



Let's get physical: Stories from behind your company's gate

Firat Acar, Moritz Thomas – November 2024

Contents

- About us
- Stories
- Takeaways & QA

20929

Tet	Thi	Aye	Maly		Flour	Mar	May	Jul	Nov	Dec
78	2	11	Y		10	10	11	10	16	21
7	3	2		11	10	11	11	11	11	11
8	22	23	24	25	26	27	28	29	29	29
9	20	21	22	23	24	25	26	27	28	29
10	19	10	10	10	11	11	11	11	11	10
11	21	22	23	24	25	26	27	28	29	29
12	20	21	22	23	24	25	26	27	28	29
23	20				26	26	27	28	28	28
					26	26	27	28	28	28
					29	29	29	29	29	29
					31	2	3	3	3	3



Disclaimer:

Story details (names, locations, sectors, dates, ...) are anonymized.

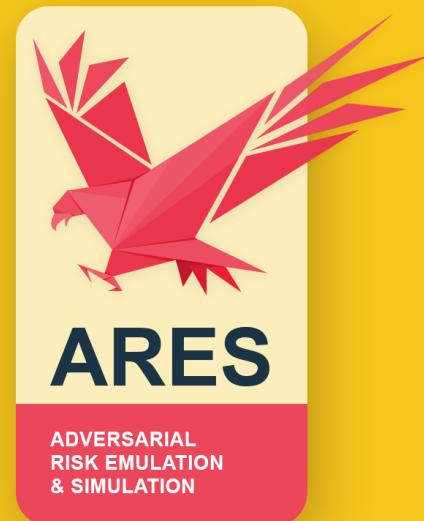
About us



Firat Acar

Red Teamer

firat.acar@nviso.eu



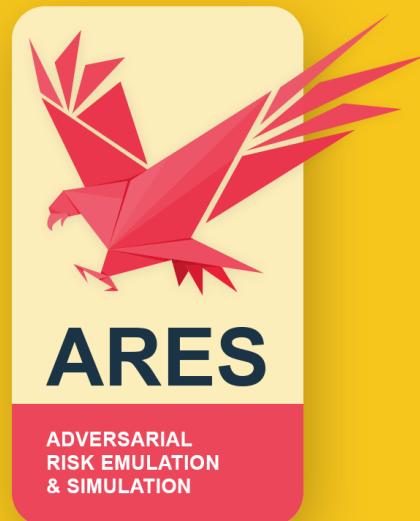
About us



Moritz Thomas

Red Teamer, R&D

moritz.thomas@nviso.eu





Story time!



Mountain
Base

Mountain Base



Objectives:

- Gain physical access
- Plant rogue device



Mountain Base – Recon



- Remote location
- Extensive underground area
- Closed to public
 - Guided tours!

Mountain Base – Recon



- High-security locks
- Keypad & Card Reader
- Lots of traffic



Mountain Base – Entry?



Phase II

{ Covert Entry
Overt Entry



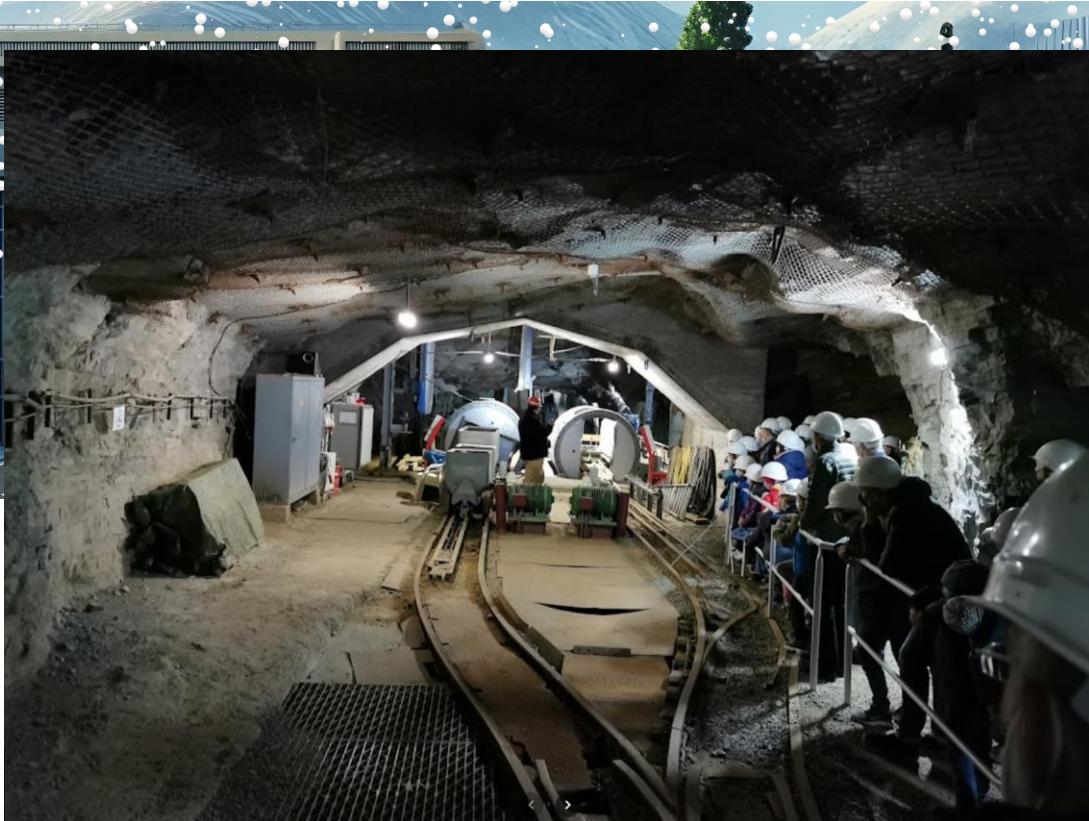
Mountain Base – Entry I



Social
Engineering



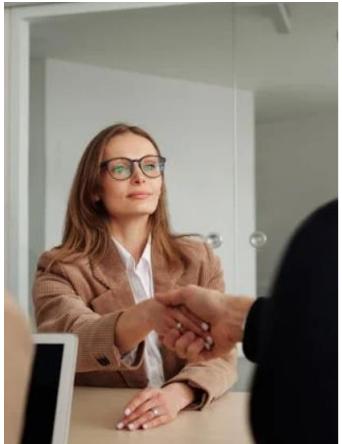
Persistence



www.rvso.eu

Was gehts zusammen? 🧑

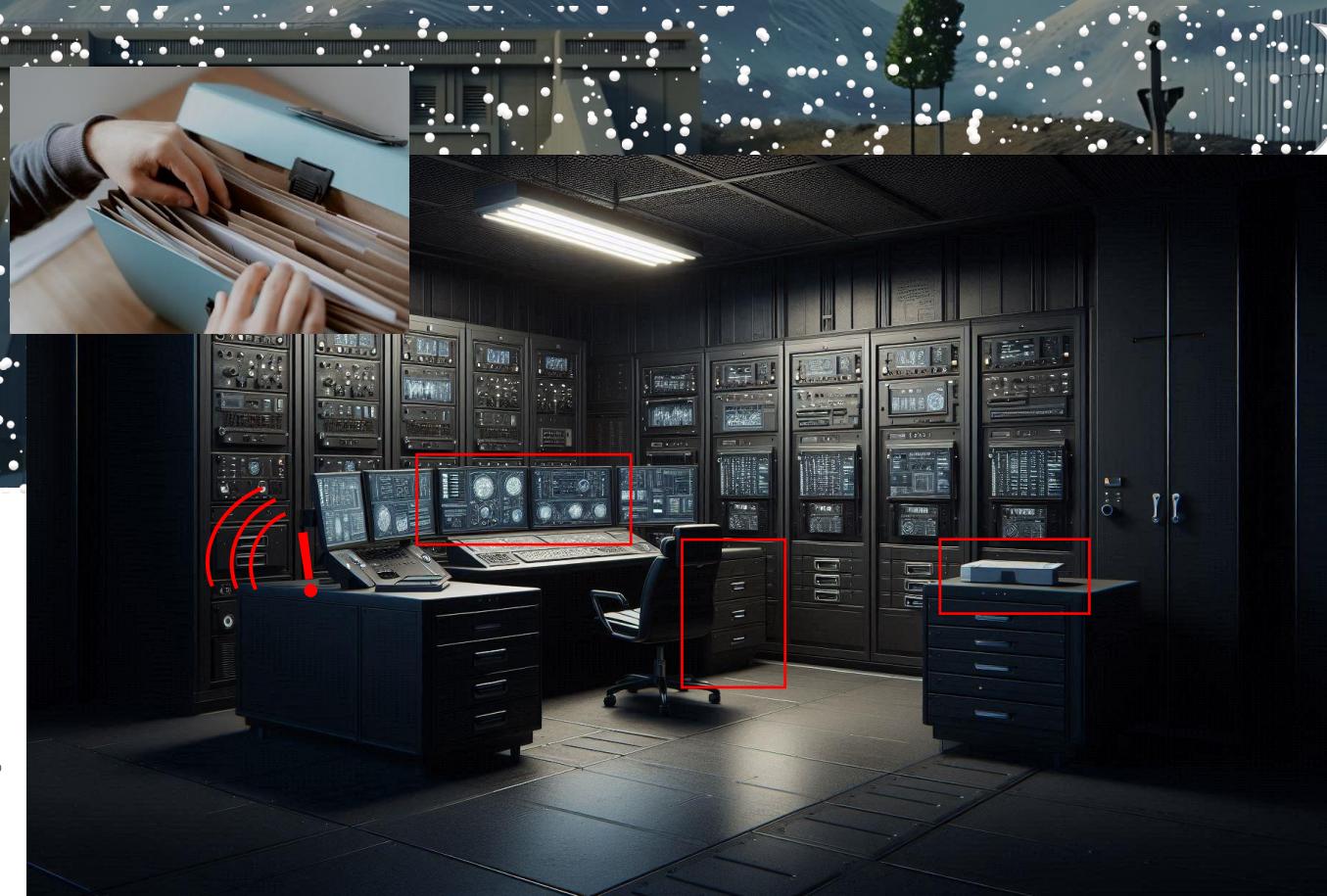
Mountain Base – Entry I - Results



- Process oriented
 - Diversions spark suspicion
- Persistent & Assertive
- Internal incident raised at HQ

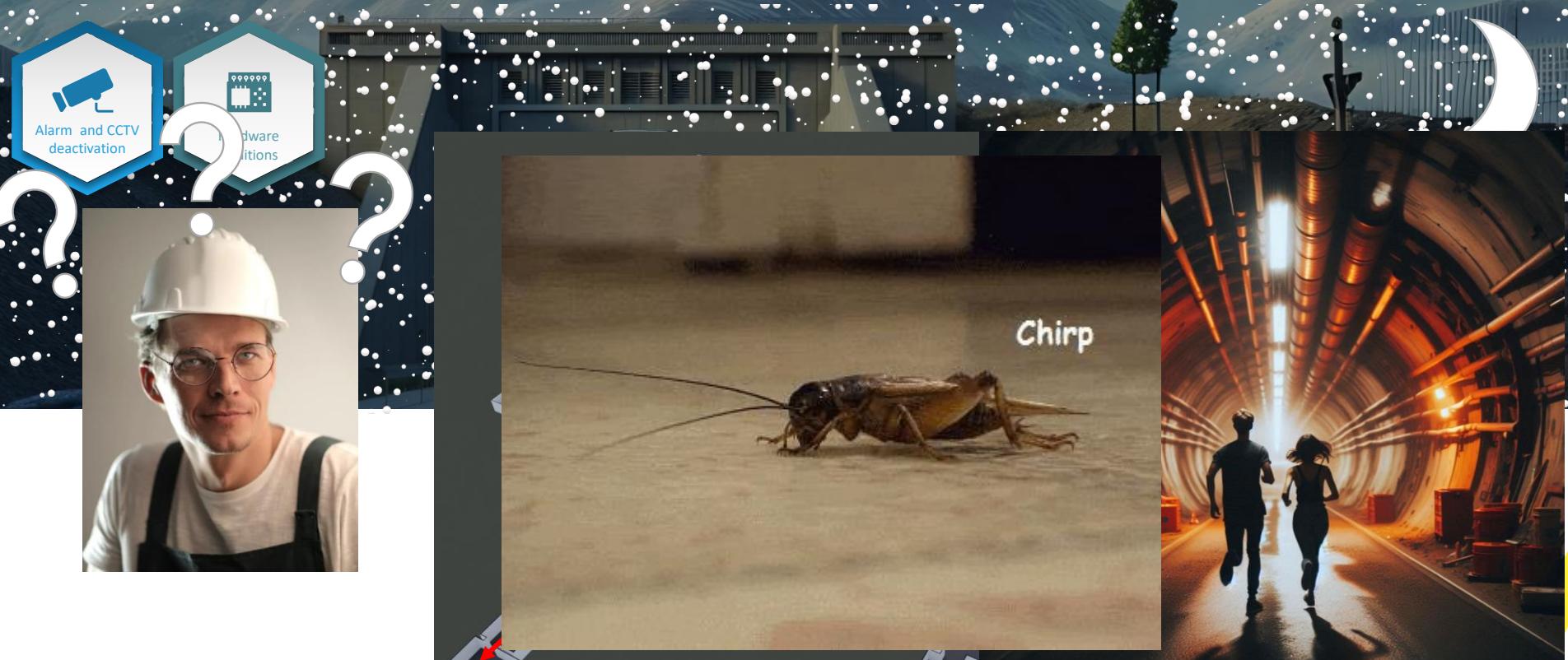


Mountain Base – Entry II



If I were you...
I'd **RUN!**

Mountain Base – Entry II



Mountain Base – Entry II - Results



- Leg-up successful
- Heavy security at entrance only
- Local incident raised
 - No connection to first incident
 - Plant-wide investigation & search





Who are you?

Who are you?



Objectives:

- Gain physical access
- Plant rogue devices
- Pictures of sensitive documents



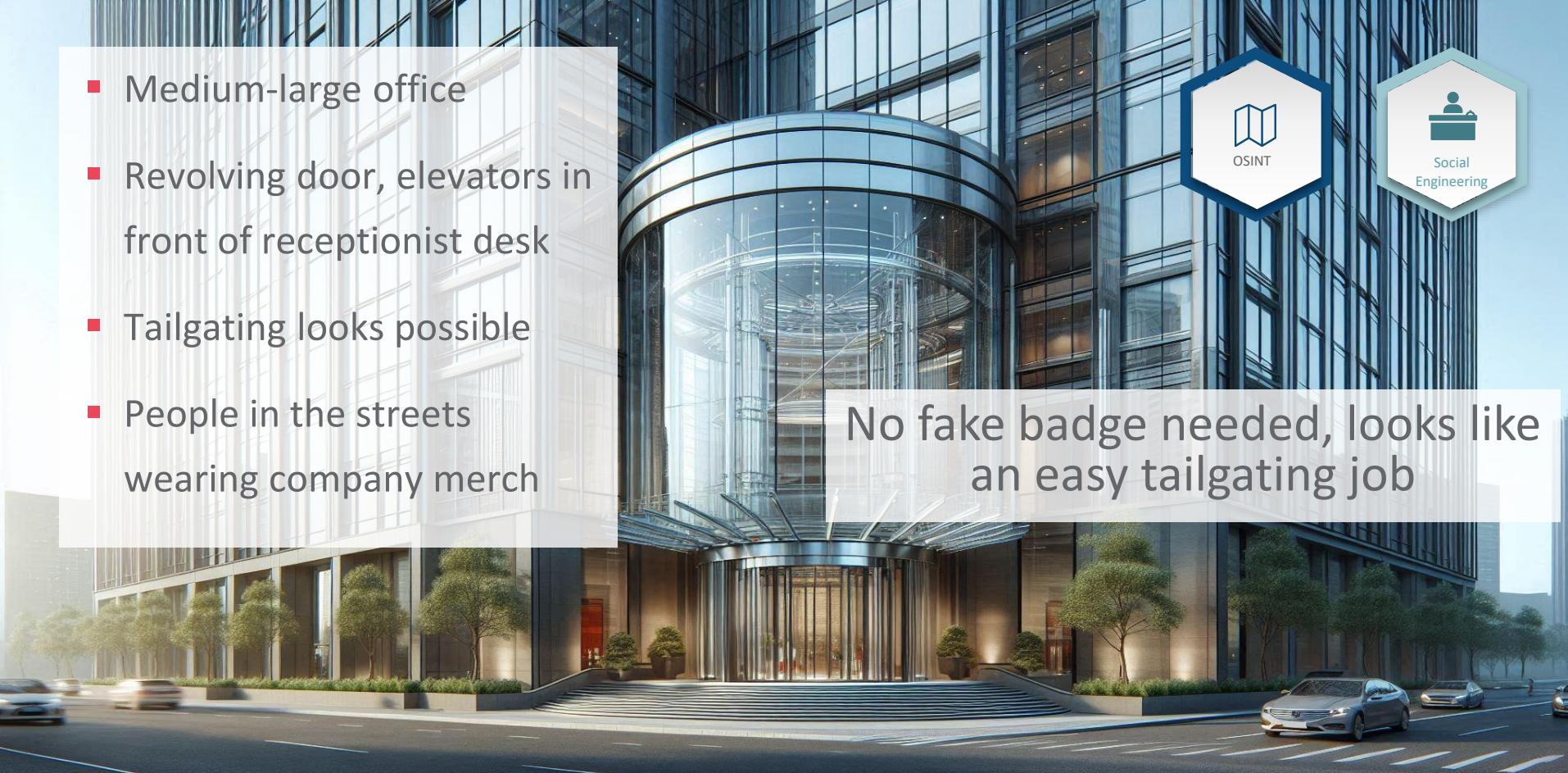
Hardware
Additions



Document
access

Who are you? - Recon

- Medium-large office
- Revolving door, elevators in front of receptionist desk
- Tailgating looks possible
- People in the streets wearing company merch



No fake badge needed, looks like an easy tailgating job

Who are you? - Action

Without too much preparation, I went straight ahead



Door turned me back twice while trying to tailgate, it was a bit awkward...



Eventually, I made it in by talking to an employee, who brought me to the receptionist





Well, at least I am inside, but stuck here for the time being



You can wait here for your contact person

It seems all doors and elevators require badges, so how do we get out of here?



Badging is normally required to enter the canteen



Sadly, they went outside the building, which left me in the hall, hiding from the receptionist



A photograph of a group of seven business professionals in a modern elevator. From left to right: a man in a dark suit, a man with a grey beard in a dark suit, a woman in a grey blazer, a man in a dark suit wearing a black balaclava, a woman in a grey blazer, an older man with glasses in a dark suit, and a woman in a grey blazer. They are all looking towards the right. The elevator has wooden paneling and a control panel with buttons on the right.

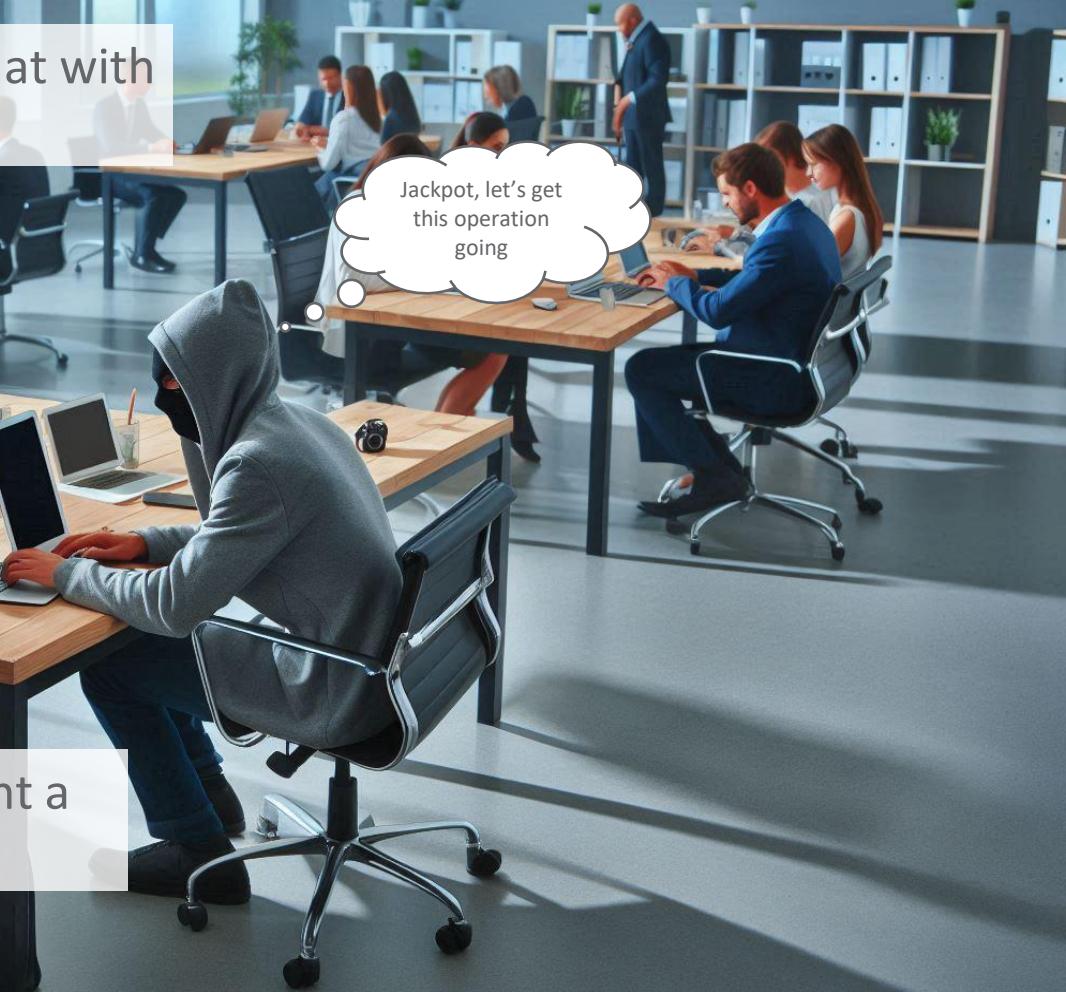
Eventually, a group arrived that went into the elevators, I quickly snuck inside with them...

I followed them into their office floor and sat down at a desk somewhere

Two guys came up to have a small chat with me, but left afterwards.



But look who's back, and they brought a friend... the receptionist lady





They started questioning me, sometimes talking through eachother

Who are you? This is a sensitive department, only authorized personnel is allowed!

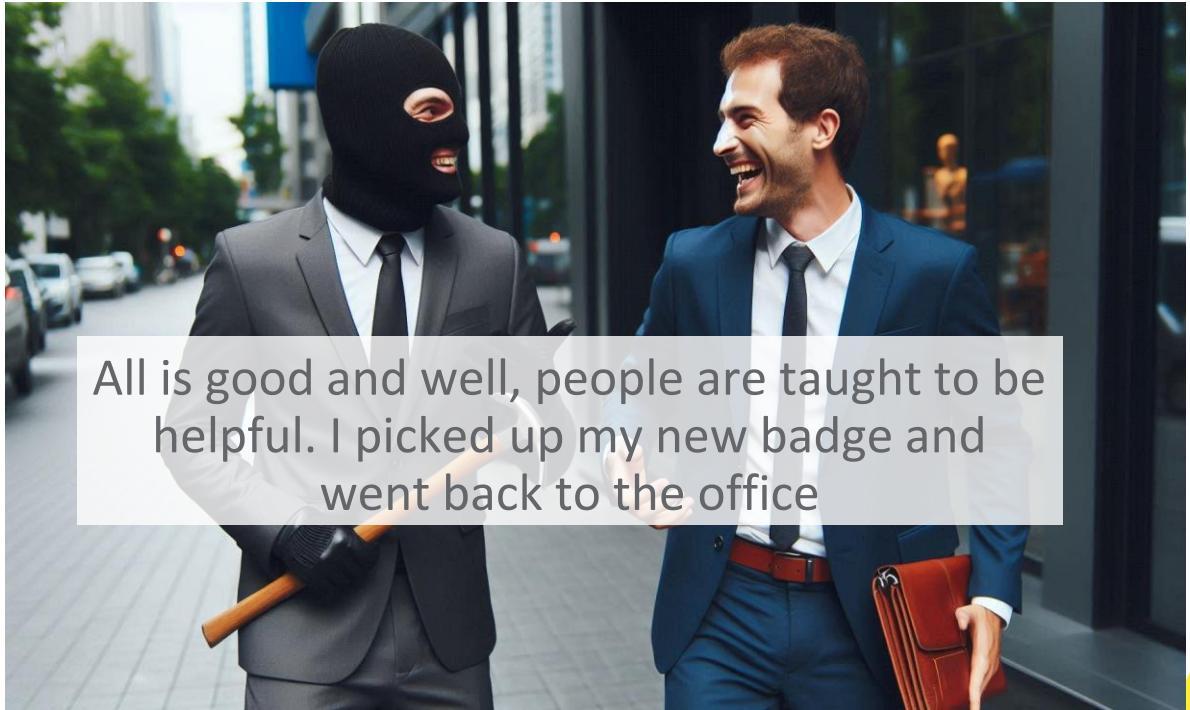
What are you doing here? You were supposed to be waiting downstairs!

Do you have a contact person and their number? I have to call them.

Somehow, using pure improvisation, I managed to convince them to let me go... with a bonus present



Alright, I will guide you outside. We will get you a visitor's badge for another floor.



All is good and well, people are taught to be helpful. I picked up my new badge and went back to the office

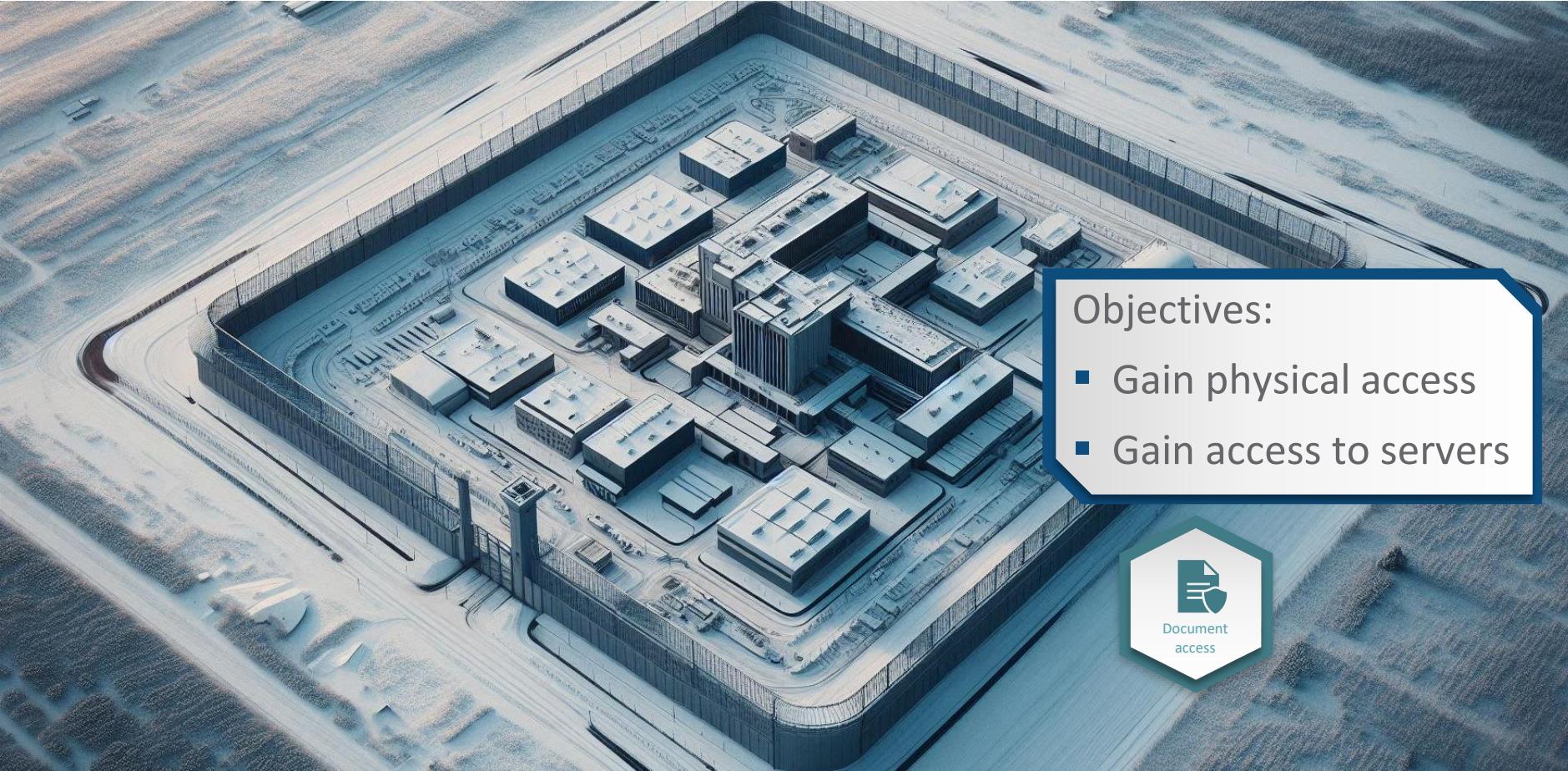
Sometimes though, silence is golden,
especially when you've already won...





Industrial Plant

Industrial Plant

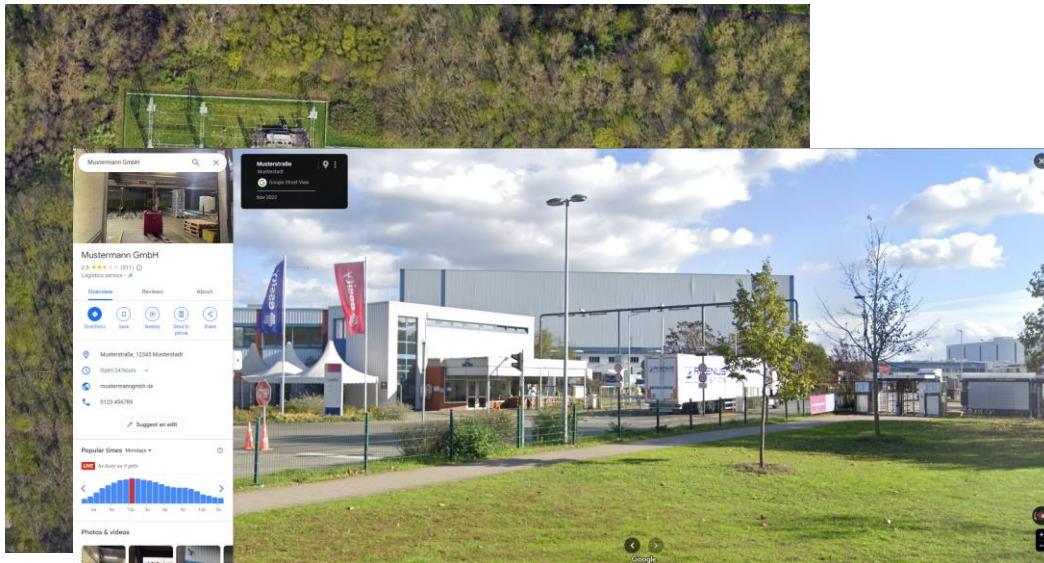


Objectives:

- Gain physical access
- Gain access to servers

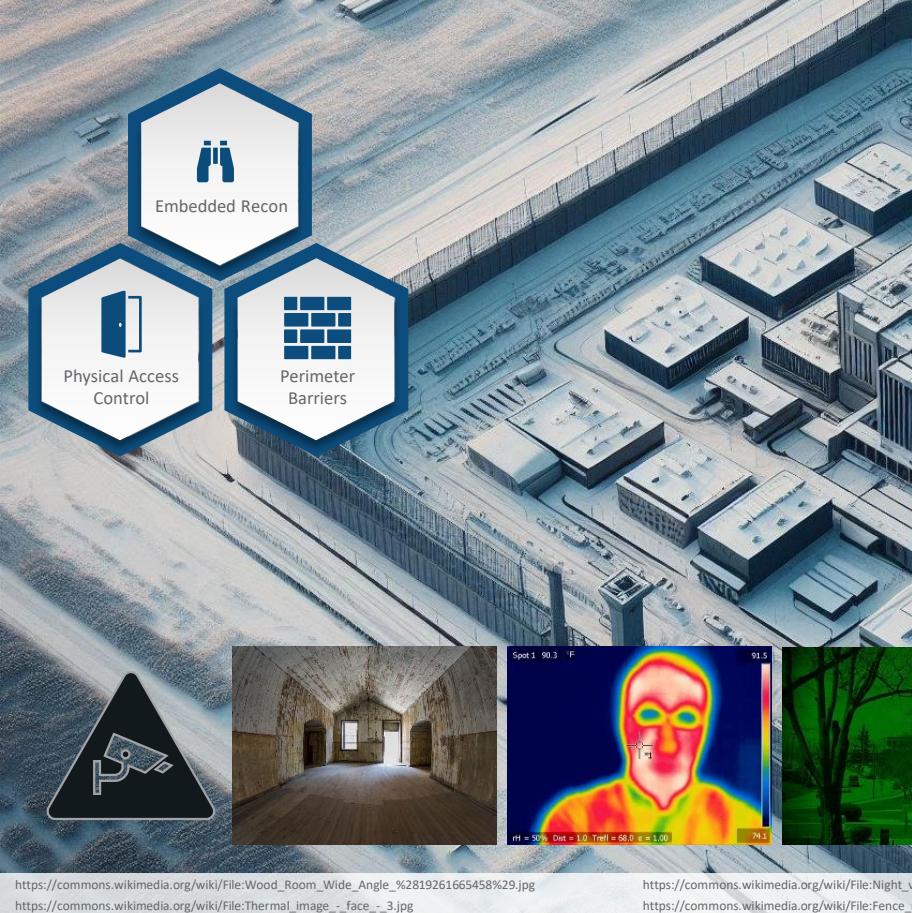


Industrial Plant – Recon



- Remote location
- Extensive area
- Closed to public

Industrial Plant – Recon



- Single gate, few doors
- Lots of cameras
- Some sensors installed on fences
- One spot to jump the fence!



https://commons.wikimedia.org/wiki/File:Wood_Room_Wide_Angle_%2819261665458%29.jpg

https://commons.wikimedia.org/wiki/File:Thermal_image_-_face_-_3.jpg

https://commons.wikimedia.org/wiki/File:Night_vision_filter_example_-_Pixel_Photo_Editor.jpg

https://commons.wikimedia.org/wiki/File:Fence_motion_sensor_gold_base.jpg

Industrial Plant – Option #1: Jump the fence

- Easy to get in!
- Hard to get out...
- Suspicious at night
- Can't hide: footprints

WT's Verdict: Won't do.



Industrial Plant – Option #2: Cleaning staff

- Pretext:

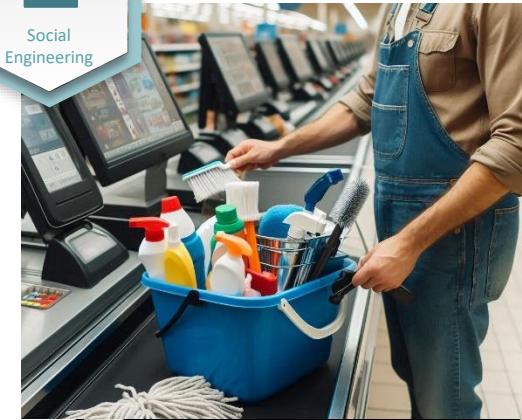
- Little preparation
- Simple execution
- Good enough?

- No keys/keycards.

WT's Verdict: Go for it!



Industrial Plant - Entry

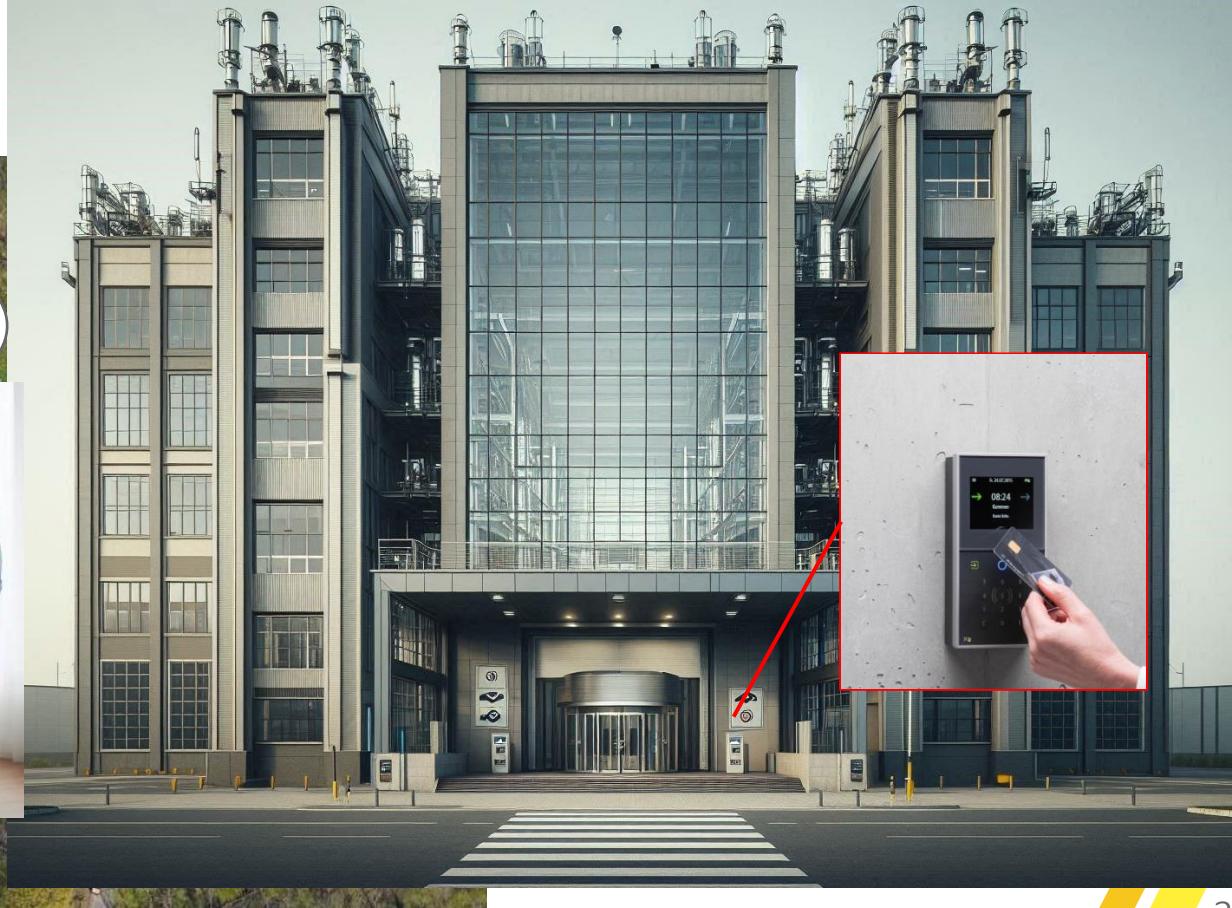




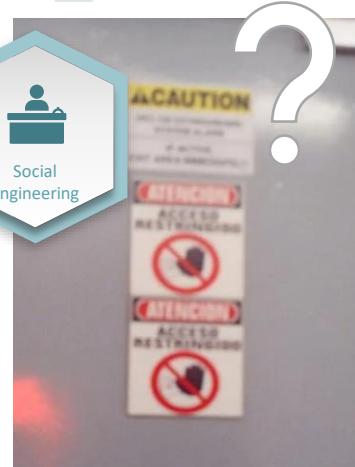
Industrial Plant - Entry



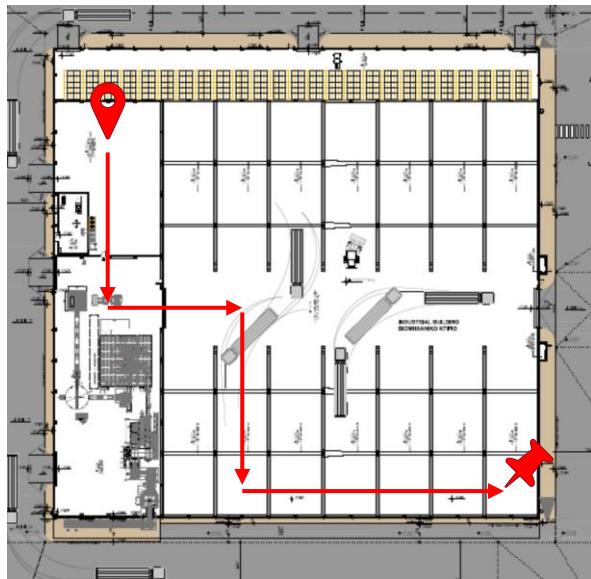
Social
Engineering



Industrial Plant - Entry



Industrial Plant - Entry



Industrial Plant - Entry



Industrial Plant – Results



- Social engineering successful
- Bypassed perimeter security
- Lacking security awareness of staff
- Local incident raised
 - Wanted posters



Aliases: Patrick Brian, Patrick M. Brian, Patrick M. Bryan, Edward L. Houston, Roger H. Shannon

Takeaways



- Trust but verify: be persistent & assertive



- Ensure that visitors are always accompanied by staff



- Always verify a visitor's contact person before letting them in



NVISO

Thank you!



Firat Acar



firat.acar@nviso.eu



[firat-ac](#)



Moritz Thomas



moritz.thomas@nviso.eu



[moritzlthomas](#)