# 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**
Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

A. chmod 666
B. chmod 774
C. chmod 775
D. chmod 777

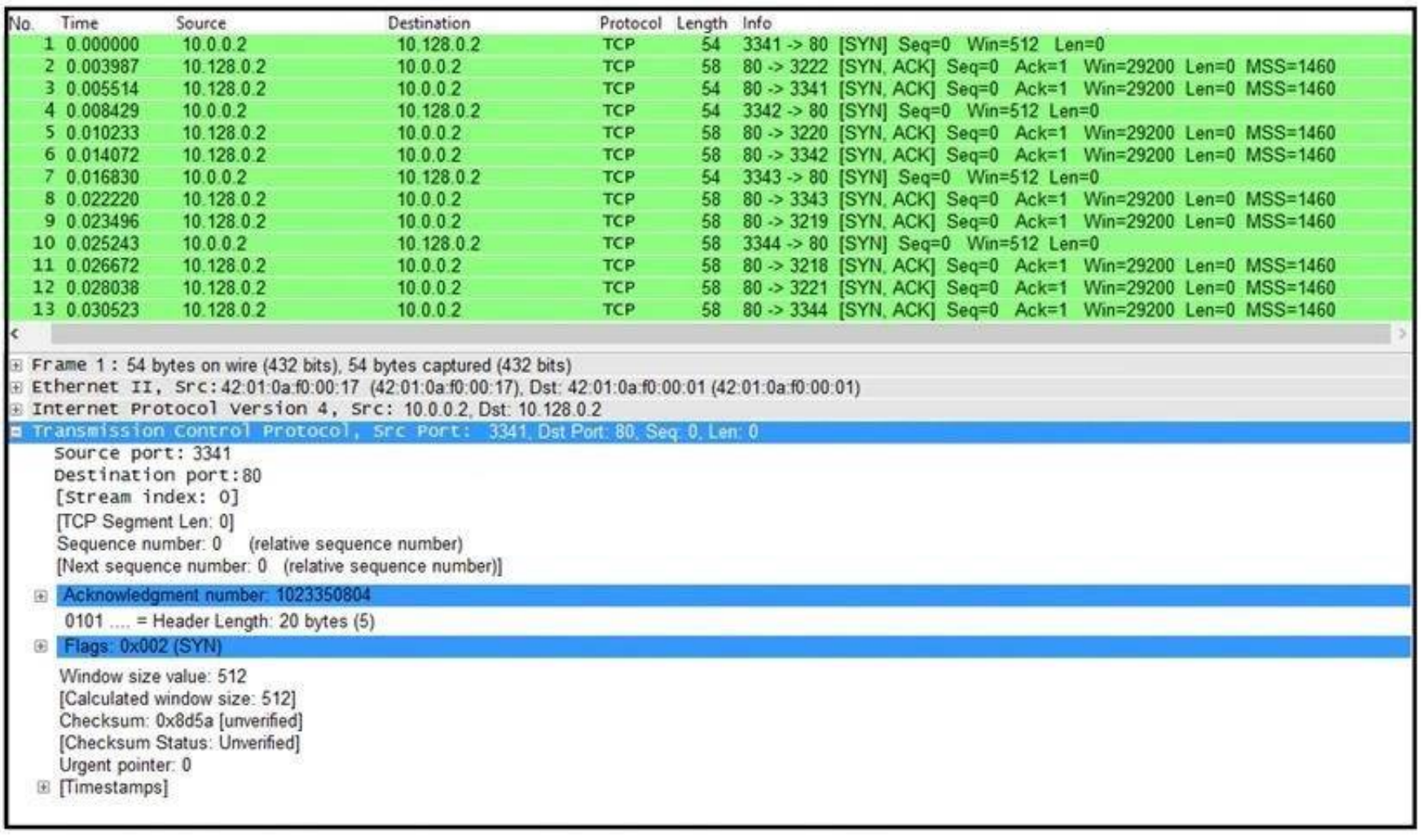
**Answer:** D

**NEW QUESTION 3**
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 4**
Refer to the exhibit.




What is the threat in this Wireshark traffic capture?

A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
B. A flood of ACK packets coming from a single source IP to multiple destination IPs

C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
D. A flood of SYN packets coming from a single source IP to a single destination IP

**Answer:** D

**NEW QUESTION 5**
How is a SIEM tool used?

A. To collect security data from authentication failures and cyber attacks and forward it for analysis
B. To search and compare security data against acceptance standards and generate reports for analysis
C. To compare security alerts against configured scenarios and trigger system responses
D. To collect and analyze security data from network devices and servers and produce alerts

**Answer:** D

**NEW QUESTION 6**
Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.

**Answer Area**

| | |
|---|---|
| vulnerability assessment | gathering information on a target for future use |
| persistence | probing the target to discover operating system details |
| exploit | confirming the existence of known vulnerabilities in the target system |
| cover tracks | using previoulsy identified vulnerabilities to gain access to the target system |
| reconnaissance | inserting backdoor access or covert channels to ensure access to the target system |
| enumeration | erasing traces of actions in audit logs and registry entries |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| | |
|---|---|
| vulnerability assessment | persistence |
| persistence | reconnaissance |
| exploit | vulnerability assessment |
| cover tracks | exploit |
| reconnaissance | enumeration |
| enumeration | cover tracks |

**NEW QUESTION 7**
An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. Which two behaviors triggered UEBA? (Choose two.)

A. domain belongs to a competitor
B. log in during non-working hours

C. email forwarding to an external domain
D. log in from a first-seen country
E. increased number of sent mails

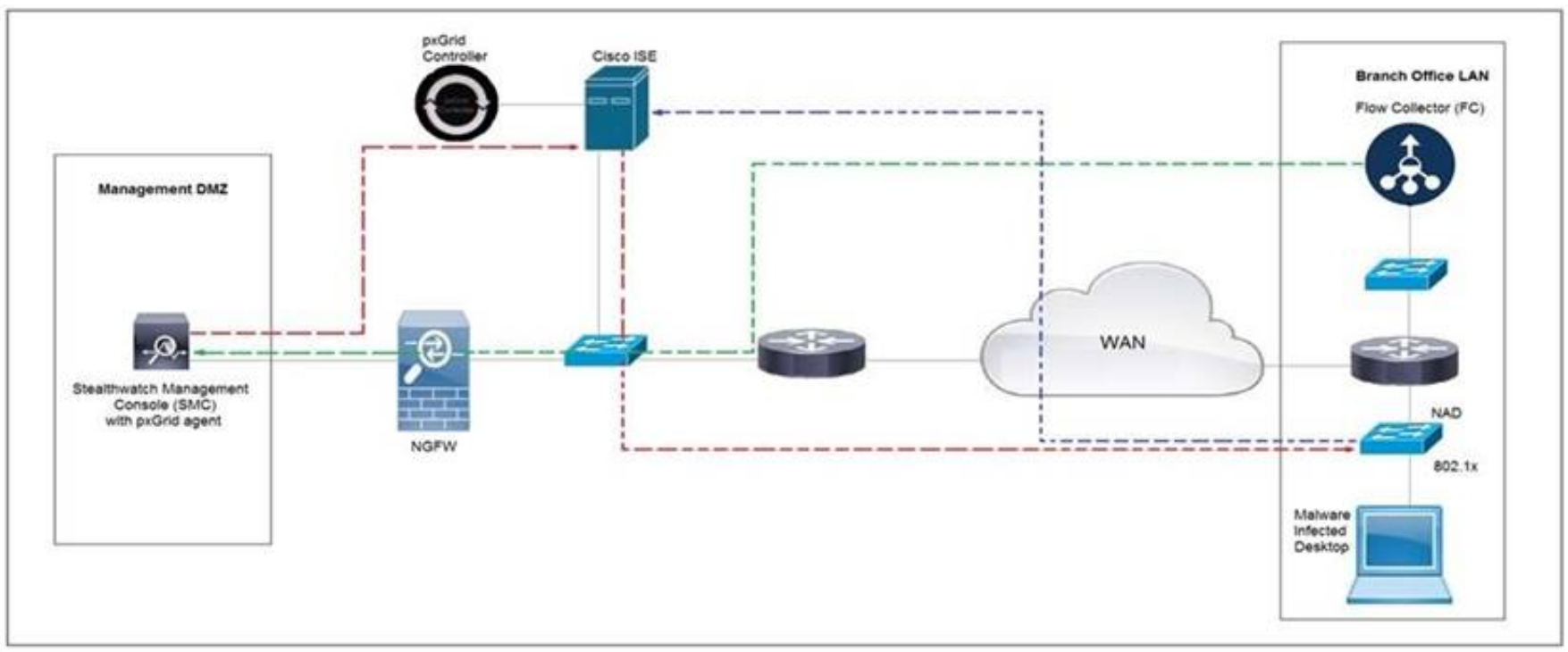
**Answer:** AB

**NEW QUESTION 8**
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 9**
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**
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

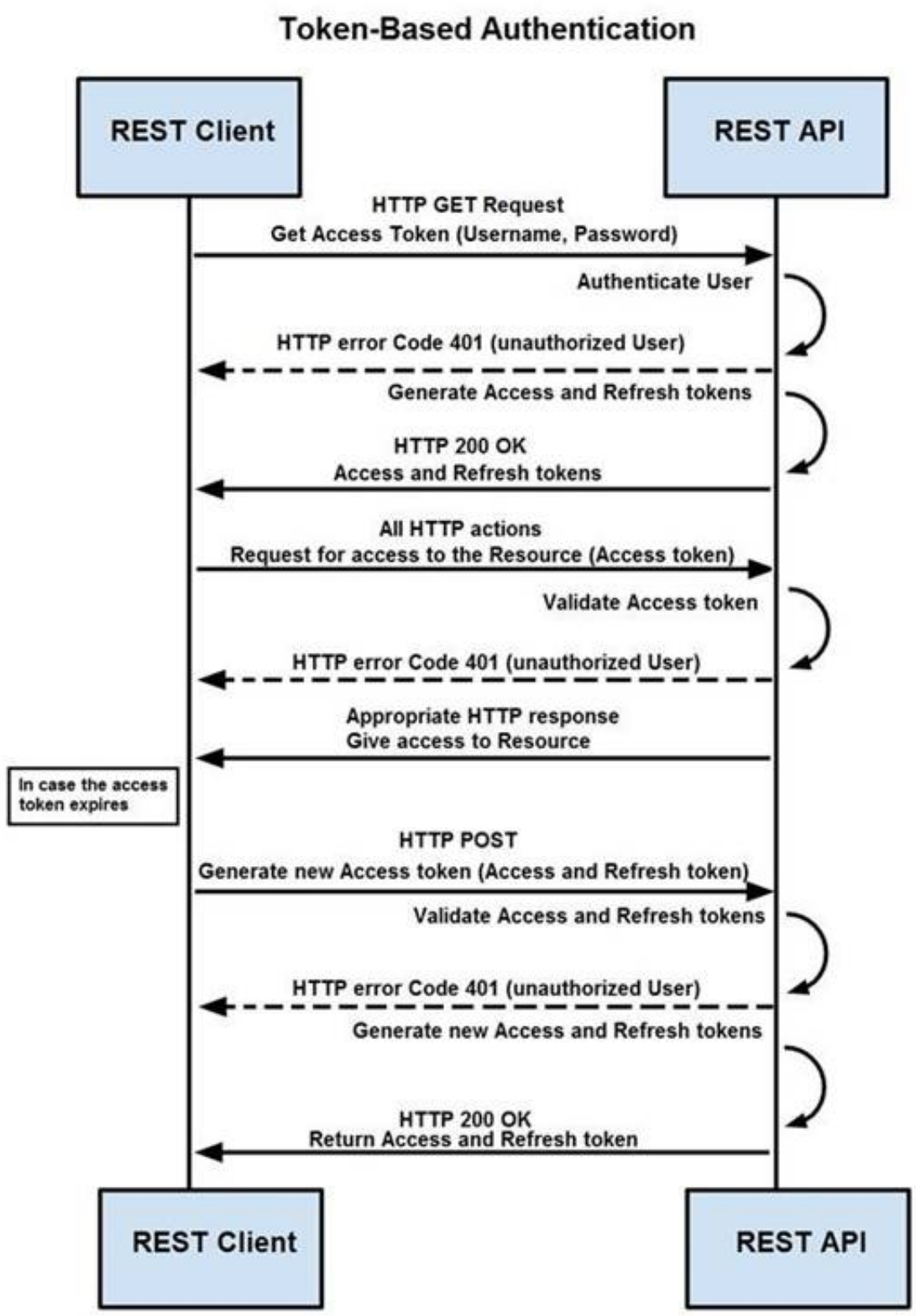
**Answer:** D

**NEW QUESTION 10**
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 14**
Refer to the exhibit.

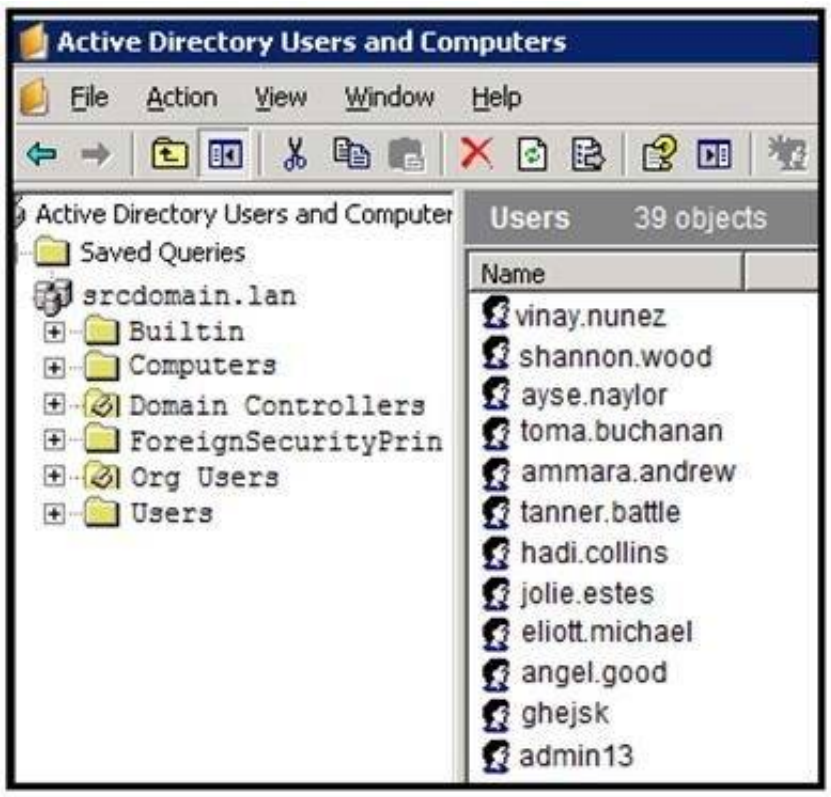



How are tokens authenticated when the REST API on a device is accessed from a REST API client?

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 16**
Refer to the exhibit.

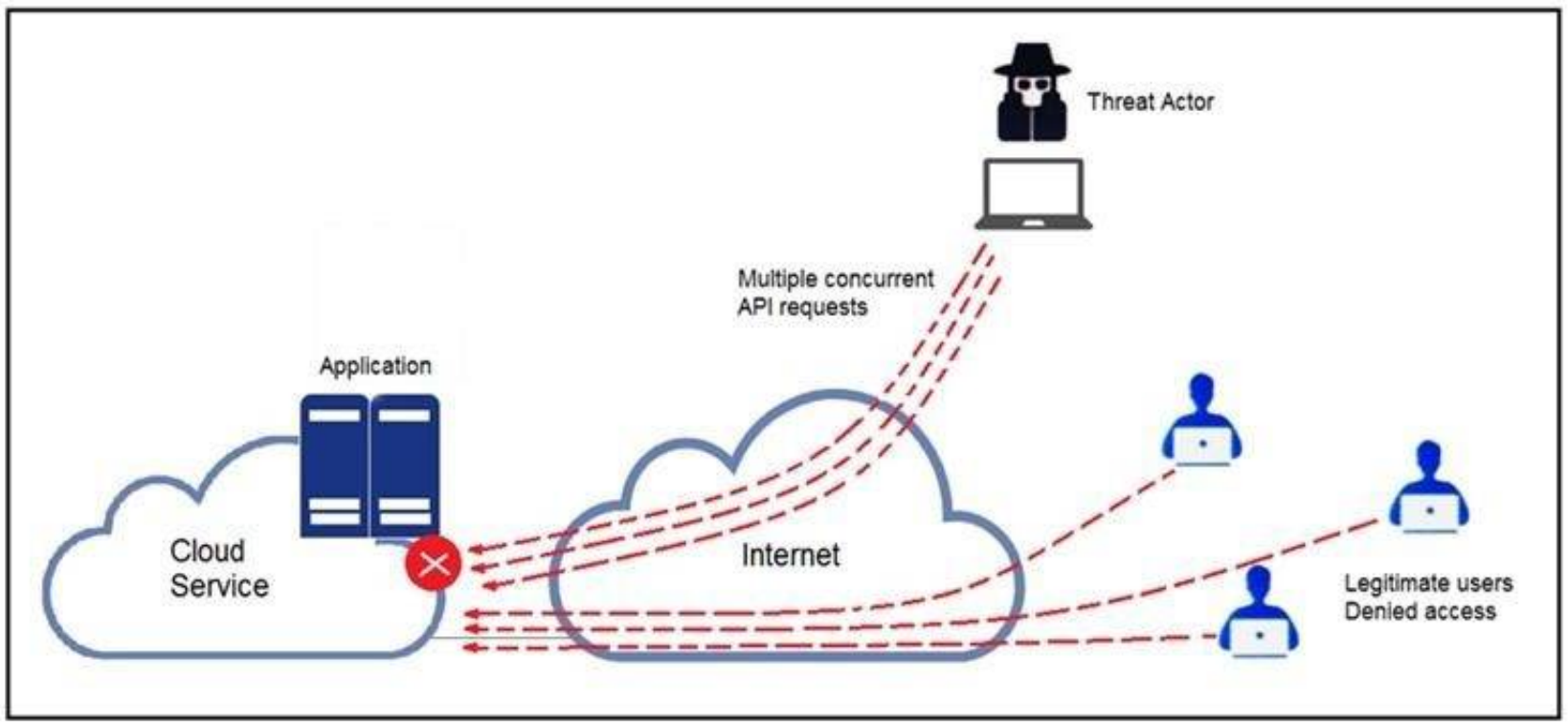



An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the 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 21**
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 26**

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 31**
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

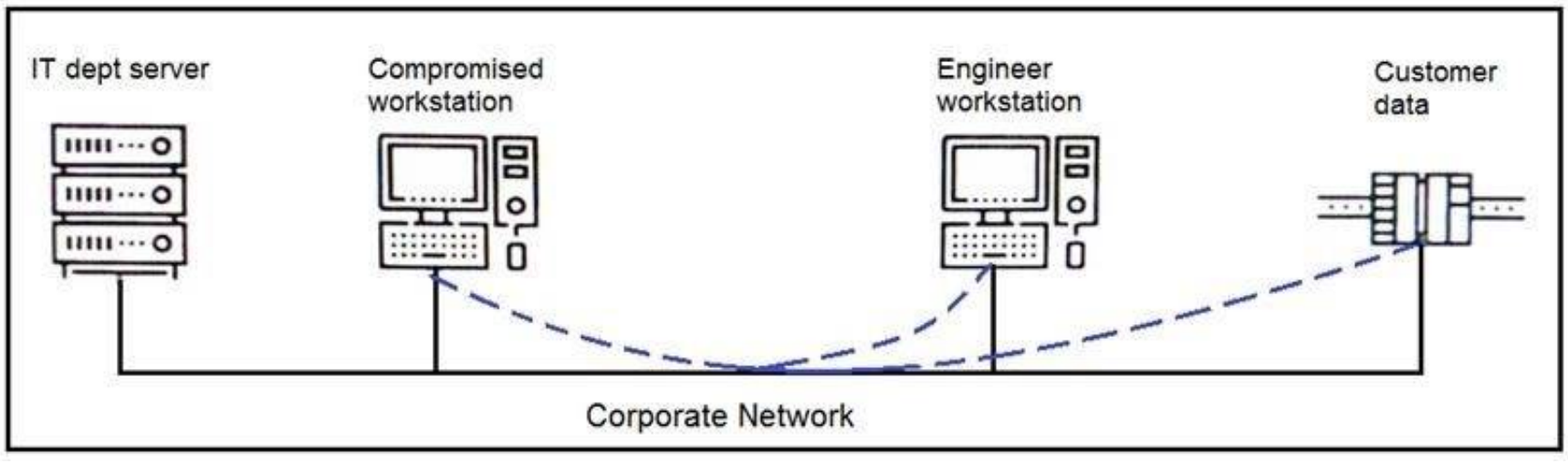
**Answer:** A

**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 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 44**
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**
An engineer receives a report that indicates a possible incident of a malicious insider sending company information to outside parties. What is the first action the engineer must take to determine whether an incident has occurred?

A. Analyze environmental threats and causes
B. Inform the product security incident response team to investigate further
C. Analyze the precursors and indicators
D. Inform the computer security incident response team to investigate further

**Answer:** C

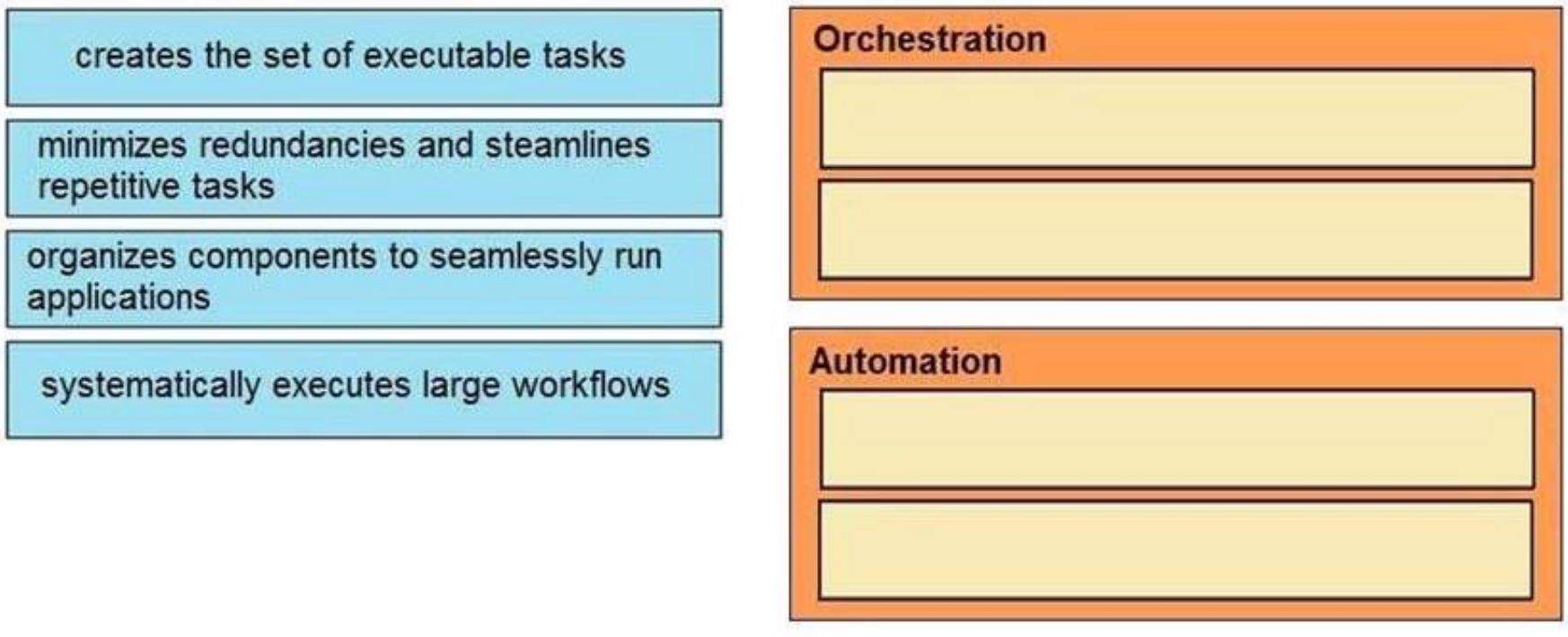
**NEW QUESTION 51**
A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

A. Determine the systems involved and deploy available patches
B. Analyze event logs and restrict network access
C. Review access lists and require users to increase password complexity
D. Identify the attack vector and update the IDS signature list

**Answer:** B

**NEW QUESTION 52**
Drag and drop the function on the left onto the mechanism on the right.

**Answer Area**

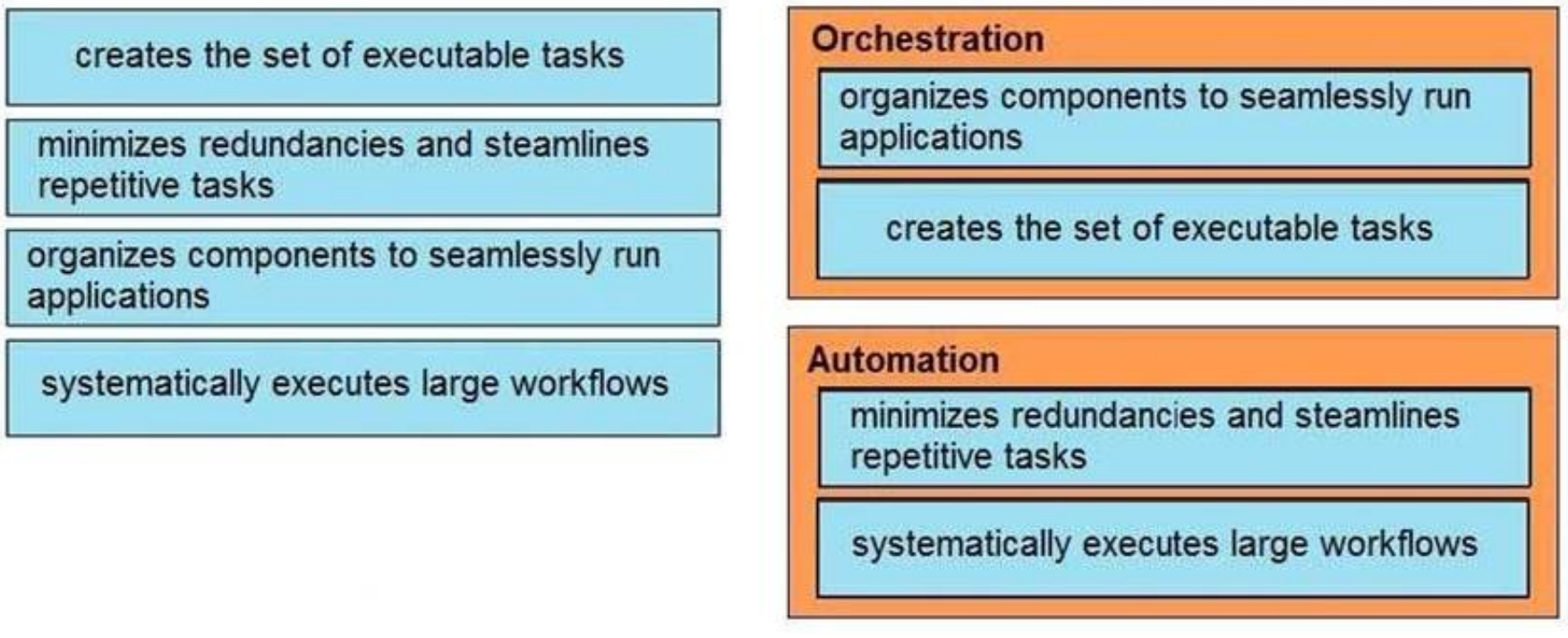



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**




**NEW QUESTION 54**
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 56**
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 58**
Refer to the exhibit.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 ( msg:"PROTOCOL-
IMAP login brute force attempt";
flow:to_server,established,no_stream;
content:"LOGIN",fast_pattern,nocase; detection_filter:track
by_dst, count 5, seconds 900; metadata:ruleset community;
service:imap; reference:url,attack.mitre.org/techniques/T1110;
classtype:suspicious-login; sid:2273; rev:12; )
```

IDS is producing an increased amount of false positive events about brute force attempts on the organization's mail server. How should the Snort rule be modified to improve performance?

A. Block list of internal IPs from the rule
B. Change the rule content match to case sensitive
C. Set the rule to track the source IP
D. Tune the count and seconds threshold of the rule

**Answer:** B

**NEW QUESTION 61**
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,isBanjonTail(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 64**
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 67**
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 69**
What is a principle of Infrastructure as Code?

A. System maintenance is delegated to software systems
B. Comprehensive initial designs support robust systems
C. Scripts and manual configurations work together to ensure repeatable routines
D. System downtime is grouped and scheduled across the infrastructure

**Answer:** B

**NEW QUESTION 74**
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 78**
A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user's working hours, what must the analyst do next to detect an abnormal behavior?

A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period
B. Create a rule triggered by 1 successful VPN connection from any nondestination country
C. Create a rule triggered by multiple successful VPN connections from the destination countries
D. Analyze the logs from all countries related to this user during the traveling period

**Answer:** D

**NEW QUESTION 82**
.....

# 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/