**ICS Threat Hunting Lab Guide (APT33 Simulation – 2-Day JSON Logs)**

**Lab Environment Setup Instructions**

**Prerequisites:**

* Elastic Stack (Kibana + Elasticsearch) is already running (e.g., via Malcolm or Docker Desktop)
* You have the following two files locally:
  + apt33\_ics\_day1.json
  + apt33\_ics\_day2.json

**Note:** These JSON files contain Zeek-style, line-delimited logs with fields like log\_type, @timestamp, id.orig\_h, modbus.func\_code, etc.

**Step 1: Upload the JSON Files via Kibana (No Filebeat Required)**

**🔹 A. Open Kibana**

1. Open your browser and go to:

http://localhost:5601

1. From the **Kibana home screen**, click:

Upload a file

Or, go to:

Analytics → Discover → "Upload a file"

**🔹 B. Upload apt33\_ics\_day1.json**

1. Click **"Upload a file"**
2. Drag or browse for apt33\_ics\_day1.json
3. Kibana will parse and preview the log data
4. Click **"Import"**
5. Set the index name:

ics\_day1

1. Click **"Import"** again
2. Once done, click **"View data in Discover"**

Repeat for:

**🔹 C. Upload apt33\_ics\_day2.json**

1. Use the same process above
2. Set the index name:

ics\_day2

**Step 2: Create Data Views (Index Patterns)**

**A. Navigate to:**

Stack Management → Data Views

**B. Create two data views:**

1. **Data View Name**: ics\_day1
   * Index pattern: ics\_day1
   * Time field: @timestamp
2. **Data View Name**: ics\_day2
   * Index pattern: ics\_day2
   * Time field: @timestamp

Now you're ready to hunt!

**Step 3: Conduct a Threat Hunt in Discover**

**🔹 A. Open Discover**

* Go to:

Analytics → Discover

* Select ics\_day1 from the data view dropdown

**B. Explore Day 1 — Establish the Baseline**

**Objective**: Identify normal ICS and IT traffic

1. In the search bar, type:

tags: not "apt33"

1. Add the following columns using the "Fields" panel:
   * @timestamp
   * log\_type
   * id.orig\_h
   * id.resp\_h
   * modbus.func\_code
   * dnp3.function\_code
   * http.uri
   * dns.query
   * tags

Students should observe:

* Modbus and DNP3 traffic between 192.168.1.100 and outstations
* Normal IT traffic (HTTP, DNS) from external or IT clients
* No malicious writes or odd ports

**C. Explore Day 2 — Detect Attacker Behavior**

Switch to ics\_day2 in the top-left dropdown.

**Objective**: Identify attacker activity from 192.168.3.30 (APT33)

1. Use this filter:

tags: "apt33"

1. Add the same fields as before.

Students should:

* Observe Modbus/DNP3 Write function codes (5, 6, 15, 16)
* See 192.168.3.30 initiating RDP or HTTP connections
* Discover DNS queries to suspicious external domains (e.g., malicious.biz)
* Find beaconing patterns to public C2 IPs (e.g., 8.8.8.8, 203.0.113.50)

**Step 4: IOC Pivoting & Timeline Building**

1. In **Discover**, expand specific log entries
2. Use the **filter icon** next to IPs or fields to:
   * Pivot on id.orig\_h: "192.168.3.30"
   * Filter by specific ports (e.g., 502 for Modbus)
   * Narrow time range to off-hours (e.g., 01:00–06:00 UTC)
3. Build a timeline:
   * RDP → Modbus → DNS → HTTP
   * Use @timestamp to correlate activity

**Threat Intelligence Mapping: APT33 + MITRE ICS ATT&CK**

| **Behavior** | **Log Type** | **Technique ID** | **Description** |
| --- | --- | --- | --- |
| Modbus write coils | modbus.log | T0855 | Unauthorized Command Message |
| Network probing | conn.log | T0846 | Network Sniffing |
| RDP lateral movement | rdp.log | T0866 | Remote Services |
| DNS queries to external domains | dns.log | T0861 | Standard Application Layer Protocol |
| Beacon to HTTP C2 | http.log | T0887 | Application Layer Protocol - Web Protocols |

**Discussion Questions**

1. What function codes were suspicious?
2. Which IPs initiated suspicious connections?
3. What log types were most useful?
4. What’s the difference between Day 1 and Day 2?
5. How would you alert on this behavior using a SIEM?