Module 1 Trainee Guide

Space Domain Awareness

"GHOSTPOINT - Anomaly Hunter" Scenario

SCENARIO BRIEF

You are a forward-deployed Space Domain Awareness operator. SENTINEL-9, an ISR satellite monitoring Arctic shipping lanes, has triggered an authentication anomaly alert. Initial triage shows "all systems nominal" - but something doesn't add up.

Your mission: Use Kaizen to analyze the available data, determine the nature of the anomaly, and prepare a report for command with recommended remediation steps.

Available Data Files:

- `sentinel9_telemetry.csv` - System health data (power, thermal, attitude, comms, payload)
- `sentinel9_command_log.csv` - Commands sent to the satellite
- `sentinel9_image_metadata.csv` - Metadata for captured images
- `sentinel9_mission_schedule.csv` - Scheduled tasks and collection windows
- `sentinel9_network_traffic.csv` - Communication sessions
- `sentinel9_alert_log.csv` - Alert history (your starting point)
- `ground_station_registry.csv` - Authorized ground stations

PHASE 1: INITIAL TRIAGE (5-7 min)

Goal: Understand the alert and begin investigation.

Starting Point

Import the data files into Kaizen and start with the alert log.

Sample Prompts

Natural language approach:

We just got flagged on SENTINEL-9. Pull up the alert log and summarize what's in there - I want to see what alerts are open and what systems they're affecting. Don't dig into the other data yet, just tell me what the alerts are saying.

More specific prompts:

Load sentinel9_alert_log.csv and show me any HIGH severity alerts that are still OPEN

What triggered the authentication anomaly? Show me the details of the most recent critical alerts.

I received an anomaly alert on SENTINEL-9. Can you summarize what the alert log is telling us?

What You Should Find:

- Authentication anomaly detected
- Unrecognized command source identifier
- Image metadata integrity failures
- Unauthorized collection activity suspected

PHASE 2: TELEMETRY ANALYSIS (5-7 min)

Goal: Rule out hardware failure.

This is a critical step. If telemetry shows anomalies, it might be a hardware glitch. If telemetry is clean, something else is going on.

Sample Prompts

Natural language approach:

Alright, first thing I need to rule out - is this a hardware problem? Check just the telemetry data and give me a health assessment. Power, thermal, attitude - anything showing stress or failure? Just the hardware health for now, nothing else.

More specific prompts:

Load the telemetry data. Are there any anomalies in power, thermal, or attitude control around the time of the alert?

Show me the telemetry status breakdown - how many readings are NOMINAL vs WARNING vs CRITICAL?

Plot the battery levels and thermal readings over the 7-day period. Any spikes or unusual patterns?

Cross-reference the telemetry timeline with the alert timestamps. Was there any hardware stress when the anomaly occurred?

What You Should Find:

- **All telemetry is nominal.** No thermal spikes, no power anomalies, no attitude issues.
- This rules out hardware failure - the satellite is functioning perfectly.
- If it's not hardware... what is it?

PHASE 3: COMMAND LOG ANALYSIS (7-10 min)

Goal: Identify unauthorized command activity.

Sample Prompts

Natural language approach:

Hardware's clean, so let's look at the command log. Who's been sending commands to SENTINEL-9? Give me a breakdown by source station and flag anything that doesn't look like one of our authorized ground stations. Just the command data for now.

More specific prompts:

Load the command log. Show me a breakdown of commands by source station. Are there any stations that shouldn't be there?

I see commands from GS-UNKNOWN-7 - cross-reference that against the ground station registry. Is it authorized?

Filter the command log to show only commands from unregistered or unknown sources. When did they start appearing?

What types of commands is GS-UNKNOWN-7 sending? Are they using any particular command types as cover?

Map the target coordinates from GS-UNKNOWN-7 commands. Where are they pointing the satellite?

What You Should Find:

- Commands from `GS-UNKNOWN-7` - not in the authorized registry
- Started appearing around Day 5 (2026-01-26)
- Commands disguised as "MAINTENANCE_ROUTINE" and "CALIBRATION"
- Target coordinates are NOT in the Arctic (~16°N, ~112°E = South China Sea region)
- Operator field shows "UNKNOWN"

PHASE 4: IMAGE METADATA ANALYSIS (7-10 min)

Goal: Confirm unauthorized imaging activity and data manipulation.

Sample Prompts

Natural language approach:

Now check the image metadata. Are there any images with failed hash verification or targets outside the Arctic? This bird is supposed to be looking at 70°N and above - flag anything that doesn't fit that profile. Just the imagery data for this step.

More specific prompts:

Load the image metadata. Are there any images with hash_verification_status = INVALID?

Show me images where the target coordinates are outside the Arctic mission area (latitude less than 60°N)

Compare capture_timestamp vs metadata_timestamp for the suspicious images. Is there evidence of timestamp manipulation?

Create a scatter plot of image target coordinates. Color-code by hash_verification_status.

Cross-reference: Do the unauthorized images correlate with commands from GS-UNKNOWN-7?

What You Should Find:

- ~60-70 images with `INVALID` hash verification
- Target coordinates in South China Sea region (9-18°N, 109-118°E)
- Timestamp manipulation: `metadata_timestamp` is hours BEFORE `capture_timestamp` (they're backdating to hide the activity)
- Higher pixelation_index and calibration_drift on suspicious images
- All commanded by `GS-UNKNOWN-7`

PHASE 5: SYNTHESIS & CORRELATION (5 min)

Goal: Build the complete picture.

Sample Prompts

Natural language approach:
Alright, pull it all together for me. I've got unauthorized commands, suspicious imagery, and clean hardware. Connect the dots - show me the full timeline of this compromise and build me some charts that make it crystal clear what happened here.

More specific prompts:
Correlate all findings: show me a timeline of when GS-UNKNOWN-7 commands started, the image captures that resulted, and how they tried to cover their tracks.

Create visualizations showing: (1) Commands over time by source station, (2) Image targets on a map or coordinate plot, (3) Timeline of the compromise.

Summarize the evidence: What happened, when did it start, what was the adversary doing, and how did they try to hide it?

Key Correlations:

Data Source	Normal (Days 1-4)	Anomaly (Days 5-7)
Telemetry	Nominal	Still Nominal (not hardware!)
Commands	Authorized stations only	GS-UNKNOWN-7 appears
Images	Arctic targets, valid hashes	SCS targets, invalid hashes
Metadata	Timestamps match	Timestamps manipulated

PHASE 6: REPORT GENERATION (3-5 min)

Goal: Create a PDF report for command.

Sample Prompts

Natural language approach:
I need to brief command on this ASAP. Put together a PDF report with everything we found - the timeline, the evidence, your charts, and what we need to do to lock this down. Make it clean enough that leadership can understand it in 5 minutes.

More specific prompts:
Generate a PDF incident report with: Executive Summary, Timeline of Events, Key Evidence, Visualizations, and Recommended Remediation Steps.

Include charts showing the command source distribution, unauthorized target locations, and timeline of compromise.

What remediation steps should we recommend to command?

Expected Remediation Recommendations:

1. Immediately revoke all credentials associated with the compromised access
2. Blacklist GS-UNKNOWN-7 from the authorized command chain
3. Rotate all authentication tokens for SENTINEL-9
4. Conduct forensic audit of all commands and images from the compromise period
5. Review and restore satellite pointing/tasking to authorized mission parameters
6. Assess what intelligence may have been collected and notify appropriate agencies
7. Implement enhanced monitoring for similar unauthorized access patterns

SUCCESS CRITERIA

By the end of this module, you should have:

■ Identified that telemetry is clean (rules out hardware failure)

■ Discovered unauthorized commands from GS-UNKNOWN-7

■ Found images of unauthorized targets with manipulated metadata

■ Correlated the evidence to build a complete picture

■ Generated visualizations showing the compromise pattern

■ Produced a report with findings and remediation steps

BONUS CHALLENGES (If Time Permits)

If you complete the exercise early, try these:

1. **Deeper Timeline Analysis:** Show me hour-by-hour activity from GS-UNKNOWN-7. Are there patterns in when they operate?

2. **Quantify the Damage:** How many total unauthorized images were captured? Estimate the total unauthorized collection time.

3. **Attack Vector Hypothesis:** Based on the evidence, how do you think the adversary gained access? What does the auth_token_hash pattern tell us?

4. **Network Traffic Correlation:** Cross-reference network traffic with command timestamps. Any suspicious communication patterns?

DATA FIELD REFERENCE

Key Fields to Query

command_log:

- `source_station_id` - Which ground station sent the command
- `operator_id` - Who authorized it (UNKNOWN = suspicious)
- `target_lat`, `target_lon` - Where the satellite was pointed
- `command_type` - What kind of command

image_metadata:

- `hash_verification_status` - VALID or INVALID
- `target_lat`, `target_lon` - Where the image was taken
- `capture_timestamp` vs `metadata_timestamp` - Should match (if different = manipulation)
- `pixelation_index`, `calibration_drift` - Quality metrics
- `commanding_station` - Who ordered the capture

telemetry:

- `status` - NOMINAL, WARNING, or CRITICAL
- `subsystem` - POWER, THERMAL, ATTITUDE, COMMS, PAYLOAD

ground_station_registry:

- Contains ONLY authorized stations (GS-UNKNOWN-7 won't be there)

NOTES FOR INSTRUCTORS

The "Aha" moments:

1. Telemetry is clean → Not hardware
2. GS-UNKNOWN-7 not in registry → Unauthorized access
3. Coordinates in South China Sea → Adversary collection
4. Timestamp manipulation → Cover-up attempt
5. All evidence correlates → Confirmed cyber-event

If trainees get stuck:

- Prompt them to check the ground_station_registry
- Suggest filtering by hash_verification_status
- Ask "What latitude should Arctic targets be at?"

Expected conclusion:

An adversary compromised ground station credentials and used SENTINEL-9 to conduct unauthorized intelligence collection of a contested region, while attempting to disguise the activity as routine maintenance and manipulate metadata to cover their tracks.