MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 3: "Blackout Friday" — Coordinated Systems Attack

North Coast International Airport (NCIA)
Duration: 2 Hours | Cyber + Physical Crisis
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW — THE FULL STORY

Who: "Chaos Collective" — a loosely organized hacktivist group that targets critical infrastructure to expose security weaknesses. Not state-sponsored. Not financially motivated. Their goal is public embarrassment: demonstrate that a single person on airport WiFi can trigger a mass evacuation, and then post the proof online. The operator is a 24-year-old computer science student named Marcus Webb, sitting in the Concourse A food court with a laptop and a $9 latte.

How — The Attack Chain:

- **Step 1 — Reconnaissance (weeks prior):** Webb visited NCIA twice as a passenger. He connected to Guest WiFi and ran network scans. He discovered Firewall Rule 49 — Guest WiFi (VLAN 70) can reach VLAN 50 on port 443. He found the PA controller's web admin interface at 10.1.50.10:443.
- **Step 2 — Credential Discovery:** The PA controller (Cisco UCM) was installed 18 months ago by Convergent AV Solutions. The web admin credentials were never changed from the vendor default: **admin / Converg3nt!**. Webb found this default in Convergent's public installation guide, which is hosted on their website. He tried it. It worked.
- **Step 3 — FIDS Discovery:** From the Guest WiFi, Webb also found that Rule 48 (VLAN 70 → VLAN 10:DNS) allows DNS queries. He used DNS to enumerate VLAN 10 hosts and discovered the FIDS server at 10.1.10.25. The FIDS management console runs on port 8080 (HTTP). Rule 48 only allows port 53, so he can't reach port 8080 directly from VLAN 70. But he CAN reach VLAN 50 on 443 (Rule 49). From the PA controller (which is on VLAN 50), he pivoted through the PA controller's diagnostic shell to reach the FIDS management console on VLAN 10:8080. The PA controller has unrestricted access to VLAN 10 because VLAN 50 → VLAN 10 is permitted for FIDS display traffic.
- **Step 4 — Execution (Today):** Webb buys a ticket on a 5:30 PM flight. Clears security. Sits in the food court. At 2:47 PM, he sends a kill command to the FIDS server via the management console (stop service + clear display cache). All 38 screens go black. He waits 8 minutes for the chaos to build. At 2:55 PM, he uses the PA controller's emergency broadcast function to inject the evacuation message across all PA zones. He pre-typed the message and configured it for "Emergency — All Zones." One click.
- **Step 5 — Exfiltration:** Webb closes his laptop, walks to his gate, and waits. He has a boarding pass. He looks like every other passenger. At 3:30 PM, the Chaos Collective posts on social media: "We just evacuated an airport from the food court WiFi. One firewall rule. One default password. 6,000 people running. Your infrastructure is a joke. Fix it. #BlackoutFriday"

The Teaching Point: The entire attack was possible because of two failures: (1) a single overly-broad firewall rule (Rule 49) that let Guest WiFi reach the PA controller, and (2) default vendor credentials that were never changed. Total cost of the attack: $9 (latte) + $0 (public WiFi). Total damage: mass panic, injuries, sterile area compromise, 14 flights disrupted, national media coverage, and an FAA/TSA investigation.

PHASE 0: BRIEFING 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing to all teams. Give Systems Reference Card to IT (Team B) only. Set the scene: day before Thanksgiving, 6,200 passengers, FIDS just crashed, PA evacuation message just played. Chaos is in progress.	Teams organize. Ops takes command of the physical crisis. IT begins investigating the FIDS crash. TSA/Security assesses the sterile area breach. PIO monitors social media and prepares statements.

PHASE 1: THE CHAOS 0:10 — 0:35

Goal: Manage the immediate crisis. Establish whether there is a real threat. Begin the re-screening debate.

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	AOC Console	Ops / Security	AOC reports: "The PA message did NOT come from this console. Nobody in the AOC authorized that announcement. We've checked every operator on shift. None of them pressed anything. But here's the problem — we don't know how to verify where it DID come from. The PA system has a web admin interface that we don't routinely monitor. IT needs to check the PA controller logs."	Ops and Security now know: the evacuation was unauthorized. This is critical — it means there may be no real security threat. But you can't ASSUME that. IT needs to investigate the PA system to confirm. Security must decide: treat it as real until proven otherwise?
0:15	I-02	TSA FSD	Ops / Security	TSA Federal Security Director calls: "I've got a checkpoint in chaos. People running both directions. Two passengers fell. One has a possible broken wrist. We've shut down the checkpoint. Emergency exits on Concourse A gates 6, 8, and 12 were opened by passengers. Concourse B gates 3 and 7 also breached. That's five unscreened egress points. I need to know: is there a real threat? Because if there isn't, I need to know RIGHT NOW so I can start making the re-screening decision. And if there IS a real threat, we need to do a full ground stop and bring in VIPR teams."	TSA wants a binary answer: real threat or not? The team doesn't know yet. The correct answer right now is: "We have not confirmed a threat. The PA message was unauthorized. We are investigating. We recommend treating the checkpoint breach as a security event requiring re-screening, pending investigation results."
0:22	I-03	Social Media	PIO	Social media monitor report: • Passenger video of the stampede near Gate B-7 — 47K views in 8 minutes • #NCIAevacuation trending locally • @NCIAirport receiving hundreds of panicked DMs • Local TV station has dispatched a crew — ETA 15 minutes • One passenger tweet: "People are hurt. Where is airport security? No one is telling us what's going on." CNN travel desk has called the airport media line.	PIO must issue an immediate statement. Suggested: "NCIA is responding to a PA system malfunction that triggered an unauthorized evacuation message. There is no confirmed security threat at this time. Airport operations staff and TSA are working to restore normal operations. Passengers should follow instructions from airport and airline personnel." The word 'malfunction' is intentional — it's accurate if this is a cyberattack (the PA system was used in an unintended way) and it doesn't commit to 'attack' or 'hack' prematurely.

Time	ID	From	To	Event / Message	Expected Action
0:28	I-04	Airlines	Ops / PIO	Delta, United, and American station managers call simultaneously: "What is happening? Do we board? Do we delay? Do we cancel? We have 14 departures in the next 3 hours and our passengers are standing in a parking lot. We need a decision in 10 minutes or we start cancelling ourselves."	Airlines need a decision: board or hold. If re-screening is ordered, no boarding for 2-3 hours. If no re-screening, they can start re-boarding in 15-20 minutes. This forces the re-screening decision.

PHASE 2: THE INVESTIGATION 0:35 — 1:05

Goal: IT traces the attack chain. The puzzle pieces come together. The connection between FIDS and PA is revealed.

Time	ID	From	To	Event / Message	Expected Action
0:35	I-05	IT Analysis	All	IT reports on FIDS: "The FIDS server didn't crash — it was killed. Someone accessed the FIDS management console (port 8080, HTTP) and sent a service stop command followed by a display cache clear. The management console access log shows a session from IP address 10.1.50.10 at 2:46 PM — one minute before the screens went dark. 10.1.50.10 is the PA controller. Someone used the PA controller to reach the FIDS server. These attacks are connected — same source."	The FIDS and PA attacks are linked. The PA controller was the pivot point. IT should now investigate: how was the PA controller compromised? And how did someone reach the PA controller from outside VLAN 50?
0:42	I-06	IT Analysis	All	IT reports on the PA controller: "We pulled the PA controller audit logs. At 2:44 PM, someone logged into the web admin interface from IP 10.1.70.47. That IP is on VLAN 70 — **Guest WiFi**. A device on our public WiFi network accessed the PA controller. We checked the firewall rules and found Rule 49 — added 6 months ago during the WiFi upgrade. It allows VLAN 70 to reach VLAN 50 on port 443. The PA admin interface runs on 443. The Guest WiFi is NOT isolated. Anyone sitting in the terminal with a laptop can reach the PA system's admin interface." (Pause.) "And the login credentials? We checked with Convergent AV Solutions. The admin password is still the vendor default: admin / Converg3nt!. It's in their publicly-available installation guide. It was never changed after deployment 18 months ago."	THE ANSWER. The attack chain is: Guest WiFi → Rule 49 → PA controller (default creds) → pivot to FIDS server (VLAN 50 → VLAN 10 allowed). Two vulnerabilities: overly-broad firewall rule + default password on critical infrastructure. Let this sink in. Someone on PUBLIC WIFI took down FIDS and triggered a mass evacuation using a DEFAULT PASSWORD.
0:50	I-07	IT	All	DECISION: "The attacker accessed both systems from Guest WiFi device 10.1.70.47. That device is still connected. We can see it on the wireless controller — it's associated with an access point in the Concourse A food court. Options: A) Kill the WiFi session and blackhole the MAC address — attacker loses access but we lose forensic trail. B) Leave the session active but isolate it to a monitoring sandbox — capture any further activity. C) Identify the device owner via CCTV (food court camera + MAC address + AP location) and coordinate with law enforcement for a physical approach." Also: should we change the PA controller password NOW? If we do, the attacker can't send another message. But if we don't, there could be a Phase 3.	Option C is ideal but takes time and coordination with LEO. Option A is fast but loses the trail. Option B is the intelligence play. The PA password should be changed IMMEDIATELY — preventing Phase 3 is more important than preserving access for forensics.

Time	ID	From	To	Event / Message	Expected Action
1:00	I-08	CCTV / LEO	All	CCTV review of the Concourse A food court identifies a male, mid-20s, with a laptop at a table near the AP that served 10.1.70.47. He's been sitting there since 2:30 PM. He closed his laptop at approximately 2:58 PM — 3 minutes after the PA message — and walked to Gate A-14. He appears calm while everyone around him is panicking. Gate A-14 is the 5:30 PM departure to Atlanta. He's still in the gate area. Law enforcement is ready to approach on your order.	Decision: approach now or wait? If the team is confident this is the attacker, law enforcement can detain and interview. The laptop is critical evidence.

PHASE 3: THE RECKONING 1:05 — 1:40

Goal: Resolve the re-screening question. Hacktivist claim goes public. Root cause analysis. Remediation planning.

Time	ID	From	To	Event / Message	Expected Action
1:05	I-09	Social Media	PIO / All	The Chaos Collective posts on X (Twitter) and Reddit simultaneously: "We just evacuated @NCIAirport from the food court WiFi. One firewall rule. One default password. 6,000 people running. Your infrastructure is a joke. Fix it before someone with worse intentions finds the same holes. #BlackoutFriday #AirportSecurity #ChaosCollective" The post includes a screenshot of the PA controller admin interface (with credentials redacted) and a timestamp proving they were logged in. Post is going viral. 200K impressions in 10 minutes.	The hacktivist claim changes the narrative. This is now a confirmed cyberattack, not a malfunction. PIO must update all communications. But the claim also confirms: there was no real security threat. The evacuation was manufactured. Does this change the re-screening decision? Also: the hacktivists just told the ENTIRE WORLD about a vulnerability that STILL EXISTS on your network. Other attackers now know about Rule 49 and default creds.
1:15	I-10	Facilitator	All	THE RE-SCREENING DECISION. The facilitator forces the call: "It's been 2 hours since the sterile area breach. 4,000 passengers exited through 5 unsecured doors. You now know there was no real security threat — the evacuation was manufactured by a hacktivist. But that doesn't change the fact that sterile area integrity was compromised. TSA policy is clear: if sterile area integrity is lost, all passengers must be re-screened. But it's the day before Thanksgiving. Re-screening 4,000 passengers will take 2.5 hours. 14 flights will be cancelled. Thousands will miss Thanksgiving. What do you do? Make the call. Defend it."	There is no right answer. The best answer is nuanced: partial re-screening of passengers who exited through the 5 specific emergency doors (CCTV can identify them), combined with enhanced random screening of all re-entering passengers. This is the compromise between full compliance and operational reality. The team must defend their choice.
1:25	I-11	Facilitator	All	ROOT CAUSE & REMEDIATION. The failure chain: 1. Firewall Rule 49 (added 6 months ago during WiFi upgrade) — allowed Guest WiFi to reach VLAN 50. 2. PA controller default credentials (18 months, never changed) — admin / Converg3nt! 3. FIDS management console on HTTP (not HTTPS) with no authentication beyond IP-based access. 4. No monitoring or alerting on PA controller logins. 5. No network segmentation between PA controller and FIDS server (VLAN 50 → VLAN 10 open). 6. No Guest WiFi traffic monitoring or anomaly detection. Each team: what's your top remediation priority?	IT: Delete Rule 49 immediately. Change PA credentials. Add authentication to FIDS console. Implement proper Guest WiFi isolation. Security: Improve emergency exit alarm response time. Stage re-screening resources. Ops: Pre-built crowd management plans for mass evacuations. PA counter-message templates. PIO: Pre-drafted statements for cyberattack vs. malfunction vs. false alarm.

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 questions: 1. The $9 Attack: A student with a laptop and a latte just evacuated your airport. What's the ROI on changing default passwords? 2. The Re-Screening Dilemma: What did you decide? Would a different answer be better? 3. The PA Trust Problem: After today, can you trust the PA system? If you can't, how do you communicate during a REAL emergency? 4. Guest WiFi: Should public WiFi at an airport ever touch ANY internal network? 5. The 8-Minute Gap: FIDS died at 2:47. PA fired at 2:55. In those 8 minutes, could you have prevented the PA attack if you'd known FIDS was deliberate?	Debrief and capture lessons.

END OF MSEL