A close-up of a sign

AI-generated content may be incorrect.

🎯 **Goal for this Project:**

To create an end-to-end workflow where an AI tool (like ChatGPT) helps me analyze threat intelligence (such as APT reports), engineer custom detections from it, deploy them to Microsoft Sentinel, and perform threat hunting using KQL queries.

🧰 **Required Tools & Accounts:**

✅ Free OpenAI ChatGPT or GPT-5 account (or Claude/Gemini if preferred)

✅ Microsoft Sentinel (Free Tier on Azure works)

✅ Access to threat intelligence reports / articles (e.g., JINX-0132, Lazarus, etc.)

[Recorded Future](https://www.recordedfuture.com/)

[Falcon Adversary Intelligence](https://www.crowdstrike.com/en-us/resources/data-sheets/crowdstrike-falcon-adversary-intelligence/)

[Cryptocurrency APT Intelligence: Unveiling Lazarus Group’s Intrusion Techniques | by SlowMist | Medium](https://medium.com/@slowmist/cryptocurrency-apt-intelligence-unveiling-lazarus-groups-intrusion-techniques-a1a6efda7d34)

🧭 Step-by-Step Walkthrough:

📥 **Step 1 – Threat Intelligence Analysis:**

* How to use ChatGPT to summarize an APT report (e.g., Lazarus) and extract:
  + TTPs (MITRE ATT&CK techniques)
  + IOCs (IPs, domains, file names, hashes)
  + Tooling or behavior (e.g., Docker abuse, SSH pivoting, GitHub delivery)

**🤖 Step 2 – Use AI Tool to Generate Detection Ideas:**

Prompt [ChatGPT](https://chatgpt.com/) with:

Using this threat intelligence, create a list of SIEM security use cases, and provide some example KQL queries that I can run in MS Sentinel. A screenshot of a computer

AI-generated content may be incorrect.

Result: [SIEM use cases and KQL](https://chatgpt.com/c/689cd102-1fec-832c-b92b-dc301f7716b0)

🛠️ **Step 3 – Detection Engineering:**

**Search best practice:** past 90 days to 1 year for indicators in the network

Paste and test the AI-generated KQL queries in Sentinel’s “Logs” blade.

Modify or fine-tune the queries to filter out false positives.

Examples:

* + Outbound traffic to malicious IPs
  + Python file executions
  + SSH lateral movement

🔔 **Step 4 – Create Analytics Rule in Sentinel**A screenshot of a computer

AI-generated content may be incorrect.

Convert working KQL into an Analytic Rule (Scheduled Query).

Set threshold, severity, and alert logic.

🔍 Step 5 – Threat Hunting

Go to the “Hunting” blade in Sentinel and run the detections manually.

✅ Final Outcome:

A fully working threat-hunting system powered by ChatGPT + Microsoft Sentinel, capable of:

Analyzing real-world threat reports

Creating detections based on IOCs & TTPs

Hunting threats across your environment

Saving time using AI to do the heavy lifting

**What I Have Learned:**

* How to find threat intelligence
* How to turn threat intelligence into detection rules
* How to perform threat hunting
* How to use A.I. Tool to do this for me
* Explained the overall workflow:
  + From analyzing threat intelligence using AI to hunting threats in Sentinel using custom detections.