Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

NEW QUESTION 1
The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment

Answer: D

NEW QUESTION 2
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled “Invoice RE: 0004489”. The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B. Ask the company to execute the payload for real time analysis
C. Investigate further in open source repositories using YARA to find matches
D. Obtain a copy of the file for detonation in a sandbox

Answer: D

NEW QUESTION 3
Refer to the exhibit.

```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware--162d9 a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
          ],
          "is_family": false,
          "kil_chain_phases": [
            {
              "kill_chain_name": "mandant-attack-lifecycle-model",
              "phase_name": "establish-foothold"
            }
          ]

        },
        {
          "type": "relationship",
          "spec_version": "2.1",
          "id": "relationship--864af2e5",
          "created": "2020-08-15T18:03:58.029Z",
          "modified": "2020-08-15T18:03:58.029Z",
          "relationship_type": "indicates",
          "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4"
          "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
        }
    ]
}
```


Which indicator of compromise is represented by this STIX?

A. website redirecting traffic to ransomware server
B. website hosting malware to download files
C. web server vulnerability exploited by malware
D. cross-site scripting vulnerability to backdoor server

Answer: C

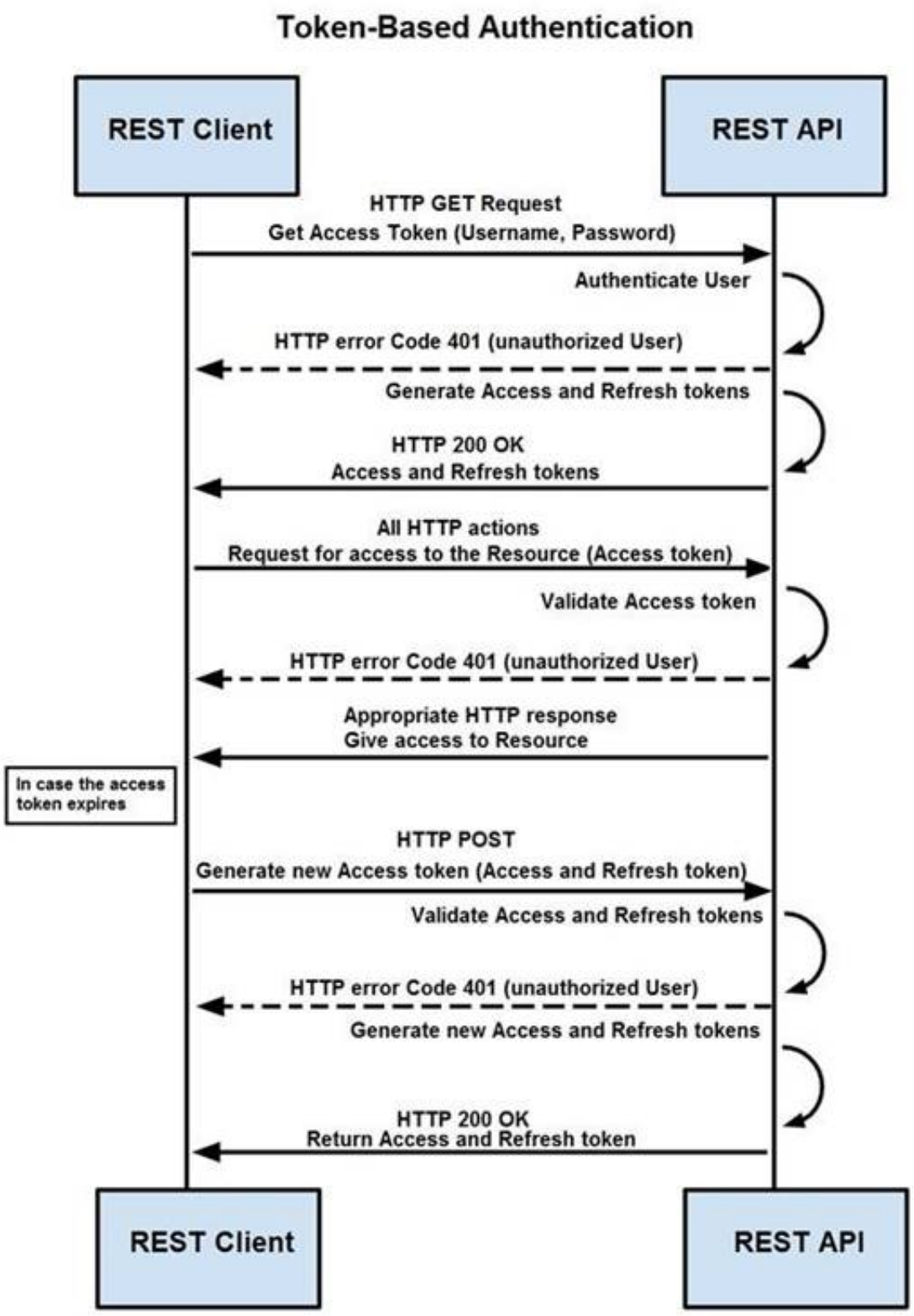
NEW QUESTION 4
What is a limitation of cyber security risk insurance?

A. It does not cover the costs to restore stolen identities as a result of a cyber attack
B. It does not cover the costs to hire forensics experts to analyze the cyber attack
C. It does not cover the costs of damage done by third parties as a result of a cyber attack
D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer: A

NEW QUESTION 5

Refer to the exhibit.



How are tokens authenticated when the REST API on a device is accessed from a REST API client?

A. The token is obtained by providing a passwor
B. The REST client requests access to a resource using the access toke
C. The REST API validates the access token and gives access to the resource.
D. The token is obtained by providing a passwor
E. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
F. The token is obtained before providing a passwor
G. The REST API provides resource access, refreshes tokens, and returns them to the REST clien
H. The REST client requests access to a resource using theaccess token.
I. The token is obtained before providing a passwor
J. The REST client provides access to a resource using the access toke
K. The REST API encrypts the access token and gives access to the resource.

Answer: D

NEW QUESTION 6
What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface
B. to create the logic that triggers alerts when anomalies occur
C. to identify vulnerabilities within an operating system
D. to analyze attacks to identify threat actors and points of entry

Answer: A

NEW QUESTION 7
A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities

C. Review the server backup and identify server content and data criticality to assess the intrusion risk
D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

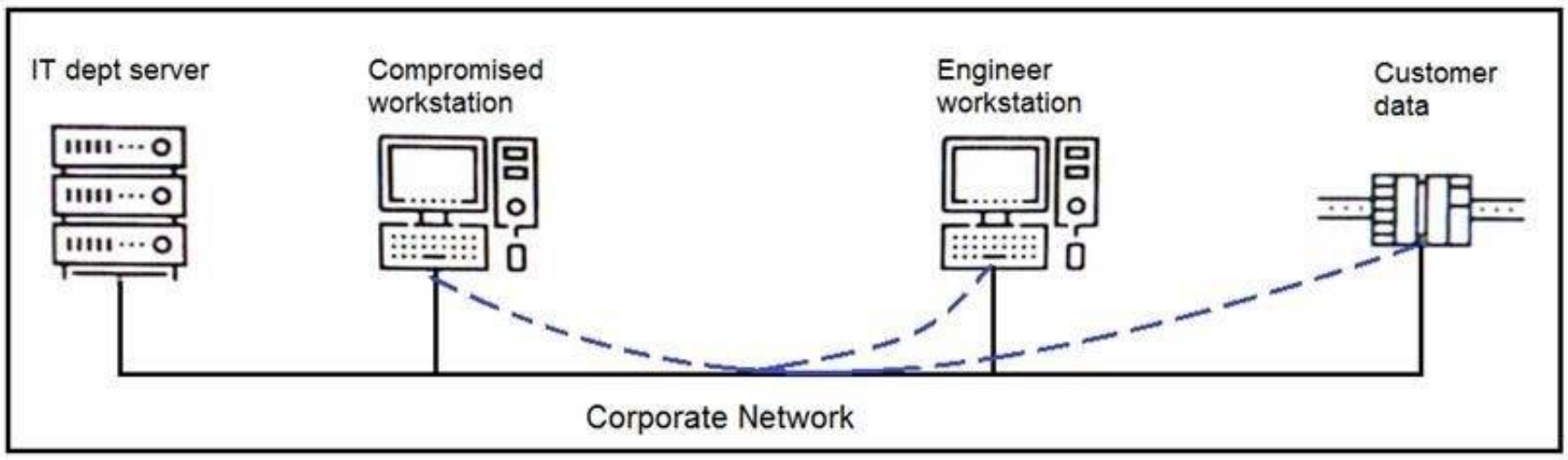
Answer: C

NEW QUESTION 8
An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions
B. Unpack the file in a sandbox to see how it reacts
C. Research the malware online to see if there are noted findings
D. Disassemble the malware to understand how it was constructed

Answer: C

NEW QUESTION 9
Refer to the exhibit.



An engineer received a report that an attacker has compromised a workstation and gained access to sensitive customer data from the network using insecure protocols. Which action prevents this type of attack in the future?

A. Use VLANs to segregate zones and the firewall to allow only required services and secured protocols
B. Deploy a SOAR solution and correlate log alerts from customer zones
C. Deploy IDS within sensitive areas and continuously update signatures
D. Use syslog to gather data from multiple sources and detect intrusion logs for timely responses

Answer: A

NEW QUESTION 10
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

Answer: C

NEW QUESTION 10
Refer to the exhibit.

Analysis Report

ID	12cbeee21b1ea4	**Filename**	ee482400446236cb315ad7ed035bd77ad4014039ec9bfebc8f2.eml
OS	Windows 7 64-bit	**Magic Type**	SMTP mail, ASCII text
		Analyzed As	eml
Started	10/13/20 06:22:43	**SHA256**	ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639ec9bfebc8f2
Ended	10/13/20 06:29:19		
Duration	0:06:36	**SHA1**	d700bca5b65aaf0c613d702d9a28a6084692224
Sandbox	rcn-work-042 (pilot-d)	**MD5**	58d1163715089192a8177a5244b9658f

Behavioral Indicators

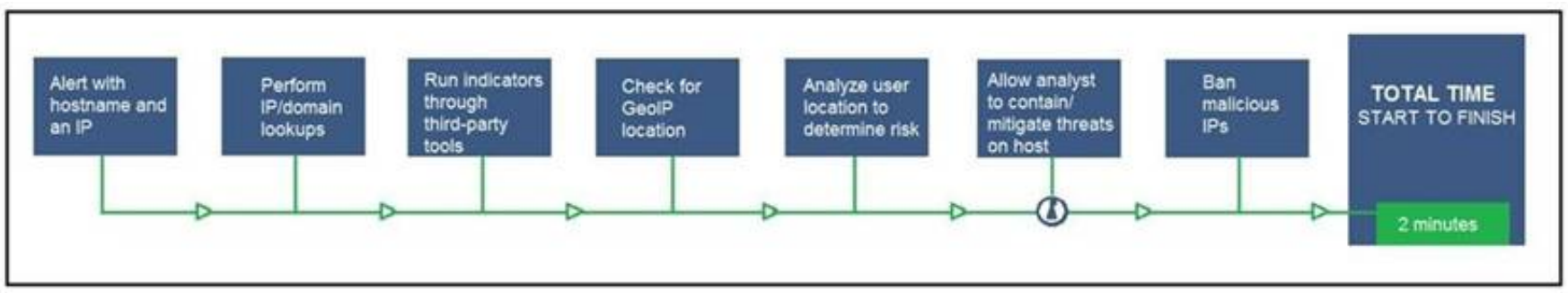
Email References Localhost in Received Message Trace	**Severity: 40**	**Confidence: 100**
Document Contains Embedded Material and Minimal Content	**Severity: 50**	**Confidence: 80**
Download Forced Open/Save Prompt	**Severity: 50**	**Confidence: 75**
Email With Different Sender and Return-Path Detected	**Severity: 60**	**Confidence: 60**
Process Users Very Large Command-Line	**Severity: 40**	**Confidence: 80**
File Downloaded to Disk	**Severity: 30**	**Confidence: 90**
Potential Code Injection Detected	**Severity: 50**	**Confidence: 50**
HTTP Client Error Response	**Severity: 50**	**Confidence: 50**
Sample Communicates With Only Benign Domains	**Severity: 20**	**Confidence: 95**
Executable with Encrypted Sections	**Severity: 30**	**Confidence: 30**
Outbound Communications to Nginx Web Server	**Severity: 25**	**Confidence: 25**
Outbound HTTP POST Communications	**Severity: 25**	**Confidence: 25**
Document Queried Domain	**Severity: 25**	**Confidence: 25**
Executable Imported the IsDebuggerPresent Symbol	**Severity: 20**	**Confidence: 20**

Cisco Advanced Malware Protection installed on an end-user desktop automatically submitted a low prevalence file to the Threat Grid analysis engine. What should be concluded from this report?

A. Threat scores are high, malicious ransomware has been detected, and files have been modified
B. Threat scores are low, malicious ransomware has been detected, and files have been modified
C. Threat scores are high, malicious activity is detected, but files have not been modified
D. Threat scores are low and no malicious file activity is detected

Answer: B

NEW QUESTION 13
Refer to the exhibit.



An engineer configured this SOAR solution workflow to identify account theft threats and privilege escalation, evaluate risk, and respond by resolving the threat. This solution is handling more threats than Security analysts have time to analyze. Without this analysis, the team cannot be proactive and anticipate attacks. Which action will accomplish this goal?

A. Exclude the step “BAN malicious IP” to allow analysts to conduct and track the remediation
B. Include a step “Take a Snapshot” to capture the endpoint state to contain the threat for analysis
C. Exclude the step “Check for GeoIP location” to allow analysts to analyze the location and the associated risk based on asset criticality
D. Include a step “Reporting” to alert the security department of threats identified by the SOAR reporting engine

Answer: A

NEW QUESTION 14
An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

A. Restrict the number of requests based on a calculation of daily average
B. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
C. Implement REST API Security Essentials solution to automatically mitigate limit exhaustio
D. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
E. Increase a limit of replies in a given interval for each AP
F. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
G. Apply a limit to the number of requests in a given time interval for each AP
H. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

NEW QUESTION 19
An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

A. HIPAA
B. FISMA
C. COBIT
D. PCI DSS

Answer: D

NEW QUESTION 20
An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu
B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
D. Discovery, System Network Configuration Discovery, Duqu

Answer: A

NEW QUESTION 25
An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

A. data clustering
B. data regression
C. data ingestion
D. data obfuscation

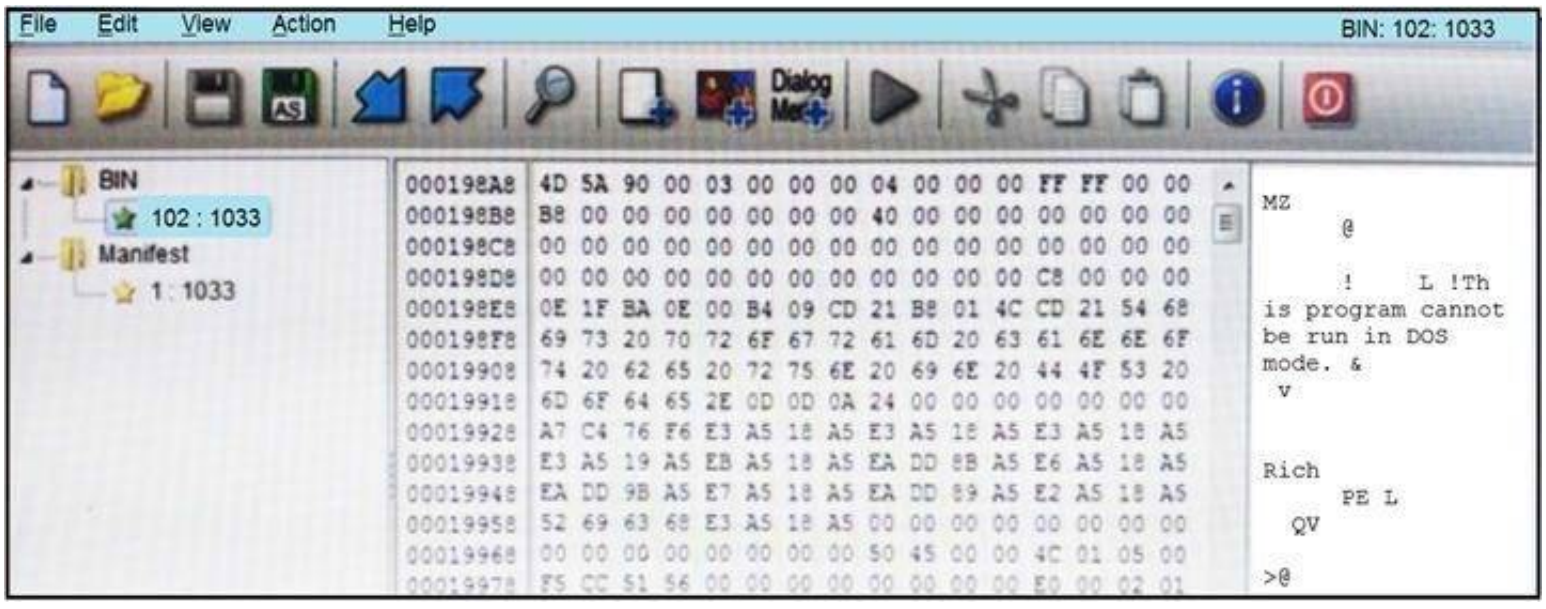
Answer: A

NEW QUESTION 29
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

Answer: C

NEW QUESTION 32
Refer to the exhibit.



An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

A. a DOS MZ executable format
B. a MS-DOS executable archive
C. an archived malware
D. a Windows executable file

Answer: D

NEW QUESTION 33
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

Answer: D

NEW QUESTION 34
A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

A. Mask PAN numbers
B. Encrypt personal data
C. Encrypt access
D. Mask sales details

Answer: B

NEW QUESTION 39
Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Answer Area

not visible to the victim	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives

A. Mastered
B. Not Mastered

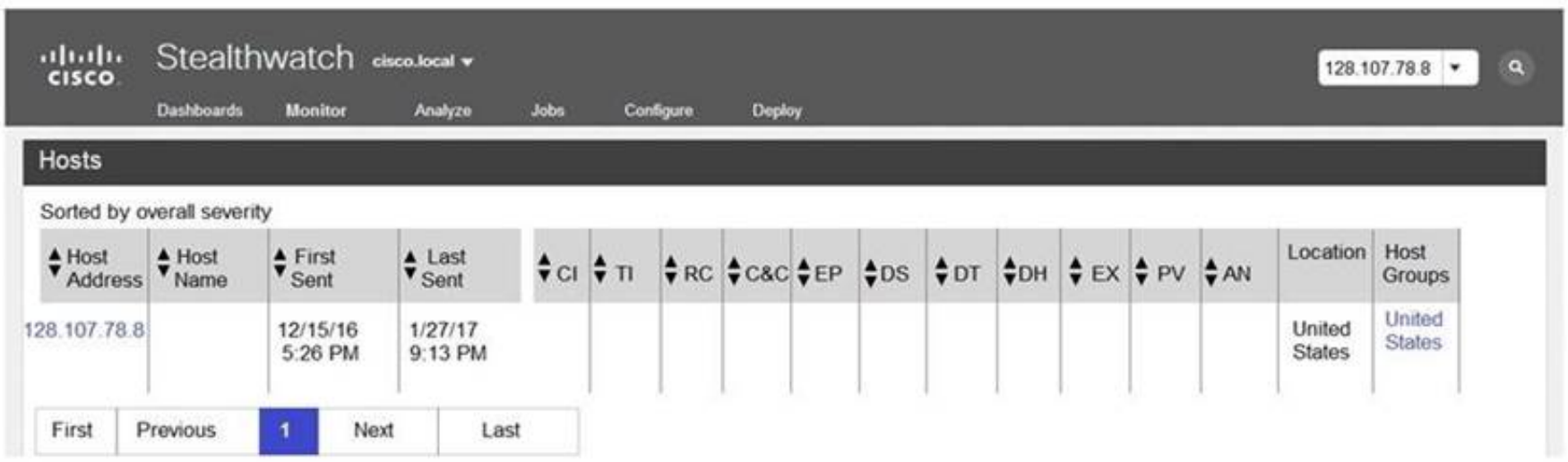
Answer: A

Explanation:

Answer Area

not visible to the victim	system phones connecting to countries where no staff are located
virus scanner turning off	malware placed on the targeted system
malware placed on the targeted system	not visible to the victim
open port scans and multiple failed logins from the website	large amount of data leaving the network through unusual ports
large amount of data leaving the network through unusual ports	USB with infected files inserted into company laptop
system phones connecting to countries where no staff are located	virus scanner turning off
USB with infected files inserted into company laptop	open port scans and multiple failed logins from the website

NEW QUESTION 40
Refer to the exhibit.



The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

Answer Area

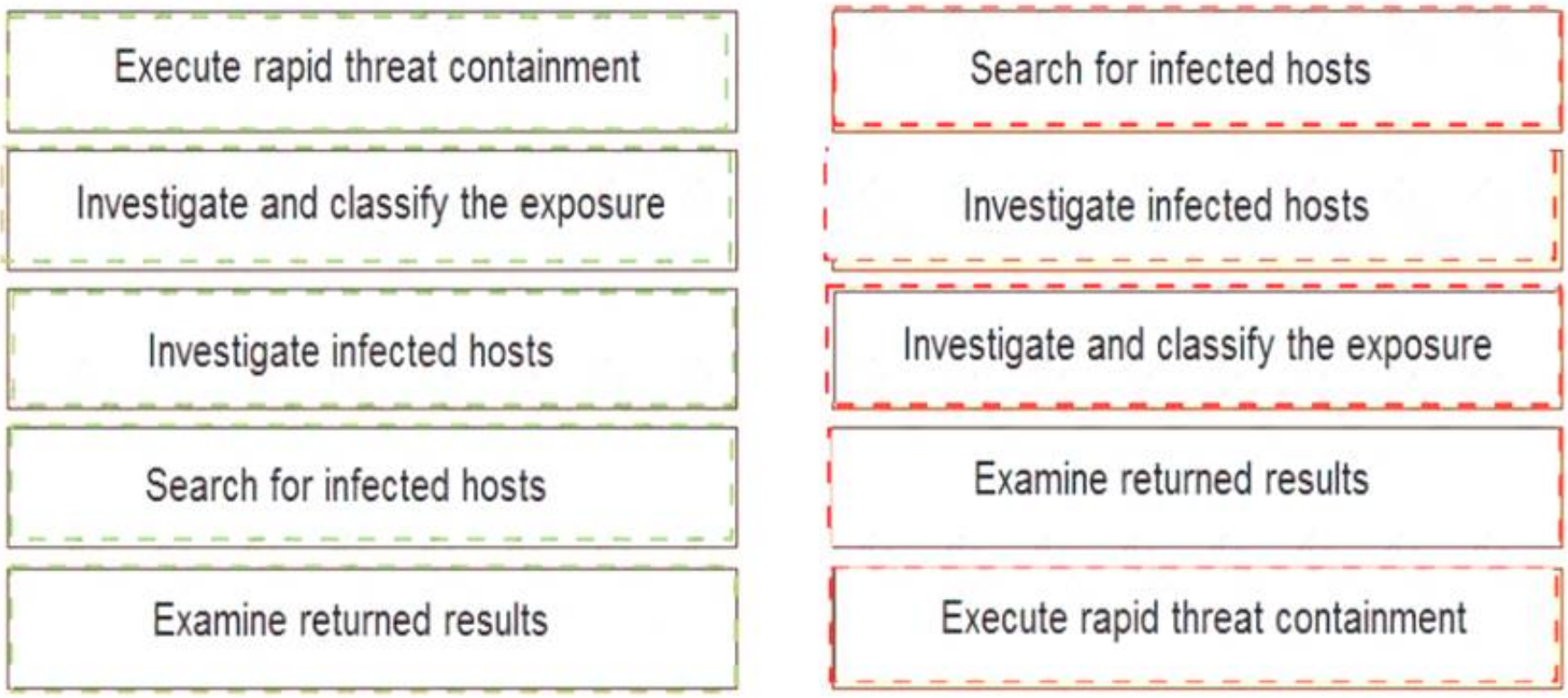
Execute rapid threat containment	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4
Examine returned results	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 43

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

350-201 Practice Exam Features:

* 350-201 Questions and Answers Updated Frequently

* 350-201 Practice Questions Verified by Expert Senior Certified Staff

* 350-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year