Identification & Analysis

A. Unusual accounts: Look for unusual user accounts created specially in RDP or administrator group (C:\> lusrmgr.msc or C:\> net localgroup administrators). Unusual Registry Keys: Look for registry keys in Run and Run once location.
    B. HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    C. HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
    D. HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
    E. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
    F. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

G. Unusual Processes: Check for unknown process specially starting with ‘SYSTEM’ or ‘Administrator’ privileges.
    H. Use taskmgr.exe or tasklist /v option for listing verbose output.

I. Auto Start Program: Check AutoStart program of windows C:\Users\user_name\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

J. Unusual Services: Check for unusual services by services.msc or net start.

K. Unusual Network Connectivity: Check for file share and network connectivity
    L. Netstat -aon
    M. Netbios sessions nbtstat -S

N. Unusual Schedule Tasks: Look for unusual schedule tasks
    O. Schtasks /query