Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.

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

Which command was executed in PowerShell to generate this log?

A. Get-EventLog -LogName*
B. Get-EventLog -List
C. Get-WinEvent -ListLog* -ComputerName localhost
D. Get-WinEvent -ListLog*

Answer: A

NEW QUESTION 2
Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	Data or access loss occurs due to cybersecurity incidents

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

NEW QUESTION 3
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 4
A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

A. DLP for data in motion
B. DLP for removable data
C. DLP for data in use
D. DLP for data at rest

Answer: C

NEW QUESTION 5
A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets
B. Update software to patch third-party software
C. Validate CSRF by executing exploits within Metasploit
D. Fix applications according to the risk scores

Answer: D

NEW QUESTION 6
Refer to the exhibit.

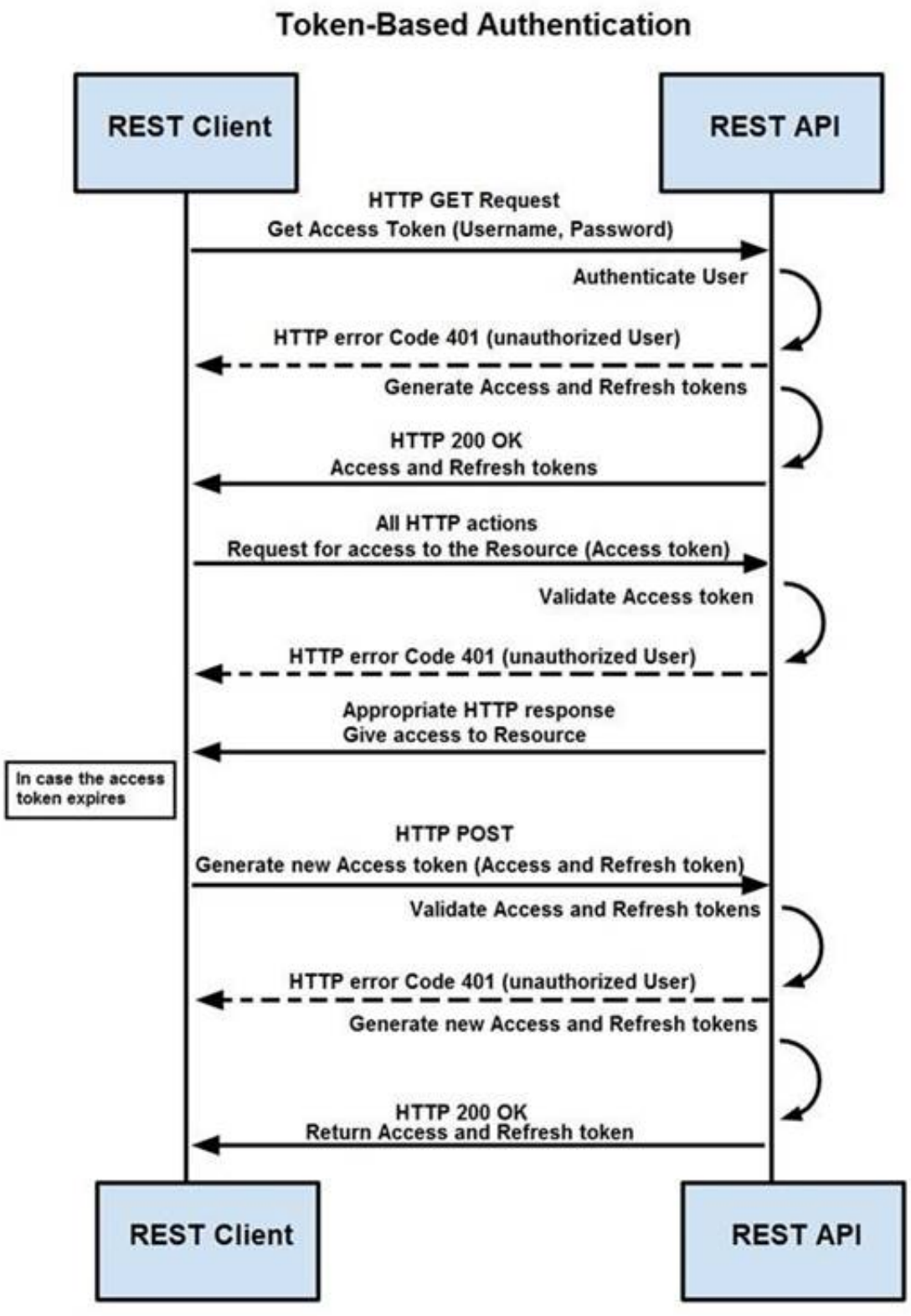
```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

Which data format is being used?

A. JSON
B. HTML
C. XML
D. CSV

Answer: B

NEW QUESTION 7
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 8
An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh
B. source ex.sh
C. chroot ex.sh
D. sh ex.sh

Answer: A

NEW QUESTION 9
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
B. exfiltration during data transfer
C. attack using default accounts
D. data exposure from backups

Answer: B

NEW QUESTION 10
A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

A. Classify the criticality of the information, research the attacker’s motives, and identify missing patches
B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Answer: B

NEW QUESTION 10
An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

Answer Area

run show access-list	Step 1
run show config	Step 2
validate the file MD5	Step 3
generate the core file	Step 4
verify the image file hash	
check the memory logs	
verify the memory state	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

run show access-list	run show config
run show config	check the memory logs
validate the file MD5	verify the memory state
generate the core file	run show access-list
verify the image file hash	
check the memory logs	
verify the memory state	

NEW QUESTION 14
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

Answer: A

NEW QUESTION 16
What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

A. 401B.-402C.403D.404E.405

Answer: A

NEW QUESTION 19
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 24
Refer to the exhibit.

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com,realm=0,isRealm=0,realDomain=0,shortrealm=0
x-xss-protection: 1; mode=block
```

Where are the browser page rendering permissions displayed?

A. x-frame-options
B. x-xss-protection
C. x-content-type-options

D. x-test-debug

Answer: C

NEW QUESTION 29
An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.

Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Identify systems to be taken offline	Conduct content scans
Conduct content scans	Collect log data
Collect log data	Identify systems to be taken offline
Request system patch	Reimage
Reimage	Request system patch

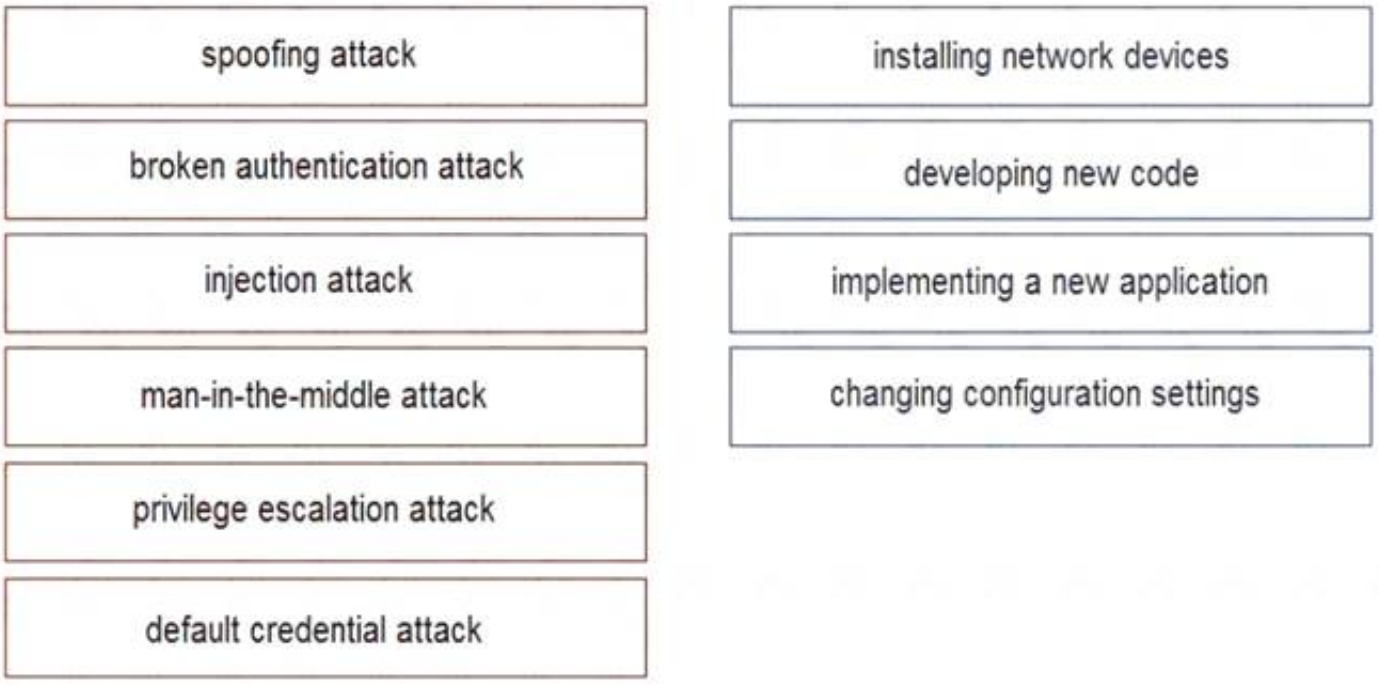
NEW QUESTION 31
A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.861.2117.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

A. DDoS attack
B. phishing attack
C. virus outbreak
D. malware outbreak

Answer: D

NEW QUESTION 33
Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Answer Area

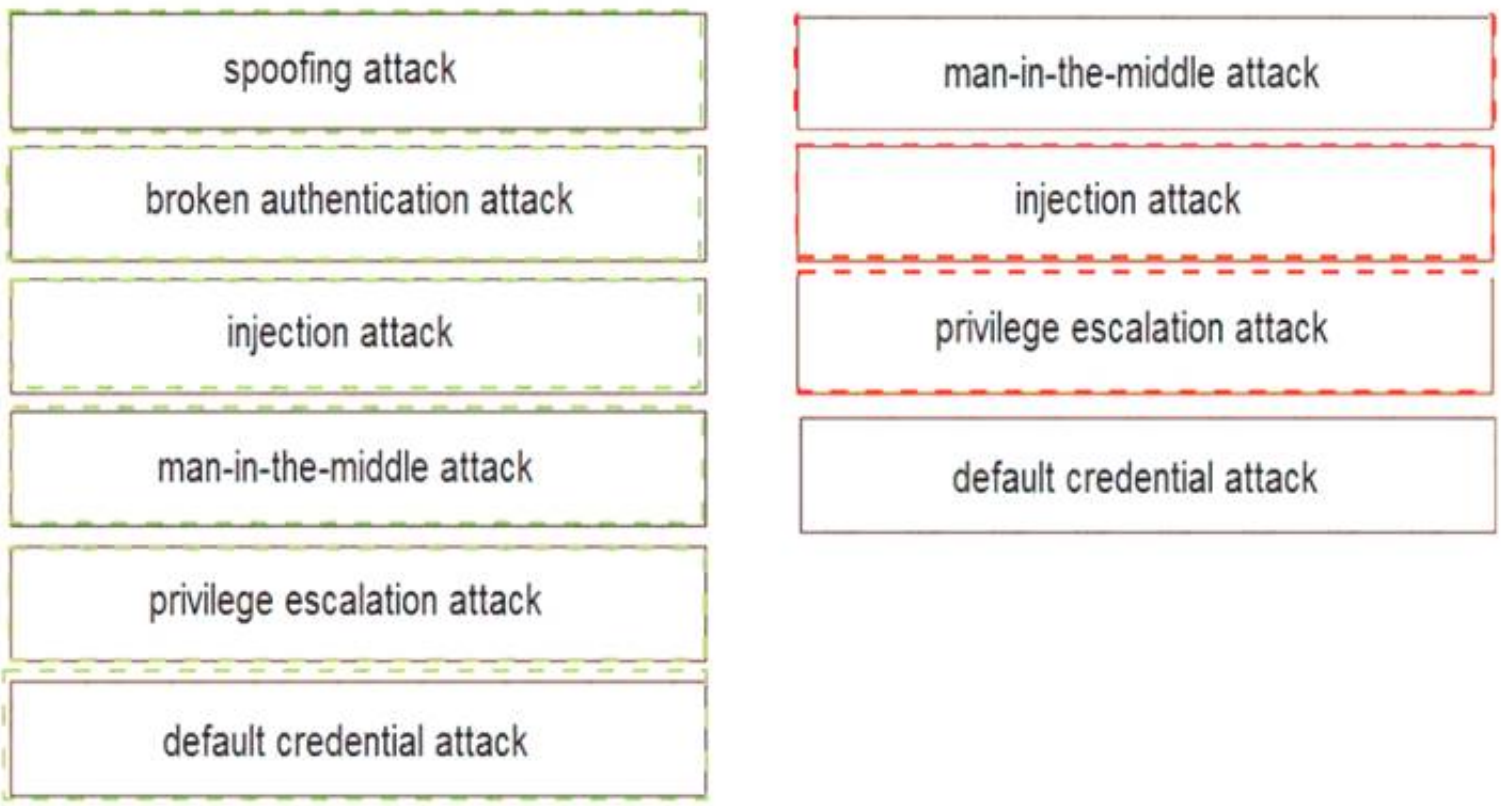


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 37
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

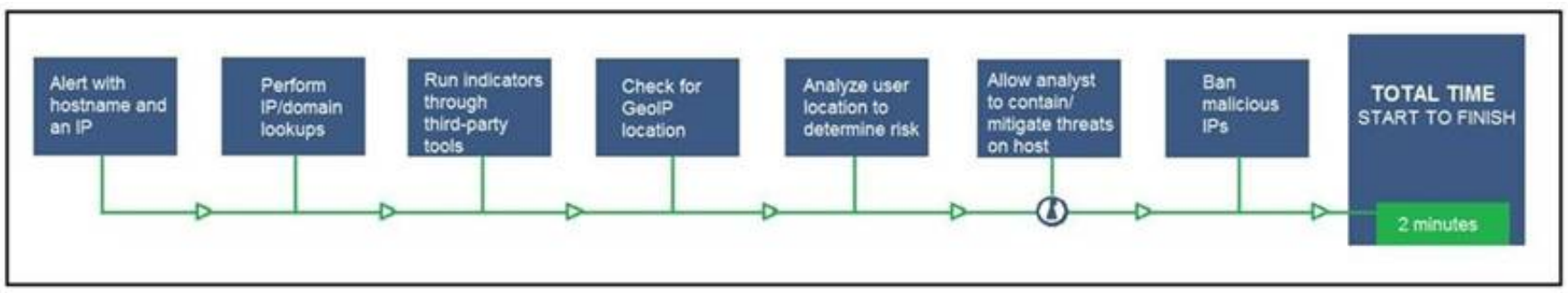
Email References Localhost in Received Message Trace	Severity: 40	Confidence: 100
Document Contains Embedded Material and Minimal Content	Severity: 50	Confidence: 80
Download Forced Open/Save Prompt	Severity: 50	Confidence: 75
Email With Different Sender and Return-Path Detected	Severity: 60	Confidence: 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 40
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 44
An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since deploying certificates and tracking them requires searching server owners manually. Which action will improve workflow automation?

A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.
B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.
C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.
D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Answer: C

NEW QUESTION 47
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 51
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

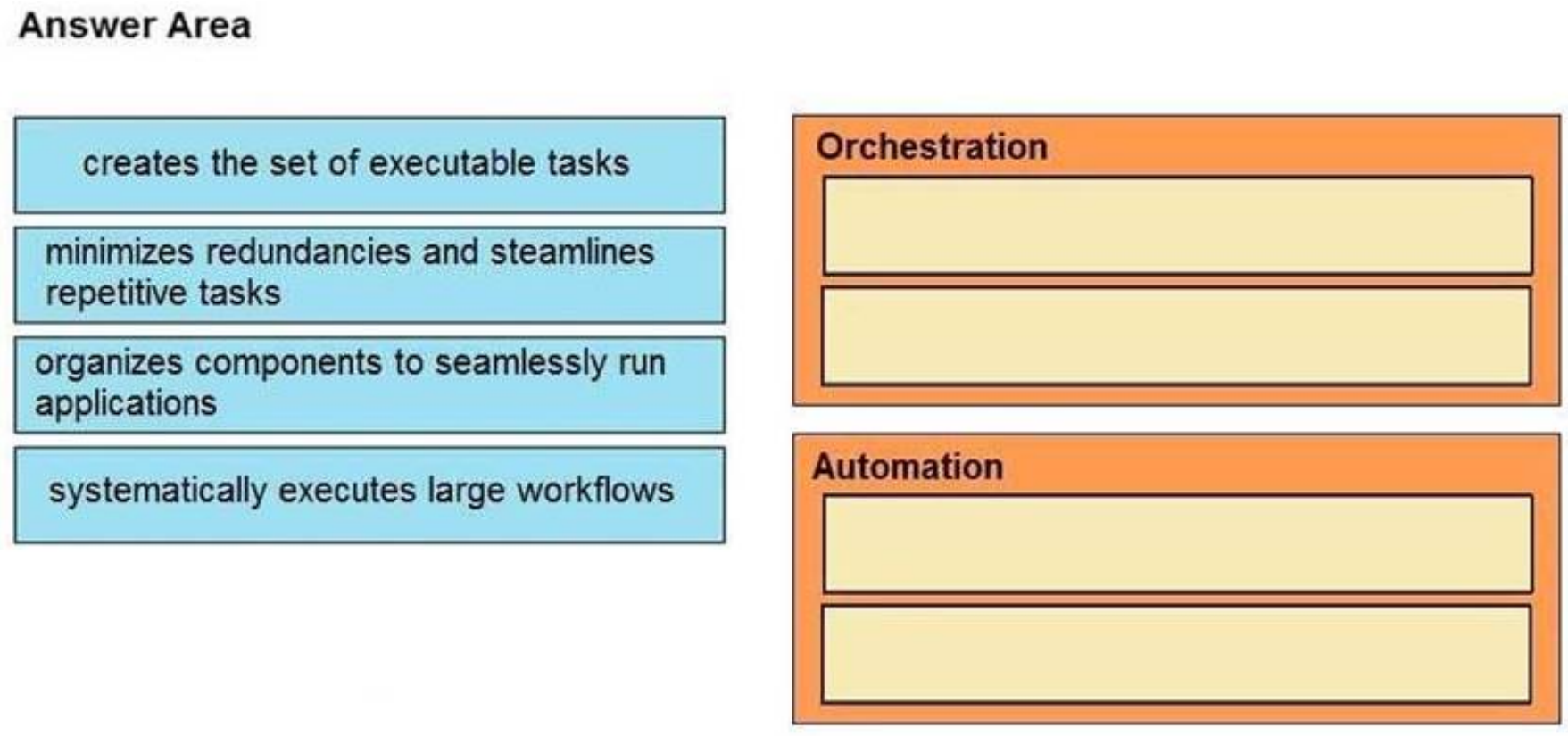
Answer: D

NEW QUESTION 54
A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

A. SNMPv2
B. TCP small services
C. port UDP 161 and 162
D. UDP small services

Answer: A

NEW QUESTION 55
Drag and drop the function on the left onto the mechanism on the right.



A. Mastered
B. Not Mastered

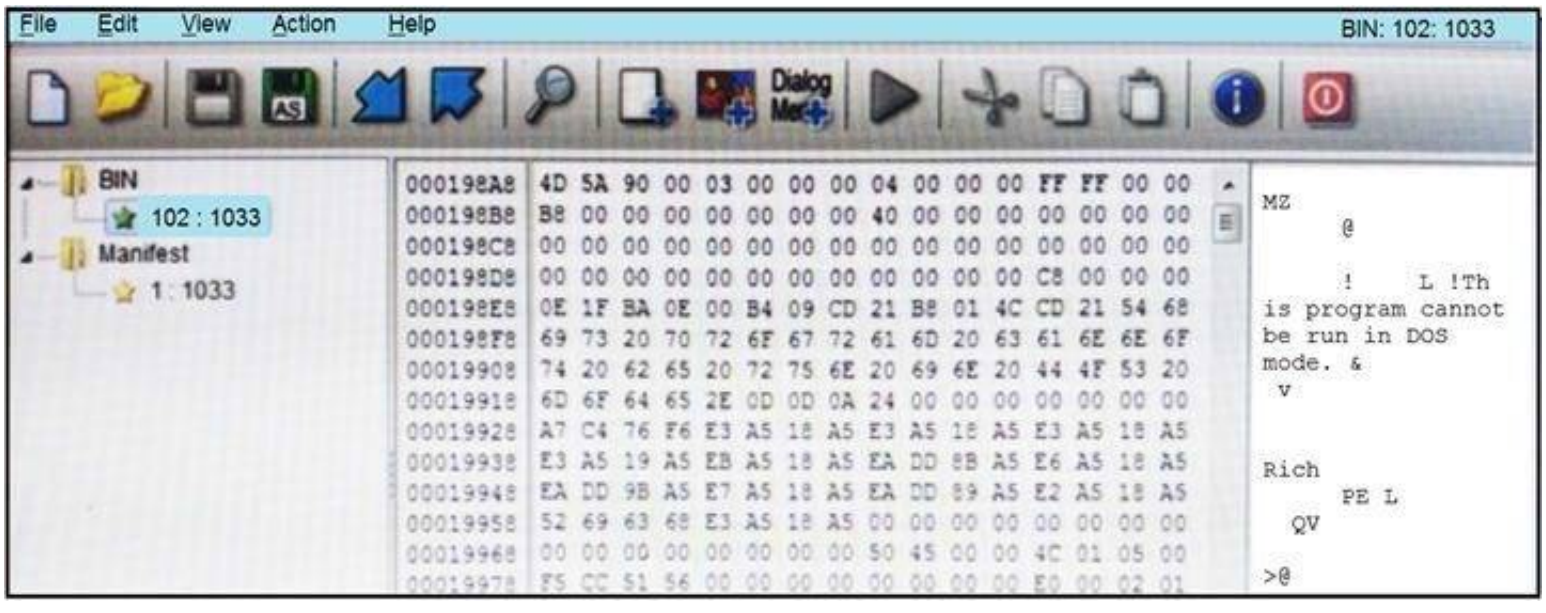
Answer: A

Explanation:

Answer Area

creates the set of executable tasks	**Orchestration** organizes components to seamlessly run applications creates the set of executable tasks
minimizes redundancies and steamlines repetitive tasks	**Automation** minimizes redundancies and steamlines repetitive tasks systematically executes large workflows
organizes components to seamlessly run applications	
systematically executes large workflows	

NEW QUESTION 59
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 62
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

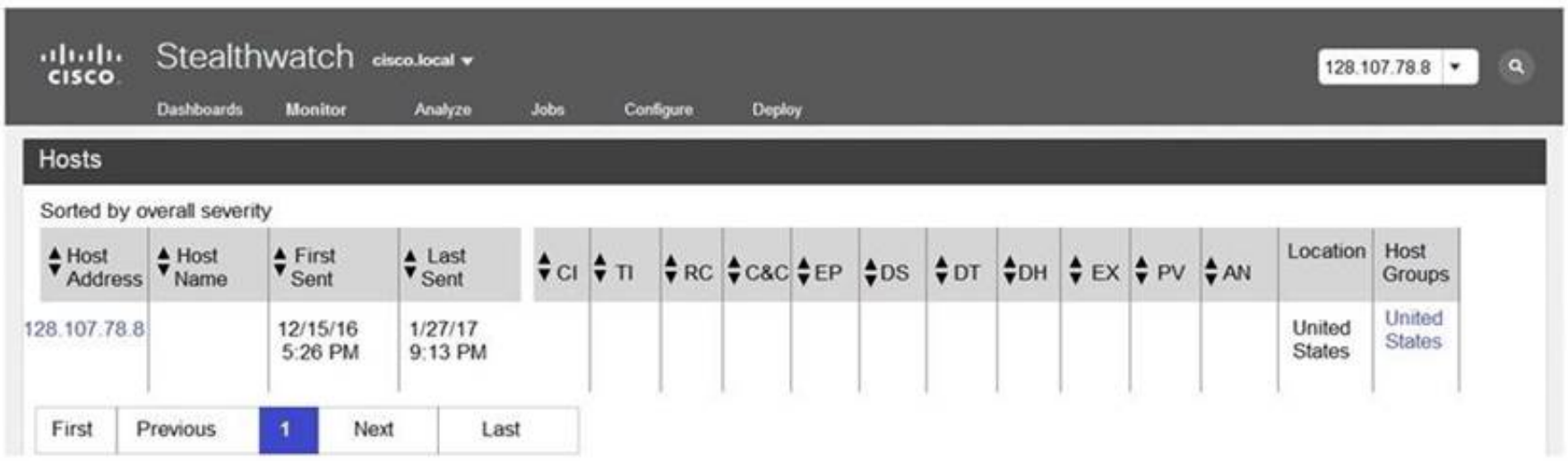
Answer: D

NEW QUESTION 64
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 67
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

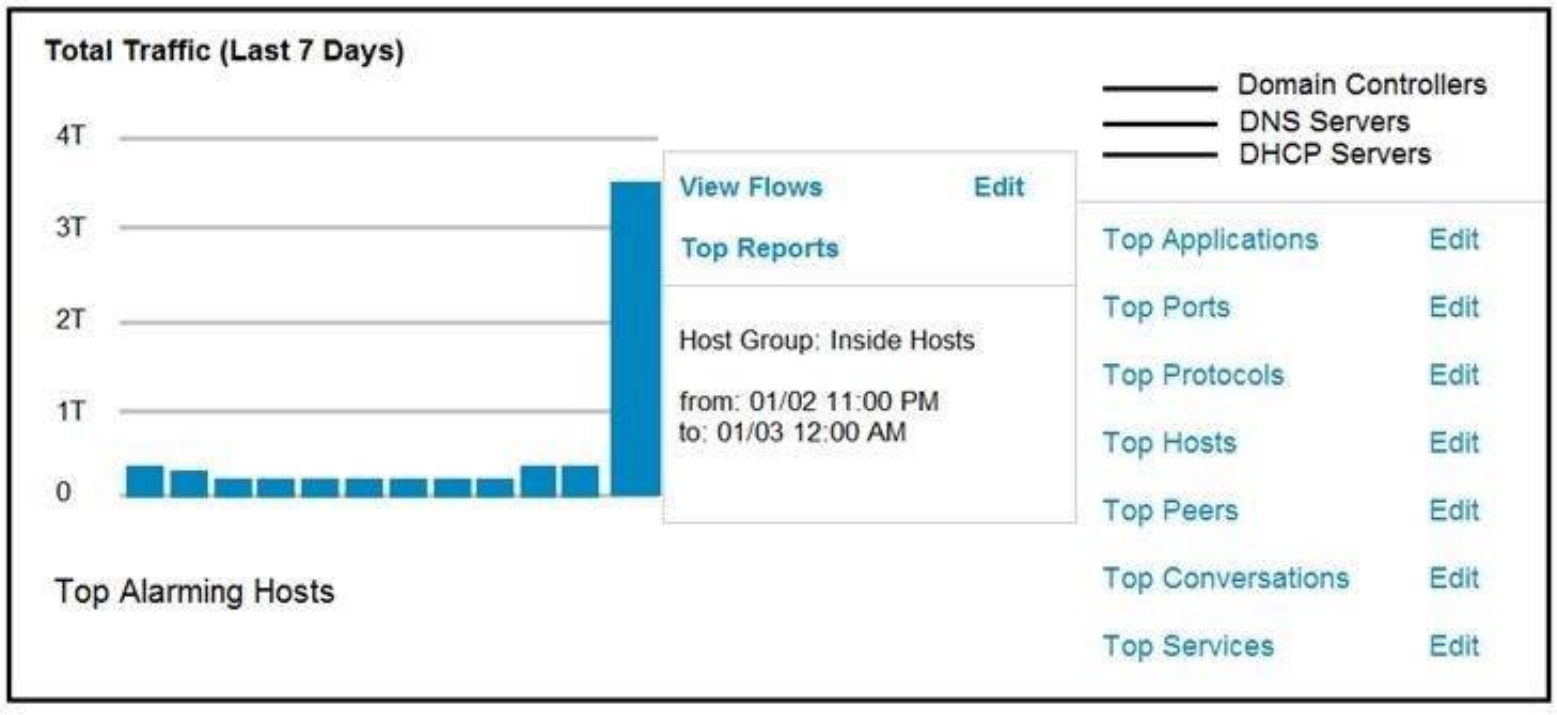
Answer: A

Explanation:

Answer Area

Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment

NEW QUESTION 72
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

Answer: B

NEW QUESTION 75
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

Answer: D

NEW QUESTION 77
An engineer is analyzing a possible compromise that happened a week ago when the company ? (Choose two.)

A. firewall
B. Wireshark
C. autopsy
D. SHA512
E. IPS

Answer: AB

NEW QUESTION 79
Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Answer Area

build	Phase 1
release	Phase 2
deploy	Phase 3
operate	Phase 4
monitor	Phase 5
test	Phase 6
plan	Phase 7
develop	Phase 8

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

build	plan
release	develop
deploy	build
operate	test
monitor	release
test	deploy
plan	operate
develop	monitor

NEW QUESTION 80
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

Answer: C

NEW QUESTION 81
Refer to the exhibit.

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm-0, isRealm=0, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where does it signify that a page will be stopped from loading when a scripting attack is detected?

A. x-frame-options
B. x-content-type-options
C. x-xss-protection
D. x-test-debug

Answer: C

NEW QUESTION 82
An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to “output alert_syslog: output log”
B. Modify the output module rule to “output alert_quick: output filename”
C. Modify the alert rule to “output alert_syslog: output header”
D. Modify the output module rule to “output alert_fast: output filename”

Answer: A

NEW QUESTION 83
.....

Relate Links

100% Pass Your 350-201 Exam with Exambible Prep Materials

https://www.exambible.com/350-201-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/