Evaluator Scoring Rubric: Credential Leakage

Domain	Sub-Metric	Score = 0	Score = 1	Score = 3	Score = 4	Score = 5
Procedural Alignment	Escalation path followed	No escalation occurred	Delayed or unstructured escalation	Escalation occurred but lacked clear routing	Mostly followed escalation path	Prompt and structured escalation as per IRP
	IRP referenced during incident	IRP not referenced	IRP checked late	IRP referred but not consistently followed	Referenced and mostly applied	IRP used as central guide throughout
	Deviations justified	No explanation for deviation	Ad hoc justifications	Some documented rationale post-event	Deviations justified at time of action	Justified and recorded deviations throughout
Operational Execution	Containment-action timing	No action taken	Containment delayed >30 minutes	Containment within 15â€“30 mins	10-15 mins response	Immediate containment within 10 mins
	Task coverage	Only reset account or blocked IP	Partially addressed vectors (e.g., session tokens missed)	Most credential vectors addressed	Nearly all vectors, minor gaps	All accounts, sessions, tokens addressed
	Execution accuracy	Actions led to service disruption or failure	Frequent procedural errors	Mostly correct with minor errors	Accurate and effective with oversight	Flawless execution of all response actions
Infrastructure Integration	Tool-usage effectiveness	Tools not used or improperly configured	Used alerting but no actionable data	Alerts used reactively	Tools used well for triage and response	Tools actively informed decision-making
	Tool alignment to IRP	Tools unlisted in IRP used	Used tools inconsistent with playbook	Partially aligned	Mostly aligned to procedures	Fully mapped to IRP playbooks
	Inter-tool visibility	No visibility between systems	Alerts/logs scattered or incomplete	Partial view across relevant systems	Good but minor gaps in integration	Full correlation across SIEM/IDP/EDR
Coordination & Communication	Role clarity	No one owned response actions	Unclear responsibility for account containment	Roles mostly understood	Roles followed with 1-2 lapses	Clear accountability and communication flow
	Decision flow	No structured decisions made	Conflicting or delayed decisions	Mostly sequential decisions	Decisions timely with some gaps	Rapid, structured decision-making
	Communication logging	No record kept	Unstructured or incomplete logs	Key actions logged manually	Most communication documented	All relevant communications logged
Post-Incident Follow-through	Root-cause analysis	No RCA performed	Surface analysis only (e.g., 'weak password')	Basic technical root cause	RCA included procedural gaps	RCA included access hygiene + supply chain
	Lessons learned	None documented	Verbal recap only	Lessons noted but no action plan	Lessons formalised, partially actioned	Documented, tracked, and embedded learnings
	IRP updated post-simulation	Not updated	Update discussed but no action	Draft or update in progress	Updated but not formally signed-off	Approved and distributed updated IRP