#Characteristic-Based-Alerting

##Premise

- Signature based alerting is ineffective as changes to remove the detected signature are often easily implemented.
- Specific attack tactics and techniques will cause a detectable characteristic. These characteristics can be detected through targeted specific detection rules that baseline normal usage and detect outliers.
- By focusing detection rules on devices, device types, users or user groups, it is possible to reduce the environmental noise and detect attack characteristics (changes in behaviour/operations)
- The detection of a single outlier may be a false positive but the detection of multiple characteristics for a single technique on a single device is more likely to be a true positive. This is designed to work with alert aggregation techniques.

##Requirements

- Alerting based on Mitre Attack techniques
- Alerts context is as narrowly focused as possible
- Rules specific to individual devices to enable the creation of an accurate baseline
- Alerting designed to detect the characteristics that the technique will induce, such as a change in network flow, an unusual process spawn sequence or an unusual use of addressing (URL)

##Pros

- Narrow context alerting enables:
    - Low false positive count
    - High fidelity alerting
- Avoiding the use of signatures increases the time that the alert remains effective
    - Signature based alerts can go stale in a shorter period of time, as attackers change TTPs or code to alter signatures. This leads to higher maintenance effort for signature based alerting.

##Cons

- Narrow focus necessitates greater alert quantity
    - Can be partially mitigated through effective device categorisation and management through SOAR
- High fidelity alerting can lead to high alert counts
    - Effective alert aggregation can fully mitigate this.
- Increase alert count may increase SIEM resource demands
- Alert aggregation is required, such as Symptomatic Aggregate Alerting or Risk Based Alerting.
    - The implementation of alert aggregation is an effective SOC improvement to reduce alert fatigue and improve alert accuracy metrics.

##Method

Detections based on the induced characteristics created by individual Mitre Attack techniques, not signatures. As each technique is an attack and not normal device or user behaviour it induces a change in a characteristic that can be detected. Attackers may try to tailor their actions such that the induced characteristic is negligible when compared to the enterprise environment. However when compared to the individual device, device type, user or user group these characteristics can be more easily detected.