Microsoft Sentinel in 30 Days

- **Problem**
  - Our client was on an aging SIEM platform that was end of life and needed to be replaced.
  - They were constrained on data ingestion due to capacity and scaling of an on-premise managed system.
  - They were limited in how they could react to the alerts that were generated, and their SOC teams processes were very manual.
- **Solution**
  - We reviewed their existing SIEM platform to understand the current state as well as discussing their strategy for security operations.
  - Reviewed their cloud strategy to understand how they were using public cloud.
  - Using the information gathered, defined an architecture for Microsoft Sentinel that would be scalable and secure as the customer moves along their cloud journey.
  - Deployed and configured Microsoft Sentinel with the necessary log sources, analytic rules/workbooks, initial automation framework and access control model to help them scale their usage of Microsoft Sentinel.
- **Benefits**
  - Our client was able to quickly get Microsoft Sentinel deployed and configured in a scalable and secure manner.
  - They have a defined process for onboarding new log sources, configuring and tuning analytic rules to remove false positive alerts, streamlining SOC operations as well as starting with limited automation for remediation.