MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 2: "The Long Game" — Advanced Persistent Threat

North Coast International Airport (NCIA)
Duration: 2 Hours | Target: Ops, IT/Cyber, PIO, Security/Legal
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: Long-term network compromise, strategic incident response, breach notification, trust in systems, and recovery planning when you don't know what you don't know.

The Threat: The "Meridian Collective" — an Eastern European cybercrime group — gained access to NCIA's network 90 days ago via a spear-phishing email to an HR coordinator. They used the initial foothold to move laterally to the Domain Controller and the AODB server. They have been quietly exfiltrating data via DNS tunneling ever since. The compromised Domain Controller gives them access to every credential in the organization.

What Was Taken (Full Scope — reveal gradually): Employee PII for all 340 NCIA staff (SSNs, addresses, salary). 90 days of flight operations data from the AODB (manifests, schedules, gate assignments). Active Directory password hashes for every account. PACS configuration data — door codes, access groups, camera maps. A copy of the Airport Security Program (ASP) stored on the file server.

Key Design Principle: Unlike Scenario 1, there is no single dramatic moment. The tension in this exercise comes from the slow, nauseating realization of how much damage has been done — and how few good options remain. Every inject peels back another layer.

PHASE 0: BRIEFING & ORIENTATION 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing Packet and Forensic Evidence Packet. Walk through the scenario setup. Emphasize: this is not a real-time attack. The attack happened months ago. You are making strategic decisions, not chasing an intruder.	Players review materials, form teams. IT team should study the forensic exhibits carefully.

PHASE 1: SCOPING THE DAMAGE 0:10 — 0:40

Goal: The team processes the initial forensic evidence and tries to understand how bad this is. Each inject reveals the compromise is deeper than they thought.

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	Marcus Chen (Sys Admin)	IT Team	Marcus presents his findings to the team (the Forensic Evidence Packet). "I found this during a routine DNS audit. The C2 domain is confirmed malicious. Three systems are beaconing to it. The earliest queries I can find go back 90 days. This isn't a script kiddie — this is organized."	IT team begins mapping the scope. Ops should ask: "What does this mean for the systems we're running right now?" First critical question: Is the attacker still active?
0:17	I-02	IT Team Analysis	All	IT reports (facilitator delivers if needed): "The Domain Controller is one of the compromised systems. That means the attacker has every username and password hash in the organization. Every account. Every admin credential. They can log into anything as anyone."	The team should realize this is not a localized breach — it's total compromise of the identity infrastructure. Do they reset all passwords immediately? If so, how — without the Domain Controller being trusted?
0:24	I-03	Marcus Chen	IT / Ops	"I checked the AODB server. There are traces of the database export utility (bcp.exe) running nightly for the past three months. Someone has been pulling full database dumps — flight data, gate assignments, airline schedules. And... I found queries that look like they pulled passenger name records. I don't know how many, but it could be every passenger who flew through NCIA in the last 90 days."	Ops should ask: how many passengers is that? (Answer: tens of thousands.) Legal/Compliance should start thinking about breach notification obligations. Does this include any sensitive flight info — federal air marshal movements? Military charters?
0:32	I-04	Security Team Review	All	Security team reports (facilitator delivers): "We pulled the file server access logs. The compromised service account (svc_update_04) accessed the S:\\Security drive 47 days ago. That drive contains the current Airport Security Program (ASP), the PACS configuration database, security camera placement maps, and the terminal vulnerability assessment from last year. If they downloaded that, they have a complete blueprint of our physical security."	CRITICAL: The ASP is SSI (Sensitive Security Information). Unauthorized disclosure must be reported to TSA. Security must assess whether physical security changes are needed immediately — door codes, camera positions, access group configurations.

PHASE 2: THE HARD QUESTIONS 0:40 — 1:15

Goal: Force the team to make strategic decisions with no clean answers. Every choice has a cost. The injects create pressure from all directions.

Time	ID	From	To	Event / Message	Expected Action
0:40	I-05	Marcus Chen	IT / Ops	"I checked the backup server. Bad news. The attacker's service account accessed the backup server 60 days ago. I can't tell if they planted anything in the backup images or just copied data off them. But it means I cannot guarantee that any backup taken in the last 60 days is clean. The last backup I would trust is from... 91 days ago. And that one only covers the file server — it doesn't include the AODB or the Domain Controller."	CRITICAL DECISION: Can they restore from backup? If the backups are compromised, restoring them re-introduces the attacker. Do they rebuild from scratch? That could take days or weeks. What do they run on in the meantime?
0:48	I-06	Phone Call	Ops / Security	TSA Regional Office calls: "This is Regional Director Harmon with TSA. We've received intelligence from DHS/CISA that data consistent with an airport security program appeared on infrastructure associated with a foreign threat actor. We need to know: has your ASP been compromised? If so, we need to initiate ASP revision procedures. This call is SSI — do not discuss with media."	Security/Legal must confirm the ASP was likely exfiltrated. TSA will want a timeline and a remediation plan. They may require immediate changes to physical security procedures. Students should discuss: what does it mean to revise an ASP on an emergency basis?
0:55	I-07	HR Dept	Ops / Legal	HR Director calls: "I just got an email from an employee — she says her Social Security number and home address are listed on some kind of hacker website. She's panicking. She wants to know what we're doing about it. And she's not the only one — two other employees just told me the same thing. How do I answer them? Are all 340 of our people exposed?"	The employee PII breach is now public (at least among staff). Legal must assess state breach notification laws — most require notification within 30-72 hours of discovery. Do they offer credit monitoring? Who writes the notification letter? PIO needs to prepare for this to leak externally.
1:02	I-08	Phone Call	Ops	The airport's airline affairs liaison reports: "I just got off the phone with Delta, United, and American. They want a joint call by end of day. They want to know if their operational data — flight schedules, crew rosters, passenger data — was exposed through NCIA's systems. Delta is threatening to disconnect from the AODB until they get assurances. If Delta disconnects, we lose real-time data for 40% of our flights."	Ops must manage the airline relationship. What can they honestly tell the airlines? If airlines disconnect from the AODB, FIDS goes manual. Back to whiteboards. How do you reassure a partner when you can't yet guarantee your own systems?
1:08	I-09	Phone Call	PIO	Reporter from the Tribune calls: "I'm working on a story. I have sources telling me NCIA has been the target of a major cyberattack and that employee personal data is being sold online. I'm running this at 5 PM tonight with or without your comment. Do you want to get ahead of it?"	PIO must decide: give a statement now and control the narrative, or decline and risk a hostile story. What can they say without confirming details they haven't verified? Do they coordinate with the airlines on messaging? With TSA?

PHASE 3: RECOVERY PLANNING & STRATEGIC DECISIONS

1:15 — 1:40

Goal: The team must now look forward. The damage is done — how do they recover? Force decisions about rebuilding infrastructure, accepting outside help, and long-term posture changes.

Time	ID	From	To	Event / Message	Expected Action
1:15	I-10	Phone Call	Ops / IT	DHS CISA (Cybersecurity & Infrastructure Security Agency) calls: "We can have a CISA Incident Response Team on-site within 24 hours. They will bring forensic tools, analysts, and threat intelligence. However — we will take lead on the investigation. Our team will have full access to your network, servers, and logs. We'll coordinate with the FBI for any criminal prosecution. Do you want our assistance?"	DECISION: Accept CISA help and give up some control, or handle it internally with limited resources? What does it mean for the airport's autonomy? For the speed of recovery? For the public perception ("the feds had to come bail us out")?
1:22	I-11	Facilitator	All	STRATEGIC PLANNING EXERCISE. The facilitator poses three scenarios and asks each team to take a position: OPTION A: "Scorched Earth" — Shut down all servers, rebuild every system from scratch using clean OS installs. Estimated time: 5-7 days. The airport runs on manual operations during the rebuild. OPTION B: "Surgical Strike" — Isolate and rebuild only the three confirmed compromised systems. Leave everything else running. Risk: other systems may be compromised and you don't know it. OPTION C: "Monitor & Contain" — Don't shut anything down. Instead, deploy monitoring tools on every system and watch for further attacker activity while building a parallel clean network. Risk: the attacker is still inside and may escalate if they realize they've been detected.	Each team argues for their preferred option. Ops makes the final call. There is no right answer — each option has real costs and real risks. The discussion IS the learning objective.
1:32	I-12	Facilitator	All	NOTIFICATION PLANNING. The facilitator asks the team to build a notification timeline: — Who do you notify first? Second? Third? — When do you notify employees about the PII breach? — When do you go public? — What do you tell the airlines? — What do you report to TSA about the ASP? — Do you notify passengers whose data may have been in the AODB? — Who writes the breach notification letter, and what does it say?	Team builds a prioritized notification plan. Legal/Compliance should drive this. PIO should be drafting actual statements. Ops should be thinking about timing — you don't want the press conference to happen while you're still rebuilding the Domain Controller.

PHASE 4: DEBRIEF / HOT WASH

1:40 — 2:00

Time	ID	From	To	Event / Message	Expected Action
1:40	END	Facilitator	All	ENDEX. Structured debrief — "3-Up / 3-Down" method, followed by key discussion questions: 1. When you read "90 days" — what was your first reaction? When did you realize how bad it was? 2. Which decision was the hardest — and what ultimately drove your choice? 3. What would you have done differently if you had detected this at Day 1 instead of Day 90? 4. What investments or policies would have prevented or shortened this compromise? 5. How did you handle the tension between "be transparent" and "don't panic everyone"?	Team reflects. Facilitator captures lessons learned. Exercise complete.

END OF MSEL