QA Definition for SOC Analysts (L1, L2, L3)

QA Definition			
QA Points	**L1**	**L2**	**L3**
1. Accuracy	5 points to follow predefined playbooks accurately; identification of deviations and appropriate escalation. If anyone of above is miising will lead to fewer and so as 0 points.	5 points to apply playbooks with flexibility; adaptation of steps based on context and required improvements suggestion. If anyone of the above is falling back, this will lead to fewer and so as 0 points.	5 for adequated desigining, review and optimization of playbooks. They need to ensure that they should be aligned with trending threat landscapes and current business needs. If anyone of the above is falling back, this will lead to fewer and so as 0 points.
2. Analytical Thinking, Choices & Complexity	5 points when analyst recognises basic patterns in any alert and can distinguish false positives. If anyone of above is miising will lead to fewer and so as 0 points.	5 points where analyst can correlate multi-source data, can make informed decisions under pressure and can handle alerts with moderate complexity. If anyone of above is miising will lead to fewer and so as 0 points.	5 points where analyst can solve complex, ambiguous problems for triggered alerts, can conduct root cause analysis and leads threat hunting initiatives. If anyone of above is miising will lead to fewer and so as 0 points.
3. Documentation	5 points to Log alerts and triage steps clearly and consistently. In case of missing of any artefact or logs will lead to 1 and so as to 0 points.	5 points for producing detailed incident reports with timelines, impact, and response actions. In case of missing of any artefact or logs will lead to 1 and so as to 0 points.	5 points for delivering executive summaries, threat intelligence briefs, and post-incident reviews. In case of incorrect or unformatted reports will lead to 1 and so as to depending on quality as 0 points.

4. Communication & Teamwork	5 points where L1s are able to Communicate clearly with L2 and can follow escalation protocols adequately. in case of missing the timeline or unnecessary escalation will lead to 1 points and sa as to 0.	5 points where L2s are able to coordinate clearly with L1 and L3, can communicate their findings effectively to stakeholders. In case of any communication gap will lead to 1 and so as to 0 points.	5 points where L3s are ablt to lead cross-functional teams during incidents and can mentor junior analysts when and wherevere required. in case of any communication gap will lead to 1 point and so as to 0 points.
5. Mistakes	Mistakes are expected; focus on learning and avoiding repetition. In case same mistake repitation will lead to 0 marks.	Fewer mistakes; expected to identify and correct L1 errors. In case same mistake repitation will lead to 0 marks. Failure to identify L1s mistake will also lead to 1 and so as to 0 points basis of severity of mistake.	Rare mistakes; responsible for systemic improvements and root cause analysis. Basis of mistakes severity, 0 for more, 1 for less and 2 for no mistakes can be added.
6. Growth Scale, Adaptability & Continuous Learning	5 for eagerness to learn and adaptation towards feedback and new tools. Less points for negative behavior towards responsibilities.	5 points for adaptation towards evolving threats and technologies. Less points for not updated knowledge.	5 points for new innovation and contribution to training and knowledge sharing. Less points for absence of any of above.
7. Procedure	5 points for suggestion of minor improvements to triage steps or alert tuning. Less points if failed to identify any.	5 points for recommendation of tuning of detection rules and playbooks adequately. less points for less tuning suggestions or failed to identify any.	10 points to propose new detection usecases and threat models. less points if failed to identify any.

8. Metrics	5 points for following accurate alert acknowledgment time and SLA adherence. In case of any miss to this timing will lead to 1 and so as to 0 points.	5 points for following accurate Mean time to investigate (MTTI), accurate escalation and follow accurate incident resolution time. In case of any miss to this timing will lead to 1 and so as to 0 points.	5 points to follow threat detection coverage, threat hunting success rate, new playbook creation, new usecases creation. In case of identification of any will lead to less points.