PRACTICAL ASSESSMENT

SOC TRACK

Contents
SOC ENGINEERING

Duration
6 hours

Date
28/8/2025

SOC ENGINEERING PRACTICAL ASSESSMENT

I. SOC ENGINEERING: PRACTICAL

To access elastic, use this link http://198.96.95.202:5601/login?next=%2F

Username: we-innovate-quiz

Password: dT%t9(YaKCpWwh*D

A. SIEM

1. Hostname Format:
   - Change the "PC Name" in your windows server machine and you **MUST** follow the format:
   GROUP#- FIRSTNAME-LASTNAME

2. Local Audit Policies:
   - Add local audit policies to your windows server machine.

3. Log Generation:
   - Generate some administrative activities that trigger logs.

4. Log Transmission:
   - Send logs using Winlogbeat.

B. Fluentbit

1. Regex Parser:
   - Write a regex parser for this **log file** (extract at least 8 key fields, but you **MUST** extract the source IP and Destination IP).

2. Log Indexing:
- Send the parsed logs to the SIEM.
- Your index should be named: group#-firstname-lastname-fluentbit

3. Dashboard Creation:
   - Create a descriptive dashboard for the logs, visualize some important fields. (bonus)

C. SOAR

Create a new workflow in n8n and do the following steps:

1. IP Extraction:
   - Using the Fluentbit index created in elastic, extract all **destination IP** addresses. (you will need to use Elasticsearch Api to get the logs from the index)

2. Threat Intelligence:
   - Send the IP addresses to VirusTotal to scan their reputation.

3. Email Notification:
- Send an email to **soc.weinnovate@gmail.com** containing the filtered IP addresses that seem to be malicious. The subject of your email **MUST** be in this format: GROUP#_FIRSTNAME_LASTNAME

- **Bonus Challenge:**
  • Integrating additional threat intelligence feeds (ex: AbuseIPDB).
  • Using winlogbeat index created extract logs with event id: [4720,4725,4726]
  • Extract Most important details from extracted logs (ex: event.action, related users, targetUser).
  • Send an email to Soc.WeInnovate@gmail.com containing Extracted details, The subject of your email MUST be in this format: GROUP#_FIRSTNAME_LASTNAME_Account_Management_Summary