Threat Intelligence Hero Scenarios

Usama Shabbir

Revealing the malicious actors involved in Cyber threats

Cyber threats encompass a wide range of malicious activities aimed at disrupting, damaging, or gaining unauthorized access to computer systems, networks, or personal devices. Cyber security analysts perform a brief analyzes using any threat intelligence platform to proactively identify and understand the tactics, techniques, and procedures (TTPs) of malicious actors. They analyze data from various sources, providing actionable insights that can help predict and mitigate potential threats before they cause harm.

Scenarios

Sub-Scenario 1: Cyber Security Analysts responding to phishing attack

TARGET PERSONA/USER ROLE: Security Analyst

SITUATION: A phishing attack took place in a sensitive organization to steal financial information.

DECISIONS ENABLED:

A. From which source does this attack took place?

B. Who is behind this attack?

C. How to mitigate such attacks?

CURRENT PRACTICE: A resource intensive task is performed including data extraction, filtration and refinement to gain insight into the attacks various features like source location and personal. This practice is a bit tedious as we need to filter through trillions of records.

OBJECTIVE: To Empower the security analysts team with the live, historical and reverse data for threat detection.

SAMPLE PROMPT AND EXPECTED RESPONSE:

Before consulting with Copilot for security analysts need to find the domains or IPs from which attack took place. This will act as a starting point for analysis and can be easily found out using the logs.

- **Analyst:** Who are the registrants of such suspicious domains?
- **Copilot:** Returns the registrant names or the owners of such domains.
- **Analyst:** List domain names that are registered under the name or email of above personal.
- **Copilot:** Returns a list of domains owned by malicious actors.
- **Analysts:** Perform the reverse dns analysis on the malicious Ips to get malicious domain names.
- **Copilot:** Returns a list of domains.
- **Analysts:** Get the live WHOIS details of all domains extracted till now. Mark the red zone geographical area based on the registrant details. And further get the contact details from WHOIS too.

After all this analysis we will be having a list of domain names there owner details and geographical location. We can took following remedial actions:

- take legal actions against the owner of domains.
- blacklist the domains and IPs for future interaction with your system.
- Blacklist the company under which these domains were registered.
- Blacklist the owner of such domains too for future interaction.