SOC Analysts Interview Qs. Round 2

A. Participant Context

1. Please briefly describe your role, work experience, and area of focus.
2. Where are you located (time zone-wise), and what type of organization do you work with (e.g., enterprise, government, startup, MSSP)?

B. Alert Triage & Prioritization

3. Can you walk me through your typical workflow after receiving a security alert?
4. What tools or data sources do you rely on to determine whether an alert is a true positive?
5. How do you decide which alerts to prioritize when multiple come in at once?
6. How do you currently correlate information from different platforms? Aggregate it and use it?
7. What information do you wish were more easily available to help you make those decisions?

C. Explainability Needs

7. What kind of explanation would make you feel more confident in acting on an AI-generated alert?
8. Do you find confidence scores, feature contributions, or attack attribution helpful? Why or why not?
9. What formats are most helpful for explanations? (e.g., short text, visual timelines, confidence heatmaps)

D. Prototype or Product Feedback (if applicable)

10. Based on the dashboard you saw (or based on the description), what stands out as most useful?
11. What would you change or add to make it more aligned with your workflow?
12. Was there anything that felt unclear, redundant, or overwhelming?

E. Root Cause & Post-Incident Learning

13. During root cause analysis, what are your must-have insights?
14. How do you currently document lessons learned and improve future detection?
15. How could explainability features support that post-incident process?