

Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)



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

The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

- A. Determine the assets to which the attacker has access
- B. Identify assets the attacker handled or acquired
- C. Change access controls to high risk assets in the enterprise
- D. Identify movement of the attacker in the enterprise

Answer: D

NEW 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

Answer: C

NEW QUESTION 4

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

- A. Assess the network for unexpected behavior
- B. Isolate critical hosts from the network
- C. Patch detected vulnerabilities from critical hosts
- D. Perform analysis based on the established risk factors

Answer: B

NEW QUESTION 5

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 6

Employees report computer system crashes within the same week. An analyst is investigating one of the computers that crashed and discovers multiple shortcuts in the system's startup folder. It appears that the shortcuts redirect users to malicious URLs. What is the next step the engineer should take to investigate this case?

- A. Remove the shortcut files
- B. Check the audit logs
- C. Identify affected systems
- D. Investigate the malicious URLs

Answer: C

NEW QUESTION 7

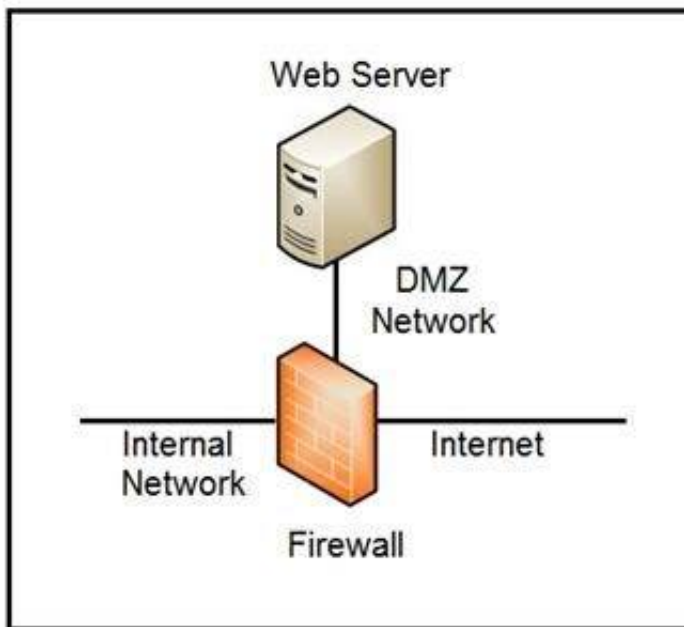
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open 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 8

Refer to the exhibit.



Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

- A. Create an ACL on the firewall to allow only TLS 1.3
- B. Implement a proxy server in the DMZ network
- C. Create an ACL on the firewall to allow only external connections
- D. Move the webserver to the internal network

Answer: BD

NEW QUESTION 9

Refer to the exhibit.

URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

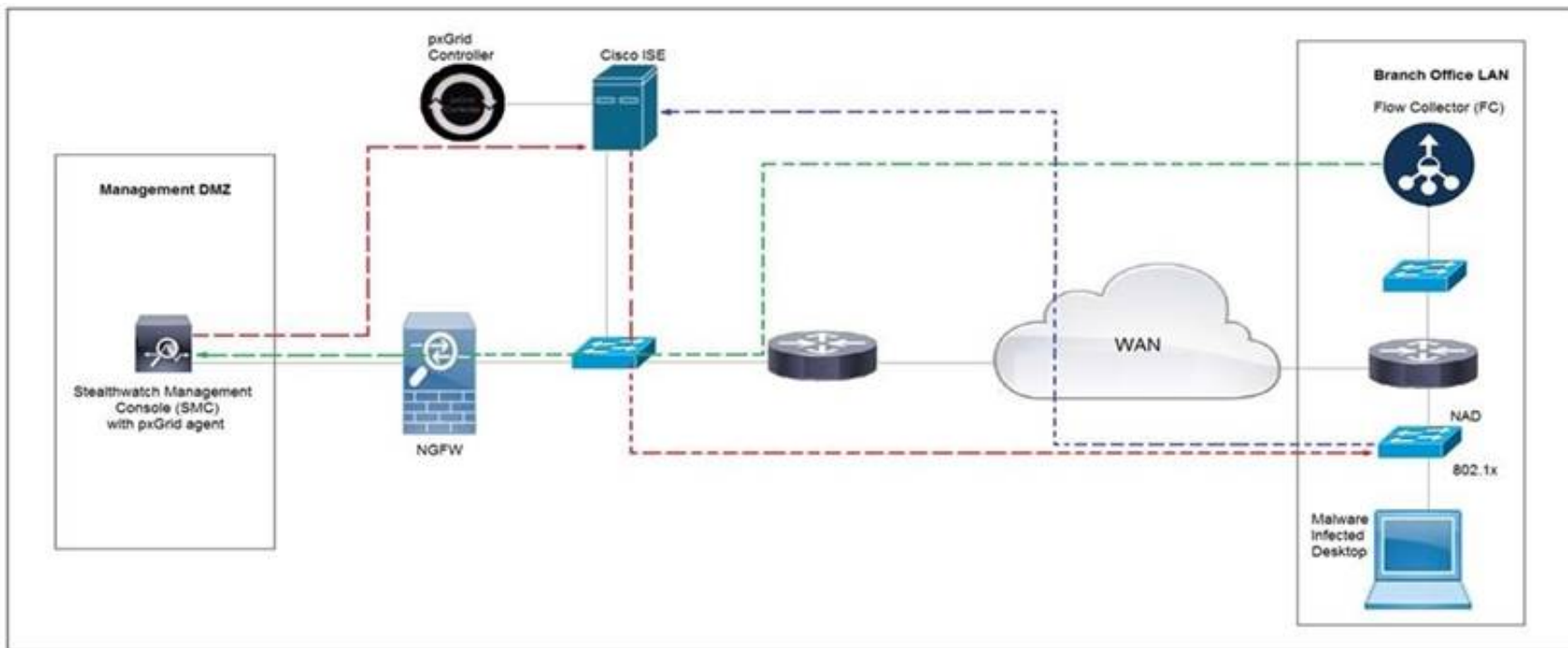
At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

- A. exploitation
- B. actions on objectives
- C. delivery
- D. reconnaissance

Answer: C

NEW QUESTION 10

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

Answer: B

NEW QUESTION 10

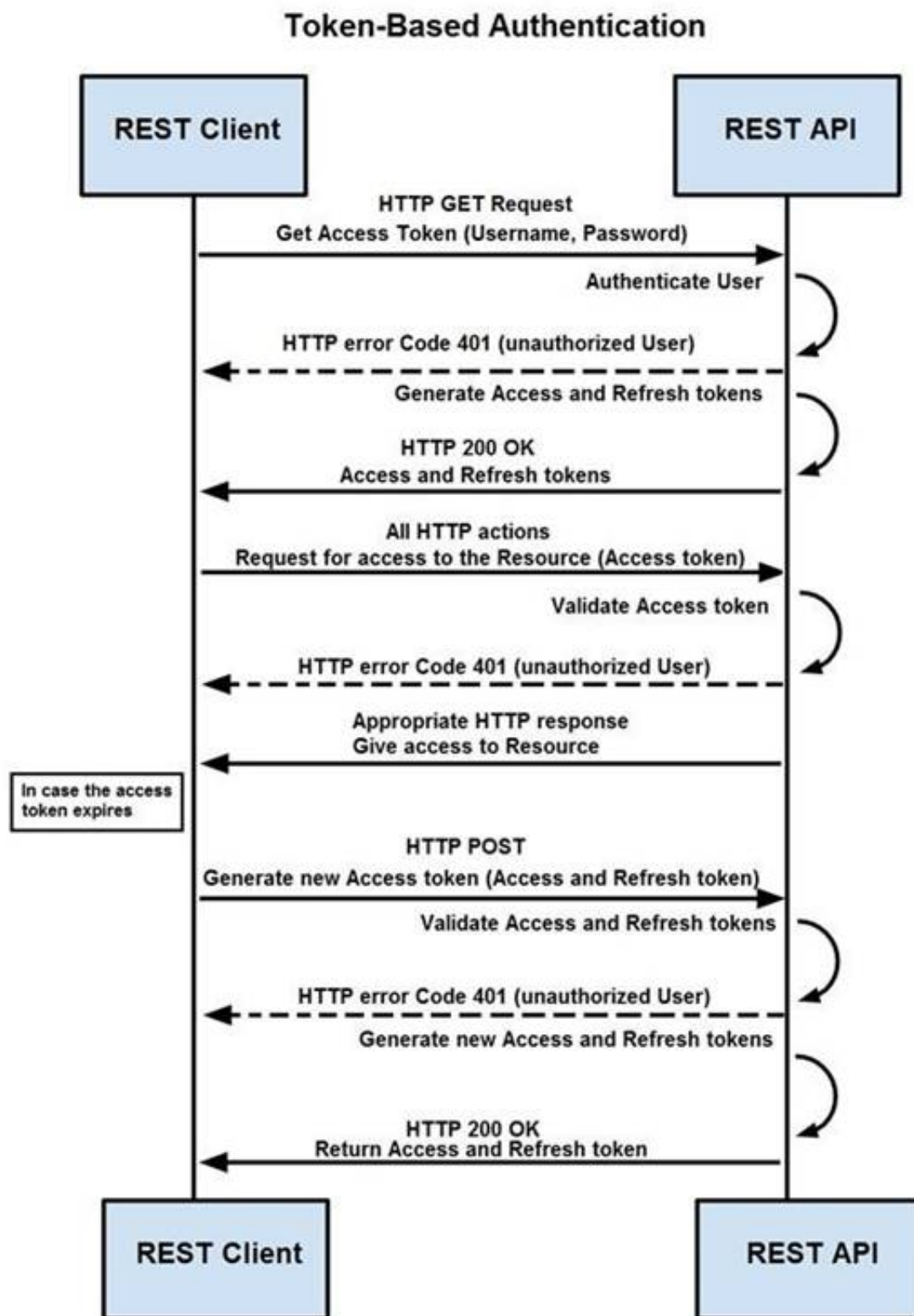
According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

- A. Perform a vulnerability assessment
- B. Conduct a data protection impact assessment
- C. Conduct penetration testing
- D. Perform awareness testing

Answer: B

NEW QUESTION 13

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

Answer: D

NEW QUESTION 16

Refer to the exhibit.



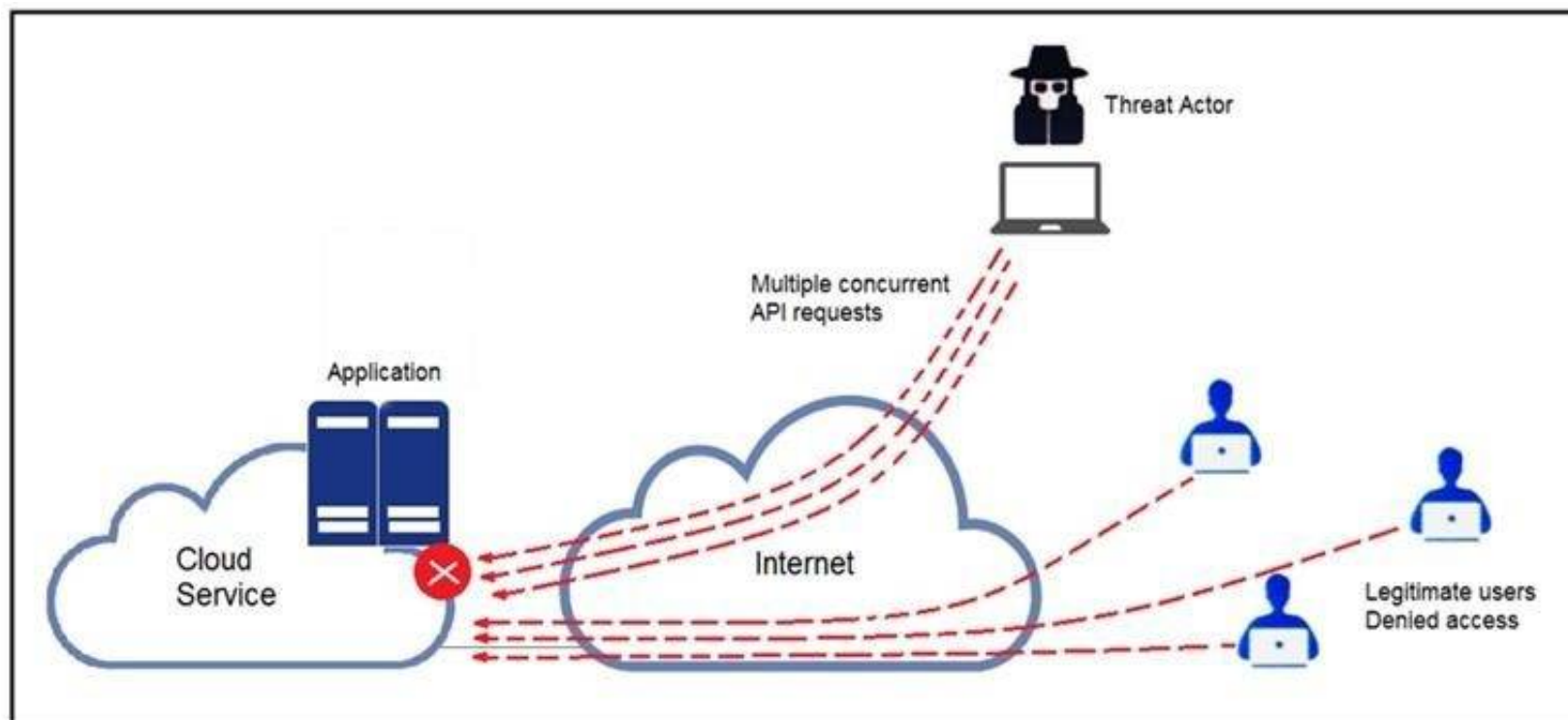
An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the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

Answer: D

NEW QUESTION 19

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

Answer: A

NEW QUESTION 22

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 23

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 28

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 32

An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

- A. Investigate the vulnerability to prevent further spread
- B. Acknowledge the vulnerabilities and document the risk
- C. Apply vendor patches or available hot fixes
- D. Isolate the assets affected in a separate network

Answer: D

NEW QUESTION 35

Drag and drop the cloud computing service descriptions from the left onto the cloud service categories on the right.

Answer Area

triggers a block of code when triggered by a specific event	SaaS
allows renting full servers or virtual machines	PaaS
focuses on developing, testing, and delivering applications	IaaS
allows hosting and managing a virtual environment	FaaS

- A. Mastered
- B. Not Mastered

Answer: A

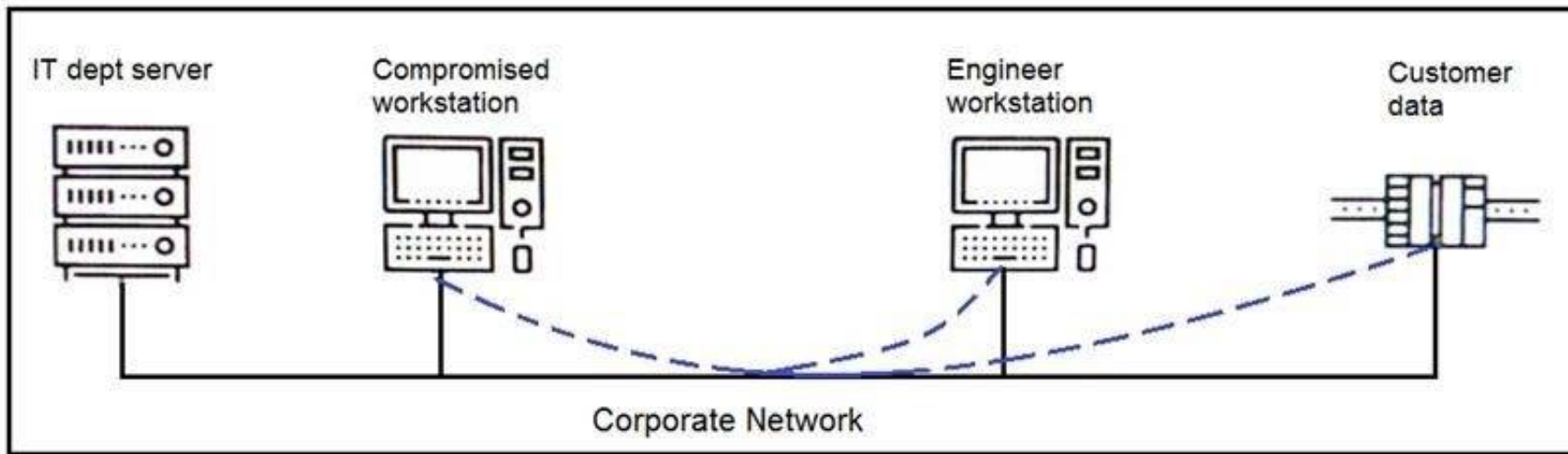
Explanation:

Answer Area

triggers a block of code when triggered by a specific event	focuses on developing, testing, and delivering applications
allows renting full servers or virtual machines	allows hosting and managing a virtual environment
focuses on developing, testing, and delivering applications	allows renting full servers or virtual machines
allows hosting and managing a virtual environment	triggers a block of code when triggered by a specific event

NEW QUESTION 38

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 42

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 46

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 48

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 53

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 58

A company’s web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

- A. assessment scope
- B. event severity and likelihood
- C. incident response playbook
- D. risk model framework

Answer: D

NEW QUESTION 60

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 62

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials. How should the workflow be improved to resolve these issues?

- A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts
- B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats
- C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts
- D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts

Answer: B

NEW QUESTION 66

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

spoofing attack

broken authentication attack

injection attack

man-in-the-middle attack

privilege escalation attack

default credential attack

installing network devices

developing new code

implementing a new application

changing configuration settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

spoofing attack

broken authentication attack

injection attack

man-in-the-middle attack

privilege escalation attack

default credential attack

man-in-the-middle attack

injection attack

privilege escalation attack

default credential attack

NEW QUESTION 69

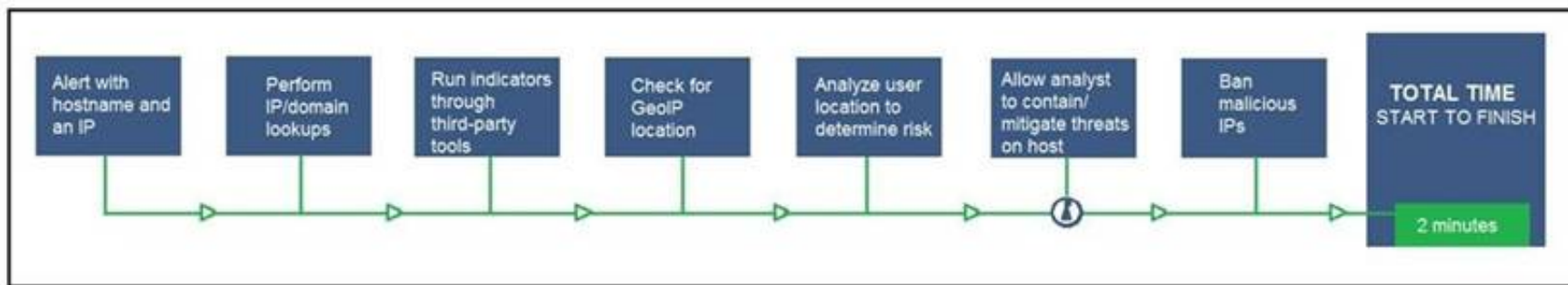
An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

- A. continuous delivery
- B. continuous integration
- C. continuous deployment
- D. continuous monitoring

Answer: A

NEW QUESTION 71

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 GeolP 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 72

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 74

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 78

An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach. Which indicator generated this IOC event?

- A. ExecutedMalware.ioc
- B. Crossrider.ioc
- C. ConnectToSuspiciousDomain.ioc
- D. W32 AccesschkUtility.ioc

Answer: D

NEW QUESTION 81

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 83

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 86

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 89

Refer to the exhibit.

```
def map_to_lowercase_letter(s):
    return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
    dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
    return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
    for c0 in xrange(97,123):
        for c1 in xrange(97, 123):
            for c2 in xrange(97,123):
                for c3 in xrange (97,123):
                    domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
                    domain = next_domain(domain)
                    if seed.startswith(domain):
                        return False
    return True
seeds = {
    "nhcisatformalisticirekb.com",
    "egfesatformalisticirekb.com",
    "qwfusatformalisticirekb.com",
    "eijhsatformalisticirekb.com",
    "siowsatformalisticirekb.com",
    "dhansatformalisticirekb.com",
    "zvogsatformalisticirekb.com",
    "yaewsatformalisticirekb.com",
    "wgxfsatformalisticirekb.com",
    "vfxlsatformalisticirekb.com",
    "usjssatformalisticirekb.com",
    "selzsatformalisticirekb.com",
    "nzjqsatformalisticirekb.com",
    "kencsatformalisticirekb.com",
    "fzkxsatformalisticirekb.com",
    "babysatformalisticirekb.com",
}
for seed in seeds:
    print seed,isBanjoriTail(seed)
```

What results from this script?

- A. Seeds for existing domains are checked
- B. A search is conducted for additional seeds
- C. Domains are compared to seed rules
- D. A list of domains as seeds is blocked

Answer: B

NEW QUESTION 93

Refer to the exhibit.

```
#!/usr/bin/env python3

import re

def (username, minlen):
    if type(username) != str:
        raise TypeError
    if minlen < 3:
        raise ValueError
    if len(username) < minlen:
        return False
    if not re.match('[a-z0-9._]*$', username):
        return False
    if username[0].isnumeric():
        return False
    return True
```

An organization is using an internal application for printing documents that requires a separate registration on the website. The application allows format-free user creation, and users must match these required conditions to comply with the company's user creation policy:

- > minimum length: 3
- > usernames can only use letters, numbers, dots, and underscores
- > usernames cannot begin with a number

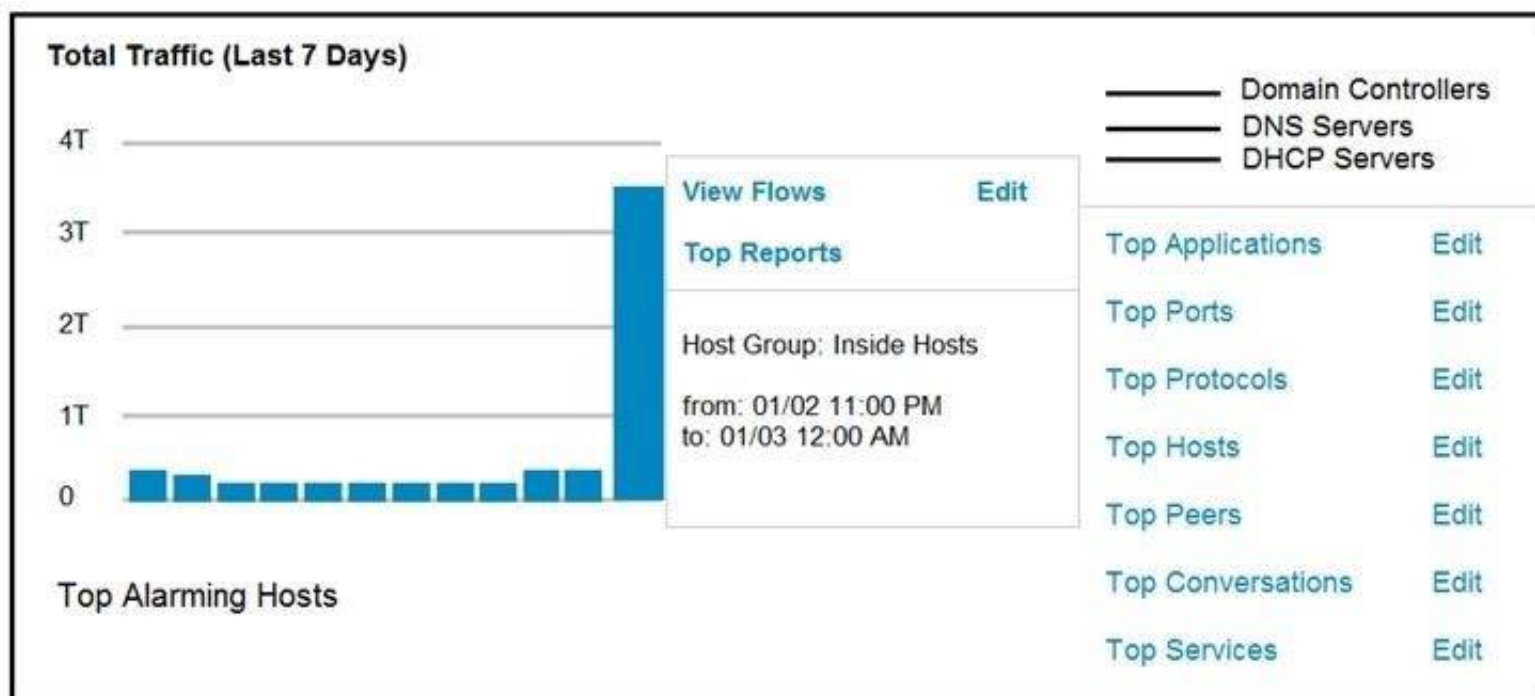
The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able to create format-free usernames. Which change is needed to apply the restrictions?

- A. modify code to return error on restrictions def return false_user(username, minlen)
- B. automate the restrictions def automate_user(username, minlen)
- C. validate the restrictions, def validate_user(username, minlen)
- D. modify code to force the restrictions, def force_user(username, minlen)

Answer: B

NEW QUESTION 96

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 98

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

Answer: C

NEW QUESTION 99

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

- A. Run the sudo sysdiagnose command
- B. Run the sh command
- C. Run the w command
- D. Run the who command

Answer: A

NEW QUESTION 103

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 350-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 350-201 Practice Test Here](#)