CONTROLLER HANDBOOK

Scenario 8: "Countdown"

Anonymous Threat — Logic Bomb Hunt — Time-Budget Investigation
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Duration: 2 Hours (including briefing and debrief)

Scope: Unique mechanic — time-budget investigation. Players choose actions from a menu, each costing scenario minutes. The clock ticks toward 12:00 PM when a logic bomb will detonate on the AODB server. The team must find and neutralize it before time runs out.

Why This Is Different: In all other scenarios, injects come TO the players on a schedule. In this scenario, the players drive the investigation. They choose what to look at. The facilitator is reactive, not proactive — handing out clue cards when requested. Forced events fire at fixed clock times to inject operational pressure, but the investigation itself is player-driven.

Exercise Objectives

- **Prioritization Under Pressure:** 305 minutes of possible actions, 180 minutes of clock. What do you do first? What do you skip?
- **Cyber Investigation Skills:** Can IT identify the attack vector (scheduled task + orphaned service account) from the available evidence?
- **Physical vs. Cyber Triage:** The email doesn't say "cyberattack." Do teams waste time on physical sweeps, or do they read the clues pointing to digital?
- **Contractor Off-Boarding:** The vulnerability was an orphaned service account. Do teams recognize this as a systemic failure?
- **Contingency Planning:** If you can't find the bomb, can you at least prepare for impact?

2. HOW TO RUN THE CLOCK

Setup

- Write a large clock on the whiteboard: **09:00**. Update it every time an action is taken.
- Below the clock, draw a line at **12:00** labeled "DEADLINE."
- Keep a running list of actions taken and their costs next to the clock.
- The visual pressure of watching the clock advance is half the exercise.

Pacing (Real Time vs. Scenario Time)

The scenario clock runs on action costs, not real time. In practice:

- Each action takes 2-4 minutes of REAL time to discuss, decide, and receive the clue card.

- But costs 10-30 minutes of SCENARIO time.
- A team that takes 8-10 actions will use about 130-180 scenario minutes and 30-40 real minutes.
- Forced events fire at scenario clock times (10:00, 10:30, 11:00, 11:30, 11:45, 12:00) — which means you deliver them when the clock reaches that point, regardless of real time.
- The investigation phase (0:10 to 1:30 real time) should feel fast and pressured.
- Reserve 20-30 minutes of real time for the debrief after the clock resolves.

When They Request an Action

1. Confirm the action: "You want to take A-06, Audit VPN Logs? That costs 10 minutes."
2. Advance the clock on the whiteboard.
3. Hand them the corresponding Clue Card from the deck.
4. Let them read it and discuss before they choose their next action.
5. If the advanced clock has passed a forced event time, deliver that event immediately.

When They Request a Custom Action

If the team wants to do something not on the menu — encourage it. Assign a time cost based on complexity (5-20 minutes) and provide an appropriate result. Examples:

- "Can we call NexGen Solutions and ask about Volkov?" — 10 minutes. Result: NexGen confirms Volkov's contract ended normally. They note he created a service account for the migration. They don't know it's still active.
- "Can we trace the external IP 73.189.22.104 from the VPN log?" — 10 minutes. Result: Residential ISP in the NCIA metro area. Could be anyone, but it's local.
- "Can we read the PowerShell script?" — 5 minutes (they need A-05 first). Result: AES-256 encryption targeting .mdf and .ldf database files. Writes ransom note. Deletes FIDS config. It's a logic bomb, not ransomware — no communication channel, no payment mechanism. This is revenge.

3. COMMON TEAM PATHS

Path A: The Speedrunners (Optimal)

A-06 (VPN) → A-14 (Interview) → A-05 (AODB Inspect) → Neutralize. 65 minutes. Clock at 10:05. These teams read the baseline info carefully, noticed the contractor mention, and went straight to VPN logs. They'll solve it with time to spare.

Path B: The Thorough Investigators (Common)

A-01 (Email trace, dead end) → A-04 (Firewall, useful) → A-07 (SIEM, slow) → A-06 (VPN, critical) → A-05 (AODB, critical) → Neutralize. About 85 minutes. Clock at 10:25. They wasted 15 minutes on the email trace and 20 on the SIEM review, but they got there. Still GOLD.

Path C: The Physical-First Team (Suboptimal)

A-09 (Terminal sweep, 20 min) → A-10 (Ramp sweep, 25 min) → A-13 (TSA call, 10 min) → then pivot to cyber. 55 minutes spent on physical actions yielding nothing. Clock at 09:55 before they start looking at the network. They can still solve it but they've burned a third of their time.

Path D: The Kitchen Sink (Worst Case)

Team tries to do everything. Full network scan (30 min), both physical sweeps (45 min), email trace (15 min). Clock hits 10:30 before they've looked at VPN logs or the AODB server. They're behind. The 11:00 checkpoint should refocus them. They may still get SILVER.

4. NEUTRALIZATION RULES

When the team says "we want to neutralize the threat," they must describe specifically what they're doing.

- **CORRECT:** "Delete the AODB_IndexMaintenance scheduled task and disable the svc_nexgen_aodb account." → THREAT NEUTRALIZED. Cost: 10 minutes. The logic bomb is disarmed.
- **PARTIAL:** "Delete the scheduled task." → Bomb disarmed, but the service account is still active. Volkov could reconnect and create a new task. Partial credit — SILVER at best.
- **PARTIAL:** "Take the AODB server offline." → Bomb can't fire, but AODB is down anyway — you've created the same outage the bomb would have caused. Technically a win, but a pyrrhic one.
- **WRONG:** "Block all external traffic." → Doesn't help. The scheduled task is local. It runs whether or not there's internet connectivity. Time wasted.
- **WRONG:** "Evacuate the terminal." → The threat is cyber, not physical. You've evacuated 3,000 passengers for nothing. Time and credibility wasted.

5. EVALUATION

Outcome	Criteria	Points
GOLD	Found the logic bomb AND properly neutralized it (deleted task + disabled account) before 12:00.	100
SILVER	Found the logic bomb but only partially neutralized (deleted task but not account, or took server offline) OR identified the threat but ran out of time.	75
BRONZE	Did not find the bomb but had strong contingency plans: backups taken, network isolation plan ready, communications drafted, CISA contacted.	50
FAIL	12:00 arrived with no identification and no contingency plan. AODB goes down. The team is caught flat-footed.	25

Bonus Points

- **+10:** Team identified Volkov by name before the reveal.
- **+10:** Team took A-18 (Emergency Backups) as insurance even while investigating.
- **+5:** Team requested a creative custom action that yielded useful results.
- **+5:** PIO had a contingency communication plan ready by 11:00.

END OF CONTROLLER HANDBOOK