30: Lab 30: Implementing allow lists and deny lists

Security+ (Exam SY0-701)

Congratulations, you passed!

Duration: 18 minutes, 16 seconds

☑ What are the Applocker primary conditions for enforcing or triggering a rule? (Select all that apply) *Score: 1*

- ☑ Publisher
- ☑ Path
- ☑ File hash
- ☐ File size
- ☐ Date and time

Congratulations, you have answered the question correctly.

☑ Which of the following statements are true in regards to AppLocker rules? (Select all that apply). *Score: 1*

- ☑ A hash rule denies execution if the file is renamed.
- ☐ A path rule denies execution if the file is renamed.
- ☐ A path rule denies execution if the file is moved to another directory.
- ☑ A hash rule denies execution if the file is moved to another directory.

Congratulations, you have answered the question correctly.

☑ What type of AppLocker rule can be bypassed by renaming or moving an executable file? *Score: 1*

- ○ File hash
- ○ Date and time
- ● Path
- ○ Publisher

Congratulations, you have answered the question correctly.

☑ The function being performed by AppLocker in this lab is generally known as? *Score: 1*

- ● Block listing
- ○ Allow listing
- ○ Grey listing
- ○ Secure listing

Congratulations, you have answered the question correctly.

☑ What access control options are available to block a user's ability to execute an application within Windows natively? (Select all that apply) *Score: 1*

☑ AppLocker
☑ NTFS permissions
☑ Remove the executable
☐ Change the filename
☐ Enable object access auditing

Congratulations, you have answered the question correctly.

☑ What type of security control denies execution unless the process is explicitly authorized? (Select all that apply) *Score: 1*

☑ allow list
☑ approved list
☐ deny list
☐ blocked list
☐ egress filter

Congratulations, you have answered the question correctly.

☑ Which of the following is a valid definition of a block list (or deny list)? *Score: 1*

● generally allows execution, but explicitly prohibits listed processes
○ denies execution unless the process is explicitly authorized
○ prevents access to only pre-authorized accounts
○ triggers a recording of events into a log file

Congratulations, you have answered the question correctly.