Using Cyber Threat Intelligence and Forming a Hypothesis

By Grant Knoetze

What is CTI?

- CTI is intelligence that is gathered on adversaries, typically APT groups.
- We use the Mitre Attack framework and matrices to gather intelligence on APT groups, including their TTP’s.
- You can use this to formulate your hypothesis for your threat hunting.
- You can also use Microsoft Threat reports for up to date threat intelligence on the latest and common threats and vulnerabilities that are taking place in the wild.

Forming a Hypothesis Based on CTI

- Use Mitre Attack to study the APT groups targeting the specific type of enterprise that you are defending (i.e.: health, finance)
- https://attack.mitre.org/groups/
- Utilize Microsoft Threat Intelligence to remain up to date with attackers latest TTP’s.