HACKTHEBOX

30-60-90 Day SOC Analyst onboarding checklist

Days 0–30

Foundations and familiarization

□ **Focus:** Understand the SOC ecosystem, tools, and workflows while building core defensive fundamentals and learning what meaningful signals look like in practice.

□ **Goals:**
- □ Get oriented with SOC processes, tooling, and team workflows
- □ Learn the fundamentals of alert triage, detection, and escalation
- □ Begin hands-on defensive learning tied to real SOC activity

□ **HTB Academy Content:**
- □ Security Monitoring & SIEM Fundamentals
- □ Intro to Network Traffic Analysis
- □ Working with IDS/IPS

□ **Defensive Labs:**
- □ Meerkat
- □ Blue Team Fundamentals (BFT)

□ **On-the-job activities:**
- □ Assigned onboarding buddy or mentor
- □ Shadow live alert triage and investigations
- □ Attend regular 1:1 check-ins
- □ Review dashboards, alert queues, and ticket workflows
- □ Begin distinguishing high-signal alerts from background noise

□ **Milestones:**
- □ Completes orientation and foundational Academy modules
- □ Demonstrates familiarity with SOC tools and workflows
- □ Begins contributing to low-priority alert triage
- □ Understands escalation paths and response expectations

Days 31–60
Practice and situational awareness

□ **Focus:** Build confidence using SOC tools and processes while transitioning from guided learning to independent analysis and response.

□ **Goals:**
- □ Handle alerts with minimal guidance
- □ Detect anomalies and correlate data across sources
- □ Participate in mock incidents or threat-hunting activities
- □ Understand how detection and triage decisions impact response outcomes

□ **HTB Academy Content:**
- □ Network Traffic Analysis
- □ Detection Engineering
- □ Windows Logging Fundamentals
- □ YARA & Sigma for SOC Analysts

□ **Defensive Labs:**
- □ Exitiabilis
- □ Pulse
- □ GroundZero

□ **Threat Range:** Participate in realistic defensive scenarios to assess:
- □ Investigation depth and prioritization
- □ Decision-making under pressure
- □ Communication and collaboration
- □ Tool and process confidence

□ **On-the-job activities:**
- □ Resolve real alerts using internal playbooks
- □ Submit detection or tuning suggestions
- □ Participate in incident retrospectives or threat hunts

□ **Milestones:**
- □ Completes intermediate Academy modules
- □ Confidently manages alert queues
- □ Contributes to post-incident reviews
- □ Completes first Threat Range benchmark

Days 61–90
Autonomy and progression

□ **Focus:** Take end-to-end ownership of investigations and demonstrate readiness for long-term contribution and growth.

□ **Goals:**
- □ Own investigations from detection through response
- □ Take responsibility for a security domain (EDR, threat intel, log tuning, etc.)
- □ Complete advanced labs or full attack-chain simulations
- □ Demonstrate consistent, high-quality decision-making

□ **HTB Academy Content:**
- □ Threat Hunting
- □ YARA Rules
- □ Malware Traffic Analysis

□ **Defensive Labs:**
- □ HorsePanda-D
- □ Superset-D
- □ Ore

□ **Threat Range:**
- □ Defend against full scenarios testing detection quality, escalation accuracy, and response speed
- □ Where possible, scenarios aligned to the organization's tooling stack

□ **On-the-job activities:**
- □ Lead a mock incident or create internal training material
- □ Propose new alert logic or automation ideas
- □ Support or mentor incoming analysts

□ **Milestones:**
- □ Completes full onboarding plan
- □ Completes Threat Range readiness scenario
- □ Demonstrates independent, end-to-end analysis
- □ Defines next six-month development goals with manager (certification or skill milestone)

Bonus tips for managers

□ Set clear expectations tied to 30–60–90 milestones
□ Use hands-on labs and Threat Range to validate real-world readiness
□ Track progress transparently and benchmark consistently
□ Encourage collaboration and knowledge sharing
□ Use HTB reporting to identify skill gaps early