Windows 10 Security & Audit

John Tannahill, CA, CISM, CGEIT, CRISC, CSX-P
jtannahi@rogers.com

Windows 10 Editions

- Home
- Pro
- Enterprise
- Education
- Mobile
- IoT Editions

Windows 10 Builds

- Windows 10 (initial version released July 2015)
- Windows 10 Version 1511
- Windows 10 Version 1607 and Windows Server 2016
- Windows 10 Version 1703
  - KB4015583 (OS Build 15063.138)
  - KB4016251 (OS Build 15063.13)
- winver

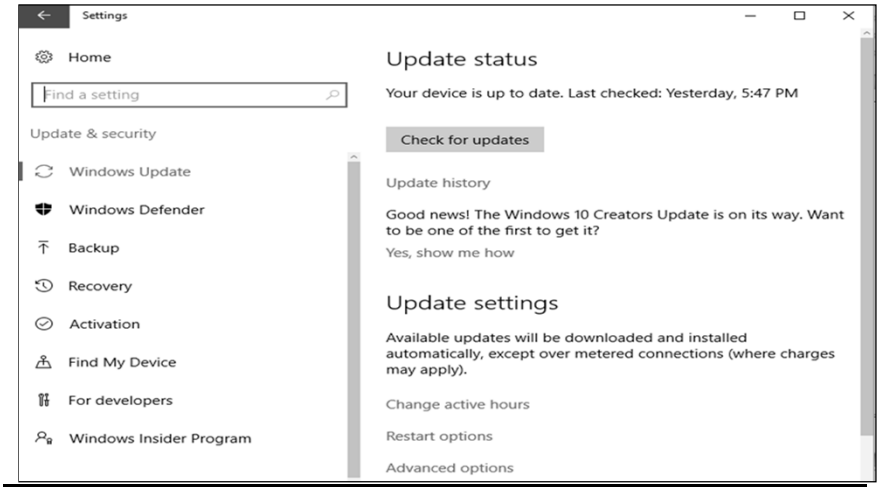
3

Windows 10 Creators Update

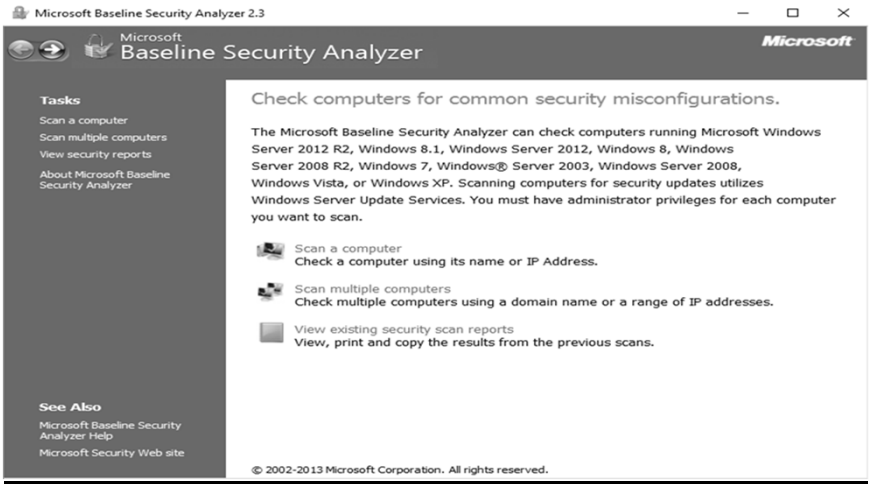
- 3D
- Game Streaming
- Microsoft Edge updates
- Store updates
- Cortana updates
- Security
  - Windows Defender Security Center
  - Dynamic Lock
- Privacy

4

Windows Update

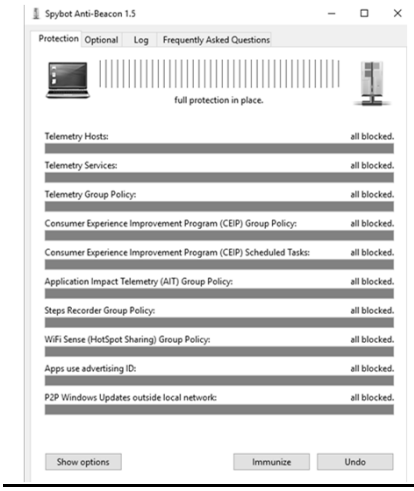


MBSA



6

Windows 10 Telemetry



7

Windows 10 Security Overview

- VBS Security
- Secure Boot
- Windows Hello
- Passport
- Credential Guard
- Device Guard
- Windows Defender
- User Access Control
- Security Event Logs
- Encryption
- Bitlocker
- Applocker
- Microsoft Edge Security

8

VBS Security

- Virtualization-based security technology
- Powers security features including Credential Guard and Device Guard
- **Pass The Hash Attack Mitigation**

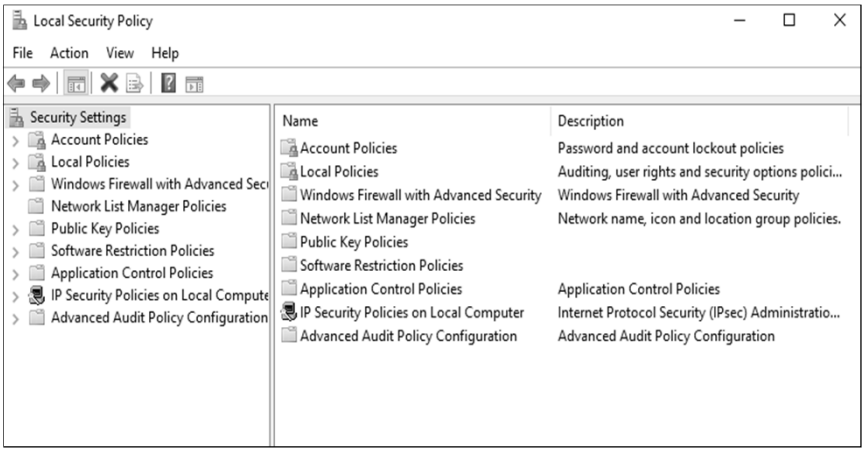
9

Secure Boot

- Unified Extensible Firmware Interface (UEFI) Secure Boot
- Checks OS loader and drivers to ensure signed by an approved digital signature
- Prevents low-level malware e.g. rootkits interfering with the boot process
- Disabling Secure Boot

10

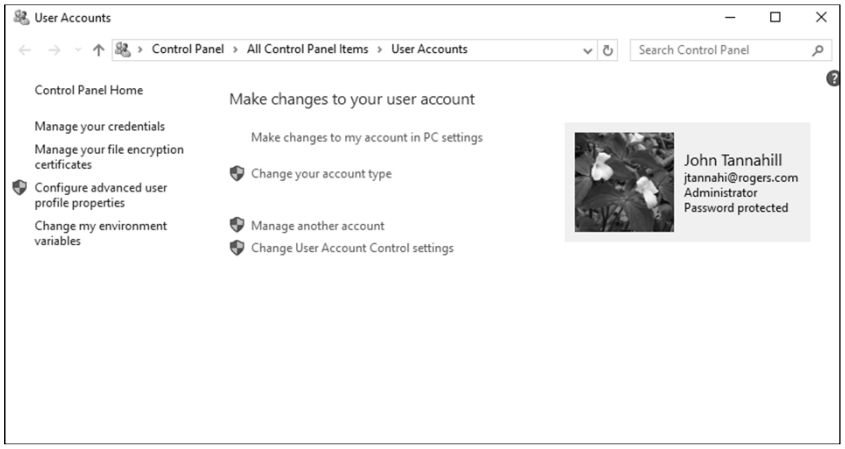
Local Security Policy



Windows 10 in a Windows Domain

- OU Design
  - Windows 10 Users OU
  - Windows 10 Computers OU
- GPO Design
  - Baseline Security settings

User Accounts and Passwords



13

Windows Hello

- Windows Hello - biometrics to allows sign in to devices, apps, online services, and networks
- Face, iris, fingerprint
- Dynamic Lock

14

Passport

- Single Sign-in to services
- Two factor Authentication
  - Windows Hello

15

Credential Guard (source: Microsoft)

- Introduced in Windows 10 Enterprise and Windows Server 2016
- Credential Guard uses VBS to isolate secrets so that only privileged system software can access them
- Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket **(e.g. MimiKatz)**
- Credential Guard prevents attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

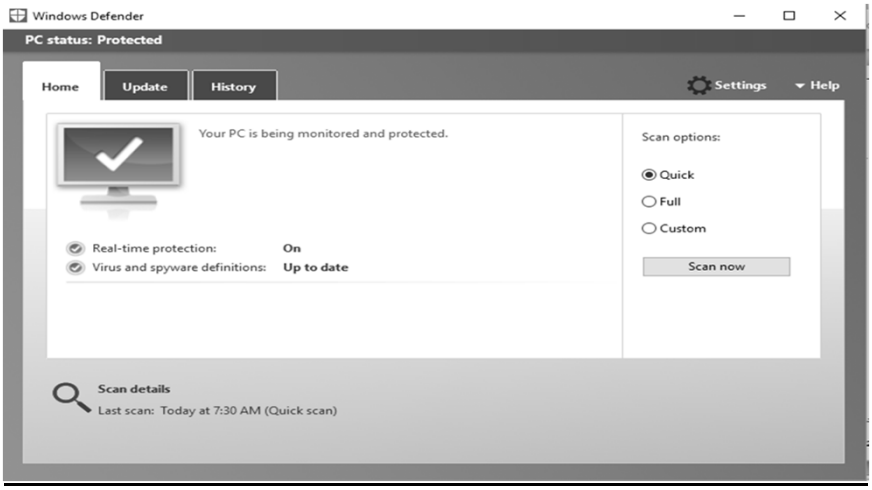
16

Device Guard

- Hardware and software security features lock a device down so that it can only run trusted applications
- Code integrity policy (one per device)
- Untrusted apps cannot run
- AppLocker replacement
- Uses Virtual Secure Mode (VSM) to isolate the Code Integrity service from the Windows kernel

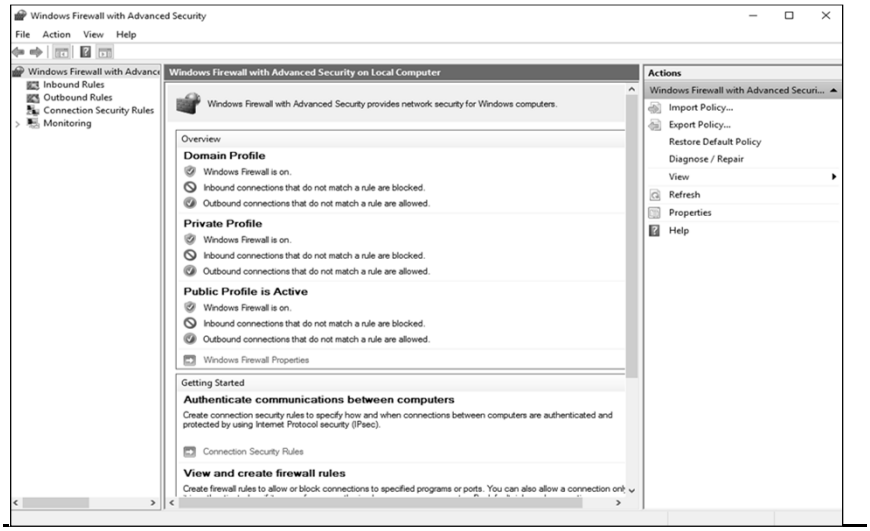
17

Windows Defender



18

Windows Firewall

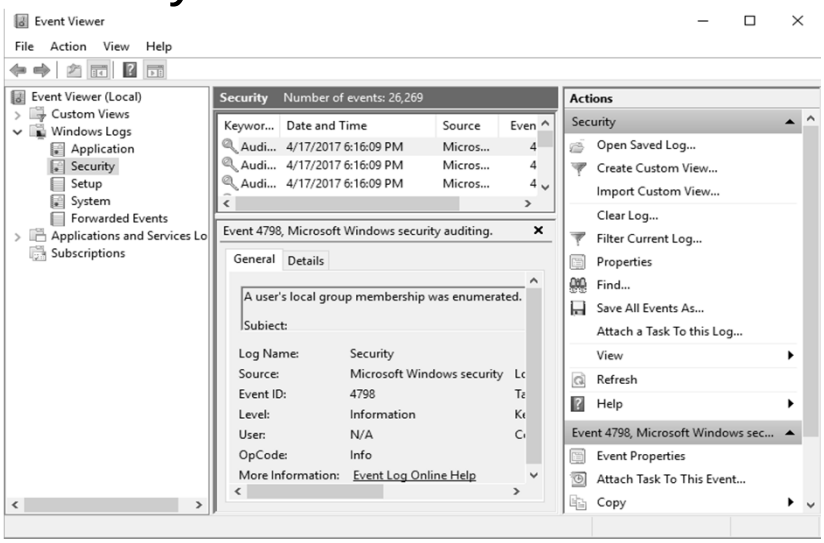


Firewall Configuration

- Netsh command
- netsh advfirewall show allprofiles
- netsh advfirewall set allprofiles state on
- netsh advfirewall firewall add rule name="TCP Port 80" dir=in action=allow protocol=TCP localport=80
- netsh advfirewall firewall add rule name="TCP Port 80" dir=out action=allow protocol=TCP localport=80

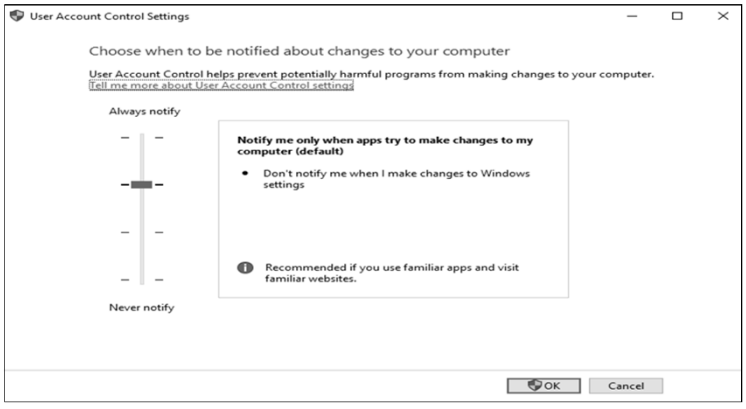
20

Security Events



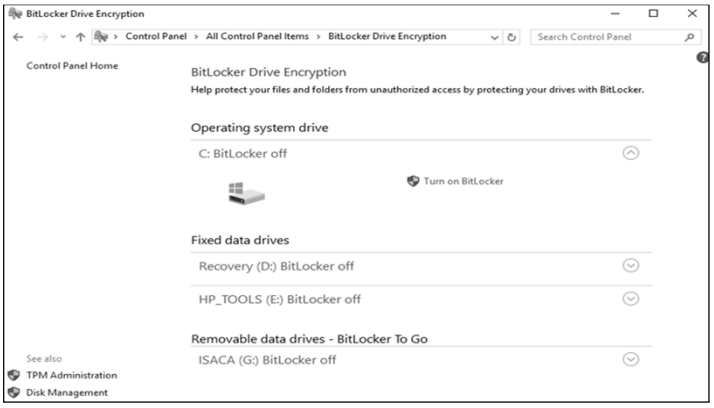
User Account Control (UAC)

- UAC used for malware mitigation



Enterprise Features

- BitLocker Drive Encryption
- Network Access Protection

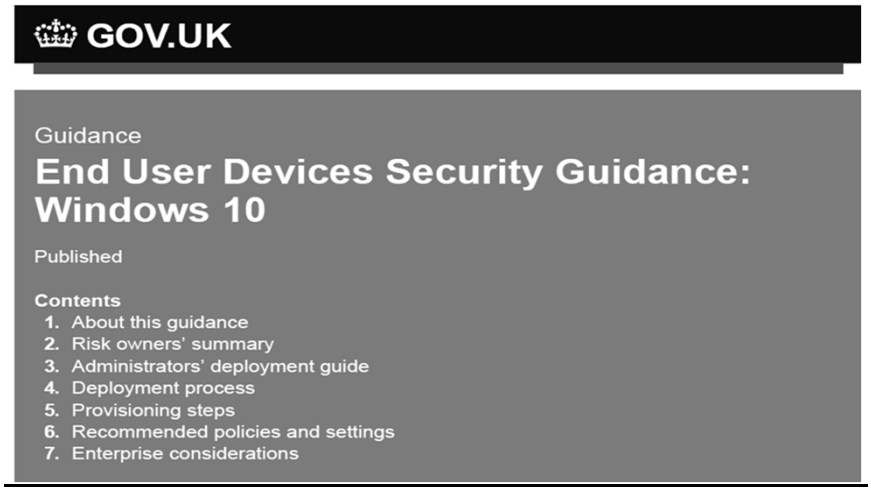


Microsoft Edge Security

- Note: Windows 10 has two built-in browsers (Edge and IE 11)
- Legacy Browser Helper Objects such as ActiveX, Java etc. removed
- AppContainer
- Private Browsing
- Advanced Settings

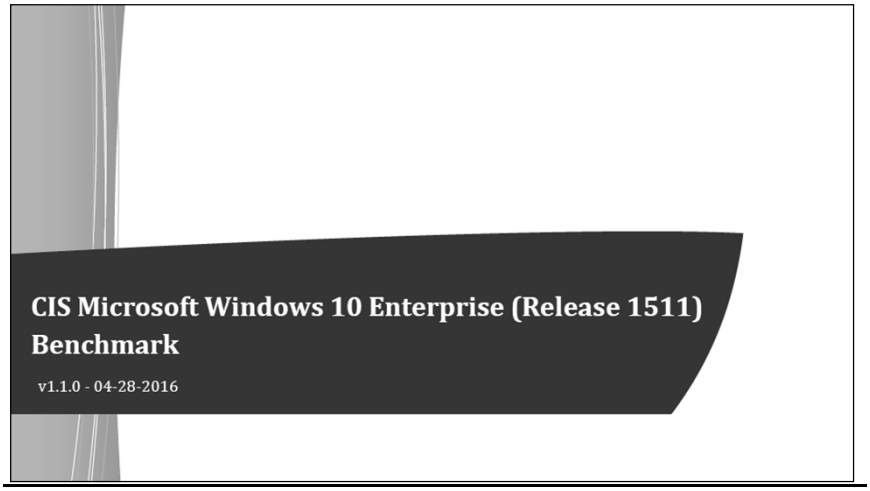
24

GOV.UK Security Guidance



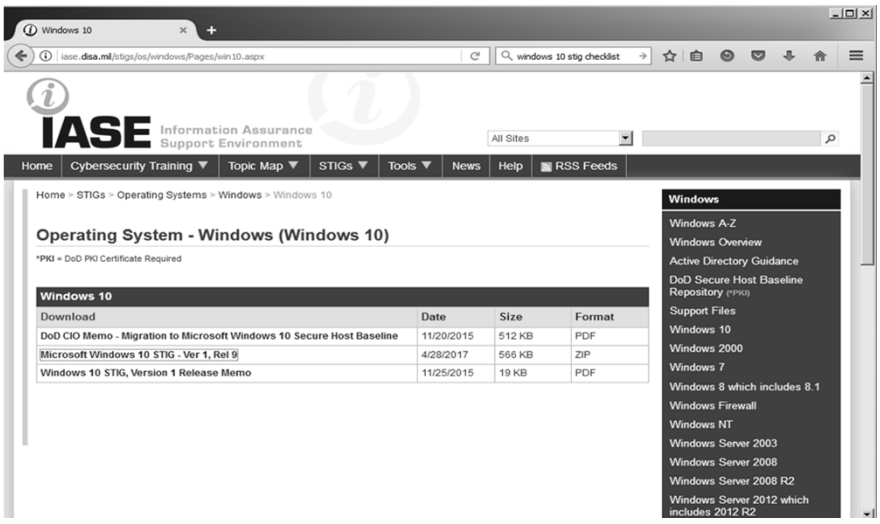
25

Windows 10 CIS Benchmark (cisecurity.org)



26

Windows 10 STIG



Key Audit Areas

- Deployment
  - Image Build Process
- Configuration
  - Applications; Firewall; Anti-Virus; Anti-Malware
- Security Hardening
  - Group Policy Objects (GPO)
- Update Management Process
  - Windows Update

Audit Tools

- Powershell
- netsh
- net commands
- netstat –ano (Network Services and Mapping to Processes)
- icacls (Directory & File Permissions)
- Sysinternals Suite
  - available from Microsoft site

Summary

- New security features of Windows 10
- Active Directory Deployment & Security
  - Understand GPO Mechanism
- Understand Client Endpoint Risks
  - Threat Landscape
  - Key Mitigation Strategies