02: Lab 02 - Assisted - Configuring examples of security control types
Security+ (Exam SY0-701)

Congratulations, you passed!

Duration: 21 minutes, 24 seconds

☑ Who should have access to a share containing sensitive data like CertEnroll? *Score: 1*

- ○ Everyone
- ○ Administrators
- ○ Authenticated Users
- ◉ Only users with a role requirement for such data

Congratulations, you have answered the question correctly.

☑ Which of the following would be an effective method to directly block access to Rene and other similar users from accessing an admin-only resource? *Score: 1*

- ○ Create a new domain for non-administrative users
- ◉ Create the Non-admin group and make all non-admins a member
- ○ Set deny Full Control on the Everyone group
- ○ Create a clone object and set Deny on the Domain Users group

Congratulations, you have answered the question correctly.

☑ **check if the Everyone group has access to '\\10.1.16.1\CertEnroll' share** *Score: 1*
Select the **Score** button to validate this task:
```
No access for 'Everyone' to SMB Share 'CertEnroll'

Task complete
```

☑ **confirm if the C:\LABFILES\empty directory was deleted** *Score: 1*
Select the **Score** button to validate this task:
```
C:\LABFILES\empty deleted ...

Task complete
```

☑ The results of the find operation indicate what? *Score: 1*

- ○ Jamie is an administrator

- (●) Folder deletion is not being audited
- ( ) Users are unable to access empty folders
- ( ) User activity is being tracked

Congratulations, you have answered the question correctly.

☑ **confirm if the C:\LABFILES\pcaps directory was deleted and check for an event log record with an event ID of 4663 and an Object Name of C:\LABFILES** *Score: 1*

Select the **Score** button to validate this task:

```
C:\LABFILES\pcaps deleted ...

Event log record found with ID 4663 and Object Name C:\LABFILES\pcaps

Task complete
```

☑ What is the purpose of a detective control? *Score: 1*

- ( ) Deny access to an object
- ( ) Notify subjects about system policies
- ( ) Inform users of the proper steps to perform an activity
- (●) Create a record of events and activities

Congratulations, you have answered the question correctly.

☑ **confirm the existence of LegalNoticeCaption and LegalNoticeText registry keys with non-zero values $result = $False** *Score: 1*

Select the **Score** button to validate this task:

```
Registry keys LegalNoticeCaption and LegalNoticeText exist

Task complete
```

☑ What is the goal of directive controls? *Score: 1*

- ( ) Defense
- (●) Compliance
- ( ) Prohibition
- ( ) Tracking

Congratulations, you have answered the question correctly.

☑ What are the dual purposes of corrective controls? (Select two) *Score: 1*

- [x] Address an unwanted or less secure state or event
- [ ] Record evidence of user and event activities
- [x] Return the system to a normal and generally secure condition
- [ ] Provide guidance on proper user behavior

Congratulations, you have answered the question correctly.

☑ **confirm if the notes.txt file exists and contains "This is important"** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\notes.txt exists and contains 'This is important'

Task complete
```

☑ **confirm if C:\Users\jaime\hash.txt exists and is not empty** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\hash.txt exists

Task complete
```

☑ **confirm if the calchash.ps1 file exists and contains the "Get-FileHash" command** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\calchash.ps1 exists and contains the 'Get-FileHash' command

Task complete
```

☑ **confirm if the check.ps1 file exists and contains the "Get-Content" cmdlet** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\check.ps1 exists and contains the 'Get-Content' cmdlet

Task complete
```

☑ What is the typical means (which was used in this exercise) to detect changes in a file? *Score: 1*

- ○ encryption
- ○ authentication
- ○ authorization
- ◉ hashing

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of preventive controls? *Score: 1*

- ◉ Stop unwanted activity from succeeding
- ○ Record information about activities
- ○ Give instructions
- ○ Restore a system back to preferred condition
- ○ Persuade a perpetrator to go elsewhere
- ○ Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of detective controls? *Score: 1*

- ○ Stop unwanted activity from succeeding
- ◉ Record information about activities

- Give instructions
- Restore a system back to preferred condition
- Persuade a perpetrator to go elsewhere
- Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of directive controls? *Score: 1*

- Stop unwanted activity from succeeding
- Record information about activities
- Give instructions
- Restore a system back to preferred condition
- Persuade a perpetrator to go elsewhere
- Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of corrective controls? *Score: 1*

- Stop unwanted activity from succeeding
- Record information about activities
- Give instructions
- Restore a system back to preferred condition
- Persuade a perpetrator to go elsewhere
- Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the purpose of the dot and slash in front of the filenames in the PowerShell scripts and when executing PowerShell scripts? *Score: 1*

- Allow for administrator execution
- Reference the current working directory
- To set the security content of the process
- For avoiding detection by an IDS

Congratulations, you have answered the question correctly.