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.pass2lead.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

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

A. chmod 666

B. chmod 774

C. chmod 775

D. chmod 777

Correct Answer: D

Reference: https://www.pluralsight.com/blog/it-ops/linux-file-permissions

QUESTION 2

A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

A. Create a follow-up report based on the incident documentation.

B. Perform a vulnerability assessment to find existing vulnerabilities.

C. Eradicate malicious software from the infected machines.

D. Collect evidence and maintain a chain-of-custody during further analysis.

Correct Answer: D

QUESTION 3

A patient views information that is not theirs when they sign in to the hospital\\'s online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time.

What is the first step the analyst should take to address this incident?

A. Evaluate visibility tools to determine if external access resulted in tampering

B. Contact the third-party handling provider to respond to the incident as critical

C. Turn off all access to the patient portal to secure patient records

D. Review system and application logs to identify errors in the portal code

Correct Answer: C

QUESTION 4

An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization\\'s service area. What are the next steps the engineer must take?

A. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.

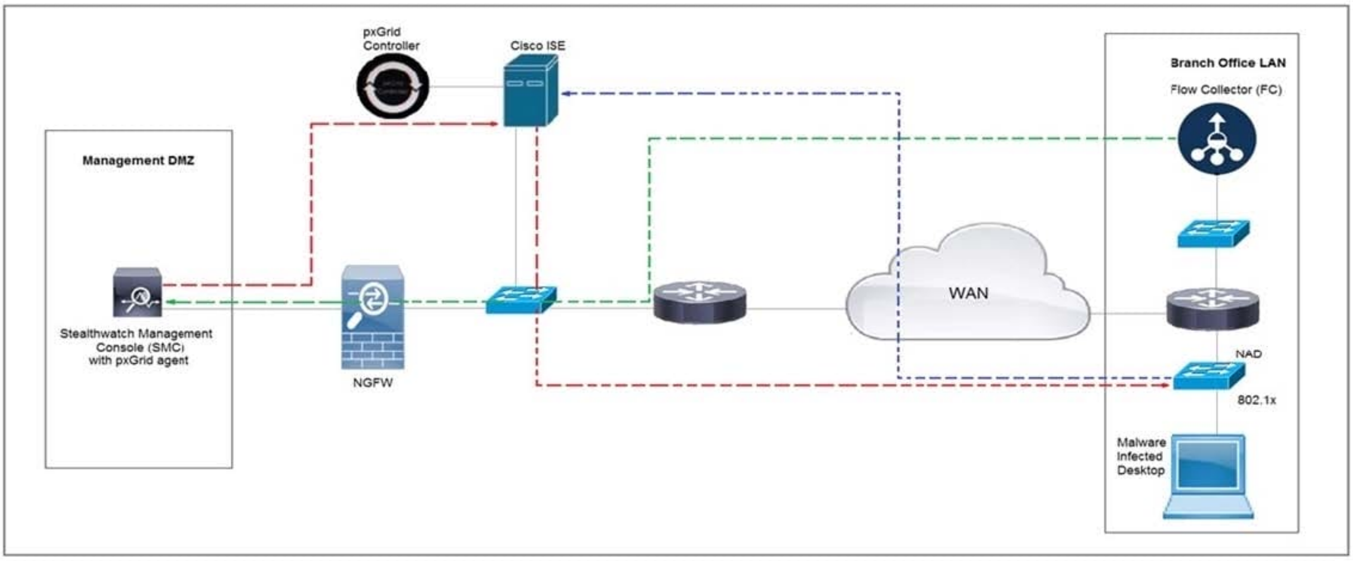
B. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.

C. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in question, and cross-correlate other source events.

D. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

Correct Answer: A

QUESTION 5



Refer to the exhibit. Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy.

Which telemetry feeds were correlated with SMC to identify the malware?

A. NetFlow and event data

B. event data and syslog data

C. SNMP and syslog data

D. NetFlow and SNMP

Correct Answer: B

350-201 VCE Dumps 350-201 Study Guide 350-201 Braindumps