



# Balancing Efficiency and Security - Unveiling the Risks in Cloud-Based Endpoint Management

Oleksandr Kazymyrov  
Sikkerhetsfestivalen 2024





Oleksandr Kazymyrov

Information Security Expert

Bergen, Vestland, Norway · [Contact info](#)

500+ connections



Open to

Add profile section

More

# Who am I?



# What is Storebrand?



## Storebrand: Comprehensive Financial Services and Management

### Overview:

- **Founded:** 1767
- **Headquarters:** Norway
- **Services:** Insurance, banking, asset management, and pensions
- **Focus:** Sustainability and ESG (Environmental, Social, and Governance) criteria

### Asset Management:

Storebrand is renowned for its extensive asset management services. The company manages a diverse portfolio of assets, emphasizing sustainable and responsible investment strategies. Their approach involves integrating ESG factors into the investment process to promote long-term value creation and risk management.



# Storebrand in the cloud



Microsoft Pulse



**TRANSFORMER**  
**BEDRIFTSOPTIMALISERING**

## Storebrand flyttet over 1000 milliarder kroner til skyen med Azure

AA pulse.microsoft.com



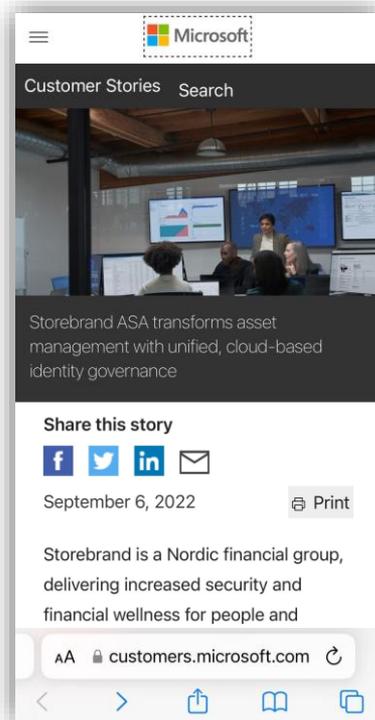
E24 Børs Bli abonnent

## Storebrand flytter hele kapitalforvaltningen ut i skyen

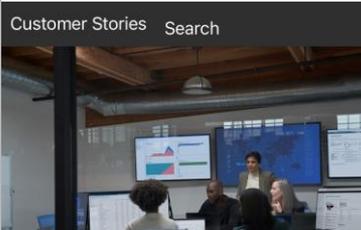
Som en av de første kapitalforvalterne i verden har Storebrand flyttet hele kapitalforvaltningen ut i en sky, noe som skal gi «uante muligheter». Nå vil flere banker følge etter.



AA e24.no



Microsoft Customer Stories Search



Storebrand ASA transforms asset management with unified, cloud-based identity governance

Share this story

September 6, 2022 Print

Storebrand is a Nordic financial group, delivering increased security and financial wellness for people and

AA customers.microsoft.com



FINANSWATCH Siste Søk Logg inn Meny

10.07.2023 | kl. 15:01 BANK

## Storebrand flytter Swift til skyen

Storebrand migrerer i disse dager infrastrukturen til Swift fra fysiske datasentre til en skybasert løsning.

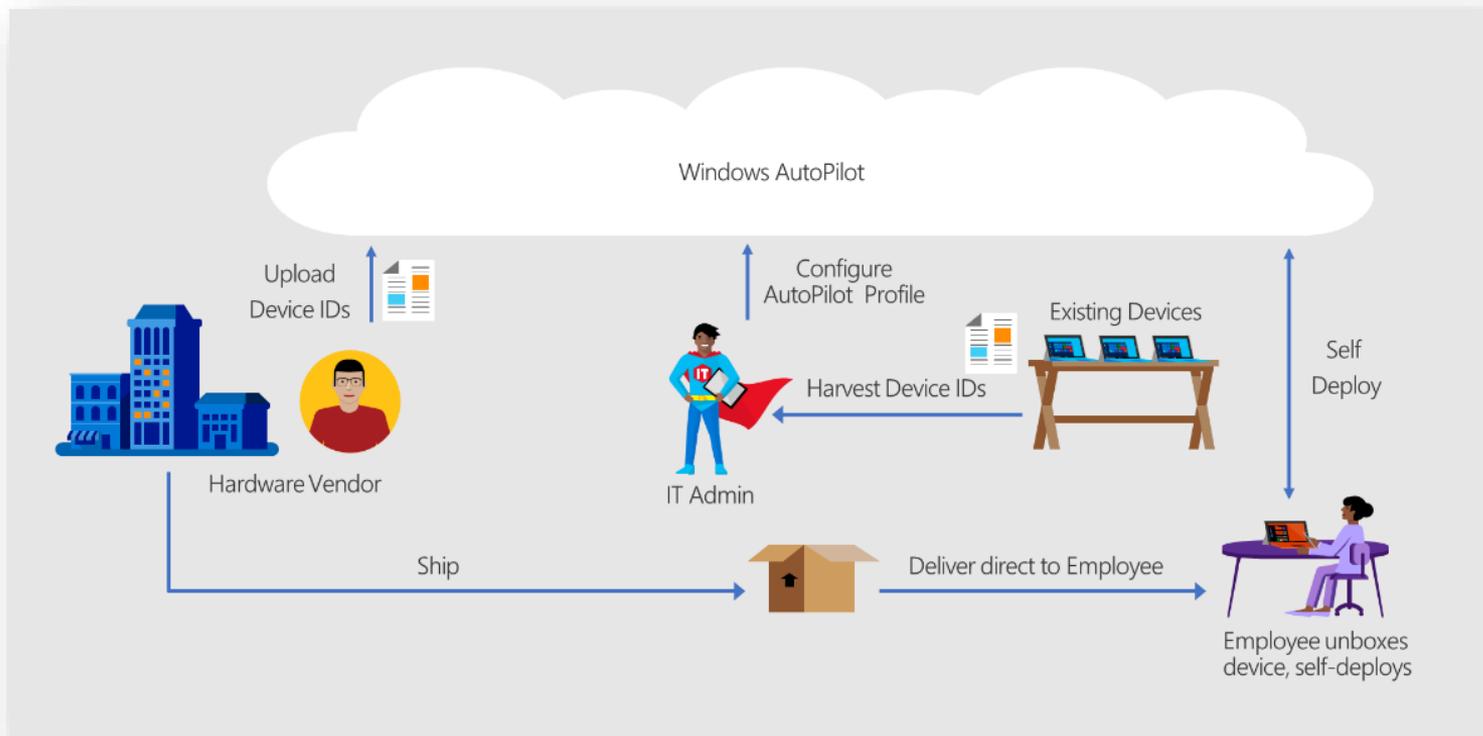


TRYGGERE: – Vi sparer selvsagt noe i året på å kutte ut serverne. Det viktigste er imidlertid at internasjonale pengetransaksjoner nå er både tryggere og enklere å drifte, sier konserndirektør Trygve Håkedal i Storebrand. | Foto: Storebrand

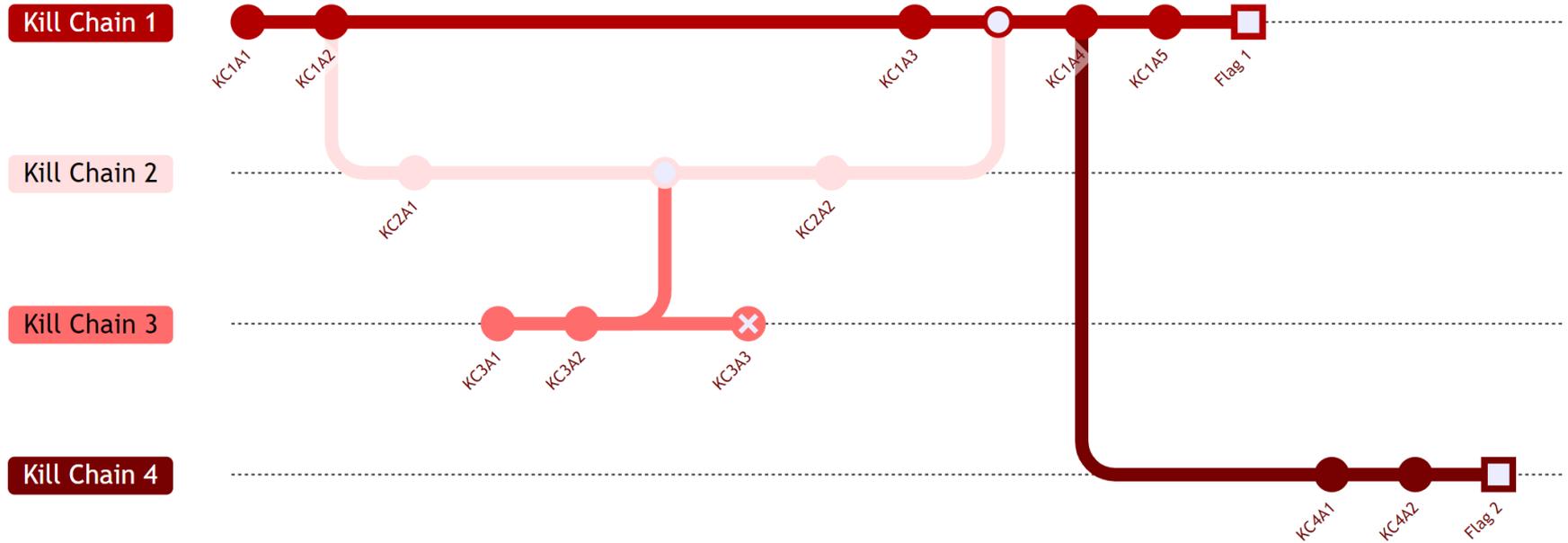
AA finanswatch.no



# Out-of-box experience (OOBE) via Intune

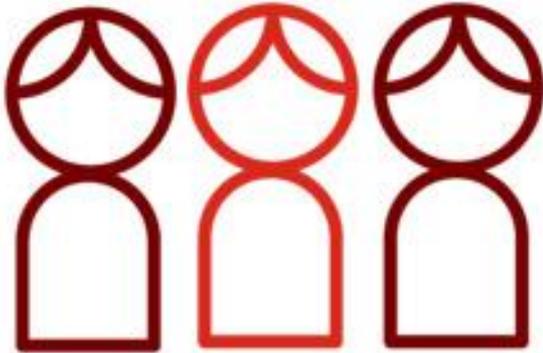


# Cyber kill chain for offensive operations



# Threat actors

Insider threat



Advance Persistence Threat



# Environment



The principle of least privilege is followed



Microsoft Intune is used as Mobile Device Management (MDM)

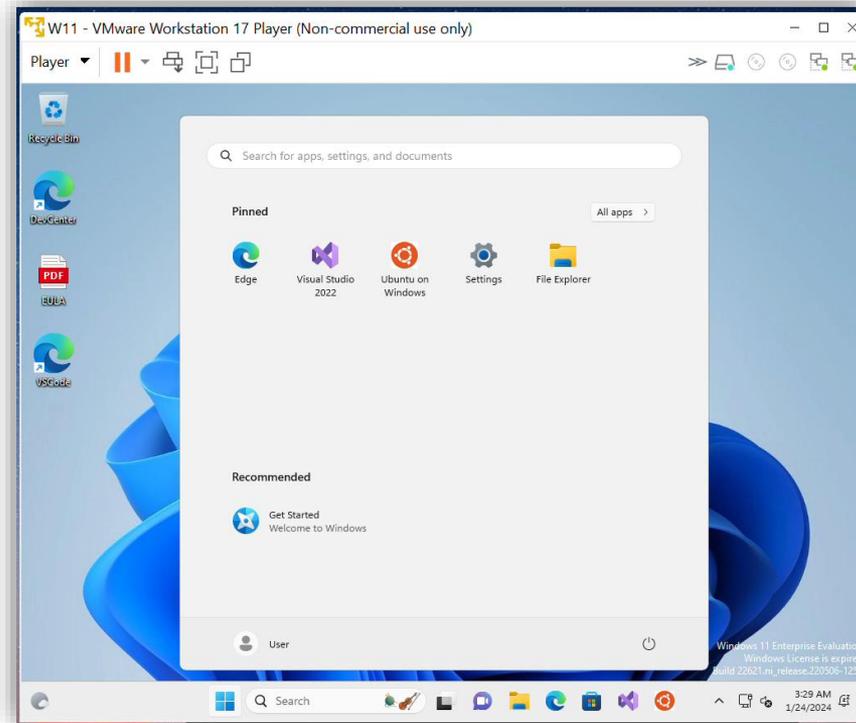


EDR is tuned

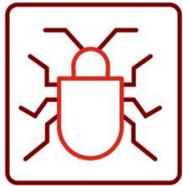


Requirements for compliant device in Conditional Access in Microsoft Entra ID

# Bypassing compliant device using VMWare



# Threat and goal



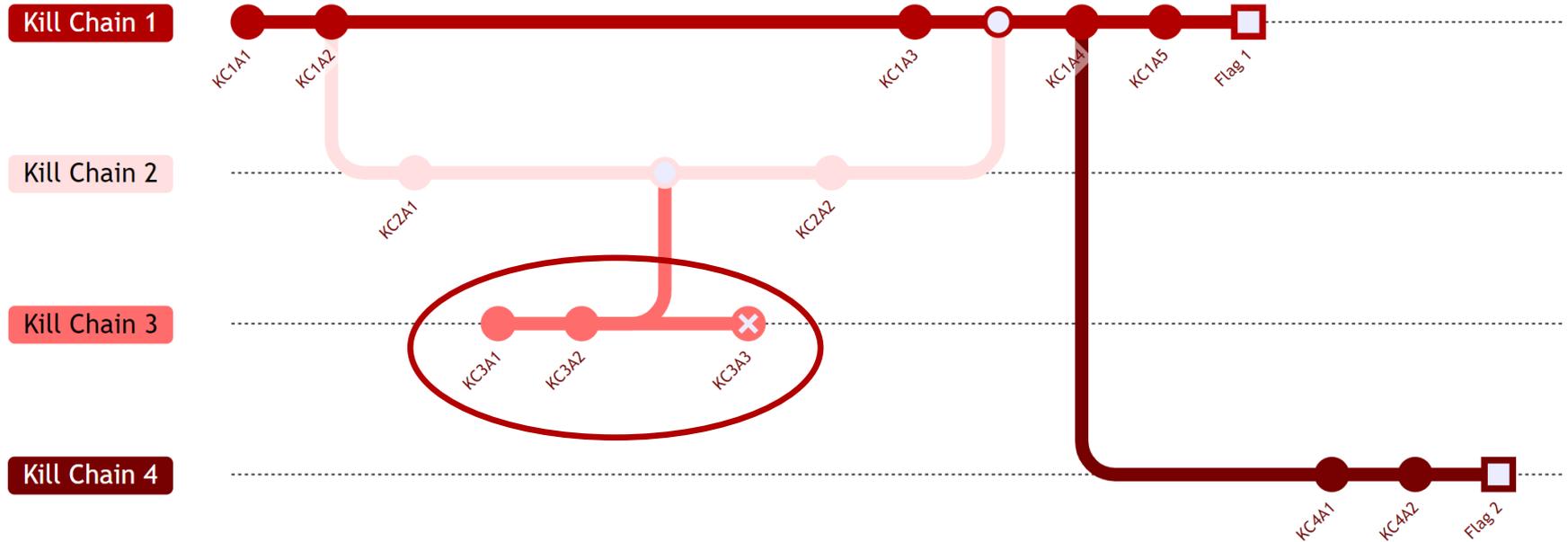
An insider threat or an advanced persistent threat (APT) with physical access to a PC could deploy a backdoor or rootkit.

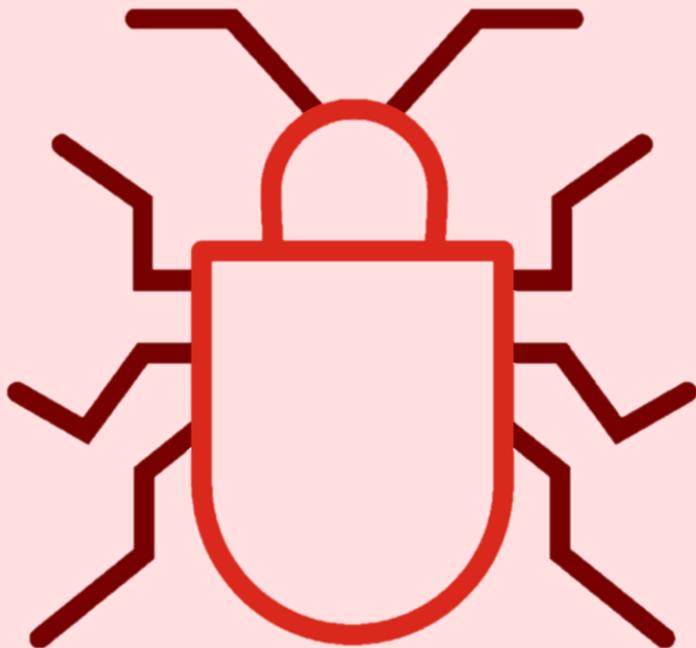


Evaluate the current configuration of MDM from an adversary's perspective using the 'assume breach' approach



# The goal from the offensive perspective





“

Using the example of creating a user with administrative privileges simply serves to illustrate the concept of a backdoor. In practical scenarios, a more sophisticated approach would involve deploying a Remote Access Trojan (RAT) equipped with rootkit capabilities, which could embed itself in the kernel space, offering deeper control and concealment.

Backdoor note

# Option 1: collect logs

## Collect logs

You can enable the ability for users to collect ESP logs in the ESP policy. When a timeout occurs in the ESP, the user can select the option to **Collect logs**. Log files can be copied to a USB drive.

You can also collect logs through a Command Prompt window on the device. If you are in OOBE on a non-S mode device, press Shift+F10.

Enter the appropriate command, based on your scenario:

- For all Autopilot scenarios and ESP:

On Windows 10 versions earlier than 1809, enter `licensingdiag.exe`.

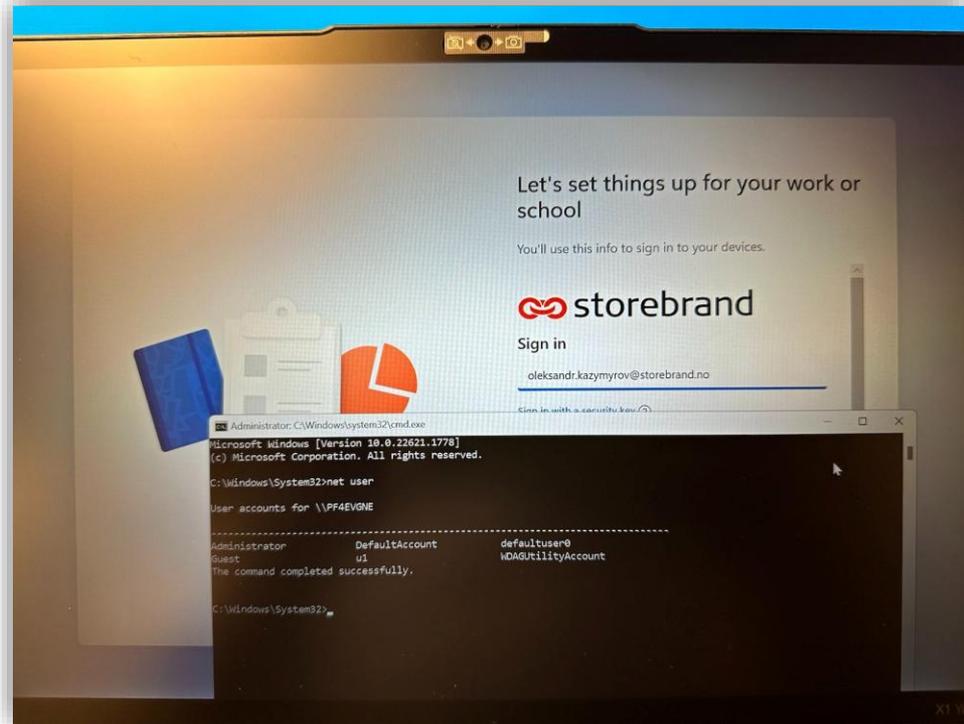
On Windows 10, version 1809 and later versions:

- For user-driven mode, enter the following command:

```
Console Copy
mdmDiagnosticstool.exe -area Autopilot -cab <pathToOutputCabFile>
```

- For self-deploying, white glove, and any other scenarios in which a physical device is used, enter the following command:

```
Console Copy
mdmDiagnosticstool.exe -area Autopilot;TPM -cab <pathToOutputCabFi
```



# Prevent privileged escalation during OOB

## Prevent privileged escalation during OOB

Today's blog post concerns a security risk often overlooked by IT admins and organizations. It involves **creating a local admin account** using OOB **during** or **before** deploying a device—a critical aspect that, in my opinion, needs to be addressed. Read the blog post to prevent privileged escalation during OOB or unauthorized access and enhance security.

<https://call4cloud.nl/>

## 2022-03 Update: The Search for Sp... Uhh Shift+F10

by: rudyooms - March 17, 2022

Last Updated on May 22, 2023 by [rudyooms](#)

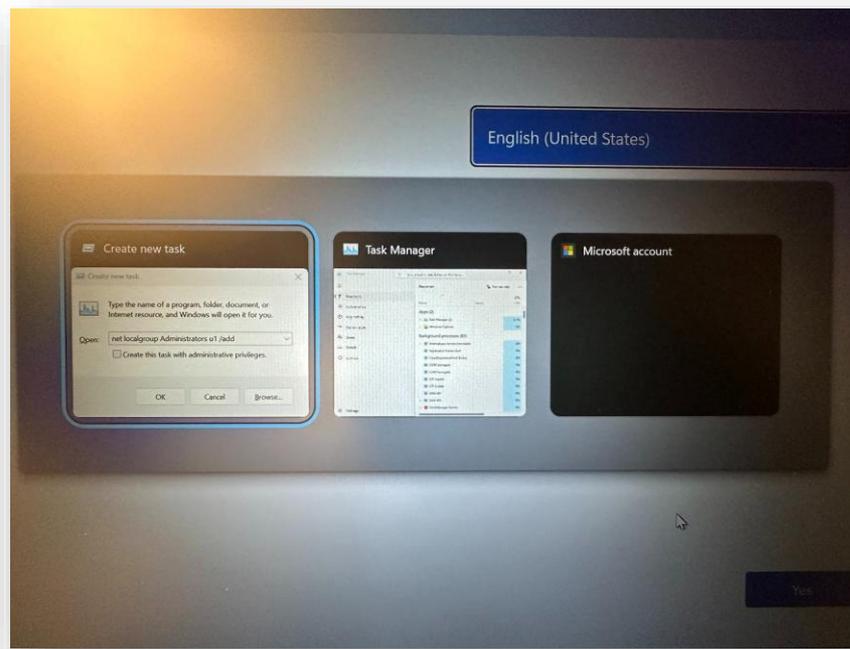
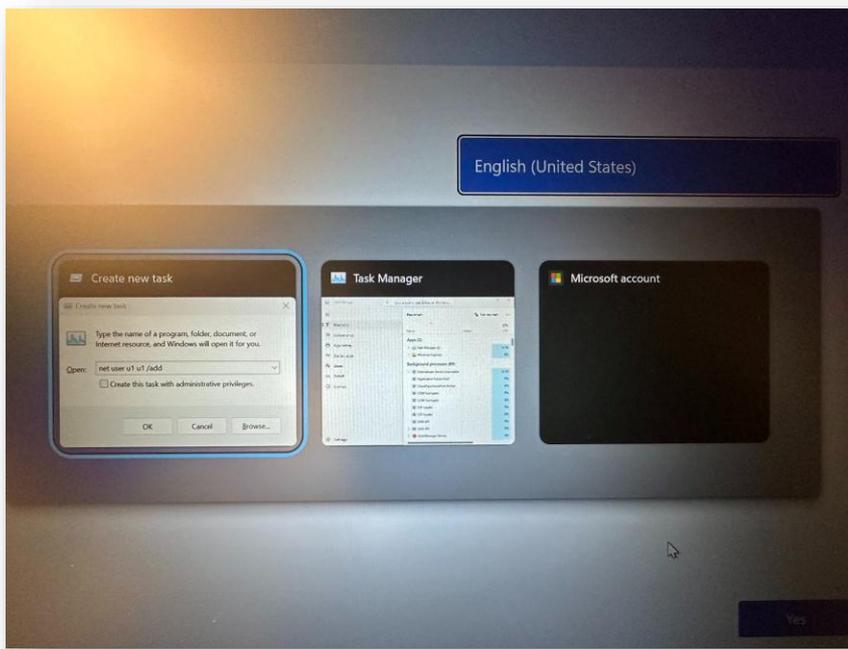
This blog will be about Microsoft's **"their" solution** to remove the lingering Windows.old folder after a remote wipe. I noticed that when using Microsoft their solution, my older solution to **block the shift+F10** functionality will be disabled. This solution was also using the **Push-Button reset** options

I will divide this blog into multiple parts

<https://www.bilalelhaddouchi.nl/>

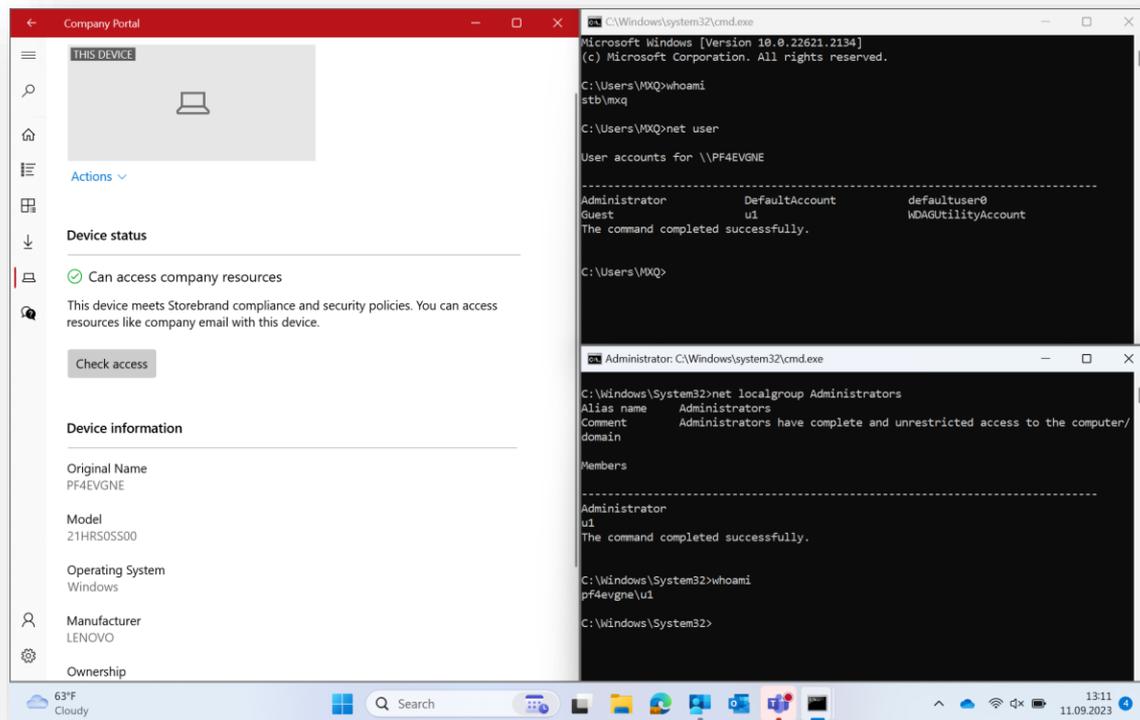


# Option 2: Blind command injection



Ctrl + Shift + Esc → Alt + N → CMD

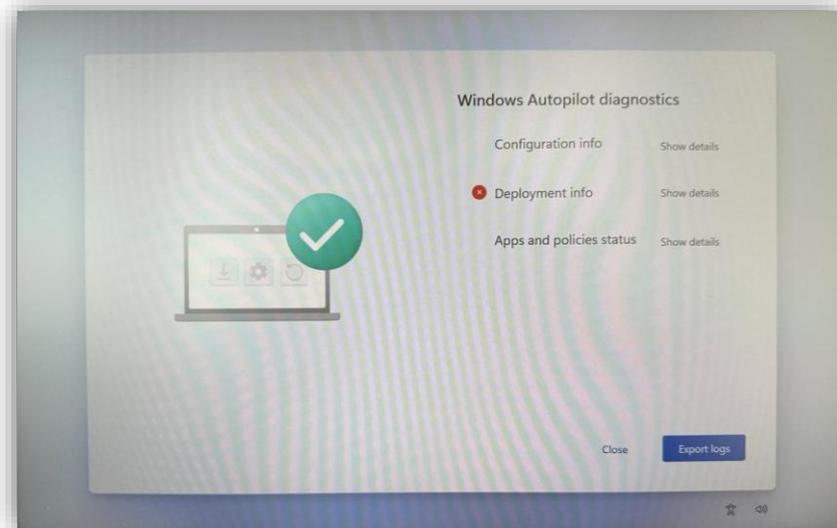
# Option 2: Blind command injection



# Option 3: Windows Autopilot diagnostics

Run a privileged command line

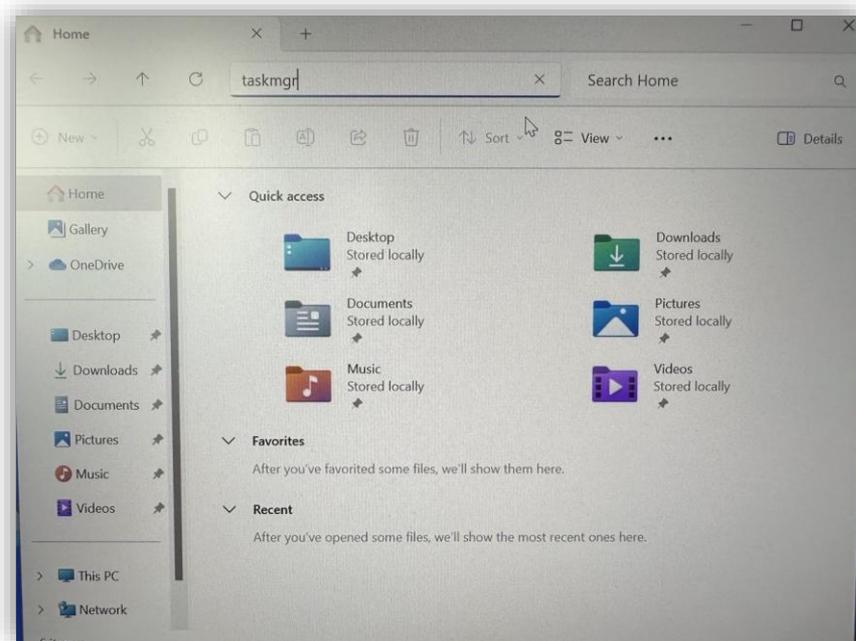
1. Ctrl-Shift-D → Export logs



# Option 3: Windows Autopilot diagnostics

## Run a privileged command line

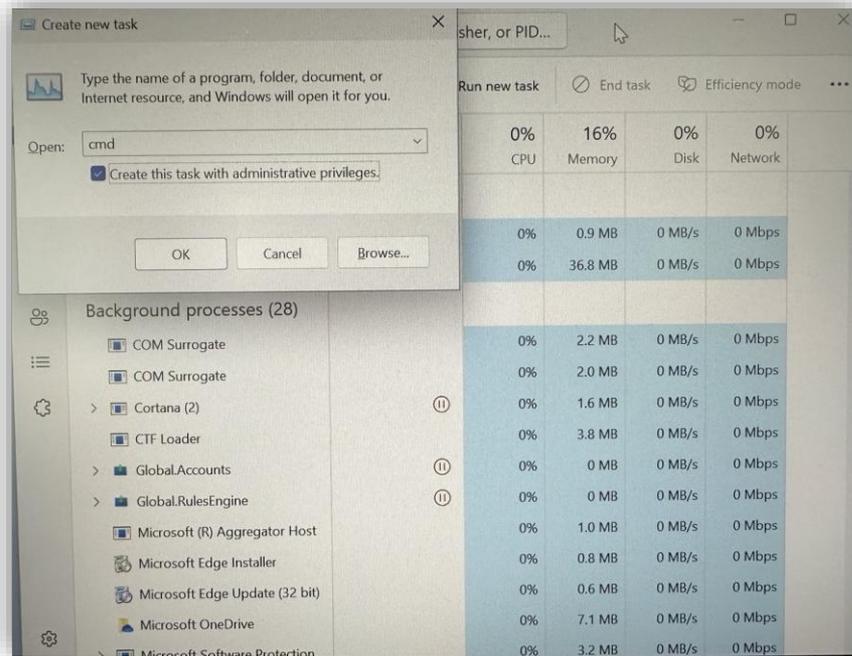
1. Ctrl-Shift-D → Export logs
2. Right click Local Disc (C:) → Open in new window
3. Alt + Tab (choose explorer)
4. Ctrl + L → taskmgr → Enter



# Option 3: Windows Autopilot diagnostics

## Run a privileged command line

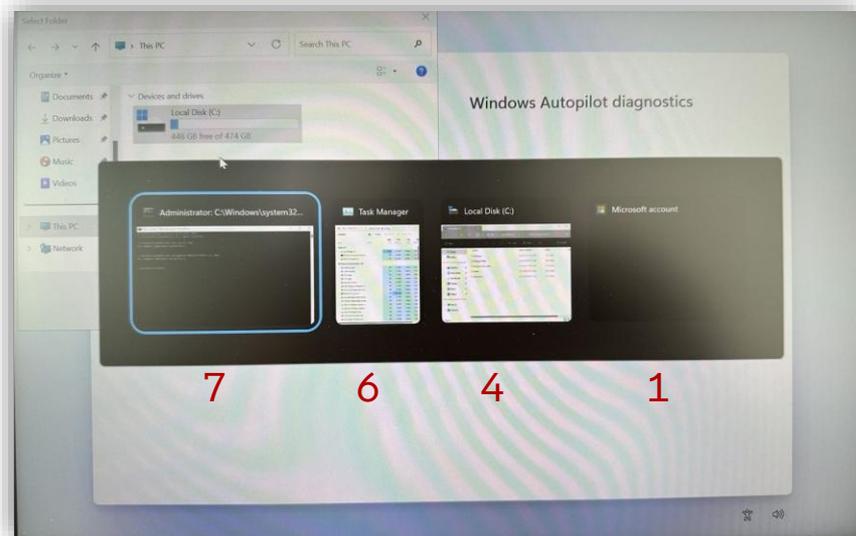
1. Ctrl-Shift-D → Export logs
2. Right click Local Disc (C:) → Open in new window
3. Alt + Tab (choose explorer)
4. Ctrl + L → taskmgr → Enter
5. Alt + Tab (choose taskmgr)
6. Alt + n → cmd → Tab → Space → Enter



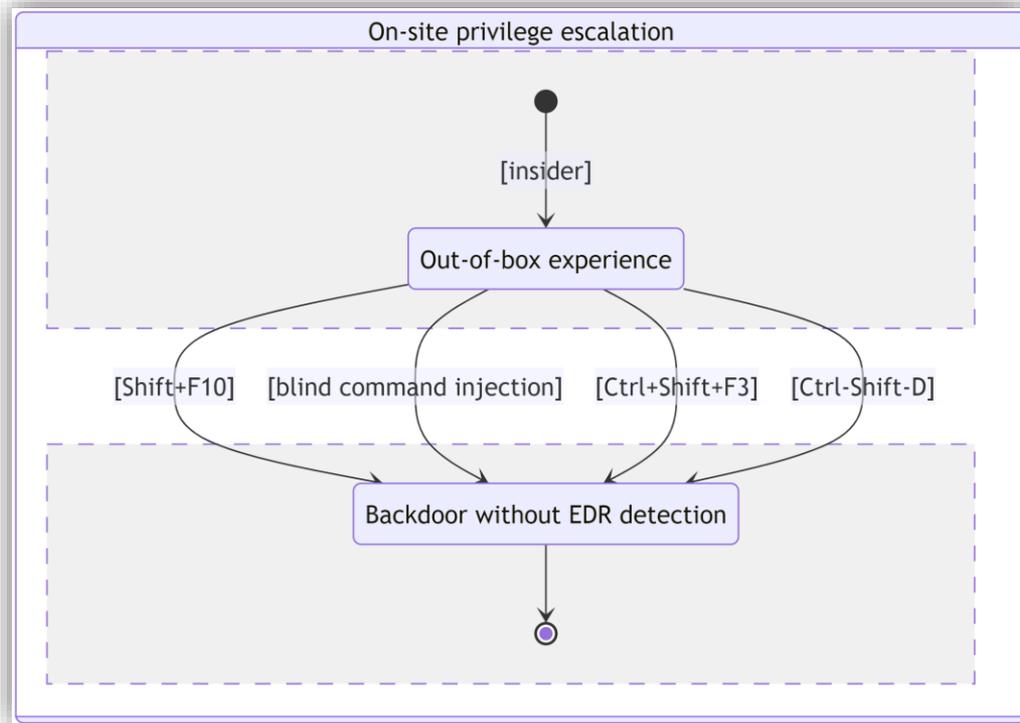
# Option 3: Windows Autopilot diagnostics

Run a privileged command line

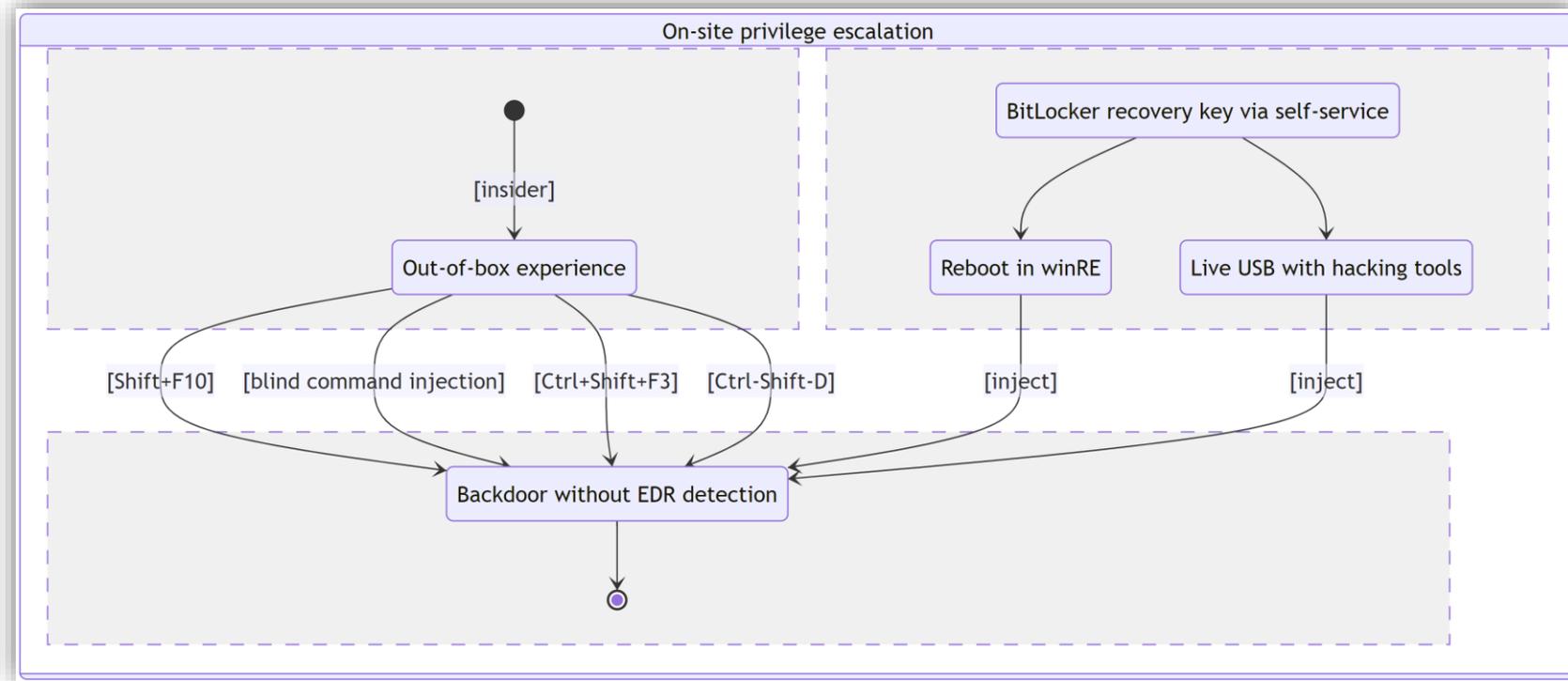
1. Ctrl-Shift-D → Export logs
2. Right click Local Disc (C:) → Open in new window
3. Alt + Tab (choose explorer)
4. Ctrl + L → taskmgr → Enter
5. Alt + Tab (choose taskmgr)
6. Alt + n → cmd → Tab → Space → Enter
7. Inject a backdoor  
`net user u1 u1 /add`  
`net localgroup Administrators u1 /add`



# High-level overview: OOB



# High-level overview



# Finding your BitLocker recovery key

The screenshot shows a web browser window at <https://myaccount.microsoft.com/device-list>. The user is logged in as Kazymyrov, Oleksandr. The page title is "Enheter" (Devices). A modal window is open, displaying the BitLocker recovery key for the device "PF4EVGNE".

**BitLocker-nøkler for PF4EVGNE**

Operativsystemstasjon

**Nøkkel-ID:**  
4489b201-eaf4-403a-b89c-1ba7c5cb6685

[Vis gjenopprettingsnøkkel](#)

Enheter

Hvis du mister en enhet eller ikke lenger bruker den, kan du kontakte administratoren.

PF4EVGNE

Enheten administreres av Intune.

[Vis BitLocker-nøkler](#)

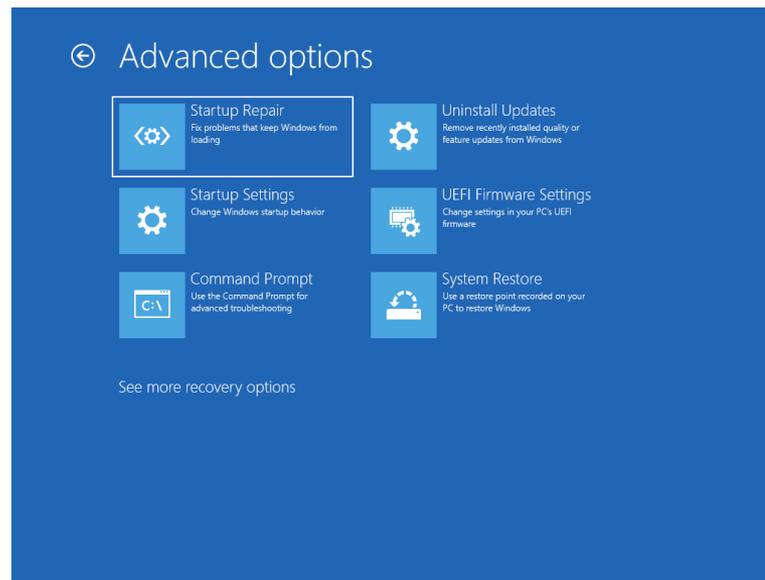
# Windows Recovery Environment (winRE)

## Recovery Mode

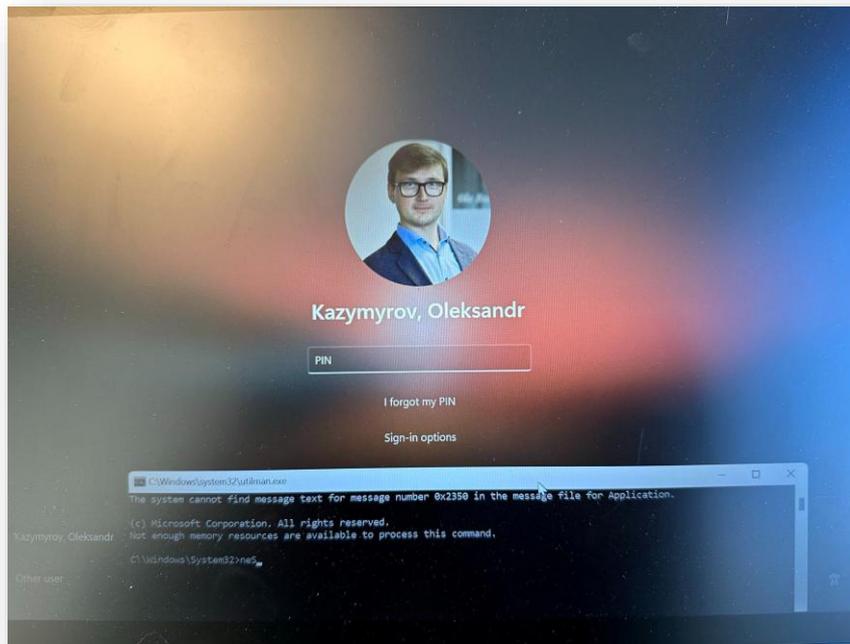
1. Hold down the power button for 10 seconds to turn off your device.
2. Press the power button again to turn on your device.
3. On the first sign that Windows has started (for example, some devices show the manufacturer's logo when restarting) hold down the power button for 10 seconds to turn off your device.
4. Press the power button again to turn on your device.
5. When Windows starts again, hold down the power button for 10 seconds to turn off your device.
6. Press the power button again to turn on your device.
7. This time, allow your device to fully start up.

Source: [Recovery options in Windows](#)

## Command prompt



# Using Utilman.exe backdoor



PoC: OpSec insecure

## Storebrand IT : Your device is non-compliant

Dear colleague,

The device listed below is currently not in compliance with our IT Security policies. You need to remediate this issue within 12 hours or you will loose access to company data.

Please open Company Portal app and follow the steps to remediate your compliance issues or contact Storebrand IT Support for assistance.

Best regards,

Storebrand IT Support

Norway +47 22311150 & Sweden +46 84517771

### Device Details:

**OS family:** Windows

**OS version:** 10.0.22000.1455

**Model:** 21CD0014MX

**Serial number:** PF40931S

**Device name:** PF40931S

# Live USB

## Live USB with Linux

1. Disable Secure Boot
2. Load from Live USB (Kali)
3. Use **dislocker** to unlock disk using password or recovery key
4. Use **chntpw** to activate and clean password for Administrator
5. Enable Secure Boot
6. Load normally

## chntpw



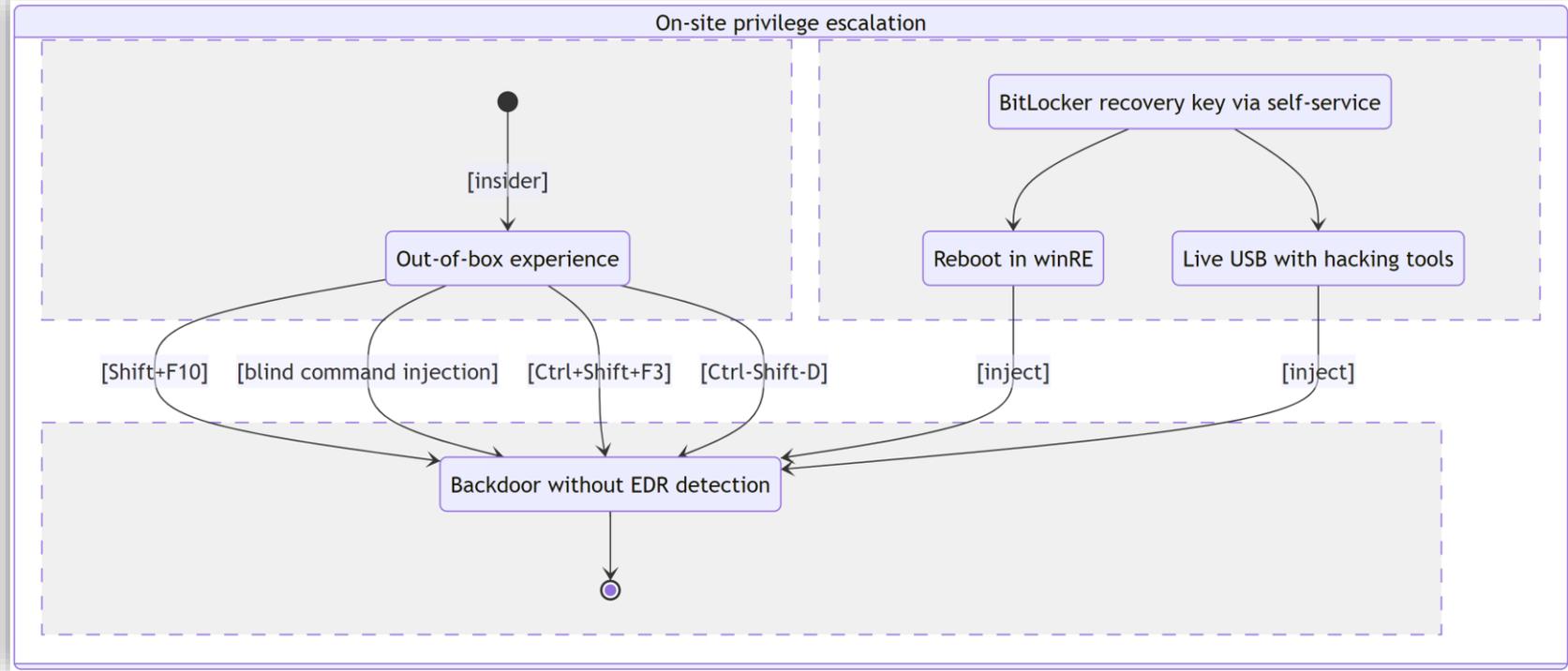
# EDR after changes over Live USB

The screenshot shows the Microsoft Defender Security Center interface for a device named 'pf3w3bqw'. The device status is 'Active' and 'win11'. The 'Incidents and alerts' tab is selected, showing a notification about Microsoft Defender XDR. Below the notification, there are options for 'Export', 'Search for name or ID', 'Customize columns', and '6 Months' filter. The 'Filter set' is 'Save' and there is an 'Add filter' button. The filter criteria include 'Incident name', 'Incid...', 'Tags', 'Severity', and 'Investigation'.

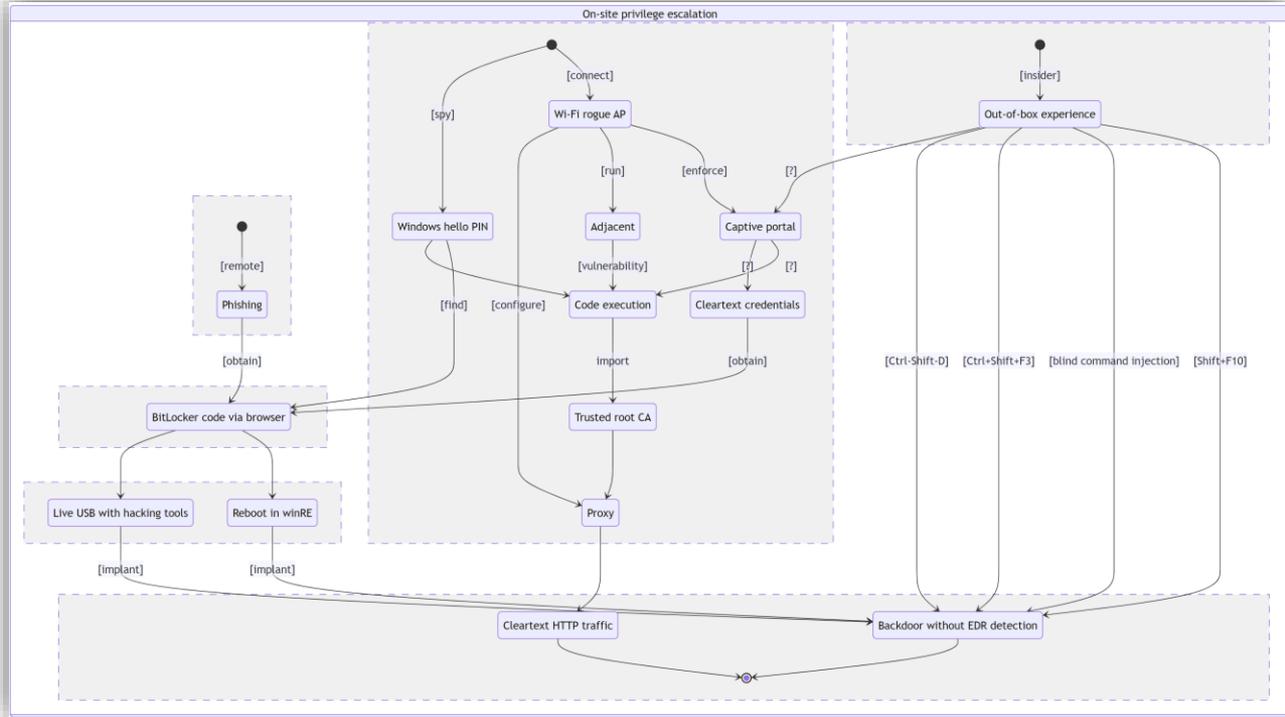
The screenshot shows the Windows Task Manager 'Users' tab. It displays a table of user resource usage for 'Administrator' and 'MXQ (53)'. The table has columns for User, Status, CPU, Memory, Disk, and Network.

User	Status	72% CPU	45% Memory	6% Disk	0% Network
Administrator		0.2%	859,5 MB	0,1 MB/s	0 Mbps
> MXQ (53)		12,2%	893,9 MB	0,8 MB/s	0,3 Mbps

# Zoom out



# Zoom out



# Conclusions

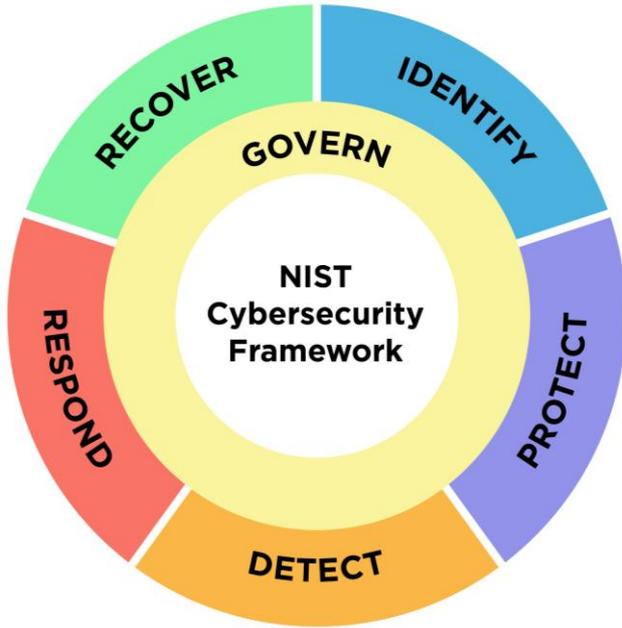
- [Bug Or Feature: Privilege Escalation In Windows Autopilot \(2020\)](#)

"We have completed our investigation and found the issue submitted to us is not a security issue and is by design; this issue doesn't meet security servicing bug bar." © Microsoft

- Block untrusted devices via Conditional Access
- Split effort (ref. the Pareto principle)
  - Detect/Respond: 20% effort gives 80% value
  - Protect: 80% effort gives 20% value



# NIST CSF 2.0



- Identify
  - A backdoor can be implanted during OOB
- Protect
  - Numerous methods to cope with individual issues
- Detect
  - Threat hunting on PC resets
- Respond
  - Correlation with valid requests
  - Initiate insider threat investigation
- Recovery
  - Containment and eradication of identities and assets
- Govern
  - Establish/maintain procedures and playbooks