Vendor: Cisco

Exam Code: 350-701

Exam Name: Implementing and Operating Cisco Security Core Technologies (SCOR)

Version: DEMO

QUESTION 1
A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file prevalence
B. file discovery
C. file conviction
D. file manager

Answer: A
Explanation:
Prevalence: AMP displays all files that are running across your organization, ordered by prevalence, to help you surface previously undetected threats seen by a small number of users. Files opened by only a few users may be malicious.

QUESTION 2
What is the function of the crypto isakmp key cisc406143794 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

A. It prevents all IP addresses from connecting to the VPN server.
B. It configures the pre-shared authentication key.
C. It configures the local address for the VPN server.
D. It defines what data is going to be encrypted via the VPN.

Answer: B
Explanation:
This command is used to configure pre-shared-key for IPsec remote acess users on the Cisco router. Address is mentioned as 0.0.0.0 0.0.0.0 because the users will be connecting from random ip addresses and it is almost impossible to mention all the ip addresses. Hence, 0.0.0.0 0.0.0.0 is used to allow all public ip addresses.

QUESTION 3
Which standard is used to automate exchanging cyber threat information?

A. TAXIL
B. MITRE
C. IoC
D. STIX

Answer: A
Explanation:
TAXII, short for Trusted Automated eXchange of Intelligence Information, defines how cyber threat information can be shared via services and message exchanges.

QUESTION 4
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. NTLMSSP
B. Kerberos

C. CHAP
D. TACACS+
E. RADIUS

Answer: AB
Explanation:

Overview of Acquire End-User Credentials

Server Type/Realm	Authentication Scheme	Supported Network Protocol	Notes
Active Directory	Kerberos NTLMSSP Basic	HTTP, HTTPS Native FTP, FTP over HTTP SOCKS (Basic authentication)	Kerberos is only supported in Standard mode. It is not supported in Cloud Connector mode.
LDAP	Basic	HTTP, HTTPS Native FTP, FTP over HTTP SOCKS	–

QUESTION 5
Refer to the exhibit. What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

```
ASA# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: SFR
         SFR: card status Up, mode fail-open monitor-only
              packet input 0, packet output 44715478687, drop 0, reset-drop 0
```

A. The module is operating in IDS mode.
B. The module fails to receive redirected traffic
C. Traffic is blocked if the module fails.
D. Traffic continues to flow if the module fails.
E. The module is operating in IPS mode.

Answer: AD
Explanation:
sfr {fail-open | fail-close [monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated

environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

QUESTION 6
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

A. blocks malicious websites and adds them to a block list
B. does a real-time user web browsing behavior analysis
C. provides a defense for on-premises email deployments
D. uses a static algorithm to determine malicious
E. determines if the email messages are malicious

Answer: BE
Explanation:
Cisco® Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception - based threats.
The Advanced Phishing Protection engine on the email gateway checks the unique behavior of all legitimate senders, based on the historic email traffic to your organization. The cloud service interface of the Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

QUESTION 7
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

A. monitor
B. allow
C. block
D. trust

Answer: B
Explanation:
Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html

QUESTION 8
When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?

A. records
B. flow exporter
C. flow sampler

D. flow monitor

Answer: D
Explanation:
Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.

QUESTION 9
What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?

A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
B. Cisco AMP for Endpoints prevents connections to malicious destinations, and Cisco Umbrella works at the file level to prevent the initial execution of malware
C. Cisco AMP for Endpoints automatically researches indicators of compromise and confirms threats and Cisco Umbrella does not
D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before damage can be done, and Cisco Umbrella provides the first line of defense against Internet threats

Answer: D
Explanation:
AMP for Endpoints provides a suite of response capabilities to quickly contain and eliminate threats across all endpoints, before damage can be done.
Umbrella provides the first line of defence against the threats on the internet, protecting against malware, phishing, and command and control callbacks wherever your users go.
https://blogs.cisco.com/security/prevent-detect-and-respond-with-cisco-amp-for-endpoints
https://learn-umbrella.cisco.com/webcasts/cisco-umbrella-first-line-of-defense-against-threats

QUESTION 10
A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

A. The hosts must run Cisco AsyncOS 10.0 or greater.
B. The hosts must run different versions of Cisco AsyncOS.
C. The hosts must have access to the same defined network.
D. The hosts must use a different datastore than the virtual appliance.

Answer: C
Explanation:

Migrate Your Virtual Appliance to Another Physical Host

You can use VMware® VMotion™ to migrate a running virtual appliance to a different physical host.

Requirements:

- Both physical hosts must have the same network configuration.
- Both physical hosts must have access to the same defined network(s) to which the interfaces on the virtual appliance are mapped.
- Both physical hosts must have access to the datastore that the virtual appliance uses. This datastore can be a storage area network (SAN) or Network-attached storage (NAS).
- The Cisco Secure Email Virtual Gateway must have no mail in its queue.

https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf

QUESTION 11
What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence
B. Supports STIX information
C. allows users to describe threat motivations and abilities
D. exchanges trusted anomaly intelligence information
E. determines how threat intelligence information is relayed

Answer: BE
Explanation:
TAXII, short for Trusted Automated eXchange of Intelligence Information, defines how cyber threat information can be shared via services and message exchanges. It is designed specifically to support STIX information, which it does by defining an API that aligns with common sharing models. The three principal models for TAXII include:
TAXII defines four services. Users can select and implement as many as they require, and combine them for different sharing models.

QUESTION 12
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenIOC
C. CybOX
D. STIX

Answer: B
Explanation:
OpenIOC is an open framework, meant for sharing threat intelligence information in a machine-readable format.
https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-open-indicators-of-compromise-openioc-framework-ed9d

QUESTION 13
Which Cisco WSA feature supports access control using URL categories?

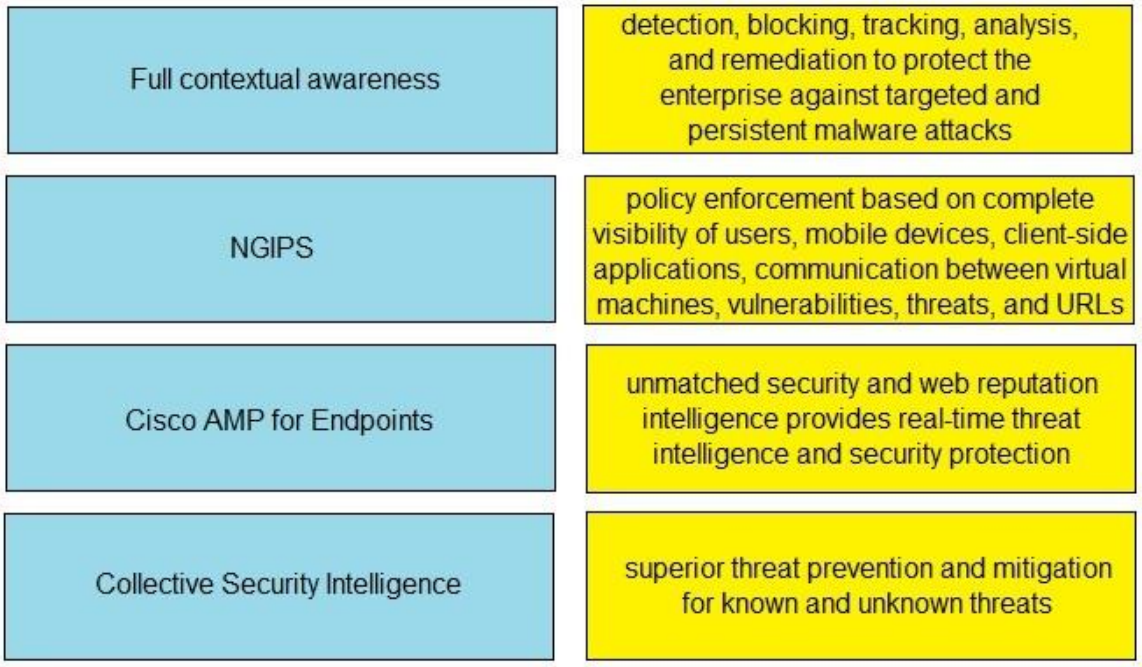
A. transparent user identification
B. SOCKS proxy services
C. web usage controls
D. user session restrictions

Answer: C
Explanation:
Overview of Categorizing URL Transactions
Using policy groups, you can create secure policies that control access to web sites containing questionable content. The sites that are blocked, allowed, or decrypted depend on the categories

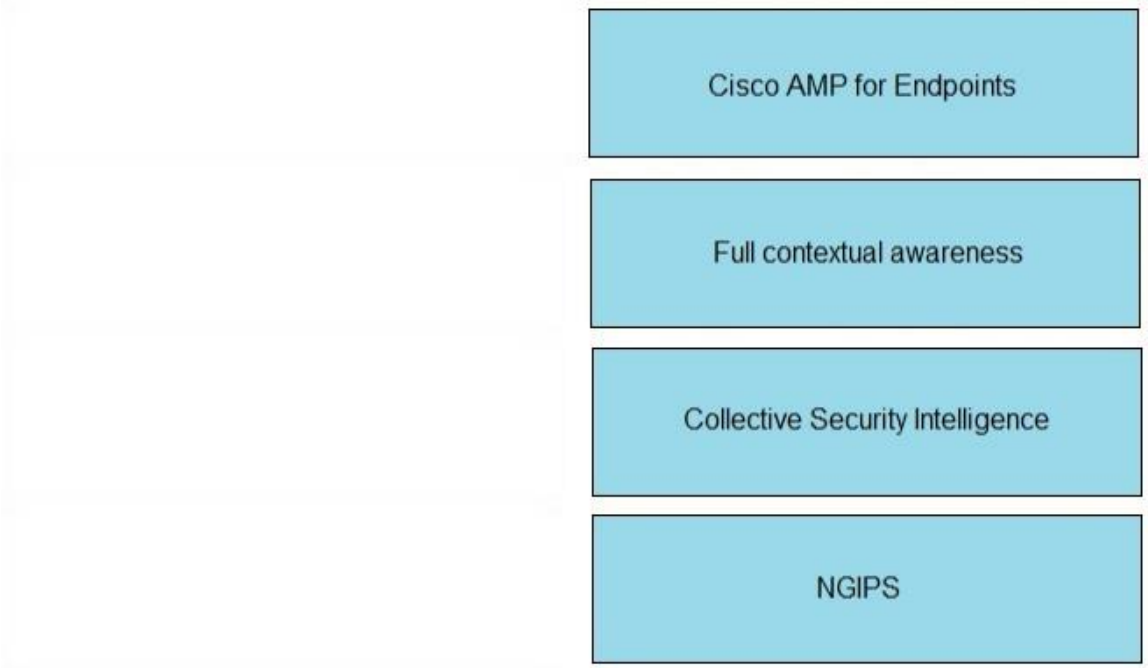
you select when setting up category blocking for each policy group. To control user access based on a URL category, you must enable Cisco Web Usage Controls.

QUESTION 14
Drag and Drop Question

Drag and drop the security solutions from the left onto the benefits they provide on the right.



Answer:



QUESTION 15
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

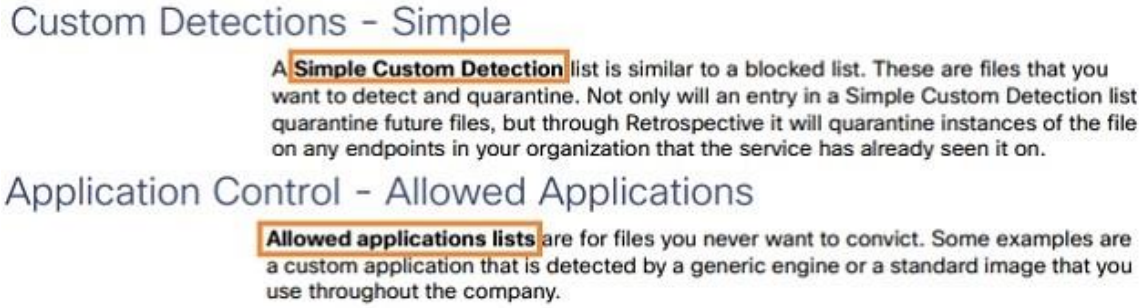
A. inter-EPG isolation
B. inter-VLAN security
C. intra-EPG isolation
D. placement in separate EPGs

Answer: C
Explanation:
Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch
Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from on another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent.

QUESTION 16
What are two list types within Cisco AMP for Endpoints Outbreak Control? (Choose two.)

A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL

Answer: BD
Explanation:



QUESTION 17
Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settings
D. destination lists

Answer: D

Explanation:
To block a URL, simply enter it into a blocked destination list, or create a new blocked destination list just for URLs. To do this, navigate to Policies > Destination Lists, expand a Destination list, add a URL and then click Save.
https://support.umbrella.com/hc/en-us/articles/115004518146-Umbrella-Dashboard-New-Features-Custom-blocked-URLs

QUESTION 18
Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D
Explanation:
AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

The following example shows how to configure a remote user to receive traps at the "priv" security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group3 v3 priv
Device(config)# snmp-server user username group-name [remote host [udp-port port]] {v1 | v2c | v3 [encrypted]
                {des | 3des | aes {128 | 192 | 256}} privpassword] [access [ipv6 nacl] {acl-number | acl-name}]
                snmp-server host-group inside net1 trap version 3 user-list engineering
```

Table 1 SNMP Version 3 Security Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication.
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

QUESTION 19
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
Explanation:
Platform-as-a-service (PaaS) is another step further from full, on-premise infrastructure management. It is where a provider hosts the hardware and software on its own infrastructure and delivers this platform to the user as an integrated solution, solution stack, or service through an internet connection.

QUESTION 20
Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Answer: A
Explanation:
Software-defined southbound application program interfaces (SDN southbound APIs) are used to communicate between the SDN Controller and the switches and routers of the network.

QUESTION 21
Which two request methods of REST API are valid on the Cisco ASA Platform? (Choose two.)

A. put
B. options
C. get
D. push
E. connect

Answer: AC
Explanation:
Available request methods are:
GET – Retrieves data from the specified object.
PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.
POST – Creates the object with the supplied information.
DELETE – Deletes the specified object.
PATCH – Applies partial modifications to the specified object.
https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

QUESTION 22
What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Answer: D
Explanation:
Telemetry - Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/active-threat-analytics-premier.pdf

QUESTION 23
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:
Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation. Each of these techniques performs all required escaping of dangerous characters before the SQL statement is passed to the underlying database system.
https://tools.cisco.com/security/center/resources/sql_injection.html

QUESTION 24
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

A. SDN controller and the cloud
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the management solution

Answer: D
Explanation:
How Do Northbound APIs Work?
Northbound APIs are the link between the applications and the SDN controller. The applications can tell the network what they need (data, storage, bandwidth, and so on) and the network can deliver those resources, or communicate what it has.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**