Microsoft Sentinel is an excellent SIEM. It combines advanced analytics with significant customization capabilities. However, applying advanced analytics to your custom logs is hard.

This hackathon project gathered the best Sentinel content minds to resolve this issue. Devika, Ofer, Will, Edi, Jitesh, and Ofer, joined forces to create powerful custom analytics in Sentinel. We wanted to create a solution using only Sentinel's content building blocks, such as KQL, Logic Apps, Analytic Rules, and Workbooks so that anyone (that's You!) can join and contribute.

Let's first look at the challenge. KQL is powerful and supports advanced analytics. But there are two caveats:

First, analytic rules that build behavioral profiles each time they run are inefficient. This is why analytic rules are limited to looking back only 14 days, hence profiling only a fortnight.

Secondly, analytics is complicated, and using KQL for analytics is no exception.

So, how did we go about solving those challenges?

We have used Logic Apps to ensure efficiency by summarizing the data and generating predictions. Those are written back to the Sentinel workspace and are used by analytic rules to detect anomalies. And to make things simpler, all elements read their configuration from Watchlists, eliminating the need for editing Logic Apps or KQL queries.

Let's look at the details:

Devika's scheduled Logic App summarizes new events from your selected sources. The Logic App creates aggregative time bins, which are much more efficient for longer-term analysis. Using a Watchlist, you can decide which sources and fields to analyze, thus connecting your custom logs to our solution.

The bins are then analyzed by Will's scheduled Logic Apps, which create predictions. These must look back into history, but since they analyze aggregated data, they are still performant. To start with, we implemented two prediction algorithms: time series decomposition and rare relationships.

Ofer's rule then compares the predictions to the current data and generates anomalies, which are specially annotated Sentinel alerts. Use a workbook to investigate anomalies or analyze them with other indicators to trigger an incident. We have created an example rule that aggregates our anomalies, but your rule should combine other signals to generate incidents.

This is a work in progress. You can find what we have delivered so far on our GitHub repository at https://aka.ms/Sentinel-Custom-Analytics. Since it is all Sentinel content, you can use this as a starting point for your experimentation with Sentinel custom analytics.