KQL Technique Mapping Best Practice

Detection Query Process

Select ATT&CK Technique and Sub-techniques

Select Use Cases

Research

How the Technique works

Identify

Data Sources -Availability

Detection Scenario – how attack can present itself, what events to monitor

Visualise

Useful info from KQL search – Source type, Columns, Event Codes & Fields

Extract/Review

Detection Query

Write

Revise

Fine Tune Detection

1. Select Use Case:
   1. First starting with selecting the Att&ck techniques and sub-techniques, usually follows the completion of a threat model.
2. Research:
   1. Do your homework on the Att&ck Technique identified. Sources include MITRE website, online searches and forums. The goal is to understand how the technique works and how it can be exploited in relation to the use case as well as the organisation.
3. Identify:
   1. Identify which data sources need to be monitored and leveraged for the technique. Checking availability of the data sources in the environment is crucial, as not all data sources identified in Att&ck may be onboarded.
4. Visualise:
   1. In this step try to visualise and hypothesise the technique within the use case scenario. What events need to be monitored to detect it, best to write this on paper. How will the Att&ck present itself in. Attackers only need to be right once.
5. Extract / Review:
   1. Review logs, begin to pick out useful information necessary for the detection query. Look for relevant information such as; columns, event codes, field names, event and device types.
6. Write:
   1. Develop query
   2. Follow Microsoft best practices for optimal performance e.g. “has” over “contains”
7. Revise:
   1. Fine tuning is needed before deployment into production environment. This will include revisiting the detection query to reduce the number of potential FP’s. This step may also include bringing in allow and block lists.
   2. Peer review