



# **Staying ahead of Threats - Building Hunts in Microsoft Sentinel**

---

Azure Innovators Hub | Public Sessions

Michalis Michalos, October 5<sup>th</sup> 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

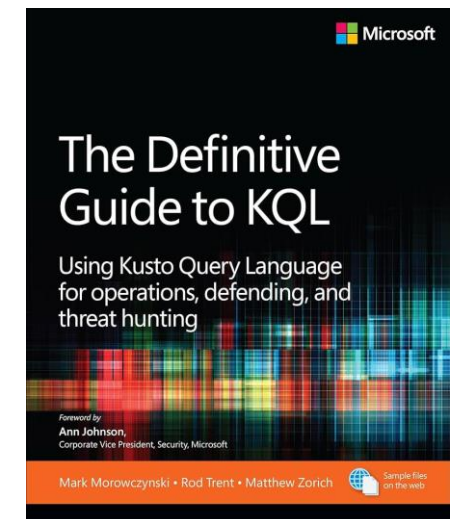
---

- Blogging at [michalos.net](https://michalos.net)
- [github.com/cyb3rmik3/KQL-threat-hunting-queries](https://github.com/cyb3rmik3/KQL-threat-hunting-queries)
- [github.com/cyb3rmik3/MDE-DFIR-Resources](https://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.*

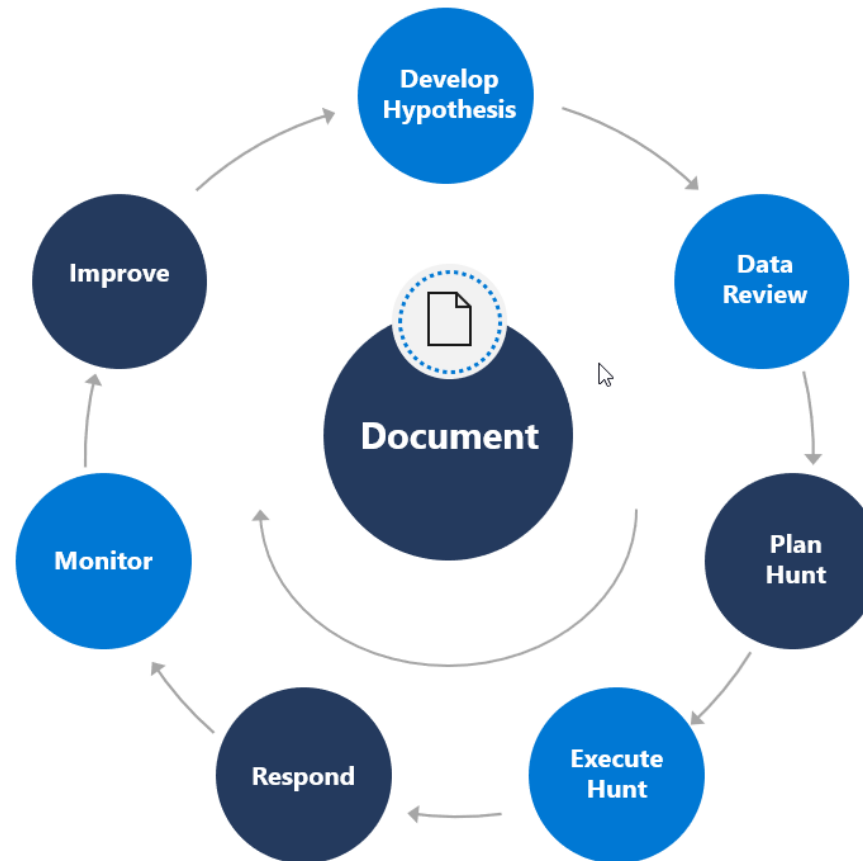
**Structured:** threat hunters look for suspicious tactics, techniques, and procedures (TTPs).

**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?

The screenshot displays the Microsoft Sentinel Hunting interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The user's email, michalis@michalos.net, is visible in the top right corner.

The main heading is "Microsoft Sentinel | Hunting", with the selected workspace being "siem-law-01".

On the left, a sidebar lists various sections: General, Threat management (Incidents, Workbooks), Hunting (selected), Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, and Content management.

The main content area shows a summary of hunting metrics: 2/2 Open / total hunts, 1 Validated hypotheses, 1 Incidents created, and 0 Analytic rules created. Below this, there are tabs for Hunts (Preview), Queries, Livestream, and Bookmarks.

The "Hunts (Preview)" tab is active, displaying a table of hunts. The table has columns for Hunt name, Status, Hypothesis, Owner, Created time, and Last updated. Two hunts are listed: "RMM - Test" (Active, Validated) and "Account Manip..." (New, Invalidated).

A detailed view of the "RMM - Test" hunt is shown on the right. It includes the hunt name, description, and content. The hunt is owned by "Michalis ..." and is currently "Active". The hypothesis is "Validated".

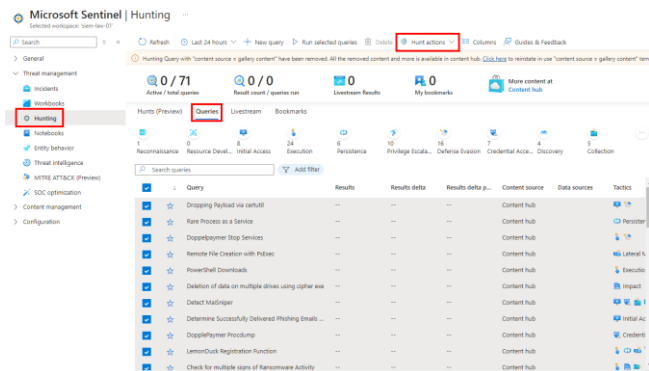
Hunt name	Status	Hypothesis	Owner	Created time	Last updated
RMM - Test	Active	Validated	Michalis Mi...	10/5/2024, 10:3...	10/5/2024, 10:3...
Account Manip...	New	Invalidated	Michalis Mi...	10/3/2024, 9:48...	10/3/2024, 9:48...

# 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.

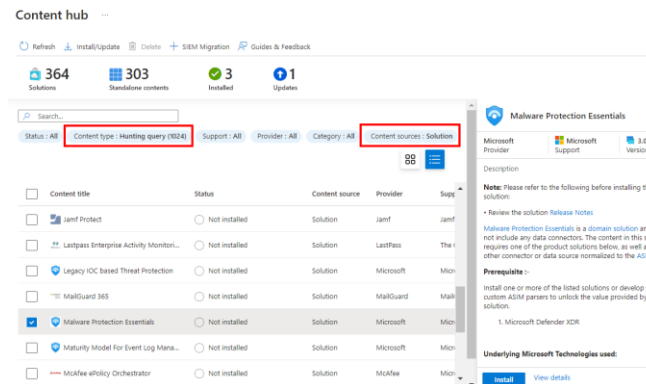
- Create a hunt by using Queries available in Hunting



## New threat campaign

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

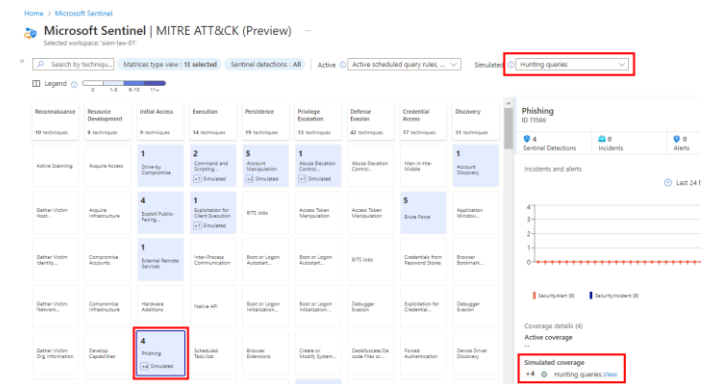
- Leverage Content hub to deploy new campaigns



## 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?

---



SIGN UP

LOG IN

## 50 Threat Hunting Hypothesis Examples

Blog | March 13, 2023

[https://bit.ly/TH\\_HypoEx](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)

Home > Microsoft Sentinel | Hunting >

### Create hunting query ...

Do not use fixed time ranges, either directly or in a function, in your query. Otherwise, we cannot show changes in query results over time.

Name \*

CustomExt - Detect Known RAT RMM Process Patterns

Description

Attackers will eventually leverage legitimate desktop support and remote access tools (RATs) to establish an interactive command and control channel to target systems within networks.

Query \*

```
FolderPath contains "manageengine", "ManageEngine",
FolderPath contains "fastclient", "FastClient",
FolderPath contains "logmein", "LogMeIn",
FolderPath contains "bomgar", "Bomgar",
FolderPath contains "netviewer", "NetViewer",
FolderPath contains "ultraviewer", "UltraViewer",
FolderPath contains "dwrccs", "Dmaware",
FolderPath contains "splashtop", "Splashtop",
FolderPath contains "zerotier", "ZeroTier",
FolderPath contains "supremo", "Supremo",
FolderPath contains "ntracast"
```

View query results >

Entity mapping

Host

HostName Devices + Add identifier

+ Add new entity

Tactics and techniques (2)

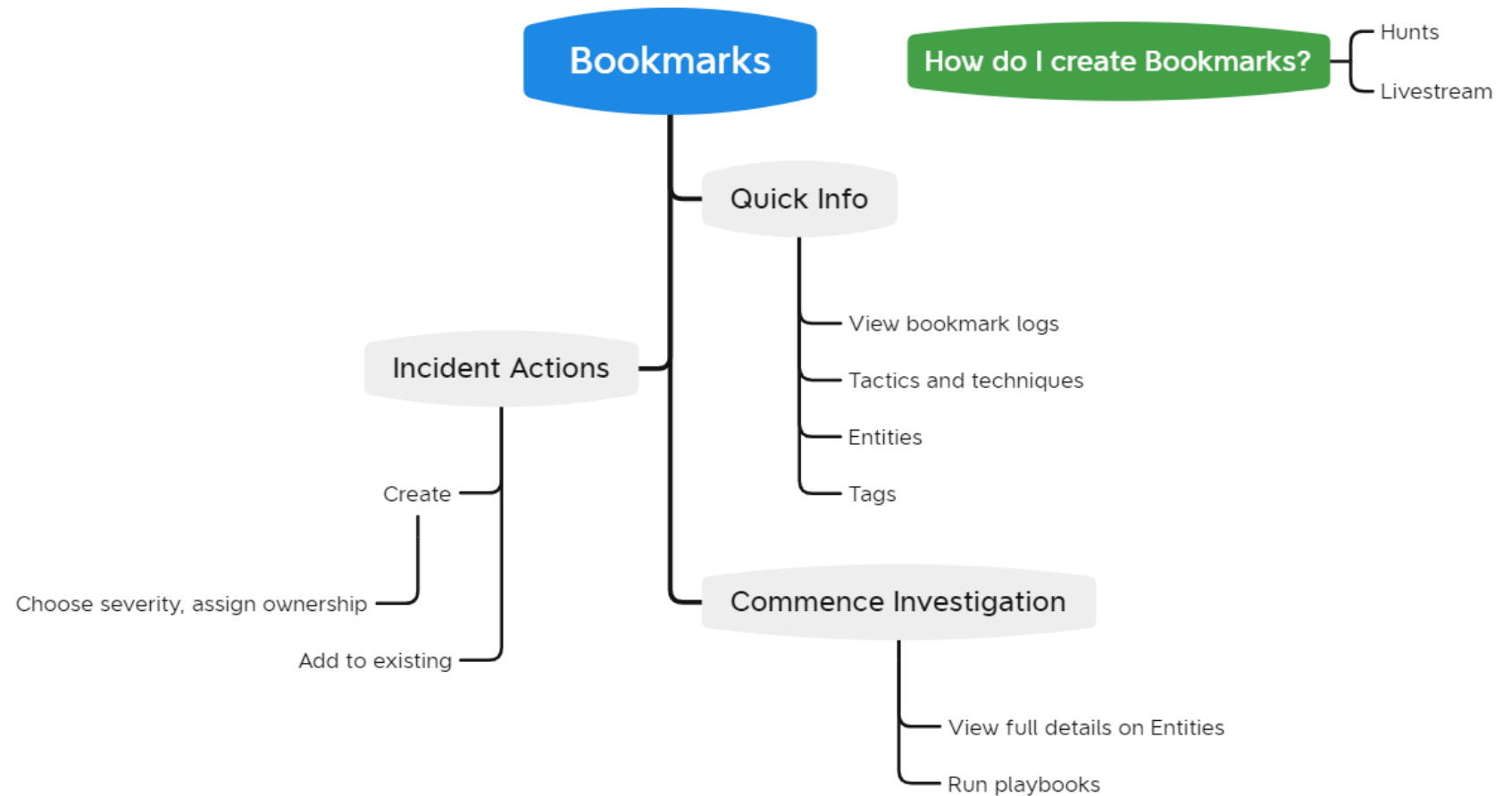
# Let's go Hunt!

---

*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



# Other things to do?

---

You can add comments to your Hunt

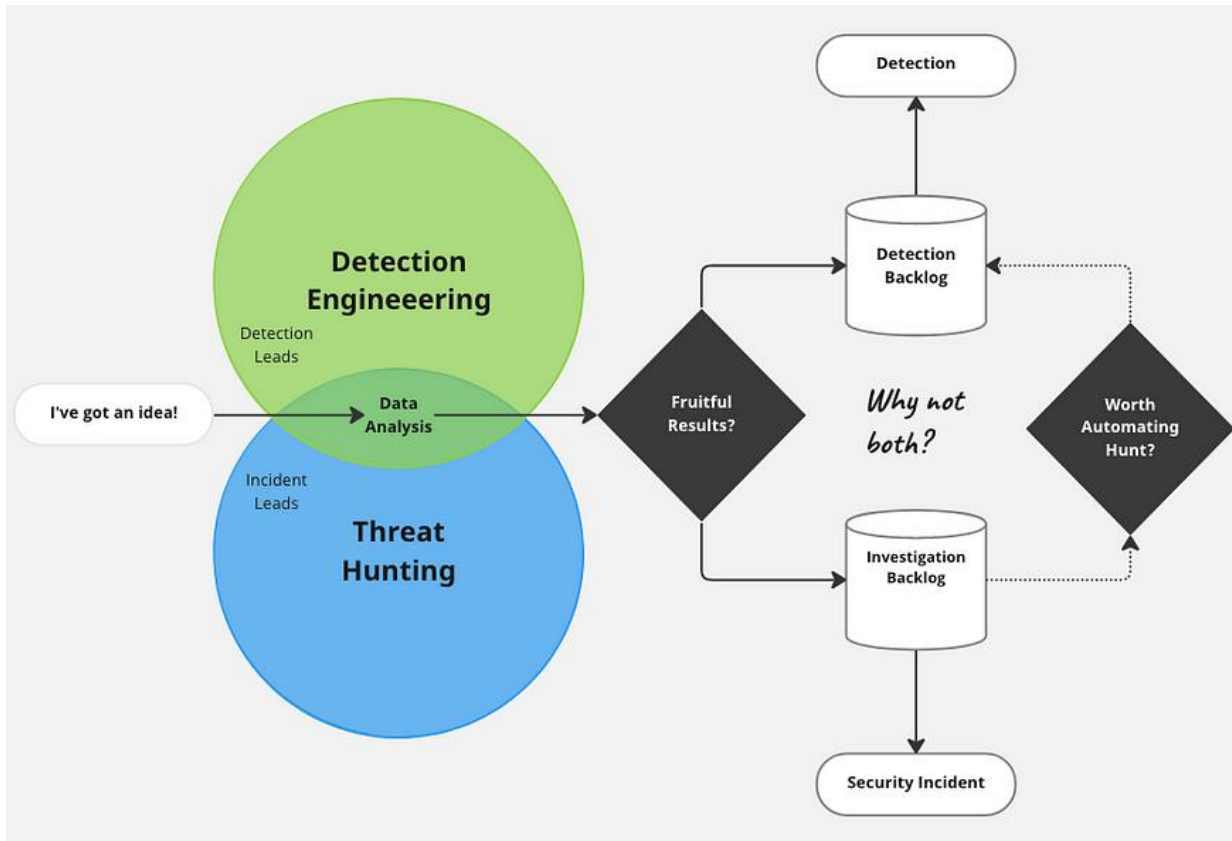
You can change the status of your Hunt

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](https://michalos.net)

[x.com/cyb3rmik3](https://x.com/cyb3rmik3)

[linkedin.com/in/mmihalos](https://linkedin.com/in/mmihalos)