ATHANASIUS J.K GADOSEY

Week 1

Practical Task: My First Alert

1. Deconstruct the Alert:

   The following are the most important pieces of information:
   - **Timestamp**: 2025-11-05 09:32:15 UTC
   - **User**: jane.doe – this shows the account under which the script (process) was executed.
   - **Process**: powershell.exe – this is usually used to execute a script by abusing the Windows environment.
   - **Destination IP**: 198.51.100.5 – This could likely be a remote connection of the target.
   - **Destination Port**: 4898 – this shows the port on which the destination IP of the target is listening from.
   - **Command Line**: powershell.exe -nop -enc

2. Initial Hypothesis (A Gut Feeling):

   This could likely be a True Positive alert malicious script, based on the suspicious evidence used, such as powershell.exe -nop -enc.

3. Investigative Questions:

   The following are the questions asked to confirm my hypothesis;
   - What does the **PowerShell** script executed do (I mean, is the command downloading or data exfiltration?
   - Was the user (jane.doe) performing any scripting activity around that time?
   - Did the **Dedication IP (198.51.100.5)** appear in any other alert?

4. Iniital Triage & Priority:

   The alert is marked “medium,” and I will usually treat it as High.
   This is because the executed script used an encoded PowerShell command that connected to an unusual network port, making it a red flag. It often means something harmful is happening ~~in~~ the system. An action should be used quickly to prevent any possible data theft.

5. Recommended Next Step:
   The next step is to decode the PowerShell command to see what it actually does, and disconnect the affected computer(I mean DESKTOP-B4K2L8) from the network to stop the threat from spreading.