Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE
100%

Defense in Depth

LATEST SUBMISSION GRADE
100%

1. Question — 1 / 1 point

How are attack vectors and attack surfaces related?

- An attack vector is the sum of all attack surfaces.
- They're not actually related.
- They're the same thing.
- (selected) An attack surface is the sum of all attack vectors.

Correct
Yep! An attack surface is the sum of all attack vectors in a system or environment.

2. Question — 1 / 1 point

Having detailed logging serves which of the following purposes? Check all that apply.

- [x] Event reconstruction

Correct
Exactly! Having logs allows us to review events and audit actions taken. If an incident occurs, detailed logs allow us to recreate the events that caused it.

- [x] Auditing

Correct
Exactly! Having logs allows us to review events and audit actions taken. If an incident occurs, detailed logs allow us to recreate the events that caused it.

- [ ] Vulnerability detection
- [ ] Data protection

Correct
Great, you got all the right answers.

3. Question — 1 / 1 point

Securely storing a recovery or backup encryption key is referred to as _____.

- Key obfuscation
- (selected) Key escrow
- Key backup
- Key encryption

Correct
That's right! Key escrow is the act of securely storing a backup or recovery encryption key for a full-disk-encrypted set up.

4. Question — 1 / 1 point

A hacker gained access to a network through malicious email attachments. Which one of these is important when talking about methods that allow a hacker to gain this access?

- An attack surface
- An ACL
- (selected) An attack vector
- A 0-day

Correct
Right on! An attack vector can be used by an attacker to compromise and gain unauthorized access to a system.

5. Question — 1 / 1 point

When looking at aggregated logs, you are seeing a large percentage of Windows hosts connecting to an Internet Protocol (IP) address outside the network in a foreign country. Why might this be worth investigating more closely?

- (selected) It can indicate a malware infection.
- It can indicate ACLs are not configured correctly.
- It can indicate log normalization.
- It can indicate what software is on the binary whitelist.

Correct
Well done! When looking at aggregated logs, you should pay attention to patterns and correlations between traffic. For example, if you are seeing a large percentage of hosts all connecting to a specific address outside your network, that might be worth investigating more closely, as it could indicate a malware infection.

6. Question — 1 / 1 point

Which of these protects against the most common attacks on the internet via a database of signatures, but at the same time actually represents an additional attack surface that attackers can exploit to compromise systems?

- Security Information and Event Management (SIEM) system
- Full disk encryption (FDE)
- Binary whitelisting software
- (selected) Antivirus software

Correct
Great work! Antivirus, which is designed to protect systems, actually represents an additional attack surface that attackers can exploit to compromise systems.

7. Question — 1 / 1 point

What is the purpose of application software policies? Check all that apply.

- [x] They serve to help educate users on how to use software more securely.

Correct
Nice job! Application policies serve to help educate users on how to use software more securely.

- [x] They define boundaries of what applications are permitted.

Correct
Nice job! Application policies define boundaries of what applications are permitted or not permitted.

- [ ] They take log data and convert it into different formats.
- [ ] They use a database of signatures to identify malware.

Correct
Great, you got all the right answers.

8. Question — 1 / 1 point

What is the combined sum of all attack vectors in a corporate network?

- The Access Control List (ACL)
- The risk
- The antivirus software
- (selected) The attack surface

Correct
Right on! An attack surface is the combined sum of all the various attack vectors that are present in a given system or environment.