MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 5: "Carbon Copy" — Badge Cloning & Physical-Cyber Convergence

North Coast International Airport (NCIA)
Duration: 2 Hours | IT/Cybersecurity Lead Scenario
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: Physical-cyber convergence. A cloned airport badge is used to access a network infrastructure room. The investigation requires PACS log analysis, CCTV correlation, RFID technology understanding, and physical inspection of compromised spaces. The puzzle has a specific answer the students must assemble.

The Full Story: A criminal actor — later identified as Viktor Sorin, a foreign national — targeted NCIA's network infrastructure for a client who wanted persistent access to airport communications and flight data. Sorin identified Carlos Mendez as a target because Mendez's badge had access to the sterile side and Mendez frequented the Vendor Break Room (V-1) — one of the few doors still using a 125 kHz legacy reader. Two days before the exercise, Sorin sat at a table near Mendez in the public-side food court, used a concealed Proxmark3 RFID reader to capture the 125 kHz credential from Mendez's badge (effective range: 6-12 inches through clothing), and wrote the captured number to a blank T5577 card. On Thursday morning, he used the clone to enter the sterile side, navigate to Electrical Room B via maintenance corridors (all 125 kHz legacy readers), and installed a **rogue wireless access point** — a modified TP-Link router configured as a bridge, connected to an open port on the Cisco switch, hidden behind the UPS battery backup. The rogue AP provides external wireless access to the NCIA internal network from the Concourse B parking structure. He was inside for 12 minutes, then exited via a different door and left the airport.

The Puzzle Pieces: Students must: (1) Confirm the clone via PACS frequency analysis, (2) Identify the cloning method by finding the Wednesday V-1 anomaly, (3) Trace the clone's path to Electrical Room B, (4) Physically inspect E-2 and find the rogue AP, (5) Match CCTV footage to identify the clone holder, (6) Recognize that the clone only worked on 125 kHz legacy readers — mapping the systemic vulnerability.

Key Design Note: The Wednesday double-tap at V-1 is the "aha" moment. Why did Mendez's badge read twice at the same door in 27 seconds? He didn't — someone near him was using a Proxmark3 to capture his credential, and the capture attempt triggered a phantom read. If the IT team spots this in the logs, they can determine when and where the badge was cloned.

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. Give PACS Forensic Evidence Packet to IT team only. Walk through the duplicate credential alert. Emphasize: this is a puzzle. There is a specific answer. The IT team leads. The evidence is in the logs and the footage.	Teams organize. IT should immediately begin studying the PACS log. Security should ask: where is Mendez right now? Where is the clone holder right now?

PHASE 1: CONFIRM THE CLONE 0:10 — 0:35

Goal: Students confirm this is a real clone (not a glitch), locate the real Mendez, and begin analyzing the PACS data for patterns.

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	Security Officer	All	Security officer reports: "I located Carlos Mendez. He's in the Concourse A kitchen right now — SkyWay Catering prep for the morning flights. I showed him the duplicate alert. He says he has his badge — it's right there on his lanyard. He swears he didn't go near Door S-4 at 7:38. He says he's been in the kitchen since 7:04 and his coworkers confirm it. His badge looks normal — no visible damage or tampering."	Clone confirmed: Mendez was in the kitchen while "his badge" was at S-4. This is not a glitch. IT should note: the 07:38 S-4 event was at 125 kHz, but Mendez's morning entry at 06:55 was at 13.56 MHz. Why would the same badge read at different frequencies?
0:18	I-02	IT Team Analysis	All	IT reports (or facilitator delivers if IT hasn't identified it yet): "We've found something critical in the log. Every event we can confirm as the real Mendez — his morning entry, his kitchen access, his lunch break — reads at 13.56 MHz on the iCLASS readers. But the duplicate events — the ones that triggered the alert — all read at 125 kHz. That's the legacy frequency. The clone isn't a copy of Mendez's encrypted smart card. It's a copy of the legacy 125 kHz credential number that his card also carries for backwards compatibility. Someone captured the unencrypted 125 kHz signal and wrote it to a blank prox card. This is a classic Proxmark3 attack."	This confirms the technical method. The IT team should now ask: when was the credential captured? Looking at the log: Wednesday at 10:22 — the anomalous 125 kHz read at V-1. If they haven't spotted the Wednesday V-1 anomaly yet, the next inject will push them there.
0:26	I-03	Facilitator (Nudge)	IT	If the IT team hasn't noticed the Wednesday V-1 entries, the facilitator prompts: "Your PACS log covers 72 hours. You've been looking at Thursday. Go back to Wednesday. Is there anything unusual in Mendez's access pattern?"	IT should find the Wednesday 10:22/10:23 double-read at V-1: Mendez's badge was read at 125 kHz twice in 27 seconds at the same door. That's not normal behavior — it's consistent with someone nearby using a Proxmark3 reader that triggered a phantom read on the door's 125 kHz antenna. The Vendor Break Room (V-1) is the capture location.

PHASE 2: TRACE THE PATH 0:35 — 1:10

Goal: Students map the clone's complete movement, identify Electrical Room B as the target, physically inspect E-2, and discover the rogue AP. CCTV gives them a face.

Time	ID	From	To	Event / Message	Expected Action
0:35	I-04	IT / Security	All	IT presents the clone's movement timeline (from PACS Forensic Packet, Exhibit C): S-4 (entry) → M-3 (maintenance corridor) → E-2 (Electrical Room B — 12 minutes inside) → M-3 (exit corridor) → S-6 (exit to non-sterile). "The clone was inside Electrical Room B for 12 minutes. That room houses the Concourse B network switch closet. They didn't go near the gates, the ramp, or any passenger area. They went straight to network infrastructure."	The pattern is clear: this was not random access. The clone holder targeted a specific room — one that houses a network switch, fiber patch panel, and wireless AP. Ops should order an immediate physical inspection of E-2. IT should go with them.
0:43	I-05	CCTV Review	Security / All	Security reports on CCTV review: "We pulled footage from the camera covering Door S-4 at 07:38. We see a male, approximately 5'10, wearing a grey maintenance jumpsuit, baseball cap, and a lanyard with a badge. He holds the badge to the reader and enters. We do NOT recognize him — he's not a known airport employee or vendor. The badge on his lanyard appears to be a plain white card — not the standard NCIA badge with photo and hologram. We also pulled the camera at S-6 when he exits at 08:07. Same individual. He's carrying a black backpack that appears heavier leaving than when he entered. There's no camera in the maintenance corridor or inside Electrical Room B."	The CCTV confirms: this is a stranger using a cloned badge. The plain white card is consistent with a T5577 blank programmed with Mendez's 125 kHz credential. The backpack potentially contained tools and equipment. Security should run the facial image against vendor/employee databases and share with TSA and law enforcement. "No camera in the maintenance corridor or E-2" is a security gap the team should flag.
0:52	I-06	IT Inspection Team	All	IT team reports back from Electrical Room B: "We found it. There's a device hidden behind the UPS battery backup, connected to Port 23 on the Cisco 2960 switch. It's a modified TP-Link wireless router — looks like it's been configured as a network bridge. It's powered by a USB cable tapped into the UPS. It has two antennas and it's broadcasting a hidden SSID. Based on the signal strength and antenna configuration, this device could be reached from the parking structure. Someone could sit in a car in the Concourse B lot and have direct access to the VLAN that this switch serves — which is the Concourse B operational network. That's gate management terminals, FIDS displays, and a trunk link to the core switch. The device MAC address is 50:C7:BF:XX:XX:XX — that's a TP-Link OUI. It's been connected for approximately 30 minutes."	THIS IS THE ANSWER TO THE PUZZLE. The clone was used to gain physical access to install a rogue wireless bridge that provides persistent remote access to the airport's internal network from the parking lot. The physical intrusion was the delivery mechanism for a cyber attack. IT must: (1) Do NOT disconnect the device yet — photograph and document it. (2) Identify what traffic it has already passed. (3) Check the switch port config for any changes. (4) Determine what VLAN it's on and what it can reach.

Time	ID	From	To	Event / Message	Expected Action
1:00	I-07	IT Analysis	All	IT provides deeper analysis of the rogue AP: "We examined the switch port. Port 23 was configured as an access port on VLAN 60 — Baggage/OT. But whoever installed this device reconfigured it as a trunk port. A trunk port passes traffic from ALL VLANs. That means this rogue AP doesn't just have access to Concourse B ops — it has access to Server VLAN 10, Admin VLAN 20, Security Camera VLAN 30, Retail VLAN 40, and Management VLAN 99. If someone connects to this device from the parking lot, they are on the inside of our entire network. Firewalls, IDS, all our perimeter security — irrelevant. They're already past all of it."	The trunk port reconfiguration is the technical climax. Someone with switch configuration knowledge changed a port from access to trunk mode in 12 minutes. That means the clone holder: (1) knew the switch model, (2) had the default/known credentials for the switch CLI, (3) knew enough about NCIA's VLAN structure to configure the trunk correctly. This was not opportunistic — it was planned. The team should ask: are switch management credentials the same across all closets? (Probably yes. That's another finding.)

PHASE 3: WHO AND WHY 1:10 — 1:40

Goal: Identify the clone holder, understand the motive, make containment decisions, and build the security remediation plan.

Time	ID	From	To	Event / Message	Expected Action
1:10	I-08	TSA / Law Enforcement	Security	TSA/FBI response: "We ran your CCTV still through the FBI's facial recognition database. We have a potential match: Viktor Sorin, 34, Ukrainian national. He's flagged in Interpol's database — not as a terrorist, but as a known associate of a cybercrime-as-a-service operation based in Eastern Europe. They sell network access to the highest bidder. We believe Sorin was hired to establish persistent access to your network. He installs the hardware. Someone else — the client — uses it remotely. If that rogue AP is still broadcasting, the client may already be on your network. Or they may not have connected yet. Either way — whoever hired Sorin now knows how to get in, and they can do it from the parking lot."	CRITICAL: The immediate question is whether to disconnect the rogue AP now or leave it and monitor for incoming connections to identify the client. Disconnecting secures the network but loses the chance to catch the buyer. Leaving it running means someone may be actively on your network right now. FBI will have an opinion. Let the team discuss.
1:18	I-09	IT / Facilitator	All	DECISION POINT. The facilitator frames the choice: OPTION A — "Pull the Plug": Disconnect the rogue AP immediately. Port 23 goes dark. The network is secured. But whoever hired Sorin will know the device was found — and they'll try another method. You've won the battle but the adversary adapts. OPTION B — "Honeypot": Leave the rogue AP connected but isolate VLAN traffic through it to a monitored sandbox. Let the client connect. Capture their traffic, IP address, and activity. Feed disinformation. Work with the FBI to trace them. OPTION C — "Silent Kill": Reconfigure Port 23 back to an access port on an unused VLAN. The AP still appears to be connected but can't reach anything real. The client doesn't know the device is neutralized until they try to use it.	Each option has trade-offs. Option A is safest. Option B is the most intelligence-rich but risky. Option C is the most elegant technically. Let IT argue for their preferred approach, Ops and Security weigh risk, and command makes the call.
1:26	I-10	Facilitator	All	SYSTEMIC VULNERABILITY ASSESSMENT. The facilitator asks: "The clone only worked because of 125 kHz legacy readers. How many do you have? (Answer: 12.) Those 12 readers are open doors for anyone with a $25 Proxmark3. The rogue AP was connected to Port 23 — a port that was configured as access, not trunk. Sorin reconfigured it. Were there any alerts when the port config changed? (Answer: No. Because NCIA doesn't have switch port change monitoring.) Sorin knew the switch credentials. Are your switch management passwords unique per closet? (Answer: No. Same credentials on every IDF closet in the building.) The switch was accessible on the Management VLAN from any device plugged into an open port. Is there 802.1X port authentication? (Answer: No.) There is no camera in the maintenance corridor or inside E-2. Why is there no camera covering access to your network infrastructure?"	This is the systemic findings discussion. Each question reveals a failure: 1. Legacy 125 kHz readers still in production 2. No switch port change monitoring/alerting 3. Shared management credentials across all IDFs 4. No 802.1X port authentication 5. No CCTV coverage of infrastructure rooms 6. Open/unused switch ports not disabled Build the remediation plan on the whiteboard.

Time	ID	From	To	Event / Message	Expected Action
1:32	I-11	Facilitator	All	REMEDIATION PLANNING. Each team addresses their area: — IT: Rogue AP disposition. 802.1X deployment timeline. Switch credential rotation. Port change monitoring (SNMP traps / syslog). Disable unused ports. VLAN audit. Legacy reader replacement schedule. — Security: Camera coverage for infrastructure rooms. Enhanced badge authentication — disable 125 kHz legacy mode on all dual-mode readers. Badge audit for all vendor personnel. TSA notification. — Ops: Airline impact of any network changes. Communication plan for badge system changes. — PIO: Prepare for the possibility that this becomes public. What's the headline you want vs. the headline you'll get?	Push for specific timelines and ownership. The technical remediation list is long — prioritize by risk. Disabling legacy 125 kHz mode is the single most impactful change.

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

Time	ID	From	To	Event / Message	Expected Action
1:40	END	Facilitator	All	ENDEX. 3-Up / 3-Down, followed by key discussion questions: 1. When did you confirm this was a clone and not a glitch? What evidence convinced you? 2. The Wednesday V-1 double-tap — did you spot it? What does that tell you about log analysis? 3. Twelve minutes in Electrical Room B. How do you prevent physical access to network infrastructure? 4. Legacy readers: $25 to clone a badge. What's the cost of replacing 12 readers vs. the cost of this incident? 5. Option A/B/C — what did you choose and why? What would the FBI have recommended?	Team reflects. Facilitator captures lessons learned. Exercise complete.

END OF MSEL