MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 6: "Friendly Fire" — Self-Inflicted Network Outage

North Coast International Airport (NCIA)
Duration: 2 Hours | Puzzle: Three Theories, One Answer
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: Incident misidentification. Confirmation bias. Change management failures. What happens when the "attacker" is sitting in the room and doesn't know it.

The Full Story: At 2:00 AM Wednesday, automated scanning from IP range 185.220.0.0/16 probed NCIA's firewall management interface (3 failed SSH attempts). This scanning was real — it appeared on CISA advisory TI-2026-0312. IT Manager Jordan Kelley saw the advisory Wednesday morning and decided to block the IP range as an emergency threat mitigation. He wrote a firewall rule at 09:45 AM. The rule was supposed to block **inbound external traffic from 185.220.0.0/16**. Instead, Kelley made three critical errors: (1) he set Source Zone to "any" instead of "Untrust", (2) he set Source Address to "any" instead of 185.220.0.0/16, and (3) he set Destination to 10.1.40.0/24 (the Retail VLAN) instead of a server-side address. The resulting rule blocks ALL traffic from ANY source to the Retail VLAN — including internal Server VLAN traffic. He inserted it at position 3, above the inter-VLAN allow rules, so it takes priority. Then he was called to a meeting and didn't run post-change verification. Two minutes later, every POS terminal in the airport went dark.

Why It Looks Like an Attack: Simultaneously, two red herrings create plausible alternative theories. RetailLink (the POS vendor) pushed a firmware update at 9:30 AM — 17 minutes before the outage. And the SIEM shows real SSH scanning from 185.220.101.34 the night before. Both are genuine events. Neither caused the outage. But they provide just enough evidence for the team to chase the wrong theory.

The Puzzle: Three theories. Two red herrings. One correct answer. The team must: (1) Eliminate Theory A (external attack — the SSH attempts failed, no access gained), (2) Eliminate Theory B (vendor compromise — the firmware update didn't change gateway settings), (3) Confirm Theory C by reading the actual firewall rule and identifying the three errors. The "aha" moment is when IT reads the rule and realizes: Source Zone = any, Source Address = any, Destination = the Retail VLAN. That's not a targeted attack. That's a typo.

Key Design Principle: This exercise teaches confirmation bias. The SSH scanning and the vendor update are real events that make Theory A and Theory B feel true. Teams will *want* it to be an attack because attacks are exciting and internal errors are embarrassing. The facilitator should let them chase the wrong theory for a while before the evidence redirects them. The discomfort of admitting "we did this to ourselves" is the lesson.

PHASE 0: BRIEFING 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing Packet. Give Network Evidence Packet to IT only. Present all three theories equally. Do NOT hint at the answer. The team should feel genuinely uncertain about which theory is correct.	Teams organize. IT begins reviewing evidence. All teams should note the dual-clock: investigate AND manage the operational impact simultaneously.

PHASE 1: CHASE THE THEORIES 0:10 — 0:40

Goal: The team pursues all three theories. Each inject reinforces one theory before the next inject undermines it. The evidence oscillates — keeping the team uncertain.

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	Vendor Manager	Ops / IT	Airport's tenant coordinator calls: "I'm getting hammered by vendors. SkyLounge, Hudson News, the duty-free shop — every single one is cash-only. Passengers are furious. The Starbucks in Concourse A has a line out the door and they can't process a single card. I need a timeline for restoration. What do I tell 47 tenants?"	Ops must manage the operational fallout NOW — independent of the investigation. Options: coordinate cash-only signage, direct passengers to ATMs, contact airline clubs about POS workarounds. The tenant coordinator needs answers, not "we're investigating."
0:17	I-02	RetailLink Vendor	IT	Phone call from RetailLink support: "We heard your terminals are down. We did push firmware v4.2.1 at 9:30 this morning — it's a routine PCI compliance patch. We've checked our end and the update completed successfully on all 47 terminals. The terminals are online — they're just not reaching your payment gateway. This looks like a network issue on YOUR side, not a terminal issue on ours. Also, FYI — we flagged unusual API queries against our cloud portal yesterday from an IP we didn't recognize. We reported it to our security team. Unrelated, probably, but I wanted to mention it."	ELIMINATES THEORY B — partially. The firmware update didn't change terminal network settings. The terminals are online. The problem is between the terminals and the gateway — that's network, not vendor. But the "unusual API queries" comment re-fuels Theory A (external attack). IT should note: the vendor issue and the outage may be coincidental, not causal.
0:25	I-03	IT SIEM Analysis	All	IT reports on SIEM analysis: "We found the SSH scanning from last night — 185.220.101.34. Three failed login attempts against the firewall between 2:00 and 2:15 AM. All three failed — wrong credentials. No access was gained. But here's the thing: that IP is from a known scanning botnet flagged in CISA advisory TI-2026-0312. Someone was actively probing our firewall 7 hours before the outage. Coincidence? We also see that Jordan Kelley wrote a firewall rule this morning at 09:45 specifically to block that IP range. The rule is in the change log as CM-2026-0087. We should look at that rule."	This introduces the critical timeline: scan at 2 AM → Kelley writes blocking rule at 9:45 → outage at 9:47. The IT team should now want to inspect the actual rule. If they pivot to reading the firewall rule, they're on the right track. If they stay focused on the SSH scanning, they're still chasing Theory A.

Time	ID	From	To	Event / Message	Expected Action
0:33	I-04	Social Media / Media	PIO	PIO monitors social media: trending posts include "@NCIAirport card readers are all down — anyone else stuck paying cash?" and "Is NCIA under cyberattack?? Nothing is working." A local reporter has DM'd the airport's account: "We're hearing reports of a major system outage at NCIA. Is this a cyberattack? We're going live at noon. Comment?"	PIO must decide: what do you say? You don't know the cause yet. If you say "we're under investigation for a cyberattack" and it turns out to be a typo, that headline lives forever. If you say "it's a minor technical issue" and it IS an attack, you look like you covered it up. The correct statement is neutral: "We're experiencing a temporary system issue affecting some retail terminals. We're working to restore service and will provide updates as available."

PHASE 2: THE EVIDENCE CONVERGES 0:40 — 1:10

Goal: Theory A collapses. Theory C gains traction. The team reads the actual firewall rule and finds the errors. The "aha" moment.

Time	ID	From	To	Event / Message	Expected Action
0:40	I-05	IT Firewall Analysis	All	IT reports on the firewall rule CM-2026-0087: "We pulled the actual rule from the running config. It was supposed to block inbound traffic from 185.220.0.0/16. But that's not what it says. Source Zone is set to 'any' — not 'Untrust.' That means it applies to ALL zones, including internal VLANs. Source Address is set to 'any' — not 185.220.0.0/16. That means ALL source addresses. Destination is 10.1.40.0/24 — the Retail VLAN. Action is DENY. Position 3 — above the inter-VLAN allow rules. This rule says: deny ALL traffic from ANYWHERE going to the Retail VLAN. That's not a targeted block on an external threat. That's a kill switch on our Retail VLAN. And it was put there by Jordan Kelley at 9:45 this morning. Two minutes before every POS terminal went dark." (Silence.)	THE ANSWER. Theory C confirmed. The outage was caused by an overly broad firewall rule written by the IT Manager himself. Three errors: wrong source zone, wrong source address, and the rule was placed above the allow rules in the policy order. This is the emotional pivot. The team expected an attacker. They got a typo. Let the room absorb it. Then someone will ask: "Can we just delete the rule and fix it?" (Yes — but that's not the end of the exercise.)
0:50	I-06	Facilitator	IT	DECISION: "The fix is straightforward — delete rule TI-2026-0312-Block and traffic between VLAN 10 and VLAN 40 will be restored instantly. Do you delete it now?" But wait: the original threat was real. 185.220.0.0/16 WAS scanning your firewall last night. If you delete the rule entirely, you're removing the protection Kelley was trying to add. If you rewrite it correctly, you have to get it right THIS time. Option A: Delete the rule. Restore service immediately. Deal with the threat intel later. Option B: Rewrite the rule correctly (Source Zone: Untrust, Source Address: 185.220.0.0/16, Dest: any) and apply the corrected version. Takes 5-10 more minutes. Option C: Delete the rule AND apply a temporary block on 185.220.101.34 (the specific scanning IP) as a targeted measure while a proper rule is designed and peer-reviewed.	Option C is the best answer — it restores service AND addresses the real threat with a narrow, targeted block. But any option that restores service is acceptable. The real question is: does the IT team want someone to peer-review the corrected rule before it's applied? (They should. That's the change management lesson.)

Time	ID	From	To	Event / Message	Expected Action
0:58	I-07	Phone Call	Ops / IT	Delta station manager calls: "Our check-in kiosks were timing out for 45 minutes. I've got 200 passengers who couldn't use self-service check-in. My agents are processing them manually and we're looking at a 40-minute delay on three departures. I need a root cause analysis by end of day, and I need assurance this won't happen again. Was this a cyberattack?"	Ops must decide what to tell the airline. The truth is embarrassing: it was a misconfigured firewall rule — your own IT team's mistake. But the airline needs an honest answer. If they find out later that you misrepresented the cause, trust is broken. The correct approach: "The outage was caused by an internal configuration error that has been corrected. It was not a cyberattack. We are implementing additional controls to prevent recurrence."
1:05	I-08	Phone Call	PIO / Ops	Reporter calls PIO: "We're going live at noon with the NCIA outage story. We have multiple passenger reports that the airport's payment systems were down for over an hour. One source is telling us it was a cyberattack. Can you confirm or deny?"	PIO now faces the hardest version of this question. They know it WASN'T a cyberattack. But saying "it was our own mistake" is embarrassing. Saying "no comment" lets the cyberattack narrative run. The correct approach: issue a statement that's honest without being self-flagellating. "At approximately 9:47 AM, a configuration error in our network infrastructure caused a temporary disruption to retail payment systems. The issue was identified and corrected within [X] minutes. This was not a cyberattack. We are reviewing our change management procedures to prevent recurrence."

PHASE 3: THE RECKONING 1:10 — 1:40

Goal: Root cause analysis. Change management failures. Process improvements. And the hardest question: what do you do about Jordan Kelley?

Time	ID	From	To	Event / Message	Expected Action
1:10	I-09	Facilitator	All	ROOT CAUSE ANALYSIS. The facilitator walks through the failure chain: 1. Real threat detected (SSH scanning) — appropriate concern. 2. Kelley decides to write a blocking rule — reasonable response. 3. The rule was self-approved — NCIA policy allows emergency threat mitigation without peer review. 4. Three errors in the rule: wrong source zone, wrong source address, rule position above allow rules. 5. No post-change verification — Kelley was called to a meeting and didn't check. 6. The outage was detected in 2 minutes — but cause identification took [however long it took the team]. "Where did the process fail? Was it the person, the policy, or both?"	This is the systems-thinking discussion. Kelley made a mistake, but the system ALLOWED the mistake: no peer review, no automated validation, no post-change testing requirement, no firewall rule syntax checking. The question is not "fire Kelley" — it's "what controls would have caught this before it went live?"
1:20	I-10	Facilitator	All	THE JORDAN KELLEY QUESTION. The facilitator asks directly: "Jordan Kelley is your IT Manager. He wrote the rule. He self-approved it. He didn't verify it. He crashed your retail network for [X] minutes. 47 tenants couldn't process transactions. Airlines delayed flights. You may have PCI reporting obligations. The media called. Do you discipline him? Fire him? Or do you recognize that the system allowed a single person to make a change with no review, no validation, and no verification — and that if Kelley hadn't made this mistake, someone else eventually would have? What do you do with Jordan?"	This is the exercise's emotional peak. Some will want to fire him. Others will defend him. The best answer is nuanced: Kelley made a mistake, but the organization failed to prevent it. A blame-free culture that focuses on process improvement is more resilient than one that fires the person who made the error. But there IS accountability for skipping post-change verification. Let the room argue. The argument IS the exercise.
1:30	I-11	Facilitator	All	PROCESS IMPROVEMENT. Each team addresses their area: — IT: Mandatory peer review for all firewall changes (no self-approval). Automated rule validation (syntax check against known-good patterns). Mandatory post-change verification checklist. Firewall rule change staging environment. Alert-on-deny-rule creation. — Ops: Retail outage playbook — what to do in the first 5 minutes when POS goes down. Cash-only signage pre-staged. ATM location communication. Airline notification protocol. — PIO: Pre-drafted holding statements for system outages (attack vs. error vs. unknown). Social media monitoring escalation triggers. — Legal: When does a network outage trigger PCI notification? When does it NOT? What's the threshold? (Answer: if no card data was compromised, PCI notification is not required — but you need to confirm no data was exposed.)	Push for specifics. "When does the peer review policy go into effect? Tomorrow? Next quarter? What does the staging environment look like? Who reviews emergency changes at 2 AM?"

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. Which theory did you pursue first? Why? How long before you pivoted? 2. Did you WANT it to be a cyberattack? Why is that instinct dangerous? 3. How long did it take to read the actual firewall rule? Could you have found it faster? 4. What would you tell the airlines? The media? The board? 5. Jordan Kelley — what did you decide? Would you feel different if it was you?	Team reflects. Facilitator captures lessons. Exercise complete.

END OF MSEL