Identification & Analysis

1. Identify Unusual accounts:

a. Look for unusual user accounts created specially in RDP or administrator group (C:\> lusrmgr.msc or C:\> net localgroup administrators).
   i. Filter out the usernames which resembles the naming convention of your organization
   ii. Search the account creation events, Event ID#4720

2. Identify Persistence in Common Registry Keys:

b. Look for registry keys in Run and Run once location.
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

3. Identify unusual Processes:

c. Check for unknown process specially starting with 'SYSTEM' or 'Administrator' privileges.
d. Use taskmgr.exe or tasklist /v option for listing verbose output.
e. Use procmon tool to monitor the process hierarchy, search the anomaly across processes.
   i. Have reference from SANS Evil Hunt Poster: https://sansorg.egnyte.com/dl/WFdH1hHnQI

4. Check Persistence in Auto Start Program Folder:

f. Check AutoStart program of windows
g. C:\Users\user_name\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

5. Unusual Services:

h. Check for unusual services by services.msc or net start.

6. Unusual Network Connectivity:

i. Check for file share and network connectivity
j. Netstat -naob
k. Netbios sessions nbtstat -S N.

7. Unusual Schedule Tasks:

l. Look for unusual schedule tasks O. Schtasks /query
m. Schedule Tasks Folder: C:\Windows\System32\Tasks