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.geekcert.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

A. customer data

B. internal database

C. internal cloud

D. Internet

Correct Answer: D

QUESTION 2

A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet.

What is the cause of the issue?

A. DDoS attack

B. phishing attack

C. virus outbreak

D. malware outbreak

Correct Answer: D

QUESTION 3

Refer to the exhibit. 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 method was used to signal ISE to quarantine the endpoints?
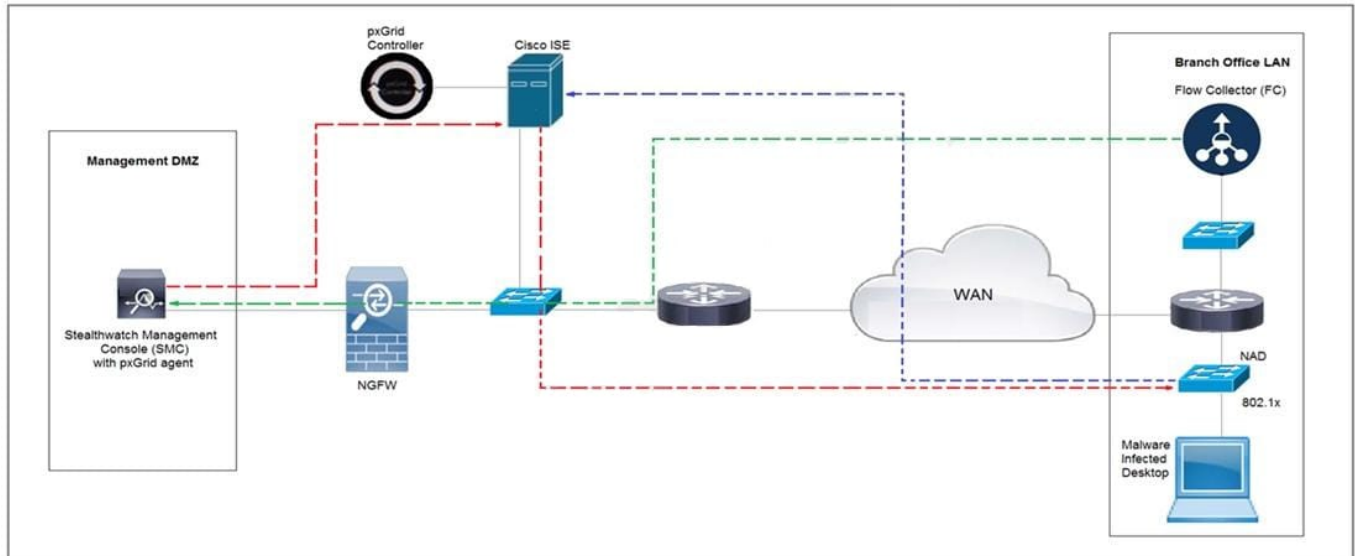
A. SNMP

B. syslog

C. REST API

D. pxGrid

Correct Answer: C

QUESTION 4

Refer to the exhibit. Which asset has the highest risk value?

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

A. servers

B. website

C. payment process

D. secretary workstation

Correct Answer: C

QUESTION 5

Refer to the exhibit. An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon – Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?

Human Interface Device Service	Activates and maintains the use of hot buttons on keyboar...	Running	Manual (Trig...
HP System Info HSA Service		Running	Automatic
HP Omen HSA Service		Running	Automatic
HP Network HSA Service		Running	Automatic
HP App Helper HSA Service		Running	Automatic
HP Analytics service		Running	Automatic
Group Policy Client	The service is responsible for applying settings configured...		Automatic (T...
GraphicsPerfSvc	Graphics performance monitor service		Manual (Trig...
Google Update Service (gupdatem)	Keeps your Google software up to date. If this service dis...		Manual
Google Update Service (gupdate)	Keeps your Google software up to date. If this service dis...		Automatic (...
Google Chrome Elevation Service (GoogleChro...			Manual
Geolocation Service	This service monitors the current location of the system an...		Disabled
GarneDVR and Broadcast User Service_136c57	This user service is used for Game Recordings and Live Broa...		Manual
Function Discovery Resource Publication	Publishes this computer and resources attached to this co...	Running	Manual (Trig...
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) net...	Running	Manual
File History Service	Protects user files from accidental loss by copying them to...		Manual (Trig...
Fax	Enables you to send and receive faxes, utilizing fax resourc...		Manual
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provi...	Running	Manual
Enterprise App Management Service	Enables enterprise application management.		Manual
Encrypting File System (EFS)	Provides the core file encryption technology used to store...		Manual (Trig...
Embedded Mode	The Embedded Mode service enables scenarios related to B...		Manuel (Trig...
ELAN Service		Running	Automatic

A. malware break

B. data theft

C. elevation of privileges

D. denial-of-service

Correct Answer: C

Latest 350-201 Dumps   350-201 VCE Dumps   350-201 Practice Test