2.2 Investigation Steps Table (for SMB Incident)

Timestamp	Action
2025-11-20 14:00:00	Isolated Windows 10 endpoint
2025-11-20 14:30:00	Collected memory dump
2025-11-20 15:00:00	Reviewed Windows Security logs
2025-11-20 15:30:00	Checked failed SMB authentication
2025-11-20 16:00:00	Validated attacker IP