

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE



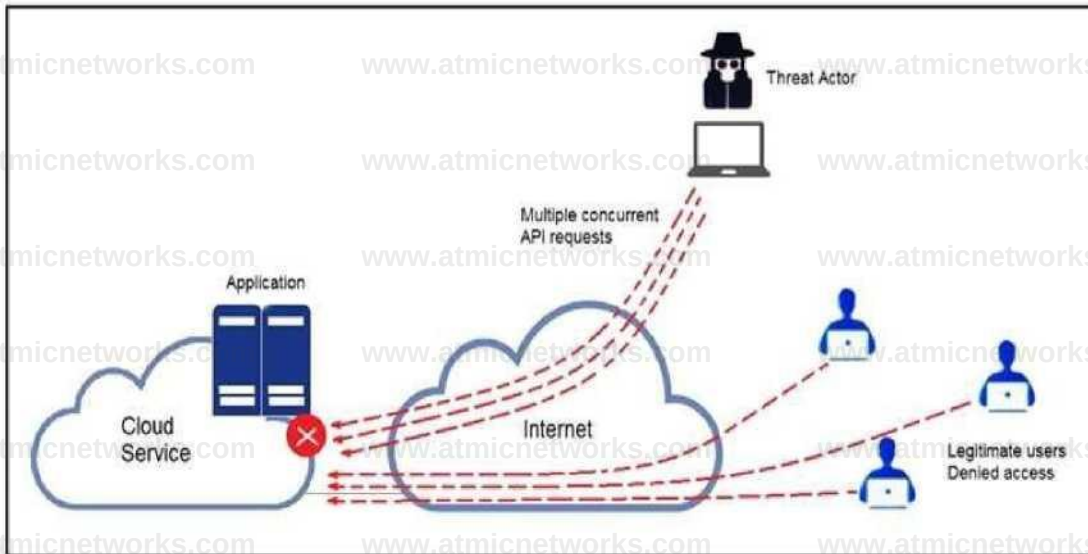
Please note that these files may not be up to date.
However, the questions will help you understand the exam format and typical question patterns.



Stay connected with our support team
for the latest file updates and exam-related information.

Question: 1

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

Question: 3

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

Question: 4

Refer to the exhibit.

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-lin-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto: http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a 2 3-40-191-15: https	CLOSE WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-195: https	TIME WAIT
TCP	192.168.1.8:55947	stackoverflow: https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241 80:https	TIME WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server1:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

- A. packet sniffer
- B. malware analysis
- C. SIEM
- D. firewall manager

Answer: A

Question: 5

Refer to the exhibit.

Analysis Report

ID	12cbee21b1ea4	Filename	fpzryrf.exe
OS	76011 B98.ama64fre.wln7sp1	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	gdr 150316-1654 7/29/1618:44 43	Analyzed As	ult
		SHA256	e9ca08a3cc2f8c9748a9e9b304c9Sal60830066e5467d3dd5927

Ended	7/29/16 18:50:39		be36fec47da
Duration	0:05:56		a2de85810M5ebcf29c5da5dd29ce03470772ad
Sandbox	phl-work-02 (pilot-d)	SHA1 MD5	0d07d778edf8d581 ftaadb 1610aaaOOS

Warnings

0 Executable Failed Integrity Check

Behavioral Indicators

0 CTB Locker Detected	Severity: 100	Confidence: 100
0 Generic Ransomware Detected	Severity: 100	Confidence: 95
0 Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100
0 Process Modified a File in a System Directory	Severity: 90	Confidence: 100
0 Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80
©Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
0	Severity: 70	Confidence: 100
0	Severity: 60	Confidence: 100
0 Process Modified File in a User Directory	Severity: 70	Confidence: 80
©Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80
©Hook Procedure Detected in Executable	Severity: 35	Confidence: 40
©Ransomware 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 has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

- A. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores do not indicate the likelihood of malicious ransomware.
- B. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores are high and do not indicate the likelihood of malicious ransomware.
- C. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are high and indicate the likelihood that malicious ransomware has been detected.
- D. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Answer: C

Question: 6

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

Question: 7

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

- A. incident response playbooks
- B. asset vulnerability assessment
- C. report of staff members with asset relations
- D. key assets and executives
- E. malware analysis report

Answer: BE

Reference: <https://cloudogre.com/risk-assessment/>

Question: 8

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

Reference: <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf>

Question: 9

Vulnerability H

A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:

- a) Be logged in to the device over telnet or SSH, or through the focal console
- b) Be logged in as a high-privileges administrative user

In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.

All software versions are affected Fixes are available now There are no workarounds or mitigations

Vulnerability B

A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:

- a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device

The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.

All software versions are affected

There are no fixes available now

Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.

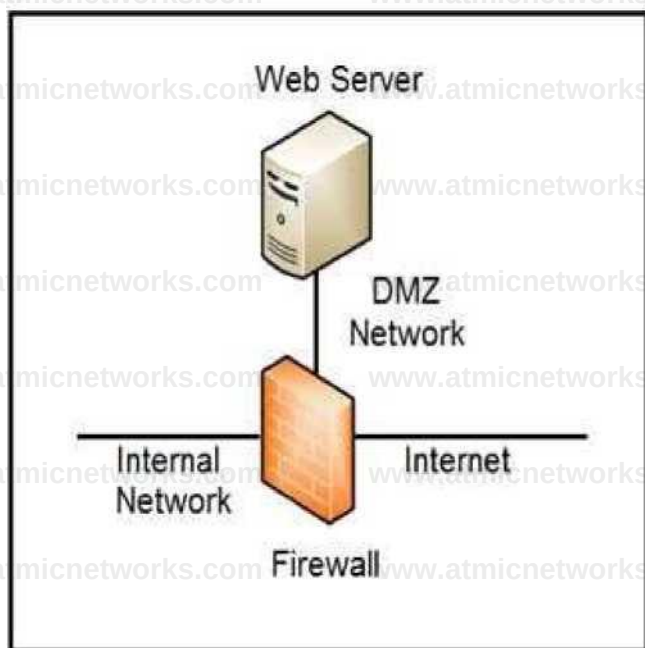
How must these advisories be prioritized for handling?

- A. The highest priority for handling depends on the type of institution deploying the devices
- B. Vulnerability #2 is the highest priority for every type of institution
- C. Vulnerability #1 and vulnerability #2 have the same priority
- D. Vulnerability #1 is the highest priority for every type of institution

Answer: D

Question: 10

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

Question: 11

DRAG DROP

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 previously 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

Answer:

Answer Area

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

Question: 12

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

Reference:

https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

Question: 13

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

Question: 14

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

Question: 15

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

Question: 16

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

Reference: <https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/>

Question: 17

An organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

- A. Host a discovery meeting and define configuration and policy updates
- B. Update the IDS/IPS signatures and reimage the affected hosts
- C. Identify the systems that have been affected and tools used to detect the attack
- D. Identify the traffic with data capture using Wireshark and review email filters

Answer: C

Question: 18

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

Question: 19

The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

- A. Conduct a risk assessment of systems and applications
- B. Isolate the infected host from the rest of the subnet
- C. Install malware prevention software on the host
- D. Analyze network traffic on the host's subnet

Answer: B

Question: 20

DRAG DROP

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

Answer:

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

Question: 21

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

Reference: <https://insights.principa.co.za/4-types-of-data-analytics-descriptive-diagnostic-predictive-prescriptive>

Question: 22

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

Question: 23

Refer to the exhibit.

Analysis Report			
io os	lzetw2ibie@4 Windows 7 64-bit	Filename ee482400446236cb315ad7ed035bd77ad4014039ec9bfebcb8f2 eml Magic Type SMTP mail. ASCII text Analyzed As eml	
started	10/13/20 06 22 43	SHA25S ee482400446236cb3f5ad7ed035bd77add40140058b6d0e6ffe639	
Ended	10/13/20 06 29 19	ec9bfebcb8f2	
Duration	0 06 36	SHA1 d700bca5b65aaf0c613d702d9a28a6084692224	
Sandbox	rcn-work-042 (pilot-d)	MD5 58d1163715089192a8177a5244b9658f	
Behavioral Indicators			
O Email References Localhost in Received Message Trace		severity: 40	confidence:
O Document Contains Embedded Material and		Severity: 50	Confidence: 80
O Download Forced Open/Save Prompt		Severity: 50	Confidence: 75
O Email With Different Sender and Return-Path		Severity: 60	Confidence: 60
O Process Users Very Large Command-Line		Severity: 40	Confidence: 80
O File Downloaded to Disk		Severity: 30	Confidence: 90
O Potential Code Injection Detected		Severity: 50	Confidence: 50
O HTTP Client Error Response		Severity: 50	Confidence: 50
O Sample Communicates With Only Benign Domains		Severity: 20	Confidence: 95
O Executable with Encrypted Sections		Severity: 30	Confidence: 30
O Outbound Communications to Nginx Web Server		Severity: 25	Confidence: 25
O Outbound HTTP POST Communications		Severity: 25	Confidence: 25
O Document Queried Domain		Severity: 25	Confidence: 25
O Executable Imported the IsDebuggerPresent		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

Question: 24

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

Question: 25

DRAG DROP

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Answer Area

Eradicate	Analyze and document the breach, and strengthen systems against future attacks
Contain	Conduct incident response role training for employees
Post-Incident Handling	Determine where the breach started and prevent the attack from spreading
Recover	Determine how the breach was discovered and the areas that were impacted
Analyze	Eliminate the root cause of the breach and apply updates to the system
Prepare	Get systems and business operations up and running, and ensure that the same type of attack does not occur again

Answer:

Answer Area



Reference:

<https://www.securitymetrics.com/blog/6-phases-incident-response-plan>

Question: 26

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

Reference: <https://www.pluralsight.com/blog/it-ops/linux-file-permissions>

Question: 27

A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network.

What is the next step in handling the incident?

- A. Block the source IP from the firewall
- B. Perform an antivirus scan on the laptop
- C. Identify systems or services at risk
- D. Identify lateral movement

Answer: C

Question: 28

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

Question: 29

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

Question: 30

Refer to the exhibit.

```

def map JoJowercase Jetter(s):
    return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map JoJowercase Jetter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = mapjoJowercaseJetter(dl[0] + dl[2] -1) dl[3] = map
    JoJowercase Jetter(dl[1] + dl[2] + dl[3]) return ".join([chr(x)
    for x in dl])
def isBanjoriTail(seed):
    for cO in xrange(97,123):
        for d in xrange(97,123):
            for c2 in xrange(97,123):
                for c3 in xrange(97,123):
                    domain = chr(cO)+chr(d)+chr(c2)+chr(c3) domain =
                    next_domain(domain) if seed.startswith(domain):
                        return False
    return True
seeds = {
    "nhcisatformalisticirekb.com",
    "eg fesatfo rm a l isti c i rekb c o m",
    "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

Question: 31

DRAG DROP

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	installing network devices
broken authentication attack	developing new code
injection attack	implementing a new application
man-in-the-middle attack	changing configuration settings
privilege escalation attack	
default credential attack	

Answer:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
injection attack	privilege escalation attack
man-in-the-middle attack	default credential attack
privilege escalation attack	
default credential attack	

Question: 32

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

Question: 33

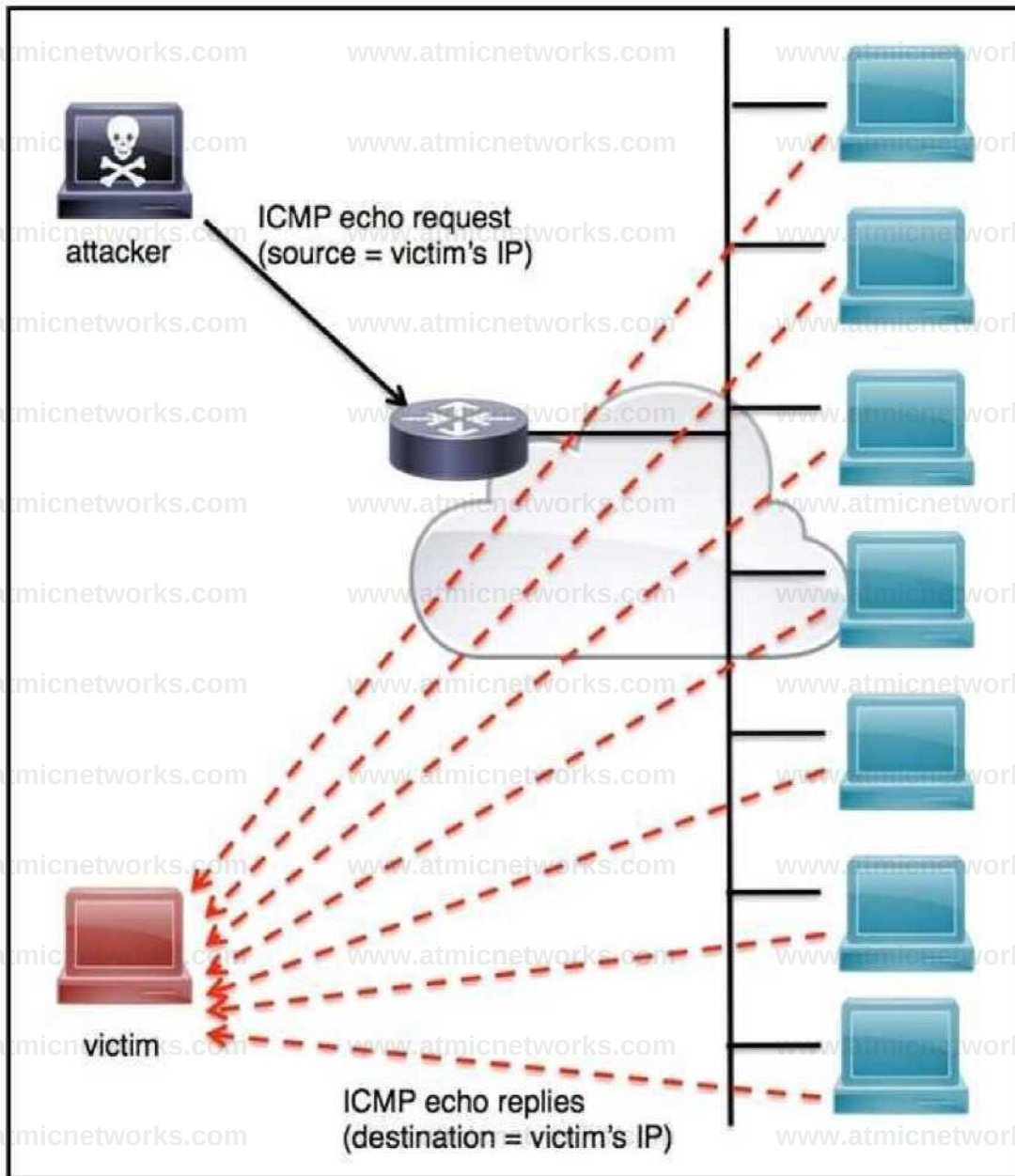
The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident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

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

Answer: D

Question: 34

Refer to the exhibit.



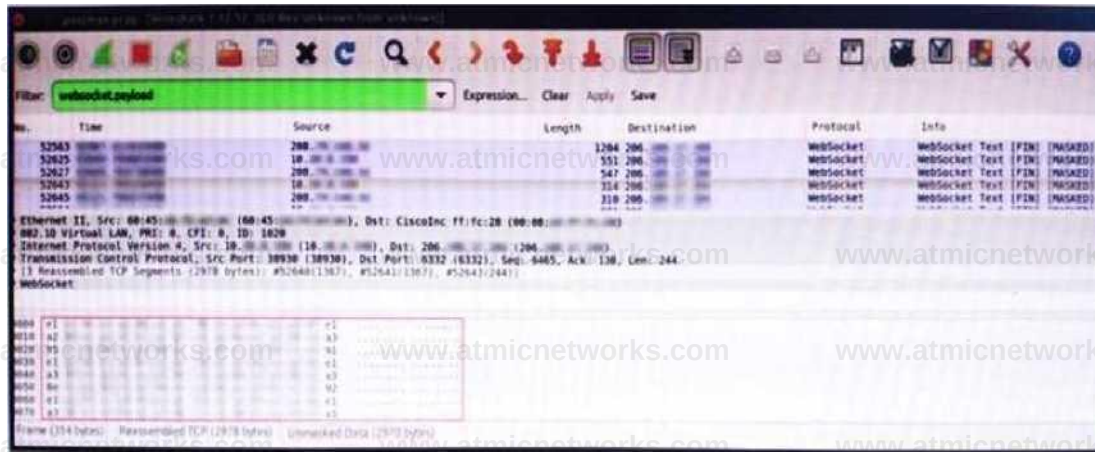
An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action 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

Reference: <https://www.ccexpert.us/pix-firewall/ip-verify-reversepath-command.html>

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

Question: 36

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

Reference:

<https://restfulapi.net/http-status-codes/#:~:text=HTTP%20defines%20these%20standard%20status,results%20of%20a%20client%27s%20request.&text=2xx%3A%20Success%20-%20Indicates%20that%20the,order%20to%20complete%20their%20request.>

Question: 37

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: 38

Refer to the exhibit.

```
def get_umbrella_dispps(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 Mtime)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})
```

Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

A- for domain in domains!]:

```
domain_status = domain_output("status")
```

while domain in domains:

```
domain_status = domain_output("status")
```

C for domain in domains:

```
domainoutput = output(domain)
domain_status = domain_output("status")
```

D- while domains in domains:

```
domain_output = output[domain] domainstatus =
domain_output("status")
```

- A. Option A
- B. Option B
- C. Option C

D. Option D

Answer: C

Question: 39

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: 40

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: 41

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: 42

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

Question: 43

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?

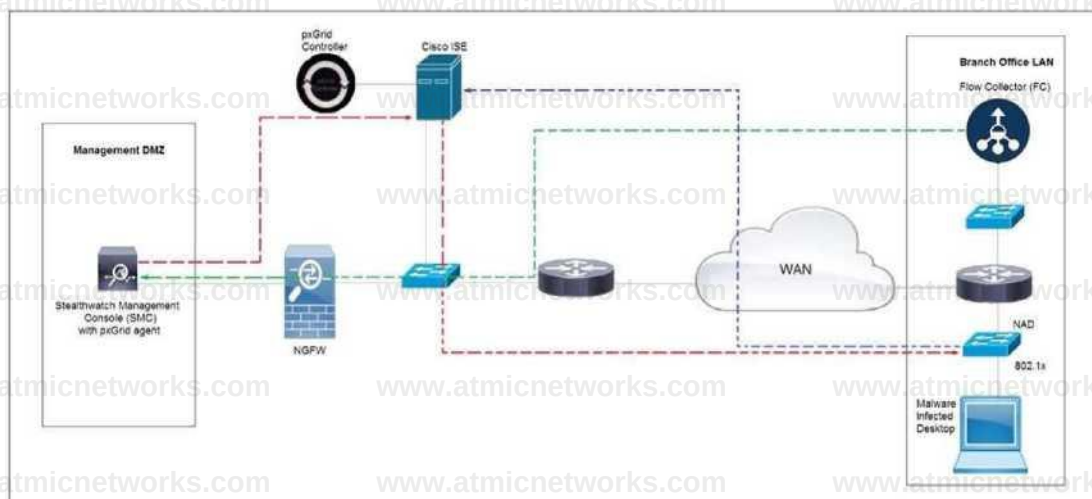
- A. Get-EventLog -LogName*
- B. Get-EventLog -List
- C. Get-WinEvent -ListLog* -ComputerName localhost
- D. Get-WinEvent -ListLog*

Answer: A

Reference: <https://lists.xymon.com/archive/2019-March/046125.html>

Question: 44

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

Question: 45

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

Reference: <https://www.endpointprotector.com/blog/what-is-data-loss-prevention-dlp/>

Question: 46

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

Question: 47

A security expert is investigating a breach that resulted in a \$32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

- A. use of the Nmap tool to identify the vulnerability when the new code was deployed
- B. implementation of a firewall and intrusion detection system
- C. implementation of an endpoint protection system
- D. use of SecDevOps to detect the vulnerability during development

Answer: D

Reference: <https://securityintelligence.com/how-to-prioritize-security-vulnerabilities-in-secdevops/>

Question: 48

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 averages. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
- B. Implement REST API Security Essentials solution to automatically mitigate limit exhaustion. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
- C. Increase a limit of replies in a given interval for each API. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
- D. Apply a limit to the number of requests in a given time interval for each API. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

Reference: <https://www.whoishostingthis.com/resources/http-status-codes/>

Question: 49

Refer to the exhibit.

```
alert tcp SETERNAL.NET any -> SHOME.NET 143 (msg:"PR0T0C0L- 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/T 1110;  
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

Question: 50

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

Question: 51

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

Reference:

https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20201231%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20201231T141156Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

Algorithm=AWS4-HMAC-SHA256&X-Amz-

Credential=AKIAIXACIED2SPMSC7GA

%2F20201231%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20201231T141156Z&X-Amz-

Expires=172800&X-Amz-SignedHeaders=host&X-Amz-

Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

Question: 52

DRAG DROP

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

Answer Area

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

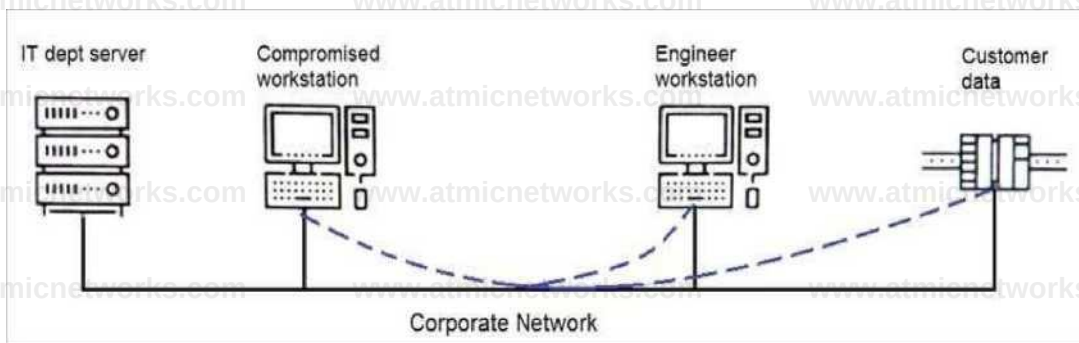
Answer:

Answer Area

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

Question: 53

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: 54

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

Reference: <https://wiki.wireshark.org/TLS>

Question: 55

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

Question: 56

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: 57

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: n<JRL=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

Reference: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs>

Question: 58

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

Reference: <https://airbrake.io/blog/http-errors/401-unauthorized-error#:~:text=The%20401%20Unauthorized%20Error%20is,client%20could%20not%20be%20authenticated.>

Question: 59

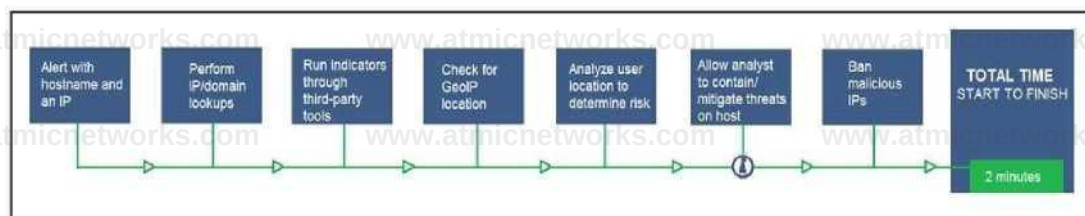
What is a principle of Infrastructure as Code?

- 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: 60

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

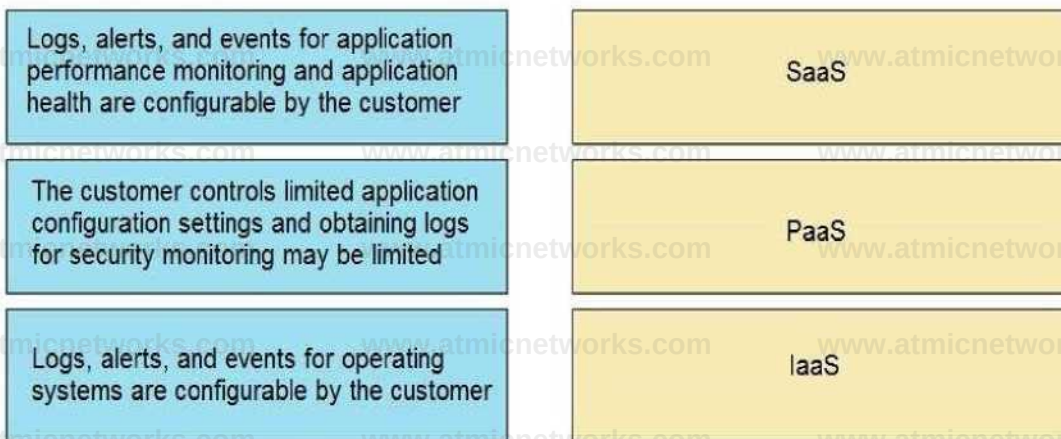
Answer: A

Question: 61

DRAG DROP

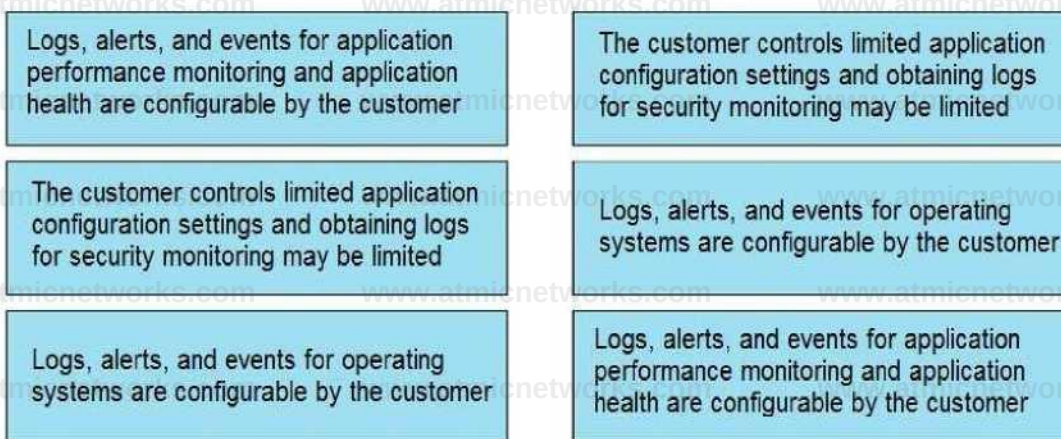
Drag and drop the telemetry-related considerations from the left onto their cloud service models on the right.

Answer Area



Answer:

Answer Area



Question: 62

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

Question: 63

DRAG DROP

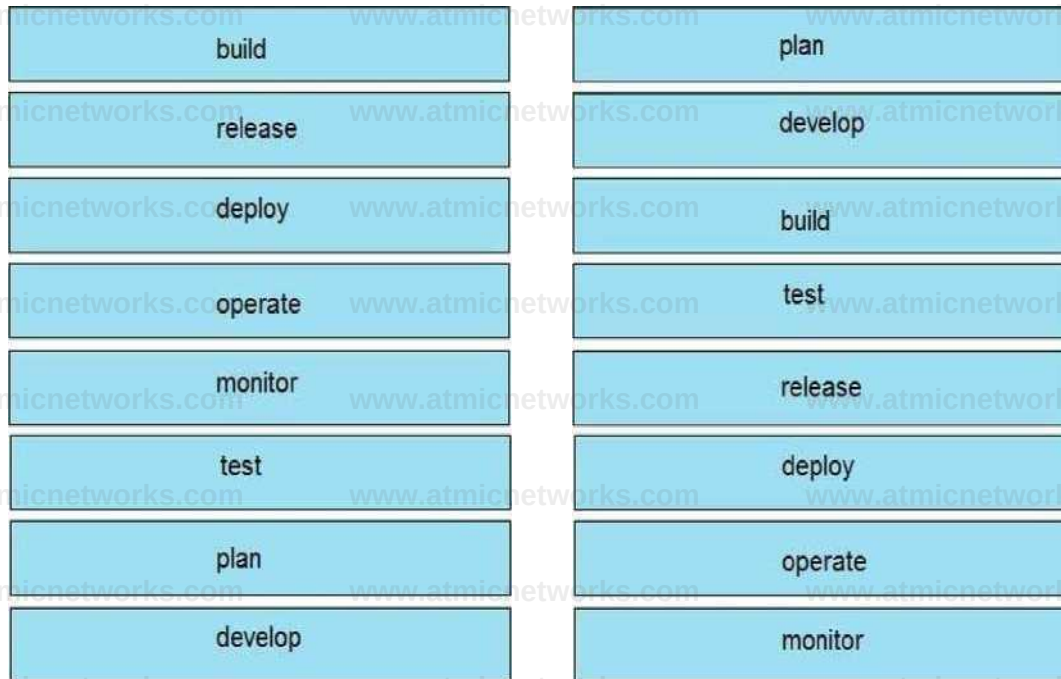
Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

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

Answer:

Answer Area



Reference:

<https://www.densify.com/resources/continuous-integration-delivery-phases>

Question: 64

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

Question: 65

How is a SIEM tool used?

- A. To collect security data from authentication failures and cyber attacks and forward it for analysis

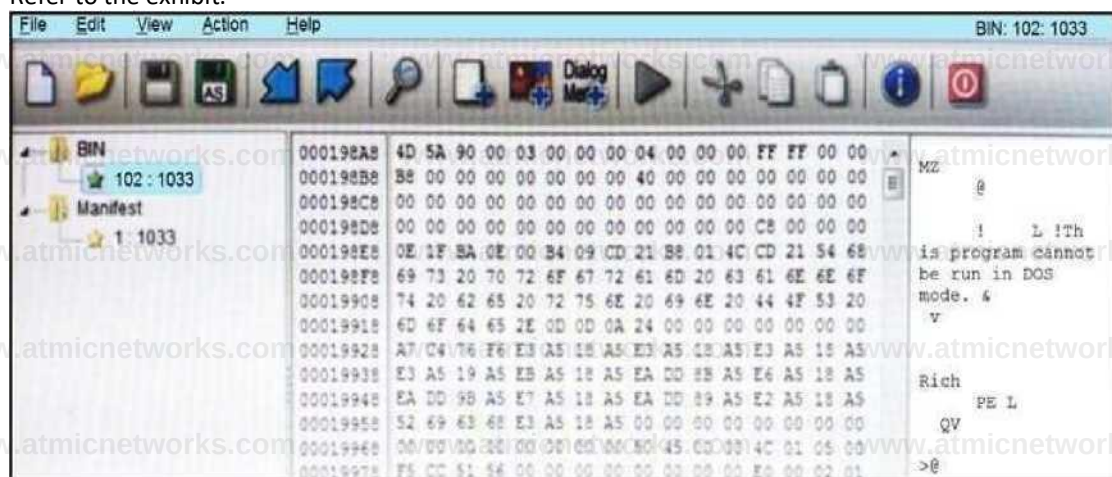
- B. To search and compare security data against acceptance standards and generate reports for analysis
- C. To compare security alerts against configured scenarios and trigger system responses
- D. To collect and analyze security data from network devices and servers and produce alerts

Answer: D

Reference: <https://www.varonis.com/blog/what-is-siem/>

Question: 66

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

Reference: <https://stackoverflow.com/QUESTION> NO:s/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-

files#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.&text=This%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

Question: 67

Refer to the exhibit.

```
using (MemoryStream memoryStream = new MemoryStream())
{
    memoryStream.Position = 32L;
    using (AesCryptoServiceProvider aesCryptoServicePrayWer = new AesCryptoServiceProvider())
    {
        aesCryptoServiceProvider KeySize = 128;
        aesCryptoServiceProvider BlockSize = 128;
        aesCryptoServiceProvider Mode = CipherMode.CBC;
    }
}
```

```

aesCryptoServiceProvider Padding = PaddingMode PKCS7;
aesCryptoServiceProvider Key = key;
aesCryptoServiceProvider C > ieractIV();
using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aesCryptoServiceProvider * i<ti- u /i;inr(X CryptoStreamMode. '-)) {
memoryStream Write(aesCryptoServicePvider.IV, 0, aesCryptoServicePvider.IV.Length);
cryptoStream Write(input, 0, input.Length);
cryptoStream.FlushFinalBlock();
Lisina (HMACSHA256 hmacSHA = new HMACSHA256(bytes))

byte[] array = hmacSHA.Lnn j' b; h?sh(memoryStreamJoArr i^ 32, memoryStreamJoArray().Length - 32);
memoryStream.Position = OL;
memoryStream.Write(array, 0, array.Length);

```

```

    }
    &&it= memOTySteam.TaAffayO;
}
} catch
}

```

An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

- A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.
- B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.
- C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.
- D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Answer: B

Question: 68

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

Reference: <https://upserve.com/restaurant-insider/restaurant-pos-pci-compliance-checklist/>

Question: 69

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

Reference: <https://nvd.nist.gov/vuln/detail/CVE-2018-0161>

Question: 70

DRAG DROP

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

Answer:

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

Question: 71

Refer to the exhibit.

```

"type": "bundle",
"id": "bundle-56be2a39",
"objects": (
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator-81f36b9-9f",
  "created": "2020-08-10T13:49:37.079Z",
  "modified": "2020-08-10T13:49:37.079Z",
  "name": "Malicious site hosting downloader",
  "indicator_types": [
    "malicious-activity"
  ],
  "pattern": "(url:value = 'http:7y2z7atc.cn/4823')",
  "pattern_type": "stix",
  "valid_from": "2020-08-10T13:49:37.079Z"
}

```

```

"type": "malware",
"spec_version": "2.1",
"id": "malware-16209a",
"created": "2020-08-13T09:15:17.182Z",
"modified": "2020-08-13T09:15:17.182Z",
"name": "7y2z7atc backdoor",
"malware_types": [
  "backdoor",
  "remote-access-trojan"
]

```

```

"is_family": false,
"kill_chain_phases": [
  {
    "kill_chain_name": "mandant-attack-lifecycle-model",
    "phase_name": "establish-foothold"
  }
]

```

```

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

```

Which indicator of compromise is represented by this STIX?

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

Answer: C

Question: 72

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
2389	848.622259	10.31.133.235	10.25.129.5	TCP	66	61118 → 80 [SYN, Seq=0 Win=8192
2389	848.622273	10.25.129.5	10.31.133.235	TCP	66	80 → 61118 [SYN, ACK] Seq=0 Ac...
2389	848.622351	10.31.133.235	10.25.129.5	TCP	60	30745 → 80 [RST] Seq=1 Win=0 L...
2389	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0 L...
2389	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0 L...
2389	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0 L...
2389	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0 L...
2389	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0 L...
2389	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0 L...
2389	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0 L...
2389	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0 L...
2389	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0 L...
2389	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0 L...
2389	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0 L...

What is occurring in this packet capture?

- A. TCP port scan
- B. TCP flood
- C. DNS flood
- D. DNS tunneling

Answer: B

Question: 73

DRAG DROP

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

allows renting full servers or virtual machines

focuses on developing, testing, and delivering applications

allows hosting and managing a virtual environment

SaaS

PaaS

IaaS

FaaS

Answer Area

Answer:

triggers a block of code when triggered by a specific event

allows renting full servers or virtual machines

focuses on developing, testing, and delivering applications

allows hosting and managing a virtual environment

focuses on developing, testing, and delivering applications

allows hosting and managing a virtual environment

allows renting full servers or virtual machines

triggers a block of code when triggered by a specific event

Question: 74

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341->80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80->3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	54	80->3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342->80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80->3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80->3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343->80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80->3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80->3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	58	3344->80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80->3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80->3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80->3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)

Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2

Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0

Source port: 3341

Destination port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 1023350804

0101 ... = Header Length: 20 bytes (5)

Flags: 0x002 [SYN]

Window size value: 512

[Calculated window size: 512]

Checksum: 0x8d5a [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[Timestamps]

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

Question: 75

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

Question: 76

What is a benefit of key risk indicators?

- A. clear perspective into the risk position of an organization
- B. improved visibility on quantifiable information
- C. improved mitigation techniques for unknown threats
- D. clear procedures and processes for organizational risk

Answer: C

Reference: [https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20\(ERM\)-,Overview,and%20mitigate%20them%20in%20time.](https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.)

Question: 77

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: 78

Refer to the exhibit.

Total Traffic (Last 7 Days)



Domain Controllers
DNS Servers
DHCP Servers

Top Applications Edit

Top Ports Edit

Top Protocols Edit

Top Hosts Edit

Top Peers Edit

Top Conversations Edit

Top Services Edit

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

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKSEC-3014.pdf>

Question: 79

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: 80

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

Reference: <https://www.redhat.com/sysadmin/exit-codes-demystified>

Question: 81

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

- A. phishing
- B. dumpster diving

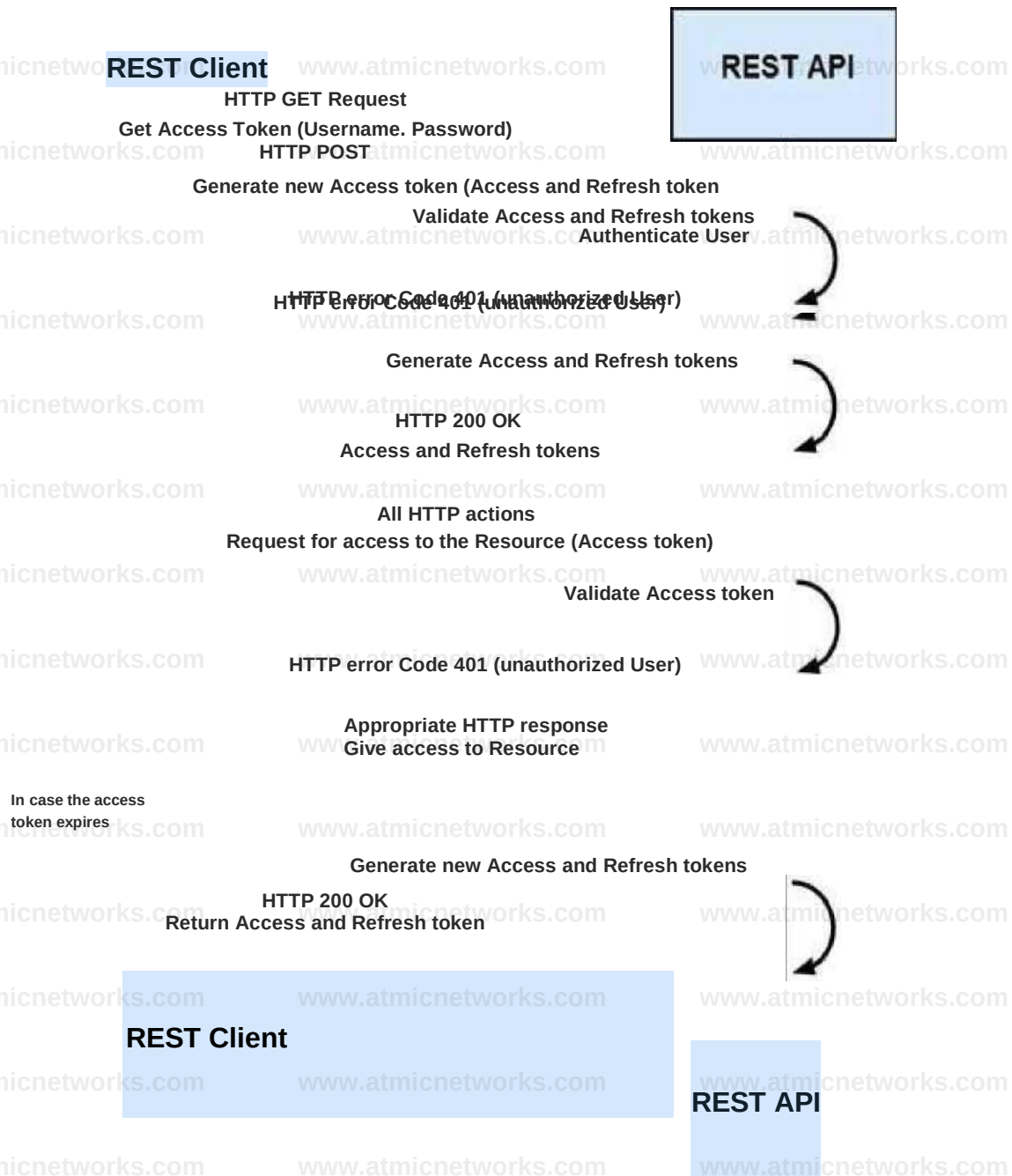
- C. social engineering
- D. privilege escalation

Answer: C

Question: 82

Refer to the exhibit.

Token-Based Authentication



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

- The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.
- The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.
- The token is obtained before providing a password. The REST API provides resource access, refreshes tokens, and returns them to the REST client. The REST client requests access to a resource using the access token.
- The token is obtained before providing a password. The REST client provides access to a resource using the

access token. The REST API encrypts the access token and gives access to the resource.

Answer: D

Question: 83

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=ww. 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

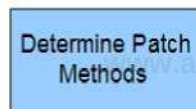
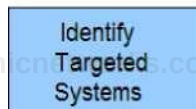
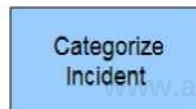
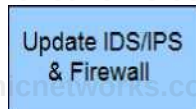
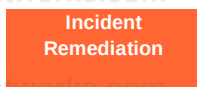
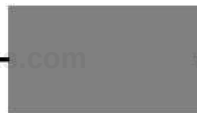
Answer: C

Reference: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

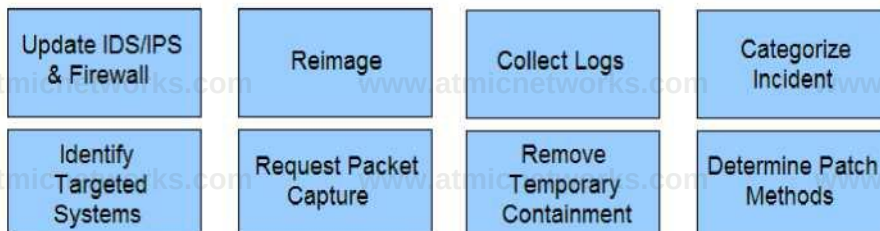
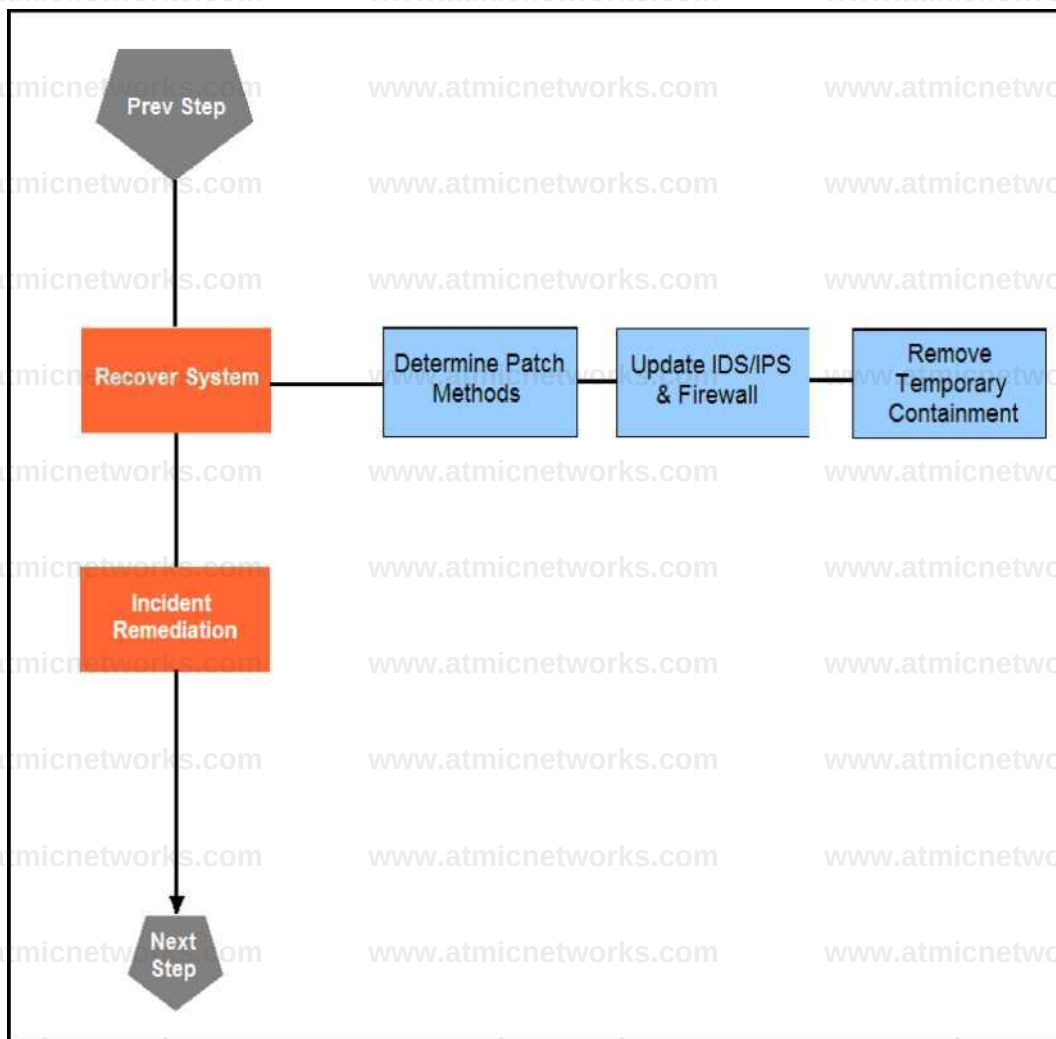
Question: 84

DRAG DROP

Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



Answer:



Question: 85

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

Question: 86

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

Reference: <https://tplinsurance.com/products/cyber-risk-insurance/>

Question: 87

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

Question: 88

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

Question: 89

DRAG DROP

Drag and drop the function on the left onto the mechanism on the right.

Answer Area

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

Answer:

Answer Area

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

Question: 90

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

Reference: <https://eclcticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/>

Question: 91

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

Question: 92

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

Question: 93

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

An employee is a victim of a social engineering phone call and installs remote access software to

allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted

database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee's laptop and the remote technician's system?

- A. No database files were disclosed
- B. The database files were disclosed
- C. The database files integrity was violated
- D. The database files were intentionally corrupted, and encryption is possible

Answer: C

Question: 94

Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters - Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

- A. servers
- B. website
- C. payment process
- D. secretary workstation

Answer: C

Question: 95

DRAG DROP

Refer to the exhibit.

ih'<h> Stealthwatch

tiKo, total v

CISCO

Dashboards Monitor Analyze Jots Configure Deploy

Hosts

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

1Last

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

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Step 1

Step 2

Step 3

Step 4

Step 5

Answer:

Answer Area

Execute rapid threat containment

Investigate and classify the exposure

Investigate infected hosts

Search for infected hosts

Examine returned results

Search for infected hosts

Investigate infected hosts

Investigate and classify the exposure

Examine returned results

Execute rapid threat containment

Question: 96
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

Question: 97

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

Question: 98

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

Question: 99

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

- A. web security solution
- B. email security solution

- C. endpoint security solution
- D. network security solution

Answer: D

Question: 100

Refer to the exhibit.



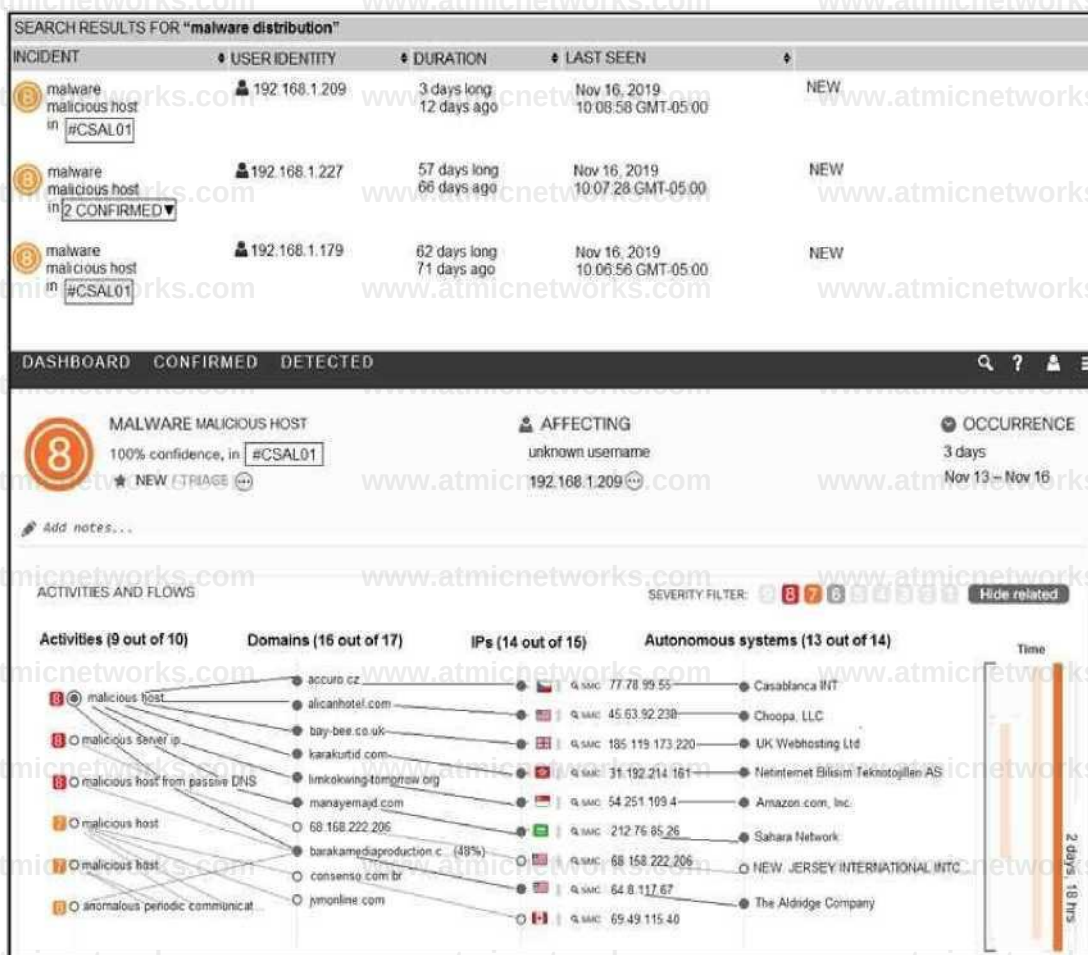
An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the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

Question: 101

Refer to the exhibit.



For IP 192.168.1.209, what are the risk level, activity, and next step?

- A. high risk level, anomalous periodic communication, quarantine with antivirus
- B. critical risk level, malicious server IP, run in a sandboxed environment
- C. critical risk level, data exfiltration, isolate the device
- D. high risk level, malicious host, investigate further

Answer: A

Question: 102

Refer to the exhibit.

Distribution Port/CI,IP *	Message *	Classification x	Application Protocol *	Client x	Application Risk*	Business # Relevance	Access Control Rule x
80 (http) / tcp	STREAMS_DATA_ON_SYN (129 2 2)	Generic Protocol Decode	Command	ICMP client	Medium	Medium	rule
80 (http)/tcp	STREAMS_DATA_ON_SYN (129 2 2)	Genenc Protocol Command Decode	DNS	DNS client	Very Low	Very High	Default Action
0 (No Code) / icmp	PROTOCOL-ICMP Echo Reply (1 408 8)	Mise Activity	DNS	DNS client	Very Low	Very High	Allow ICMP
uin7/«i	PROTOCOL-DNS TMG Firewall Client long Attempted User	udp host entry exploit attempt (3 19187 7)		Q^S	Very Very		
aoic7 ■	a PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7)	Potential Corporate Policy Violation	DNS	client	Very Low	Very High	Privilege Gain ODNS D client Low High
7	a PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	client	Very Low	Very High	
5/4/7 tudp 1918 192 168/16 address detected (1 15935 7)	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected^ 15935 7)	Potential Corporate Policy Violation	DNS	client	Very Low	Very High	
548/9 udp 1918 192 168/16 address detected^ 15935 7)	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7)	Potential Corporate Policy Violation	DNS	client	Very Low	Very High	
Potential Corporate	DNS						
owiw/uap isj8 192 168/16 address detected (1 15935:7) Poky Violation							
TM .n / an PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7) Poky Violation							
camo, a PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7) Poky Violation							
d PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7) Poky Violation							
168/16 address detecteddd 15935 7) Poky Violation							
response for rtc Potential Corporate _ buios.uop 1918 192 168/16 address detected (1 15935 7) Poky Violation							
Corporate							
uop 1918 192 168/16 address detecteddd 15935 7) Poky Violation							
PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)							
5/485/up isj8 192 168/16 address detected (1 15935 7)							
PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7) Poky Violation							
49940 / udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57214/udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
51608/udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected(1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52652 / udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55528 / udp	PROTOCOL-DNS dns response for rtc 1918 192 168 16 address detecteddd 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
61222/udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55640 / udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detecteddd 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55991 / udp	PROTOCOL-DNS dns response for rtc 1918 192 168/16 address detected (1 15935 7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	

What is the connection status of the ICMP event?

- A. blocked by a configured access policy rule B. allowed by a configured access policy rule C. blocked by an intrusion policy rule D. allowed in the default action

Answer: B

Question: 103

An analyst wants to upload an infected file containing sensitive information to a hybrid-analysis sandbox. According to the NIST.SP 800-150 guide to cyber threat information sharing, what is the analyst required to do before uploading the file to safeguard privacy?

- A. Verify hash integrity.
- B. Remove all personally identifiable information.
- C. Ensure the online sandbox is GDPR compliant.
- D. Lock the file to prevent unauthorized access.

Answer: B

Question: 104

Refer to the exhibit.

Human Interface Device Service . HP System Info	Activates and maintains the use of hot buttons on keyboar...	Running	Manual (Trig...
HSA Service		Running	Automatic
HP Omen HSA Service		Running	Automatic
HP Network HSA Service		Running	Automatic
HP App Helper HSA Service		Running	Automatic
HP Analytics service		Running	Automatic
Group Policy Client	The service is responsible for applying settings configured...		Automatic (T...
GraphicsPerfSvc	Graphics performance monitor service		Manual (Trig...
Google Update Service (gupdatem)	Keeps your Google software up to date. If this service dis...		Manual
Google Update Service (gupdate)	Keeps your Google software up to date. If this service dis...		Automatic {...
Google Chrome Elevation Service (GoogleChro...			Manual
Geolocation Service	This service monitors the current location of the system an...		Disabled
GameDVR and Broadcast User Service_i36cS7	This user service is used for Game Recordings and Live Broa...		Manual
Function Discovery Resource Publication	Publishes this computer and resources attached to this co...	Running	Manual (Trig...
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) net...	Running	Manual
File History Service	Protects user files from accidental loss by copying them to...		Manual (Trig...
Fax	Enables you to send and receive faxes utilising fax rescurc...		Manual
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service ptovi...	Running	Manual
Enterprise App Management Service	Enables enterprise application management.		Manual
Encrypting File System (EFS)	Provides the core file encryption technology used to store...		Manual (Trig...
Embedded Mode	The Embedded Mode service enables scenarios related to B...		Manual (Trig...
FI	Ronfiro	Ronfiro	Antrimatir

An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon – Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?

- A. malware break
- B. data theft
- C. elevation of privileges
- D. denial-of-service

Answer: C

Question: 105

What is needed to assess risk mitigation effectiveness in an organization?

- A. analysis of key performance indicators
- B. compliance with security standards
- C. cost-effectiveness of control measures
- D. updated list of vulnerable systems

Answer: C

Question: 106

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: nllRL=www.cisco.com,realm=0,isRealm=0,realmDomain=0,shortrealm=0 x-xss-protection: 1; mode=block

Where is the MIME type that should be followed indicated?

- A. x-test-debug
- B. strict-transport-security
- C. x-xss-protection
- D. x-content-type-options

Answer: A

Question: 107

Refer to the exhibit.

Severity	Name	Family	Count	evss
Critical	Bash Incomplete Fix Remote Code Execution Vulnerability	Gain a shell remotely	3	10
Critical	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1	10

Critical	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1	7.4
Critical	Rexecd Service Detection	Service detection	1	5.9
High	Mozilla Foundation Unsupported Application	MacOS X Local Security Checks	2	10
High	SMB Signing Disabled	Mise	1	7
Medium	SSL Certificate Cannot Be Trusted	General	1	6.5

Based on the detected vulnerabilities, what is the next recommended mitigation step?

- A. Evaluate service disruption and associated risk before prioritizing patches.
- B. Perform root cause analysis for all detected vulnerabilities.
- C. Remediate all vulnerabilities with descending CVSS score order.
- D. Temporarily shut down unnecessary services until patch deployment ends.

Answer: B

Question: 108

An engineer received an incident ticket of a malware outbreak and used antivirus and malware removal tools to eradicate the threat. The engineer notices that abnormal processes are still occurring in the system and determines that manual intervention is needed to clean the infected host and restore functionality. What is the next step the engineer should take to complete this playbook step?

- A. Scan the network to identify unknown assets and the asset owners.
- B. Analyze the components of the infected hosts and associated business services.
- C. Scan the host with updated signatures and remove temporary containment.
- D. Analyze the impact of the malware and contain the artifacts.

Answer: B

Question: 109

The SIEM tool informs a SOC team of a suspicious file. The team initializes the analysis with an automated sandbox tool, sets up a controlled laboratory to examine the malware specimen, and proceeds with behavioral analysis. What is the next step in the malware analysis process?

- A. Perform static and dynamic code analysis of the specimen.
- B. Unpack the specimen and perform memory forensics.
- C. Contain the subnet in which the suspicious file was found.
- D. Document findings and clean-up the laboratory.

Answer: B

Question: 110

A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

- A. Allow list only authorized hosts to contact the application's IP at a specific port.
- B. Allow list HTTP traffic through the corporate VLANs.
- C. Allow list traffic to application's IP from the internal network at a specific port.
- D. Allow list only authorized hosts to contact the application's VLAN.

Answer: D

Question: 111

A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?

- A. post-authorization by non-issuing entities if there is a documented business justification
- B. by entities that issue the payment cards or that perform support issuing services
- C. post-authorization by non-issuing entities if the data is encrypted and securely stored
- D. by issuers and issuer processors if there is a legitimate reason

Answer: C

Question: 112

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor's website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

- A. Determine if there is internal knowledge of this incident.
- B. Check incoming and outgoing communications to identify spoofed emails.
- C. Disconnect the network from Internet access to stop the phishing threats and regain control.
- D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

Answer: D

Question: 113

An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity.

Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization's service area.

a. What are the next steps the engineer must take?

- A. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.
- B. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.
- C. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in Question 113, and cross-correlate other source events.
- D. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

Answer: A

Question: 114

An organization had an incident with the network availability during which devices unexpectedly malfunctioned. An engineer is investigating the incident and found that the memory pool buffer usage reached a peak before the malfunction. Which action should the engineer take to prevent this issue from reoccurring?

- A. Disable memory limit.
- B. Disable CPU threshold trap toward the SNMP server.
- C. Enable memory tracing notifications.
- D. Enable memory threshold notifications.

Answer: D

Question: 115

A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

- A. Create a follow-up report based on the incident documentation.
- B. Perform a vulnerability assessment to find existing vulnerabilities.
- C. Eradicate malicious software from the infected machines.
- D. Collect evidence and maintain a chain-of-custody during further analysis.

Answer: D

Question: 116

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company's confidential document management folder using a company-owned asset al039-ice-4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

- A. Measure confidentiality level of downloaded documents.
- B. Report to the incident response team.
- C. Escalate to contractor's manager.
- D. Communicate with the contractor to identify the motives.

Answer: B

Question: 117

An engineer detects an intrusion event inside an organization's network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

- A. Disconnect the affected server from the network.
- B. Analyze the source.
- C. Access the affected server to confirm compromised files are encrypted.
- D. Determine the attack surface.

Answer: C

Question: 118

The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

- A. eradication and recovery
- B. post-incident activity
- C. containment
- D. detection and analysis

Answer: A

Question: 119

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

- A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.
- B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.
- C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.
- D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

Answer: D

Question: 120

Which action should be taken when the HTTP response code 301 is received from a web application?

- A. Update the cached header metadata.
- B. Confirm the resource's location.
- C. Increase the allowed user limit.
- D. Modify the session timeout setting.

Answer: A

Question: 121

Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

- A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.
- B. Communicate with employees to determine who opened the link and isolate the affected assets.
- C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.
- D. Review the mail server and proxy logs to identify the impact of a potential breach.
- E. Check the email header to identify the sender and analyze the link in an isolated environment.

Answer: CE

Section: (none)

Explanation

Question: 122

A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross-correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

- A. Disable BIND forwarding from the DNS server to avoid reconnaissance.
- B. Disable affected assets and isolate them for further investigation.
- C. Configure affected devices to disable NETRJS protocol.
- D. Configure affected devices to disable the Finger service.

Answer: D

Question: 123

What is idempotence?

- A. the assurance of system uniformity throughout the whole delivery process
- B. the ability to recover from failures while keeping critical services running
- C. the necessity of setting maintenance of individual deployment environments
- D. the ability to set the target environment configuration regardless of the starting state

Answer: A

Question: 124

A security architect in an automotive factory is working on the Cyber Security Management System and is implementing procedures and creating policies to prevent attacks. Which standard must the architect apply?

- A. IEC62446
- B. IEC62443
- C. IEC62439-3
- D. IEC62439-2

Answer: B

Question: 125

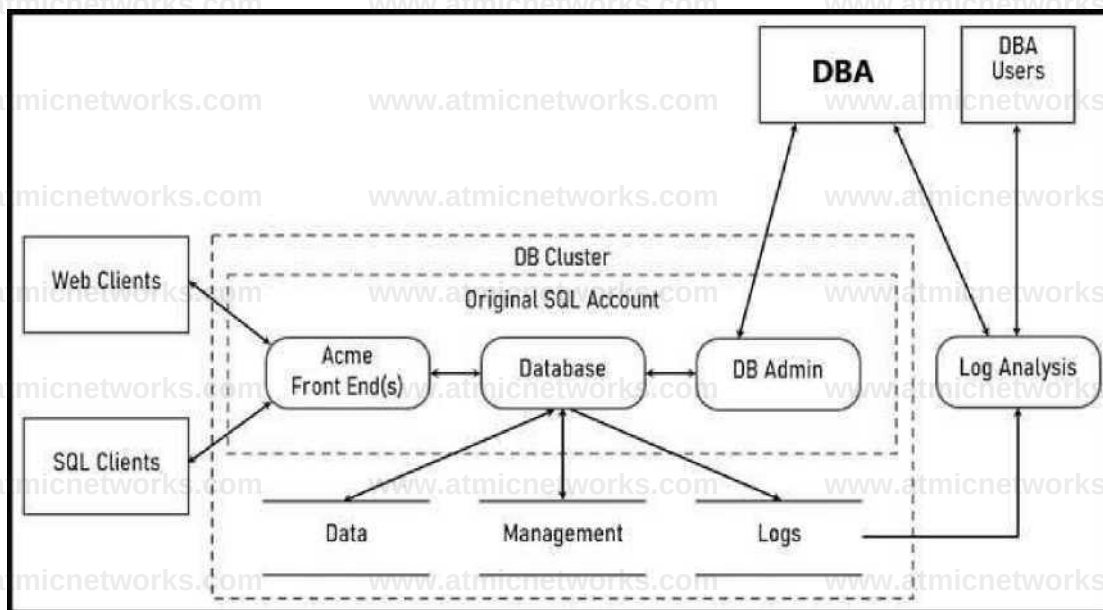
An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)

- A. Implement a patch management process.
- B. Scan the company server files for known viruses.
- C. Apply existing patches to the company servers.
- D. Automate antivirus scans of the company servers.
- E. Define roles and responsibilities in the incident response playbook.

Answer: DE

Question: 126

Refer to the exhibit.



Two types of clients are accessing the front ends and the core database that manages transactions, access control, and atomicity. What is the threat model for the SQL database?

- A. An attacker can initiate a DoS attack.
- B. An attacker can read or change data.
- C. An attacker can transfer data to an external server.
- D. An attacker can modify the access logs.

Answer: A

Question: 127

Which bash command will print all lines from the "colors.txt" file containing the non case-sensitive pattern "Yellow"?

- A. `grep -i "yellow" colors.txt`
- B. `locate "yellow" colors.txt`
- C. `locate -i "Yellow" colors.txt`
- D. `grep "Yellow" colors.txt`

Answer: A

Question: 128

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data.

a. Which type of attack is occurring?

- A. Address Resolution Protocol poisoning
- B. session hijacking attack

- C. teardrop attack
- D. Domain Name System poisoning

Answer: D

Question: 129

Refer to the exhibit.

```
HttpRequest httpRequest = (HttpRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpRequest.Accept = null;
httpRequest.Timeout = 10000;
using (HttpWebResponse httpResponse = (HttpWebResponse)httpRequest.GetResponse())
{
    using (Stream responseStream = httpResponse.GetResponseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDoc = new XmlDocument();
            xmlDoc.LoadXml(xml);
            string innerXml1 = xmlDoc.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDoc.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDoc.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDoc.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDoc.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDoc.SelectSingleNode("Response//TimeZone").InnerXml;
```

An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

- A. The file is redirecting users to a website that requests privilege escalations from the user.
- B. The file is redirecting users to the website that is downloading ransomware to encrypt files.
- C. The file is redirecting users to a website that harvests cookies and stored account information.
- D. The file is redirecting users to a website that is determining users' geographic location.

Answer: D

Question: 130

A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

- A. Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.
- B. Inform the user by enabling an automated email response when the rule is triggered.
- C. Inform the incident response team by enabling an automated email response when the rule is triggered.
- D. Create an automation script for blocking URLs on the firewall when the rule is triggered.

Answer: A

Question: 131

A cloud engineer needs a solution to deploy applications on a cloud without being able to manage and control the server OS. Which type of cloud environment should be used?

- A. IaaS
- B. PaaS
- C. DaaS
- D. SaaS

Answer: A

Question: 132

Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non-secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in this investigation? (Choose two.)

- A. Determine the type of data stored on the affected asset, document the access logs, and engage the incident response team.
- B. Identify who installed the application by reviewing the logs and gather a user access log from the HR department.
- C. Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.
- D. Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.

Answer: AD

Question: 133

A security incident affected an organization's critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

- A. Configure shorter timeout periods.
- B. Determine API rate-limiting requirements.
- C. Implement API key maintenance.
- D. Automate server-side error reporting for customers.

- E. Decrease simultaneous API responses.

Answer: BD

Question: 134

What is the impact of hardening machine images for deployment?

- A. reduces the attack surface
- B. increases the speed of patch deployment
- C. reduces the steps needed to mitigate threats
- D. increases the availability of threat alerts

Answer: A

Question: 135

What is the difference between process orchestration and automation?

- A. Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.
- B. Orchestration arranges the tasks, while automation arranges processes.
- C. Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.
- D. Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Answer: A

Question: 136

An analyst received multiple alerts on the SIEM console of users that are navigating to malicious URLs. The analyst needs to automate the task of receiving alerts and processing the data for further investigations. Three variables are available from the SIEM console to include in an automation script: console_ip, api_token, and reference_set_name. What must be added to this script to receive a successful HTTP response?

```
#!/usr/bin/python import sys import requests
```

- A. {1}, {2}
- B. {1}, {3}
- C. console_ip, api_token
- D. console_ip, reference_set_name

Answer: C

Question: 137

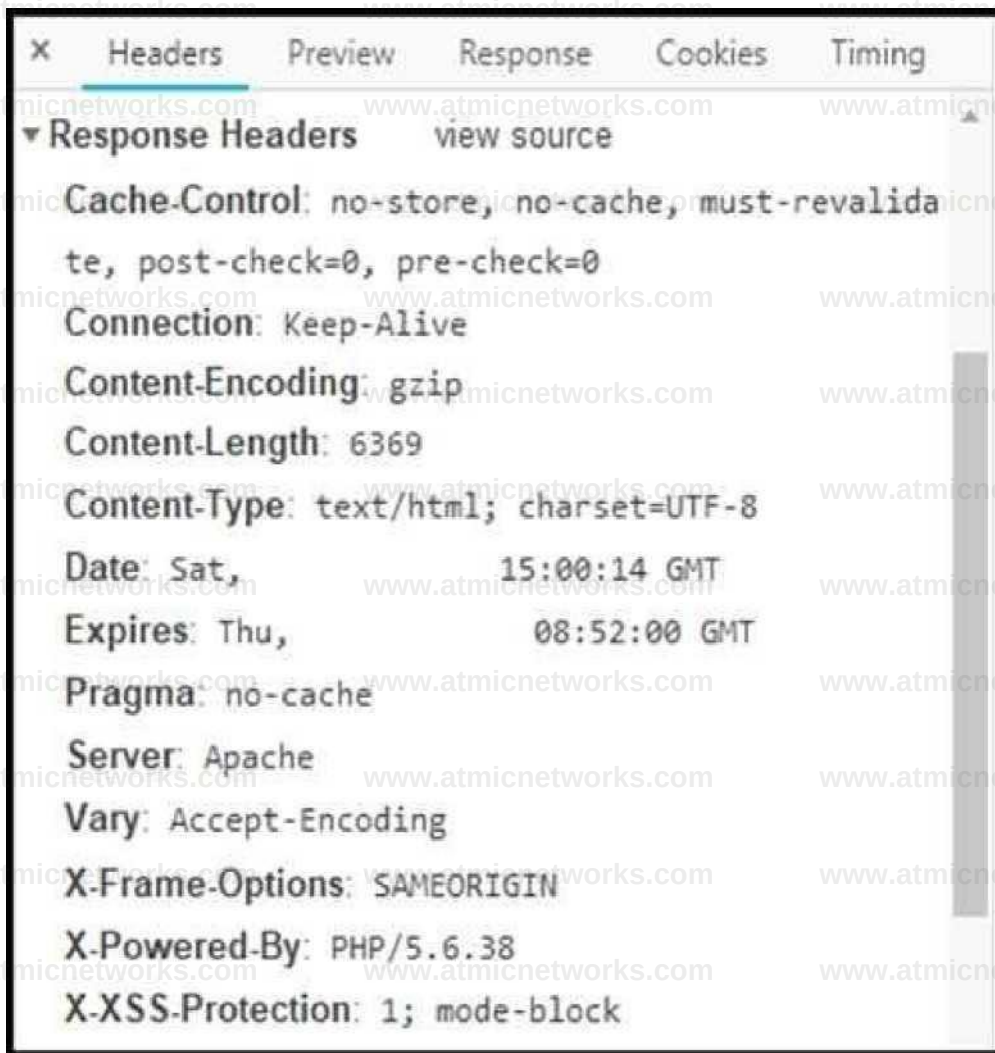
After a recent malware incident, the forensic investigator is gathering details to identify the breach and causes. The investigator has isolated the affected workstation. What is the next step that should be taken in this investigation?

- A. Analyze the applications and services running on the affected workstation.
- B. Compare workstation configuration and asset configuration policy to identify gaps.
- C. Inspect registry entries for recently executed files.
- D. Review audit logs for privilege escalation events.

Answer: C

Question: 138

Refer to the exhibit.



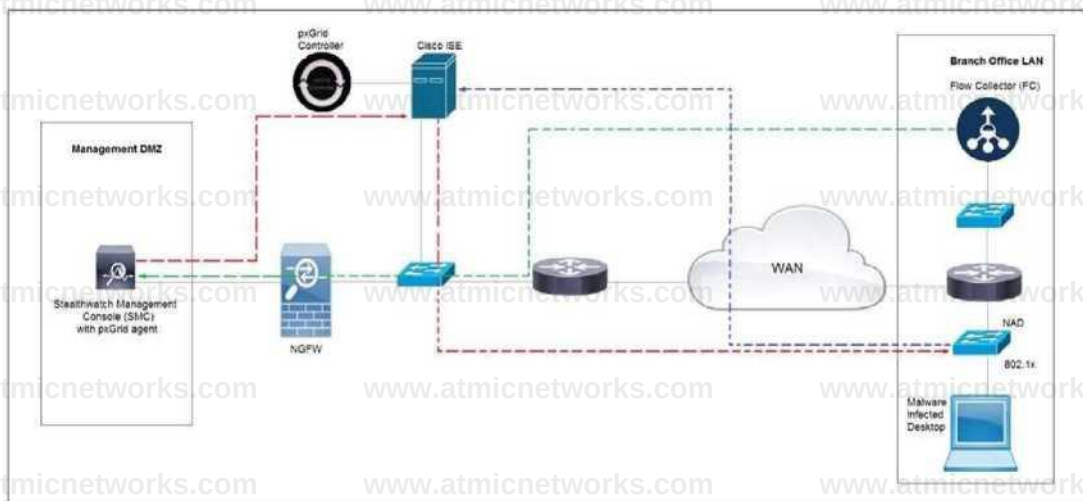
Where are the browser page rendering permissions displayed?

- A. X-Frame-Options
- B. X-XSS-Protection
- C. Content-Type
- D. Cache-Control

Answer: C

Question: 139

Refer to the exhibit.



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 method was used to signal ISE to quarantine the endpoints?

A. SNMP B. syslog C. REST API D. pxGrid

Answer: C