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.certbus.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

An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

A. diagnostic

B. qualitative

C. predictive

D. statistical

Correct Answer: C

Reference: https://insights.principa.co.za/4-types-of-data-analytics-descriptive-diagnostic-predictive-prescriptive

QUESTION 2

An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

A. Utilize the SaaS tool team to gather more information on the potential breach

B. Contact the incident response team to inform them of a potential breach

C. Organize a meeting to discuss the services that may be affected

D. Request that the purchasing department creates and sends the payments manually

Correct Answer: A

QUESTION 3

Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*

B. Get-EventLog -List

C. Get-WinEvent -ListLog* -ComputerName localhost

D. Get-WinEvent -ListLog*

Correct Answer: A

Reference: https://lists.xymon.com/archive/2019-March/046125.html

QUESTION 4

Refer to the exhibit. An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable.

What does this STIX indicate?

A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible

B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information

C. There is a possible data leak because payloads should be encoded as UTF-8 text

D. There is a malware that is communicating via encrypted channels to the command and control server

Correct Answer: C

QUESTION 5

A threat actor attacked an organization\\'s Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator\\'s account was disabled.

Which activity triggered the behavior analytics tool?

A. accessing the Active Directory server

B. accessing the server with financial data

C. accessing multiple servers

D. downloading more than 10 files

Correct Answer: C

QUESTION 6

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 7

Refer to the exhibit. An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior.

Which type of compromise is occurring?

A. compromised insider

B. compromised root access

C. compromised database tables

D. compromised network

Correct Answer: D

QUESTION 8

Which action should be taken when the HTTP response code 301 is received from a web application?

A. Update the cached header metadata.

B. Confirm the resource\\'s location.

C. Increase the allowed user limit.

D. Modify the session timeout setting.

Correct Answer: A

QUESTION 9

A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA

B. PCI-DSS

C. Sarbanes-Oxley

D. GDPR

Correct Answer: D

Reference: https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/

QUESTION 10

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data. Which type of attack is occurring?

A. Address Resolution Protocol poisoning

B. session hijacking attack

C. teardrop attack

D. Domain Name System poisoning

Correct Answer: D

QUESTION 11

A cloud engineer needs a solution to deploy applications on a cloud without being able to manage and control the server OS. Which type of cloud environment should be used?

A. IaaS

B. PaaS

C. DaaS

D. SaaS

Correct Answer: A

QUESTION 12

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

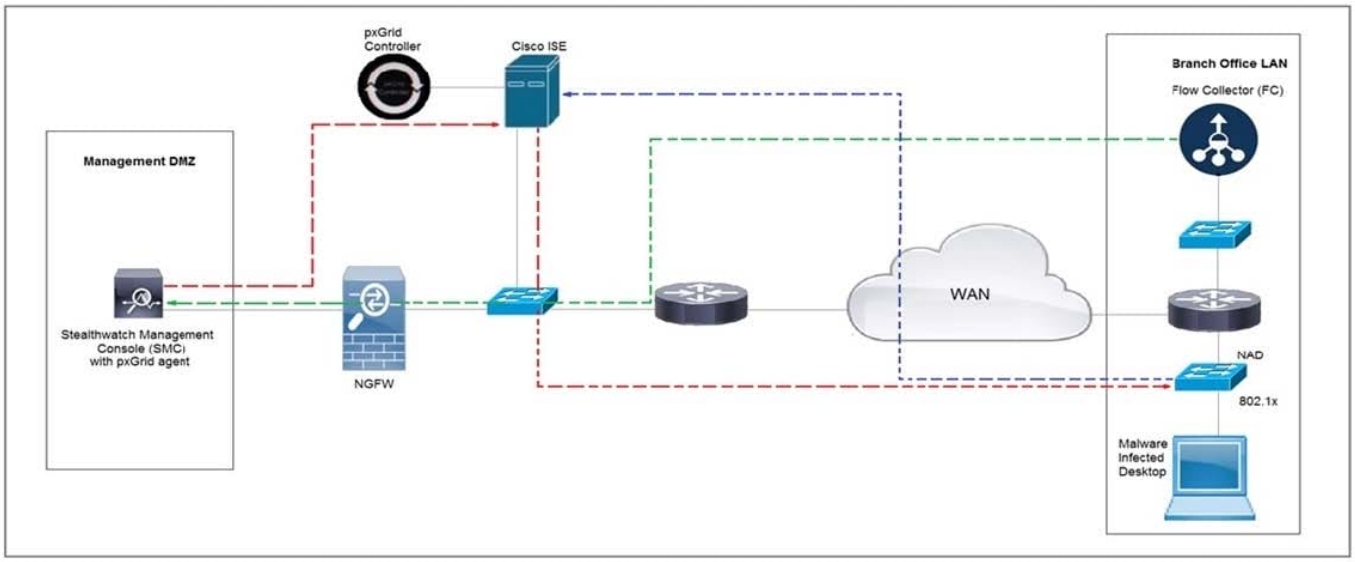
B. Contact the third-party handling provider to respond to the incident as critical

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 13



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

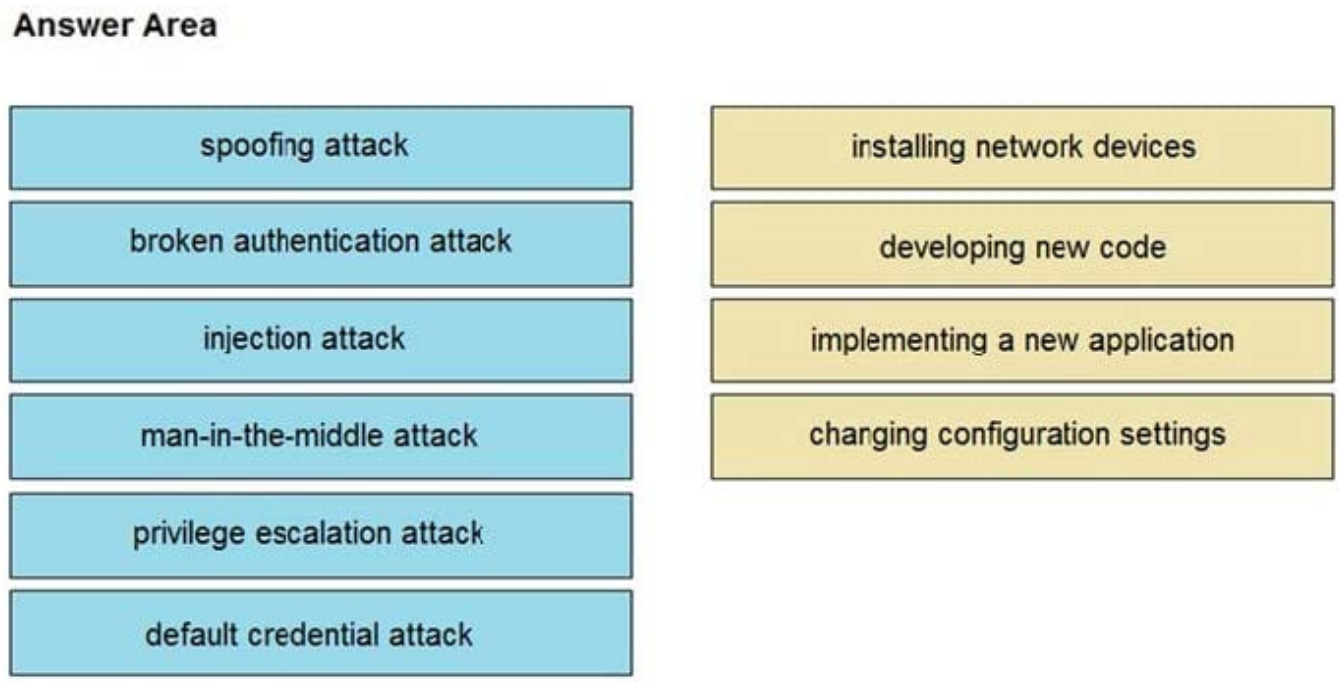
Correct Answer: B

QUESTION 14

DRAG DROP

Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Select and Place:



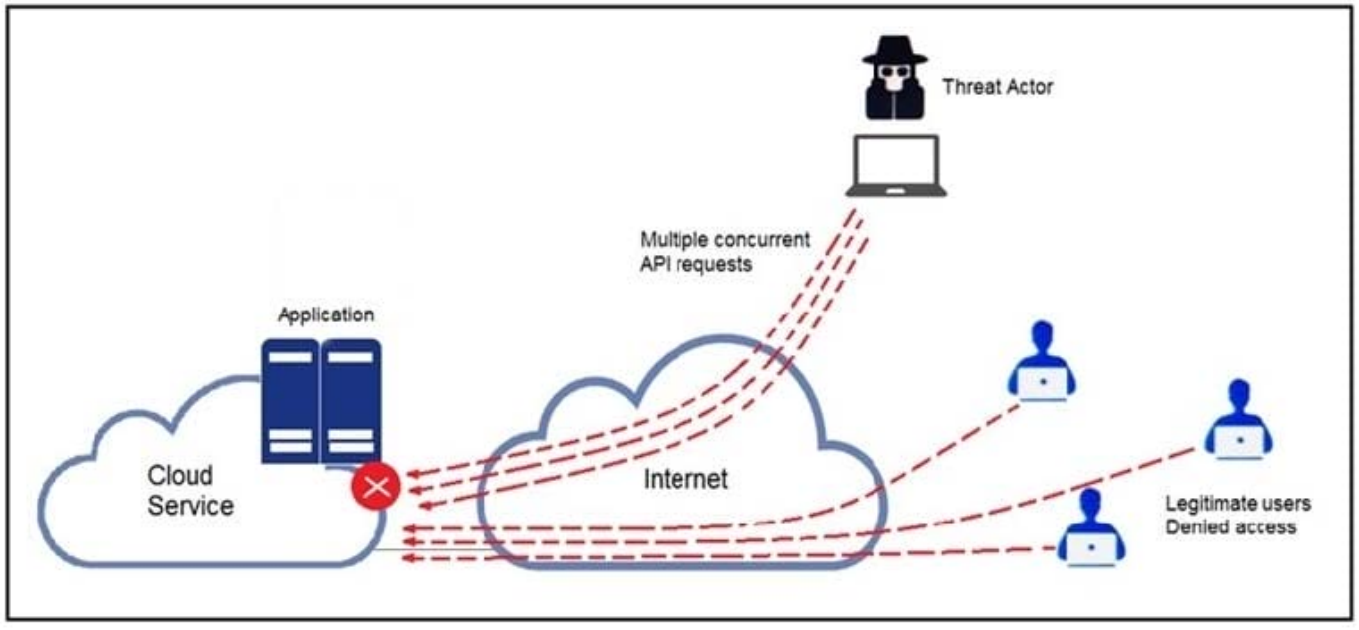
Correct Answer:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
	privilege escalation attack
	default credential attack

QUESTION 15

Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?



A. Limit the number of API calls that a single client is allowed to make

B. Add restrictions on the edge router on how often a single client can access the API

C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API

D. Increase the application cache of the total pool of active clients that call the API

Correct Answer: A