**Threat Intelligence Gathering and Threat Hunting**

In this project, I will gather:

* **Indicators of Compromise (IOCs)** from open threat intelligence sources
* Run a **threat hunt** by searching for these IOCs in my environment using

**Kusto Query Language (KQL)** in **Azure Sentinel**.

* Search the **SecurityEvents** table for potential threats that match the gathered IOCs.

This project will help me gain practical experience in combining threat intelligence with proactive threat hunting techniques. This approach is critical for SOC analysts because it shifts security from reactive alert triage to proactive threat hunting. By identifying threats that bypass standard detection rules and surfacing them through log analysis, analysts can detect stealthy adversaries (like APTs) earlier, minimize containment time, and strengthen incident response readiness.

**Step 1: Gather Threat Intelligence and IOCs**

My first task is to search for IOCs—such as malicious IP addresses, domains, file hashes, or URLs—from public threat intelligence sources. These indicators can be used to identify potential threats within your environment.

**1. Identify Open Threat Intelligence Sources**

Use the following websites to gather IOCs:

* **The Hacker News** [The Hacker News | #1 Trusted Source for Cybersecurity News](https://thehackernews.com/)
* **Dark Reading** [Dark Reading | Security | Protect The Business](https://www.darkreading.com/)
* **Bleeping Computer** <https://www.bleepingcomputer.com/>
* **VirusTotal:** A free tool for scanning files, URLs, and IP addresses for malware and other malicious activity.
* **AlienVault OTX:** Open Threat Exchange (OTX) provides crowdsourced threat data.
* **AbuseIPDB:** A database of IP addresses reported for malicious activity.
* **Spamhaus:** Lists of malicious IPs, domains, and email spammers.
* **ThreatFox:** A platform that provides a wide range of IOCs like IPs, domains, and hashes.

**2. Collect IOCs**

* **Github IOC Search Sample:** **A screenshot of a computer

  AI-generated content may be incorrect.**

<https://github.com/volexity/threat-intel/blob/main/2024/2024-08-02%20StormBamboo/iocs.csv>

Look for:

* **Malicious IP addresses**: IPs involved in botnets, DDoS attacks, or malicious traffic.
* **Domains**: Known phishing or malware distribution domains.
* **File hashes (MD5, SHA256)**: Hashes of malicious files detected by the threat intelligence sources.
* **URLs**: URLs associated with phishing sites or malicious content.

**Example IOC List (for the project):**

* IPs: 185.234.217.58, 104.28.10.33
* Domains: malicious-domain[.]com, evil-site[.]net
* File hashes: b0a8fe5b1c739f97cd6abbd18e531b9d3eb84f5f
* URLs: <http://bad-url.com/malware>

**Step 2: Prepare Your Environment for Threat Hunting in Azure Sentinel**

You will be using **Azure Sentinel** for the threat hunt. Before starting the hunt, ensure that your Sentinel instance is set up and that you're ingesting logs into the **SecurityEvents** table.

1. **Log in to Azure Sentinel:**
   * Go to [Azure Portal](https://portal.azure.com) and navigate to **Azure Sentinel**.
2. **Check Data Availability:** **A screenshot of a computer

   AI-generated content may be incorrect.**
   * Make sure that the **SecurityEvents** table is collecting logs from your environment (e.g., Windows Server security logs or other log sources). This is where you'll search for the IOCs.

**Step 3: Build a KQL Query to Search for IOCs**

Now that you’ve gathered your IOCs, it’s time to use **Kusto Query Language (KQL)** to search the **SecurityEvents** table for signs of compromise.

**1. Access the Log Analytics Workspace**

1. Open **Azure Sentinel** in the portal.
2. In the **Threat Management** section, click **Logs** to open the query editor.

**2. Write a KQL Query to Search for IOCs**

* **Search for Malicious IP Addresses:** **A screenshot of a computer

  AI-generated content may be incorrect.**

SecurityEvent  
| where IpAddress in ("185.234.217.58", "104.28.10.33")  
| project TimeGenerated, Computer, IpAddress, AccountName, EventID

* **Search for Malicious Domains in CommandLine Logs:** **A screenshot of a computer

  AI-generated content may be incorrect.**

SecurityEvent  
| where CommandLine has\_any ("[malicious-domain.com](http://malicious-domain.com)", "[evil-site.net](http://evil-site.net)")  
| project TimeGenerated, Computer, CommandLine, AccountName

* **Search for Malicious File Hashes:** **A screenshot of a computer

  AI-generated content may be incorrect.**

SecurityEvent  
| where Hash in ("b0a8fe5b1c739f97cd6abbd18e531b9d3eb84f5f")  
| project TimeGenerated, Computer, Hash, AccountName, FileName

* **Search for Malicious URLs in Network Logs:** **A screenshot of a computer

  AI-generated content may be incorrect.**

SecurityEvent  
| where CommandLine has\_any ("[http://bad-url.com/malware")  
|](http://bad-url.com/malware%22)￼|) project TimeGenerated, Computer, CommandLine, AccountName

**3. Combine IOCs into a Single Query**

To run a broader search for all types of IOCs, you can combine them in one query: A screenshot of a computer

AI-generated content may be incorrect.

SecurityEvent  
| where IpAddress in ("185.234.217.58", "104.28.10.33")  
or CommandLine has\_any ("[malicious-domain.com](http://malicious-domain.com)", "[evil-site.net](http://evil-site.net)", "[http://bad-url.com/malware")  
or](http://bad-url.com/malware%22)￼or) Hash in ("b0a8fe5b1c739f97cd6abbd18e531b9d3eb84f5f")  
| project TimeGenerated, Computer, IpAddress, CommandLine, Hash, AccountName

**Step 4: Run the Query and Analyze the Results**

1. **Run the KQL Query**:
   * Click **Run** to execute the query and see the results.
2. **Analyze the Results**:
   * Review the logs for any matches to the IOCs you gathered.
   * Investigate the event details such as the **TimeGenerated**, **Computer**, **AccountName**, and **CommandLine** information to determine the context of the potential threat.
   * If matches are found, consider taking further steps to investigate or mitigate the threat.

**What I Learned 🏆**

* **Threat Intelligence Gathering:**
  + Understanding the concept of proactive threat intelligence, which involves collecting, analyzing, and using information about potential threats to improve defenses.
  + Learning how to gather Indicators of Compromise (IoCs) such as suspicious IP addresses, domains, file hashes, and other malicious artifacts from various threat intelligence sources.
* **Leveraging KQL for Log Analysis:**
  + Writing Kusto Query Language (KQL) queries to search logs for IoCs in Sentinel’s vast data set.
  + Searching for patterns in log data that may indicate malicious activity, such as failed login attempts, unusual network traffic, or abnormal user behavior.
* **Proactive Threat Hunting:**
  + Performing threat hunting by proactively searching for malicious activity using IoCs in Microsoft Sentinel.
  + Correlating log data across multiple sources to identify advanced persistent threats (APTs) or anomalous behavior that may not trigger traditional security alerts.
  + Using time-based analysis to spot patterns and trends over specific periods, such as bursts of activity from specific IP addresses or user accounts.