Threat Hunting (Elastic + Sigma)

1. Objective

The objective of this task is to perform basic threat hunting by detecting suspicious PowerShell execution using **Sigma rules** and validating the detection using **Elastic Security**.

2. Tools Used

- Windows Virtual Machine
- Elastic Security / Kibana
- Sigma
- PowerShell

3. Sigma Rule Creation

A Sigma rule was created to detect suspicious PowerShell execution using Windows Event ID 4688 (Process Creation).

Sigma Rule

```
title: Suspicious PowerShell Execution
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    NewProcessName|contains: "powershell.exe"
condition: selection
level: high
```

4. Event Generation

To generate a suspicious process creation event, PowerShell was executed on the Windows VM.

```
powershell.exe -Command "Write-Host Test"
```

5. Log Detection in Elastic

In Kibana → Discover, the following query was used:

```
event.code:4688 AND process.name:"powershell.exe"
```

The event was successfully detected, confirming that the Sigma rule logic works.

6. MITRE ATT&CK Mapping

Detection	MITRE Tactic	Technique
PowerShell execution	Execution	T1059 – Command and Scripting Interpreter

7. Conclusion

This task demonstrated how Sigma rules can be used to detect suspicious behavior and how Elastic Security can validate real-time events. Such detections are critical in identifying malicious execution attempts early.