DUMPSARENA

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

Cisco 300-215

Version Demo

Total Demo Questions: 10

Total Premium Questions: 59

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

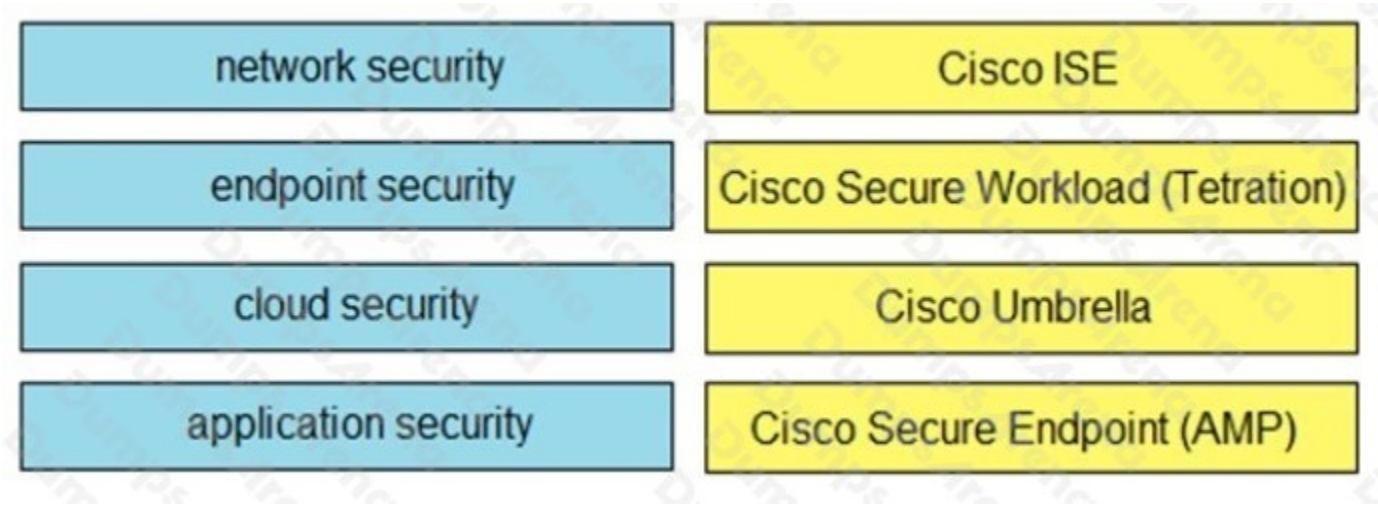
sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1 - (DRAG DROP)

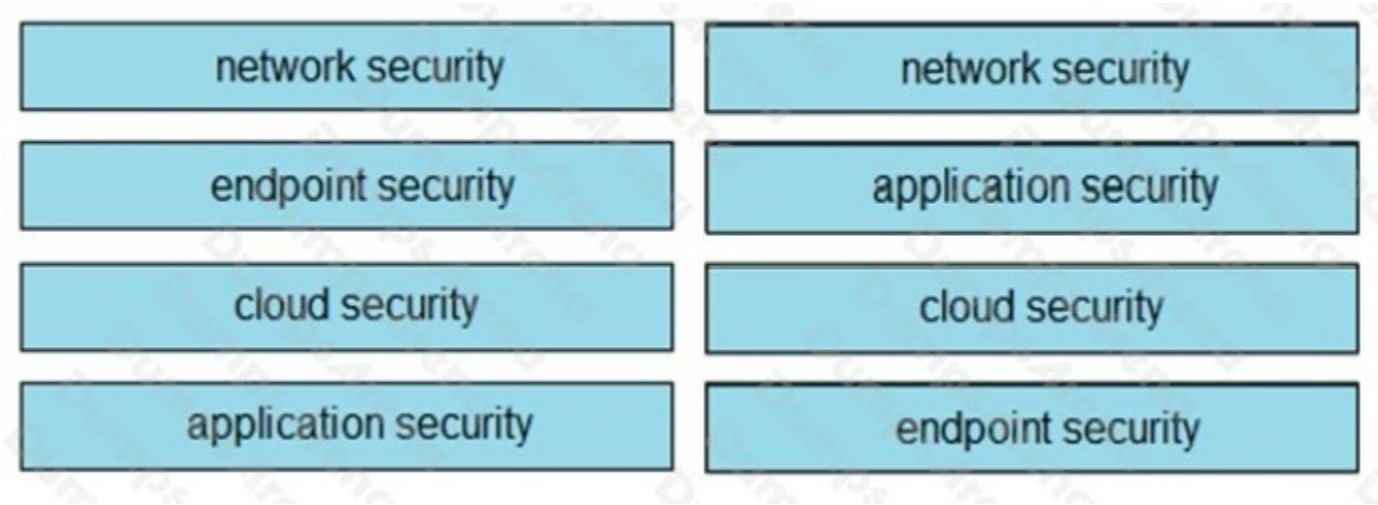
DRAG DROP

Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 2

A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident? (Choose two.)

A. verify the breadth of the attack

B. collect logs

C. request packet capture

D. remove vulnerabilities

E. scan hosts with updated signatures

ANSWER: D E

QUESTION NO: 3

An incident response team is recommending changes after analyzing a recent compromise in which:

- a large number of events and logs were involved;
- team members were not able to identify the anomalous behavior and escalate it in a timely manner;
- several network systems were affected as a result of the latency in detection;
- security engineers were able to mitigate the threat and bring systems back to a stable state; and
- the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.

Which two recommendations should be made for improving the incident response process? (Choose two.)

A. Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.

B. Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.

C. Implement an automated operation to pull systems events/logs and bring them into an organizational context.

D. Allocate additional resources for the containment phase to stabilize systems in a timely manner and reduce an attack's breadth.

E. Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

ANSWER: C E

QUESTION NO: 4

An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

A. Restore to a system recovery point.

B. Replace the faulty CPU.

C. Disconnect from the network.

D. Format the workstation drives.

E. Take an image of the workstation.

ANSWER: A E

QUESTION NO: 5

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.

B. Monitor processes as this a standard behavior of Word macro embedded documents.

C. Contain the threat for further analysis as this is an indication of suspicious activity.

D. Investigate the sender of the email and communicate with the employee to determine the motives.

ANSWER: A

QUESTION NO: 6

What is the steganography anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file

B. changing the file header of a malicious file to another file type

C. sending malicious files over a public network by encapsulation

D. concealing malicious files in ordinary or unsuspecting places

ANSWER: A

Explanation:

https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/

QUESTION NO: 7

```
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong  ag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=X509
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:536:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=RSA
7369808704:error:04093004:rsa routines:old_rsa_priv_decode:RSA lib:crypto/rsa/rsa_ameth.c:72:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=PKCS8_PRIV_KEY_INFO
7369808704:error:2306F041:PKCS12 routines:PKCS12_key_gen_uni:malloc
failure:crypto/pkcs12/p12_key.c:185:
7369808704:error:2307806B:PKCS12 routines:PKCS12_PBE_keyivgen: key gen
error:crypto/pkcs12/p12_crpt.c:55:
7369808704:error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen
failure:crypto/evp/evp_pbe.c:126:
7369808704:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit
error:crypto/pkcs12/p12_decr.c:41:
7369808704:error:2306C067:PKCS12 routines:PKCS12_item_i2d_encrypt:encrypt
error:crypto/pkcs12/p12_decr.c:144:
7369808704:error:23073067:PKCS12 routines:PKCS12_pack_p7encdata:encrypt
error:crypto/pkcs12/p12_add.c:119:
```

Refer to the exhibit. What should be determined from this Apache log?

A. A module named mod_ssl is needed to make SSL connections.

B. The private key does not match with the SSL certificate.

C. The certificate file has been maliciously modified

D. The SSL traffic setup is improper

ANSWER: D

QUESTION NO: 8

An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList

C. HKEY_CURRENT_USER\Software\Classes\Winlog

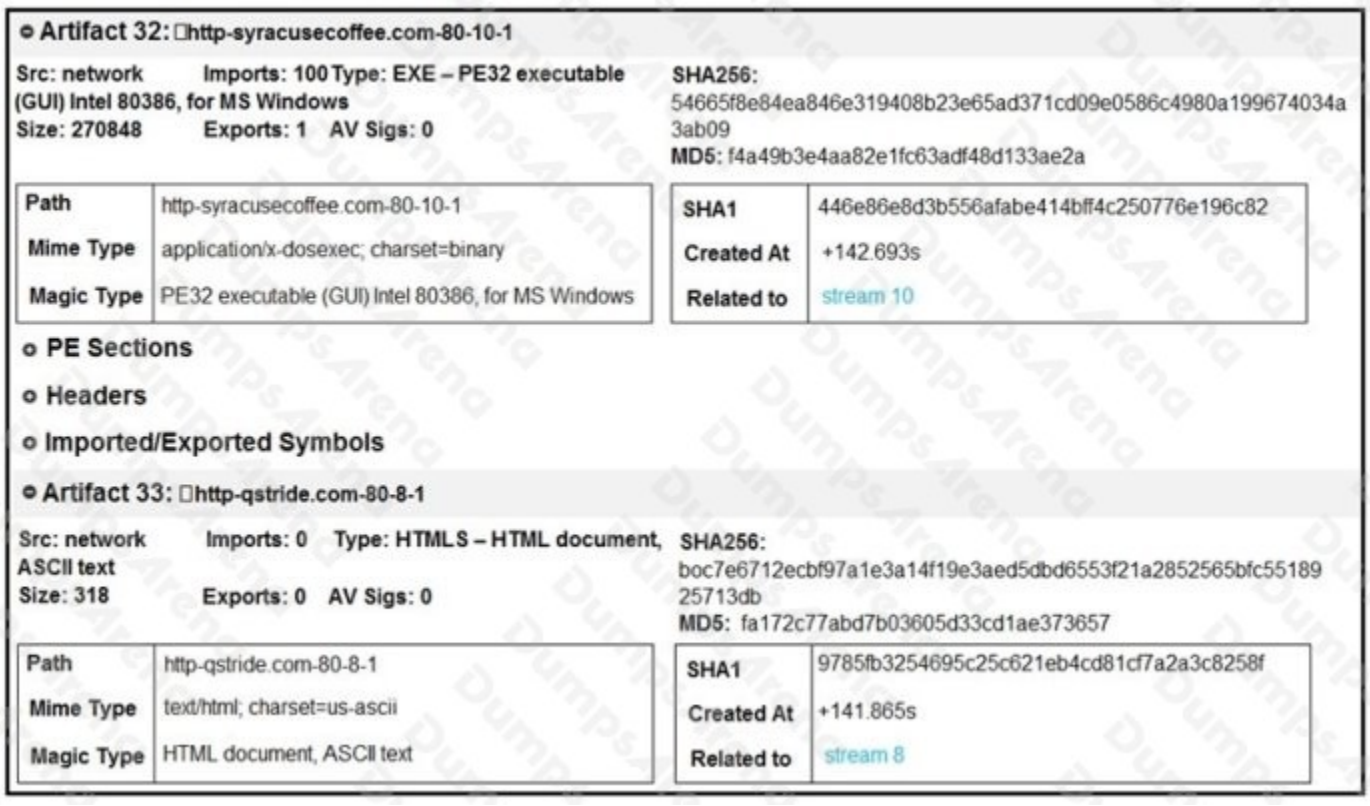
D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

ANSWER: A

Explanation:

Reference: https://www.sciencedirect.com/topics/computer-science/window-event-log

QUESTION NO: 9



Refer to the exhibit. What do these artifacts indicate?

A. An executable file is requesting an application download.

B. A malicious file is redirecting users to different domains.

C. The MD5 of a file is identified as a virus and is being blocked.

D. A forged DNS request is forwarding users to malicious websites.

ANSWER: A

QUESTION NO: 10

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-
08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-
08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-
08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```

Refer to the exhibit. Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains

B. Add a SIEM rule to alert on connections to identified domains.

C. Use the DNS server to block hole all .shop requests.

D. Block network access to identified domains.

E. Route traffic from identified domains to block hole.

ANSWER: B D