Evaluator Scoring Rubric: Phishing-led Ransomware Propagation

Domain	Sub-Metric	0 = Not Met	1 = Poorly Met	3 = Partially Met	4 = Mostly Met	5 = Fully Met
Procedural Alignment	Escalation path followed	No escalation occurred	Escalation happened too late or informally	Escalation took place, but lacked clarity or delay	Escalation mostly followed IRP, minor issues	Escalated promptly and formally as per IRP
	IRP referenced during incident	IRP not used at all	IRP was referenced only reactively or late	IRP was consulted, but inconsistently applied	IRP consulted early, mostly aligned to actions	IRP actively followed throughout
	Deviations justified	Major deviations with no explanation	Deviations explained verbally, not documented	Some deviations explained post-facto	Deviations justified with rationale	All deviations clearly documented
Operational Execution	Containment-action timing	No containment initiated	Containment initiated after major spread	Containment within 15–30 mins	Containment within 10–15 mins, minor delay	Containment within 10 minutes of detection
	Task coverage	Minimal actions taken; major gaps	Contained single endpoint only	Covered most systems but with gaps	Near complete coverage, small oversights	Full coverage across all relevant systems
	Execution accuracy	Errors caused misconfiguration/spread	Frequent mistakes in action	Mostly accurate with minor errors	Accurate execution with small oversights	All actions effective and error-free
Infrastructure Integration	Tool-usage effectiveness	Tools not used or misused	Used EDR/SIEM reactively with delay	Tools used reactively for triage	Effective use with minor config issues	Proactively used; real-time support of response
	Tool alignment to IRP	Tools used outside IRP scope	Used tools not specified in IRP	Partial alignment with IRP	Mostly aligned with IRP playbooks	Tools fully aligned with IRP tasks
	Inter-tool visibility	No correlation between tools/logs	Disconnected log sources	Some tool correlation, moderate gaps	Good visibility, minor integration gaps	Seamless, cross-platform event visibility
Coordination & Communication	Role clarity	No assigned roles, unclear responsibilities	Mixed understanding of roles	Roles defined but inconsistently followed	Mostly clear roles with some handover issues	Clear responsibilities, well-executed roles
	Decision flow	Ad hoc or contradictory decisions	Decision-making delayed or unclear	Mostly structured, some overlap	Well defined, responsive, small exceptions	Fully structured, fast and logical decisions
	Communication logging	No logs recorded	Only partial chat records or verbal only	Manual logs of key actions only	All major messages and handoffs logged	Complete and timestamped recordkeeping
Post-Incident Follow-through	Root-cause analysis	No analysis performed	Technical symptoms noted only	Technical root cause defined, no behavioural review	Root cause analysis included tech + team/process	Complete RCA covering root, contributors, context
	Lessons learned	No post-event reflection	Informal or undocumented takeaways	Notes written, no formal actions	Reviewed and partially implemented	Documented, reviewed, and integrated learnings
	IRP updated post-simulation	No changes proposed	Change discussed, not acted upon	IRP update drafted	IRP updated and circulated for feedback	IRP updated, approved, versioned and shared