HACKTHEBOX

30-60-90 Day SOC Analyst onboarding checklist

Days 0–30
Foundations and familiarization

- □ **Focus:** Understand SOC ecosystem & technical basics
- □ **Goals:**
    - □ Get familiar with SOC workflows and tools
    - □ Learn triage, detection, escalation basics
- □ **HTB Academy Modules:**
    - □ Security Monitoring & SIEM Fundamentals
    - □ Intro to Network Traffic Analysis
    - □ Working with IDS/IPS
- □ **Labs:**
    - □ Meerkat
    - □ Blue Team Fundamentals (BFT)
- □ **On-the-job:**
    - □ Shadow triage shifts
    - □ Review dashboards & ticket workflows
    - □ Weekly 1:1 with mentor/manager
- □ **Milestones:**
    - □ Completes orientation and first modules
    - □ Begins low-priority triage
    - □ Shows tooling familiarity

Days 31–60
Practice and situational awareness

- □ **Focus:** Build confidence with tools, start independent response
- □ **Goals:**
  - □ Handle alerts with less guidance
  - □ Detect anomalies & correlate data
  - □ Join threat hunts or mock incidents
- □ **HTB Academy Modules:**
  - □ Intermediate Network Traffic Analysis
  - □ Windows Event Logs & Finding Evil
  - □ YARA & Sigma for SOC Analysts
- □ **Labs:**
  - □ Exitiablis
  - □ Pulse
  - □ GroundZero
- □ **On-the-job:**
  - □ Resolve real alerts
  - □ Suggest tuning/detections
  - □ Participate in incident retrospectives
- □ **Milestones:**
  - □ Completes intermediate modules
  - □ Resolves alerts confidently
  - □ Joins post-incident reviews

Days 61–90
Autonomy and progression

- □ **Focus:** Trusted analyst with ownership & leadership
- □ **Goals:**
  - □ Own a security domain (EDR, threat intel, etc.)
  - □ Complete deep-dive labs
  - □ Draft 6-month development plan
- □ **HTB Academy Modules:**
  - □ Windows Attacks & Defense
  - □ Introduction to Digital Forensics
  - □ Detecting Windows Attacks with Splunk
- □ **Labs:**
  - □ HorsePanda-D
  - □ Superset-D
  - □ Ore
- □ **On-the-job:**
  - □ Lead mock incidents or training
  - □ Propose alert logic or automation
  - □ Mentor new analysts
- □ **Milestones:**
  - □ Completes onboarding plan
  - □ Shows independent analysis
  - □ Has clear growth plan

Bonus tips for managers:

- □ Set clear expectations and milestones
- □ Use hands-on labs for real-world experience
- □ Track progress transparently
- □ Encourage cross-team communication
- □ Leverage HTB reporting features to identify gaps