Interview Analysis Report

Position: SOC Analyst
Candidate: Mark

Overall Score
72/100

Summary

- Solid Tier 1 SOC experience with demonstrated hands-on incident response and alert triage capabilities.
- Proficient with relevant tools (Splunk, CrowdStrike, Sentinel, Defender) and shows methodical investigative approach.
- Clear career trajectory and self-awareness about skill gaps; actively pursuing Security+ certification.
- Lacks formal certifications and advanced technical skills (scripting/automation) that would strengthen candidacy.

Strengths

- Strong investigative mindset with ability to correlate data across multiple platforms and reach root cause.
- Excellent documentation practices and communication skills; comfortable escalating and collaborating cross-functionally.
- Concrete incident example demonstrates structured thinking and follow-through on compromised credential scenario.
- Clear understanding of SOC triage workflow and structured approach to alert validation.
- Motivated and self-directed; articulates realistic career progression goals (Tier 2, Threat Hunter).

Risks/Concerns

- No current certifications; Security+ is in progress but not yet completed.
- Limited scripting/automation skills acknowledged; Python and "Parsha" (unclear reference) mentioned but not demonstrated.
- Tier 1 experience only; no evidence of advanced threat hunting or complex incident response.
- Vague on specific tuning achievements and detection engineering contributions.
- Some repetition and filler language in responses suggests possible nervousness or lack of polish.

Recommendation

Mark is a competent Tier 1 candidate with solid fundamentals and good soft skills, suitable for SOC Analyst roles. Recommend conditional offer pending Security+ completion within 90 days, or proceed if internal development pipeline is priority.

Suggested Next-Step Questions

- Walk us through a false positive you identified and how you worked with the detection engineering team to tune the rule.

- Describe your experience with Python scripting?have you written any scripts to automate alert triage or log parsing?

- What is your timeline for completing Security+, and do you have experience with any other security frameworks (MITRE ATT&CK;, threat intelligence)?