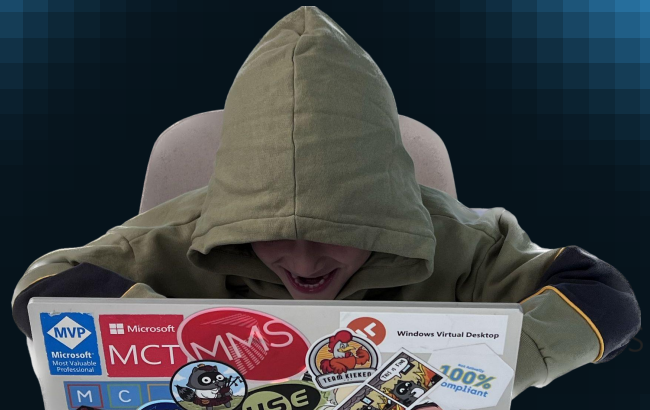
MEMUG SCOTLAND – My 5 Golden (Intune) Tips

Tim Hermie
@_Cloud_boy



Tim Hermie

@_Cloud_boy

Microsoft MVP Enterprise Mobility

Modern Workplace Architect

Founding Board Member MC2MC

SECURITY

PARK

Microsoft

SECURITY

INSPARK

Microsoft

Agenda

- Some stats and what to do about it
- What is mandatory?
- Microsoft Security Features
- Security Baselines
- Conclusion

Some statistics and what to do about it!

SECURITY

Stats

	2018	2022
MFA Enabled for Admin accounts	1,8 %	26,64 %
Breach Replay Attacker-driven sign-ins detected	4,6 Billion	5,8 Billion
Password Spray Compromised accounts detected	350.000	5 Million
Phishing High-risk enterprise sign-ins detected	23 Million	31 Million

soft


MVP
Microsoft
Most Valuable Professional
Microsoft
MCT
MMS
Windows Virtual Desktop
TEAM KIEKEN
100%
ompliant
TUSE
I Survived
MMS MOA
2022
SCAPPMAN
MMS

TIP 1

Require MFA for ALL accounts

+ Only ALLOW access to corporate resources from MANAGED devices

TIP 1

If you allow access to corporate resources from UNMANAGED devices:

- Use CAE (Continuous Access Evaluation)
- Apply Non-Persistent Browser sessions in your CA policy +
- Force re-authentication with sign-in frequency in your CA policy

What is mandatory?

TIP 2 & 3

Don’t make your users local admin on their devices. Not for any scenario.

Keep your Windows versions patched (either Feature & Quality updates)

Update your 3rd party apps

TIP 2 & 3

Use a solution like Admin By Request (or wait for the MS built-in solution for privilege elevation)

Windows Update for Business (low deferral)

SCAPPMAN or Patch My PC

SECURITY

TIP 4
Microsoft Security Features

Credential Guard

Isolate and harden key system and user secrets against compromise

Minimize the impact and breadth of a Pass the Hash style attack in the event that malicious code is already running via a local or network based vector

Bitlocker

Data protection feature that integrates with the OS and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers

Recommendation: Cycle keys + also USB

SmartScreen

Anti-phishing and anti-malware support

Reputation-based URL and app protection

OS integration

Block URLs associated with potentially unwanted applications

ASR rules

Leave hackers with fewer ways to perform attacks

ASR rules target certain software behaviors as:

- Launching executable files and scripts
- Running obfuscated or otherwise suspicious scripts
- Performing behaviors that apps don't usually initiate during normal day-to-day work

ASR rules

For gradual rollout:

- Audit
- Monitor
- Block what you can
- Finetune
- Block more
- Reports: use MDE or KQL

WhfB – Account Protection

Use Windows Hello for Business

- It's a form of MFA
- PIN is linked with device, not USER
- Leverage Cloud Trust to allow access to on-premises resources with WhfB

TIP 5
Security Baseline

Device configuration (DC)

Windows 10 profile

1. Security baselines
2. Endpoint Security
3. Settings Catalog
4. Administrative Templates Custom

1. Start with security baselines – Microsoft's recommended best practice configuration. Remake the baseline with Settings Catalog / Administrative Templates
2. Make your Endpoint Security configuration in the blade made for it. Use it for AV, Bitlocker, ASR, … (all Endpoint Security Features)
3. Fill up the gap with Settings Catalog
4. What's not yet migrated to Settings Catalog fill up with Administrative Templates and/or Custom

Dynamic Device Group

Security Baseline

Create your OWN security baseline for:

- Windows
- iOS
- Android
- MacOS
- BYOD = MAM

How to create a good baseline?

For Windows: you can use the Microsoft Security and Compliance toolkit as a start

Put a layer on top with the CIS baselines (lvl 1 – lvl 2)

How to create a good baseline?

For macOS:

Use the CIS baselines

For Android/iOS:

Unmanaged: use MAM

App Protection Policy Data Framework

Managed: use CIS

Must do's:

Update your baselines with each new version that comes out

Don't deploy in PRD, use rings for gradual rollout and minimize impact

MONITOR your baselines for drift changes

Exclusions:

Don’t allow exclusions unless it is necessary

Don’t take settings out of the baseline

Duplicate the baseline, remove settings and apply to select target group

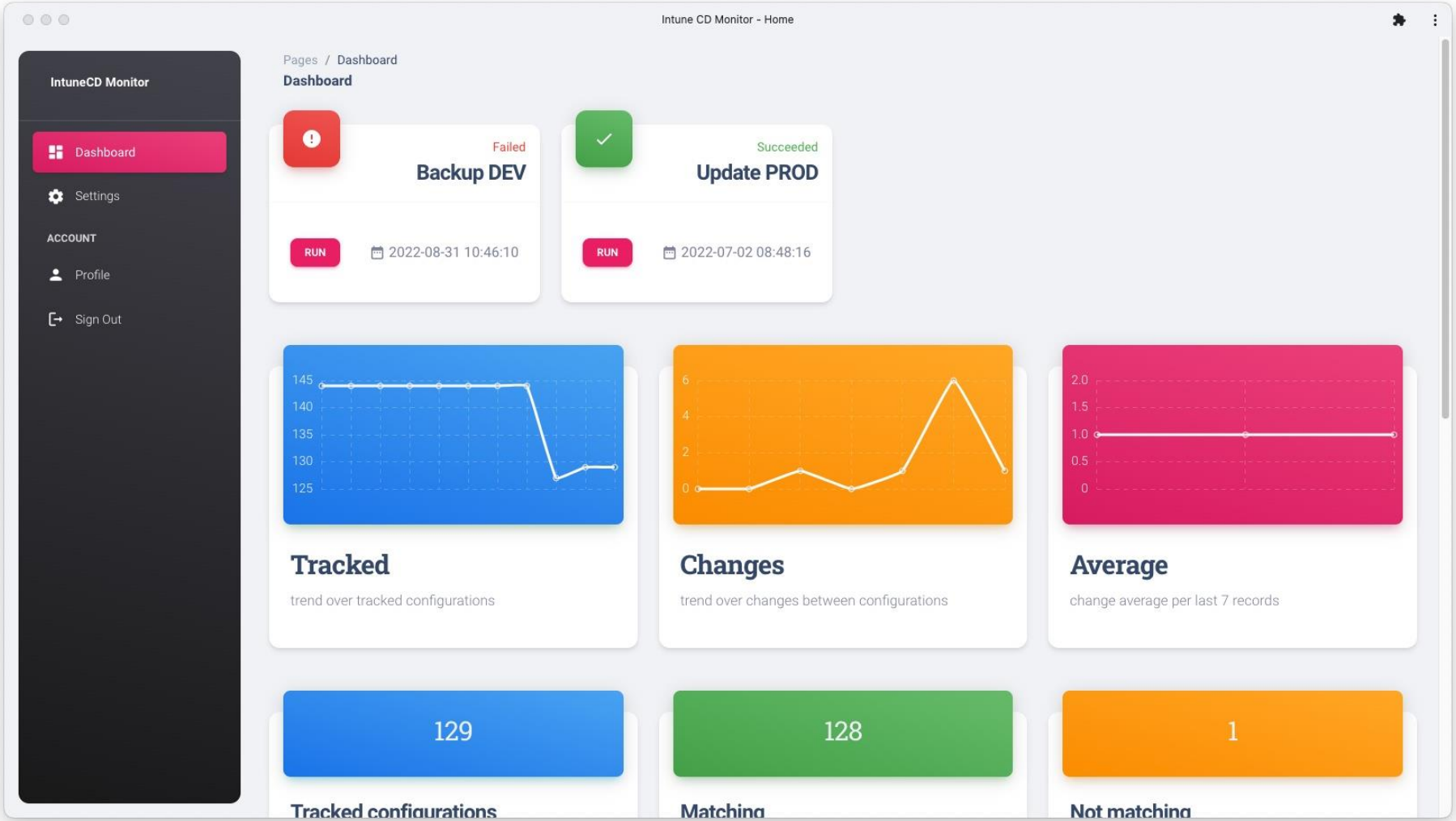
MONITOR for drift changes

Monitoring options

Leverage PowerShell and write your own code

Use community tools like IntuneCD:

https://github.com/almenscorner/IntuneCD


Intune CD Monitor - Home
IntuneCD Monitor
Dashboard
Settings
ACCOUNT
Profile
Sign Out
Pages / Dashboard
Dashboard
Failed
Backup DEV
RUN
2022-08-31 10:46:10
Succeeded
Update PROD
RUN
2022-07-02 08:48:16
145
140
135
130
125
Tracked
trend over tracked configurations
6
4
2
0
Changes
trend over changes between configurations
2.0
1.5
1.0
0.5
0
Average
change average per last 7 records
129
Tracked configurations
128
Matching
1
Not matching

Extra (with license)

Microsoft Defender Vulnerability Management Add-on

(Now in Preview)

CIS baselines (and much more integrated with MDE like NIST, MS, …)

Assess with MDE

Extra's

Extra's

Leverage Group Policy Analytics to easily recreate MS Security Baseline

Download Security And Compliance Toolkit

Upload in Policy Analytics (GPO)

Migrate with Policy Analytics

Extra's

Fun tool for monitoring / deploying:

Hardening Kitty

https://github.com/scipag/HardeningKitty

Conclusion

Conclusion

MFA!!!

Managed devices!!!

No local admins!!!

Patch everything!!!

And yes also 3rd party apps!!!

Conclusion

Leverage the MS Security Features

Put time in creating your Security Baseline

UPDATE THEM!

MONITOR THEM!

Don’t allow EXCL unless really necessary

Thank you for listening, questions?