Incident Management Training for IT Operations

Tactical Documentation

Sprint 3

“If you don’t capture it – it never happened.”

Sprint 3 – What to Expect

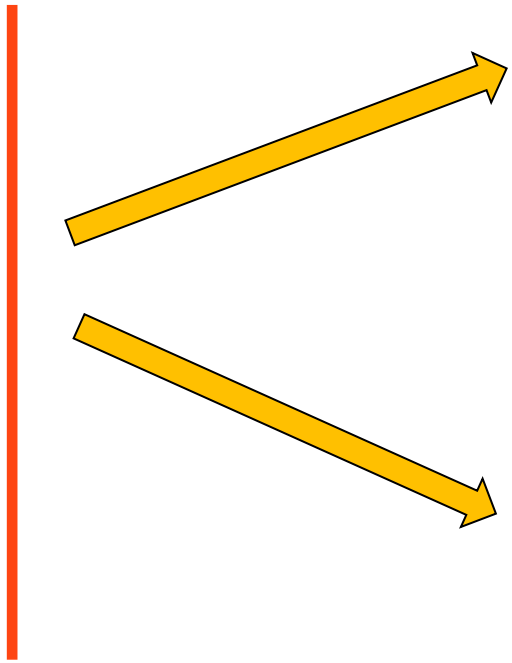
- ✔ **Presentation: Incident Documentation** – *importance of documentation; interacting with incident leadership and preparing for internal and external communications; capturing key events; time stamps; time contracts; documentation format*
- ✔ **Breakout Session 3:** Incident simulation and documentation exercise [*prepare for main session deliverables*]
- ✔ **Debrief and instructor feedback to participants**

Incident Documentation

			North Cascadia University Log4J Incident
			4/27/22
			14:10 PST START
		Resource	**Command Staff (CS)**
		Matt	**IC** = Incident Commander
		David	**LNO** = Liaison Officer
		Kevin	**S** = Scribe
			A-Reps & Problem Solvers
		Taylor	**SC** = School Contact
		Sonic	**SME** = Subject Matter Expert
	Elapsed		
Key	**Time**		
Event #	**(mm:ss)**	**From=>To**	**Key Event**
1	00:00		START: Log 4J Incident at N. Cascada Univ
2	00:21	IC=> All	Incident Bridge initiated @1410
3	00:30	IC=> All	Assigning CS positions
4	00:33	IC=> All	IC=Matt, LNO=David, S=Kevin
5	00:38	IC=> All	SC=Taylor, SME=Sonic
6	00:50	SC=>All	Log4J Attack, CAS, CIO upset
7	01:03	IC=> All	**CAN #1 - CONDITIONS:** Compromise detected at 13:57 pst at North Cascadia University. Central Authentication Server (CAS) compromised. CAS is the primary authentication service for all students. **ACTIONS:** Key roles filled and key stakeholders comtacted. Investigate nature of incidents. **NEEDS:** Collect & investigate logs. Determine next steps to protect CAS.
8	01:58	IC=>SME	Can you pull Logs? Yes
9	02:11	IC=>LNO	Add DCSIRT Log Analysis SME
10			**ADD 15 MINUTES FOR DRILL PURPOSES**
11	02;45	LNO=>IC	DCSIRT SME DeV wiLL join bridge
12	02:43	IC=>SME	Logs Avail? Yes
13	02:57	IC=>SME	Review logs & rejoin in 30min? Yes
14			**ADD 30 MINUTES FOR DRILL PURPOSES**
15	03:18	IC=>LNO	Get Business Impact in 30 minutes
16	03:48	IC=>LNO	School impact? No backup service
17	04:04	LNO=>IC	Business Impact is Major.No secondary option
18	04:10	IC=>SME	Update to log review? 10 Minutes
19	04:24		**ADD 10 MINUTES FOR DRILL PURPOSES**
20	04:30	SME=>IC	Taking system off line
21	04:48	IC=>SME	ETA to take server offline & patch

Incident Documentation & Communications

- **Questions**
- **Data**
- **Ideas**
- **Clues**
- **Statements**
- **Needs**
- **Actions**
- **SOP**



Signs
Quantifiable
Objective
Observable by others
Described

Symptoms
Non quantifiable
Subjective
Not observable by others
Described

Incident Documentation

Consider – Capture – Condense

Injects

- Investigation
- People
  - S/S
  - Customers
  - Key Players
  - CAN
  - LNO
  - Business Impact
  - Vendors

Context

Assembly
Severity
Investigation
Decision
Resolution
Conclusion
- Under Control
- All Clear

Relevance

- Description
- Explanation
- Solution
- Report
- Story
- Comment/Contribution

Documentation

- Entry
- Entry + Detail
- Timestamp
- *Tieback
- *Source

Parking Lot

Key Event

- Decision
- Timelines
- Tasking
- Deliverable
- Situational Awareness
- AAR

Incident Documentation

People

- Identify each participant by name and function

Conditions (Signs and Symptoms)

- Be specific and accurate
- Use precise numbers when known
- Write in bullet point format
- Don't capture technical jargon unless certain all will understand

Key Events

- Time: Start time, briefing times, elapsed time of the incident
- CAN Reports
- Briefing content and cadence
- Positive/negative state change
- Key decisions and logic
- Assigned tasks/work products
- Expected reactions to actions taken

Incident Management Training for IT Operations

Breakout Session 3

Small Group Exercise:

Cross Country Scenario

Overview:

Your group will be asked to plan a road trip across the U.S. using very specific parameters (trip length, start and end points, participant requirements, vehicle type, travel logistics, etc.) All parameters can be found in the **XC Scenario Briefing** on Sprint 3.

Purpose: Practice incident command and incident responder skills! Assume command, listen, lead, delegate, scribe, report, make decisions, monitor timeline, and all the other skills and techniques that go into minimizing MTTA and MTTR.

To start:

1. Access the full **XC Scenario Briefing (PDF download) and XC Scenario Worksheet** on Sprint 3: https://blackrock3onlinetraining.com/academy-resources/l1s3/
2. Go to your assigned Breakout Room and complete the exercise in the time prescribed.

Breakout Session:

Technology Scenario

Scenario Assumptions:

- Assume that incident resolution takes place in a virtual environment with a remote set of incident responders.
- Leader sets timezone.
- Any incident details not listed in the scenario overview may be filled in by the leader and/or other team members.

Breakout Room Assignments for Command Staff:

- **Leader:** Drive discussion and delegate tasks.
- **Communications:** Provide briefings as directed in exercise deliverables.
- **Tactical Documentation:** Capture details and key events of the discussion and deliverables listed in #3 and share details of notes/timeline at the end of the briefing.

Breakout Session:

Technology Scenario

Actions in Breakout Rooms:

- Leader appoints documentation and communication position
- Leader briefs the group on the scenario and integrates the information obtained by other team members.
- Leader guides the discussion to identify steps to scenario resolution including resolution plan A and plan B.
- Communications to outline a plan and written/verbal content for delivering internal and external communications.
- Unified Command (UC) is simulated during the exercise. Leader to keep track of time and dispatch Communications to UC [in the main room] at least two times during the exercise to provide updates on the resolution effort.

Breakout Session:

Technology Scenario

Minimum Deliverables:

- Identify severity level for the incident.
- Create a list of SMEs, vendors, faculty, administration, etc. that would be dispatched to the incident. Identify expected SLA for each team or individual dispatched.
- List any playbook(s) or procedure(s) the incident responders would follow or references for the listed scenario.
- List alternative technology platforms for incident resolution and incident communications (i.e., if teams or Everbridge are compromised or not available, how would the team pivot?)
- Draft overall Mission Objective(s) and resolution plan for the response. Provide an estimated time to resolve the proposed scenario.
- Leader to draft and deliver at least two sample CAN reports to the response team during the Breakout Room session.
- Identify any unique aspects or challenges of the response that may impede forward momentum of the resolution effort.
- List the potential audiences and briefing cadence that need to occur outside the resolution effort.
- List any major lessons learned [relative to the scenario] during the Breakout Room session.

Breakout Session:

Technology Scenario

Minimum deliverables in the main session at the conclusion of the exercise:

- The **Leader** will deliver a briefing on the scenario; detailed steps to resolution; and one example of a **CAN** report.
- **Communications** delivers an example of one briefing, using **IMS** briefing format, to the entire group in the Main Room session. The briefing can be related the beginning, middle or end of the incident.
- **Tactical Documentation** to share screen and describe the discussions/incident timelines; identify the key events; parking lot issues and/or other important items captured on the **timeline**.

Questions and Wrap up

IMS Functions