Session:

The modern workplace, after an audit

— Mirko Colemberg —

Thank you Sponsors

Microsoft

baseVISION

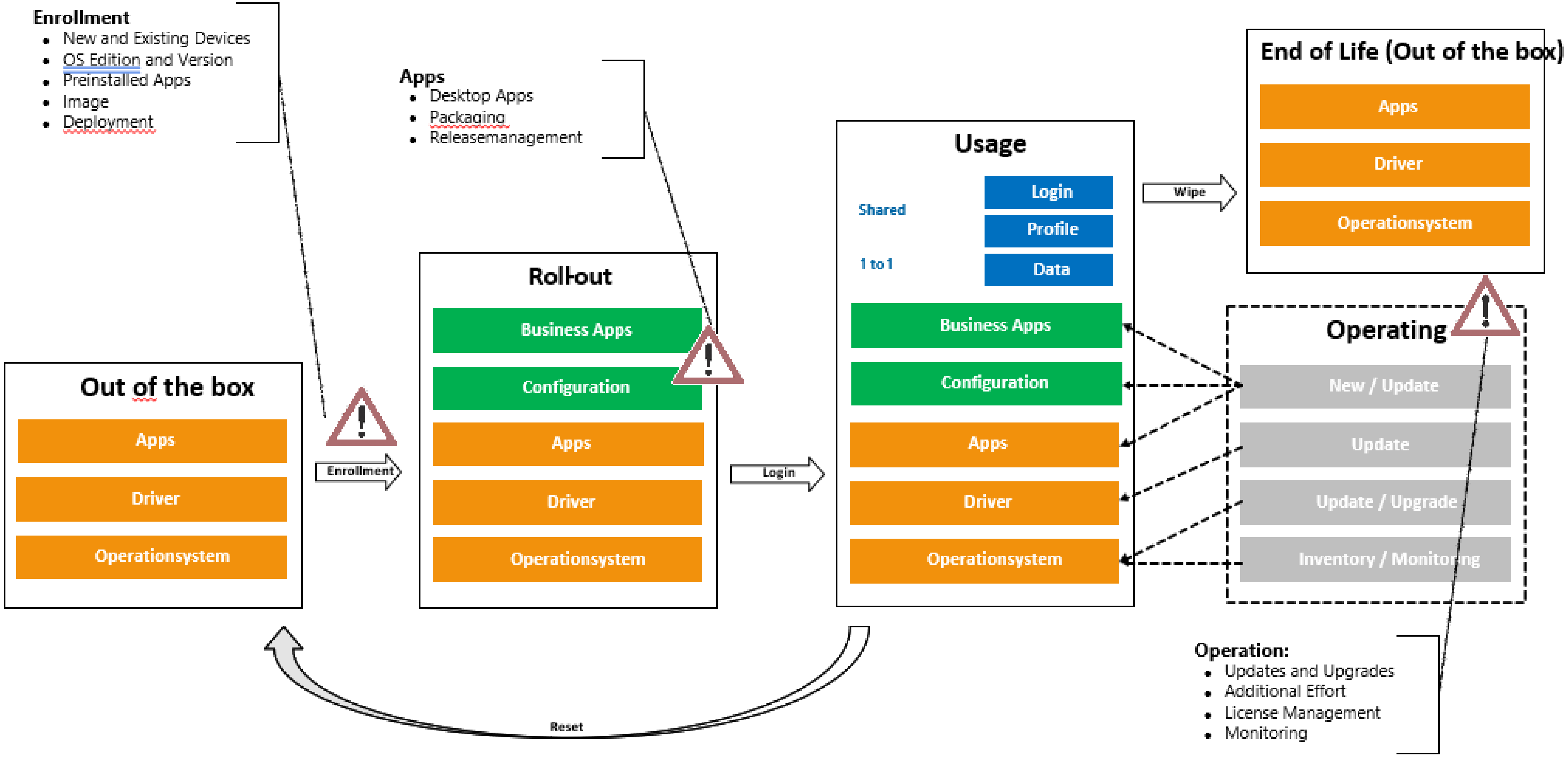
SECURE & MODERN ENDPOINT MANAGEMENT

EPIC FUSION

BRING IT ALL TOGETHER

It's our
anniversary?

Based on the Device Lifecycle



Enrollment
- New and Existing Devices
- OS Edition and Version
- Preinstalled Apps
- Image
- Deployment

Apps
- Desktop Apps
- Packaging
- Releasemanagement

Out of the box

Apps

Driver

Operationsystem

Enrollment

Roll-out

Business Apps

Configuration

Apps

Driver

Operationsystem

Login

Usage

Shared

Login

Profile

1 to 1

Data

Business Apps

Configuration

Apps

Driver

Operationsystem

Wipe

End of Life (Out of the box)

Apps

Driver

Operationsystem

Operating

New / Update

Update

Update / Upgrade

Inventory / Monitoring

Reset

Operation:
- Updates and Upgrades
- Additional Effort
- License Management
- Monitoring

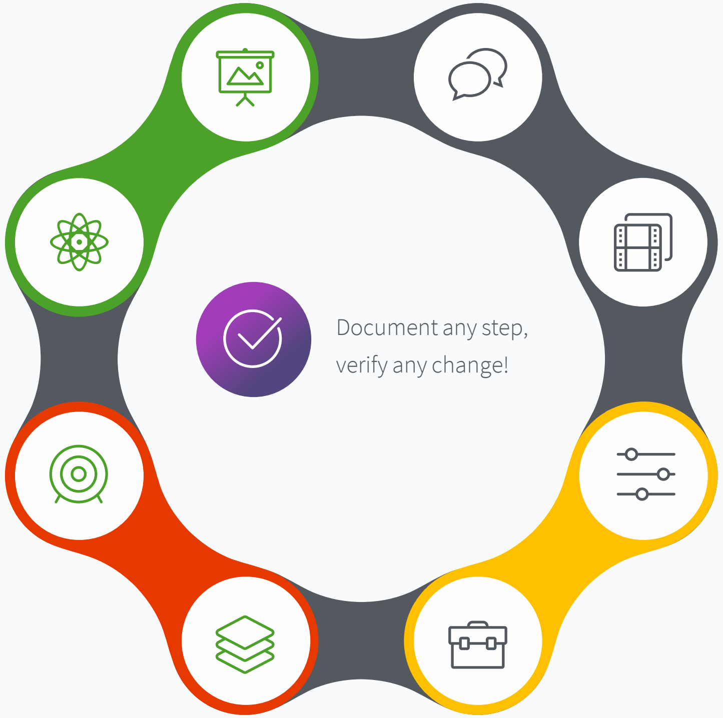
Device Hardening Lifecycle

Analyze, Vectors and Vendors.

Overview, create a matrix

Decide, what we have, where we have to go.

Test, Line of Business Devices and Applications



Document any step, verify any change!

Implement, piloting on a broader Device and App selection

Monitor, check the hardening level, excludes needed

No Excludes, only other solutions (EPM)

Report, ready for Audit.

- 3.1 Fileserver - Rights management on File shares
- 3.2 Active Directory - Different Mismatching configuration
- 3.3 Active Directory - Password expires not for all of users User
- 3.4 Active Directory - Accounts with longtime no Logon
- 3.5 Active Directory – Two Domain Admins not Protected

Patch Management - Operating system End-of-Life

etwork - not OWP-Devices in the wrong Network, no NA

ntune - two-Factor Authentication for Role based Accou

7 Asset Management - Documentation not complete

With a Zerotrust and AON-VPN is not realy a Zerotrust, you get the possibility to access LDAP ;-)

It still needs a good AD-Server (DC) Hardening!!!

- 3.15 Network - not OWP-Devices in the wrong Network, no NAC

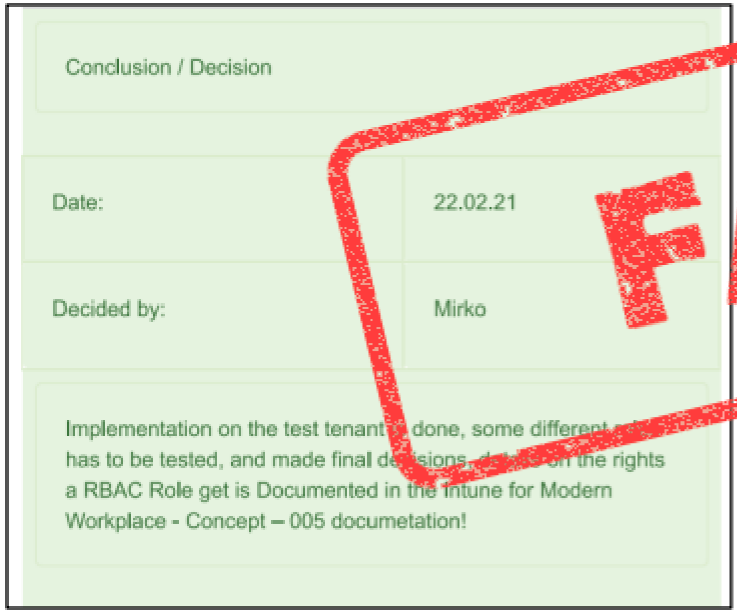
With AON-VPN it’s still possible to Access network and do Scans;-)

- 3.16 Intune - two-Factor Authentication for Role based Accounts

Some Audits are not really good controlled, we have PIM / PAG in place, there is also implemented that every User have MFA!

FAIL

- 3.17 Asset Management - Documentation not complete

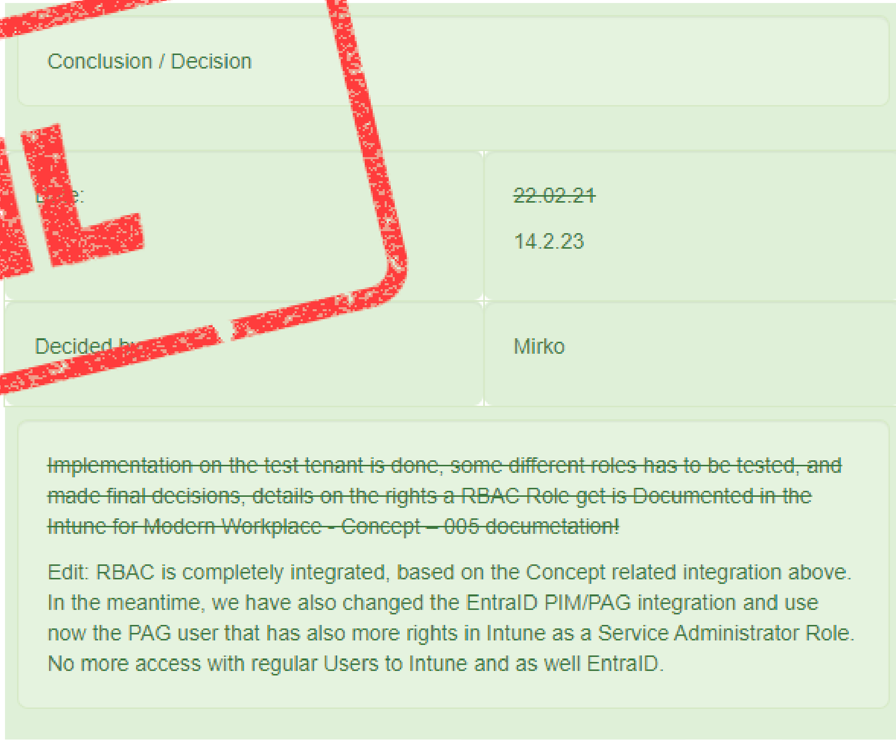


Conclusion / Decision

Date:	22.02.21
Decided by:	Mirko

Implementation on the test tenant is done, some different roles has to be tested, and made final decisions, details on the rights a RBAC Role get is Documented in the Intune for Modern Workplace - Concept – 005 documetation!

FAIL



Conclusion / Decision

Date:	~~22.02.21~~ 14.2.23
Decided by:	Mirko

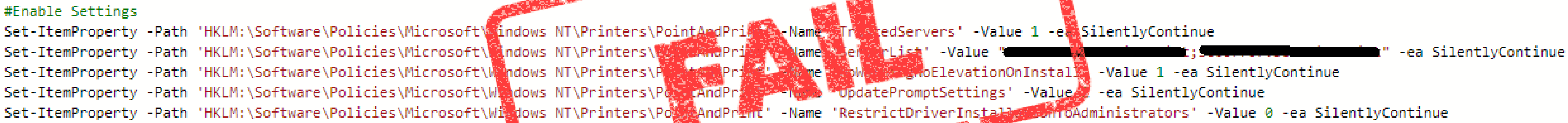
~~Implementation on the test tenant is done, some different roles has to be tested, and made final decisions, details on the rights a RBAC Role get is Documented in the Intune for Modern Workplace - Concept – 005 documetation!~~

Edit: RBAC is completely integrated, based on the Concept related integration above. In the meantime, we have also changed the EntraID PIM/PAG integration and use now the PAG user that has also more rights in Intune as a Service Administrator Role. No more access with regular Users to Intune and as well EntraID.

- 3.6 Endpoint Security - Print Nightmare Local Privilege Escalation possible
- 3.7 Endpoint Security - Office Macros
- 3.8 Endpoint Security - PowerShell Constrained Language Mode
- 3.9 Endpoint Security - Security Hardening
- 3.10 Endpoint Security - Installation of Application
- 3.11 Endpoint Security - run PowerShell Scripts without digital Signature
- 3.13 Endpoint Security - PowerShell Hardening
- 3.14 Endpoint Security - Not signed Office Macros via USB
- 3.18 Endpoint Security - Application Guard & SmartScreen for non-Edge not active
- 3.19 Endpoint Security - Non-compliant Devices
- 3.20 Endpoint Security - confusing Alerts
- 3.21 Endpoint Security - Saved WLAN PSK on a Device
- 3.22 Endpoint Security - Cached Login Credentials
- 3.23 Endpoint Security - USB Stick no check on Malware
- 3.24 Endpoint Security - No AdBlock in Browser
- 3.25 Endpoint Security - Boot von USB Stick

- Endpoint Security - Print Nightmare Local Privilege Escalation possible

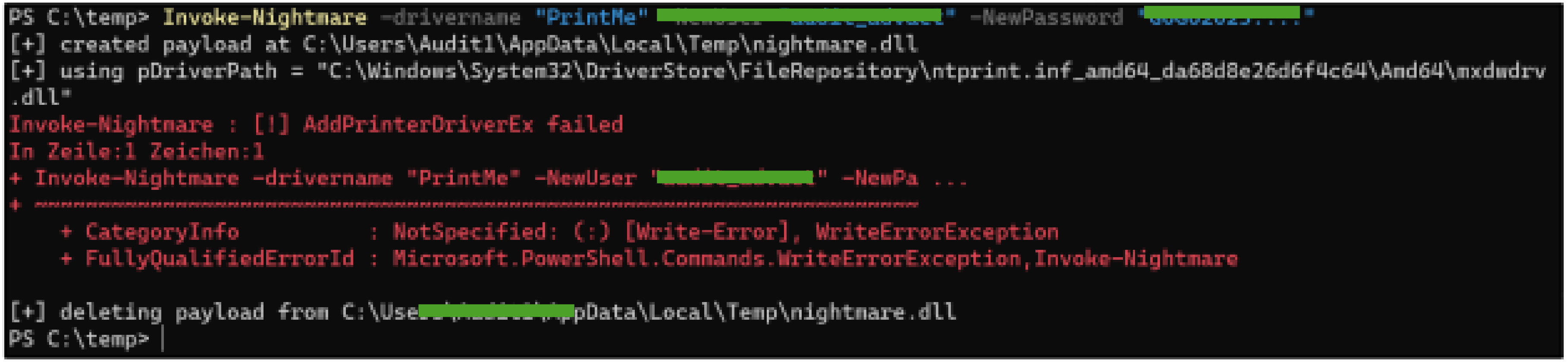
Make sure only specific Servers are allowed to update Drivers:



```
#Enable Settings
Set-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'TrustedServers' -Value 1 -ea SilentlyContinue
Set-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'ServerList' -Value "[redacted]" -ea SilentlyContinue
Set-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'NoWarningNoElevationOnInstall' -Value 1 -ea SilentlyContinue
Set-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'UpdatePromptSettings' -Value 0 -ea SilentlyContinue
Set-ItemProperty -Path 'HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -Name 'RestrictDriverInstallationToAdministrators' -Value 0 -ea SilentlyContinue
```

FAIL

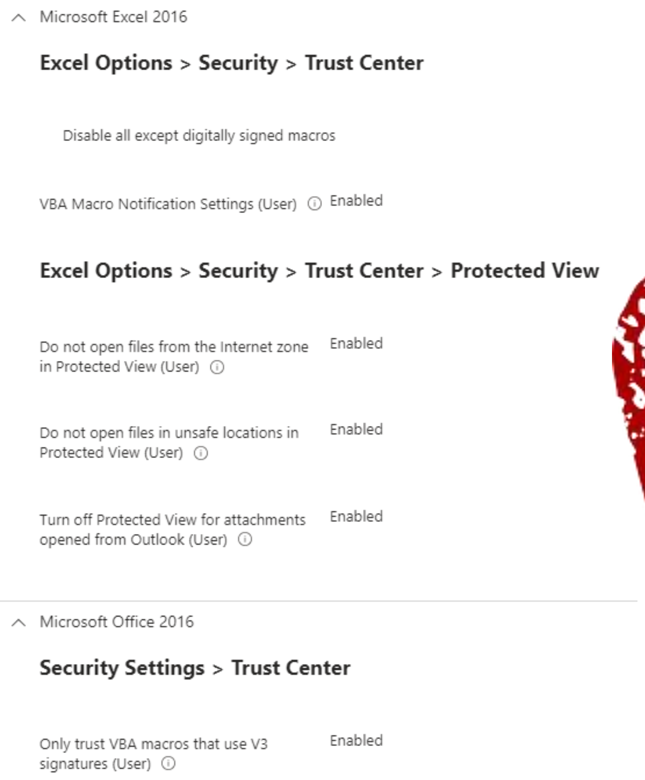
https://itm4n.github.io/printnightmare-exploitation/



```
PS C:\temp> Invoke-Nightmare -drivername "PrintMe" [redacted]" -NewPassword '[redacted]"
[+] created payload at C:\Users\Audit1\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_da68d8e26d6f4c64\Amd64\mxdwdrv
.dll"
Invoke-Nightmare : [!] AddPrinterDriverEx failed
In Zeile:1 Zeichen:1
+ Invoke-Nightmare -drivername "PrintMe" -NewUser '[redacted]" -NewPa ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-Nightmare

[+] deleting payload from C:\Use[redacted]pData\Local\Temp\nightmare.dll
PS C:\temp> |
```

- 3.7 Endpoint Security - Office Macros

ASR related, change Macros and only allow Signed Macros, it’s a workaround, because get rid of Macros ;-)



Microsoft Excel 2016

Excel Options > Security > Trust Center

Disable all except digitally signed macros

VBA Macro Notification Settings (User) ⓘ Enabled

Excel Options > Security > Trust Center > Protected View

Do not open files from the Internet zone in Protected View (User) ⓘ Enabled

Do not open files in unsafe locations in Protected View (User) ⓘ Enabled

Turn off Protected View for attachments opened from Outlook (User) ⓘ Enabled

Microsoft Office 2016

Security Settings > Trust Center

Only trust VBA macros that use V3 signatures (User) ⓘ Enabled

APPROVED

- 3.8 Endpoint Security - PowerShell Constrained Language Mode

Constrained Language mode is designed to allow basic language elements such as loops, conditionals, string expansion, and access to object properties. The restrictions prevent operations that could be abused by a malicious actor.

The Constrained Language mode permits all cmdlets and a subset of PowerShell language elements but limits the object types that can be used.

APPROVED

```
"$([Environment]::GetFolderPath("CommonDesktopDirectory"))\*.lnk"
```

• 3.9 Endpoint Security - Security Hardening

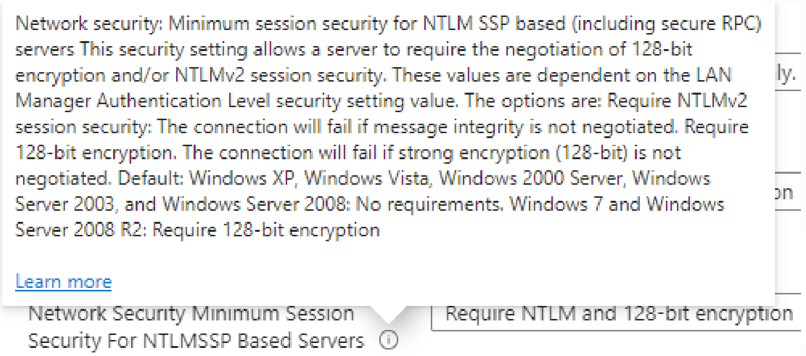
In this case;

- Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

ure 'Network security: Configure encryption types allowed for Kerberos' is set to AC_SHA1, AES256_HMAC_SHA1, Future encryption types

Server side?

IB Local machine, Client / Server, yes set it for Server (if the Devices shares, it's like a Ser



Network security: Minimum session security for NTLM SSP based (including secure RPC) servers This security setting allows a server to require the negotiation of 128-bit encryption and/or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value. The options are: Require NTLMv2 session security: The connection will fail if message integrity is not negotiated. Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. Default: Windows XP, Windows Vista, Windows 2000 Server, Windows Server 2003, and Windows Server 2008: No requirements. Windows 7 and Windows Server 2008 R2: Require 128-bit encryption

Learn more

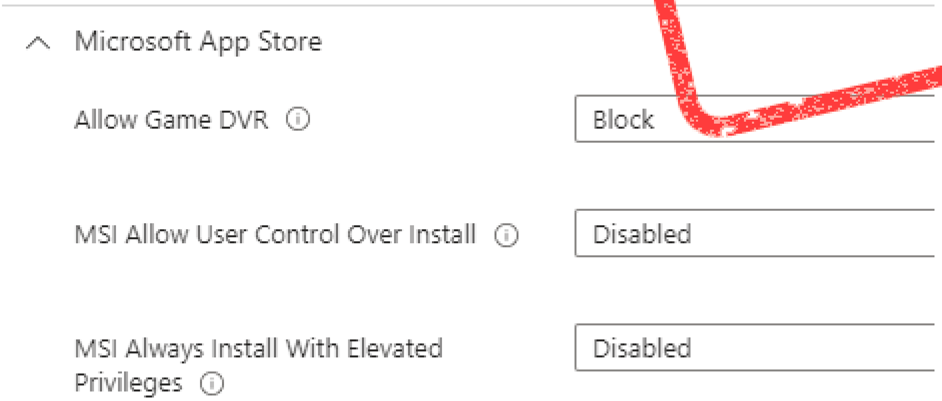
Network Security Minimum Session Security For NTLMSSP Based Servers: Require NTLM and 128-bit encryption

- 3.10 Endpoint Security - Installation of Application

Microsoft Store apps in this case.

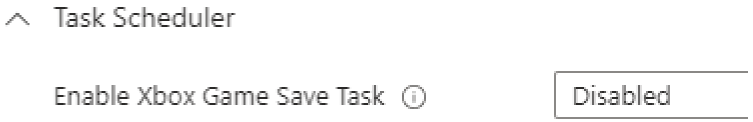
Who needs to close down Store, tell me why!

FAIL



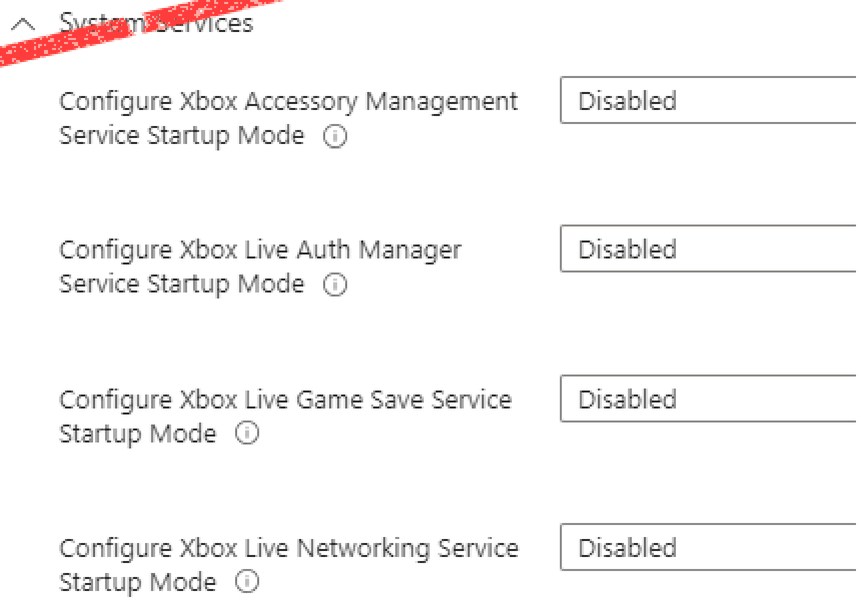
Microsoft App Store

Allow Game DVR ⓘ	Block
MSI Allow User Control Over Install ⓘ	Disabled
MSI Always Install With Elevated Privileges ⓘ	Disabled



Task Scheduler

Enable Xbox Game Save Task ⓘ	Disabled



System Services

Configure Xbox Accessory Management Service Startup Mode ⓘ	Disabled
Configure Xbox Live Auth Manager Service Startup Mode ⓘ	Disabled
Configure Xbox Live Game Save Service Startup Mode ⓘ	Disabled
Configure Xbox Live Networking Service Startup Mode ⓘ	Disabled

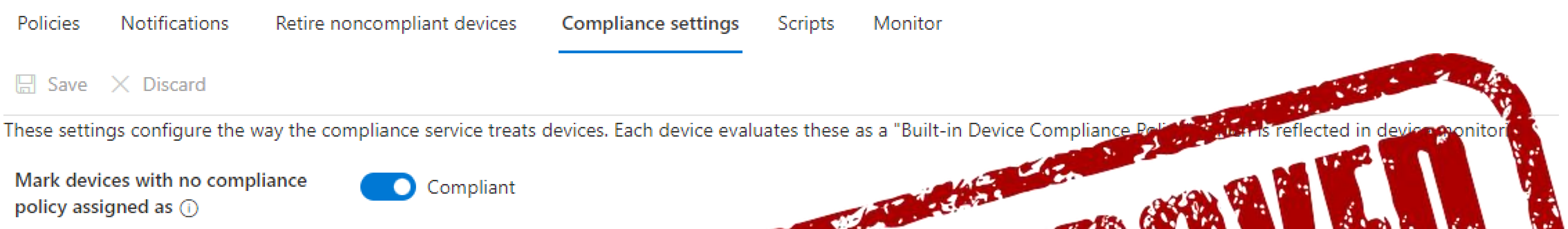
- 3.11 Endpoint Security - run PowerShell Scripts without digital Signature

Is signed PowerShell scripts a thing to secure execution of Scripts?

15 Ways to Bypass the PowerShell Execution Policy (netspi.com)

FAIL

- 3.19 Endpoint Security - Non-compliant Devices

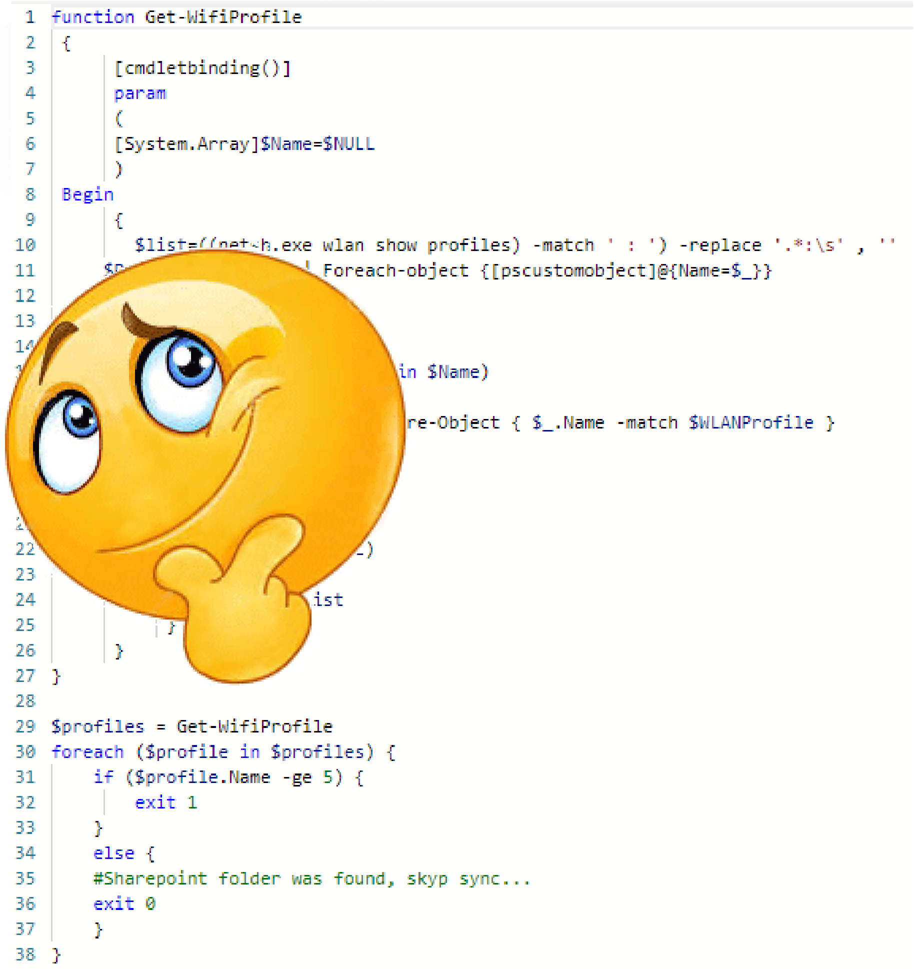


These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitori

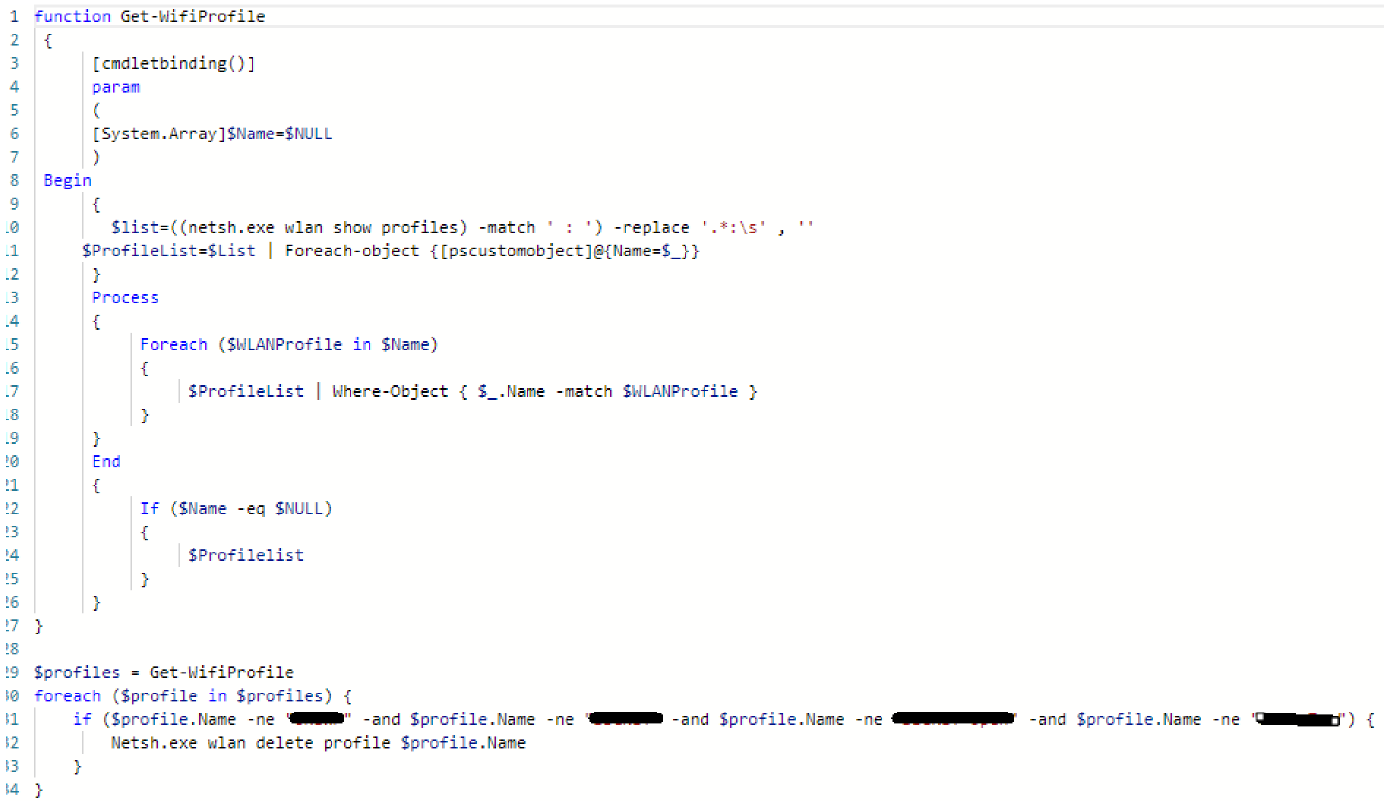
Mark devices with no compliance policy assigned as ⓘ ● Compliant

APPROVED

• 3.21 Endpoint Security - Saved WLAN PSK on a Device



```
function Get-WifiProfile
 {
        [cmdletbinding()]
        param
        (
        [System.Array]$Name=$NULL
        )
 Begin
        {
          $list=((netsh.exe wlan show profiles) -match ' : ') -replace '.*:\s' , ''
      $P                    | Foreach-object {[pscustomobject]@{Name=$_}}


                                  in $Name)

                                  re-Object { $_.Name -match $WLANProfile }




                                  )

                              ist
                 }
        }
}

$profiles = Get-WifiProfile
foreach ($profile in $profiles) {
    if ($profile.Name -ge 5) {
        exit 1
    }
    else {
    #Sharepoint folder was found, skyp sync...
    exit 0
    }
}
```

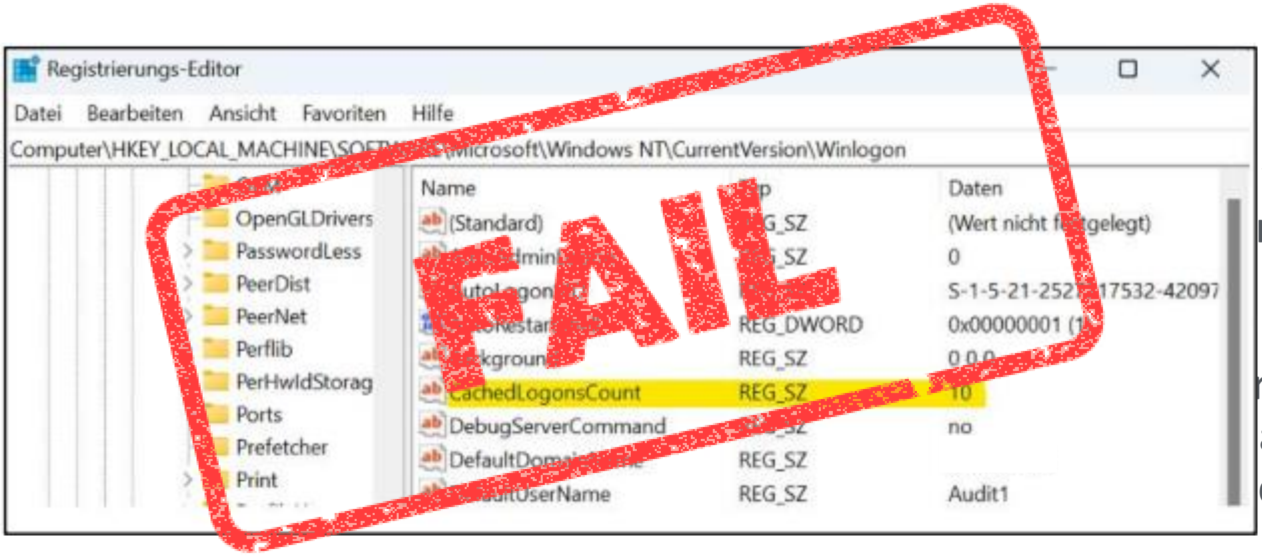


```
function Get-WifiProfile
 {
        [cmdletbinding()]
        param
        (
        [System.Array]$Name=$NULL
        )
 Begin
        {
          $list=((netsh.exe wlan show profiles) -match ' : ') -replace '.*:\s' , ''
      $ProfileList=$List | Foreach-object {[pscustomobject]@{Name=$_}}
        }
        Process
        {
                Foreach ($WLANProfile in $Name)
                {
                        $ProfileList | Where-Object { $_.Name -match $WLANProfile }
                }
        }
        End
        {
                If ($Name -eq $NULL)
                {
                        $Profilelist
                }
        }
}

$profiles = Get-WifiProfile
foreach ($profile in $profiles) {
    if ($profile.Name -ne '[redacted]" -and $profile.Name -ne '[redacted] -and $profile.Name -ne [redacted]' -and $profile.Name -ne '[redacted]') {
        Netsh.exe wlan delete profile $profile.Name
    }
}
```

3.22 Endpoint Security - Cached Login Credentials

Caching of logo y applies to domain-joined ms.

- Azure AD Jo rosoft Q&A = For AAD joined machines, creder ager – a component which is manageable ar d by the operating system.



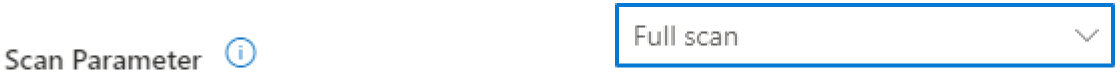
FAIL

Registrierungs-Editor

```
Computer\HKEY_LOCAL_MACHINE\SOFT      \Microsoft\Windows NT\CurrentVersion\Winlogon

                     Name                          p              Daten
  OpenGLDrivers      (Standard)                    G_SZ           (Wert nicht f  tgelegt)
> PasswordLess            dmin                     _SZ            0
> PeerDist            utologon                                    S-1-5-21-252  17532-42097
> PeerNet                   star                   REG_DWORD      0x00000001 (1
  Perflib                 kgroun                   REG_SZ         0 0 0
  PerHwldStorag      CachedLogonsCount             REG_SZ         10
  Ports              DebugServerCommand                           no
  Prefetcher         DefaultDom                    REG_SZ
> Print                  ultUserName               REG_SZ         Audit1
```

- For AAD joined machines, credential caching is related to the Primary Refresh Token that is issued when a user is authenticated against Azure AD.

3.23 Endpoint Security - USB Stick no check on Malware



Scan Parameter ⓘ

Full scan ⌄

3.24 Endpoint Security - No AdBlock in Browser

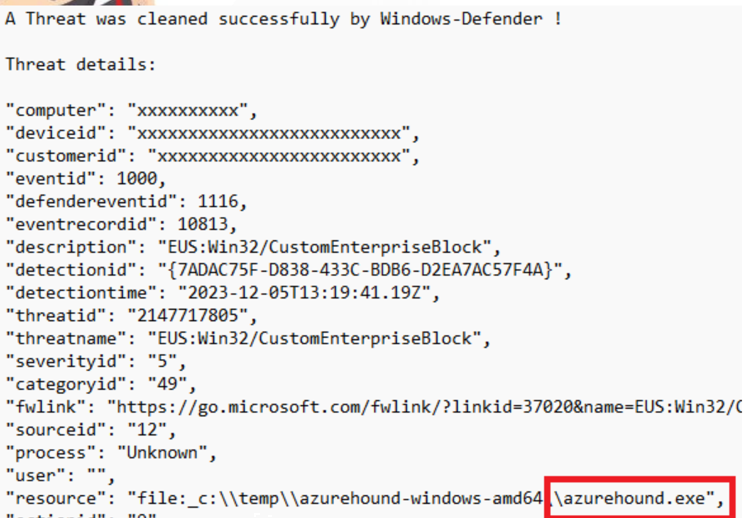
Good Idea, who of you have it?

Nicola have a point, maybe…

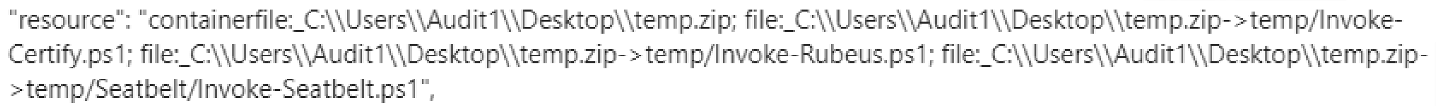
- 3.25 Endpoint Security - Boot von USB Stick

What’s about your OSD?

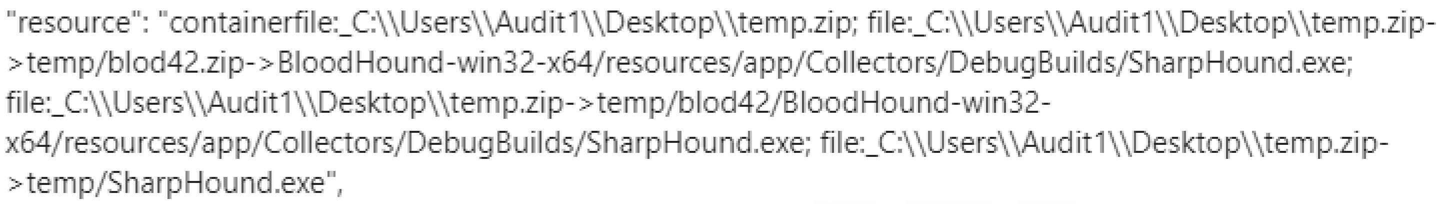
FAIL



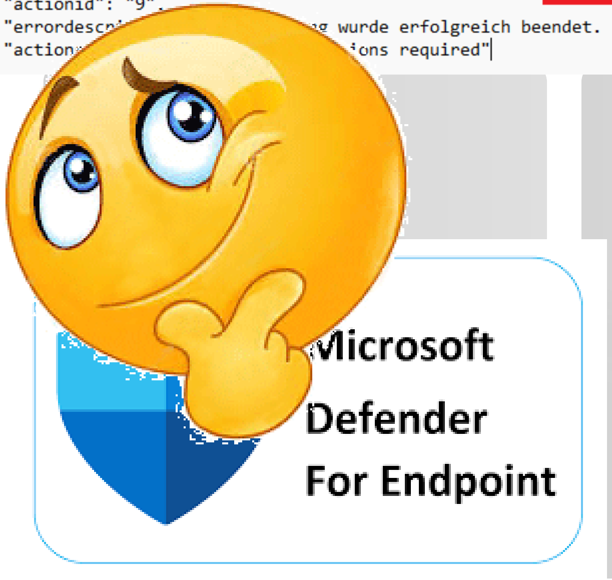
```
A Threat was cleaned successfully by Windows-Defender !

Threat details:

"computer": "xxxxxxxxxx",
"deviceid": "xxxxxxxxxxxxxxxxxxxxxxxxxx",
"customerid": "xxxxxxxxxxxxxxxxxxxxxxxx",
"eventid": 1000,
"defendereventid": 1116,
"eventrecordid": 10813,
"description": "EUS:Win32/CustomEnterpriseBlock",
"detectionid": "{7ADAC75F-D838-433C-BDB6-D2EA7AC57F4A}",
"detectiontime": "2023-12-05T13:19:41.19Z",
"threatid": "2147717805",
"threatname": "EUS:Win32/CustomEnterpriseBlock",
"severityid": "5",
"categoryid": "49",
"fwlink": "https://go.microsoft.com/fwlink/?linkid=37020&name=EUS:Win32/C
"sourceid": "12",
"process": "Unknown",
"user": "",
"resource": "file:_c:\\temp\\azurehound-windows-amd64\azurehound.exe",
"actionid": "9",
"errordescr                  g wurde erfolgreich beendet. ",
"action                      ions required"
```

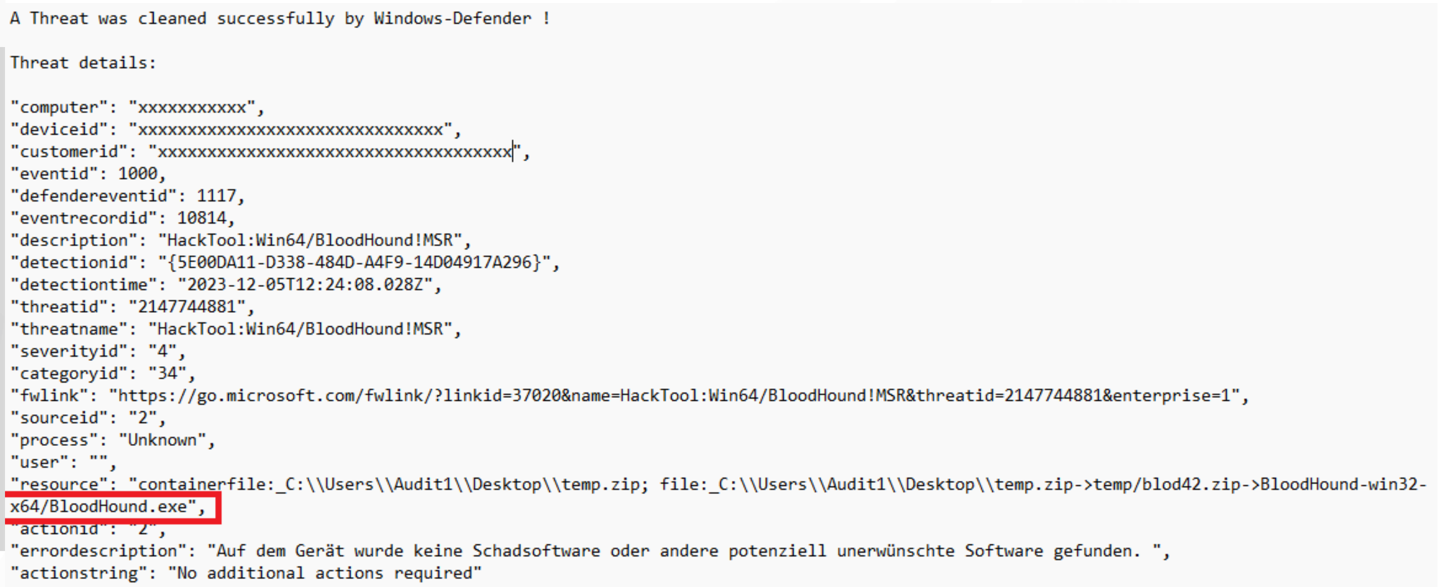


"resource": "containerfile:_C:\\Users\\Audit1\\Desktop\\temp.zip; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/Invoke-Certify.ps1; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/Invoke-Rubeus.ps1; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/Seatbelt/Invoke-Seatbelt.ps1",



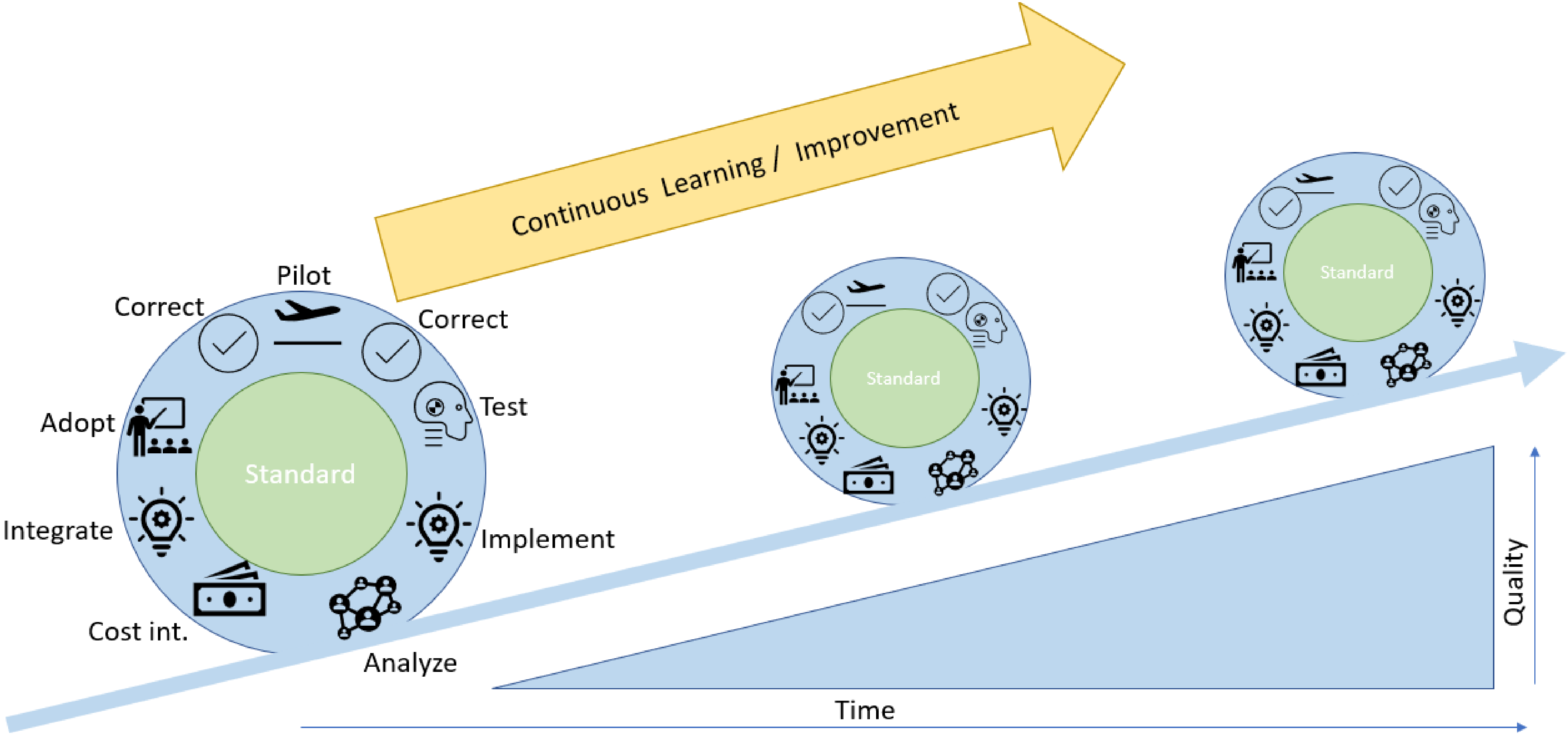
"resource": "containerfile:_C:\\Users\\Audit1\\Desktop\\temp.zip; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/blod42.zip->BloodHound-win32-x64/resources/app/Collectors/DebugBuilds/SharpHound.exe; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/blod42/BloodHound-win32-x64/resources/app/Collectors/DebugBuilds/SharpHound.exe; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/SharpHound.exe",





```
A Threat was cleaned successfully by Windows-Defender !

Threat details:

"computer": "xxxxxxxxxxx",
"deviceid": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
"customerid": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
"eventid": 1000,
"defendereventid": 1117,
"eventrecordid": 10814,
"description": "HackTool:Win64/BloodHound!MSR",
"detectionid": "{5E00DA11-D338-484D-A4F9-14D04917A296}",
"detectiontime": "2023-12-05T12:24:08.028Z",
"threatid": "2147744881",
"threatname": "HackTool:Win64/BloodHound!MSR",
"severityid": "4",
"categoryid": "34",
"fwlink": "https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:Win64/BloodHound!MSR&threatid=2147744881&enterprise=1",
"sourceid": "2",
"process": "Unknown",
"user": "",
"resource": "containerfile:_C:\\Users\\Audit1\\Desktop\\temp.zip; file:_C:\\Users\\Audit1\\Desktop\\temp.zip->temp/blod42.zip->BloodHound-win32-
x64/BloodHound.exe",
"actionid": "2",
"errordescription": "Auf dem Gerät wurde keine Schadsoftware oder andere potenziell unerwünschte Software gefunden. ",
"actionstring": "No additional actions required"
```

Continuous improvement



Benchmarks today

There are some Benchmark tools, frameworks, compliance examples around, that helps you based on CVE’s or Audit relevant settings choosing the right one to get a success and structured environment.

CIS

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

STIGVIEWER

STIGViewer® is for professionals who need access to the Security Technical Implementation Guides (STIGs) and documentation.

Unified Compliance Framework®

Canonical

Start with Ubuntu and get trusted open source for every part of your stack.

MS Security baselines

Microsoft is dedicated to providing its customers with secure operating systems, such as Windows and Windows Server, and secure apps, such as Microsoft 365 apps for enterprise and Microsoft Edge.

Benchmarks today

There are some Benchmark tools, frameworks, compliance examples around, that helps you based on CVE’s or Audit relevant settings choosing the right one to get a success and structured environment.

NCSC Device Security Guidance

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organizations are recommended to implement eight essential mitigation strategies from the Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

ACSC Essential Eight

We support the most critical organizations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, we provide effective incident response to minimize harm to the UK, help with recovery, and learn lessons for the future.

Additional Audit benchmarks

Some Devices in Production are regulated by the Industry.

For example, they have to be Certified that’s not possible to change anything, because it can be impacted to an Application to change the something that will have an impact to the production, like measurement of a high impacted value.

- Pharma industry
- Medical industry
- Oil Industry
- Etc.

- NIST SP 800-53 (Government USA, can be used for Public as well)
- PCI-DSS (finance / Credit)
- HIPAA (Healthcare USA)

FREE DOWNLOAD

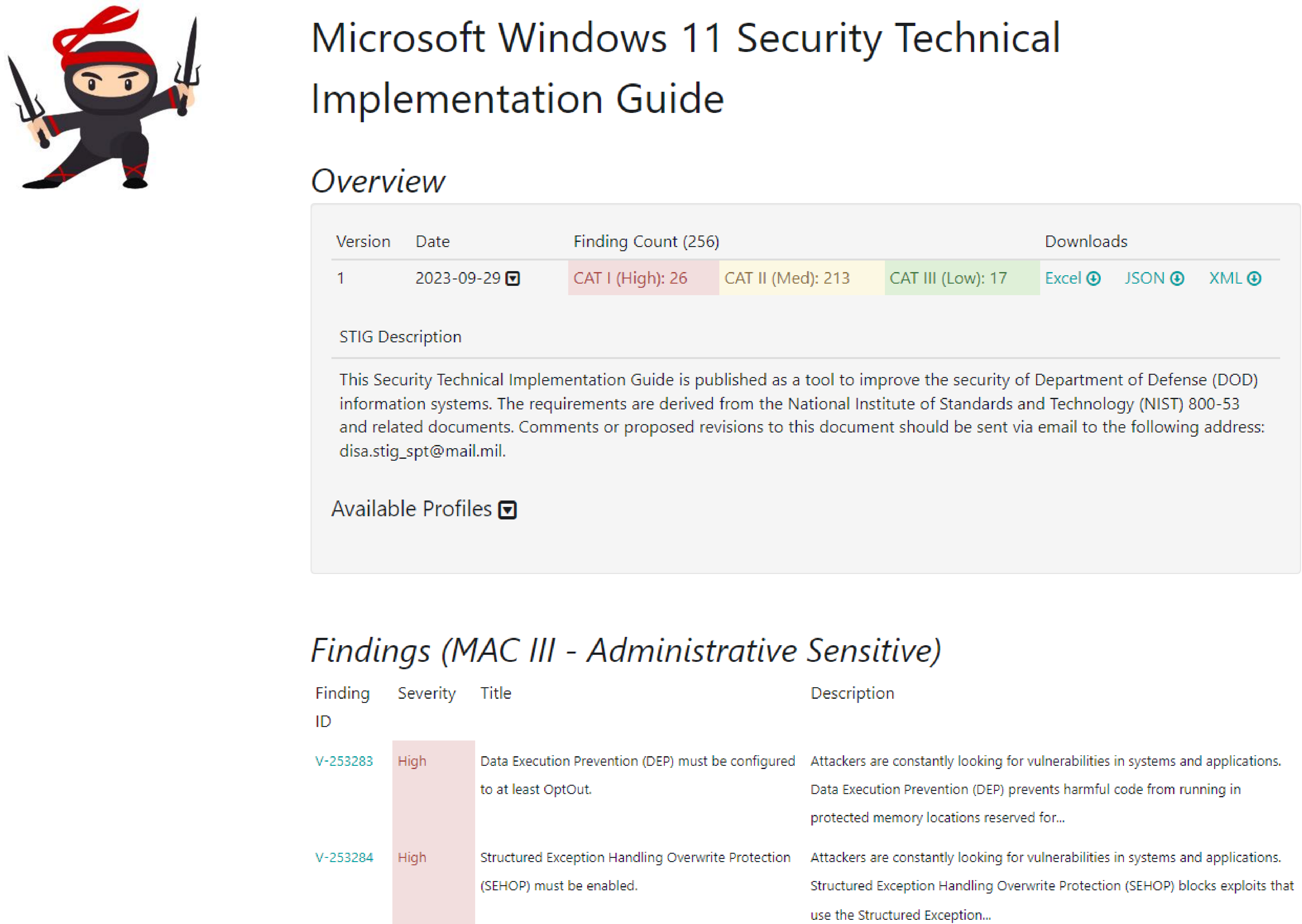
CIS Benchmark

Safeguard IT systems against cyber threats with these CIS Benchmarks. Click to download a PDF from the list of available versions.

LEARN MORE ABOUT CIS BENCHMARK →

Recent versions available for CIS Benchmark:

- Microsoft Windows 11 Enterprise (3.0.0)
- Microsoft Windows 11 Stand-alone (2.0.0)
- Microsoft Windows 10 EMS Gateway (2.0.0)
- Microsoft Windows 10 Enterprise (3.0.0)
- Microsoft Windows 10 Enterprise Release 2004 (1.9.1)
- Microsoft Windows 10 Enterprise Release 1909 (1.8.1)
- Microsoft Windows 10 Enterprise Release 1903 (1.7.1)



Microsoft Windows 11 Security Technical Implementation Guide

Overview

Version	Date	Finding Count (256)			Downloads		
1	2023-09-29 ▾	CAT I (High): 26	CAT II (Med): 213	CAT III (Low): 17	Excel ⬇	JSON ⬇	XML ⬇

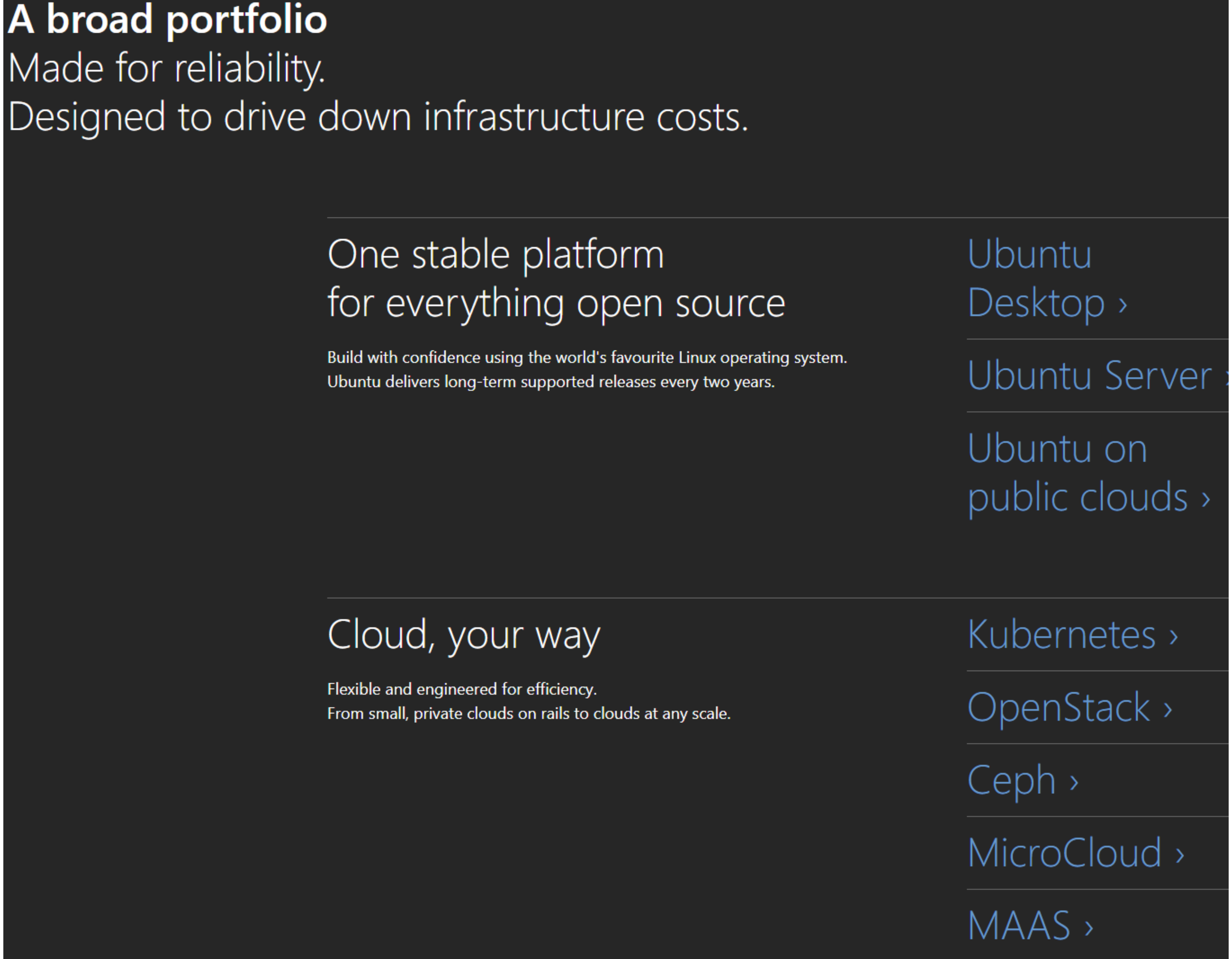
STIG Description

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DOD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Available Profiles ▾

Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-253283	High	Data Execution Prevention (DEP) must be configured to at least OptOut.	Attackers are constantly looking for vulnerabilities in systems and applications. Data Execution Prevention (DEP) prevents harmful code from running in protected memory locations reserved for...
V-253284	High	Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.	Attackers are constantly looking for vulnerabilities in systems and applications. Structured Exception Handling Overwrite Protection (SEHOP) blocks exploits that use the Structured Exception...



A broad portfolio

Made for reliability.
Designed to drive down infrastructure costs.

One stable platform for everything open source

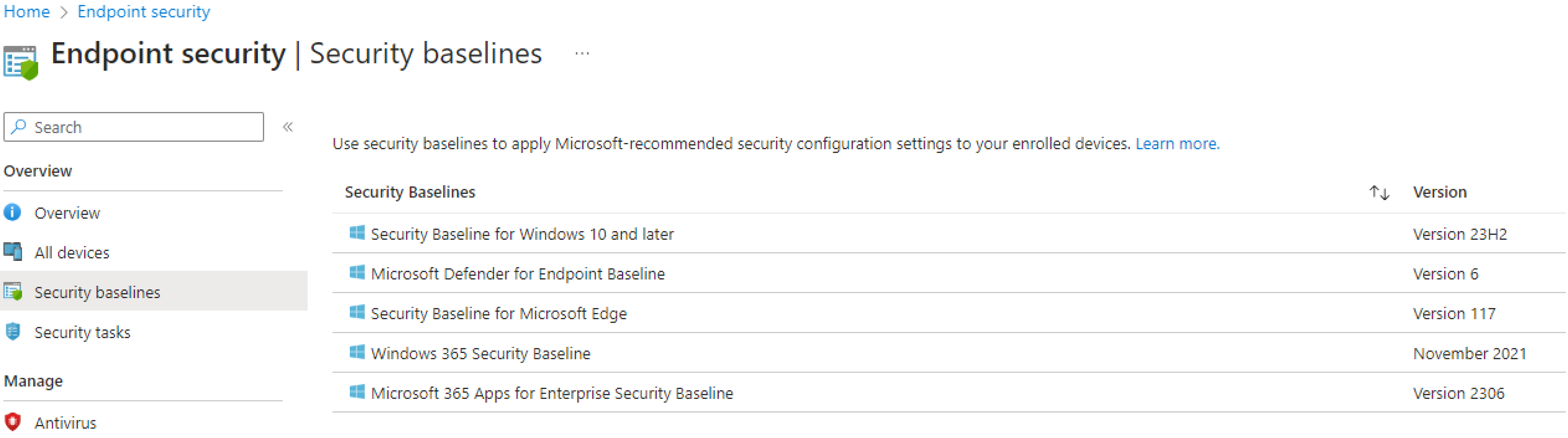
Build with confidence using the world's favourite Linux operating system.
Ubuntu delivers long-term supported releases every two years.

- Ubuntu Desktop ›
- Ubuntu Server ›
- Ubuntu on public clouds ›

Cloud, your way

Flexible and engineered for efficiency.
From small, private clouds on rails to clouds at any scale.

- Kubernetes ›
- OpenStack ›
- Ceph ›
- MicroCloud ›
- MAAS ›

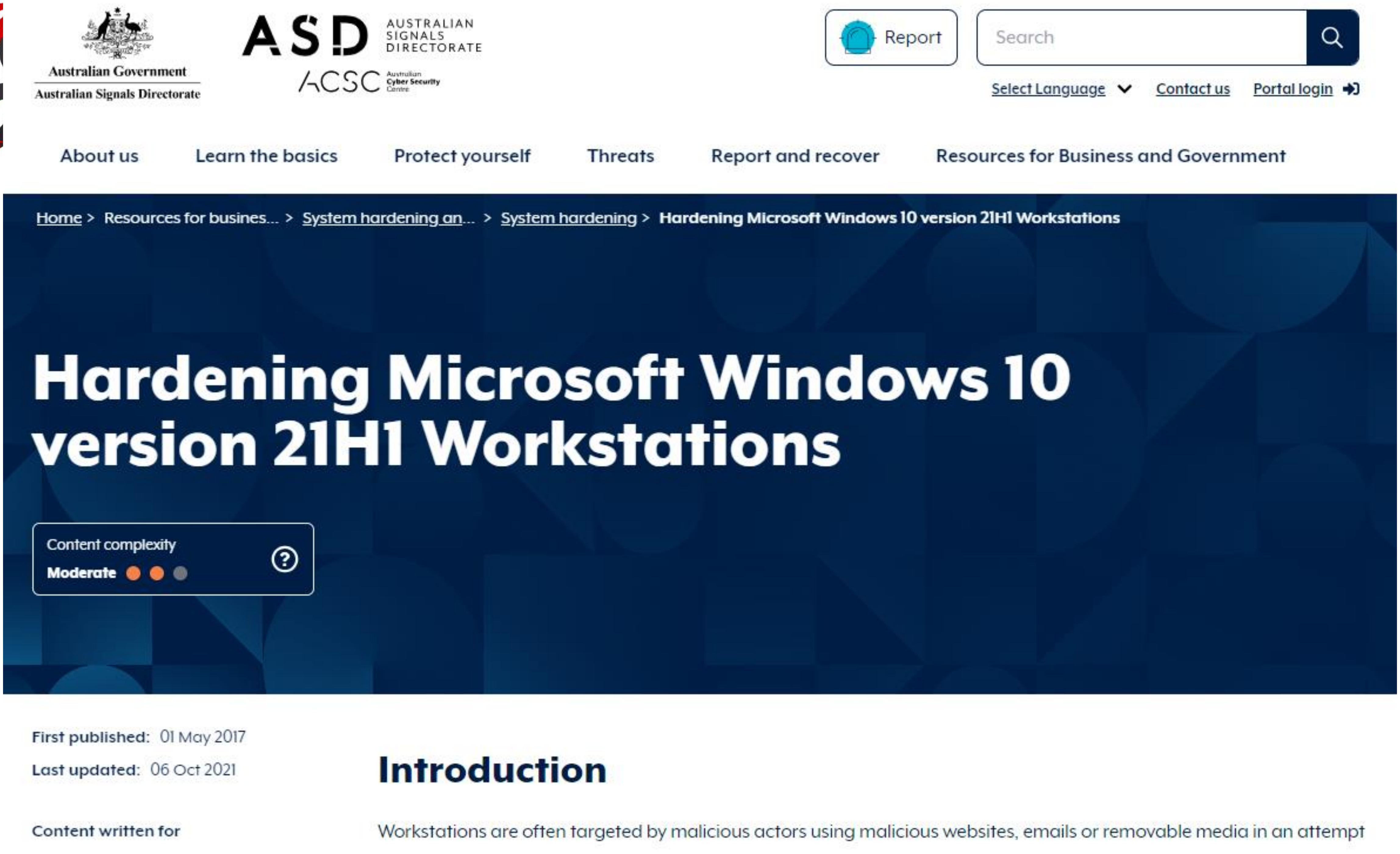


Home > Endpoint security

Endpoint security | Security baselines ...

Use security baselines to apply Microsoft-recommended security configuration settings to your enrolled devices. Learn more.

Security Baselines ↑↓	Version
Security Baseline for Windows 10 and later	Version 23H2
Microsoft Defender for Endpoint Baseline	Version 6
Security Baseline for Microsoft Edge	Version 117
Windows 365 Security Baseline	November 2021
Microsoft 365 Apps for Enterprise Security Baseline	Version 2306



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Report
Search
Select Language
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government
Home > Resources for busines... > System hardening an... > System hardening > Hardening Microsoft Windows 10 version 21H1 Workstations

Hardening Microsoft Windows 10 version 21H1 Workstations

Content complexity
Moderate ● ● ●

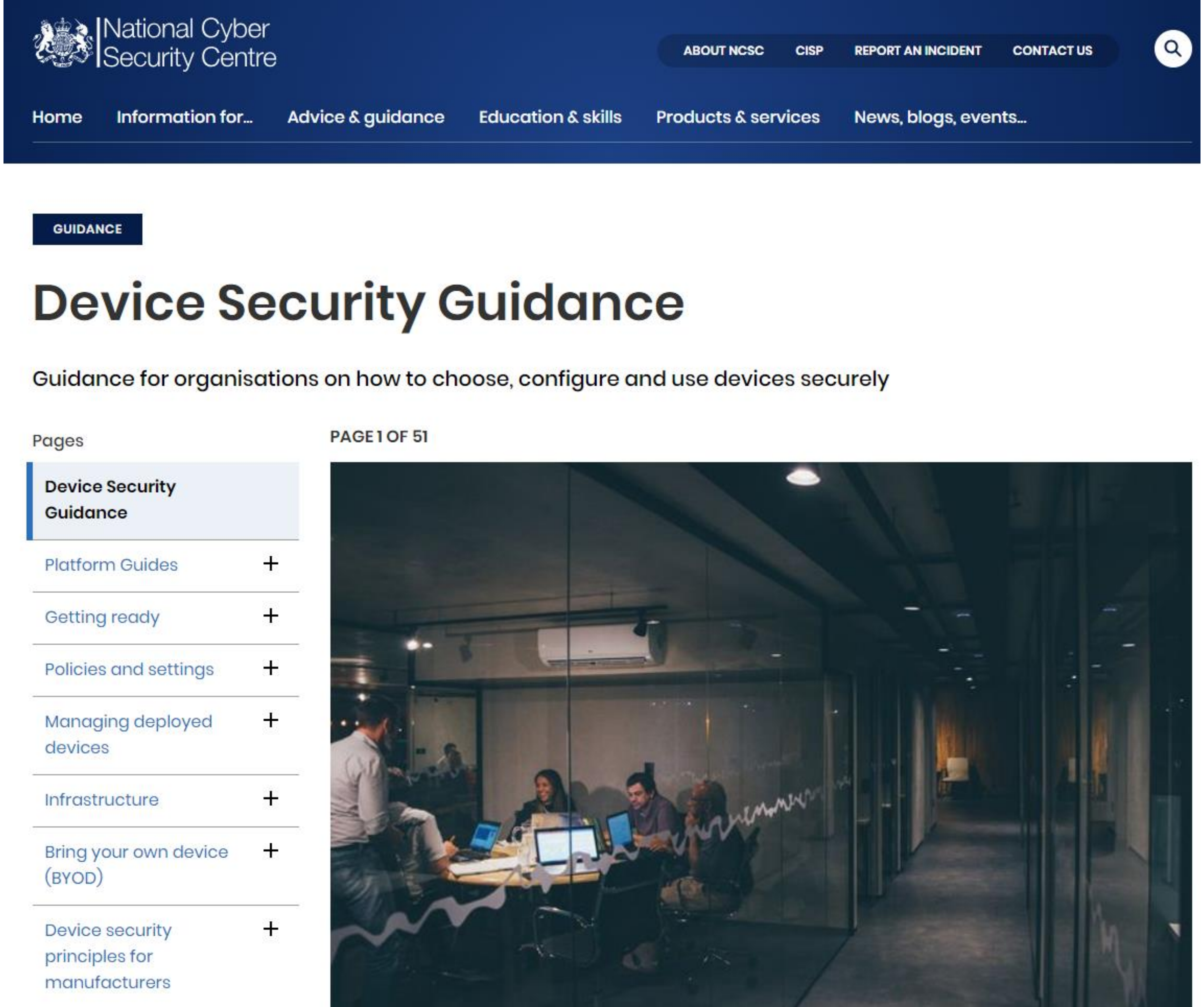
First published: 01 May 2017

Last updated: 06 Oct 2021

Content written for

Introduction

Workstations are often targeted by malicious actors using malicious websites, emails or removable media in an attempt



Device Security Guidance

Guidance for organisations on how to choose, configure and use devices securely

Uff, what options we have and have to implement?

- There are a lot of benchmarks around
- Cyber security have to be in our DNA
- Device Security, Hardening of anything
- Patching (not only OS level!)
- Baselines
- Regulations
- Confusing about how to and why
- Order from Company to get Certified (ISO, etc.)

At the end, every User in our Company has to be able to work and do the Job!

How to Start to cover anything

There is no: “Cover anything” because it’s to much

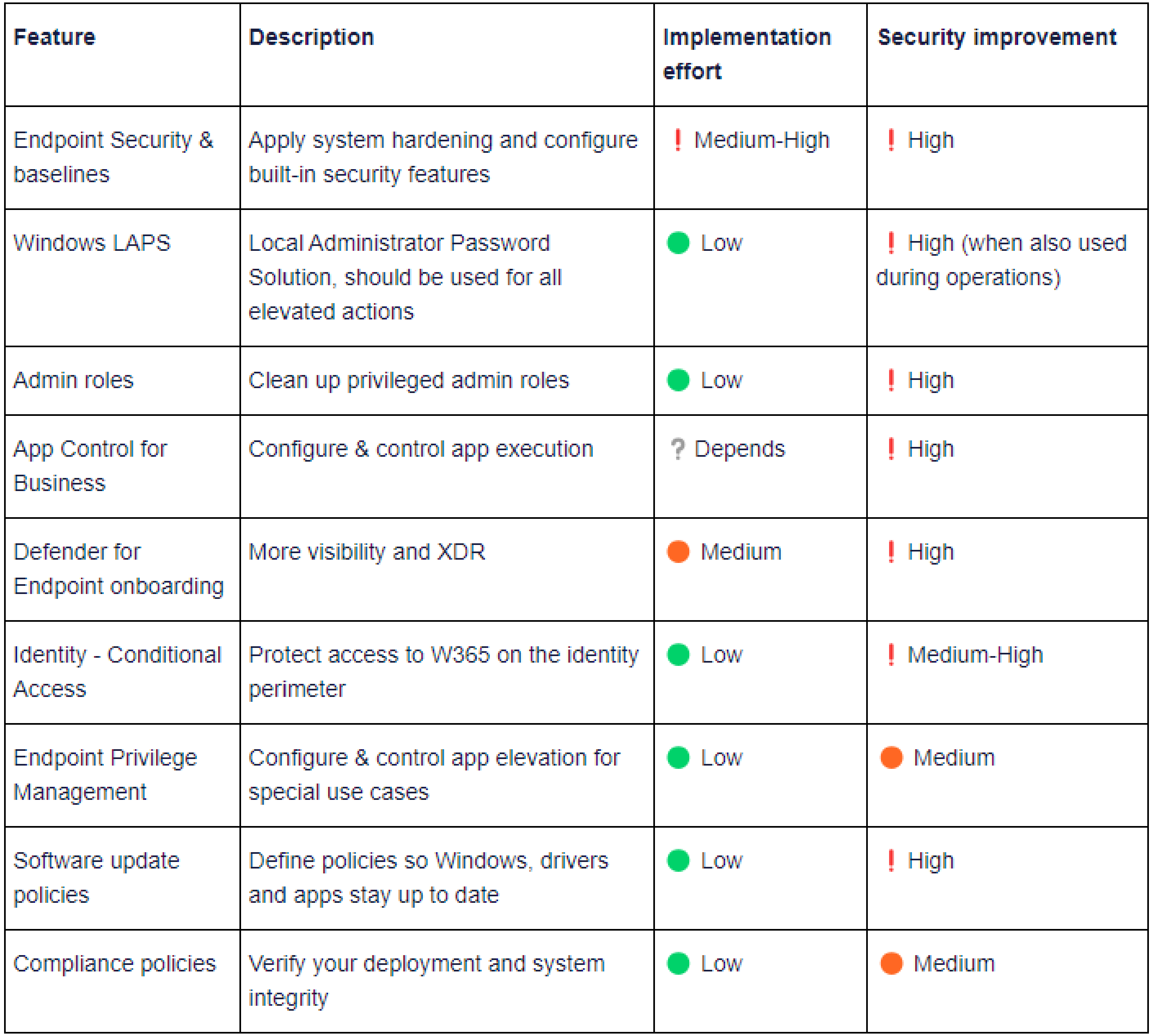
- What are the Business needs
- Create use cases
- Use cases need regulations or certification
- Start reading the Benchmarks, to add it to each use case
- Check the MS-Baselines
  - Not only for Windows

Wait there is more

Try to keep it simple!

Documentation FTW!

- Attack surface reduction
- EDGE
- Other OS, like macOS, Linux, Android, iOS, ipadOS



Feature	Description	Implementation effort	Security improvement
Endpoint Security & baselines	Apply system hardening and configure built-in security features	❗ Medium-High	❗ High
Windows LAPS	Local Administrator Password Solution, should be used for all elevated actions	🟢 Low	❗ High (when also used during operations)
Admin roles	Clean up privileged admin roles	🟢 Low	❗ High
App Control for Business	Configure & control app execution	❔ Depends	❗ High
Defender for Endpoint onboarding	More visibility and XDR	🟠 Medium	❗ High
Identity - Conditional Access	Protect access to W365 on the identity perimeter	🟢 Low	❗ Medium-High
Endpoint Privilege Management	Configure & control app elevation for special use cases	🟢 Low	🟠 Medium
Software update policies	Define policies so Windows, drivers and apps stay up to date	🟢 Low	❗ High
Compliance policies	Verify your deployment and system integrity	🟢 Low	🟠 Medium

Thank you
Niklas Tinner

Are there some Help around

Yes, community tools

Documentation FTW!

- SkipToTheEndpoint/OpenIntuneBaseline: Community-driven baseline to accelerate Intune adoption and learning. (github.com)
- ThomasKur/M365Documentation: Automatic Microsoft 365 Documentation to simplify the life of admins and consultants. (github.com)
- alexverboon/IntuneCustomCompliance: Microsoft Intune Custom Compliance (github.com)
- Sander Rozemuller | All about Identity, AVD, Automation, DevOps, Monitoring, Intune and Security

It’s easy to be complicated, but very complicated to keep it easy!

—— Mirko Colemberg ——

baseVISION

SECURE & MODERN ENDPOINT MANAGEMENT

MVP Microsoft® Most Valuable Professional

Mirko Colemberg

Senior Expert Endpoint Consultant

Contact Me

- Twitter: https://twitter.com/mirkocolemberg
- Blog: http://blog.colemberg.ch
- Mail: mirko.colemberg@basevision.ch
- Phone: +41 79 410 48 22

Session Feedback