Phishing-led Ransomware Propagation

Domain	Sub-metric	Weight (w_i)	Justification (Scenario-specific criticality)
Procedural Alignment	Escalation path followed	4	Prompt escalation critical for effective ransomware response
	IRP referenced during incident	4	Important for structured, efficient ransomware response
	Deviations justified	3	Allowance for justified deviations given scenario dynamics
Operational Execution	Containment-action timing	5	Immediate containment vital to limit spread and damage
	Task coverage	5	Broad endpoint containment critical
	Execution accuracy	5	Mistakes significantly escalate incident severity
Infrastructure Integration	Tool-usage effectiveness	4	Essential for rapid detection and containment
	Tool alignment to IRP	3	IRP-aligned tool usage enhances effectiveness
	Inter-tool visibility	3	Crucial for integrated and swift detection and response
Coordination & Communication	Role clarity	4	Important to maintain rapid, coordinated responses
	Decision flow	5	Quick and effective decisions essential
	Communication logging	4	Secondary importance; supportive of post-incident analysis
Post-incident Follow-through	Root-cause analysis	3	Essential for future incident prevention
	Lessons learned	3	Critical for continuous improvement
	IRP updated post-simulation	2	Important but less critical during immediate response

Weighted Total = 57