MASTER SCENARIO EVENTS LIST & ANSWER KEY

Scenario 8: "Countdown" — Logic Bomb Hunt

North Coast International Airport (NCIA)
Duration: 2 Hours | Mechanic: Action Menu / Time Budget
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

THE FULL STORY

Who: Dmitri Volkov, 31, IT contractor from NexGen Solutions. He completed a 6-month AODB migration project at NCIA 4 weeks ago. His contract ended normally — no drama, no complaints. But Volkov was passed over for a full-time position he'd been informally promised by the Operations Director. When the job was posted externally instead, Volkov felt betrayed. He said nothing to anyone.

What he did: During the final week of his contract, while he still had legitimate admin access to the AODB server, Volkov planted a **logic bomb**: a PowerShell script disguised as a maintenance task called `AODB_IndexMaintenance.ps1`. It was registered as a Windows Scheduled Task set to trigger at exactly 12:00:00 PM on a date 4 weeks in the future — today. When it fires, the script will: (1) stop the AODB service, (2) encrypt the AODB database files with AES-256 using a key only Volkov has, (3) delete the FIDS data feed configuration, and (4) drop a ransom note on the server desktop: "You should have hired me. — D"

How he maintained access: Volkov's domain account was properly disabled during off-boarding. But he had also configured a secondary VPN profile using a service account (`svc_nexgen_aodb`) that was created during the migration for automated tasks. That service account was never disabled because it wasn't flagged as a contractor-personal account — it looked like a system service account. Volkov used this VPN access once, 5 days ago, to verify the scheduled task was still in place. Then he sent the email this morning from a coffee shop using ProtonMail.

What happens at 12:00 if not stopped: The AODB goes down. Every FIDS display in the airport goes blank. Gate management terminals lose flight data. Airlines can't see assignments. Baggage routing data disappears. The airport doesn't go dark — lights stay on, doors work, cameras record — but all flight operational data vanishes. It's an airport without a brain. Recovery from backup takes 4-6 hours minimum.

THE CRITICAL PATH — HOW TO SOLVE IT

Students don't need to find ALL clues. They need to find the right ones in the right order. Here is the critical path — the minimum set of actions that leads to the answer:

Step	Action	Cost	What They Learn	Running Clock
1	A-06: Audit VPN Logs	10 min	svc_nexgen_aodb connected via VPN 5 days ago from an external IP. That account should be inactive.	09:10
2	A-14: Interview IT Staff	15 min	Volkov created svc_nexgen_aodb. He had full admin on the AODB server. Contract ended 4 weeks ago. Was promised full-time job.	09:25

3	A-05: Inspect AODB Server	15 min	Scheduled task AODB_IndexMaintenance found. Trigger: 12:00 PM today. Runs PowerShell script. Created 4 weeks ago by svc_nexgen_aodb.	09:40
4	A-19: Search Scheduled Tasks	15 min	Confirms only one malicious task. No other servers affected. Attack is targeted at AODB only.	09:55
—	**NEUTRALIZE: Delete the scheduled task + disable svc_nexgen_aodb**	10 min	THREAT NEUTRALIZED. Clock shows 10:05. GOLD outcome — found and stopped with nearly 2 hours to spare.	**10:05**

Critical path total: 65 minutes. If the team follows the optimal path, they solve it with 115 minutes to spare. But they won't follow the optimal path — they'll chase dead ends, debate priorities, and spend time on physical sweeps that yield nothing. That's the design. The time pressure creates urgency and forces prioritization.

ALL 20 CLUE RESULTS — ANSWER KEY

When a team requests an action, hand them the corresponding Clue Card. Results are summarized here for quick reference. Mark each action as ★ (critical path), ■ (useful context), or ✗ (dead end).

ID	Action	Min	Rating	Result Summary
A-01	Trace Email	15	✗ DEAD END	ProtonMail. End-to-end encrypted. Headers show it passed through ProtonMail's servers in Switzerland. No origin IP exposed. Sender used Tor or VPN. Tracing is a dead end. However, the email was composed with a user-agent string showing Windows 11, Chrome 122, and the timezone header is UTC-5 (Eastern Time).
A-02	Scan Email Payload	10	■ USEFUL	No malware, no attachments, no tracking pixels. But: the email contains an invisible Unicode character sequence in the subject line "12:00" — specifically U+200B (zero-width space) between the digits. This is a common technique used by people familiar with email systems to bypass simple text-matching filters. Suggests the sender has technical sophistication.
A-03	Full Network Scan	30	✗ DEAD END (EXPENSIVE)	Scan completes after 30 minutes. No critical vulnerabilities found that weren't already known. All external-facing services are patched. One finding: the VPN concentrator has a stale service account profile (svc_nexgen_aodb) that wasn't cleaned up during off-boarding. But this information is also available faster through A-06 (VPN Audit) for 10 minutes. This scan was expensive for what it returned.
A-04	Firewall Logs	15	■ USEFUL	No anomalous inbound connections from external IPs in the last 7 days. No port scans. No brute force attempts. One notable entry: 5 days ago at 2:14 AM, an outbound connection from the AODB server (10.1.10.20) to 104.248.52.117 on port 443, duration 4 seconds. Single connection. Could be a check-in or heartbeat. The external IP resolves to a DigitalOcean VPS.
A-05	Inspect AODB Server	15	★ CRITICAL PATH	Server is healthy. All services running. BUT: Windows Task Scheduler contains a task named "AODB_IndexMaintenance" that was NOT created by the standard AODB installation. Task details: Trigger = 12:00:00 PM today. Action = Execute PowerShell script C:\AODB\Maintenance\AODB_IndexMaintenance.ps1. Created by: svc_nexgen_aodb. Created: 4 weeks ago. Last modified: 5 days ago (the VPN connection). The PowerShell script, when examined, contains AES-256 encryption routines targeting the AODB database files, FIDS configuration deletion, and writes a file to the desktop called README_NCIA.txt.
A-06	VPN Access Logs	10	★ CRITICAL PATH	VPN logs show all connections for the last 30 days. One stands out: service account svc_nexgen_aodb connected 5 days ago at 2:12 AM from external IP 73.189.22.104. Session duration: 6 minutes. That account was created by NexGen Solutions contractor Dmitri Volkov during the AODB migration project. Volkov's personal account (d.volkov) was disabled during off-boarding. The service account was not — it was categorized as a system account, not a user account.
A-07	SIEM 30-Day Review	20	■ USEFUL (SLOW)	1,247 alerts in 30 days. Most are routine. After filtering: 3 notable events. (1) The VPN login from svc_nexgen_aodb 5 days ago — flagged as INFO, not WARNING, because it's a "service account." (2) A PowerShell execution on the AODB server 4 weeks ago that created a new scheduled task — logged but not alerted because scheduled task creation by admin accounts is classified as routine. (3) The outbound connection to 104.248.52.117 from the AODB server. All three were logged. None were alerted. The SIEM rules didn't classify them as threats.
A-08	DNS Query Logs	10	✗ DEAD END	No suspicious domain lookups. No DGA patterns. No known C2 domains. The AODB server resolved 104.248.52.117 via a direct IP connection — no DNS lookup at all. Clean.
A-09	Physical Sweep — Terminal	20	✗ DEAD END	Nothing found. No suspicious packages. No unattended items. No unauthorized individuals. Terminal is normal. This action was expensive and yielded nothing — the threat is digital, not physical.
A-10	Physical Sweep — Ramp	25	✗ DEAD END	Nothing found. Ramp is clean. Cargo areas normal. ARFF station secure. Another 25 minutes spent confirming the threat is not physical.
A-11	CCTV — Key Areas	20	■ USEFUL	Server room camera shows no unauthorized physical access in 24 hours. Normal IT staff entries only. BUT: reviewing the server room footage from 4 weeks ago (the week Volkov's contract ended), you can see Volkov entering the server room at 11:47 PM — after hours — badging in with his still-active credential. He spent 22 minutes inside. This is when he planted the logic bomb.

ID	Action	Min	Rating	Result Summary
A-12	PACS After-Hours Audit	10	■ USEFUL	22 after-hours access events in the last 30 days. Most are Security and IT staff with legitimate reasons. One flag: d.volkov (Dmitri Volkov) badge accessed the server room at 11:47 PM, 27 days ago. His badge was deactivated 2 days later during off-boarding. This confirms physical access during the window when the task was created.
A-13	TSA/FBI Threat Check	10	✗ DEAD END	No specific threat advisories for NCIA. FBI is not aware of any credible threats. TSA threat level remains ELEVATED (Bravo) — baseline. No actionable intelligence. However, FBI says they'll open a file if you have a specific suspect.
A-14	Interview IT Staff	15	★ CRITICAL PATH	IT staff report: Dmitri Volkov was a NexGen Solutions contractor who ran the AODB migration. Technically brilliant. Quiet. Did excellent work. He created the service account svc_nexgen_aodb for automated AODB maintenance scripts. He was informally told by the Operations Director that a full-time IT position would be created for him after the project. That position was posted externally instead. Volkov said nothing but seemed... off... his last two weeks. IT staff also note: Volkov had full admin access to the AODB server, including the ability to create scheduled tasks and install scripts.
A-15	Network Isolation Plan	10	■ GOOD PLANNING	Team drafts a plan to isolate the Server VLAN from all other segments at a moment's notice. This doesn't find the threat but ensures rapid containment if the noon event is network-based. Smart contingency — earns partial credit even if they don't find the bomb.
A-16	Evacuation Prep	15	✗ LOW VALUE	Resources staged for a physical evacuation. But the threat is cyber, not physical. These 15 minutes could have been spent on digital investigation. Not worthless — contingency planning is never wasted — but low priority given the evidence.
A-17	CISA Contact	10	■ GOOD PLANNING	CISA acknowledges the report. They can provide remote forensic assistance within 2 hours — which means they won't arrive before noon. But they recommend: check for scheduled tasks on critical servers, audit service accounts, and look for persistence mechanisms. If the team hasn't already taken A-05 or A-19, this is a strong hint to do so.
A-18	Emergency Backups	20	★ SMART INSURANCE	Snapshot backups initiated for AODB, FIDS, PACS, and DC. This doesn't stop the bomb, but if the bomb goes off, recovery is 1-2 hours from fresh backup instead of 4-6 hours from the last nightly backup. This is the best "insurance" action.
A-19	Search Scheduled Tasks	15	★ CRITICAL PATH	Query returns scheduled tasks across all Windows servers. Most are legitimate: Windows Update, backup jobs, antivirus scans. ONE stands out: on the AODB server (AODB-SVR-01), a task named AODB_IndexMaintenance. Created by svc_nexgen_aodb, 4 weeks ago. Trigger: 12:00:00 PM TODAY. Action: PowerShell script. No other servers have suspicious tasks. Attack is targeted at AODB only.
A-20	Email Metadata Cross-Ref	10	■ USEFUL	Email header timezone: UTC-5 (Eastern Time — consistent with NCIA's timezone). User-agent: Windows 11, Chrome 122. Comparing with contractor records: Volkov's NCIA-issued laptop was Windows 11. His browser history (from the IT asset log before return) shows Chrome was his default browser. Not conclusive — millions of people use this config — but combined with other evidence, it fits.

FORCED EVENTS (AUTOMATIC — NOT ACTION-DEPENDENT)

These events fire at specific clock times regardless of what the team is doing. They inject urgency and operational pressure.

Clock	Event	Purpose
10:00	Airline Operations Manager calls: "We heard there's a security situation. Should we be worried? We have 8 departures between 11 and noon."	Forces Ops to communicate with airlines under uncertainty. Do they delay flights? Hold boarding? Or say nothing and hope?
10:30	Social media: a passenger overheard airport staff saying "something might happen at noon" and tweeted it. "@NCIAirport are we safe??" Getting traction.	PIO must manage. The information has leaked. What do you say?
11:00	Facilitator announces: "One hour remaining. The clock is at 11:00. What is your current theory? What have you found? What is your contingency plan if you don't find it in time?"	Checkpoint. Forces the team to synthesize what they know. If they haven't found the scheduled task yet, this is the last push to focus on cyber investigation.
11:30	TSA calls: "We're getting reports that NCIA has received a threat. Do we need to elevate the checkpoint? We can go to enhanced screening in 15 minutes but it will create 45-minute wait times."	Decision: elevated screening costs operational efficiency but demonstrates response. Is it warranted if the threat is cyber, not physical?
11:45	Facilitator: "Fifteen minutes. If you have identified the threat and want to neutralize it, this is your last opportunity. Describe what you're doing and how."	Final chance. If they've found the scheduled task, they delete it. If they haven't, they need to describe their contingency plan for when 12:00 hits.
12:00	IF NOT NEUTRALIZED: "The clock hits 12:00. The AODB server stops responding. FIDS displays across the airport go blank. Gate management terminals show 'NO DATA.' A file appears on the server desktop: 'You should have hired me. — D'" IF NEUTRALIZED: "The clock hits 12:00. Nothing happens. The team prevented the attack."	Resolution. Either celebration or crisis management begins.

DEBRIEF QUESTIONS

- **Time Management:** "How many minutes did you spend on dead ends? What would you have done differently?"
- **Prioritization:** "What made you choose your first action? Was it the right one?"
- **Physical vs. Cyber:** "If you swept the terminal, what told you to look there? What clues pointed to a digital threat instead?"
- **Service Accounts:** "svc_nexgen_aodb was never disabled because it looked like a system account. How many orphaned service accounts do you have in your real environment?"
- **Scheduled Tasks:** "A scheduled task sat on your AODB server for 4 weeks. Nobody noticed. Do you audit scheduled tasks? How often?"
- **Contractor Off-Boarding:** "Volkov's personal account was disabled. His service account was not. What does your off-boarding checklist look like for contractors who created system accounts?"
- **The Human Factor:** "Volkov was promised a job and didn't get it. He said nothing. He smiled on his last day. Then he planted a logic bomb. What could the organization have done differently?"

END OF MSEL / ANSWER KEY