MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 1: "Glass House" — Insider Threat & Payment Card Breach

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

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: Insider Threat, Payment Card Industry (PCI) Data Security, Network Forensics, and the Ethics of Trust.

The Threat: The airport's own IT Manager (Jordan Kelley) has planted a rogue device on the network that performs a Man-in-the-Middle attack, intercepting unencrypted credit card data as it passes between the Retail/Vendor VLAN and the Internal Payment Processing Gateway. Kelley is being extorted by a criminal syndicate that has leveraged a personal financial vulnerability (substantial gambling debt). Kelley does not want to be doing this — but feels trapped.

The Operational Impact: Transaction processing slows dramatically as data is duplicated and rerouted through the rogue device. Some transactions fail entirely. Vendors lose revenue. Passengers are inconvenienced. Meanwhile, card numbers are being exfiltrated off-network via DNS tunneling.

The Twist: Throughout the exercise, the IT Manager is the most "helpful" person in the room — offering explanations, suggesting fixes, and subtly steering the investigation away from the real problem. The exercise tests whether the team can recognize that the person they trust most is the source of the threat.

PHASE 0: EXERCISE OVERVIEW & BRIEFING 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing Packets and Network Reference. Walk through the scenario setup. Assign the IT Manager role (Jordan Kelley) to a designated student or facilitator. Current sim time: 1:00 PM Wednesday.	Players review materials, form teams, ask clarifying questions. IT Manager player reads their secret briefing card.

PHASE 1: THE SLOW BURN 0:10 — 0:35

Goal: Establish the problem. Let the IT Manager steer the team toward false explanations. Build a false sense of "this is just a tech issue."

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	Vendor Mgr	Ops	Phone Call: "This is the SkyLounge manager. Our card readers have been crawling for about 20 minutes. Customers are walking out. Two duty-free shops on Concourse A say the same thing. Is there a system issue?"	Ops logs the complaint and contacts IT. Initial assumption: ISP or vendor equipment issue.
0:14	I-02	Jordan Kelley (IT Mgr)	Ops / IT Team	Jordan Kelley radios in: "Hey, I already heard about the POS slowdowns. I called our ISP — they're showing some latency on their end. Probably a routing issue upstream. I'd give it 30 minutes and it'll clear up. Also, the firmware on those Ingenico card readers is two versions behind. Could be that, too."	IT team may accept this at face value. Ops may relax. KEY: Kelley is deflecting early.
0:18	I-03	IT Helpdesk	IT Team	Ticket #3371: Network Technician Priya Deshmukh ran a routine sweep of VLAN 30 (Security Cameras) and found a device with an unrecognized MAC address (B8:27:EB:xx:xx:xx — a Raspberry Pi prefix). It's registered on the camera VLAN but is not a camera. She flagged it as "unknown — investigate."	IT should investigate the rogue device. This is the MitM tool. Kelley, if asked, will say it's "probably a test device someone left plugged in" and offer to "go pull it after we deal with the POS issue."
0:23	I-04	Pilot Report	IT Team	Forwarded email from airline ops: Two pilots using NCIA's crew Wi-Fi to update electronic flight bags received "Invalid SSL Certificate" warnings when connecting to an internal crew scheduling portal. They reported it to their airline IT, who forwarded it to NCIA.	IT should recognize SSL stripping as a sign of interception. Kelley will say: "Those tablets are ancient. Their certificate store is probably out of date. I'll push a cert update after hours."
0:28	I-05	Sys Admin (Marcus)	IT Team	Marcus Chen tries to pull transaction logs from the core switch for the last 48 hours. There is a 4-hour gap in the logs from last Tuesday (10 PM – 2 AM). The logs simply stop, then resume. No error message. No system reboot recorded.	IT should treat missing logs as highly suspicious. Kelley will say: "Yeah, I noticed that too. Probably a syslog buffer overflow. I'll open a ticket with the switch vendor."

PHASE 2: THE TRAIL OF BREADCRUMBS 0:35 — 1:15

Goal: The injects pile up. Each one, by itself, could be routine. Together, they form a pattern — and that pattern points to someone with admin-level access. The IT Manager gets increasingly nervous and starts making bolder moves.

Time	ID	From	To	Event / Message	Expected Action
0:35	I-06	HR Dept	Ops / Security	HR calls the AOC: "We're getting Account Locked notifications for six employees who aren't even at work today. Their Active Directory accounts are getting hit with failed password attempts. Is something going on?"	Security should investigate credential-spray activity. IT should check auth logs. Kelley has been testing stolen creds.
0:40	I-07	Maint. Dept	Ops	Maintenance radio call: "Hey Ops, the secondary server closet down by Concourse B — Room 217 — is running real hot. I walked by and the door was warm to the touch. That room is usually cool. Temp sensor? We don't have one in there."	Ops should send someone to check Room 217. The decommissioned server is running a data exfiltration script. Kelley will try to volunteer to "go check it myself."
0:46	I-08	Social Media	PIO	Tweet from @CLENewsNow: "DEVELOPING: Sources say a well-known celebrity's private flight details from NCIA were leaked online, including tail number and destination. Airport has not commented. #PrivacyFail"	PIO must address media inquiry. Reality: Kelley accidentally skimmed a charter manifest while searching for card data. Kelley will say: "Leaks like that come from airline staff, not our systems."
0:52	I-09	Baggage Office	IT Team / Ops	Phone call from the Baggage Handling admin office: "This is gonna sound weird, but I just watched my mouse cursor move on its own for about three seconds. Then it stopped. My screen flickered. Nobody is at my desk but me."	IT should investigate possible remote desktop intrusion on the BHS VLAN. Kelley was checking if the Baggage VLAN is unencrypted too.
0:58	I-10	Jordan Kelley (IT Mgr)	All Teams	Kelley makes an urgent announcement: "Team, I need to reboot the core switch. I just got an alert from the vendor — there's a critical firmware vulnerability and I need to patch it NOW before we're exposed. It'll take the network down for about 5 minutes."	CRITICAL DECISION: Students must decide whether to allow the reboot. Kelley is trying to wipe volatile memory on the rogue device. If they let him, forensic evidence disappears. This is the biggest test of the exercise.
1:05	I-11	Security Intel	Security / IT	Facilitator hands Security a printed dark-web forum screenshot: An anonymous post on a carding forum mentions NCIA's specific payment gateway model by name and says: "Fresh dump incoming. Airport batch. High-limit cards. 72 hours."	Security and IT must now treat this as a confirmed data breach in progress. Law enforcement notification (Secret Service / FBI) should be discussed.
1:10	I-12	Janitor / Maint.	Ops / Security	A custodian reports: "I was cleaning the Maintenance Hallway near Concourse B and the door to that little server room — 217 — was propped open with a rolled-up piece of duct tape. I didn't touch anything. Figured I should call it in."	Physical security breach at Room 217. Security should secure the room and log it as a potential crime scene. Only Kelley has the key to this room.

PHASE 3: THE CONFRONTATION 1:15 — 1:40

Goal: The team connects the dots — or the facilitator helps them get there. The IT Manager is revealed. The exercise shifts from technical investigation to incident response decision-making and ethics.

Time	ID	From	To	Event / Message	Expected Action
1:15	I-13	Facilitator (if needed)	All	If the team hasn't connected the pattern yet, the facilitator delivers a "nudge" inject: Marcus Chen (Sys Admin) approaches the group: "I've been cross-referencing the PACS logs with the network anomalies. Every event we've flagged today — the rogue device, the log gap, the hot server closet, Room 217 being propped open — all of them correlate with times when Jordan was the only IT staff on shift. I don't want to accuse anyone, but..."	The team must decide how to handle a suspected insider. Do they confront Kelley directly? Isolate Kelley from the systems? Contact law enforcement? Preserve evidence?
1:22	I-14	Facilitator	All	THE REVEAL: The facilitator stops the clock. "PAUSE EXERCISE." The facilitator explains the full scenario: Jordan Kelley planted a Raspberry Pi on the camera VLAN configured as a MitM bridge. It intercepted unencrypted payment data between the Retail VLAN and the Payment Gateway. The stolen card data was encrypted and tunneled out via DNS queries to an external C2 server using the legacy box in Room 217. Kelley was being extorted — a criminal syndicate had leverage over a personal financial situation — and felt there was no way out."	Team absorbs the reveal. Facilitator opens the floor for initial reactions.
1:28	I-15	Facilitator	All	GUIDED DISCUSSION — The facilitator walks the room through three key questions: 1. Why was Kelley the most "helpful" person during the crisis? What red flags did you miss because you trusted the expert? 2. What "Two-Person Integrity" rules could have prevented the log deletion and the Room 217 access gap? 3. How do you handle an incident when the person who runs the network IS the suspect? Who do you call? How do you preserve evidence?	Open discussion. Facilitator guides conversation toward insider threat controls, separation of duties, and PCI compliance.

PHASE 4: DEBRIEF / HOT WASH 1:40 — 2:00

Time	ID	From	To	Event / Message	Expected Action
1:40	END	Facilitator	All	ENDEX. Facilitator conducts structured debrief using the "3-Up / 3-Down" method: — Three things the team did well. — Three things that broke or were missed. Then: Open discussion on insider threat implications, PCI-DSS requirements, and airport-specific cybersecurity challenges.	Team reflects on performance. Facilitator captures lessons learned. Exercise complete.

END OF MSEL