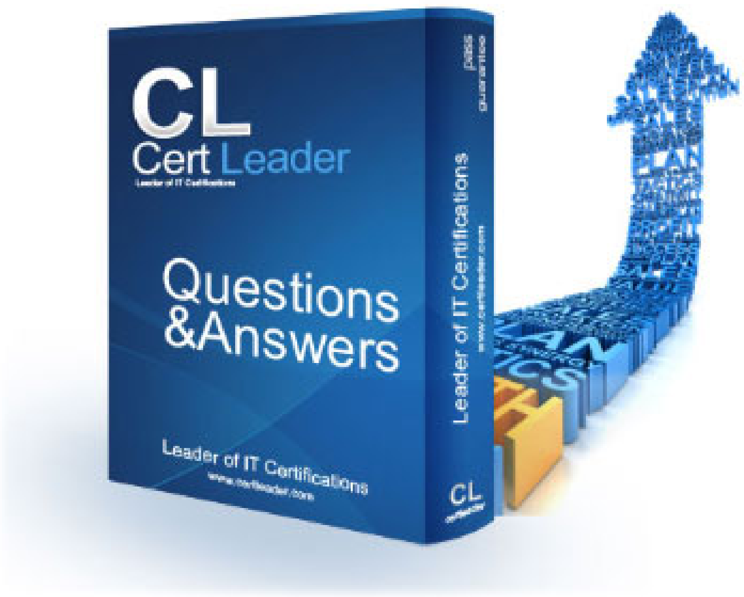
350-701 Dumps

Implementing and Operating Cisco Security Core Technologies

https://www.certleader.com/350-701-dumps.html

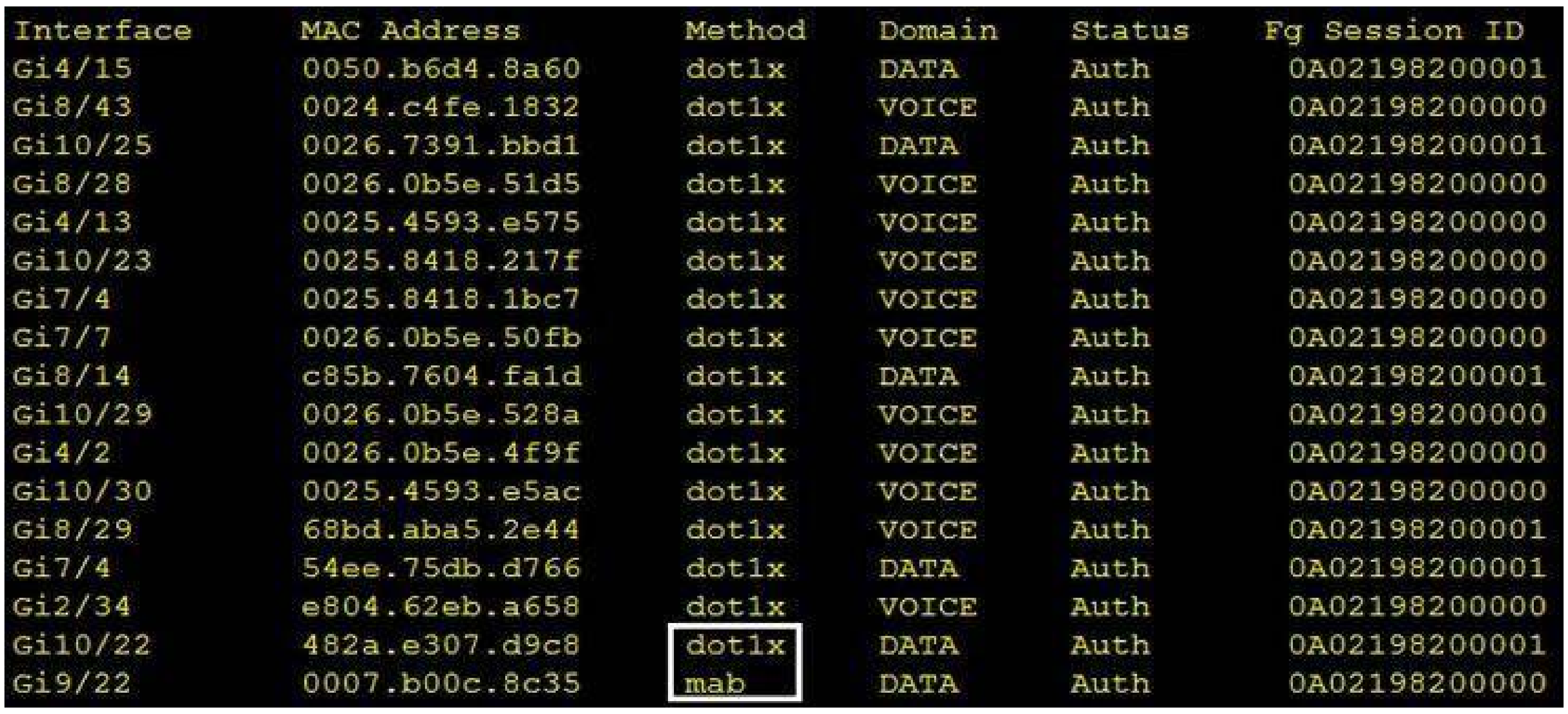


NEW QUESTION 1
Which two preventive measures are used to control cross-site scripting? (Choose two.)

A. Enable client-side scripts on a per-domain basis.
B. Incorporate contextual output encoding/escaping.
C. Disable cookie inspection in the HTML inspection engine.
D. Run untrusted HTML input through an HTML sanitization engine.
E. SameSite cookie attribute should not be used.

Answer: AB

NEW QUESTION 2
Refer to the exhibit.



```
Interface     MAC Address      Method   Domain   Status   Fg Session ID
Gi4/15        0050.b6d4.8a60   dot1x    DATA     Auth       0A02198200001
Gi8/43        0024.c4fe.1832   dot1x    VOICE    Auth       0A02198200000
Gi10/25       0026.7391.bbd1   dot1x    DATA     Auth       0A02198200001
Gi8/28        0026.0b5e.51d5   dot1x    VOICE    Auth       0A02198200000
Gi4/13        0025.4593.e575   dot1x    VOICE    Auth       0A02198200000
Gi10/23       0025.8418.217f   dot1x    VOICE    Auth       0A02198200000
Gi7/4         0025.8418.1bc7   dot1x    VOICE    Auth       0A02198200000
Gi7/7         0026.0b5e.50fb   dot1x    VOICE    Auth       0A02198200000
Gi8/14        c85b.7604.fa1d   dot1x    DATA     Auth       0A02198200001
Gi10/29       0026.0b5e.528a   dot1x    VOICE    Auth       0A02198200000
Gi4/2         0026.0b5e.4f9f   dot1x    VOICE    Auth       0A02198200000
Gi10/30       0025.4593.e5ac   dot1x    VOICE    Auth       0A02198200000
Gi8/29        68bd.aba5.2e44   dot1x    VOICE    Auth       0A02198200001
Gi7/4         54ee.75db.d766   dot1x    DATA     Auth       0A02198200001
Gi2/34        e804.62eb.a658   dot1x    VOICE    Auth       0A02198200000
Gi10/22       482a.e307.d9c8   dot1x    DATA     Auth       0A02198200001
Gi9/22        0007.b00c.8c35   mab      DATA     Auth       0A02198200000
```

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations
B. show authentication method
C. show dot1x all
D. show authentication sessions

Answer: B

NEW QUESTION 3
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two.)

A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization

Answer: AB

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

NEW QUESTION 4
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

NEW QUESTION 5
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two.)

A. TACACS+
B. central web auth
C. single sign-on
D. multiple factor auth
E. local web auth

Answer: BE

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01110.html

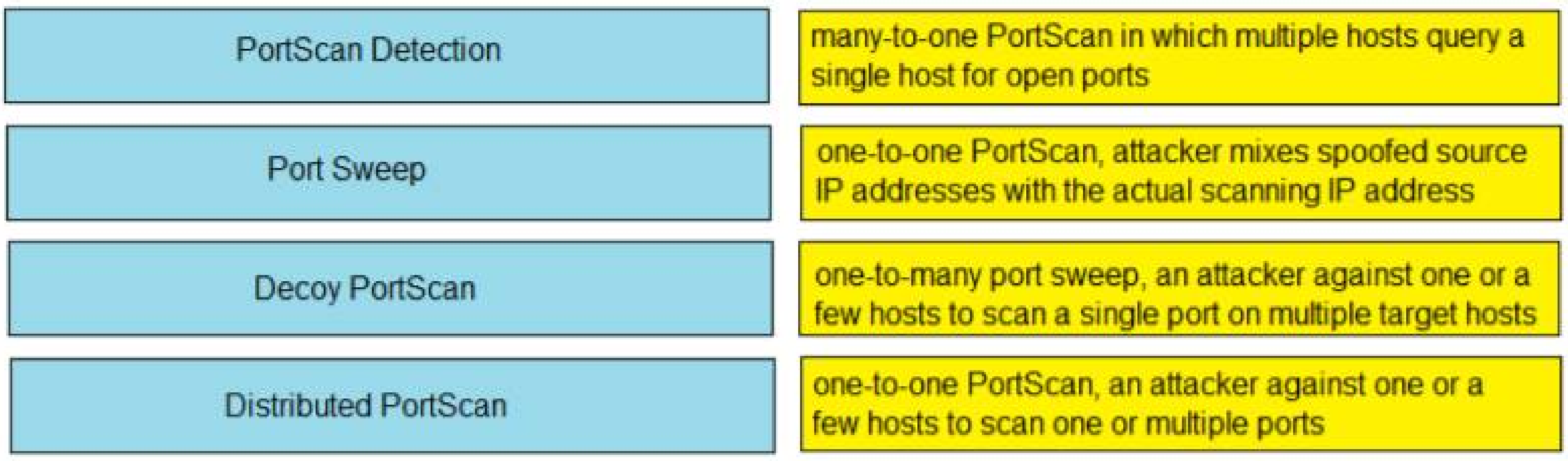
NEW QUESTION 6
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

Answer: C

Explanation:
Reference: https://tools.cisco.com/security/center/resources/sql_injection

NEW QUESTION 7
DRAG DROP
Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.



PortScan Detection

Port Sweep

Decoy PortScan

Distributed PortScan

many-to-one PortScan in which multiple hosts query a single host for open ports

one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address

one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts

one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

A. Mastered
B. Not Mastered

Answer: A

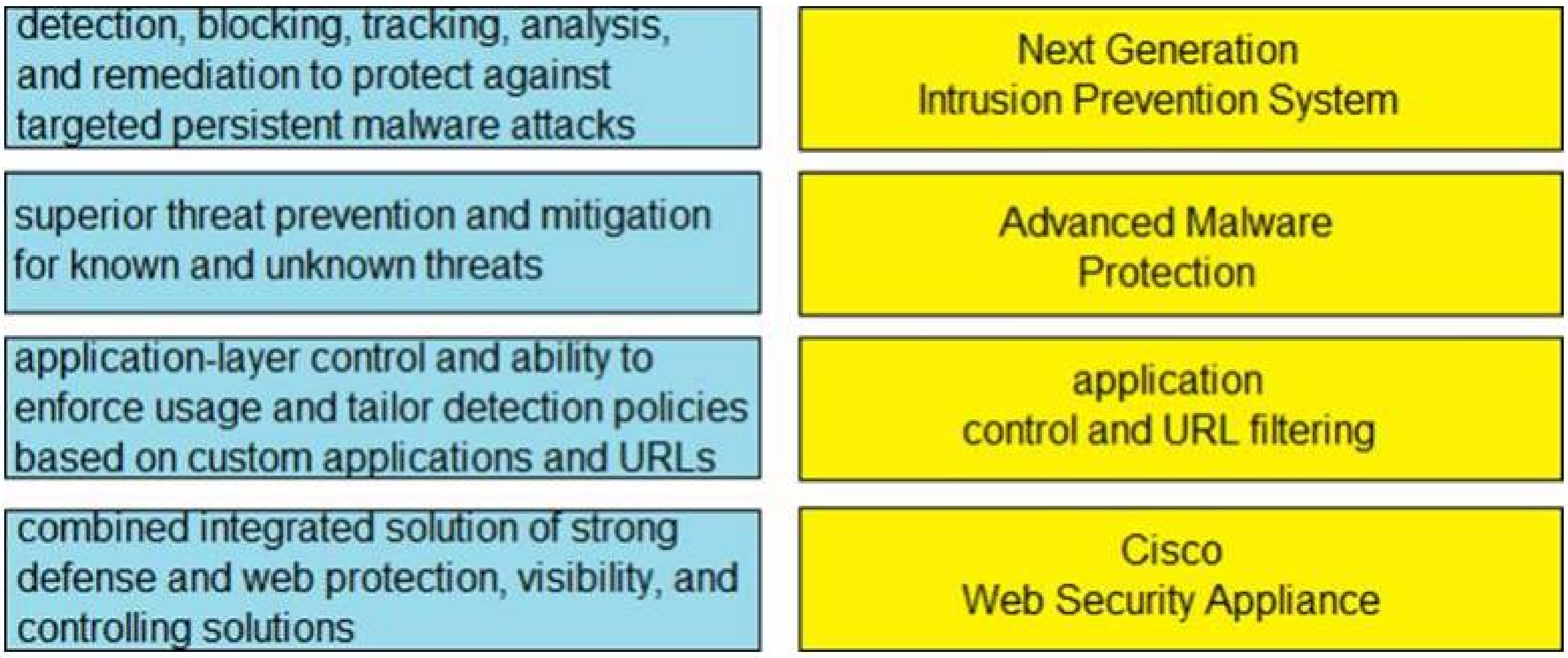
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html

NEW QUESTION 8
What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor

Answer: AD

NEW QUESTION 9
DRAG DROP
Drag and drop the capabilities from the left onto the correct technologies on the right.



detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

superior threat prevention and mitigation for known and unknown threats

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

Next Generation Intrusion Prevention System

Advanced Malware Protection

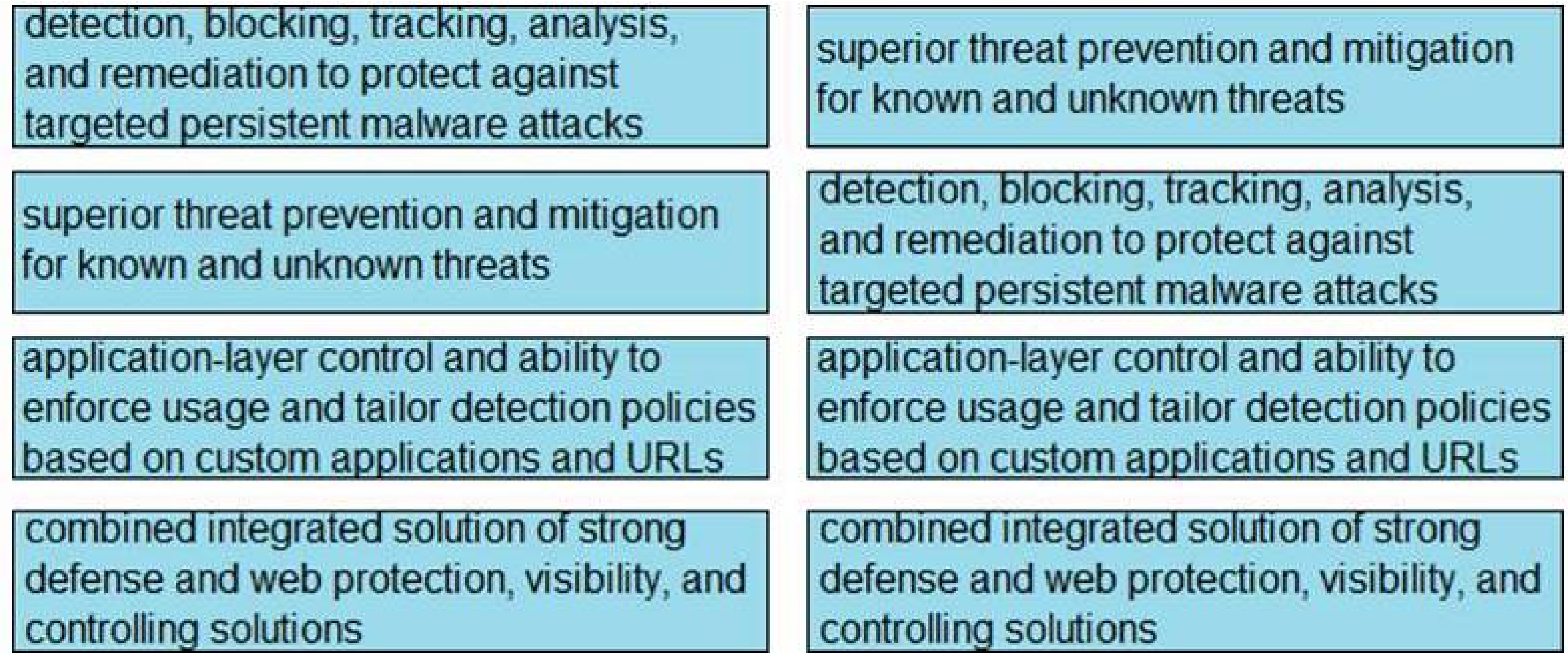
application control and URL filtering

Cisco Web Security Appliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:



detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

NEW QUESTION 10
How does Cisco Umbrella archive logs to an enterprise- owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION 10
In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Answer: A

Explanation:
Reference: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

NEW QUESTION 13
DRAG DROP
Drag and drop the descriptions from the left onto the correct protocol versions on the right.
[MISSING]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
[MISSING]

NEW QUESTION 16
Which two activities can be done using Cisco DNA Center? (Choose two.)

A. DHCP
B. design
C. accounting
D. DNS
E. provision

Answer: BE

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_00.pdf

NEW QUESTION 18
Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

A. RSA SecureID
B. Internal Database
C. Active Directory
D. LDAP

Answer: C

NEW QUESTION 23
Which two behavioral patterns characterize a ping of death attack? (Choose two.)

A. The attack is fragmented into groups of 16 octets before transmission.
B. The attack is fragmented into groups of 8 octets before transmission.
C. Short synchronized bursts of traffic are used to disrupt TCP connections.
D. Malformed packets are used to crash systems.
E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: BD

Explanation:
Reference: https://en.wikipedia.org/wiki/Ping_of_death

NEW QUESTION 24
Under which two circumstances is a CoA issued? (Choose two.)

A. A new authentication rule was added to the policy on the Policy Service node.
B. An endpoint is deleted on the Identity Service Engine server.
C. A new Identity Source Sequence is created and referenced in the authentication policy.
D. An endpoint is profiled for the first time.
E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Answer: BD

Explanation:
Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

NEW QUESTION 26
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program.

Answer: DE

NEW QUESTION 27
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.
C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

NEW QUESTION 31
Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS
B. XaaS
C. IaaS
D. SaaS

Answer: A

NEW QUESTION 32
On which part of the IT environment does DevSecOps focus?

A. application development
B. wireless network
C. data center
D. perimeter network

Answer: A

NEW QUESTION 35
What is a characteristic of traffic storm control behavior?

A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
B. Traffic storm control cannot determine if the packet is unicast or broadcast.
C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html

NEW QUESTION 40
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Answer: D

Explanation:
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

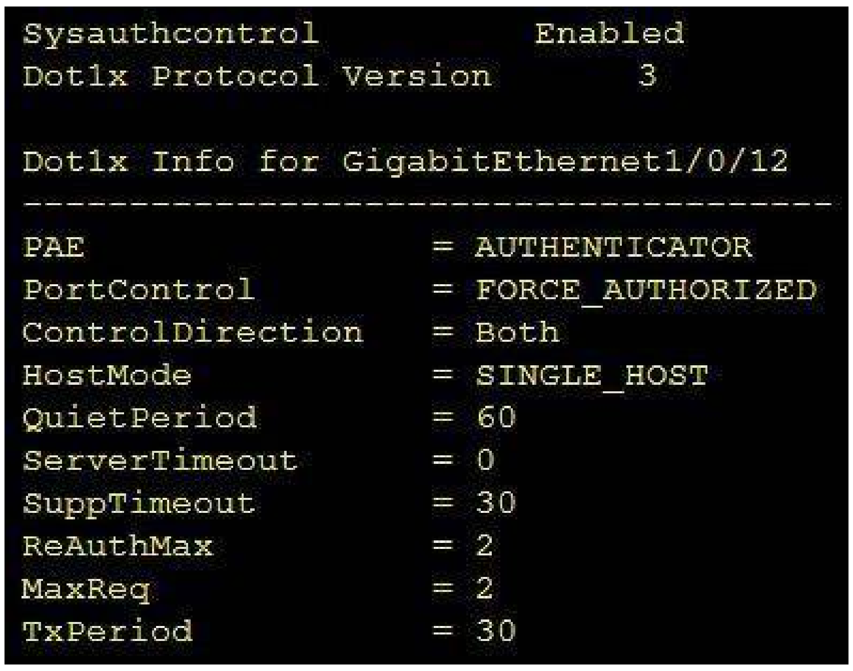
NEW QUESTION 44
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

NEW QUESTION 46
Refer to the exhibit.



```
Sysauthcontrol            Enabled
Dot1x Protocol Version        3

Dot1x Info for GigabitEthernet1/0/12
--------------------------------------
PAE                   = AUTHENTICATOR
PortControl           = FORCE_AUTHORIZED
ControlDirection      = Both
HostMode              = SINGLE_HOST
QuietPeriod           = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax             = 2
MaxReq                = 2
TxPeriod              = 30
```

Which command was used to display this output?

A. show dot1x all
B. show dot1x
C. show dot1x all summary
D. show dot1x interface gi1/0/12

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

NEW QUESTION 51
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: AB

Explanation:
Reference: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 52
Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d

NEW QUESTION 56
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP

Answer: DE

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

NEW QUESTION 61
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html

NEW QUESTION 63
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists

Answer: C

NEW QUESTION 64
......