Enhancing Your Workstation Security Using Windows 10 Group Policies

And other essential Windows 10 Security tips

Session 1132

ILTACON 2018

SPEAKER

James Engelhard

Chief Technology Officer

Helient Systems LLC

INTRO AND SESSION OVERVIEW

- What are the Threat Types?
- What are the Attack Vectors?
- How is Windows Addressing Security in Windows 10?
- How can You Secure Your Systems Using Group Policy?
- How can You Ensure Compliance with Security “Best Practices”?
- How can You Address Evolving Threats and Recommendations?

PART 1: YOU ARE UNDER ATTACK

ATTACK TYPES & VECTORS

WINDOWS DEFENDER CAN HELP

Wait, What?!?!?

PART 2: DEFEND YOURSELF!

YOUR HARDWARE PLAYS A PART

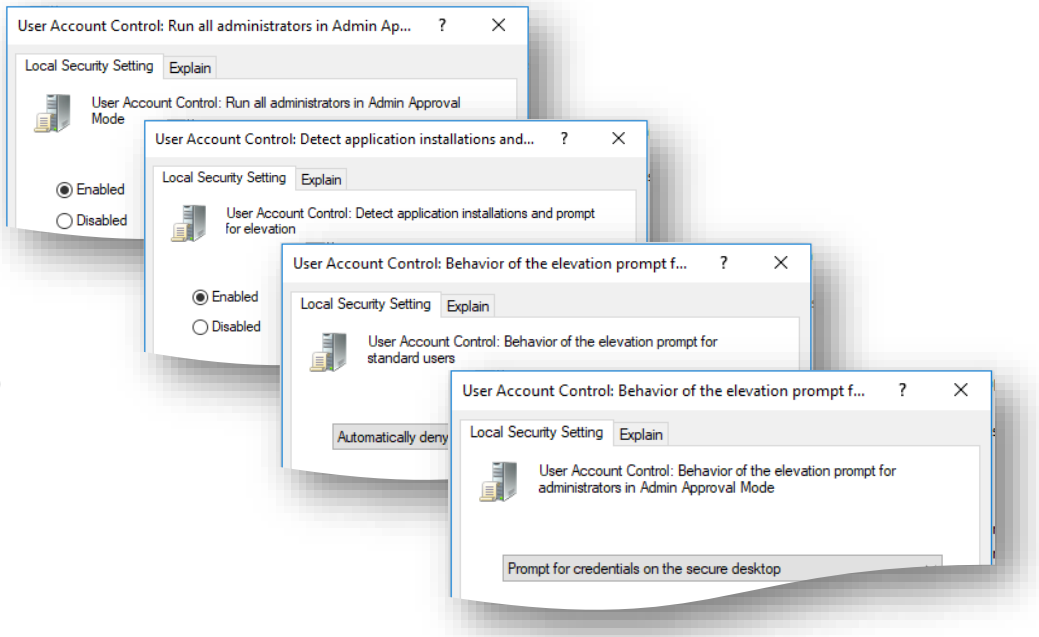
A BIG part!

VIRTUALIZATION BASED SECURITY

SECURING AUTHENTICATION & CREDS

SECURING THE OS AND CONFIGURATION

- User Account Control
  - Always prompt
- Run with Least Required Privileges
  - Never login as an admin (neither Domain nor Local)
  - Elevate when needed
  - Tiered Elevation



Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

SECURING THE OS

with WDAV; WDAC; WDAG and other exploit protection

PART3: MAINTAIN YOUR DEFENSES

MICROSOFT SECURITY COMPLIANCE TOOLKIT (SCT)

- Replaces the Microsoft Security Compliance Manager
- A Collection of Tools and Assets for Evaluating and Securing Windows 10 According to Microsoft Recommendations
- Policy Analyzer
- LGPO
- Policy Rules and Sample Policies

MICROSOFT SECURITY COMPLIANCE TOOLKIT

ILTACON 2018

DEMO: SCT IN PRACTICE

Using the Security Compliance Toolkit to Audit and Maintain a Secure Desktop

Q&A

ILTACON 2018