CLUE CARDS DECK

Scenario 8: "Countdown"

North Coast International Airport (NCIA)

Print, cut, and keep face-down. Hand to teams when they request the corresponding action.

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE UNTIL REQUESTED

CONTROLLER DOCUMENT

CLUE CARD: A-01 Cost: 15 MIN | DEAD END

TRACE THE EMAIL

RESULT (Hand this card to the team):

The email was sent via ProtonMail — an end-to-end encrypted email service based in Switzerland. Email headers show it routed through ProtonMail's servers (185.70.40.x range). The sender used either Tor or a commercial VPN — no origin IP is exposed. Tracing the sender through the email infrastructure is a dead end. However, the email's MIME headers contain metadata: the email was composed on a system running Windows 11 with Chrome 122 as the mail client. The timezone header indicates UTC-5 (Eastern Time — the same timezone as NCIA). The sender is technically sophisticated (knows how to use encrypted email, used a taunting tone suggesting familiarity with the airport), and is likely in the local area.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

This costs 15 minutes and yields no direct lead. The metadata (Windows 11, Chrome, Eastern timezone) becomes useful later if the team takes A-20 (Cross-Reference), but on its own it's too generic.

CLUE CARD: A-02 Cost: 10 MIN | USEFUL

SCAN EMAIL FOR PAYLOADS

RESULT (Hand this card to the team):

No malware. No attachments. No tracking pixels. No embedded links. One technical finding: the subject line "12:00" contains invisible Unicode characters — specifically, U+200B (zero-width space) inserted between each digit: 1[ZWS]2[ZWS]:[ZWS]0[ZWS]0. This is a technique used to bypass simple keyword-matching email filters. It has no functional impact but indicates the sender understands email security filtering at a technical level. Assessment: the sender is not a random person making a hoax threat. They have technical knowledge of email systems.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

The zero-width space trick confirms technical sophistication. Combined with the ProtonMail usage and taunting tone, this points to someone with IT skills — not a passenger or disgruntled non-technical employee.

CLUE CARD: A-03 Cost: 30 MIN | DEAD END (EXPENSIVE)

FULL NETWORK VULNERABILITY SCAN

RESULT (Hand this card to the team):

Enterprise-wide scan completed across all VLANs. FINDINGS: - 3 systems with missing patches (low severity, non-exploitable from external) - 2 open ports that should be closed (TCP 8080 on a test server, TCP 5900 on an IT workstation) - 1 stale VPN service account profile: svc_nexgen_aodb — created 6 months ago, last authenticated 5 days ago, no disable date set No critical vulnerabilities. No evidence of active exploitation. No external-facing services are compromised. NOTE: The stale VPN account (svc_nexgen_aodb) is also discoverable through A-06 (VPN Audit) which costs only 10 minutes.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

This action costs 30 minutes — the most expensive on the menu — and its only useful finding (the stale VPN account) is available faster through A-06 for 10 minutes. Teams that take this first have burned a sixth of their total time.

CLUE CARD: A-04 Cost: 15 MIN | USEFUL

REVIEW FIREWALL LOGS

RESULT (Hand this card to the team):

Firewall logs for the last 7 days reviewed. No anomalous inbound connections from external sources. No port scans. No brute force attempts. ONE notable outbound entry: 5 days ago, 02:14:08 AM — the AODB server (10.1.10.20) initiated an outbound HTTPS connection to external IP 104.248.52.117 on port 443. Duration: 4 seconds. Bytes transferred: 1,247. Single connection — not repeated. The external IP resolves to a DigitalOcean VPS registered to a privacy-protected account. The 4-second, 1,247-byte transaction is consistent with a check-in beacon or heartbeat — a quick "I'm still here" message from a planted payload. The connection originated from the AODB server — not from any workstation.

■ CONTROLLER NOTE (Keep this — do not hand to team):

The outbound beacon from the AODB server is a strong clue. It tells IT: something on the AODB server called home 5 days ago. Combined with A-06 (VPN login also 5 days ago), this confirms the AODB server has been tampered with.

CLUE CARD: A-05 Cost: 15 MIN | ★ CRITICAL

INSPECT AODB SERVER

RESULT (Hand this card to the team):

Remote desktop session to AODB-SVR-01 (10.1.10.20). Server health: Normal. All services running. CPU and memory nominal. FINDINGS: Windows Task Scheduler contains a task named **AODB_IndexMaintenance**. - Created: 4 weeks ago (exact date matches Volkov's last week under contract) - Created by: svc_nexgen_aodb - Last modified: 5 days ago at 02:13 AM (matches VPN login timing) - Trigger: ONE TIME — 12:00:00 PM TODAY - Action: Execute PowerShell — C:\AODB\Maintenance\AODB_IndexMaintenance.ps1 The PowerShell script contains: - Stop-Service commands for the AODB and FIDS data feed services - AES-256 encryption routine targeting all .mdf and .ldf database files - Deletion of the FIDS XML feed configuration - Creates file C:\Users\Public\Desktop\README_NCIA.txt with content: "You should have hired me. — D" THIS IS THE LOGIC BOMB.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

THIS IS THE ANSWER. If the team takes this action, they've found the bomb. They now need to: (1) delete the scheduled task, (2) delete or quarantine the PowerShell script, and (3) disable svc_nexgen_aodb to prevent reconnection. All three = GOLD.

CLUE CARD: A-06 Cost: 10 MIN | ★ CRITICAL

AUDIT VPN ACCESS LOGS

RESULT (Hand this card to the team):

VPN access logs for the last 30 days: 247 total VPN sessions. All from recognized accounts except ONE: Account: svc_nexgen_aodb Connected: 5 days ago, 02:08 AM Disconnected: 5 days ago, 02:14 AM (6-minute session) Source IP: 73.189.22.104 (residential ISP, local metro area) Resources accessed: AODB-SVR-01 (10.1.10.20) via RDP This account was created by NexGen Solutions contractor Dmitri Volkov during the AODB migration project. It was classified as a "service account" for automated maintenance tasks. During off-boarding, Volkov's personal account (d.volkov) was disabled. This service account was not disabled because it was categorized as a system account in Active Directory, not as a contractor-personal account. svc_nexgen_aodb is currently ACTIVE in Active Directory with VPN access.

■ CONTROLLER NOTE (Keep this — do not hand to team):

This is the first critical path clue. It identifies the orphaned service account AND the fact that someone used it 5 days ago to access the AODB server. At 10 minutes, it's the cheapest critical clue. Teams that start here are on the optimal path.

CLUE CARD: A-07 Cost: 20 MIN | USEFUL (SLOW)

SIEM 30-DAY REVIEW

RESULT (Hand this card to the team):

1,247 alerts in 30 days. After filtering to HIGH and CRITICAL: 3 relevant events: 1. VPN authentication — svc_nexgen_aodb — 5 days ago, 02:08 AM. Classified as INFO (service account login). No alert triggered. 2. PowerShell execution on AODB-SVR-01 — 4 weeks ago, 11:52 PM. New scheduled task created via PowerShell. Classified as INFO (admin action by service account). No alert triggered. 3. Outbound connection from AODB-SVR-01 to 104.248.52.117 — 5 days ago, 02:14 AM. Classified as LOW (single HTTPS connection to unknown external IP). No alert triggered because single connections don't meet the threshold. All three events were LOGGED but NOT ALERTED. The SIEM rules classified service account activity and single outbound connections as low-priority. The evidence was there — but nobody was looking.

■ CONTROLLER NOTE (Keep this — do not hand to team):

This action takes 20 minutes and confirms what A-06 and A-04 already reveal faster. The key lesson: the SIEM had the data. It just didn't flag it. This is a strong post-exercise discussion point about SIEM tuning and alert fatigue.

CLUE CARD: A-08 Cost: 10 MIN | DEAD END

DNS QUERY LOG ANALYSIS

RESULT (Hand this card to the team):

DNS query logs reviewed for the last 30 days. No suspicious domain lookups. No domain generation algorithm (DGA) patterns. No queries to known command-and-control domains. No data exfiltration patterns. The AODB server's outbound connection to 104.248.52.117 was made via direct IP — no DNS lookup was performed. The script uses a hardcoded IP address, not a domain name. DNS analysis is clean.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

Dead end. The attacker used a hardcoded IP, bypassing DNS entirely. This is technically realistic — sophisticated attackers often avoid DNS to evade exactly this kind of monitoring.

CLUE CARD: A-09 Cost: 20 MIN | DEAD END

PHYSICAL SWEEP — TERMINAL

RESULT (Hand this card to the team):

Security teams swept all public and non-public areas of the terminal. No suspicious packages. No unattended items. No unauthorized individuals identified. All doors secured. All access points normal. TSA checkpoint operating normally with no concerns. The terminal is clean. The threat does not appear to be physical.

■ CONTROLLER NOTE (Keep this — do not hand to team):

20 minutes spent confirming what the evidence already suggested: the threat is digital. The email was sent to the IT support address, not the general tip line. The sender taunted with technical confidence. Physical sweeps are understandable but low-priority.

CLUE CARD: A-10 Cost: 25 MIN | DEAD END

PHYSICAL SWEEP — RAMP

RESULT (Hand this card to the team):

Ramp, cargo, baggage makeup, and ARFF station swept. Nothing found. All areas normal. No unauthorized vehicles. No suspicious cargo. ARFF station secured. Fuel farm normal. The airside is clean.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

25 minutes — the second most expensive action — for nothing. If a team takes both A-09 and A-10, they've spent 45 minutes (25% of their budget) on physical sweeps that yield zero. This is the cost of not reading the clues.

CLUE CARD: A-11 Cost: 20 MIN | USEFUL

CCTV — KEY AREAS (24 HRS)

RESULT (Hand this card to the team):

CCTV review of server room, IDF closets, and electrical rooms for the last 24 hours: No unauthorized physical access in the last 24 hours. All entries are recognized IT staff. EXTENDED REVIEW (4 weeks): At the facilitator's suggestion, footage from 27 days ago was reviewed. At 11:47 PM, Dmitri Volkov is seen badging into the server room using his still-active credential. He spends 22 minutes inside. He is carrying a laptop. This is the session when he planted the logic bomb. His badge was deactivated 2 days after this access.

■ CONTROLLER NOTE (Keep this — do not hand to team):

The 24-hour review is clean. The 4-week review shows Volkov. If the team specifically asks to look back further than 24 hours, reward them with the Volkov sighting. If they don't ask, give them the 24-hour clean result and move on.

CLUE CARD: A-12 Cost: 10 MIN | USEFUL

PACS AFTER-HOURS AUDIT

RESULT (Hand this card to the team):

After-hours access events (9 PM - 6 AM) for the last 30 days: 22 events total. 20 events are Security and IT staff with legitimate after-hours work. 1 flagged event: d.volkov — Server Room access at 11:47 PM, 27 days ago. Badge deactivated 2 days later during off-boarding. 1 unflagged event: j.kelley (IT Manager) — Server Room at 10:30 PM, 14 days ago. Legitimate after-hours maintenance (confirmed by change log). Volkov had after-hours physical access to the server room during his last week on contract.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

This confirms the physical access timeline. Volkov was in the server room after hours, right before his contract ended. Combined with A-06 (VPN) and A-05 (AODB inspect), the picture is complete: physical access to plant the bomb, VPN access 5 days ago to verify it.

CLUE CARD: A-13 Cost: 10 MIN | DEAD END

TSA/FBI THREAT CHECK

RESULT (Hand this card to the team):

TSA: No specific threat advisories for NCIA. Threat level remains ELEVATED (Bravo). No credible intelligence about planned attacks on airports in the region. FBI: No active investigations related to NCIA. No specific threats in their system. They recommend: report the email to IC3 and continue your internal investigation. If you develop a suspect, they'll open a case. No actionable external intelligence.

■ CONTROLLER NOTE (Keep this — do not hand to team):

Dead end for the investigation, but reasonable due diligence. The FBI offer to open a case if there's a suspect is useful later — once the team identifies Volkov, they should circle back.

CLUE CARD: A-14 Cost: 15 MIN | ★ CRITICAL

INTERVIEW IT STAFF

RESULT (Hand this card to the team):

IT staff report on Dmitri Volkov (NexGen Solutions contractor): "Dmitri was here for 6 months doing the AODB migration. Really good at his job. Quiet guy. He created the svc_nexgen_aodb service account for the automated maintenance scripts that run nightly on the AODB server. He had full admin access — domain admin equivalent on the AODB server specifically. Here's the thing nobody talks about: the Ops Director told Dmitri — informally, verbally — that there would be a full-time IT position for him when the project ended. Dmitri was counting on it. He even started apartment hunting. Then HR posted the position externally because policy requires it. Dmitri applied but... they hired someone else. An internal candidate. His last two weeks he was still professional, still did good work. But he was definitely hurt. He didn't say anything angry — that's what was weird. He just got quiet."

■ CONTROLLER NOTE (Keep this — do not hand to team):

This establishes motive AND confirms Volkov had the access and skills. The detail about the promised job is the human element — the anger that drove the logic bomb. "He just got quiet" should feel ominous.

CLUE CARD: A-15 Cost: 10 MIN | GOOD PLANNING

NETWORK ISOLATION PLAN

RESULT (Hand this card to the team):

Team has drafted a rapid network isolation plan: - Server VLAN 10 can be isolated from all other VLANs within 2 minutes by applying a pre-staged firewall rule. - AODB server can be individually isolated by disabling its switch port. - Plan is documented and ready to execute on command. This does not find the threat, but it prepares you to contain a network-based attack quickly.

■ CONTROLLER NOTE (Keep this — do not hand to team):

Smart contingency action. Even if they don't find the bomb, being ready to isolate demonstrates good incident response thinking. Award bonus points.

CLUE CARD: A-16 Cost: 15 MIN | LOW VALUE

EVACUATION PREP

RESULT (Hand this card to the team):

Terminal evacuation resources staged: - TSA notified of possible evacuation scenario - Airline ops alerted to hold boarding on request - PA announcement scripts drafted - Re-screening plan prepared (estimated 2.5 hours for full terminal) Evacuation resources are ready if needed, but all current evidence points to a digital threat, not a physical one.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

Not wrong — but 15 minutes spent on physical contingency when the threat is cyber. Low value relative to cyber investigation actions.

CLUE CARD: A-17 Cost: 10 MIN | GOOD PLANNING

CISA EMERGENCY CONTACT

RESULT (Hand this card to the team):

CISA 24/7 Operations Center contacted. Report filed. CISA response: "We've logged your report. We can have a remote incident response team available within 2 hours. In the meantime, our immediate recommendations: 1. Check all critical servers for scheduled tasks with imminent trigger times. 2. Audit service accounts — especially any created by contractors or third parties. 3. Look for persistence mechanisms: scheduled tasks, registry run keys, WMI subscriptions. 4. If you find a payload, preserve it for forensic analysis before deleting." CISA won't arrive before noon, but their recommendations are strong.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

CISA's recommendations are basically the answer key: check scheduled tasks, audit service accounts. If the team hasn't taken A-05 or A-19 yet, this should push them there. It's a $10 hint — well worth it.

CLUE CARD: A-18 Cost: 20 MIN | SMART INSURANCE

EMERGENCY BACKUPS

RESULT (Hand this card to the team):

Emergency snapshot backups initiated: - AODB server: backup in progress... complete. Snapshot stored on isolated backup NAS. - FIDS server: backup complete. - PACS database: backup complete. - Domain Controller: backup complete. If the noon event damages any of these systems, recovery from this fresh backup will take approximately 1-2 hours instead of 4-6 hours from the last nightly backup. This doesn't stop the threat, but it limits the damage.

■ CONTROLLER NOTE (Keep this — do not hand to team):

This is the best insurance action. 20 minutes is expensive, but if the bomb goes off, recovery is much faster. Teams that take this action AND find the bomb earn bonus points for thinking defensively while investigating.

CLUE CARD: A-19 Cost: 15 MIN | ★ CRITICAL

SEARCH SCHEDULED TASKS (ALL SERVERS)

RESULT (Hand this card to the team):

PowerShell query executed across all Windows servers: Get-ScheduledTask | Where-Object {$_.Date -gt (Get-Date).AddDays(-60)} Results across 8 servers: - DC-01: 2 tasks (Windows Update, backup) — legitimate - FIDS-SVR: 1 task (data feed refresh) — legitimate - PACS-SVR: 1 task (database maintenance) — legitimate - AODB-SVR-01: 3 tasks. Two legitimate (nightly backup, index optimization). ONE ANOMALOUS: **AODB_IndexMaintenance** — Created 4 weeks ago by svc_nexgen_aodb. Trigger: 12:00:00 PM TODAY. Action: PowerShell script. - All other servers: clean The attack is targeted at the AODB server only. No other servers are affected.

■ **CONTROLLER NOTE (Keep this — do not hand to team):**

If the team takes this before A-05, they find the bomb from a different angle — broad search instead of targeted inspection. Either path works. This also confirms there's only ONE bomb — no secondary devices on other servers.

CLUE CARD: A-20 Cost: 10 MIN | USEFUL

EMAIL METADATA CROSS-REFERENCE

RESULT (Hand this card to the team):

Email metadata from A-01 (if taken): Windows 11, Chrome 122, UTC-5 timezone. Cross-referencing with personnel and contractor records: - 127 NCIA employees use Windows 11 (too common to narrow) - Contractor IT asset records: Dmitri Volkov's NCIA-issued laptop was a Dell Latitude running Windows 11. Browser history log (captured before device return) shows Chrome 122 as default browser. - Volkov's home address is in the NCIA metro area (consistent with UTC-5). Not conclusive on its own — millions use this configuration. But it's consistent with the Volkov hypothesis if you already have one.

■ CONTROLLER NOTE (Keep this — do not hand to team):

This is a confirmation clue, not a discovery clue. It only matters if the team has already developed Volkov as a suspect. On its own, it's too generic. But in combination with A-06 and A-14, it adds another thread.

END OF CLUE CARDS DECK