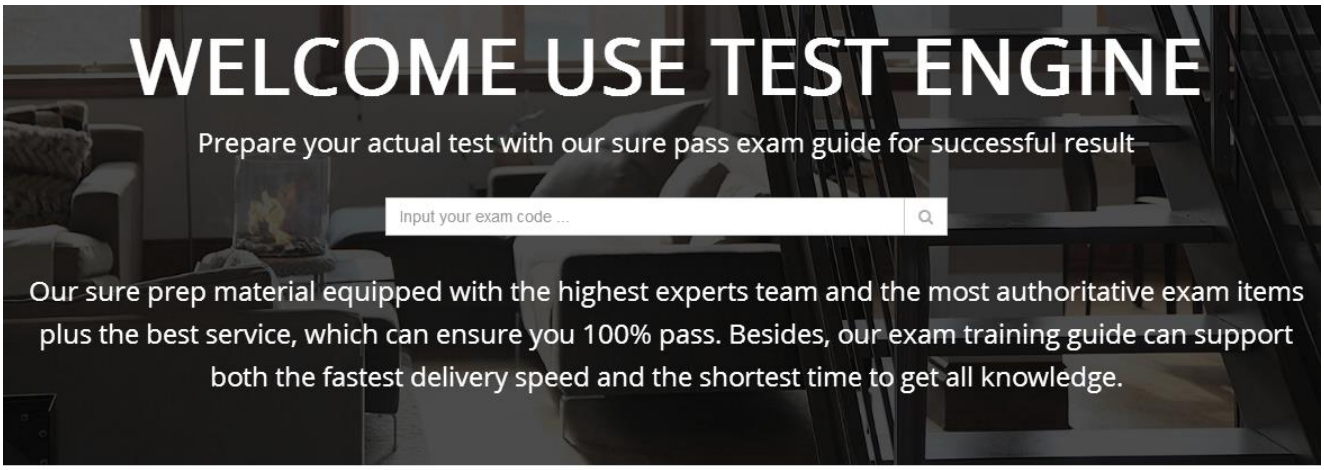
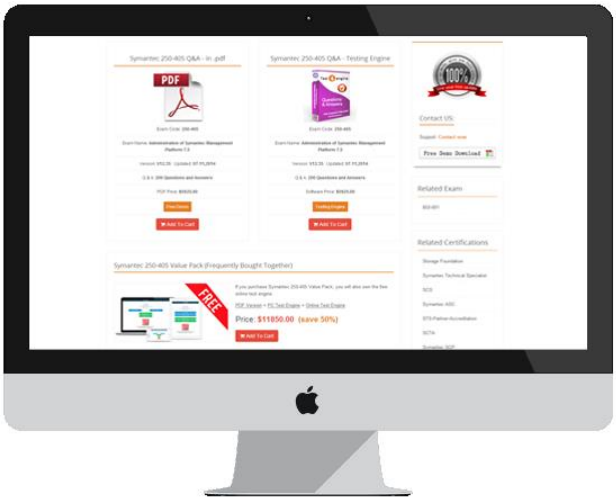
Prep4sureGuide

Prep4sureGuide





Quality and Value

Prep4sureGuide Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our Prep4sureGuide testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

Prep4sureGuide offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

HAPPY CUSTOMERS	DOWNLOADS	TEAM MEMBERS	SHARES
32694	62152	32694	56692

http://www.prep4sureguide.com

Prepare your actual test with our sure pass exam guide for successful result

Question #:1

Malware is currently spreading through an organization's network. An Incident Responder sees some detections in SEP, but there is NOT an apparent relationship between them.

How should the responder look for the source of the infection using ATP?

A. Check for the file hash for each detection

B. Isolate a system and collect a sample

C. Submit the hash to Virus Total

D. Check of the threats are downloaded from the same domain or IP by looking at incidents

Answer: D

Question #:2

A large company has 150,000 endpoints with 12 SEP sites across the globe. The company now wants to implement ATP: Endpoint to improve their security. However, a consultant recently explained that the company needs to implement more than one ATP manager.

Why does the company need more than one ATP manager?

A. An ATP manager can only connect to a SQL backend

B. An ATP manager can only support 30,000 SEP clients

C. An ATP manager can only support 10 SEP site connections.

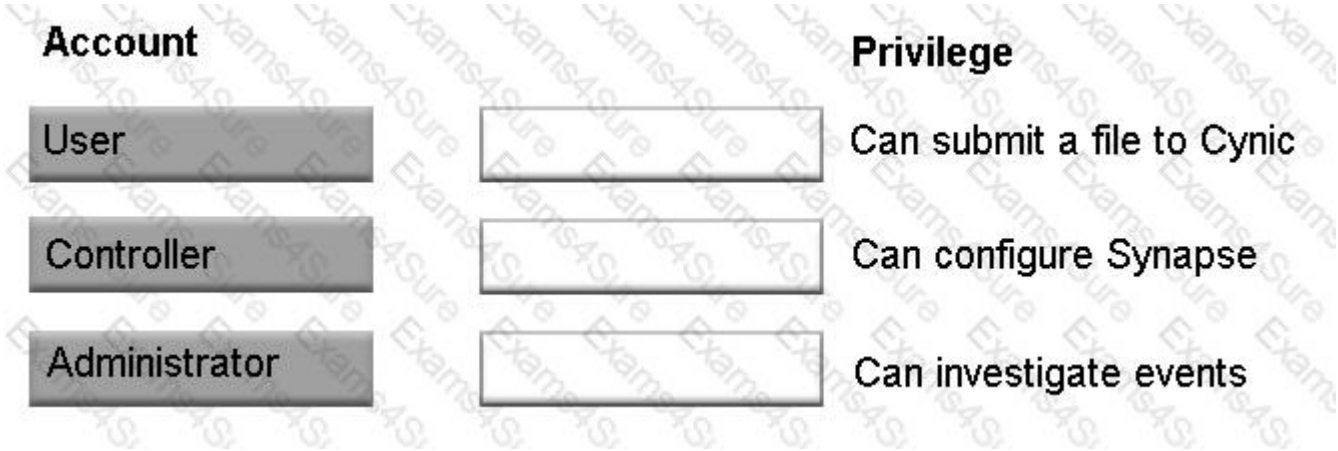
D. An ATP manager needs to be installed at each location where a Symantec Endpoint Protection Manager (SEPM) is located.

Answer: D

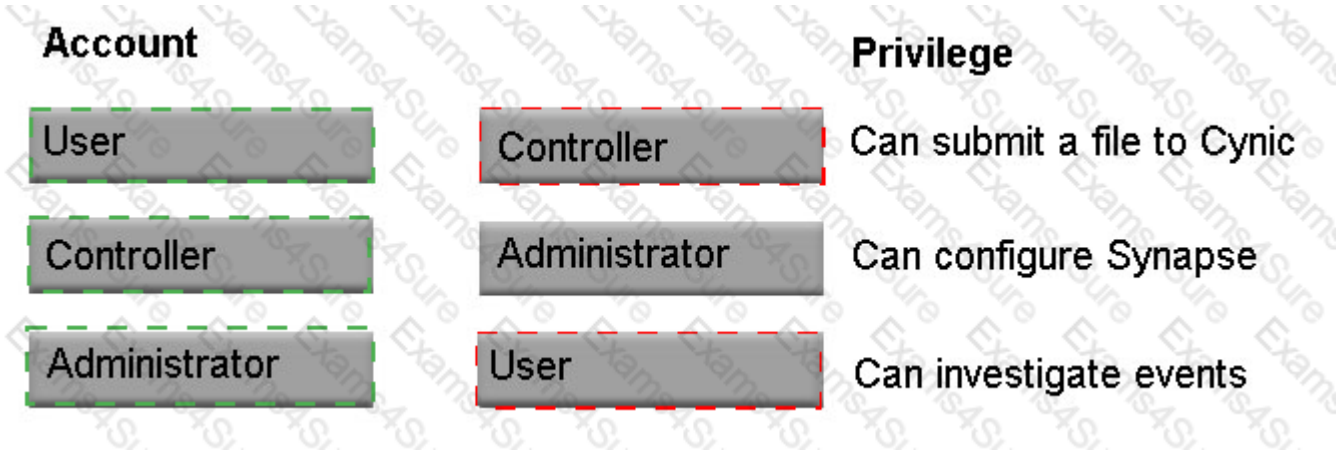
Question #:3

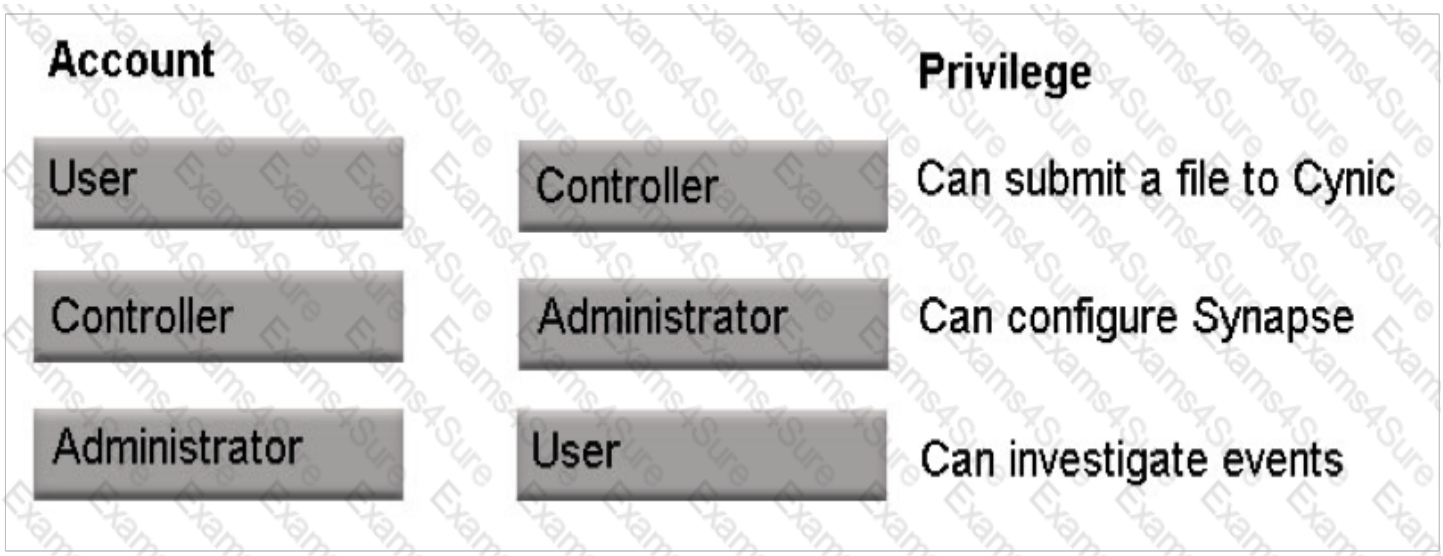
Which level of privilege corresponds to each ATP account type?

Match the correct account type to the corresponding privileges.



Answer:





Question #:4

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Answer: A

Question #:5

What is a benefit of using Microsoft SQL as the Symantec Endpoint Protection Manager (SEPM) database in regard to ATP?

A. It allows for Microsoft Incident Responders to assist in remediation

B. ATP can access the database using a log collector on the SEPM host

C. It allows for Symantec Incident Responders to assist in remediation

D. ATP can access the database without any special host system requirements

Answer: D

Question #:6

What impact does changing from Inline Block to SPAN/TAP mode have on blacklisting in ATP?

A. ATP will continue to block previously blacklisted addresses but NOT new ones.

B. ATP does NOT block access to blacklisted addresses unless block mode is enabled.

C. ATP will clear the existing blacklists.

D. ATP does NOT block access to blacklisted addresses unless TAP mode is enabled.

Answer: B

Question #:7

Where can an Incident Responder view Cynic results in ATP?

A. Events

B. Dashboard

C. File Details

D. Incident Details

Answer: D

Question #:8

Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an endpoint?

A. System Lockdown

B. Intrusion Prevention System

C. Firewall

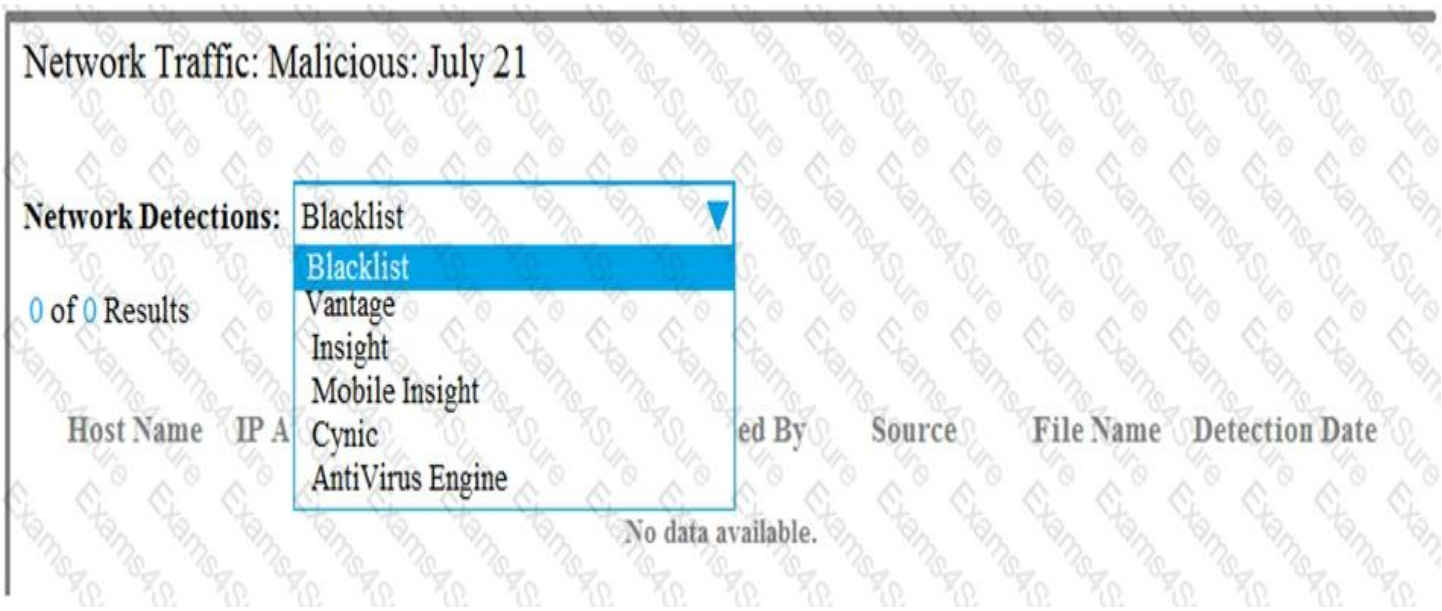
D. SONAR

Answer: A

Question #:9

Refer to the exhibit. An Incident Responder wants to see what was detected on a specific day by the IPS engine.

Which item must the responder choose from the drop-down menu?



A. Insight

B. Cynic

C. Vantage

D. Blacklist

Answer: A

Question #:10

An ATP Administrator has deployed ATP: Network, Endpoint, and Email and now wants to ensure that all connections are properly secured.

Which connections should the administrator secure with signed SSL certificates?

A. ATP and the Symantec Endpoint Protection Manager (SEPM)

ATP and SEP clients

Web access to the GUI

B. ATP and the Symantec Endpoint Protection Manager (SEPM)

ATP and SEP clients

ATP and Email Security.cloud

Web access to the GUI

C. ATP and the Symantec Endpoint Protection Manager (SEPM)

D. ATP and the Symantec Endpoint Protection Manager (SEPM)

Web access to the GUI

Answer: C

Question #:11

Which two widgets can an Incident Responder use to isolate breached endpoints from the Incident details page? (Choose two.)

A. Affected Endpoints

B. Dashboard

C. Incident Graph

D. Events View

E. Actions Bar

Answer: C E

Question #:12

What does a Quarantine Firewall policy enable an ATP Administrator to do?

A. Isolate a computer while it is manually being remediated

B. Submit files to a Central Quarantine server

C. Filter all traffic leaving the network

D. Intercept all traffic entering the network

Answer: A

Question #:13

An Incident Responder has noticed that for the last month, the same endpoints have been involved with malicious traffic every few days. The network team also identified a large amount of bandwidth being used

over P2P protocol.

Which two steps should the Incident Responder take to restrict the endpoints while maintaining normal use of the systems? (Choose two.)

A. Report the users to their manager for unauthorized usage of company resources

B. Blacklist the domains and IP associated with the malicious traffic

C. Isolate the endpoints

D. Blacklist the endpoints

E. Find and blacklist the P2P client application

Answer: C E

Question #:14

Which final steps should an Incident Responder take before using ATP to rejoin a remediated endpoint to the network, according to Symantec best practices?

A. Run an additional antivirus scan with the latest definitions. If the scan comes back as clean, rejoin the computer to the production network.

B. Run Windows Update to patch the system with the latest service pack. Once the system is up-to-date, rejoin the computer to the production network.

C. Use SymDiag to run a Threat Scan Analysis on the machine. Once the analysis comes back as clean, rejoin the computer to the production network.

D. Upgrade the client to the latest version of SEP. Once the client is upgraded, rejoin the computer to the production network.

Answer: D

Question #:15

An Incident Responder needs to remediate a group of endpoints but also wants to copy a potentially suspicious file to the ATP file store.

In which scenario should the Incident Responder copy a suspicious file to the ATP file store?

A. The responder needs to analyze with Cynic

B. The responder needs to isolate it from the network

C. The responder needs to write firewall rules

D. The responder needs to add the file to a whitelist

Answer: A

Question #:16

Which two user roles allow an Incident Responder to blacklist or whitelist files using the ATP manager?

(Choose two.)

A. Administrator

B. Controller

C. User

D. Incident Responder

E. Root

Answer: A B

Question #:17

An Incident Responder observers and incident with multiple malware downloads from a malicious domain. The domain in question belongs to one of the organization suppliers. The organization to the site to continue placing orders. Network is configured in Inline Block mode?

How should the Incident responder proceed?

A. Whitelist the domain and close the incident as a false positive

B. Identify the pieces of malware and blacklist them, then notify the supplier

C. Blacklist the domain and IP of the attacking site

D. Notify the supplier and block the site on the external firewall

Answer: D

Question #:18

During a recent virus outlook, an Incident found that the incident Response team was successful in identifying malicious that were communicating with the infected endpoint.

Which two (2) options should be incident Responder select to prevent endpoints from communicating with malicious domains?

A. Use the isolation command in ATP to move endpoint to quarantine network.

B. Blacklist suspicious domain in the ATP manager.

C. Deploy a high-Security antivirus and Antispyware policy in the Symantec Endpoint protection Manager (SEPM.)

D. Create a firewall rule in the Symantec Endpoints Protection Manager (SEPM) or perimeter firewall that blocks

E. traffic to the domain.

F. Run a full system scan on all endpoints

Answer: A B

Question #:19

How can an Incident Responder generate events for a site that was identified as malicious but has NOT

triggered any events or incidents in ATP?

A. Assign a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager

(SEPM).

B. Run an indicators of compromise (IOC) search in ATP manager.

C. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that

blocks traffic to the domain.

D. Add the site to a blacklist in ATP manager.

Answer: D

Question #:20

What is the main constraint an ATP Administrator should consider when choosing a network scanner model?

A. Throughput

B. Bandwidth

C. Link speed

D. Number of users

Answer: B

Question #:21

How should an ATP Administrator configure Endpoint Detection and Response according to Symantec best practices for a SEP environment with more than one domain?

A. Create a unique Symantec Endpoint Protection Manager (SEPM) domain for ATP

B. Create an ATP manager for each Symantec Endpoint Protection Manager (SEPM) domain

C. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for each domain

D. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for the primary domain

Answer: C

Question #:22

An Incident Responder is going to run an indicators of compromise (IOC) search on the endpoints and wants to use operators in the expression.

Which tokens accept one or more of the available operators when building an expression?

A. All tokens

B. Domainname, Filename, and Filehash

C. Filename, Filehash, and Registry

D. Domainname and Filename only

Answer: C

Question #:23

A medium-sized organization with 10,000 users at Site A and 20,000 users at Site B wants to use ATP:

Network to scan internet traffic at both sites.

Which physical appliances should the organization use to act as a network scanner at each site while using the fewest appliances and assuming typical network usage?

A. Site A 8840 x4 – Site B 8880 x2

B. Site A 8880 x2 – Site B 8840 x1

C. Site A 8880 x1 – Site B 8840 x6

D. Site A 8880 x1 – Site B 8880 x2

Answer: D

Question #:24

What is the minimum amount of RAM required for a virtual deployment of the ATP Manager in a production environment?

A. 48 GB

B. 64 GB

C. 16 GB

D. 32GB

Answer: A

Question #:25

An Incident Responder notices traffic going from an endpoint to an IRC channel. The endpoint is listed in an incident. ATP is configured in TAP mode.

What should the Incident Responder do to stop the traffic to the IRC channel?

A. Isolate the endpoint with a Quarantine Firewall policy

B. Blacklist the IRC channel IP

C. Blacklist the endpoint IP

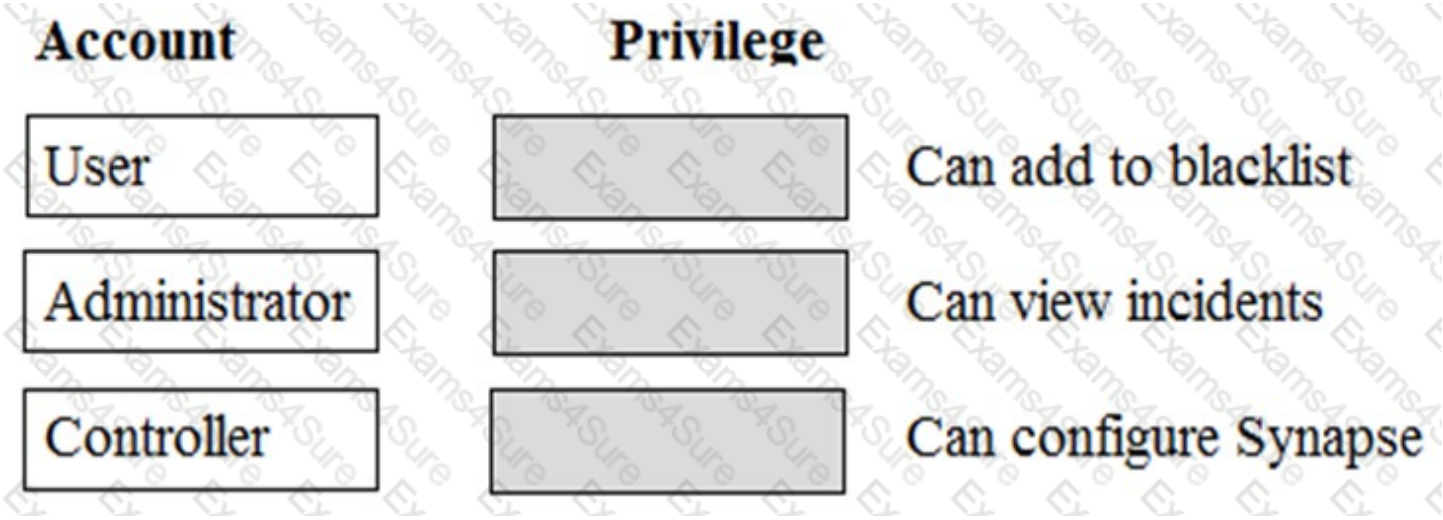
D. Isolate the endpoint with an application control policy

Answer: C

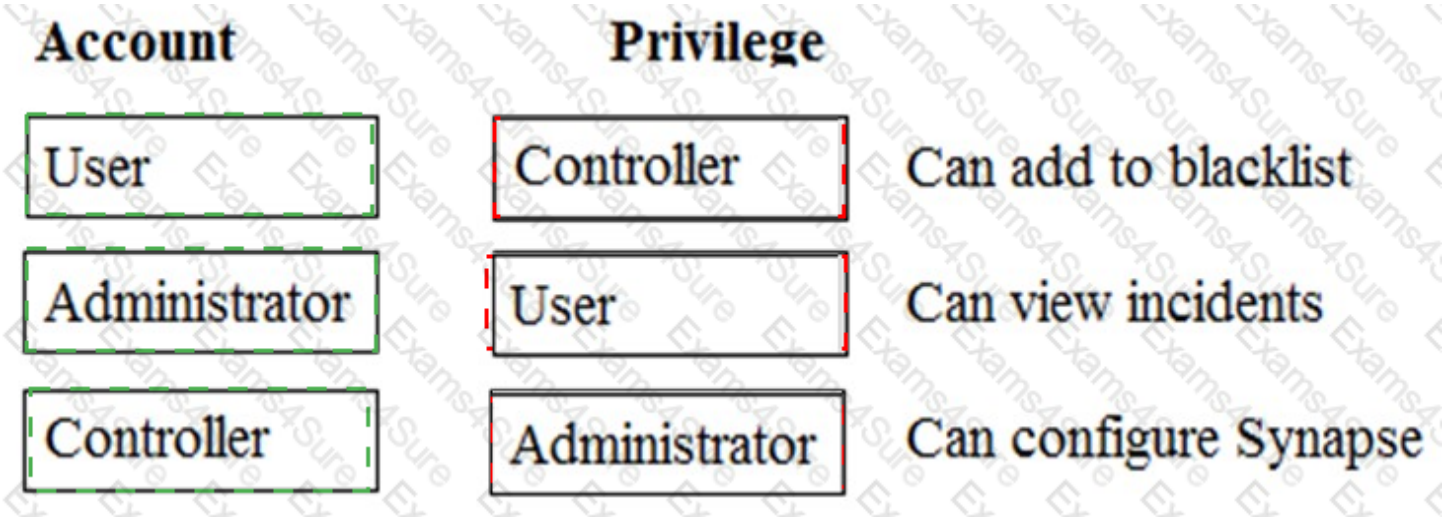
Question #:26

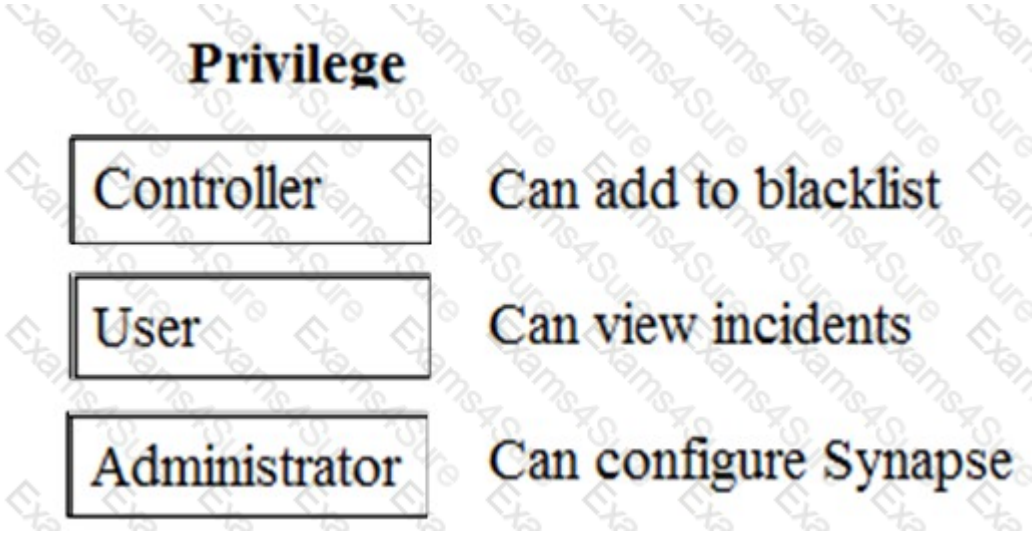
Which level of privilege corresponds to each ATP account type?

Match the correct account type to the corresponding privileges.



Answer:





Question #:27

Which two non-Symantec methods for restricting traffic are available to the Incident Response team? (Choose two.)

A. Temporarily disconnect the local network from the internet.

B. Create an Access Control List at the router to deny traffic.

C. Analyze traffic using Wireshark protocol analyzer to identify the source of the infection.

D. Create a DNS sinkhole server to block malicious traffic.

E. Isolate computers so they are NOT compromised by infected computers.

Answer: C D

Question #:28

An organization is considering an ATP: Endpoint and Network deployment with multiple appliances.

Which form factor will be the most effective in terms of performance and costs?

A. Virtual for management, physical for the network scanners and ATP: Endpoint

B. Physical for management and ATP: Endpoint, virtual for the network scanners

C. Virtual for management and ATP: Endpoint, physical for the network scanners

D. Virtual for management, ATP: Endpoint, and the network scanners

Answer: B

Question #:29

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Answer: B

Question #:30

Which threat is an example of an Advanced Persistent Threat (APT)?

A. ILOVEYOU

B. Conficker

C. MyDoom

D. GhostNet

Answer: D

Question #:31

Which detection method identifies a file as malware after SEP has queried the file's reputation?

A. Skeptic

B. Vantage

C. insight

D. Cynic

Answer: C

Question #:32

An Incident Responder wants to run a database search that will list all client named starting with SYM.

Which syntax should the responder use?

A. hostname like “SYM”

B. hostname “SYM”

C. hostname “SYM*”

D. hostname like “SYM*”

Answer: A

Question #:33

An Incident Responder runs an endpoint search on a client group with 100 endpoints. After one day, the responder sees the results for 90 endpoints.

What is a possible reason for the search only returning results for 90 of 100 endpoints?

A. The search expired after one hour

B. 10 endpoints are offline

C. The search returned 0 results on 10 endpoints

D. 10 endpoints restarted and cancelled the search

Answer: C

Question #:34

During a recent virus outbreak, an Incident Responder found that the Incident Response team was successful in identifying malicious domains that were communicating with the infected endpoints.

Which two options should the Incident Responder select to prevent endpoints from communicating with malicious domains? (Select two.)

A. Use the isolate command in ATP to move all endpoints to a quarantine network.

B. Blacklist suspicious domains in the ATP manager.

C. Deploy a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

D. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that blocks traffic to the domain.

E. Run a full system scan on all endpoints.

Answer: D E

Question #:35

An Incident Responder wants to use a STIX file to run an indicate of components (IOC) search.

Which format must the administrator use for the file?

A. .csv

B. .xml

C. .mht

D. .html

Answer: B

Question #:36

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Answer: B

Question #:37

Which attribute is required when configuring the Symantec Endpoint Protection Manager (SEPM) Log Collector?

A. SEPM embedded database name

B. SEPM embedded database type

C. SEPM embedded database version

D. SEPM embedded database password

Answer: D

Question #:38

Which Advanced Threat Protection (ATP) component best isolates an infected computer from the network?

A. ATP: Email

B. ATP: Endpoint

C. ATP: Network

D. ATP: Roaming

Answer: B

Question #:39

Which two actions an Incident Responder take when downloading files from the ATP file store? (Choose two.)

A. Analyze suspicious code with Cynic

B. Email the files to Symantec Technical Support

C. Double-click to open the files

D. Diagnose the files as a threat based on the file names

E. Submit the files to Security Response

Answer: A C

Question #:40

Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security.cloud

B. Web security.cloud

C. Skeptic

D. Symantec Messaging Gateway

Answer: A

Question #:41

An Incident Responder wants to create a timeline for a recent incident using Syslog in addition to ATP for the After Actions Report.

What are two reasons the responder should analyze the information using Syslog? (Choose two.)

A. To have less raw data to analyze

B. To evaluate the data, including information from other systems

C. To access expanded historical data

D. To determine what policy settings to modify in the Symantec Endpoint Protection Manager (SEPM)

E. To determine the best cleanup method

Answer: B E

Question #:42

Which policies are required for the quarantine feature of ATP to work?

A. Firewall Policy and Host Integrity Policy

B. Quarantine Policy and Firewall Policy

C. Host Integrity Policy and Quarantine Policy

D. Quarantine and Intrusion Prevention Policy

Answer: C

Question #:43

In which scenario should an Incident Responder manually submit a file to the Cynic portal?

A. There is a file on a USB that an Incident Responder wants to analyze in a sandbox.

B. An Incident Responder is unable to remember the password to the .zip archive.

C. The file has generated multiple incidents in the ATP manager and an Incident Responder wants to blacklist the file.

D. The file is a legitimate application and an Incident Responder wants to report it to Symantec as a false positive.

Answer: D

Question #:44

Which threat is an example of an Advanced Persistent Threat (APT)?

A. Zeus

B. Melissa

C. Duqu

D. Code Red

Answer: C

Question #:45

Why is it important for an Incident Responder to copy malicious files to the ATP file store or create an image of the infected system during the Recovery phase?

A. To have a copy of the file policy enforcement

B. To test the effectiveness of the current assigned policy settings in the Symantec Endpoint Protection Manager (SEPM)

C. To create custom IPS signatures

D. To document and preserve any pieces of evidence associated with the incident

Answer: B

Question #:46

Which default port does ATP use to communicate with the Symantec Endpoint Protection Manager (SEPM) web services?

A. 8446

B. 8081

C. 8014

D. 1433

Answer: B

Question #:47

Which two actions can an Incident Responder take in the Cynic portal? (Choose two.)

A. Configure a SIEM feed from the portal to the ATP environment

B. Configure email reports on convictions

C. Submit false positive and false negative files

D. Query hashes

E. Submit hashes to Insight

Answer: D E

Question #:48

While filling out the After Actions Report, an Incident Response Team noted that improved log monitoring could help detect future breaches.

What are two examples of how an organization can improve log monitoring to help detect future breaches? (Choose two.)

A. Periodically log into the ATP manager and review only the Dashboard.

B. Implement IT Analytics to create more flexible reporting.

C. Dedicate an administrator to monitor new events as they flow into the ATP manager.

D. Set email notifications in the ATP manager to message the Security team when a new incident is

occurring.

E. Implement Syslog to aggregate information from other systems, including ATP, and review log data in a single console.

Answer: D E

Question #:49

An Incident Responder discovers an incident where all systems are infected with a file that has the same name and different hash. As a result, the organism view has multiple entries for the malicious file.

What is causing this issue?

A. This is a polymorphic threat

B. This is a DDoS attack

C. The file has multiple hashes

D. The file is trying to phone home

Answer: A

Question #:50

What is the role of Synapse within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Answer: B

Question #:51

An ATP Administrator set up ATP: Network in TAP mode and has placed URLs on the blacklist.

What will happen when a user attempts to access one of the blacklisted URLs?

A. Access to the website is blocked by the network scanner but an event is NOT generated

B. Access to the website is blocked by the network scanner and a network event is generated

C. Access to the website is allowed by the network scanner but blocked by ATP: Endpoint and an endpoint event is generated

D. Access to the website is allowed by the network scanner but a network event is generated

Answer: D

Question #:52

How does an attacker use a zero-day vulnerability during the Incursion phase?

A. To perform a SQL injection on an internal server

B. To extract sensitive information from the target

C. To perform network discovery on the target

D. To deliver malicious code that breaches the target

Answer: D

Question #:53

Which stage of an Advanced Persistent Threat (APT) attack do attackers break into an organization's network to deliver targeted malware?

A. Incursion

B. Discovery

C. Capture

D. Exfiltration

Answer: A

Question #:54

Which two ATP control points are able to report events that are detected using Vantage?

Enter the two control point names:

ATP: network; ATP: Endpoint

Question #:55

Which two (2 non-Symantec method for restricting traffic are available to the Incident response team?

A. Temporarily disconnects the local network from the Internet.

B. Create an Access Control List at the router to deny traffic.

C. Analyze traffic using wire shark protocol analyzer to identify the source of the infection.

D. Create a DNS a sinkhole server to block malicious traffic.

E. Isolate computers so they are NOT compromised by infested computers.

Answer: A E

Question #:56

What is the role of Cynic within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Answer: D

Question #:57

Why is it important for an Incident Responder to review Related Incidents and Events when analyzing an incident for an After Actions Report?

A. It ensures that the Incident is resolved, and the responder can clean up the infection.

B. It ensures that the Incident is resolved, and the responder can determine the best remediation method.

C. It ensures that the Incident is resolved, and the threat is NOT continuing to spread to other parts of the environment.

D. It ensures that the Incident is resolved, and the responder can close out the incident in the ATP manager.

Answer: C

Question #:58

An Incident Responder documented the scope of a recent outbreak by reviewing the incident in the ATP manager.

Which two entity relationship examples should the responder look for and document from the Incident Graph? (Choose two.)

A. An intranet website that is experiencing an increase in traffic from endpoints in a smaller branch office.

B. A server in the DMZ that was repeatedly accessed outside of normal business hours on the weekend.

C. A network share is repeatedly accessed during and after an infection indicating a more targeted attack.

D. A malicious file that was repeatedly downloaded by a Trojan or downloader that infected multiple endpoints.

E. An external website that was the source of many malicious files.

Answer: D E

Question #:59

Which threat is an example of an Advanced Persistent Threat (APT)?

A. Koobface

B. Brain

C. Flamer

D. Creeper

Answer: C

Question #:60

Which threat is an example of an Advanced Persistent Threat (APT)?

A. Loyphish

B. Aurora

C. ZeroAccess

D. Michelangelo

Answer: B

Question #:61

Which access credentials does an ARP Administrator need to set up a deployment of ATP: Endpoint , Network and Email?

A. Email security. Cloud credential for email correlation, credential for the Symantec Endpoint Protection Manager (SEPM) database, and System Administrator logging for the SEPM.

B. Active Directory logging to the Symantec endpoint Protection Manager (SEPM) database and an Email Security. Cloud login with full access

C. Symantec Endpoint protection Manager (SEPM) login and ATP: Email login with service permissions

D. Credentials for the Symantec Endpoint protection Manager (SEPM) database, and an administrator loging or Symantec Messaging Gateway

Answer: A

Question #:62

What occurs when an endpoint fails its Host Integrity check and is unable to remediate?

A. The endpoint automatically switches to using a Compliance location, where a Compliance policy is applied to the computer.

B. The endpoint automatically switches to using a System Lockdown location, where a System Lockdown policy is applied to the computer.

C. The endpoint automatically switches to using a Host Integrity location, where a Host Integrity policy is applied to the computer.

D. The endpoint automatically switches to using a Quarantine location, where a Quarantine policy is applied to the computer.

Answer: D

Question #:63

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as “finding incursions”?

A. Protect

B. Identify

C. Respond

D. Detect

Answer: B

Question #:64

In which two locations should an Incident Responder gather data for an After Actions Report in ATP? (Choose two.)

A. Policies page

B. Action Manager

C. Syslog

D. Incident Manager

E. Indicators of compromise (IOC) search

Answer: C D

Question #:65

Which endpoint detection method allows for information about triggered processes to be displayed in ATP?

A. SONAR

B. Insight

C. System Lockdown

D. Antivirus

Answer: B

Question #:66

Which best practice does Symantec recommend with the Endpoint Detection and Response feature?

A. Create a unique Cynic account to provide to ATP

B. Create a unique Symantec Messaging Gateway account to provide to ATP

C. Create a unique Symantec Protection Manager (SEPM) administrator account to provide to ATP

D. Create a unique Email Security.cloud portal account to provide to ATP

Answer: C

Question #:67

Which access credentials does an ATP Administrator need to set up a deployment of ATP: Endpoint, Network, and Email?

A. Email Security.cloud credentials for email correlation, credentials for the Symantec Endpoint Protection Manager (SEPM) database, and a System Administrator login for the SEPM

B. Active Directory login to the Symantec Endpoint Protection Manager (SEPM) database, and an Email Security.cloud login with full access

C. Symantec Endpoint Protection Manager (SEPM) login and ATP: Email login with service permissions

D. Credentials for the Symantec Endpoint Protection Manager (SEPM) database, and an administrator login for Symantec Messaging Gateway

Answer: C

Question #:68

Which service is the minimum prerequisite needed if a customer wants to purchase ATP: Email?

A. Email Protect (antivirus and anti-spam)

B. Email Safeguard (antivirus, anti-spam, encryption, data protection and image control)

C. Symantec Messaging Gateway

D. Skeptic

Answer: A

Question #:69

Which two questions can an Incident Responder answer when analyzing an incident in ATP? (Choose two.)

A. Does the organization need to do a healthcheck in the environment?

B. Are certain endpoints being repeatedly attacked?

C. Is the organization being attacked by this external entity repeatedly?

D. Do ports need to be blocked or opened on the firewall?

E. Does a risk assessment need to happen in the environment?

Answer: B E

Question #:70

Which National Institute of Standards and Technology (NIST) cybersecurity function includes Risk Assessment or Risk Management Strategy?

A. Recover

B. Protect

C. Respond

D. Identify

Answer: D

Question #:71

An Incident responder added a files NDS hash to the blacklist.

Which component of SEP enforces the blacklist?

A. Bloodhound

B. System Lockdown

C. Intrusion Prevention

D. SONAR

Answer: B

Question #:72

An Incident Responder wants to investigate whether msscrt.pdf resides on any systems.

Which search query and type should the responder run?

A. Database search filename “msscrt.pdf”

B. Database search msscrt.pdf

C. Endpoint search filename like msscrt.pdf

D. Endpoint search filename =“msscrt.pdf”

Answer: A

Question #:73

ATP detects a threat phoning home to a command and control server and creates a new incident. The treat is NOT being detected by SEP, but the Incident Response team conducted an indicators of compromise (IOC) search for the machines that are contacting the malicious sites to gather more information.

Which step should the Incident Response team incorporate into their plan of action?

A. Perform a healthcheck of ATP

B. Create firewall rules in the Symantec Endpoint Protection Manager (SEPM) and the perimeter firewall

C. Use ATP to isolate non-SEP protected computers to a remediation VLAN

D. Rejoin the endpoints back to the network after completing a final virus scan

Answer: C

Question #:74

A customer has information about a malicious file that has NOT entered the network. The customer wants to know whether ATP is already aware of this threat without having to introduce a copy of the file to the infrastructure.

Which approach allows the customer to meet this need?

A. Use the Cynic portal to check whether the MD5 hash triggers a detection from Cynic

B. Use the ATP console to check whether the SHA-256 hash triggers a detection from Cynic

C. Use the ATP console to check whether the MD5 hash triggers a detection from Cynic

D. Use the Cynic portal to check whether the SHA-256 hash triggers a detection from Cynic

Answer: C

Question #:75

An Incident Responder launches a search from ATP for a file hash. The search returns the results immediately. The responder reviews the Symantec Endpoint Protection Manager (SEPM) command status and does NOT see an indicators of compromise (IOC) search command.

How is it possible that the search returned results?

A. The search runs and returns results in ATP and then displays them in SEPM.

B. This is only an endpoint search.

C. This is a database search; a command is NOT sent to SEPM for this type of search.

D. The browser cached result from a previous search with the same criteria.

Answer: A

Question #:76

Which section of the ATP console should an ATP Administrator use to create blacklists and whitelists?

A. Reports

B. Settings

C. Action Manager

D. Policies

Answer: D

Question #:77

Which two tasks should an Incident Responder complete when recovering from an incident? (Choose two.)

A. Rejoin healthy endpoints back to the network

B. Blacklist any suspicious files found in the environment

C. Submit any suspicious files to Cynic

D. Isolate infected endpoints to a quarantine network

E. Delete threat artifacts from the environment

Answer: B E

Question #:78

An Incident Responder has reviewed a STIX report and now wants to ensure that their systems have NOT been compromised by any of the reported threats.

Which two objects in the STIX report will ATP search against? (Choose two.)

A. SHA-256 hash

B. MD5 hash

C. MAC address

D. SHA-1 hash

E. Registry entry

Answer: A B

Question #:79

What is the role of Vantage within the Advanced Threat Protection (ATP) solution?

A. Network detection component

B. Event correlation

C. Reputation-based security

D. Detonation/sandbox

Answer: A

Question #:80

A network control point discovered a botnet phone-home attempt in the network stream.

Which detection method identified the event?

A. Vantage

B. Insight

C. Antivirus

D. Cynic

Answer: C

Question #:81

What are the prerequisite products needed when deploying ATP: Endpoint, Network, and Email?

A. SEP and Symantec Messaging Gateway

B. SEP, Symantec Email Security.cloud, and Security Information and Event Management (SIEM)

C. SEP and Symantec Email Security.cloud

D. SEP, Symantec Messaging Gateway, and Symantec Email Security.cloud

Answer: C

Question #:82

An organization has five (5) shops with a few endpoints and a large warehouse where 98% of all computers are located. The shops are connected to the warehouse using leased lines and access internet through the warehouse network.

How should the organization deploy the network scanners to observe all inbound and outbound traffic based on Symantec best practices for Inline mode?

A. Deploy a virtual network scanner at each shop

B. Deploy a virtual network scanner at the warehouse and a virtual network scanner at each shop

C. Deploy a physical network scanner at each shop

D. Deploy a physical network scanner at the warehouse gateway

Answer: D

Question #:83

Which stage of an Advanced Persistent Threat (APT) attack do attackers send information back to the home base?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Answer: D

Question #:84

Why is it important for an Incident Responder to analyze an incident during the Recovery phase?

A. To determine the best plan of action for cleaning up the infection

B. To isolate infected computers on the network and remediate the threat

C. To gather threat artifacts and review the malicious code in a sandbox environment

D. To access the current security plan, adjust where needed, and provide reference materials in the event of a similar incident

Answer: D

Question #:85

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Answer: B

Question #:86

Which stage of an Advanced Persistent Threat (APT) attack do attackers map an organization's defenses from the inside?

A. Discovery

B. Capture

C. Exfiltration

D. Incursion

Answer: A

Question #:87

Which SEP technologies are used by ATP to enforce the blacklisting of files?

A. Application and Device Control

B. SONAR and Bloodhound

C. System Lockdown and Download Insight

D. Intrusion Prevention and Browser Intrusion Prevention

Answer: C

Question #:88

Which section of the ATP console should an ATP Administrator use to evaluate prioritized threats within the environment?

A. Search

B. Action Manager

C. Incident Manager

D. Events

Answer: B

Question #:89

What is the earliest stage at which a SQL injection occurs during an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Capture

D. Discovery

Answer: B

Question #:90

What are two policy requirements for using the Isolate and Rejoin features in ATP? (Choose two.)

A. Add a Quarantine firewall policy for non-compliant and non-remediated computers.

B. Add a Quarantine LiveUpdate policy for non-compliant and non-remediated computers.

C. Add and assign an Application and Device Control policy in the Symantec Endpoint Protection Manager (SEPM).

D. Add and assign a Host Integrity policy in the Symantec Endpoint Protection Manager (SEPM).

E. Add a Quarantine Antivirus and Antispyware policy for non-compliant and non-remediated computers.

Answer: A D

Question #:91

Which two steps must an Incident Responder take to isolate an infected computer in ATP? (Choose two.)

A. Close any open shares

B. Identify the threat and understand how it spreads

C. Create subnets or VLANs and configure the network devices to restrict traffic

D. Set executables on network drives as read only

E. Identify affected clients

Answer: A E

Question #:92

In which scenario would it be beneficial for an organization to eradicate a threat from the environment by deleting it?

A. The Incident Response team is identifying the scope of the infection and is gathering a list of infected systems.

B. The Incident Response team is reviewing detections in the risk logs and assigning a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

C. The Incident Response team completed their analysis of the threat and added it to a blacklist.

D. The Incident Response team is analyzing the file to determine if it is a threat or a false positive.

Answer: C

Question #:93

Which two database attributes are needed to create a Microsoft SQL SEP database connection? (Choose two.)

A. Database version

B. Database IP address

C. Database domain name

D. Database hostname

E. Database name

Answer: B D

Question #:94

Which action should an Incident Responder take to remediate false positives, according to Symantec best

practices?

A. Blacklist

B. Whitelist

C. Delete file

D. Submit file to Cynic

Answer: B

Question #:95

An ATP administrator is setting up correlation with Email Security cloud.

What is the minimum Email Security cloud account privilege required?

A. Standard User Role -Port

B. Standard User Role - Service

C. Standard User Role - Support

D. Standard User Role - Full Access

Answer: B

Question #:96

An organization recently deployed ATP and integrated it with the existing SEP environment. During an outbreak, the Incident Response team used ATP to isolate several infected endpoints. However, one of the endpoints could NOT be isolated.

Which SEP protection technology is required in order to use the Isolate and Rejoin features in ATP?

A. Intrusion Prevention

B. Firewall

C. SONAR

D. Application and Device Control

Answer: B