What group policies should be enabled to make sure that Powershell actions are logged and can be viewed in EventViewer?

1) Open the Group Policy Management console and create a new Group Policy Object.

2) The **Computer Configuration> Policies> Administrative Settings> Windows Components> Windows PowerShell** section contains options for enabling logging.

3) There are two main areas to focus on for PowerShell logging to the SIEM: "**Turn on Module Logging**" and "**Turn on PowerShell Script Block Logging.**" These two will both log PowerShell actions, however, are slightly different in what they log.

4) Using the **Turn on PowerShell Transcription** group policy, you can enable automatic logging of all PowerShell commands run and output results on the computer.

5) The **Turn on Script Execution** policy lets you configure the script execution policy, controlling which scripts are allowed to run.

6) To view the event log, go to **Programs and Services logs> Microsoft> Windows> PowerShell> Operating**.