Step 1: Access the Template

- Open the **Pyramid of Pain** template using the provided link.
- If you don’t have a Google account, download the template and work on it offline.

Step 2: Review the Alert Details

- The suspicious file hash:
  SHA256:
  `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`
- **Timeline of Events:**
  - **1:11 PM** - Employee receives an email with an attachment.
  - **1:13 PM** - Employee downloads and opens the file.
  - **1:15 PM** - Malicious executables are created.
  - **1:20 PM** - Intrusion Detection System (IDS) detects the threat and alerts the SOC.

Step 3: Search VirusTotal for the File Hash

- **Go to** VirusTotal
- **Enter the SHA256 hash** in the search bar and analyze the report.

Step 4: Determine if the File is Malicious

Look at the following VirusTotal sections:

1. **Vendors' Ratio**
   - How many security vendors have flagged the file as malicious?

   - A high ratio means a strong likelihood of malware.
2. **Community Score**
   - A **negative score** indicates the file is widely reported as malicious.
3. **Detection Tab**
   - Review the list of security vendors and their assessments.
   - Check if major AV engines (e.g., Microsoft, Kaspersky, McAfee) marked the file as malicious.

➡️ **Conclusion:**
If the file is flagged by multiple vendors, has a negative community score, and is associated with known malware families, it is likely **malicious**.

Step 5: Identify Indicators of Compromise (IoCs)

Use the **Details, Relations, and Behavior** tabs in VirusTotal to identify three IoCs:

1️⃣ Hash Value

- Find another **MD5** or **SHA-1** hash for the same malware under the **Details** tab.

2️⃣ IP Address

- Identify an **IP address** the malware contacted.
- Found in:
  - **Relations tab → Contacted IP addresses**
  - **Behavior tab → IP Traffic**

3️⃣ Domain Name

- Find a **malicious domain** associated with the malware.
- Found in:
  - **Relations tab → Contacted domains**

    - Check if the domain has been flagged by security vendors.

4️⃣ Network/Host Artifact

- Identify **artifacts created by the malware** (e.g., registry modifications, created files).
- Found in:
    - **Behavior tab → Sandbox reports**
    - Look for **file system modifications or registry changes**.

5️⃣ Tools Used

- Check if the malware used **external tools** for execution.
- Found in:
    - **Behavior tab → Execution details**
    - Look for usage of PowerShell, Mimikatz, or other hacker tools.

6️⃣ Tactics, Techniques, and Procedures (TTPs)

- Find **MITRE ATT&CK TTPs** associated with the malware.
- Found in:
    - **Behavior tab → MITRE ATT&CK section**
    - Look for techniques like:
        - **T1059**: Command and Scripting Interpreter
        - **T1204**: User Execution
        - **T1027**: Obfuscated Files or Information

Step 6: Document Findings in the Pyramid of Pain

- Fill in the **Pyramid of Pain template** with the collected IoCs.

- Indicate the **malicious verdict** on the first slide.
- Justify the decision using:
  - Vendors’ analysis
  - Community score
  - Malware behaviors and IoCs

Step 7: Save and Submit

- Once completed, **save the Pyramid of Pain template**.
- Submit the file as required for the course.