

Implement Windows defender gradual rollout

- Mattias Melkersen Kalvåg
- Senior consultant - Mindcore
- Twitter @MMelkersen
- MVP Enterprise Mobility



NORDIC

— VIRTUAL SUMMIT —

Implement Windows defender gradual rollout

- Kent Agerlund
- Principal consultant – twoday CTGlobal
- LinkedIn: <https://www.linkedin.com/in/kentagerlund/>
- Microsoft Regional Director
- MVP Enterprise Mobility



NORDIC

– VIRTUAL SUMMIT –

Defender gradual rollout

WHY?

Early failure detection...

To catch impact as it occurs and address it quickly before a larger rollout.



RISK = HAZARD x EXPOSURE

Remember January 13th?

KEEP CALM

It's Friday the 13th!



Windows Update ✓
@WindowsUpdate

After installing security intelligence update build 1.381.2140.0 for Microsoft Defender, application shortcuts in the Start menu, pinned to the taskbar, and on the Desktop might be missing or deleted.
learn.microsoft.com/en-us/windows/...

Microsoft 365 Status ✓ @MSFT365Status · 13. jan.

Svarer [@MSFT365Status](#)

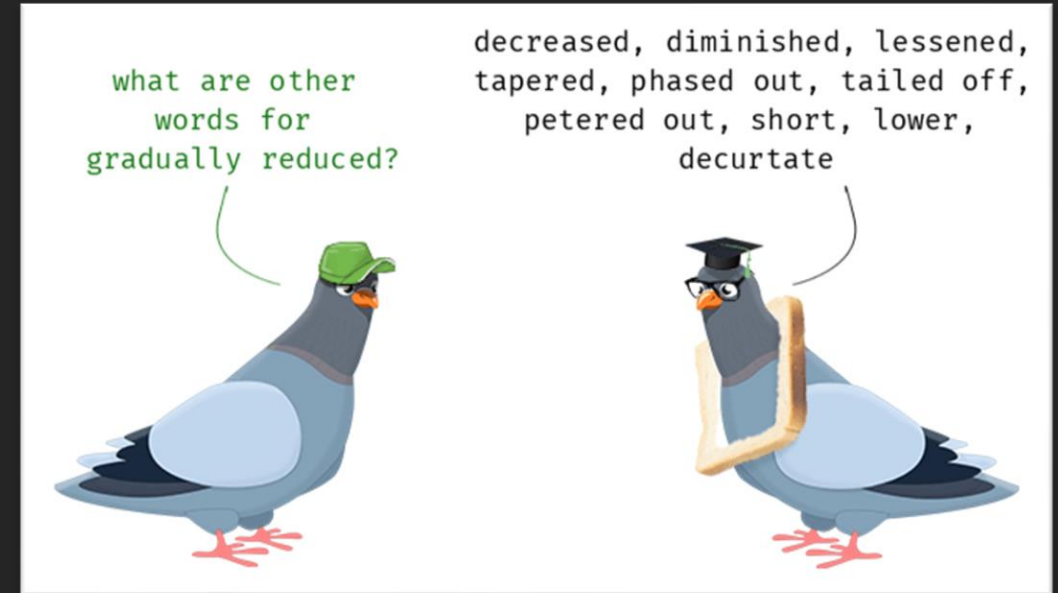
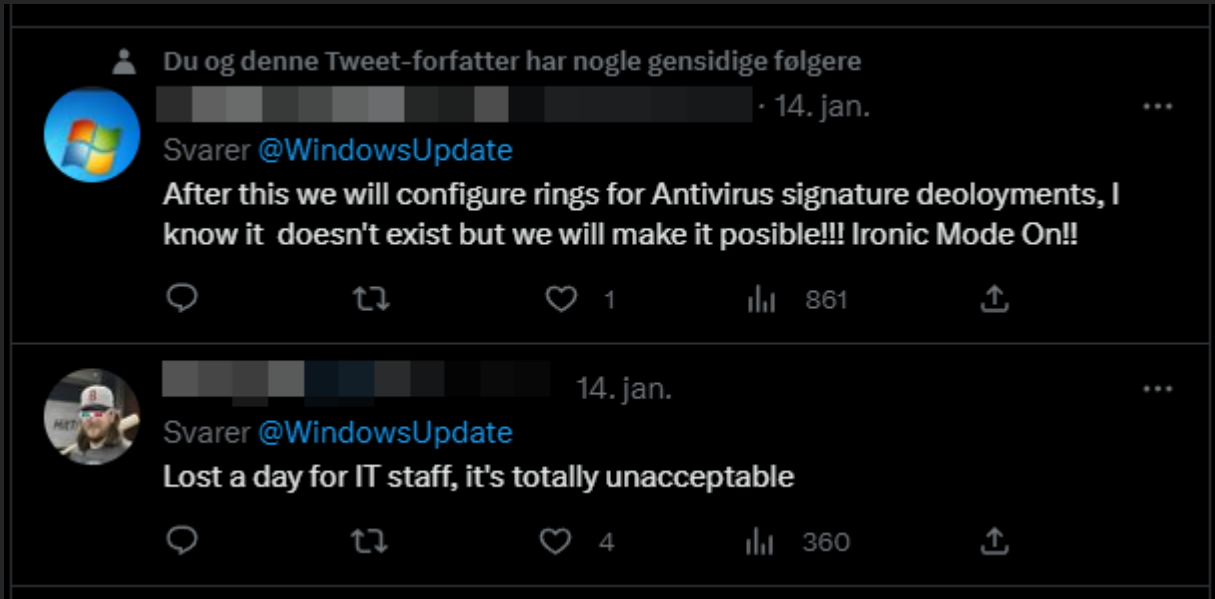
The revert is in progress and may take several hours to complete. We recommend placing the offending ASR rule into Audit Mode to prevent further impact until the deployment has completed. For more details and instructions, please follow the SI MO497128 in your admin center.



Microsoft 365 Status ✓
@MSFT365Status

We've identified that a specific rule was resulting in impact. We've reverted the rule to prevent further impact whilst we investigate further. For more information, please follow the SI MO497128 in your admin center.

So, we ask again **WHY?**



So, this is not **YOU** next time something blow up, because you **reduced risk** by implementing gradual rollout!

Now you know WHY!

Application shortcuts might not work from the Start menu or other locations

Status	Originating update	History
Resolved	N/A	Resolved: 2023-01-18, 19:28 PT Opened: 2023-01-13, 13:40 PT

After installing security intelligence update build **1.381.2140.0** for Microsoft Defender, application shortcuts in the Start menu, pinned to the taskbar, and on the Desktop might be missing or deleted. Additionally, errors might be observed when trying to run executable (.exe) files which have dependencies on shortcut files. Affected devices have the **Attack Surface Reduction (ASR)** rule **"Block Win32 API calls from Office macro"** enabled. After installing security intelligence build 1.381.2140.0, detections resulted in the deletion of certain Windows shortcut (.lnk) files that matched the incorrect detection pattern.

Source: [Windows 11, version 22H2 known issues and notifications | Microsoft Learn](#)

Change logs for security intelligence update version 1.381.2140.0

This page lists newly added and updated threat detections included in security intelligence updates for [Microsoft Defender Antivirus](#) and other Microsoft antimalware. If you don't find the latest security intelligence update version in the selector below, please refresh this page or let us know us know through the feedback smiley.

Looking for the latest update? [Download the latest update](#)

Security intelligence update version

1.381.2140.0



▼

Released on

1/13/2023 8:21:49 AM



Added threat detections

Name	Severity
 	Severe
Behavior:Win32/Cartel.SA	Severe
Behavior:Win32/LnkLaunchSusProc.SB	Severe
Ransom:Win64/Cartel.SA	Severe

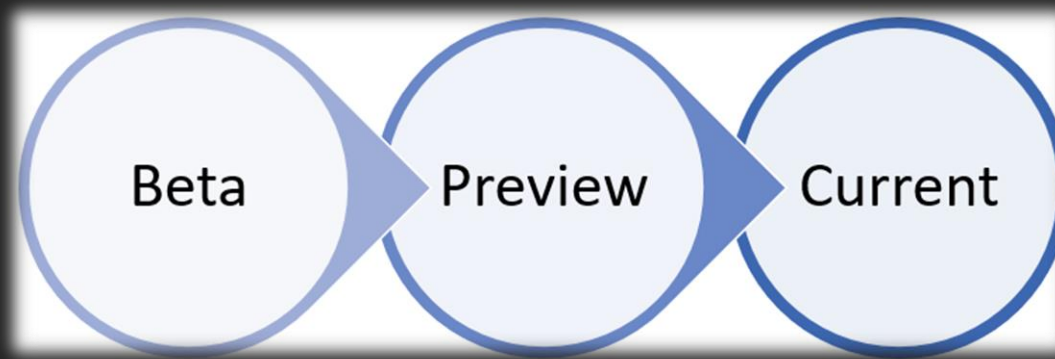
Overview of Microsoft Defender components

Update type	Description	Release	Source
Security intelligence updates	New and updated malware detections	Multiple times a day	Antimalware updates change log - Microsoft Security Intelligence
Engine updates	Updates to core detection engine	Monthly	Manage Microsoft Defender Antivirus updates and apply baselines Microsoft Learn
Platform updates	Updates to the product. New features and fixes	Monthly	Manage Microsoft Defender Antivirus updates and apply baselines Microsoft Learn

Update channels for **monthly updates**

1. Beta Channel
2. Current Channel (Preview)
3. Current Channel (Staged)
4. Current Channel (Broad)
5. Critical

Test updates before others
Early gradual release
Later gradual release
Last gradual release
Delayed 48 hours

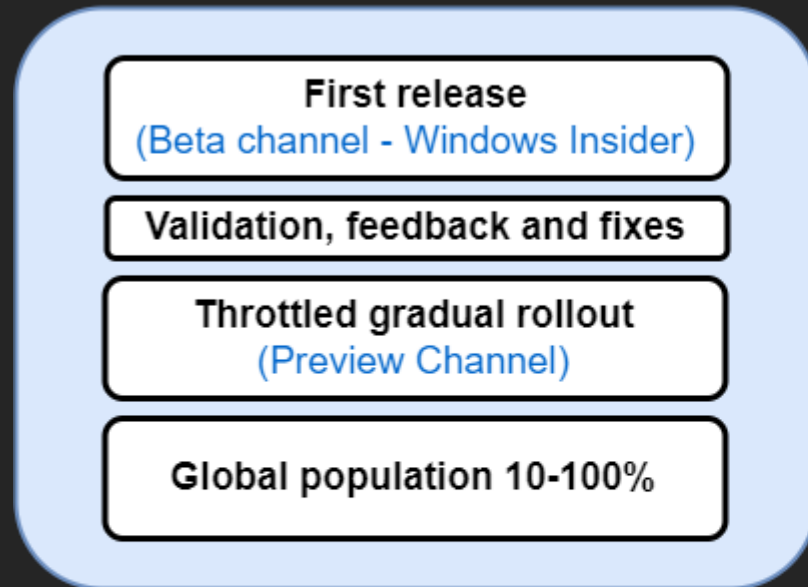


Update channels for **daily updates**

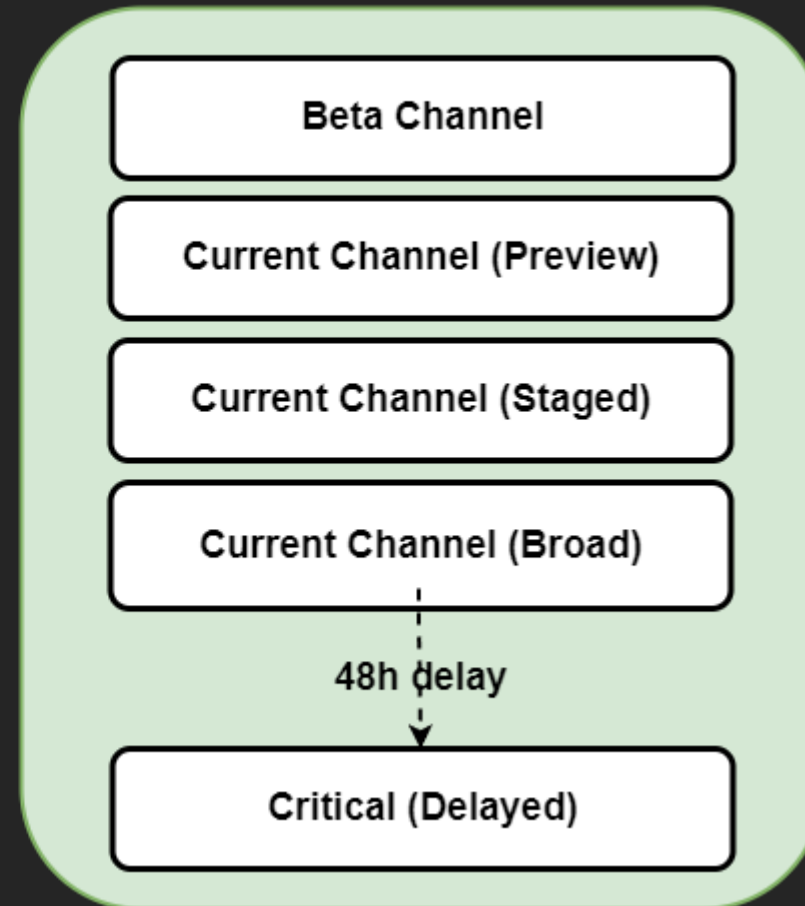
1. Beta Channel	Test updates before others
2. Current Channel (Preview)	Early gradual release
1. Current Channel (Staged)	Later gradual release
2. Current Channel (Broad)	Last gradual release
5. Critical	Delayed 48 hours

Default rollout vs gradual highlevel

Microsoft Defender gradual rollout model



Update Channels



Source: [Manage Microsoft Defender Antivirus updates and apply baselines](https://learn.microsoft.com/en-us/windows/defender/manage/updates) | Microsoft Learn

```
Administrator: Windows PowerShell
PS C:\Users\MattiasMelkersen> Invoke-RestMethod -Uri "https://www.microsoft.com/security/encyclopedia/adlpackages.aspx?action=info" | Select -ExpandProperty versions | Format-List

engine      : 1.1.19900.2
signatures  : signatures
platform    : 4.18.2211.5

PS C:\Users\MattiasMelkersen> Get-MpComputerStatus | Select AMEngineVersion, AMProductVersion, AntivirusSignatureVersion, AntivirusSignatureLastUpdated | Format-list | Format-List

AMEngineVersion      : 1.1.20000.2
AMProductVersion     : 4.18.2301.6
AntivirusSignatureVersion : 1.381.3303.0
AntivirusSignatureLastUpdated : 08-02-2023 04:08:08
```

Windows Insider

```
Administrator: Windows PowerShell
PS C:\Program Files\Windows Defender> Invoke-RestMethod -Uri "https://www.microsoft.com/security/encyclopedia/adlpackages.aspx?action=info" | Select -ExpandProperty versions | Format-List

engine      : 1.1.19900.2
signatures  : signatures
platform    : 4.18.2211.5

PS C:\Program Files\Windows Defender> Get-MpComputerStatus | Select AMEngineVersion, AMProductVersion, AntivirusSignatureVersion, AntivirusSignatureLastUpdated | Format-list | Format-List

AMEngineVersion      : 1.1.19900.2
AMProductVersion     : 4.18.2211.5
AntivirusSignatureVersion : 1.381.3303.0
AntivirusSignatureLastUpdated : 08-02-2023 04:08:08

PS C:\Program Files\Windows Defender>
```

Normal PROD

Ways to apply gradual rollout settings

1. Group policy
2. Intune
3. PowerShell

On-Prem / Hybrid / Legacy
Hybrid / Cloud only / Modern
all scenario



Using Intune for gradual rollout **HOW?**

No **template**

No **settings catalog**

No **endpoint security**



Defender CSP!

[Defender CSP - Windows Client Management | Microsoft Learn](#)

EngineUpdatesChannel

PlatformUpdatesChannel

SecurityIntelligenceUpdatesChannel

Configuration/EngineUpdatesChannel

Scope	Editions	Applicable OS
✓ Device ✗ User	✗ Home ✓ Pro ✓ Enterprise ✓ Education ✓ Windows SE	✓ Windows 10, version 1607 [10.0.14393] and later

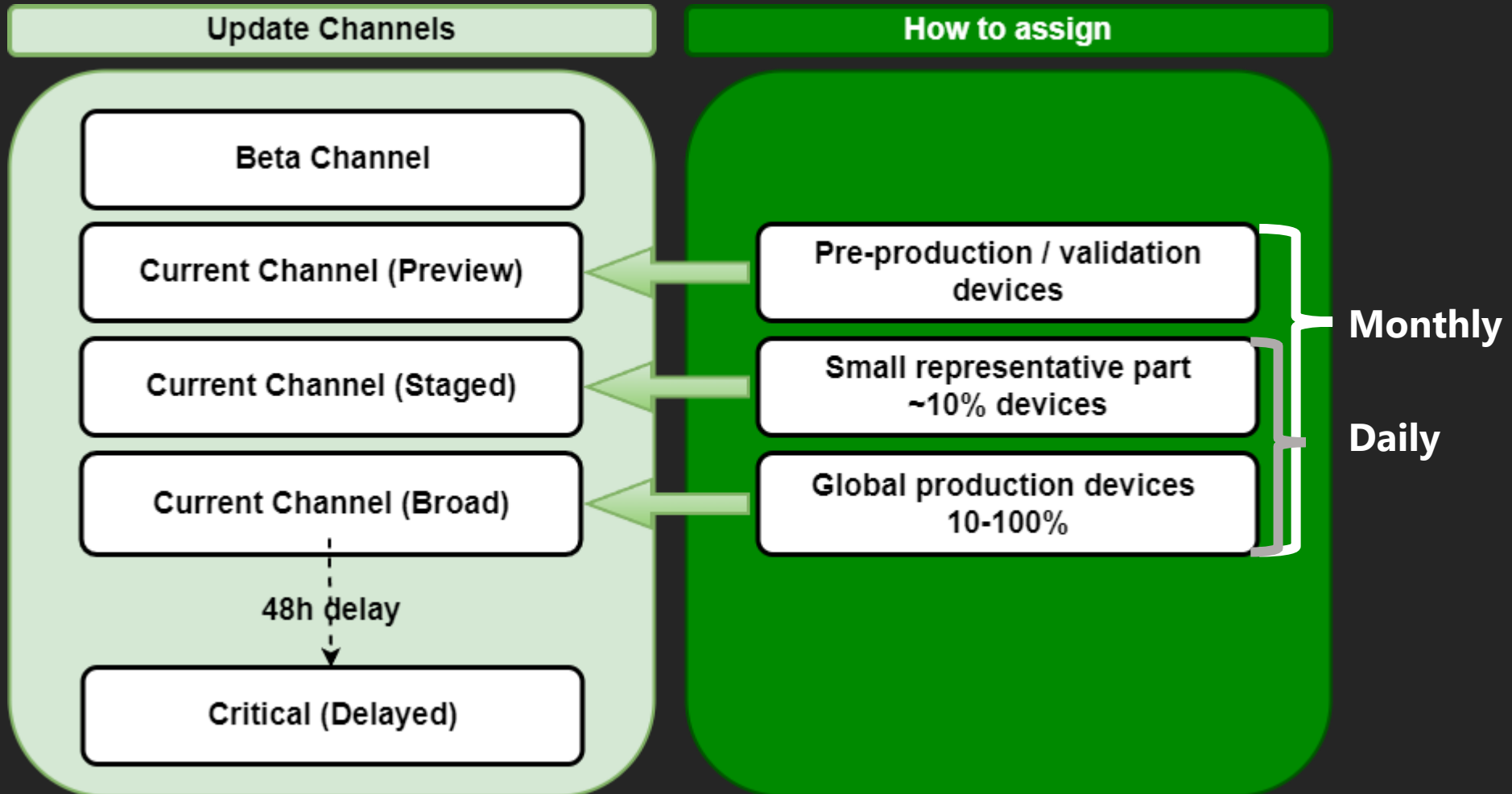
Configuration/PlatformUpdatesChannel

Scope	Editions	Applicable OS
✓ Device ✗ User	✗ Home ✓ Pro ✓ Enterprise ✓ Education ✓ Windows SE	✓ Windows 10, version 1607 [10.0.14393] and later

Configuration/SecurityIntelligenceUpdatesChannel

Scope	Editions	Applicable OS
✓ Device ✗ User	✗ Home ✓ Pro ✓ Enterprise ✓ Education ✓ Windows SE	✓ Windows 10, version 1607 [10.0.14393] and later


Assign devices



Creating Ring rollout structure

DEMO





Creating Intune policies

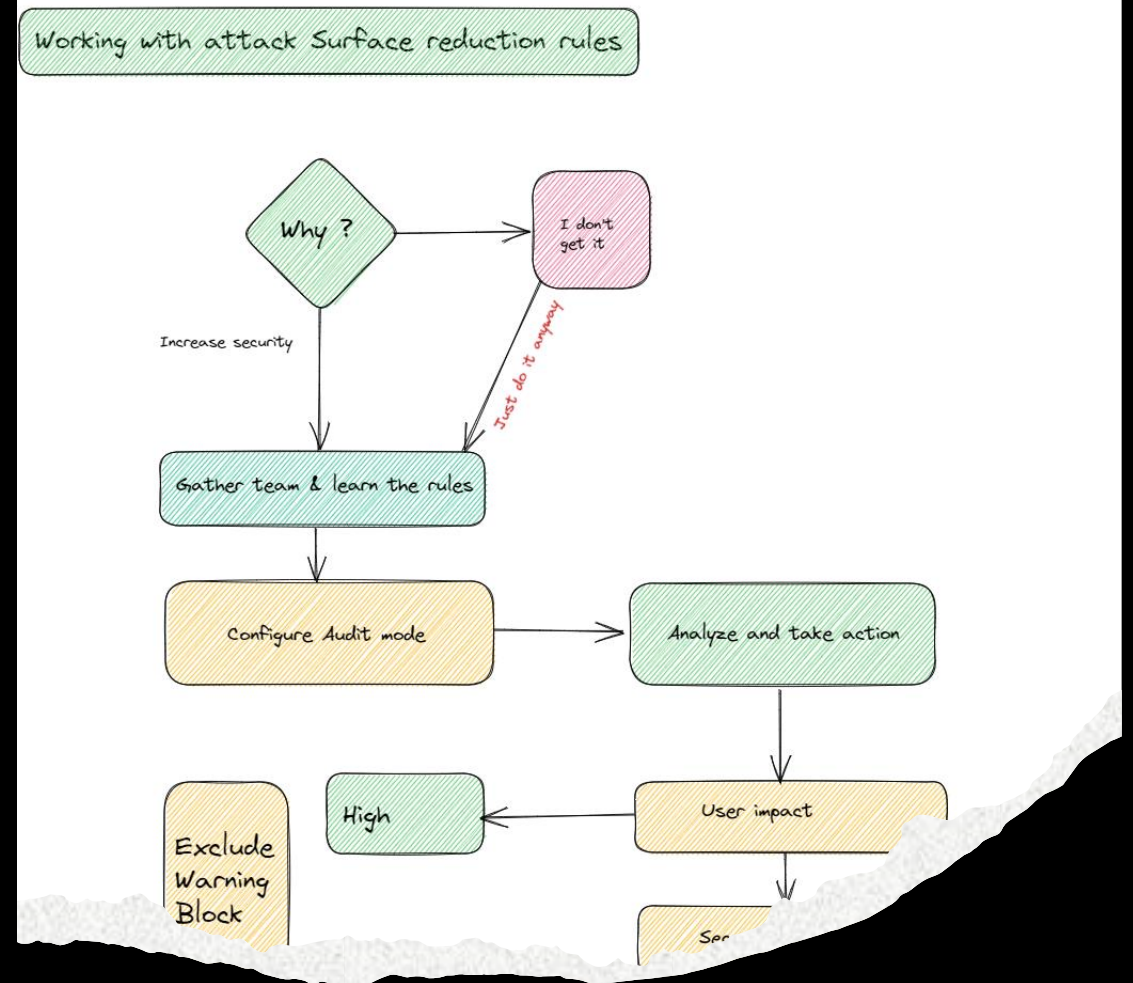
DEMO



Policies

Starting the Attack surface journey

DEMO



Other products to use gradual rollout

- Teams
- Edge
- OneDrive
- Microsoft 365 apps for ...
- Windows
- ...



Help YOUR company reduce risk

Updates needs to be installed whether you like it or not.

THANK YOU for attending!

Want to see more?

[How to start working with Attack Surface Reduction rules like a boss - YouTube](#)



Please give us feedback

Nordic Virtual Summit 2023 - 4th
edition

