ACTION MENU CARD

Scenario 8: "Countdown" — Your Investigation Options

Each action costs scenario time. Choose wisely. You have 180 minutes.
Give this card to all teams at exercise start.

DIGITAL FORENSICS

ID	Action	Time Cost	Description
A-01	Trace the Email	15 min	Analyze email headers from the anonymous threat. Attempt to trace origin IP, mail server path, and sender identity.
A-02	Scan Email for Embedded Payloads	10 min	Analyze the email body and headers for embedded malware, tracking pixels, steganographic content, or encoded messages.
A-03	Full Network Vulnerability Scan	30 min	Run an enterprise-wide vulnerability scan across all VLANs. Checks for open ports, unpatched services, and misconfigurations.
A-04	Review Firewall Logs (Last 7 Days)	15 min	Pull and analyze firewall logs for anomalous inbound/outbound connections, denied traffic, and policy violations.
A-05	Inspect AODB Server	15 min	Remote into the AODB server. Check running processes, scheduled tasks, recent file changes, and service status.
A-06	Audit VPN Access Logs	10 min	Review all VPN connection logs for the last 30 days. Check for active sessions, unusual source IPs, and revoked credentials.
A-07	Review SIEM Alerts (Last 30 Days)	20 min	Pull all SIEM alerts from the last 30 days. Filter for high-severity events, anomalous login patterns, and escalation triggers.
A-08	DNS Query Log Analysis	10 min	Review internal DNS logs for suspicious domain lookups — known C2 domains, data exfiltration patterns, DGA-style queries.

PHYSICAL / OPERATIONAL

ID	Action	Time Cost	Description
A-09	Physical Sweep — Terminal Interior	20 min	Send security teams to sweep the terminal for suspicious packages, unattended items, or unauthorized individuals.
A-10	Physical Sweep — Ramp & Airside	25 min	Sweep the ramp, cargo areas, baggage makeup, and ARFF station for anything unusual.
A-11	CCTV Review — Last 24 Hours (Key Areas)	20 min	Review CCTV footage from the last 24 hours at: server room, IDF closets, electrical rooms, and Security office.
A-12	PACS Audit — After-Hours Access	10 min	Pull PACS log for all after-hours access events (9 PM to 6 AM) in the last 30 days. Flag unusual patterns.
A-13	Contact TSA — Threat Advisory Check	10 min	Call TSA and FBI to check for any specific threat advisories or intelligence related to NCIA.
A-14	Interview IT Staff — Recent Contractors	15 min	Interview current IT staff about the NexGen Solutions contractor (Dmitri Volkov) and his work on the AODB migration.

RESPONSE PLANNING

ID	Action	Time Cost	Description
A-15	Prepare Network Isolation Plan	10 min	Draft a plan to isolate critical network segments (Server, Security, OT) at a moment's notice if the threat is cyber.

A-16	**Prepare Terminal Evacuation Plan**	**15 min**	Stage resources for a potential terminal evacuation if the threat is physical. Coordinate with TSA and airlines.
A-17	**Activate CISA Emergency Contact**	**10 min**	Call CISA's 24/7 operations center. Report the threat. Request emergency technical assistance.
A-18	**Back Up Critical Systems**	**20 min**	Initiate emergency snapshot backups of AODB, FIDS server, PACS database, and Domain Controller.

ADVANCED INVESTIGATION			
ID	**Action**	**Time Cost**	**Description**
A-19	**Search for Scheduled Tasks Across All Servers**	**15 min**	Query all Windows servers for scheduled tasks created in the last 60 days. Flag any task with a trigger time near 12:00.
A-20	**Cross-Reference Email Metadata with Employee/Contractor Records**	**10 min**	Analyze email header metadata (timezone, language, user-agent) and cross-reference with personnel records.

TOTAL TIME IF YOU DO EVERYTHING: 305 minutes. You have 180. You cannot do it all. **Prioritize.**

CUSTOM ACTIONS: If you want to do something not on this list, describe it to the facilitator. They will assign a time cost and provide results. Creativity is rewarded — but wild guesses cost time.