1. **Detects processes (Image) that have an unusually high number of network connections in a given hour compared to their 24-hour historical baseline**.

```
index="main" sourcetype="WinEventLog:Sysmon" EventCode=3
   | bin _time span=1h
   | stats count as NetworkConnections by _time, Image
   | streamstats time_window=24h avg(NetworkConnections) as avg
  stdev(NetworkConnections) as stdev by Image
   | eval isOutlier=if(NetworkConnections > (avg + (0.5*stdev)), 1, 0)
   | search isOutlier=1
```

➔ Search for Sysmon network connection events (EventCode=3).

↓ `sourcetype="WinEventLog:Sysmon" EventCode=3`

➔ Group events into **1-hour intervals**

↓ `| bin _time span=1h`

➔ Count the number of network connections (count) for each process (Image) per hour.

↓ `| stats count as NetworkConnections by _time, Image`

➔ For each process (Image), calculate:
- Running average (avg)
- Running average (avg)
- Running standard deviation (stdev)

Uses a **24-hour** sliding window for more dynamic baseline detection.

↓
```
| streamstats time_window=24h avg(NetworkConnections)
  as avg stdev(NetworkConnections) as stdev by Image
```

➔ Marks an event as an outlier (**isOutlier=1**) if the current hourly connection count:
- Exceeds the **average + half the standard deviation**.
- Otherwise, **isOutlier** is set to **0**.

↓
```
| eval isOutlier=if(NetworkConnections > (avg + (0.5*stdev)),
    1, 0)
```

➔ Only show entries that are considered outliers (potentially abnormal network activity).

↓ `| search isOutlier=1`

2. **Detection Of Abnormally Long Commands**

   Attackers frequently employ excessively long commands as part of their operations to accomplish their objectives.

   After reviewing the results, we notice some benign activity that can be filtered out to reduce noise. Let's apply the following modifications to the search.

3. **Detection Of Abnormal cmd.exe Activity**

   The following search identifies unusual **cmd.exe** activity within a certain time range. It uses the bucket command to group events by hour, calculates the count, average, and standard deviation of cmd.exe executions, and flags outliers

4. **Detection Of Processes Loading A High Number Of DLLs In A Specific Time**

   It is not uncommon for malware to load multiple DLLs in rapid succession. The following SPL can assist in monitoring this behavior.

   After reviewing the results, we notice some benign activity that can be filtered out to reduce noise. Let's apply the following modifications to the search.