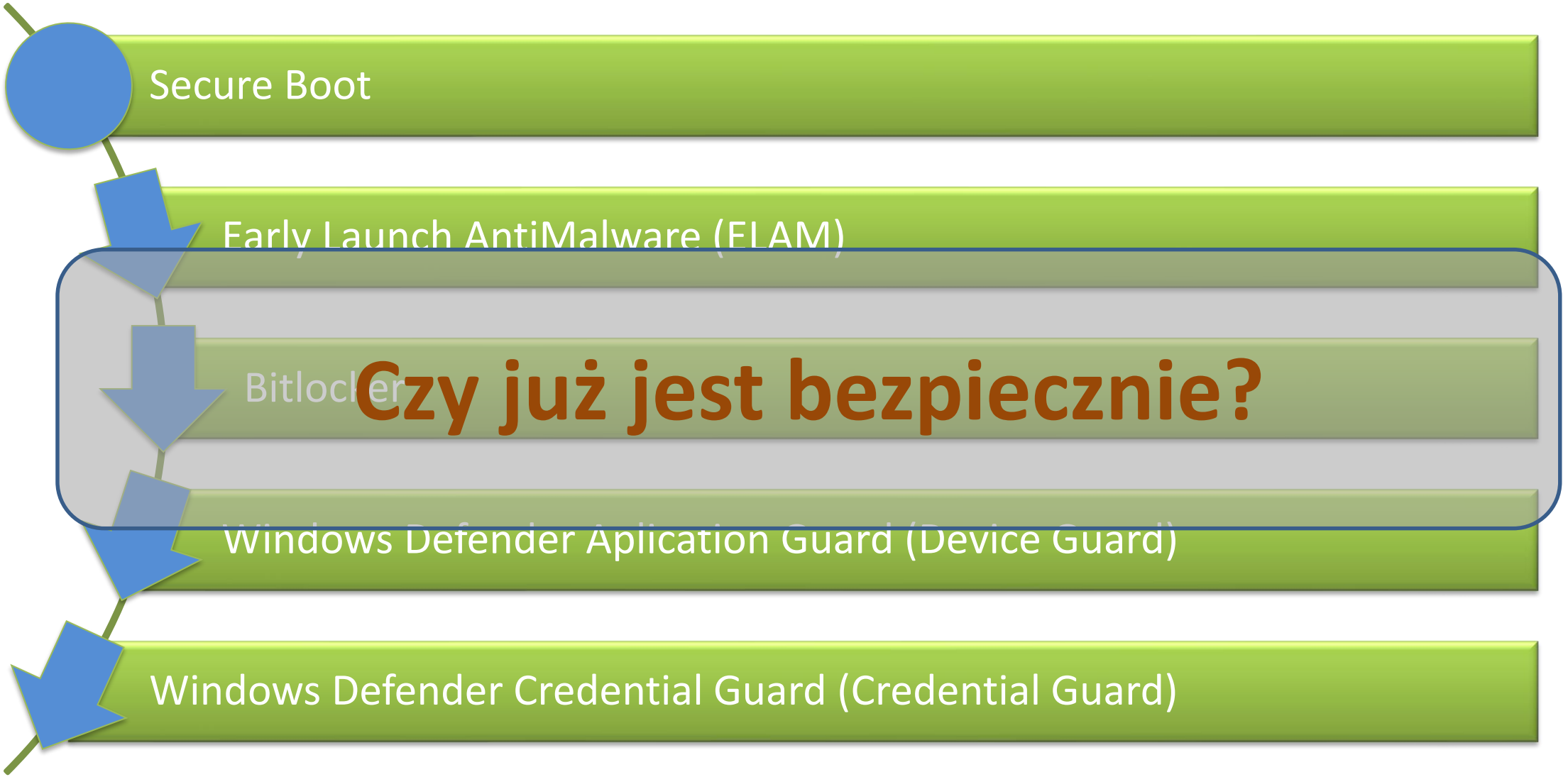
Windows Hello w przedsiębiorstwie

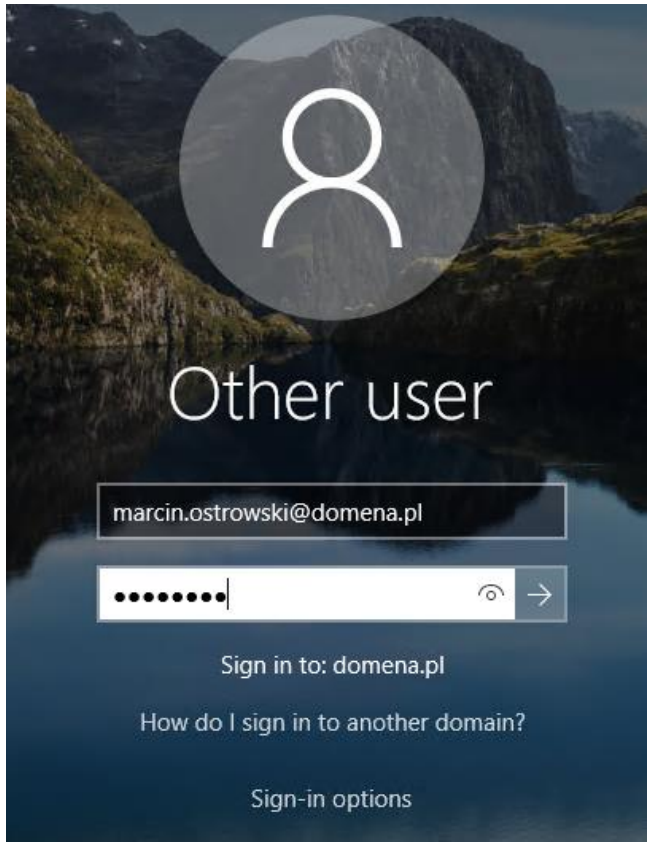
Marcin Ostrowski
marcin.ostrowski@cbsg.pl
MCT,MCSE,MCSA

Techniki zabezpieczania Windows 10



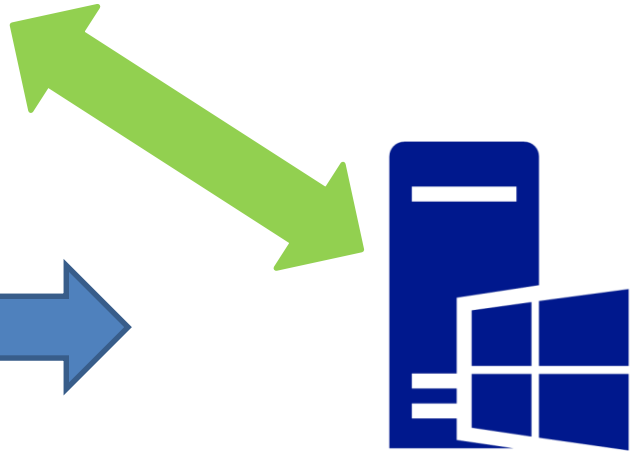
Jak zidentyfikować problem bezpieczeństwa?

Proces logowania przy użyciu hasła



Microsoft Active Directory

Dostęp do zasobów



Jan.Kowalski@domena.pl

W10001.domena.pl

\\FS001\Public

1) Konto komputera

2) Konto użytkownika

Windows Hello for Business – sposoby logowania

ITechDay

Logowanie za pomocą PIN – warunek konieczny

Dodatkowe możliwe sposoby logowania:

- za pomocą wzorca tęczówki
- odciskiem palca
- za pomocą kamery rozpoznającej twarz

Windows Hello for Business - wymagania

ITechDay

Acivte Directory Domain Service

- schemat domeny na poziomie Windows Server 2016 lub nowszym
- Group policy
- szablony administracyjne (ADMX) wersja 1703 lub nowsza

Active Directory Certificate Services

- wersja Windows Server 2012 lub nowsza
- Certificate Authority Web Enrollment
- Network Device Enrollment service

Active Directory Federation Services

- wersja Windows Server 2016 z zainstalowaną aktualizacją KB4022723
- włączona usługą rejestracji urządzeń

Windows 10

- wersja 1703 lub nowsza
- edycja Enterpise lub Education

Przykłady hasła i PIN

Hasło	PIN
Pa$$w0rd	Pa$$w0rd
AlaMakota	AlaMakota
010203	010203

PIN vs hasło

	Hasło	PIN
wymuszenie minimalnej długości	TAK - GPO	TAK - GPO
wymuszenie złożoności	TAK - GPO	TAK – GPO
miejsce przechowywania	ADDS/SAM	TPM/kontener
weryfikacja wzorca	NIE	TAK – tylko dla PIN opartego o cyfry
możliwość użycia po sieci	TAK	NIE – przechowywany lokalnie na urządzeniu

Windows Hello w działaniu ☺

DEMO

Warto przeczytać

Windows Hello for Business

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

Dziękuję ☺