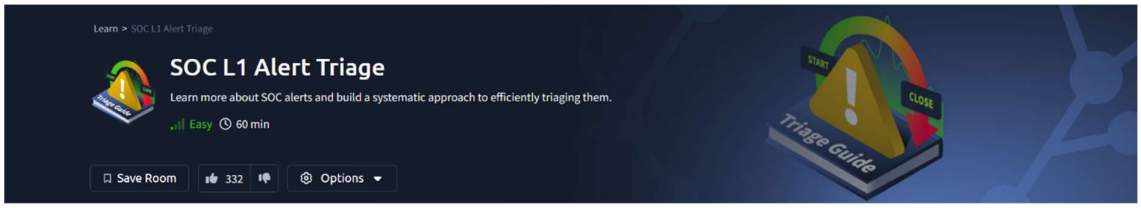
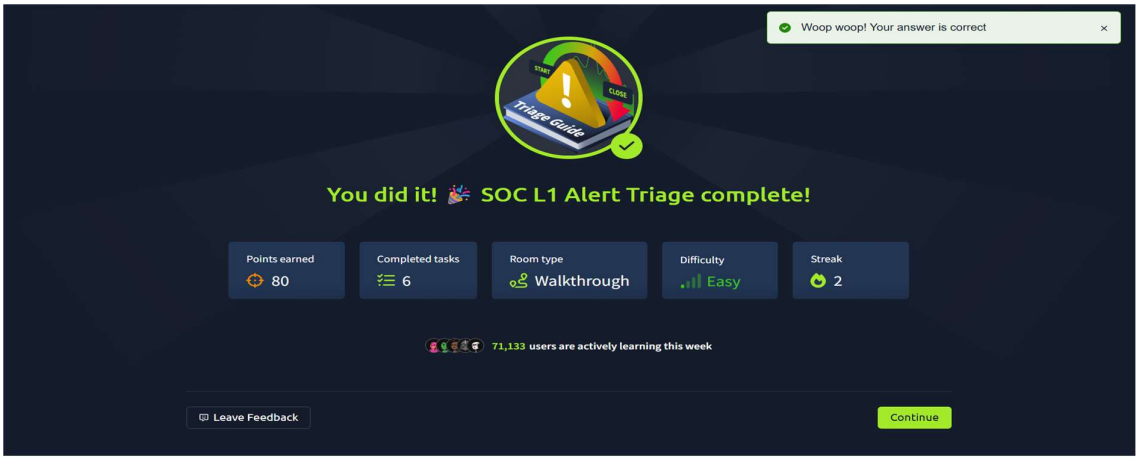
DAY – 02



✅ Just completed the TryHackMe “SOC L1 Alert Triage” room!

- **What it teaches**: How SOC Level 1 analysts handle alerts from generation to resolution.
- **Alerts**: Suspicious activities detected by SIEM/EDR/NDR tools.
- **Roles**:
  - **L1 Analyst** → first responder, triages alerts.
  - **L2 Analyst** → deeper investigation.
  - **Engineers** → configure alerts.
  - **Manager** → oversees triage quality.
- **Triage process**:

1. Filter alerts → new & unresolved only.
2. Prioritise → severity first (critical → low), then by time.
3. Investigate → check alert details, logs, threat intel.



4. Action → mark false positive or escalate.

- **Hands-on**: Practice with simulated alerts like phishing, unusual logins, data exfiltration, and usage.

👉 In short: It builds **practical triage skills** for L1 SOC Analysts—**prioritise, investigate, decide, escalate**.