Malicious PowerShell Detections

PLATFORM FEATURE UPDATE

PowerShell is a trusted management tool for system administrators that is also frequently used as an attack vector. The Malicious PowerShell Detection model utilizes a large dataset of legitimate PowerShell executions to detect string patterns associated with normal operations. PowerShell executions that break these patterns are flagged as anomalous and the behavior is summarized to help security analysts determine its significance.

Some important things to note are:

- Anomalous PowerShell executions are grouped together in one detection if they have similar signatures.
- Any execution containing 'PowerShell' in the command-line is a candidate for this detection.
- This model executes daily and produces detections for the previous day.