Building a Secure Client

Mattias Borg

IT Security Specialist, SBAB Tech

Certified Ethical Hacker

@mattiasborg82

Stefan Schörling

Microsoft MVP

@stefanschorling

Definition of a Secure Client

There is no such thing…….

But what we can do is to build a Client that is somewhat resistant to modern threats and capable of detecting possible threats and compromises

Hardware

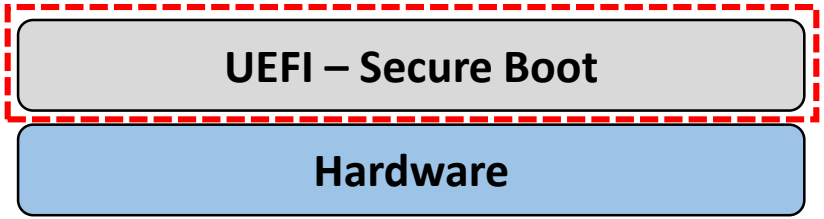
- UEFI
- TPM 2.x
- Windows Hello Support
  - Fingerprint Reader
  - Camera
- Microsoft - Hardware Security Testability Specification

https://msdn.microsoft.com/en-us/library/windows/hardware/mt712332.aspx

Hardware

UEFI – Secure Boot

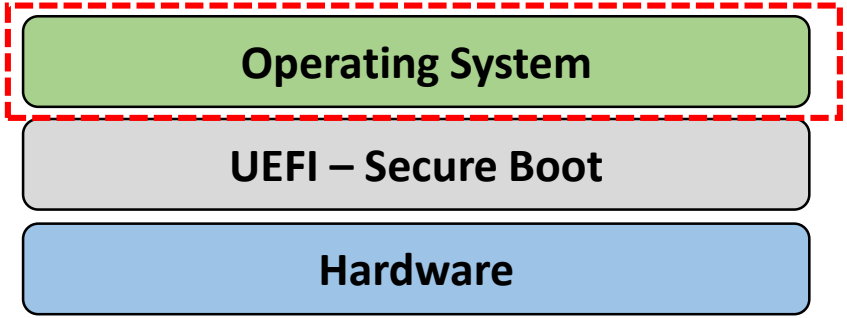
- UEFI
- TPM 2.x
- Boot Order
- Password
- Secure Boot
- Maintain and Update
- Lockdown UEFI Config
- WAN/LAN Switching



http://www.intelsecurity.com/resources/pr-bios-secure-boot-attacks-uncovered.pdf
http://www.uefi.org/learning_center/presentationsandvideos
https://msdn.microsoft.com/en-us/library/windows/hardware/mt712332.aspx

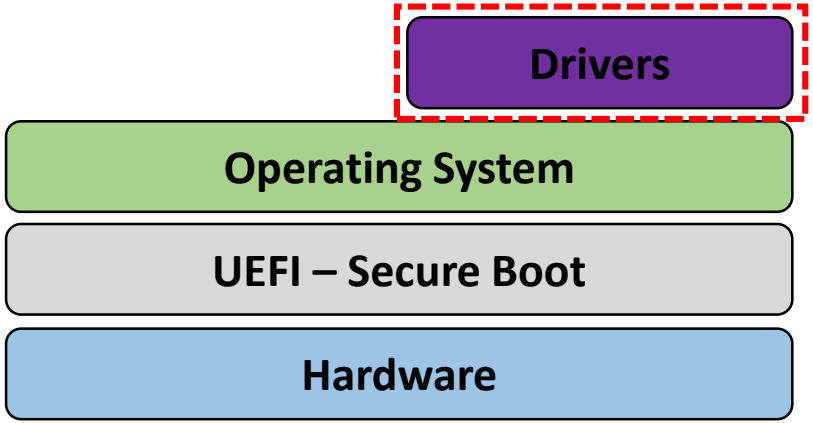
Operating System

- Best Practices
  - Secure Deployment
  - Patched Image
  - Enabled Features for Security
    - Credential Guard
    - Device Guard
  - F8 Support
  - Untrusted Fonts
  - Auditing
  - IPSEC



Drivers

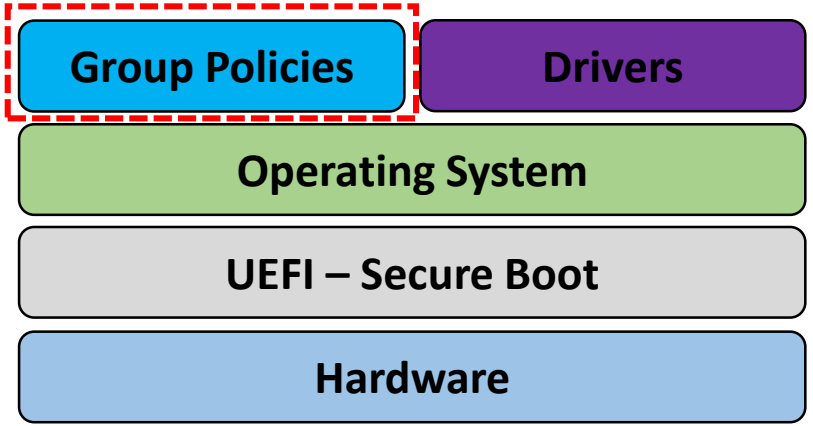
- Signed Drivers
- Certification Checklist



Group Policies

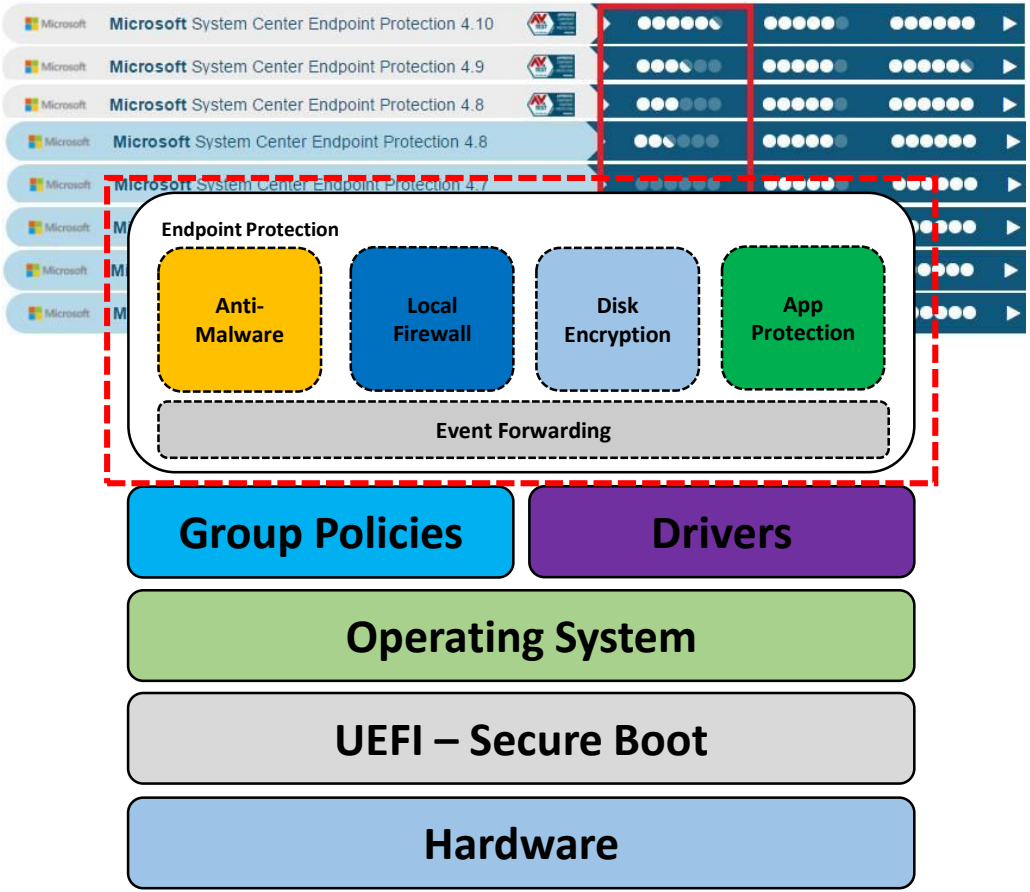
- Use Baselines
- Evaluate Security Settings
- Security Compliance Manager
  - Evaluate with Desired State

https://technet.microsoft.com/en-us/itpro/windows/manage/new-policies-for-windows-10
https://www.microsoft.com/en-us/download/details.aspx?id=53353



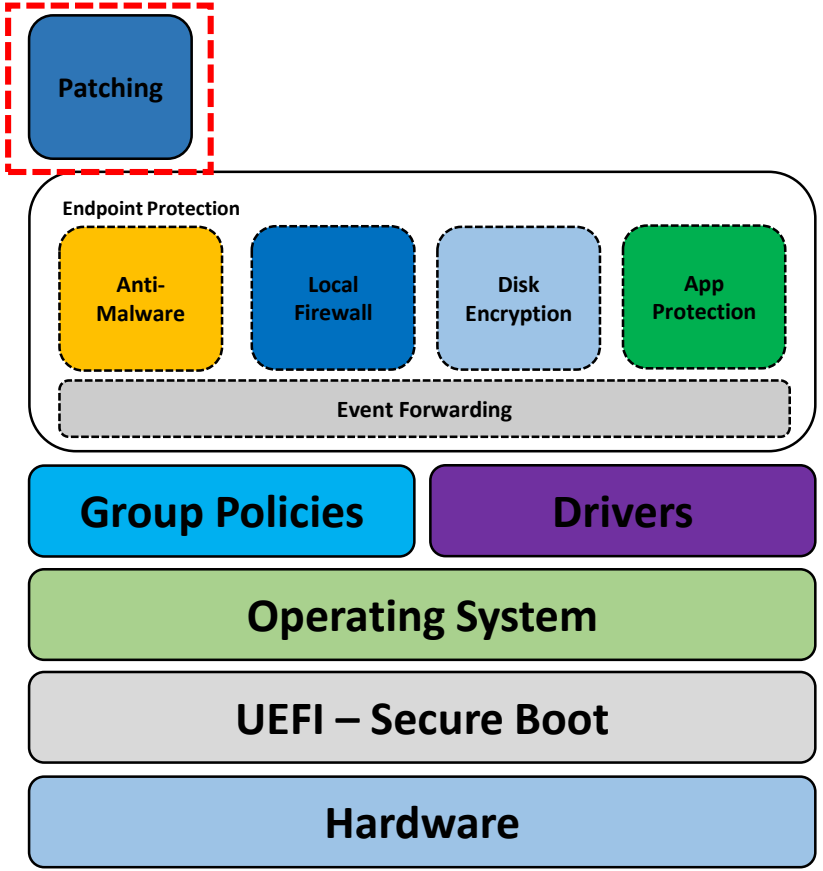
Endpoint Protection

- Antimalware
- Local Firewall
- Disk Encryption
  - Algorithm
  - Pre Boot - DMA
  - Key Replacement
  - Auditing
- App Protection
  - App Locker
- Event Forwarding



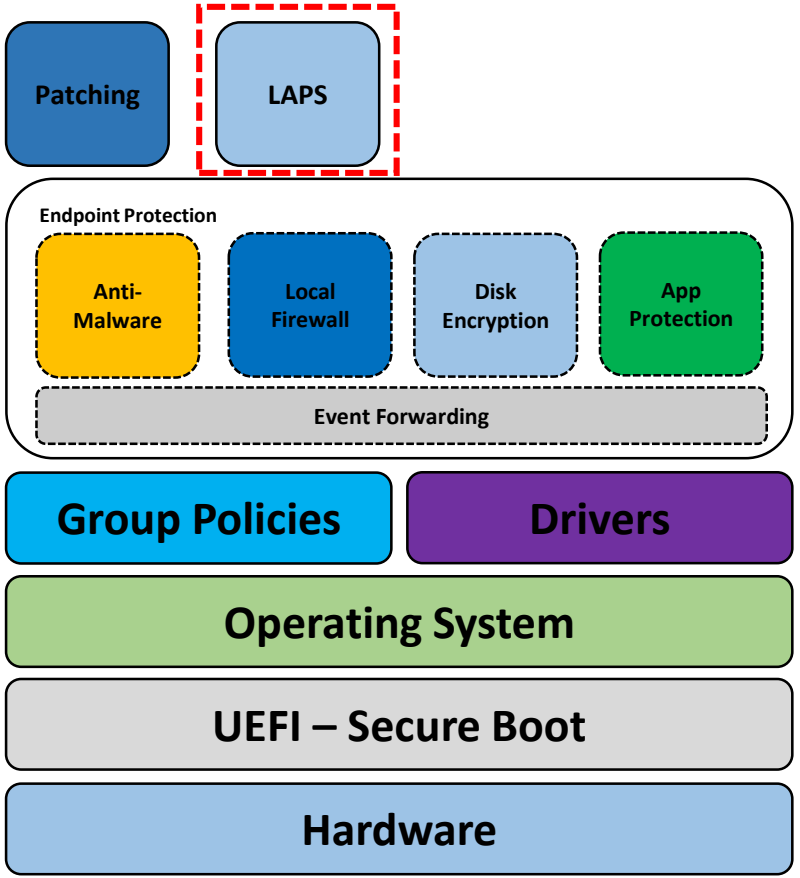
Patching

- Microsoft
  - Products
  - Categories
- 3rd Party
  - Secunia
  - Shavlik
  - Etc
- MBSA



LAPS

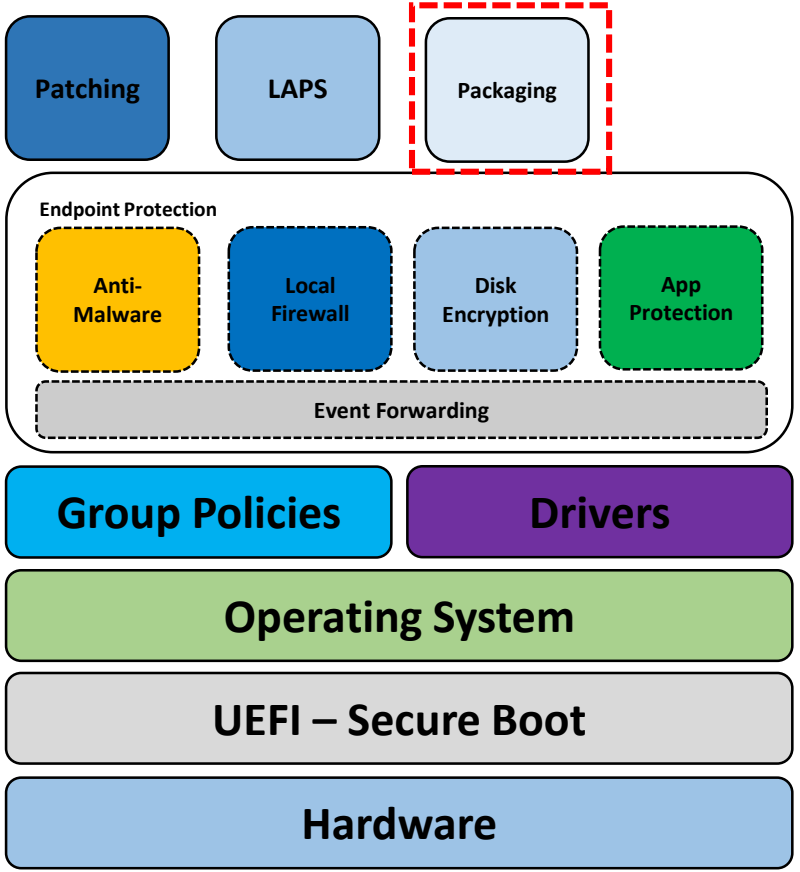
- Local Administrator Password Solution
  - Components
    - Active Directory
    - GPO
    - LAPS Agent
  - Benefits
    - PTH Mitigation
    - Secure Password Management



https://technet.microsoft.com/en-us/mt227395.aspx
https://www.microsoft.com/en-us/download/details.aspx?id=46899

Packaging

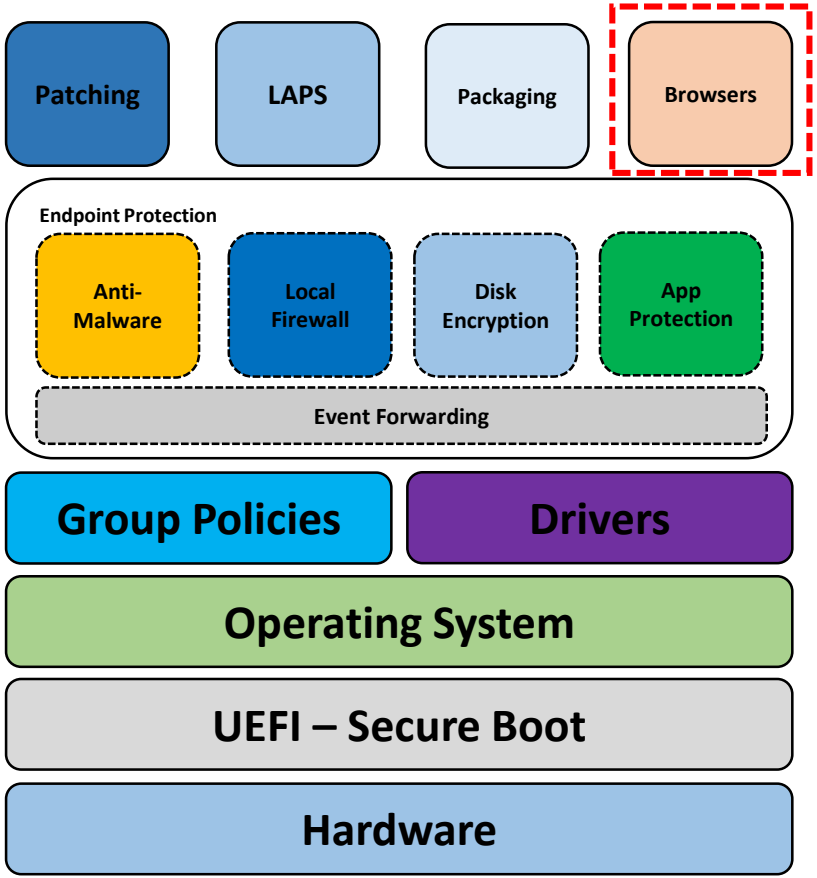
- Microsoft MSI Packaging Guidelines
- Privilege Escalation
  - Windows-privsec-check
    - Missing “” in Service Path
      - C:\Program Files\IDT\WDM\STacSV.exe
      - C:\Program.exe



https://msdn.microsoft.com/en-us/library/windows/desktop/bb204770(v=vs.85).aspx
https://github.com/pentestmonkey/windows-privesc-check

Browsers

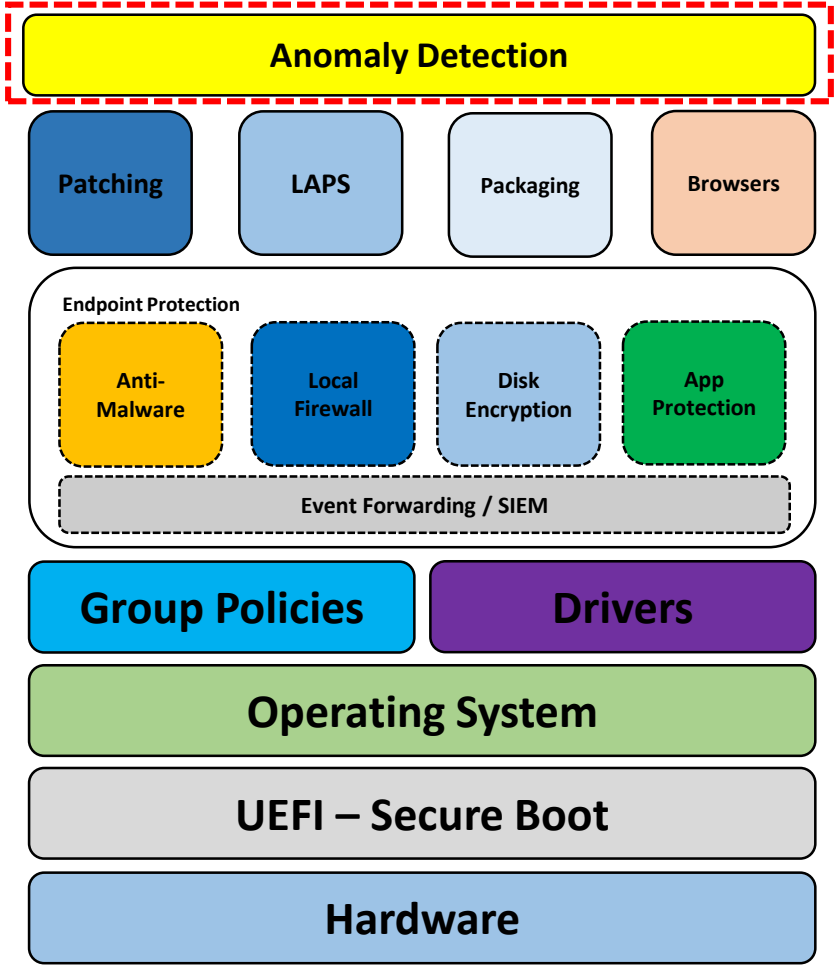
- Native Browsers
  - Group Policies
  - Edge application Guard
  - Smart Screen
- 3rd Party Browsers
  - Chrome
  - Firefox



https://www.us-cert.gov/publications/securing-your-web-browser
https://blogs.windows.com/msedgedev/2016/09/27/application-guard-microsoft-edge/
https://docs.google.com/document/d/1iu6I0MhyrvyS5h5re5ai8RSVO2sYx2gWI4Zk4Tp6fgc/edit
https://blogs.windows.com/msedgedev/2015/12/16/smartscreen-drive-by-improvements/#HE5XfCofMiy1S7QM.97

Anomaly Detection

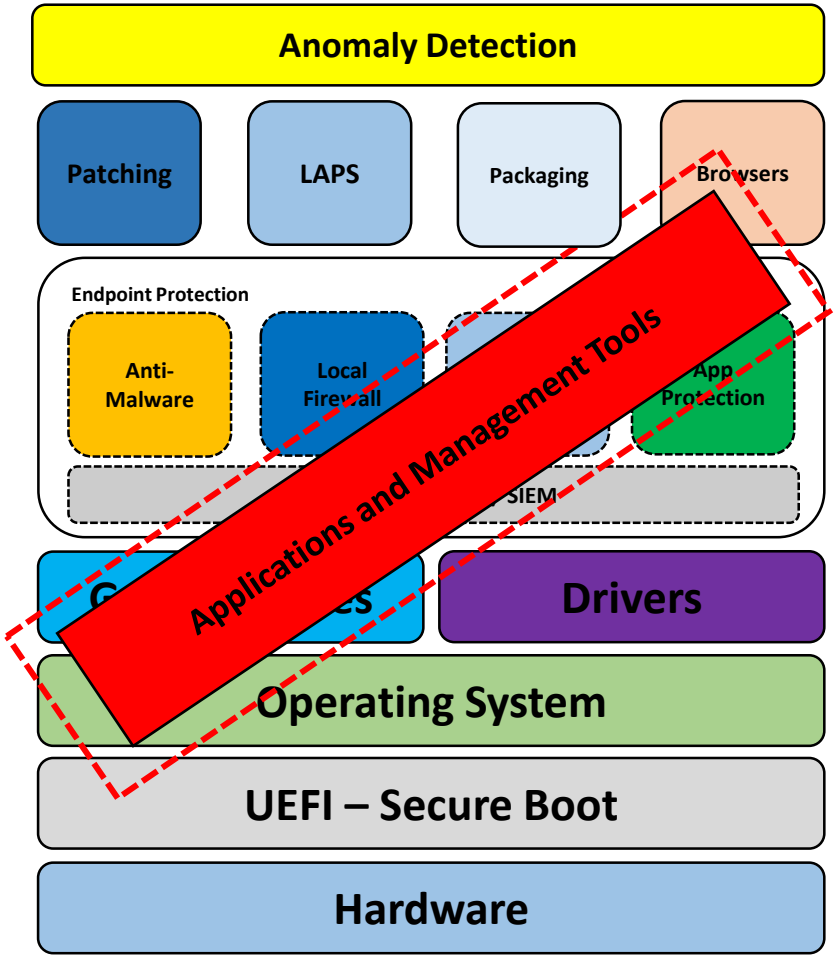
- Microsoft
  - Defender ATP
  - Sysinternals Sysmon
- 3rd Party
  - Cisco AMP
  - FireEye



https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp

Applications

- Office
- Antivirus
- SCOM
- SCCM
- Etc



Working with Client Security

- Vulnerability Scanning
- Penetration Testing
- Threat modelling
- Active Monitoring
- KPIs

Links and references

- Windows 10 Security Baselines
  - https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-security-baselines
- Security Compliance Manager 4.0
  - https://www.microsoft.com/en-us/download/details.aspx?id=53353
- Active Monitoring
- KPIs
- NIST - www.nist.gov
- CERT.SE - www.cert.se

System Center User Group

www.scug.se

www.youtube.com/scugse

#scugse