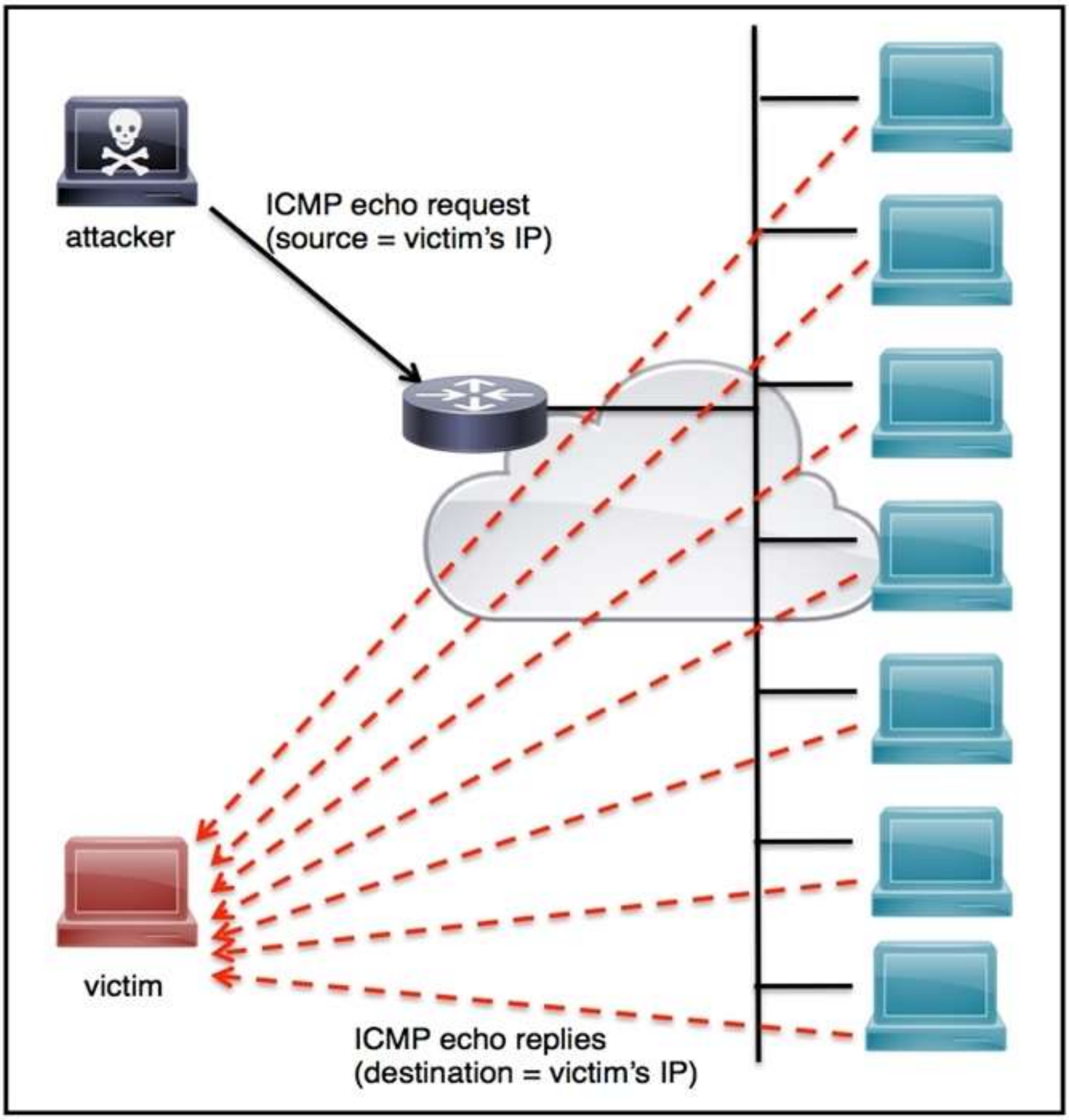
- **Vendor:** Cisco
- **Exam Code:** 350-201
- **Exam Name:** Performing CyberOps Using Core Security Technologies
- **New Updated Questions from** Braindump2go **(Updated in** July/2021**)**

QUESTION 1

Refer to the exhibit. An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets.

The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address.

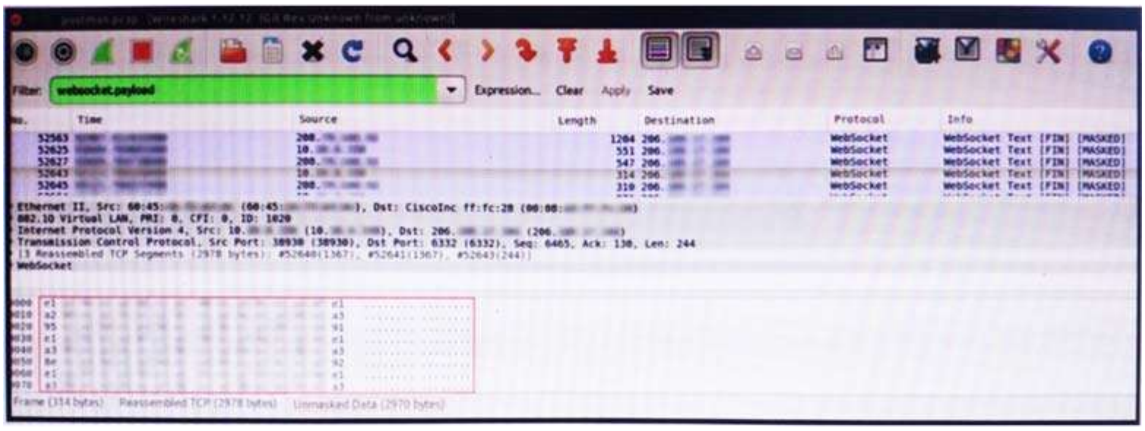
Which action does the engineer recommend?



A. Use command ip verify reverse-path interface
B. Use global configuration command service tcp-keepalives-out
C. Use subinterface command no ip directed-broadcast
D. Use logging trap 6

Answer: A
Explanation:
https://www.ccexpert.us/pix-firewall/ip-verify-reversepath-command.html

QUESTION 2
Refer to the exhibit. An engineer is analyzing this Vlan0392-int12-239.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?



```
No.     Time                     Source                 Length  Destination       Protocol    Info
52563   [redacted]               200.[redacted]         1204    206.[redacted]    WebSocket   WebSocket Text [FIN] [MASKED]
52625   [redacted]               10.[redacted]          551     206.[redacted]    WebSocket   WebSocket Text [FIN] [MASKED]
52627   [redacted]               200.[redacted]         547     206.[redacted]    WebSocket   WebSocket Text [FIN] [MASKED]
52643   [redacted]               10.[redacted]          314     206.[redacted]    WebSocket   WebSocket Text [FIN] [MASKED]
52645   [redacted]               200.[redacted]         310     206.[redacted]    WebSocket   WebSocket Text [FIN] [MASKED]

Ethernet II, Src: 60:45:[redacted] (60:45:[redacted]), Dst: CiscoInc ff:fc:28 (00:08:[redacted])
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1020
Internet Protocol Version 4, Src: 10.[redacted] (10.[redacted]), Dst: 206.[redacted] (206.[redacted])
Transmission Control Protocol, Src Port: 38930 (38930), Dst Port: 6332 (6332), Seq: 6465, Ack: 130, Len: 244
[3 Reassembled TCP Segments (2978 bytes): #52640(1367), #52641(1367), #52643(244)]
WebSocket

0000  e1 [redacted] e1   ........ ........
0010  a2 [redacted] a3   ........ ........
0020  95 [redacted] 91   ........ ........
0030  e1 [redacted] e1   ........ ........
0040  a3 [redacted] a3   ........ ........
0050  8e [redacted] 92   ........ ........
0060  e1 [redacted] e1   ........ ........
0070  a3 [redacted] a3   ........ ........
Frame (314 bytes)   Reassembled TCP (2978 bytes)   Unmasked Data (2970 bytes)
```

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

QUESTION 3
What do 2xx HTTP response codes indicate for REST APIs?

A. additional action must be taken by the client to complete the request
B. the server takes responsibility for error status codes
C. communication of transfer protocol-level information
D. successful acceptance of the client's request

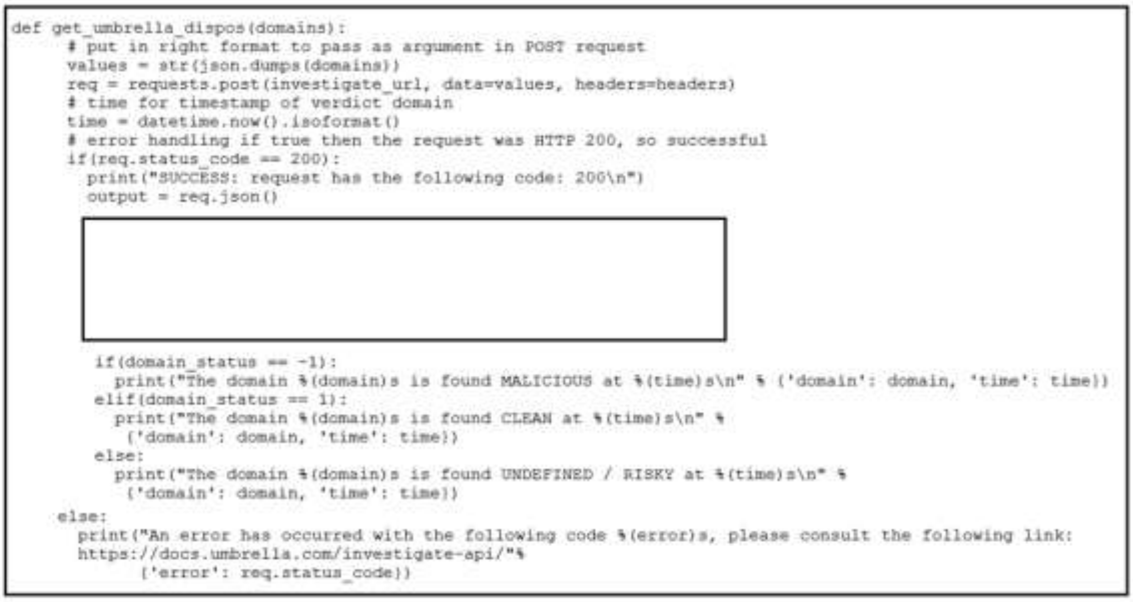
Answer: D

QUESTION 4
An engineer received an alert of a zero-day vulnerability affecting desktop phones through which an attacker sends a crafted packet to a device, resets the credentials, makes the device unavailable, and allows a default administrator account login. Which step should an engineer take after receiving this alert?

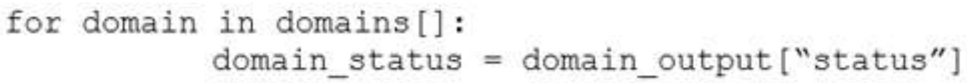
A. Initiate a triage meeting to acknowledge the vulnerability and its potential impact
B. Determine company usage of the affected products
C. Search for a patch to install from the vendor
D. Implement restrictions within the VoIP VLANS

Answer: C

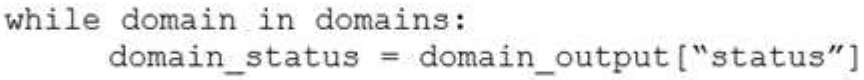
QUESTION 5
Refer to the exhibit. Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?



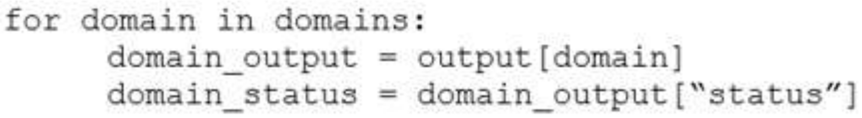
```
def get_umbrella_dispos(domains):
      # put in right format to pass as argument in POST request
      values = str(json.dumps(domains))
      req = requests.post(investigate_url, data=values, headers=headers)
      # time for timestamp of verdict domain
      time = datetime.now().isoformat()
      # error handling if true then the request was HTTP 200, so successful
      if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()




         if(domain_status == -1):
           print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % ('domain': domain, 'time': time))
         elif(domain_status == 1):
           print("The domain %(domain)s is found CLEAN at %(time)s\n" %
            ('domain': domain, 'time': time))
         else:
           print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
            ('domain': domain, 'time': time))
     else:
       print("An error has occurred with the following code %(error)s, please consult the following link:
       https://docs.umbrella.com/investigate-api/"%
             ('error': req.status_code))
```

A. 

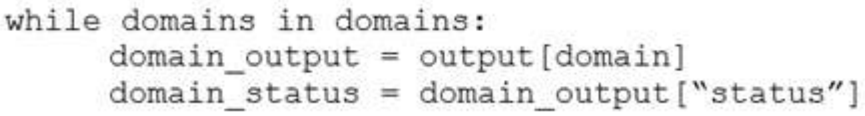
```
for domain in domains[]:
                domain_status = domain_output["status"]
```

B. 

```
while domain in domains:
       domain_status = domain_output["status"]
```

C. 

```
for domain in domains:
       domain_output = output[domain]
       domain_status = domain_output["status"]
```

D. 

```
while domains in domains:
       domain_output = output[domain]
       domain_status = domain_output["status"]
```

Answer: C

QUESTION 6
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

QUESTION 7
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

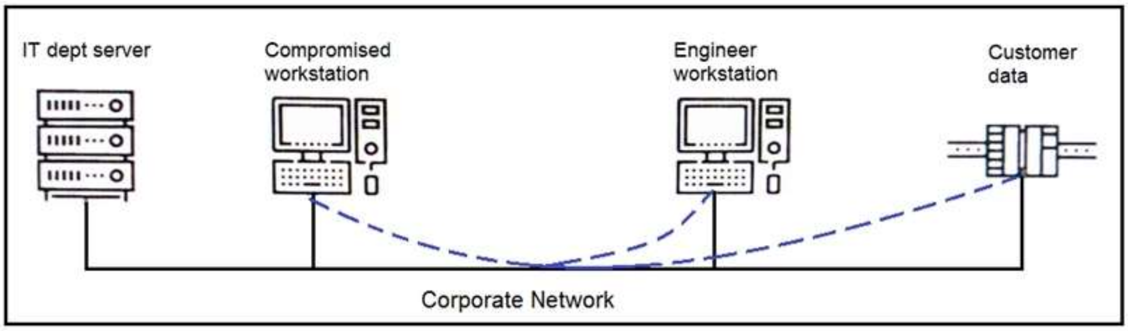
Answer: D

QUESTION 8
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

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

QUESTION 10
How does Wireshark decrypt TLS network traffic?

A. with a key log file using per-session secrets
B. using an RSA public key
C. by observing DH key exchange
D. by defining a user-specified decode-as

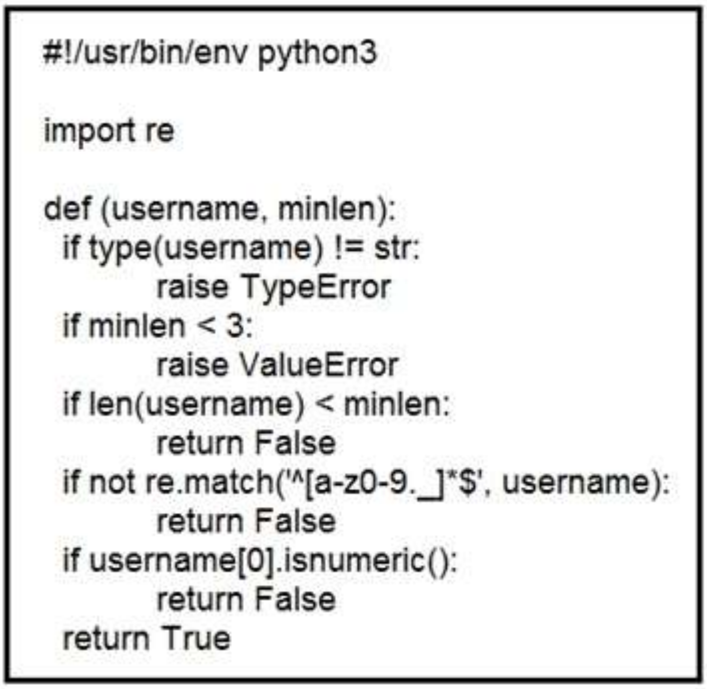
Answer: A
Explanation:
https://wiki.wireshark.org/TLS

QUESTION 11
Refer to the exhibit. 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?



```
#!/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
```

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

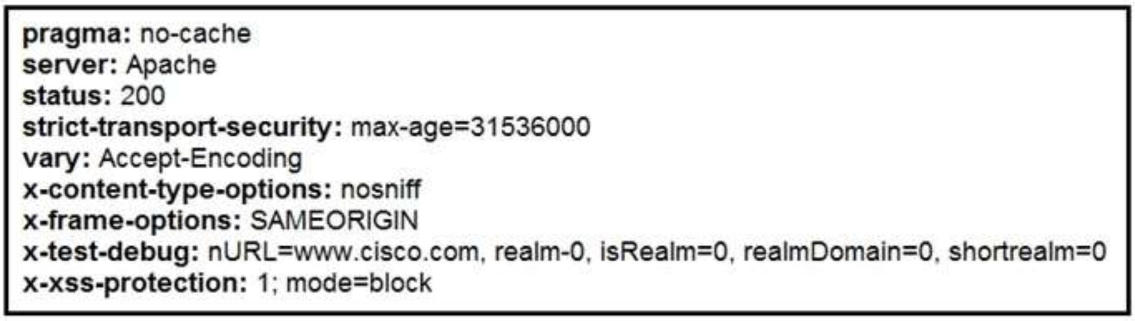
QUESTION 12
An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate 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

QUESTION 13

Refer to the exhibit. Where does it signify that a page will be stopped from loading when a scripting attack is detected?



```
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
```

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

Answer: C
Explanation:
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs

QUESTION 14
What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

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

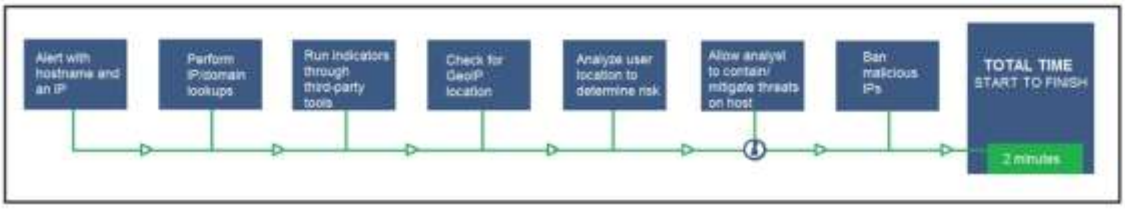
Answer: A

QUESTION 15
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

QUESTION 16
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?


Alert with hostname and an IP
Perform IP/domain lookups
Run indicators through third-party tools
Check for GeoIP location
Analyze user location to determine risk
Allow analyst to contain/ mitigate threats on host
Ban malicious IPs
TOTAL TIME START TO FINISH
2 minutes

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

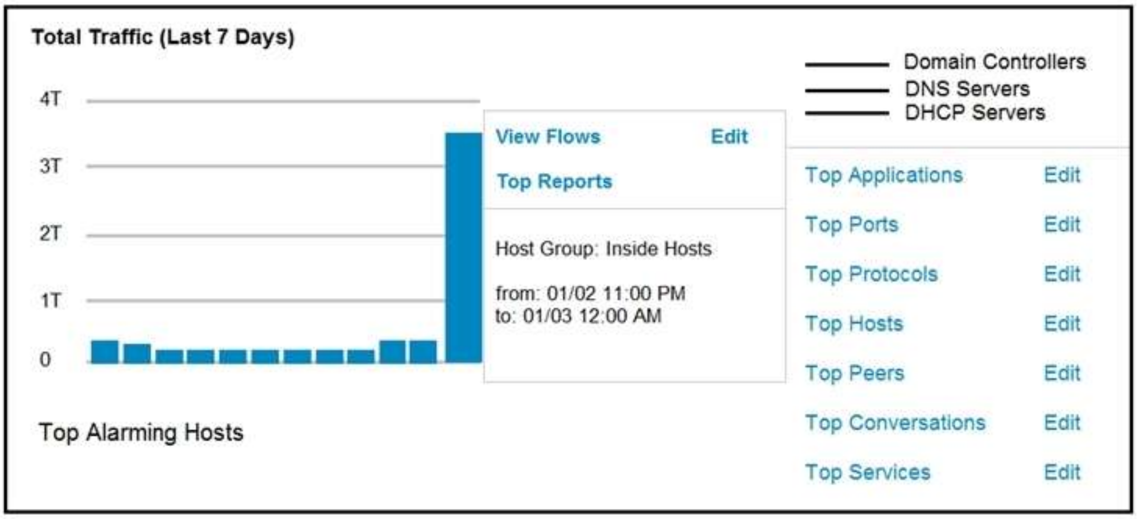
Answer: A

QUESTION 17
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

QUESTION 18
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?



Host Group: Inside Hosts

from: 01/02 11:00 PM
to: 01/03 12:00 AM

A. Top Peers
B. Top Hosts
C. Top Conversations
D. Top Ports

Answer: B
Explanation:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKSEC-3014.pdf

QUESTION 19
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

QUESTION 20
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
Explanation:
https://www.redhat.com/sysadmin/exit-codes-demystified