

Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/18/2022 2:59:33 pm • Time spent: 01:46

Score: 80%

Passing Score: 80%



▼ Question 1: ✓ Correct

Your browser has blocked you from your crucial secure intranet sites. What could be the problem?

- ➡ ☒ Your SSL certificate status has been revoked.
- ☐ You are using HTTP instead of HTTPS.
- ☐ You misconfigured a content filter.
- ☐ The firewall administrator set up a rule that blocked the users.

EXPLANATION

Your SSL certificate status has been revoked. CAs can revoke certificates for any number of reasons. Many browsers block websites with invalid certificates.

HTTP would not be possible when the websites are requiring SSL connectivity (HTTPS).

Content filtering is a strategy to keep employees from accessing unauthorized content on the web, not internally on intranet sites.

The firewall rule would only affect users going out to the internet or traffic flowing in. This would not apply to intranet sites within the corporate network.

REFERENCES

 12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_cert_secp7.question.fex

▼ Question 2: ✓ Correct

You would like to make sure users are not accessing inappropriate content online at work. Which endpoint security strategy would you employ?

- ➡ ☒ Content filtering
- ☐ Firewall rules
- ☐ Mobile device management (MDM)
- ☐ URL filters


EXPLANATION

You would choose content filtering. Online URL filtering is based on selected objectionable content. MDM doesn't provide content filtering.

Firewall rules usually pertain to data, not necessarily inappropriate content.

URL filters are for whitelisting and blacklisting sites. They are not used for filtering content.

REFERENCES

 12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_content_secp7.question.fex

▼ **Question 3:** ✓ Correct

You want to allow RDP 3389 traffic into your network for a group of users to access a particular workstation that has a special application in your office. Which endpoint security tool would you use to make this happen?

- ☐ URL filters
- ☐ Data monitoring apps
- ☐ Content filters
- ☒ Firewall rules

EXPLANATION

You would choose firewall rules to allow the traffic on port 3389 to the workstation on the private corporate network.

URL filters are a database of URLs that are allowed (whitelisted) or prohibited (blacklisted).

Content filtering is a strategy to keep employees from accessing unauthorized content on the web.

Data monitoring apps monitor data in all three states: at rest, in motion, and in use. However, this doesn't help you to allow traffic on port 3389.

REFERENCES



12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_firewall_secp7.question.fex

▼ **Question 4:** ✓ Correct

You need to remotely wipe an android phone for one of your rogue users. Which endpoint tool would you use?

- ➡ ☒ **Mobile device management (MDM)**
- ☐ Quarantining
- ☐ MAM-WE
- ☐ Mobile application management (MAM)

EXPLANATION

You would choose mobile device management (MDM). MDM offers a way to easily monitor and manage mobile devices. This includes updates, data encryption, and remote wipes of a compromised device.

MAM lets a system administrator publish, push, configure, secure, monitor, and update mobile apps. It does not provide options to remotely wipe a device.

MAM-WE is the same as MAM, but it includes enrollment into a third-party enterprise mobility management (EMM) provider. Sensitive data can be managed on any device, including personal devices.

Quarantining has to do with antivirus software finding a malicious item and isolating it or a network endpoint.

REFERENCES



12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_mdm_secp7.question.fex

▼ **Question 5:** ✓ Correct

This application endpoint-protection rule implicitly denies unless added to the rule. Which of the following processes describes this?

- ☐ Blacklisting
- ☐ Content filtering
- ☐ Quarantining
- ➡ ☒ Whitelisting

EXPLANATION

You would choose whitelisting. Whitelisting allows an IT admin to control the applications, IP addresses, URLs, and email addresses that are allowed onto the network. Whitelisting might mistakenly fail to list a needed application and interrupt workflow. Remember, whitelisting denies access until the item is added to the whitelist. This is called implicit deny. This is part of access control and is more strict than blacklisting.

Blacklisting lists the applications, IP addresses, URLs, email addresses, etc. that are to be blocked from the network.

Quarantining occurs when antivirus software finds a malicious item and quarantines it. This means that the item is placed in a folder where it cannot cause any damage to the network.

Content filtering is a strategy to keep employees from accessing unauthorized content on the web. Online URL filtering is based on selected objectionable content.

REFERENCES



12.2.2 Reconfigure and Protect Endpoints Facts

q_endpoint_prot_whitelisting_secp7.question.fex

▼ Question 6: **✕** Incorrect

You would like to enhance your incident-response process and automate as much of it as possible. Which of the following elements would you need to include? (Select two.)

- ☐ Blacklisting
- ➡ ☐ Playbooks
- ☐ Whitelisting
- ☒ Quarantining
- ➡ ☒ Runbooks

EXPLANATION

You would choose runbooks and playbooks. Runbooks are a condition-based series of protocols you can use to establish automated processes for security-incident response. A playbook is a checklist style document that specifies the steps to be taken in response to a threat or incident. The steps are listed in the order to be performed. A playbook ensures a consistent approach to security issues.

Whitelisting allows an IT admin to control the applications, IP addresses, URLs, email addresses, etc. that are allowed onto the network.

Blacklisting is the opposite of whitelisting.

Quarantining is when antivirus software finds a malicious item and quarantines it in a special folder.


REFERENCES

 12.2.4 Isolate and Containment Facts

q_isolate_contain_books_secp7.question.fex

▼ **Question 7:** ✓ Correct

You have detected and identified a security event. What's the first step you should complete?

- ☐ Segmentation
-  ☒ **Containment**
- ☐ Playbook
- ☐ Isolation

EXPLANATION

You would choose containment. Containment is the first step to complete after an event has been detected and identified.

Isolation limits the ability of a compromised process or application to do more harm to the network or its assets.

Segmentation is a strategic network design. The concept is simple: keep the sections of a network separated so that malicious actors cannot pivot within a network.

Playbooks are part of an incident-response plan. Playbooks can automate responses.

REFERENCES



12.2.4 Isolate and Containment Facts

q_isolate_contain_containment_secp7.question.fex

▼ **Question 8:** ✓ Correct

You need to limit a compromised application from causing harm to other assets in your network. Which strategy should you employ?

- ☐ SOAR
- ☐ Containment
- ☐ Segmentation
- ➡ ☒ Isolation

EXPLANATION

You would choose isolation. One way to protect the network is process isolation. This ensures that if a process is compromised, only the resources that are used by that process are at risk.

Segmentation is a strategic network design. The concept is simple-keep the sections of a network separated so that malicious actors cannot pivot within a network.

Containment is not a preemptive strategy. Containment is something you do after an event has occurred.

SOAR is a platform to compile security data generated by different security endpoints. This compiled information is then sent to a security analyst for further action.

REFERENCES




12.2.4 Isolate and Containment Facts

q_isolate_contain_isolation_secp7.question.fex

▼ Question 9:  Incorrect

You need to limit the impact of a security breach for a particular file server with sensitive company data. Which strategy would you employ?

- ☐ Containment
-  ☒ Segmentation
- ☐ SOAR
- ☐ Isolation

EXPLANATION

You would choose segmentation. You can segment using VLANs, software-defined networks, switches, subnetting, or even physical segmentation.

Isolation limits the ability of a compromised process or application to do more harm to the network or its assets.

Containment is the first step after an event has been detected and identified. Segmentation is preventative.

SOAR is a platform to compile security data generated by different security endpoints.


REFERENCES

12.2.4 Isolate and Containment Facts

q_isolate_contain_segmentation_secp7.question.fex

▼ Question 10: ✓ Correct

As a security analyst, you are looking for a platform to compile all your security data generated by different endpoints. Which tool would you use?

- ☐ GDPR
- ☐ MAM
-  ☒ **SOAR**
- ☐ MDM

EXPLANATION

You would choose SOAR (Security Orchestration, Automation, and Response). This compiled information is sent to a security analyst for further action. SOAR frees an analyst from constantly receiving security alerts as they are generated. Analysts can use parameters to automate solutions for security incidents that meet certain criteria.

An MDM is for managing mobile devices. It is not for all endpoints.

An MAM allows you to manage mobile apps on all sorts of devices, but it does not allow you to compile endpoint data.

GDPR (General Data Protection Regulation) is a framework in the EU for data protection and privacy.

REFERENCES

12.2.4 Isolate and Containment Facts

q_isolate_contain_soar_secp7.question.fex