DUMPSBOSS.

Conducting Forensic Analysis and Incident Response Using Cisco CyberOps Technologies (CBRFIR)

Cisco 300-215

Version Demo

Total Demo Questions: 19

Total Premium Questions: 191

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Forensic Analysis	132
Topic 2, Incident Response	57
Topic 3, Mix Questions	2
Total	191

QUESTION NO: 1

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= “Fy.exe”

E. Content-Type: application/octet-stream

ANSWER: C E

Explanation:

The URI-associated value **5f31ab113af08=1597090577** is useful as an indicator because it is a specific, observable artifact from the suspicious HTTP transaction. Analysts can use such a value to search packet captures, proxy logs, web-server logs, and security telemetry for repeat requests associated with the same malicious delivery infrastructure or campaign. The value is substantially more actionable for correlation than ordinary web-server implementation details because it can be matched directly against recorded HTTP request data.

Content-Type: application/octet-stream indicates that the HTTP server is delivering arbitrary binary data rather than a normal document such as HTML or plain text. In the context of the shown Emotet download activity, this response metadata helps identify the transfer of the executable payload and is valuable for network-based detection rules, especially when correlated with the request URI and downloaded file. Wireshark exposes HTTP headers and content types in its protocol dissection, allowing investigators to filter and inspect binary download responses. Cisco incident-response guidance likewise emphasizes collecting and correlating network artifacts to identify malicious file delivery and scope an incident. See the Wireshark User's Guide on display filters and Cisco Incident Response Services.

QUESTION NO: 2

An analyst is investigating a phishing message that impersonates the organization's finance department. Which two email-header fields are most useful for tracing the path the message took to reach the recipient? (Choose two.)

A. Received

B. Return-Path

C. Content-Type

D. Message body font

E. email signature block

ANSWER: A B

Explanation:

Received headers and **Return-Path** are useful fields for tracing message delivery. Each receiving mail transfer agent normally adds a Received header, creating a sequence that can show the systems that handled the message, timestamps, and the direction of delivery. Analysts should read these entries from the oldest relevant Received header toward the newest to reconstruct the message path.

The Return-Path identifies the envelope sender address used for mail delivery and bounce processing. It can differ from the visible From address, which attackers commonly spoof to impersonate a trusted department or sender. These fields should be evaluated with authentication results such as SPF, DKIM, and DMARC, rather than relying only on a displayed sender name. CISA describes preserving and analyzing email headers during phishing investigations in its phishing guidance.

QUESTION NO: 3

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: A E

Explanation:

Validate input upon submission. is an appropriate corrective action because the attack vector is malicious content delivered through a web form. Server-side input validation should enforce an allowlist of expected data formats, lengths, characters, and values before the application processes a submission. This reduces the opportunity for attacker-controlled input to be interpreted as commands, queries, paths, or other executable content. Validation must occur on the server, where an attacker cannot bypass it by modifying browser-side controls. OWASP describes input validation as a key application-layer control for reducing injection and malformed-input risks: OWASP Input Validation Cheat Sheet.

Enable file integrity monitoring. is also appropriate because the incident includes deletion of log files to conceal activity. File integrity monitoring establishes a baseline for critical files and generates alerts when protected files are created, altered, moved, or deleted. Monitoring web-application files, system binaries, configuration files, and log locations helps identify further tampering, supports investigation of the scope and timing of compromise, and provides detection capability while the vulnerability is being contained and remediated. Cisco security operations guidance emphasizes maintaining visibility and telemetry to detect and investigate malicious activity: Cisco Secure Workload.

QUESTION NO: 4

Data has been exfiltrated and advertised for sale on the dark web. A web server shows:

Database unresponsiveness

PageFile.sys changes

Disk usage spikes with CPU spikes

High page faults

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: C

Explanation:

Analyze the PageFile.sys file in the System Drive and the Virtual Memory configuration is the appropriate incident-response action because the reported indicators point to abnormal virtual-memory activity. Windows uses the page file to move memory pages between RAM and disk when physical memory is under pressure. High page-fault rates, concurrent CPU and disk spikes, and observed changes to PageFile.sys can therefore identify an unusually memory-intensive process or workload that warrants investigation. In an exfiltration case, this activity may also coincide with malware staging data, executing code, process-memory artifacts, credentials, command strings, or other evidence that was paged from physical memory to disk. The incident-response team should preserve the system state as safely as operational requirements allow, acquire the page file using forensically sound procedures, and correlate its artifacts with running-process evidence, Windows event logs, endpoint telemetry, network connections, and the timing of suspected data transfer. Reviewing the virtual-memory configuration is also important because it establishes the configured page-file location, sizing, and behavior needed to scope collection and correctly interpret the observed changes. Microsoft documents page-file operation as part of Windows virtual-memory management, and forensic practitioners recognize page files as a potentially valuable source of memory-resident artifacts. See Microsoft's page-file overview and SANS guidance on memory forensics.

QUESTION NO: 5

A cybersecurity analyst detects fileless malware activity on secure endpoints. What should be done next?

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:

Isolate the affected endpoints and conduct a detailed memory analysis to identify fileless malware execution. is the appropriate next action because fileless attacks commonly execute through memory-resident code and legitimate system utilities, leaving little or no conventional file-system evidence. Network isolation immediately contains the incident by limiting command-and-control communication, credential abuse, and lateral movement, while preserving the endpoint's current volatile state as much as possible. The response team should then collect volatile memory according to established forensic procedures, document the acquisition, and analyze the capture for active processes, injected code, network connections, loaded modules, PowerShell activity, and other execution artifacts. This approach produces actionable evidence for scoping the intrusion and supports later eradication and recovery decisions. Cisco Secure Endpoint is designed to provide endpoint telemetry and investigation capabilities that can assist responders in correlating suspicious endpoint activity; see the Cisco Secure Endpoint overview. The importance of collecting and analyzing volatile data during incident handling is also described in NIST's Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 6

Which type of record enables forensics analysts to identify fileless malware on Windows machines?

A. IIS logs

B. file event records

C. PowerShell event logs

D. network records

ANSWER: C

Explanation:

PowerShell event logs are the most useful record type for identifying fileless malware because these attacks commonly execute commands, download payloads, and invoke code directly in memory through PowerShell rather than creating a conventional malicious executable on disk. When appropriate auditing is enabled, Windows PowerShell logging can capture operational evidence such as script-block content, module activity, command invocation, engine startup, and transcription output. This information gives an investigator visibility into the actual commands and scripts that ran, including encoded commands, suspicious download cradles, reflection-based loading, credential access attempts, and execution initiated by legitimate parent processes.

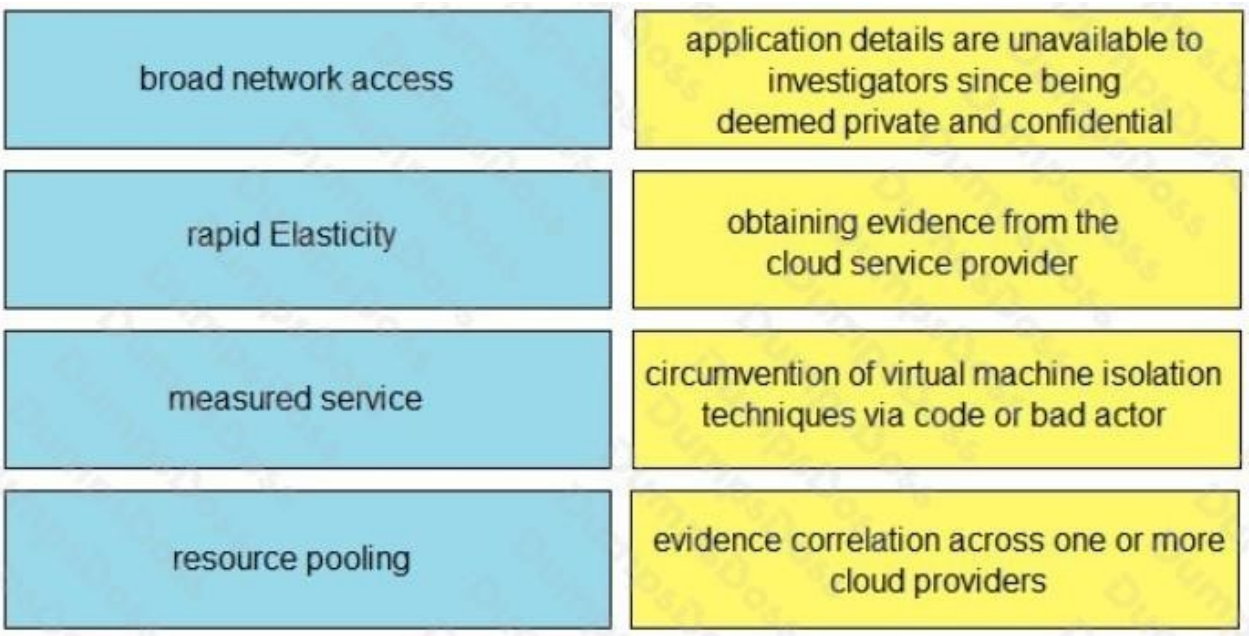
Forensic analysis of these records can establish a timeline of execution and identify indicators that would not be available from ordinary file-system artifacts. Script Block Logging is particularly valuable because it records de-obfuscated script content in many cases, making malicious behavior more visible even when an attacker attempts to conceal it. Microsoft documents the available PowerShell logging capabilities and the events they generate in about Logging Windows PowerShell. MITRE ATT&CK also identifies PowerShell as a frequently abused command and scripting interpreter in Technique T1059.001.

QUESTION NO: 7 - (DRAG DROP)

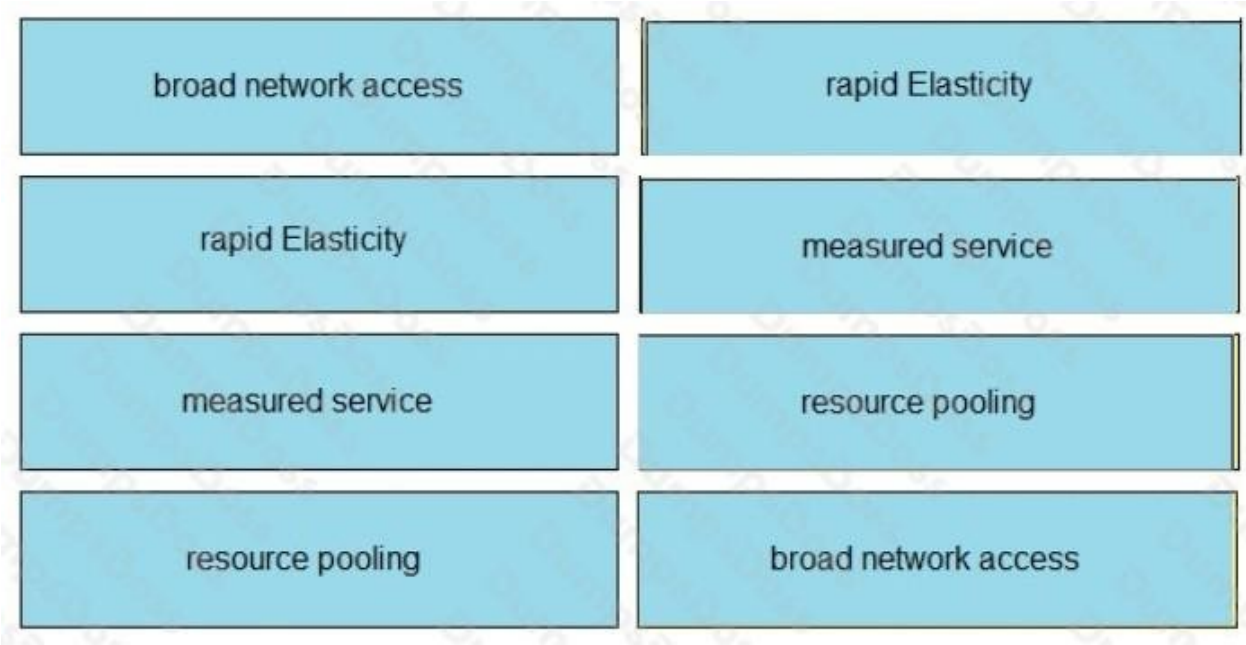
DRAG DROP

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.

Select and Place:



ANSWER:



Explanation:

Cloud evidence collection is shaped by the essential characteristics of cloud computing because those characteristics determine where data exists, who controls it, and how long it remains available. Rapid elasticity correctly aligns with application details being unavailable to investigators when those details are treated as private and confidential. Elastic environments can create, resize, move, and remove workloads quickly, so an investigator often needs provider-held records and timely access to identify the relevant workload state and associated application information.

Measured service correctly aligns with obtaining evidence from the cloud service provider. Cloud platforms measure resource consumption through metering, logging, usage records, account activity, and billing-related telemetry. Those provider-controlled records can establish activity, time frames, identities, and use of services, making provider cooperation central to collecting this evidence.

Resource pooling correctly aligns with possible circumvention of virtual-machine isolation techniques via malicious code or a bad actor. Pooled infrastructure supports multiple customers on shared physical resources while relying on logical isolation.

A compromise affecting that isolation creates a significant forensic concern because activity or impact may cross tenant boundaries in a shared environment.

Broad network access correctly aligns with evidence correlation across one or more cloud providers. Services are accessed through networks from varied locations, devices, and connected environments. A complete investigation may therefore require correlating network, identity, endpoint, and provider records from several cloud services. The NIST cloud-computing definition describes these essential characteristics, and the NIST cloud forensic challenges publication provides supporting forensic context.

QUESTION NO: 8

An analyst is using Cisco Secure Malware Analytics to investigate a submitted executable. Which two artifacts from dynamic analysis can help identify command-and-control activity? (Choose two.)

A. TCP/IP streams

B. DNS requests

C. document properties

D. PE section names

E. file creation date

ANSWER: A B

Explanation:

TCP/IP streams and **DNS requests** can help identify command-and-control activity. TCP/IP streams show connections and data exchanged by the sample during execution, while DNS requests can reveal domains resolved before communication with external infrastructure. Together, these artifacts support identification of suspicious destinations, beaconing behavior, and related indicators for threat hunting.

Document properties and PE section names are static artifacts. They can be useful during malware analysis, but they do not directly show the runtime communications generated during detonation. Cisco Secure Malware Analytics provides behavioral and network observables for submitted samples; see Cisco Secure Malware Analytics.

QUESTION NO: 9

A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries

B. Inspect processes.

C. Inspect file hash.

D. Inspect file type.

E. Inspect PE header.

ANSWER: A B

Explanation:

Inspect registry entries and **Inspect processes.** are the appropriate sandbox-analysis actions because they assess runtime behavior produced when the suspicious file executes in an isolated environment. Process inspection reveals the process tree, child-process creation, command-line activity, process injection indicators, network-related execution, and other behaviors that help determine whether the file is acting maliciously. This is particularly useful when a sample attempts

to access protected resources, because the analyst can correlate the activity with the responsible executable and its spawned processes.

Registry inspection identifies changes made during execution, including persistence mechanisms such as Run keys, service configuration, altered security settings, and newly created or modified registry values. Malware frequently uses registry modifications to survive reboots, establish execution paths, or change host behavior. A sandbox records these behavioral artifacts safely and allows analysts to review them without exposing production workstations or the centralized file server.

Cisco Secure Malware Analytics performs dynamic analysis in a controlled environment and reports observable behaviors, including process and system-modification activity. Cisco's malware-analysis overview is available at Cisco Secure Malware Analytics; guidance on malware behavioral analysis is also available from CISA.

QUESTION NO: 10

```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
 wWLu = ""
 FETw = 1
        for i=1 to len(UUf)
 if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
 sJs = sJs + mid(UUf, i, 1) '!!!
 FETw = 1
 else
 if FETw = 1 then
 NEL = Clnt (sJs) '!!!
 VlxJ = XOR_Func(NEL, key) '!!!
 wWLu = wWLu + Chr(VlxJ) '!!!
 end if
  sJs = ""
 FETw = 0
 end if
 vkB = bEBk or CFc
next
 decrypt = wWLu
 end function
         function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```

Refer to the exhibit. Which type of code created the snippet?

A. VB Script

B. Python

C. PowerShell

D. Bash Script

ANSWER: A

Explanation:

VB Script is the correct identification for the snippet. VBScript is a lightweight scripting language commonly executed by the Windows Script Host through script files such as `.vbs`. It uses Visual Basic-style syntax and frequently interacts with Windows objects through built-in scripting functions and automation objects. In forensic investigations, VBScript is often encountered in script-based droppers, login scripts, and malicious attachments because it can invoke Windows functionality without requiring a separately compiled executable. The language's object-creation capability is particularly important: VBScript can instantiate COM automation objects with `CreateObject`, allowing a script to work with components exposed by the operating system or installed applications. Microsoft documents `CreateObject` as a VBScript function that creates and returns a reference to an Automation object, a characteristic routinely seen in Windows-hosted VBScript code. The execution environment and script-host concepts are documented in Microsoft's VBScript CreateObject function reference and its Windows Script Host documentation. These language and host conventions identify the displayed code as VB Script.

QUESTION NO: 11

A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.

B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).

C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D. Analyze the Magic File type in Cisco Umbrella.

E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

ANSWER: B C

Explanation:

Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid) and evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid). Secure Malware Analytics performs dynamic analysis by executing a submitted file in an instrumented sandbox and recording the resulting host and network behavior. Reviewing TCP/IP streams allows the analyst to inspect communications generated during detonation, including connection activity and transferred data associated with the reported external IP address. This supports investigation of possible command-and-control traffic, payload retrieval, or data-exfiltration behavior.

Behavioral indicators provide the sandbox's identified suspicious actions and associated context. They are especially relevant when the alert reports filesystem manipulation such as creation of a deceptive recycle-bin-named folder. The analyst can use these indicators to confirm the behavior, identify related processes and artifacts, and determine the severity and intent of the executable. Together, network-stream review and behavioral-indicator review correlate the file's outbound communications with its local system activity, producing evidence suitable for scoping and incident-response decisions. Cisco describes Secure Malware Analytics as a solution for analyzing file behavior and providing actionable threat intelligence in its Secure Malware Analytics product documentation; Cisco support resources are available through the Secure Malware Analytics support page.

QUESTION NO: 12

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: B E

Explanation:

Provide security awareness training and block usage of external drives. is an appropriate preventive control because it addresses both the human behavior that enabled the compromise and the removable-media delivery mechanism. Employees must be trained not to connect unknown media and to report suspicious devices. Enforcing endpoint controls that restrict or block unauthorized USB mass-storage devices reduces the opportunity for malicious code to execute from a found flash drive. This is a practical defense-in-depth control for threats introduced through removable media.

Deploy MFA authentication to prevent unauthorized access to critical assets. limits the impact of stolen passwords. An attacker who captures a user credential from a compromised endpoint still needs an additional authentication factor to access protected applications and critical resources. MFA therefore provides a separate control plane from the endpoint compromise and helps prevent credential theft from becoming successful remote access or data theft. Cisco identifies MFA as a key identity-security capability, while Cisco endpoint-security guidance emphasizes combining user education and endpoint controls to reduce malware risk. See Cisco: What Is Multi-Factor Authentication? and Cisco Secure Endpoint.

QUESTION NO: 13

An employee receives an email from a “trusted” person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

ANSWER: A

Explanation:

The event detail **phishing email sent to the victim** should be included because it identifies the initiating delivery mechanism that enabled the compromise. Root cause analysis determines the underlying condition or event that allowed an incident to occur, rather than merely recording when detection tooling generated an alert. In this scenario, the malicious hyperlink was delivered through an email that appeared to come from a trusted person, and the link led to malware being downloaded after the recipient interacted with it. Recording that phishing-email event establishes the incident’s initial access vector and supports meaningful corrective actions, such as improving email filtering, URL inspection and detonation, impersonation protections, user reporting procedures, and security-awareness controls. It also enables analysts to search mail logs and identify other recipients of the same campaign, related messages, and similar indicators. NIST’s incident-handling guidance emphasizes documenting incident details and using lessons learned to identify and address the causes and control gaps associated with an incident. CISA likewise identifies phishing as a common method used to deliver malicious links and malware. See NIST SP 800-61 Rev. 2 and CISA: Recognize and Report Phishing.

QUESTION NO: 14

An analyst acquires a forensic image of a compromised workstation and calculates a SHA-256 hash before transferring the image to an evidence repository. Which forensic principle does this action support?

A. evidence integrity

B. data classification

C. nonrepudiation

D. threat attribution

ANSWER: A

Explanation:

Evidence integrity is correct because a SHA-256 hash provides a repeatable cryptographic value for the acquired image. The analyst can recalculate the hash after transfer, storage, or analysis and compare the results to verify that the evidence has not changed.

Hash values do not establish who possessed the evidence or identify the attacker. They support the integrity portion of a defensible evidence-handling process and should be recorded with acquisition details and chain-of-custody documentation. NIST describes the need to preserve the integrity of digital evidence during collection and examination in NIST SP 800-86.

QUESTION NO: 15

Refer to the exhibit.

According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name: iraniansk.com

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= “Fy.exe”

E. Content-Type: application/octet-stream

ANSWER: A D

Explanation:

Domain name: iraniansk.com is an actionable network indicator because the HTTP transaction identifies the remote host from which the suspicious payload is being retrieved. Domains associated with malware-delivery infrastructure can be used in DNS, proxy, firewall, secure web gateway, and packet-capture searches to identify other potentially affected endpoints. CISA’s Emotet guidance emphasizes using known indicators, including malicious domains and network artifacts, to detect and investigate infection activity.

filename= “Fy.exe” is also a strong indicator in this packet because the HTTP Content-Disposition filename identifies the downloaded object as a Windows executable. In the context of a download from suspicious infrastructure, a directly observed executable filename is a useful host- and network-investigation artifact: analysts can locate matching downloads, correlate them with endpoint execution telemetry, and retrieve the file for hashing and malware analysis. Together, the delivery domain and executable payload name identify both the source and the object involved in the observed Emotet download chain. See CISA’s Emotet advisory and CISA’s Emotet malware analysis report.

QUESTION NO: 16

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: A B

Explanation:

endpoint detection and response and **secure email gateway** provide complementary protections for the attack chain described. A secure email gateway reduces the likelihood that phishing messages containing malicious links reach employees in the first place. Cisco Secure Email provides email threat defense capabilities, including reputation-based analysis, anti-phishing protections, URL-related defenses, and message inspection that help identify and block malicious content before a user clicks it. Cisco describes these capabilities at Cisco Secure Email.

Endpoint detection and response is essential because targeted attacks may still evade preventive controls or use convincing social-engineering techniques. EDR continuously collects endpoint telemetry and detects suspicious behaviors associated with compromise, such as malicious process execution, persistence mechanisms, command-and-control activity, and backdoor behavior. It also supports investigation and response actions, including isolating an affected macOS endpoint to contain an incident and limit further data exposure. Cisco Secure Endpoint supports endpoint detection, investigation, and response across supported operating systems, including macOS; see Cisco Secure Endpoint. Together, secure email gateway protection addresses the phishing delivery vector, while endpoint detection and response detects and contains malicious activity that occurs on user devices after delivery or interaction.

QUESTION NO: 17

An incident response analyst is preparing to scan memory using a YARA rule. How is this task completed?

A. deobfuscation

B. XML injection

C. string matching

D. data diddling

ANSWER: C

Explanation:

string matching is correct because YARA is a pattern-matching tool designed to identify files, processes, and memory regions that exhibit characteristics associated with malware or another item of interest. A YARA rule defines one or more observable patterns, commonly text strings, hexadecimal byte sequences, or regular expressions, and then evaluates those patterns through a condition. When scanning memory, the analyst applies the rule to a memory image or process-memory region so that YARA can locate matching indicators, such as malware family names, mutex values, command-and-control domains, embedded configuration markers, or distinctive code bytes.

The condition section gives the analyst control over what constitutes a detection. For example, it can require a particular string, several strings together, a threshold number of matches, or a match at a specified offset. This combination of defined patterns and logical conditions makes YARA especially useful during incident response: it transforms threat-intelligence indicators and reverse-engineering findings into repeatable searches across acquired memory. The official YARA documentation describes rules as containing string definitions and a condition that determines when those patterns identify a target. See the YARA rule-writing documentation and the official YARA project repository.

QUESTION NO: 18

An analyst is examining a Windows executable during static malware analysis. Which Portable Executable structure identifies dynamic-link libraries and functions that the executable may call?

A. import table

B. resource section

C. certificate table

D. relocation table

ANSWER: A

Explanation:

The **import table** is correct. The PE import table identifies external DLLs and the functions that the executable imports from those libraries. An analyst can inspect imported APIs to develop an initial understanding of possible capabilities, such as process creation, registry modification, network communication, or cryptographic operations.

Imported functions do not prove that every function is executed, but they are valuable static-analysis indicators that can guide sandbox testing and reverse engineering. Microsoft documents the import directory as part of the PE format in its PE format documentation.

QUESTION NO: 19

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:

The **method of infection employed by the ransomware** is the essential item for demonstrating the incident’s underlying cause. Root cause analysis must establish how the threat first gained access or was introduced into the environment, such as through a phishing attachment, malicious link, exploitation of an internet-facing vulnerability, compromised credentials, removable media, or a supply-chain mechanism. Identifying that initial infection pathway gives the organization a defensible technical basis for determining the conditions that allowed the ransomware to execute and spread across the network.

This finding also directly supports remediation and prevention. For example, once the infection method is known, the team can map it to relevant safeguards: email filtering and user awareness for phishing, patch and vulnerability management for exploited flaws, multifactor authentication for credential abuse, or network segmentation and least privilege to limit propagation. Incident handling guidance emphasizes analyzing the incident’s cause and lessons learned so that corrective actions address the actual entry vector and reduce recurrence. Cisco incident responders should document the infection method together with supporting evidence, affected scope, timeline, and resulting control improvements in the final report. See NIST SP 800-61 Rev. 2 and CISA’s Ransomware Guide.