Deploy the Microsoft Security Baseline!

Notes from the field

Thomas Kurth, Consultant
www.wpninjas.ch
@ThomasKurth_ch

About Thomas Kurth

Focus

Microsoft EM&S
MEMCM
MTP

Working at

baseVISION
SECURE & MODERN WORKPLACE

My Blog

https://wpninjas.ch

Certifications

Microsoft MVP Most Valuable Professional

Microsoft 365 Certified Enterprise Administrator Expert

Microsoft Certified Trainer MCT Trainer 2019 - 2020

C|EH Certified Ethical Hacker

Hobbies

Rollhockey
Coding

Contact

Twitter: @ThomasKurth_ch
Mail: thomas.kurth@basevision.ch

Thanks to our Sponsors!

ACP IT for innovators.

Microsoft

NiCE
IT Management Solutions
www.nice.de

THOMAS KRENN®

VEEAM

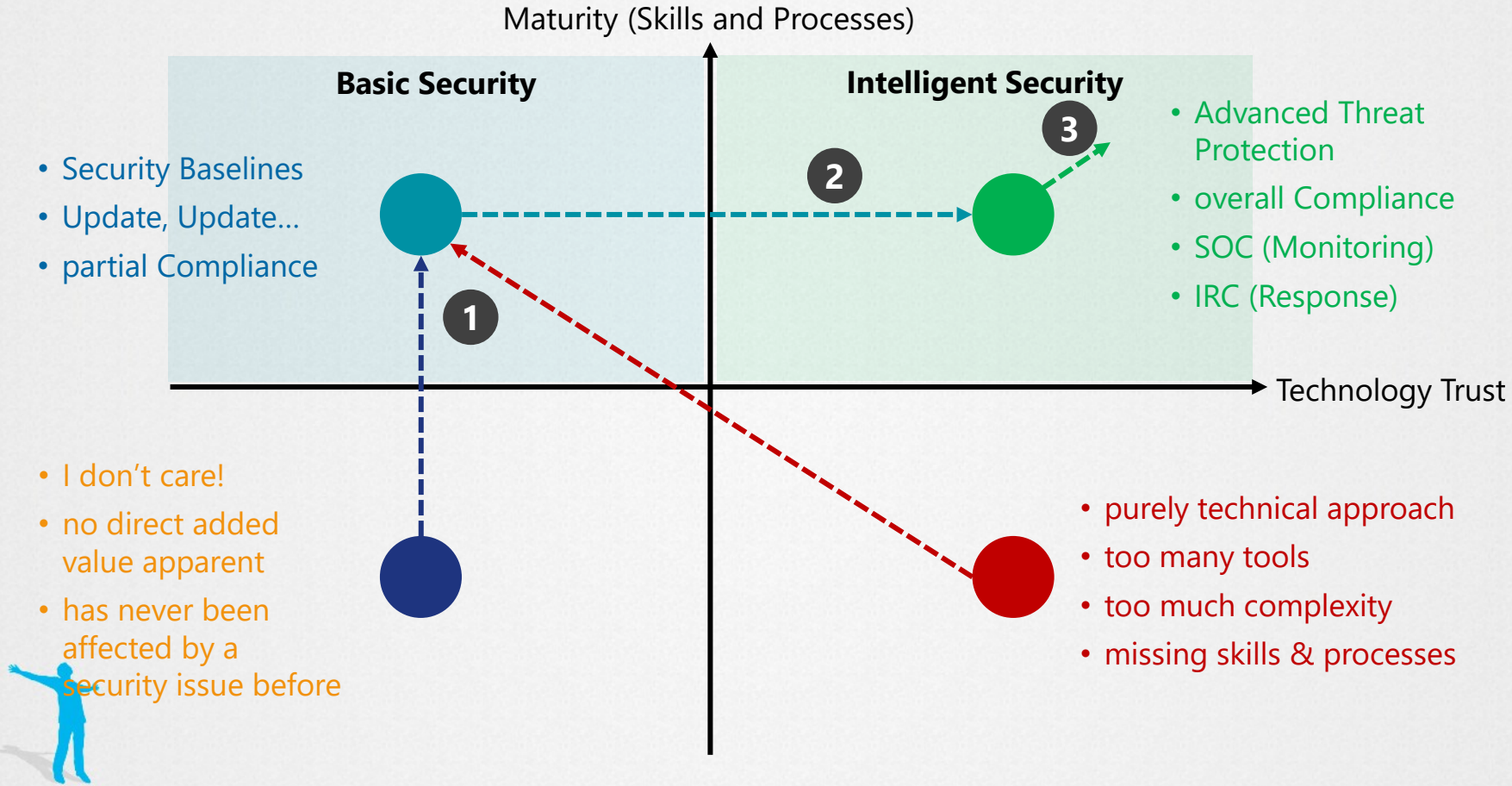
secureguard

ACP IT for innovators.

Contents

- Security Baseline
  - Microsoft Baseline
  - Documentation and Deviation Handling
- Intune vs GPO
- Rollout
  - Plan
  - Top issues
  - Preassessment
- Questions

Why is the Baseline important?



- Security Baselines
- Update, Update…
- partial Compliance

- Advanced Threat Protection
- overall Compliance
- SOC (Monitoring)
- IRC (Response)

- I don't care!
- no direct added value apparent
- has never been affected by a security issue before

- purely technical approach
- too many tools
- too much complexity
- missing skills & processes

Security Baselines

There are several sources providing security configuration guidance:

Microsoft (Free)

- **Windows / Windows Server / Domain Controller**
- **Office**
- **Edge**

CIS – Center for Internet Security (Paid)

NIST – National Institute of Standards and Technology

ACSC – Australian Cyber Security Center

UK National Cyber Security Centre

US Department of Defense

CIS Pricing

Employee Range	1-Year Total
250,000+	$15,598.00
100,000 - 249,999	$14,443.00
50,000 - 99,999	$13,288.00
25,000 - 49,999	$12,133.00
10,000 - 24,999	$11,550.00
5,000 - 9,999	$10,978.00
1,000 - 4,999	$10,395.00
500 - 999	$7,513.00
250 - 499	$5,203.00
100 - 249	$3,762.00
50 - 99	$2,310.00
up to 49	$1,452.00

MS Security Configuration Framework

https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md

Important Assumption

If a attacker is able to gain admin permission on a given system every setting can be changed according to his wish.

- Make GPO client corrupt
- Disable Applocker Service

If a setting can only be changed by an Admin and the Default value is the recommended value, then it will not be enforced by policy.

Documentation and Deviation Handling

Initial - Add columns to Excel files

- Deviation
- Deviation Explanation
- Change Request Id (Optional)
- GPO Name (Optional)
- Intune Profile Name (Optional)
- Intune Profile Path (Optional)

Update Baseline Version

- Copy existing documentation and rename to match new version
- Add new settings to Excel
- Plan rollout

Demo Compliance Toolkit

Download Experience

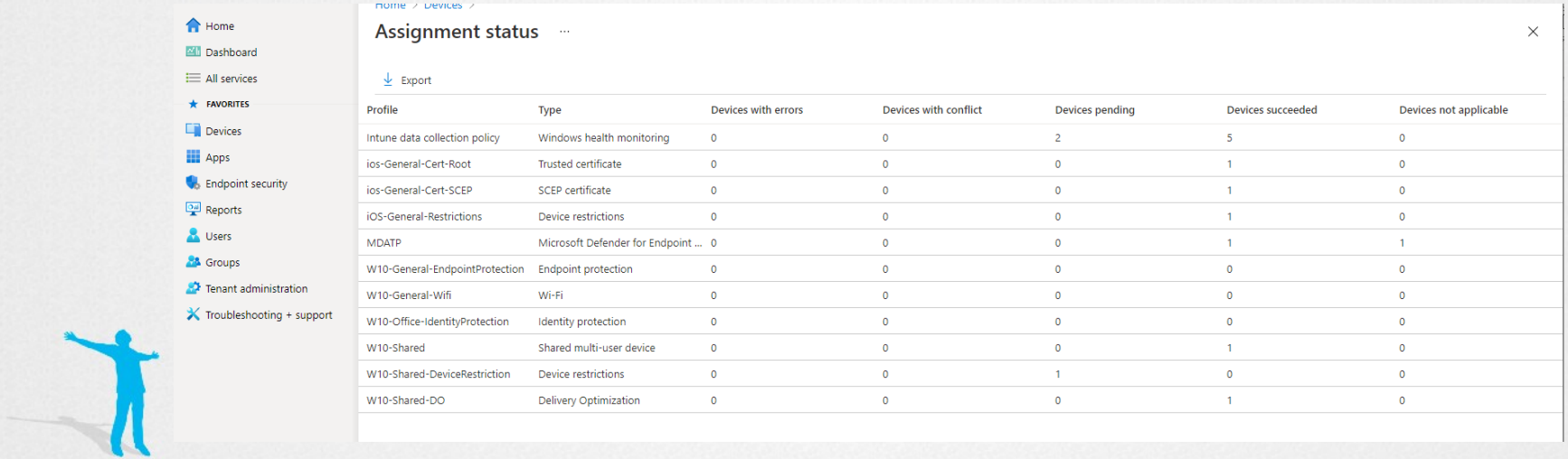
Content

- Excel
- Import

Intune vs GPO

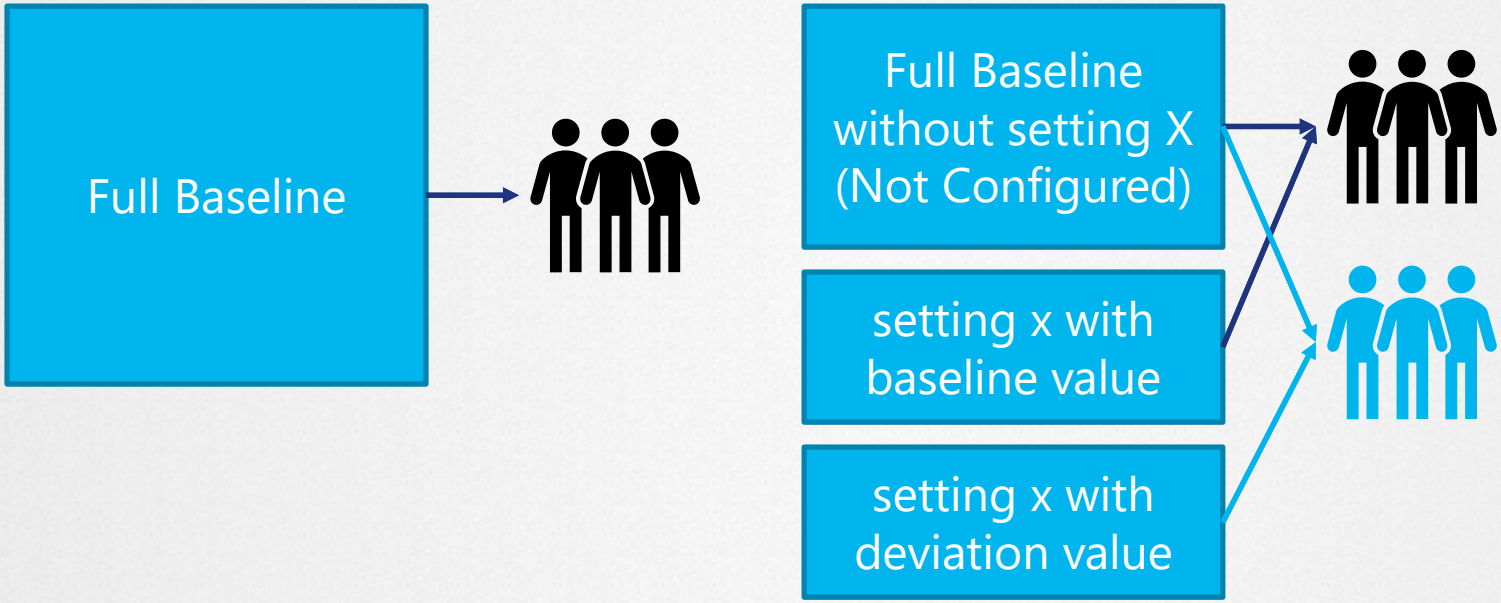
Intune Profiles

- ✓ Flexible deviations
- ✓ Conflict report
- × Multiple profile types required
- × Manual work



Profile	Type	Devices with errors	Devices with conflict	Devices pending	Devices succeeded	Devices not applicable
Intune data collection policy	Windows health monitoring	0	0	2	5	0
ios-General-Cert-Root	Trusted certificate	0	0	0	1	0
ios-General-Cert-SCEP	SCEP certificate	0	0	0	1	0
iOS-General-Restrictions	Device restrictions	0	0	0	1	0
MDATP	Microsoft Defender for Endpoint ...	0	0	0	1	1
W10-General-EndpointProtection	Endpoint protection	0	0	0	0	0
W10-General-Wifi	Wi-Fi	0	0	0	0	0
W10-Office-IdentityProtection	Identity protection	0	0	0	0	0
W10-Shared	Shared multi-user device	0	0	0	1	0
W10-Shared-DeviceRestriction	Device restrictions	0	0	1	0	0
W10-Shared-DO	Delivery Optimization	0	0	0	1	0

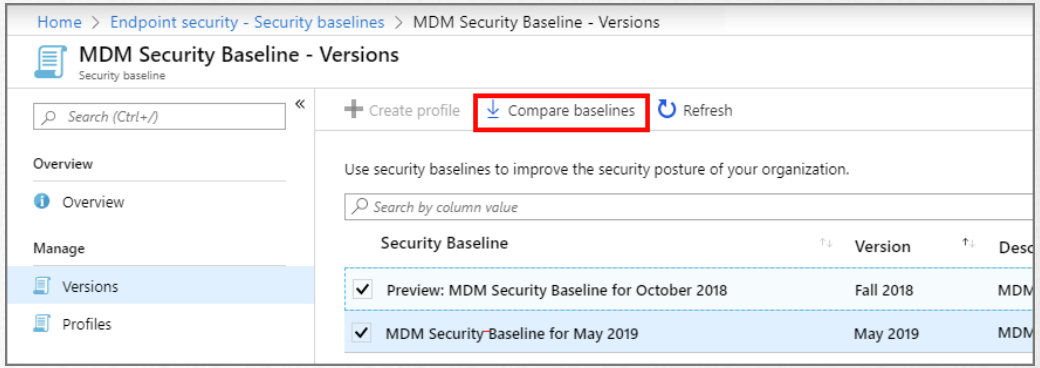
Intune Profile Deviations



Mind. 3 Profiles, 4 Assignments

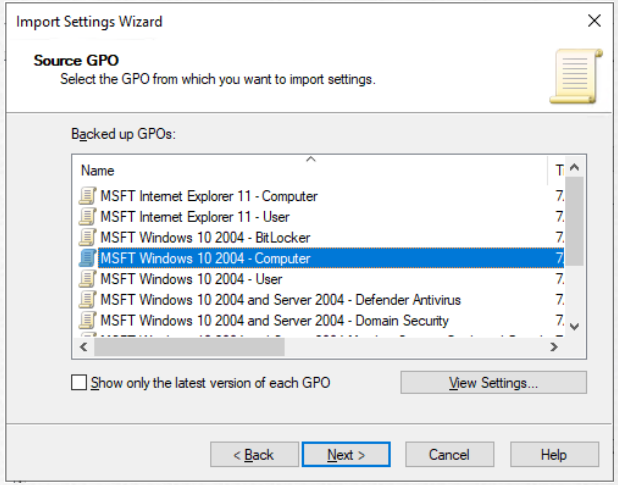
Intune Security Baselines

- ✓ Simple start
- ✓ Cloud only devices
- ✓ Deviation report
- × Limited deviation
- × Limited MS documentation



GPO

- ✓ Import possible
- ✓ AD joined devices only
- ✓ Simple deviations through inheritance
- × No reporting



Possible deployment Options

Intune Profiles

- ✓ Flexible deviations
- ✓ Conflict report
- × Multiple profile types required
- × Manual work

Intune Security Baseline

- ✓ Simple start
- ✓ Cloud only devices
- ✓ Deviation report
- × Limited deviation
- × Limited documentation

GPO

- ✓ Import possible
- ✓ AD joined devices only
- ✓ Simple deviations through inheritance
- × No reporting

Testing with Intune

Policy deployment leads to delays

Use test machine where policy is applied via local policy

- Create Snapshot if it is a VM

Policy settings not always reverted when set to not configured (Depends on CSP)

Use Github for change history

..		
ProactiveRemediations	Document proactive remediations	2 months ago
Windows-COPE-EndpointSecurity-ASR.json	Adjust defender settings	3 months ago
Windows-COPE-EndpointSecurity-Antivirus.json	Adjust defender settings	3 months ago
Windows-COPE-EndpointSecurity-Bitlocker.json	Adjust naming	3 months ago
Windows-COPE-EndpointSecurity-CredentialGuard.json	Adjust naming	3 months ago
Windows-COPE-EndpointSecurity-DeviceControl.json	Moved all possible settings to settings catalog	3 months ago
Windows-COPE-EndpointSecurity-Firewall.json	Moved all possible settings to settings catalog	3 months ago
Windows-COPE-SettingsCatalog-WindowsSecurityBaseli...	Add import, export for proactive remediation	3 months ago

Rollout

Generic plan

Setup project

- Familiarize project teams
- Setup timelines
- Define deployment strategy

Preassessment

- Microsoft 365 Defender
- Use Audit Logs

Deployment

- Dedicated support resource
- Deploy Baselines

Enforce & Review

- Enforce Settings deployed in Audit mode
- Review made deviations and remediate if necessary

Closure

- Final deviation report to CISO

Define Pilot groups

```
PS P01:\> C:\temp\Invoke-PilotDeviceSelection.ps1
DEBUG: 2021-03-14 09:05:28+01    DEBUG    Folder: C:\Windows\Logs\ Already Exists
DEBUG: 2021-03-14 09:05:28+01    DEBUG    Start Script Invoke-PilotDeviceSelection.ps1
VERBOSE: Getting FolderType for path SCCM01.kurcontoso.ch\.
VERBOSE: FolderType is Drive for path SCCM01.kurcontoso.ch\.
VERBOSE: Getting FolderType for path SCCM01.kurcontoso.ch\SCCM01.kurcontoso.ch.
VERBOSE: Getting FolderType failed - Path SCCM01.kurcontoso.ch\SCCM01.kurcontoso.ch does not have a valid top level folder.
DEBUG: Checking if item SCCM01.kurcontoso.ch\ is a container.
VERBOSE: Getting FolderType for path SCCM01.kurcontoso.ch\.
VERBOSE: FolderType is Drive for path SCCM01.kurcontoso.ch\.
DEBUG: Result of if item SCCM01.kurcontoso.ch\ is a container is True.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777219 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777220 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777221 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777231 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777234 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    Resource 16777235 is already a member.
DEBUG: 2021-03-14 09:05:29+01    DEBUG    End Script Invoke-PilotDeviceSelection.ps1

PS P01:\>
```

[Build better pilot rings for Updates with MEMCM - Workplace Ninja's (wpninjas.ch)]

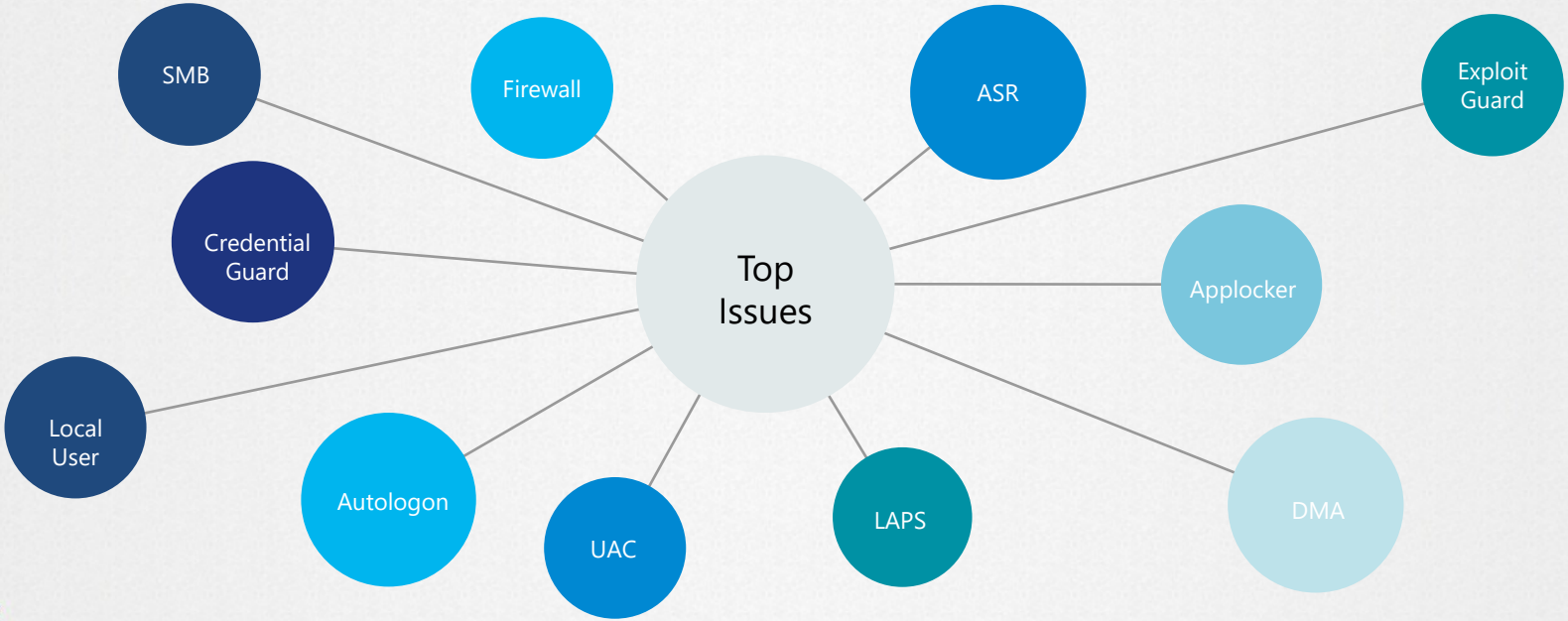
Microsoft Defender

Security Baseline Assessments (Premium Addon/Public Preview)

Security Recommendations

- Microsoft Defender for Clouds vs for Endpoints

Top Issues


SMB
Firewall
ASR
Exploit Guard
Credential Guard
Top Issues
Applocker
Local User
Autologon
UAC
LAPS
DMA

Preassessment - General

Attack Surface Reduction / Applocker / Exploit Guard / Network Protection

- Start with Audit Mode
- Collect Event logs or use Defender for Endpoint
- Evaluate attack surface reduction rules - Windows security | Microsoft Docs
- Evaluate Exploit Protection - Windows security | Microsoft Docs
- Evaluate network protection - Windows security | Microsoft Docs
- Monitor app usage with AppLocker (Windows 10) - Windows security | Microsoft Docs

Preassessment – Local Users

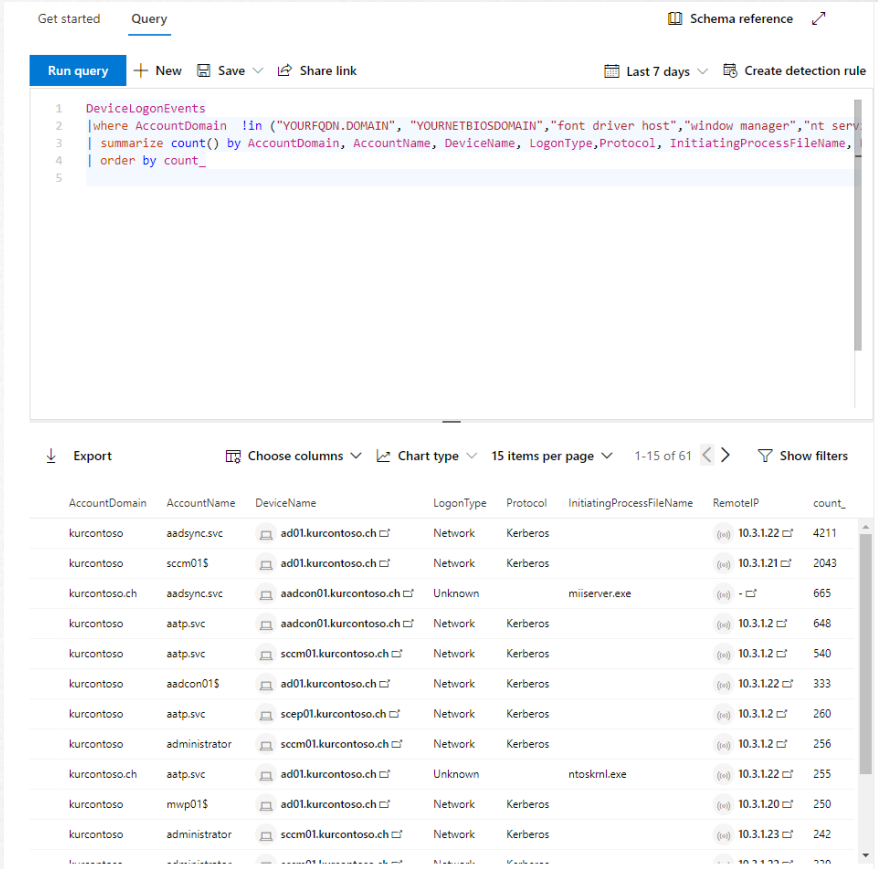
Issues which can occur:

- Local password policy will be set
- "Deny Access from Network" is enabled for local accounts
- Autologon

Detect local Account usage with MDE:

DeviceLogonEvents

```
|where AccountDomain  !in ("YOURFQDN.DOMAIN", "YOURNETBIOSDOMAIN","font driver host","window manager","nt service","nt authority","iis apppool","nt virtual machine")
| summarize count() by AccountDomain, AccountName, DeviceName, LogonType,Protocol, InitiatingProcessFileName, RemoteIP
| order by count_
```



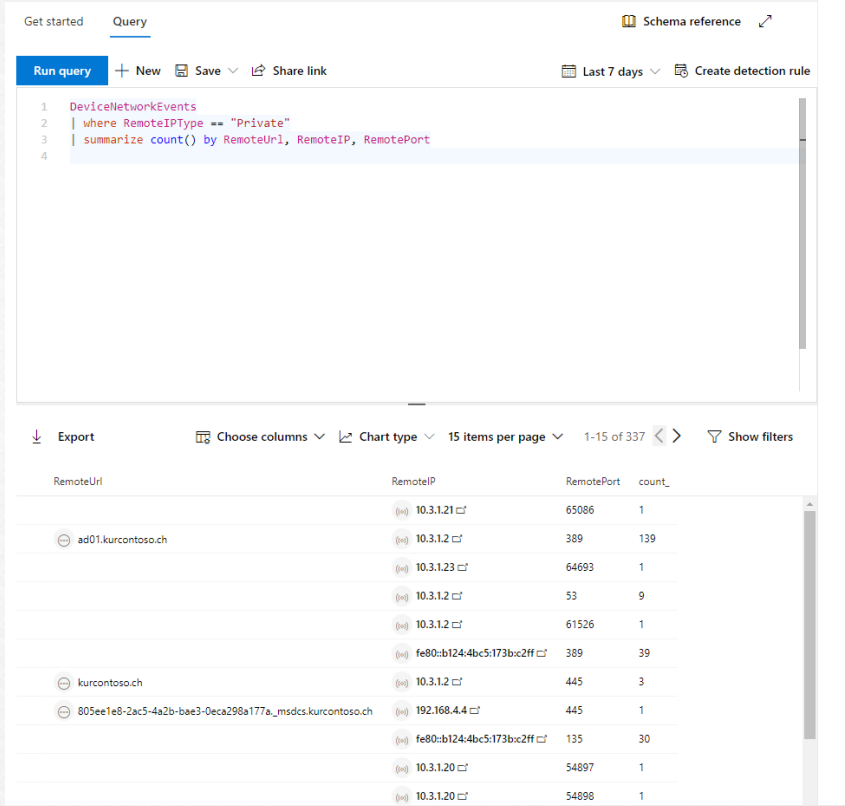
Preassessment – Firewall

Issues which can occur:

- Inbound connections required
- Dual network adapter (for example in production could be categorized as public)

Detect inbound connections with MDE:

```
DeviceNetworkEvents
| where RemoteIPType == "Private"
| summarize count() by RemoteUrl, RemoteIP, RemotePort
```



Preassessment – SMB

Issues which can occur:

- SMB v1
- Digitally sign communications (always) – Enabled

Mainly check your NAS, MFP(Scanner) and old Windows versions for compatibility

Detect SMB server:

- DeviceNetworkEvents | where RemotePort == 445 and Timestamp > ago(7d)

Check SMB traffic:

- Message Analyzer: SMB1 - Audit Active Usage using Message Analyzer | Microsoft Docs
- SMB v1 Usage Auditing: SMB1 - Audit Active Usage using Audit Log | Microsoft Docs

Preassessment - RDP

Issues which can occur:

- RDP access blocked due to failed Network level authentication (NLA)

Checks:

- Check Inventory in CM or MDE for old OS like 2003.
- CMPivot to check if it is disabled on a server:

```
Registry('hklm:\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp') |
where Property == 'SecurityLayer'
```

```
Registry('hklm:\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp') |
where Property == 'UserAuthentication'
```

Preassessment – Old Office File formats

Issues which can occur:

- Old Office file types are blocked.

Checks:

- Search file servers for xls/doc/ppt (This will not cover each document which is blocked but most of them)
- EmailAttachmentInfo | summarize count() by FileType | where FileType in ('doc','xls','ppt')
- DeviceFileEvents | where FileName endswith "doc"

Questions

1

Follow Microsoft Security Blog

https://techcommunity.microsoft.com/t5/microsoft-security-baselines

2

Follow me twitter

I share new Baselines as soon they are available

3

Questions

Thanks to our Sponsors!

ACP IT for innovators.

Microsoft

NiCE
IT Management Solutions
www.nice.de

THOMAS KRENN®

VEEAM

secureguard

ACP IT for innovators.