Evaluator Scoring Rubric: Insider Data Exfiltration

Domain	Sub-Metric	Score = 0	Score = 1	Score = 3	Score = 4	Score = 5
Procedural Alignment	Escalation path followed	No escalation occurred	Escalation too late or informal	Delayed but occurred	Mostly timely, slight delays	Prompt and formal escalation
	IRP referenced during incident	IRP not used	Referenced reactively	Inconsistently followed	Mostly followed, minor gaps	Fully followed throughout
	Deviations justified	No justification for deviations	Verbal/undocumented	Post-facto explanation	Justified with rationale	Fully documented justification
Operational Execution	Containment-action timing	No containment	Late containment (>30 mins)	15 to 30 mins delay	10 to 15 mins delay	Contained in <10 mins
	Task coverage	Minimal action taken	Major systems missed	Most systems addressed	Near-complete coverage	Full system coverage
	Execution accuracy	Errors caused harm	Frequent mistakes	Minor errors	Mostly accurate	Fully accurate execution
Infrastructure Integration	Tool-usage effectiveness	Not used or ineffective	Used reactively	Basic triage support	Effective with minor issues	Proactive and supportive
	Tool alignment to IRP	Not aligned	Tools outside IRP scope	Partially aligned	Mostly aligned	Fully aligned with IRP
	Inter-tool visibility	No correlation/logs	Fragmented visibility	Some correlation	Good with small gaps	Seamless integration
Coordination & Communication	Role clarity	Roles undefined	Unclear handoffs	Roles known, inconsistently applied	Mostly clear	Well-defined and executed
	Decision flow	Ad hoc or conflicting	Delayed or unclear	Structured but slow	Timely, minor overlaps	Fast and logical
	Communication logging	No records	Minimal/verbal	Manual log of actions	All major actions logged	Comprehensive and timestamped
Post-Incident Follow-through	Root-cause analysis	No RCA performed	Only technical symptoms	Basic cause identified	Behavioural + technical factors	Comprehensive multi-layered RCA
	Lessons learned	No reflection	Informal discussion	Noted, no action	Reviewed, partly implemented	Fully integrated lessons
	IRP updated post-simulation	No updates proposed	Discussed, not applied	Draft updates	Updated and shared	Versioned, approved, integrated