Po wykonaniu tych kroków i eksperymentów z PowerShell'em oraz politykami AppLocker, uczniowie mogą wyciągnąć kilka istotnych wniosków:

1. **Zarządzanie politykami AppLocker**: Ćwiczenie pokazuje, jak można zarządzać politykami AppLocker za pomocą PowerShell'a, co umożliwia automatyzację procesu konfiguracji i zarządzania zasadami bez konieczności interakcji z interfejsem użytkownika.

2. **Wykorzystanie PowerShell do manipulowania politykami**: Uczniowie zdobędą doświadczenie w tworzeniu, modyfikowaniu i usuwaniu polityk AppLocker za pomocą cmdletów PowerShell'a, co może być przydatne w rzeczywistych scenariuszach zarządzania systemami Windows.

3. **Różne rodzaje reguł AppLocker**: Ćwiczenie prezentuje różne rodzaje reguł AppLocker, takie jak reguły oparte na wydawcy, sumach kontrolnych (hashach) plików, ścieżkach plików czy typach plików, co pozwala na bardziej elastyczne zarządzanie zabezpieczeniami aplikacji.

4. **Bezpieczeństwo i kontrola aplikacji**: Poznanie narzędzi takich jak AppLocker i umiejętność ich wykorzystania pozwala na lepsze zrozumienie i kontrolę nad tym, które aplikacje mogą być uruchamiane w środowisku Windows, co zwiększa bezpieczeństwo systemu.

5. **Alternatywne podejścia**: Ćwiczenie zawiera również alternatywne podejścia, takie jak korzystanie z zasad grupy w przypadku problemów z niektórymi cmdletami AppLocker, co pokazuje elastyczność podejścia do zarządzania zabezpieczeniami aplikacji.

Podsumowując, uczniowie zdobędą praktyczną wiedzę na temat konfiguracji i zarządzania politykami AppLocker w środowisku Windows przy użyciu PowerShell'a, co przygotuje ich do skutecznego zarządzania bezpieczeństwem aplikacji w organizacji.