INFRASTRUCTURE SUMMIT 2019

Secure and stay secure using Security Baselines in the real world

Johan Arwidmark
Technical Fellow

Peter Lofgren
Senior Technical Architect

Get-Experts -Category Security

Johan Arwidmark	👤	Peter Lofgren
@jarwidmark	🐦	@LofgrenPeter
johan@2pintsoftware.com	✉	peter.lofgren@truesec.com
Microsoft MVP	🏆	Tallest Truesec Member
Should not eat Pizza	🍕	Eats to much pizza

Security Baselines - Agenda

- What and why Security Baselines
- Group policy is not dead
- Security Compliance Toolkit
- In an all cloud world, Intune to the rescue
- Microsoft Endpoint Manager is the way forward

What and why Security Baselines

WHAT

- Common practices for security
- Enterprise devices
- Microsoft recommendations

WHY

- Staying secure
- Eliminating “this looks like a good setting”
- Keeping up to date

Security Levels

- Define where you are today
- Level 1 – Basic
- Level 2 - Enhanced
- Level 3 - High
- Level 4 - Dev/ops workstation
- Level 5 – Administrator / PAW

LEVEL
1
Enterprise Basic Security
LEVEL
2
Enterprise Enhanced Security
LEVEL
3
Enterprise High Security
LEVEL
4
Specialized Workstation
LEVEL
5
Administrator Workstation

Level 1

- Enterprise Basic Security configuration
  - Trusted Platform Module (TPM) 2.0
  - BitLocker Drive Encryption
  - UEFI Secure Boot
  - Drivers and Firmware Distributed through Windows Update

Level 2

- Enterprise Enhanced Security configuration
  - Virtualization and HVCI Enabled

    Hypervisor Code Integrity Enabled
  - Drivers and Apps HVCI-Ready

    Hypervisor Code integrity ready (signed sealed delivered)
  - Windows Hello
  - DMA I/O Protection

Level 3

- Enterprise High Security configuration

  - System Guard

    Protect and maintain the integrity of the system as it starts up

    Validate that system integrity has truly been maintained through local and remote attestation

  - Modern Standby

  Previously known as connected standby provides and “always on” experience

Group policy is not dead

- Group policy is not a modern tool
  - BUT you already have this!
- Creating the foundation for a smooth process
- Importing the baselines
- Using “as-is” or modifying

TRUESEC

Demo: Group Policy importing, linking and tweaks

Security Compliance Toolkit (SCT)

- Tools aimed at enterprise security administrators
  - For Download, Analyze, Test, Edit, Store
  - Policy Analyzer tool
  - Local Group Policy Object (LGPO) tool
- Windows 10 security baselines
- Windows Server security baselines
- Microsoft Office security baseline

TRUESEC

Demo: Security Compliance Toolkit

Intune

- Prerequisites: Windows 10 version 1809 and later
- Preview is supported, almost!
- Easier process
- Can be extended!
- Defender ATP Baselines are not ATP only

TRUESEC

Demo: Intune Baselines

Microsoft Endpoint Manager

- MEMCM
- Configuration Items
- Configuration Baselines
- GPO to Configuration Item Conversions

TRUESEC

Demo: Microsoft Endpoint Manager

TRUESEC

Questions