OnLINE Incident Management Academy

Level 1: Sprint 3: Incident Documentation

Rob Schnepp, Ron Vidal, Chris Hawley

TIME

Tone
Interaction
Management
Engagement

Mission Objectives

- IC/GL briefing
- Timelines
- Multiple workstreams
- Comm's practice
- Forward momentum
- Clarity
- Delegation

Scribe

- **Part of Command Staff**
  - Works for the Incident Commander
  - Works with the LNO

- **Key Tactics**
  - Actively engaged on Command Channel
  - Uses elapsed time for timestamps
  - Captures Key Events with timestamps
  - Not ”court reporting” or transcribing conversations
  - Tracks time contracts set by IC w/SMEs
  - Advises IC on upcoming time contract timelines
  - Provides LNO information for next briefing
  - Basis for the After Action Review (AAR)

Incident Scribing

Elapsed Time (mm:ss)	From - To	Key Event
00:00		Start of incident
00:15		IC opens incident Comms Command channel
00:27		IC appoints LNO & Scribe
00:39	IC=>All	What do we know so far?
00:48	LNO=>IC	Network alerts fired on main ISP links at 0912 UTC. Network dispatched.
01:16	Network=>IC	Network resource arrives on Command Channel
01:23	IC=>Network	What are you seeing?
01:35	Network=>All	Currently investigating, but we see main ISP links at 97% utilization
02:19	Security=>IC	Security resource arrives on Command Channel
03:01	IC=>Security	Status?
03:12	Security=>IC	Elevated traffic on ISP links, could be a DDoS attack, checking logs
03:45	IC=>All	**CAN Report #1 -** Current CONDITIONS: At 0912 UTC, network alerts fired on main ISP links at 97%. Network and Security resources are on the Command Channel. ACTIONS: Network and Security investigating, reviewing logs and change cases, running queries and opening tickets with vendors. NEEDS: LNO to prepare initial outbound Comms and schedule first briefing at 0930 UTC. Engage Applications team to run health checks and report to IC in 10 minutes at 0925 UTC.
05:01	LNO=>IC	Copy. Sending initial outbound Comms and links to first LNO Briefing

Capturing Pertinent Information

Questions
Data
Ideas
Clues
Statements
Needs
Actions
SOP

Signs
Countable
Observable by others
Described

Symptoms
Uncountable
Subjective
Described

Correlation
Context

Assumptions &
Working Hypothesis

Group Exercise #2

Mission Objective:

Plan a cross country trip from New York City to Austin, Texas. Starting point in New York is the Empire State Building. End point in Austin is Franklin BBQ restaurant at 900 E 11th Street.

Breakout Room details:

Assigned Roles: GL, LNO, Scribe, LKT.

GL: Drive the discussion and delegate tasks.

LNO: Provide briefing at the conclusion of the exercise (deliverables listed below).

Scribe: Capture details and key events of the discussion and deliverables and share details of the notes/timeline at the end of the briefing.

LKT: Monitor incoming notices via chat from lead instructor in main room.

NEEDS: *LNO reports back to the main group at the conclusion of breakout session.*

Questions and Wrap up