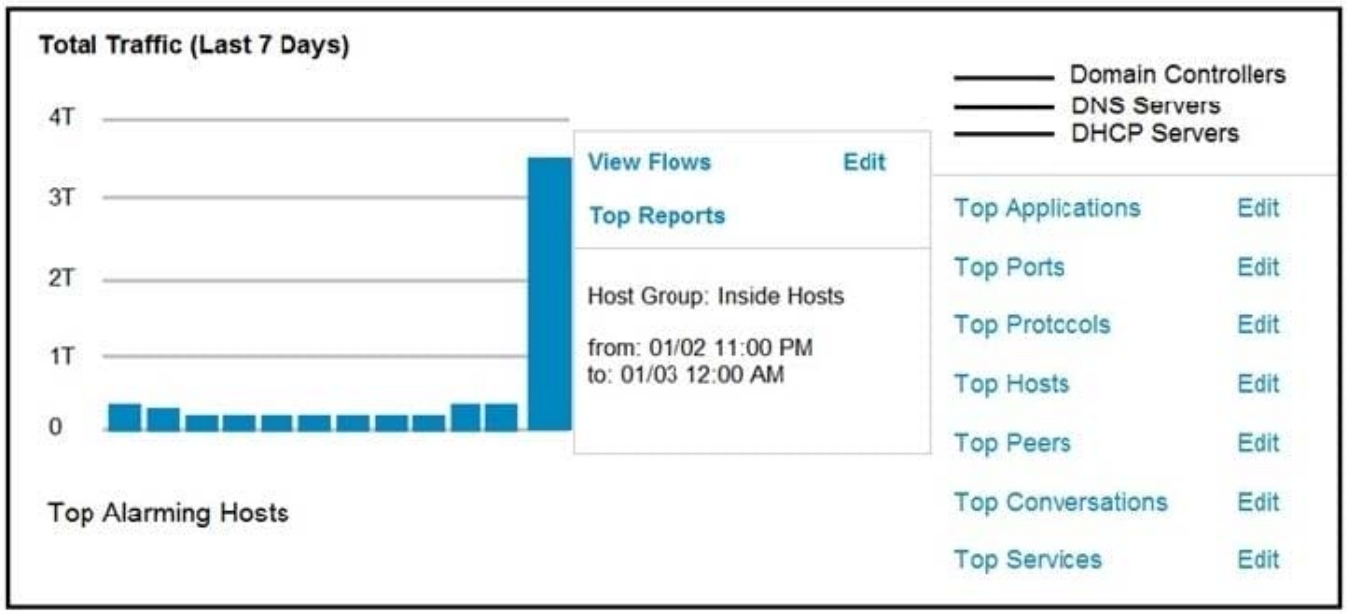
B. Report to the incident response team.

C. Escalate to contractor\\'s manager.

D. Communicate with the contractor to identify the motives.

Correct Answer: B

QUESTION 2



Refer to the exhibit. An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

A. Top Peers

B. Top Hosts

C. Top Conversations

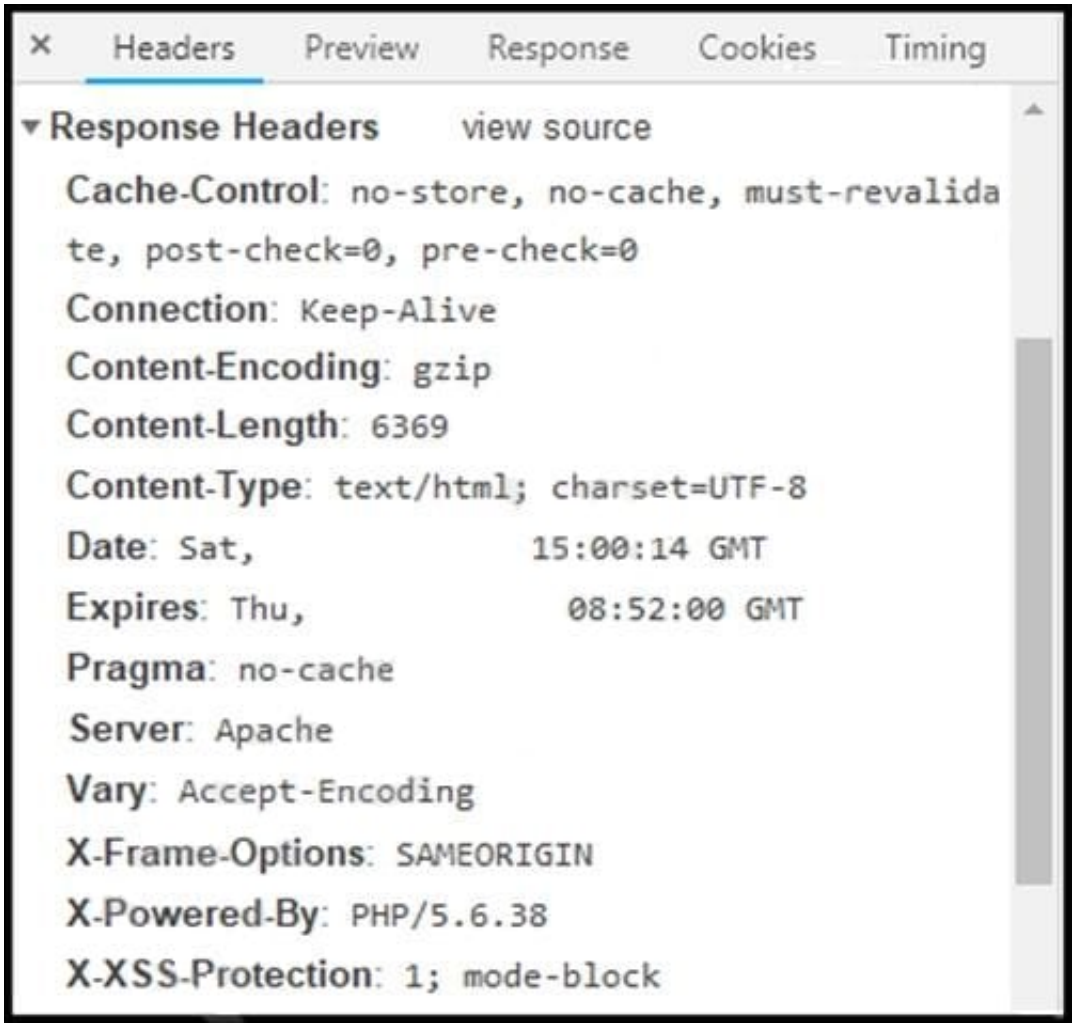
D. Top Ports

Correct Answer: B

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKSEC-3014.pdf

QUESTION 3

Refer to the exhibit. Where are the browser page rendering permissions displayed?



A. X-Frame-Options

B. X-XSS-Protection

C. Content-Type

D. Cache-Control

Correct Answer: C

QUESTION 4

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected.

What action should be taken to harden the network?

A. Move the IPS to after the firewall facing the internal network

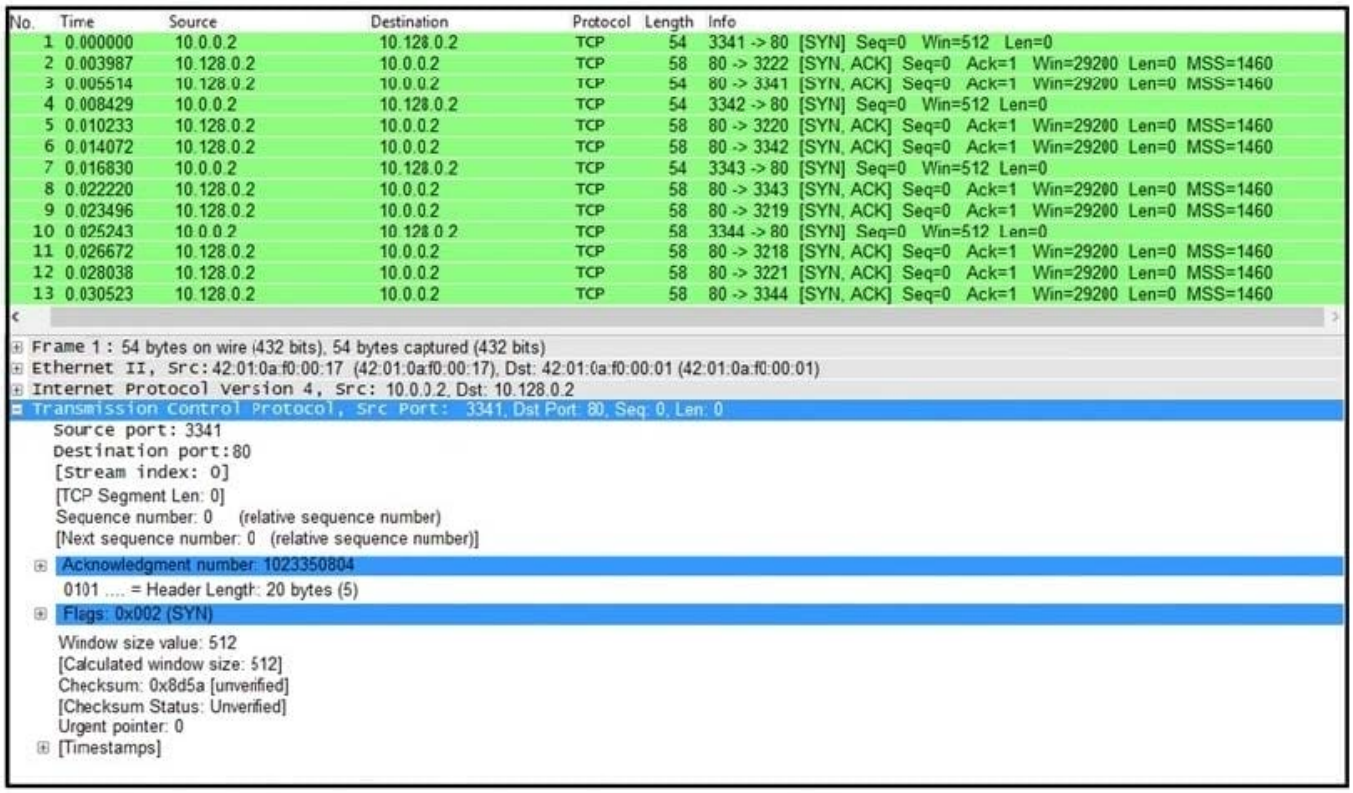
B. Move the IPS to before the firewall facing the outside network

C. Configure the proxy service on the IPS

D. Configure reverse port forwarding on the IPS

Correct Answer: C

QUESTION 5



Refer to the exhibit. What is the threat in this Wireshark traffic capture?

A. A high rate of SYN packets being sent from multiple sources toward a single destination IP

B. A flood of ACK packets coming from a single source IP to multiple destination IPs

C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs

D. A flood of SYN packets coming from a single source IP to a single destination IP

Correct Answer: D