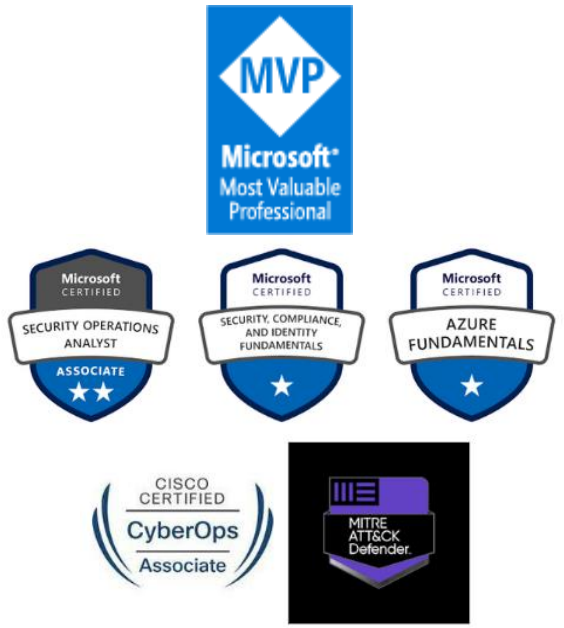
Staying ahead of Threats - Building Hunts in Microsoft Sentinel

Azure Innovators Hub | Public Sessions

Michalis Michalos, October 5th 2024

About me

- Currently working as Cyber Resilience & Intelligence Manager
- Over 11 years experience in ICT
- Working in Cybersecurity since 2019
- Electrical Engineer BSc, MSc, MBA
- Father of 2, lifetime Scout, own a wine cooler, and a watch enthusiast



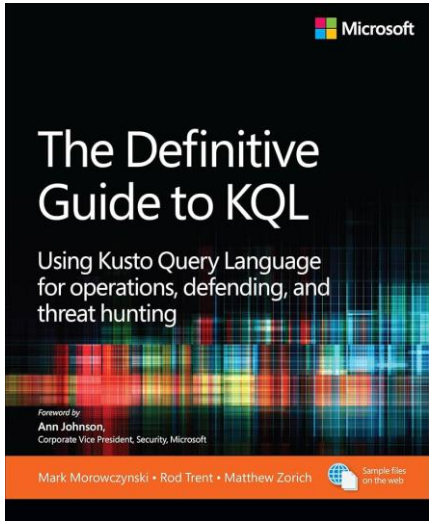
Projects

- Blogging at michalos.net
- github.com/cyb3rmik3/KQL-threat-hunting-queries
- github.com/cyb3rmik3/MDE-DFIR-Resources
- Featured in:

KQL Search

Search engine for KQL Queries

Kusto Insights



Agenda

- What is threat hunting?
- How and where to hunt
- Defining hypothesis
- Bookmarks
- Other things to do
- Closing remarks

What is threat hunting?

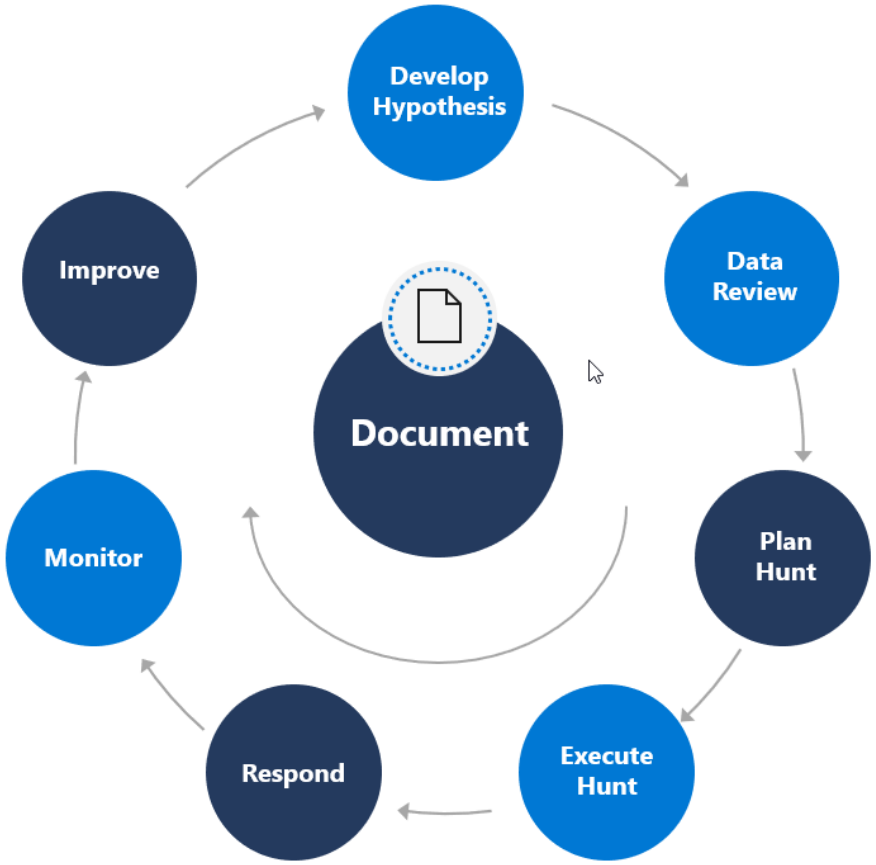
Threat hunting is the process of proactively searching for unknown or undetected threats across an organization's network, endpoints, and data.

Structured: threat hunters look for suspicious tactics, techniques, and procedures (TTPs).

Unstructured: threat hunter search for IoCs from this starting point.

Situational: prioritizing specific resources or data within the digital ecosystem.

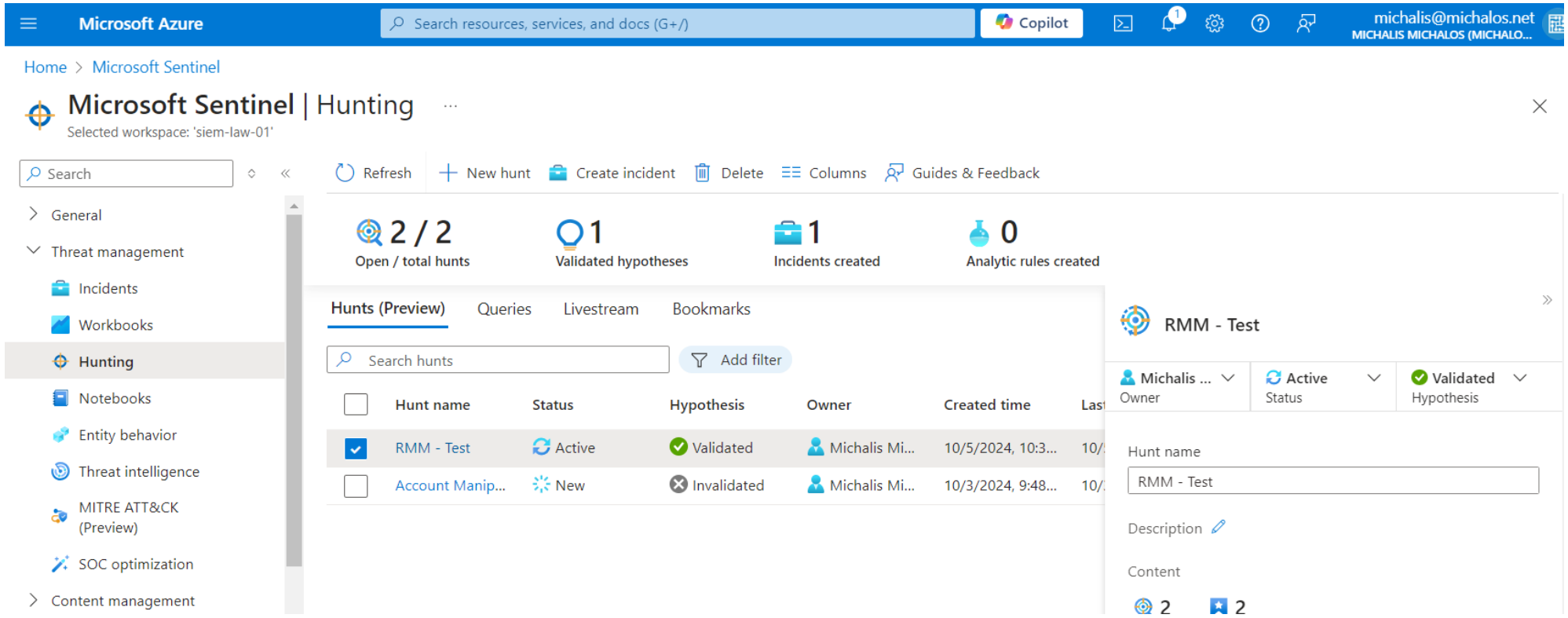
Process to threat hunting



- Create a theory or hypothesis
- Conduct research
- Identify the trigger
- Investigate the threat
- Respond and remediate

Further Threat Hunting frameworks to explore: Sqrrl, TaHiTI and PEAK.

Where do I hunt in Sentinel?

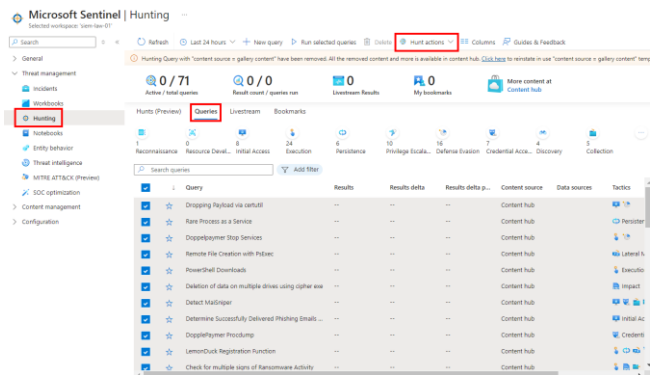


Define your hypothesis
(and deploy the easy way)

Suspicious behavior

Investigating potentially malicious activity that's visible in your environment to determine if an attack is occurring.

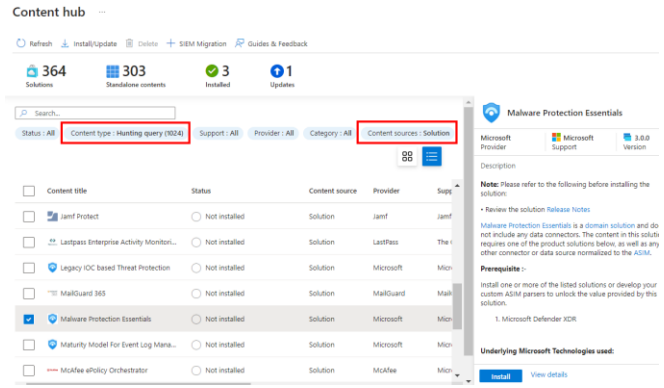
- Create a hunt by using Queries available in Hunting



New threat campaign

Look for types of malicious activity based on newly discovered threat actors, techniques, or vulnerabilities.

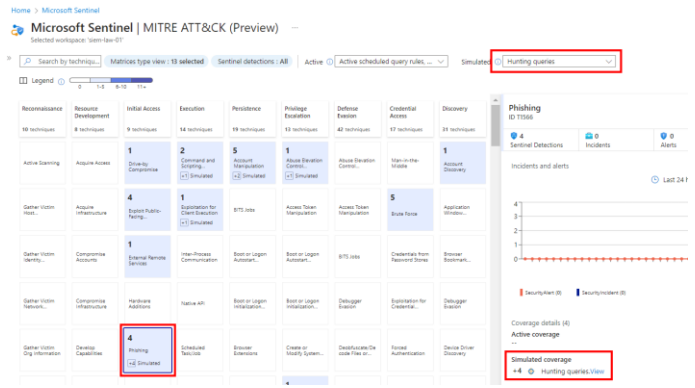
- Leverage Content hub to deploy new campaigns



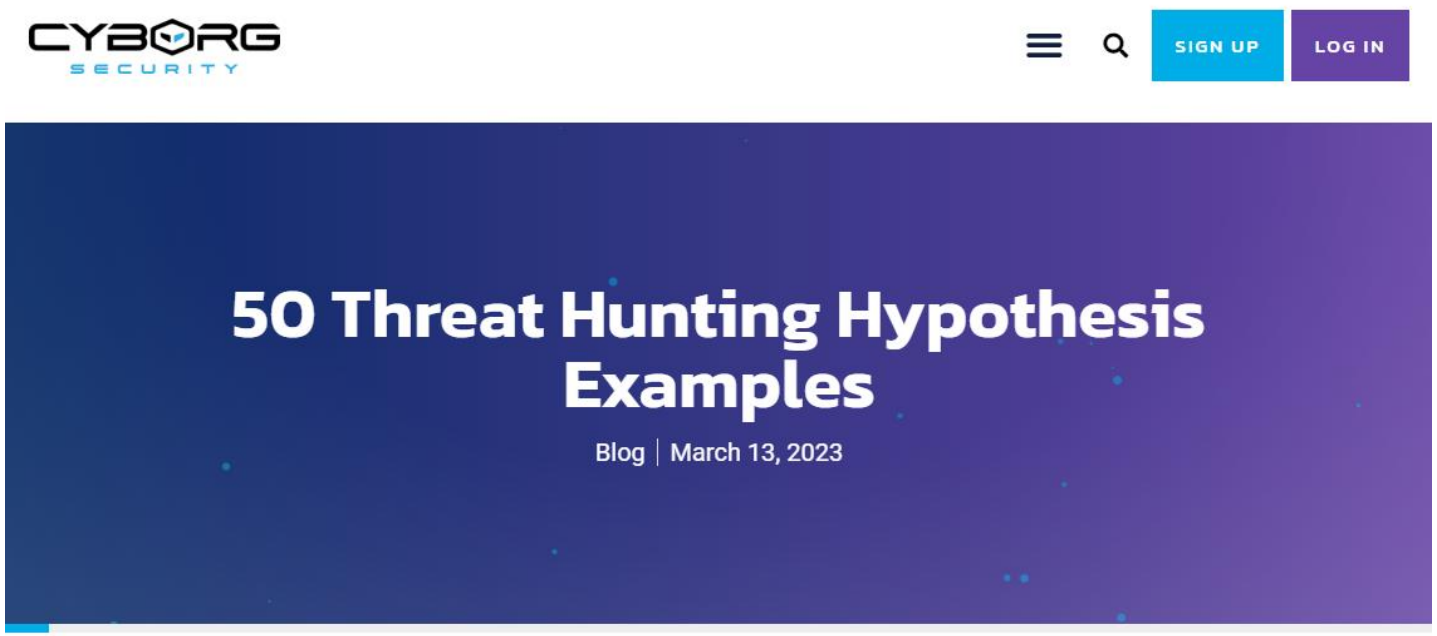
Detection gaps

Increase your detection coverage using the MITRE ATT&CK map to identify gaps.

- Take advantage of the MITRE ATT&CK map



Don’t know where to start?



https://bit.ly/TH_HypoEx

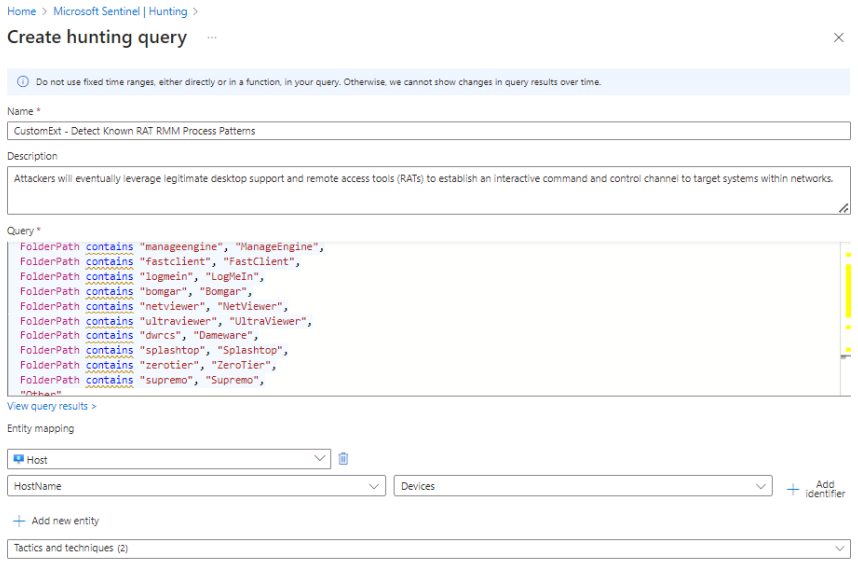
Define your hypothesis
(and deploy the hard way)

...by brushing up your KQL skills!

TEST FIRST! And then...

Create custom queries:

- Hunting > Queries > New query
- Name/Description/KQL query
- Entity mapping
- Define MITRE ATT&CK tactic, technique, and sub-technique (if applicable)

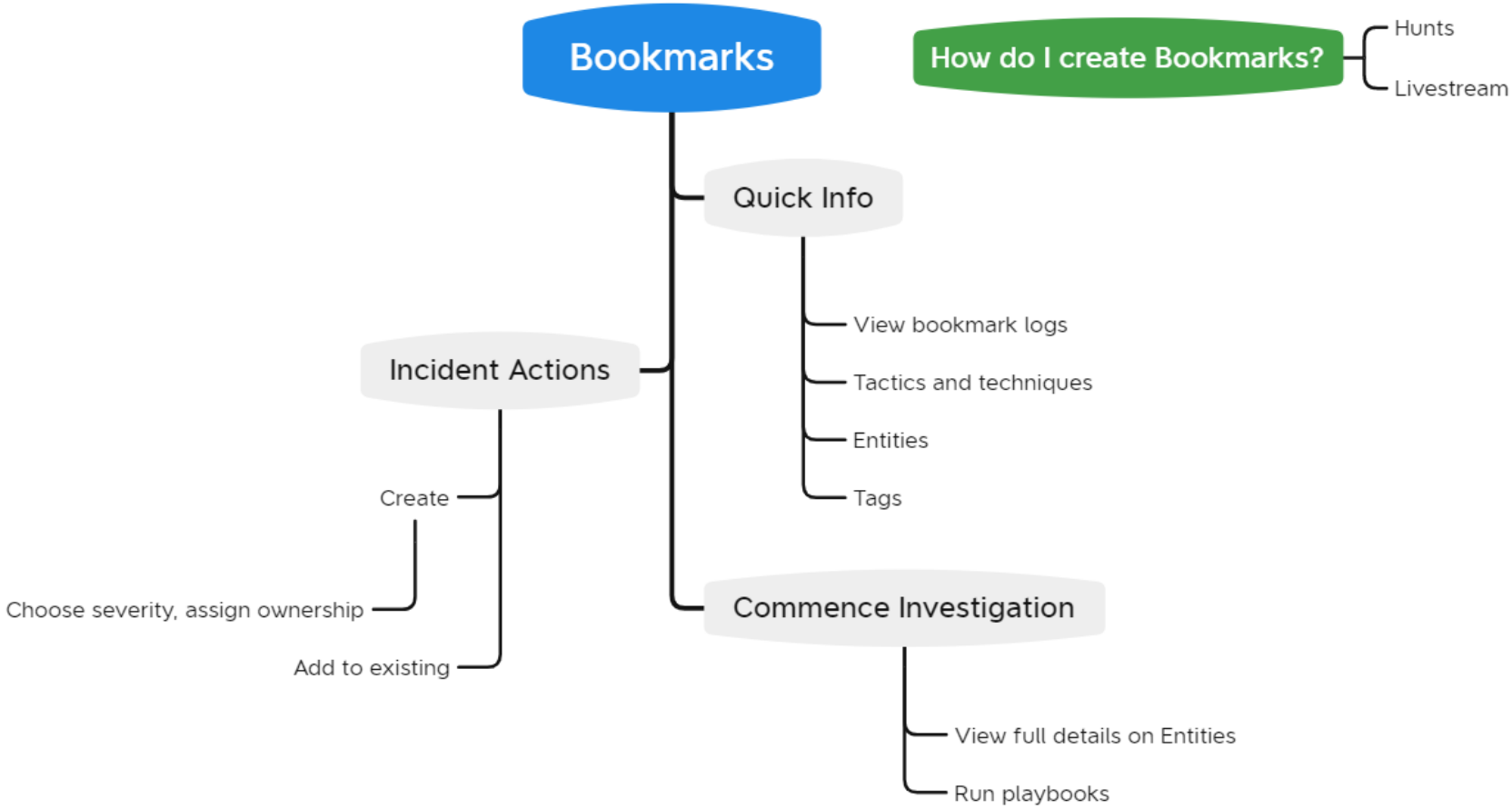


Let’s go Hunt!

Adversaries may attempt to exploit unauthorized remote access tools in an environment where remote management software is not officially used to bypass security controls and maintain persistence.

T1219 Remote Access Software

Bookmarks


Bookmarks
How do I create Bookmarks?
Hunts
Livestream
Quick Info
View bookmark logs
Tactics and techniques
Entities
Tags
Incident Actions
Create
Choose severity, assign ownership
Add to existing
Commence Investigation
View full details on Entities
Run playbooks

Other things to do?

You can add comments to your Hunt

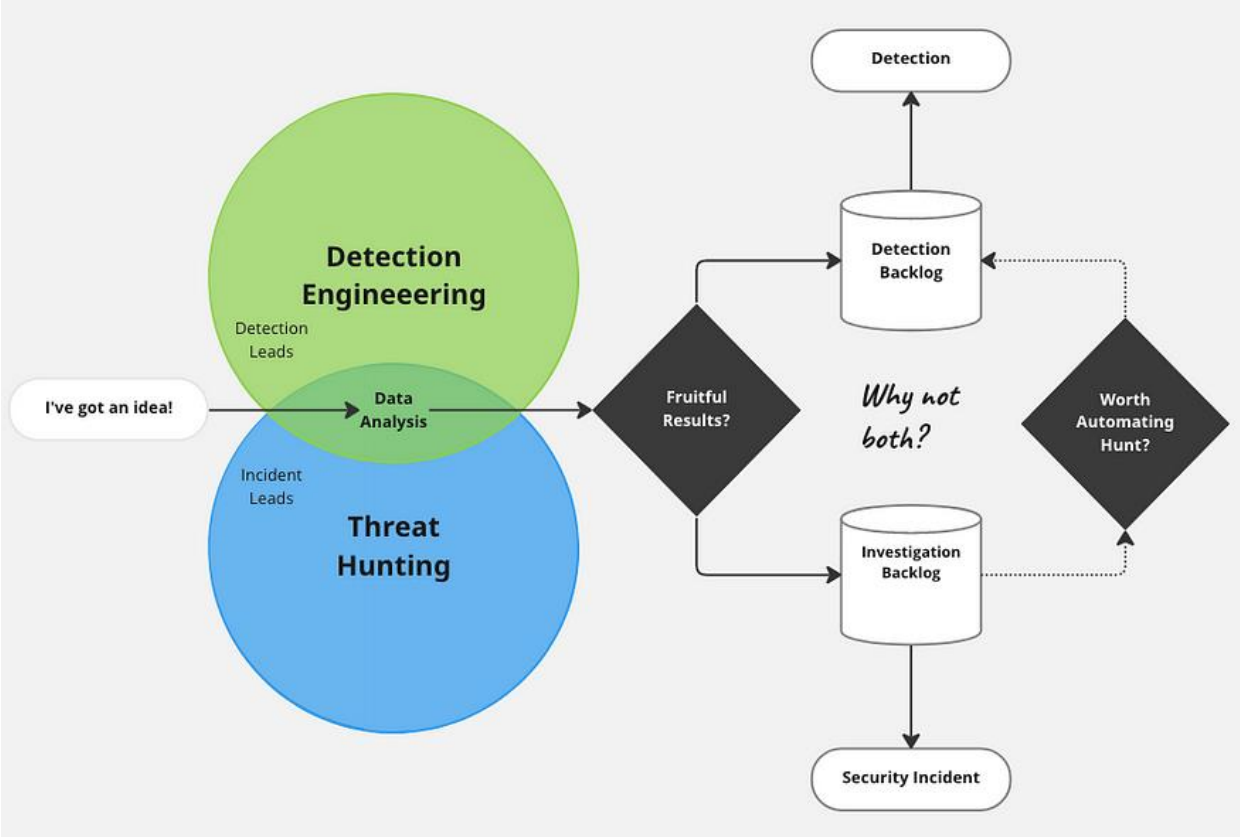
You can change the status of your Hunt

You can validate your Hunt Hypothesis

You can add Tags to contextualize

You can create an Incident from your Hunt

Not happy or just testing functionality? You can delete your hunt



https://detect.fyi/ by Alex Texeira

So maybe turn a query into an analytic?

Considering Validated Hunts

Closing remarks

MAD20 offers affordable and top-tier threat hunting training

Disneyland had a terrible first day, don't look down. Research, deploy, reconsider until you own this

Don't forget the 3 important –ing's, Formalizing, Organizing, Documenting

Always look towards growth. For example, take care of your data gaps, revisit your sources etc.

Thank you

michalos.net

x.com/cyb3rmik3

linkedin.com/in/mmihalos