FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE 04 · MEETING MINUTES · SIMULATED RECORD

Module 04 Meeting Minutes Day 4, Incident Response Preparation

How the signatures were written, and what the coverage ratings admit

A simulated record from the course scenario. See the notice inside.

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 04 meeting minutes, Day 4, Incident Response Preparation
EDITION	Course reference copy · revised 2026-09-24
CONTACT	www.d2teamcorp.org

A SIMULATED RECORD · READ IT AS A TEMPLATE FOR YOUR OWN ORGANIZATION

These minutes are simulated. Kestrel Orbital and the people in this room are the course's teaching scenario. Every identifier, target, and source in these pages is transcribed from the module inventories; nothing is invented platform data. The deliberation is dramatized so you can watch the judgment, not just the output.

What to take away. As you read, ask how this meeting would run in your real organization: who would chair it, which departments must be in the room, what your gate would be, what evidence would settle a dispute, and who would own each decision when the meeting ends. The record format itself, gate, decisions, register, actions, scope, carried forward, is the reusable part. The platform is the example; the meeting discipline is the lesson.

In the classroom. The room opens these minutes after the slides and reads Item 01, Choosing a rule format the organization can live with; Item 03, Signature 01, and the argument about baselining people; Item 05, Signature 03, written against a source that does not exist yet: the rule, the objection, the decision and its owner, from the record rather than from the slide. Then the three questions on the judgment are asked.

Day 4, Incident Response Preparation · SCOR Minutes

HOW THE SIGNATURES WERE WRITTEN, AND WHAT THE COVERAGE RATINGS ADMIT

Two things make this meeting worth reading. The room chose a rule format for reasons it can defend years later, and it published coverage ratings that admit what the signatures cannot yet see.

FIELD	RECORD
Meeting	Day 4, Incident Response Preparation
Function	Function 04, Incident Response Preparation
Date	Thursday 06 August 2026
Location	Reston mission-operations centre, conference room 2, and Kiruna on link
Chair	You, Lead, Space Cybersecurity Operations and Resilience (SCOR)
Present	Maya Reyes (Security Operations Center); Theo Lindgren (Satellite Operations Center); Dana Whitfield (Satellite Design and Engineering)
Purpose	Write the detection signatures that fire on the Day 3 sources, and the response playbooks that run when they fire.
Output	Four AN-DET signatures with honest coverage ratings, and one playbook worked end to end.

The gate. A signature is accepted only if its **Target of Detection Method** observes the same elements the driving threat targets, and only if its coverage rating states any dependency it has. A rule that claims full coverage it does not have is worse than no rule.

01 DECISIONS TAKEN

01 Choosing a rule format the organization can live with

Maya Reyes · Analyst Lead, Security Operations Center
Proposed writing the signatures in the query language of the current security information and event management platform, because that is what the team knows.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Objected on lifecycle grounds. The platform will be replaced at some point and the rule portfolio would have to be rewritten from scratch.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Added the sharing argument. Kestrel has a Space ISAC obligation. A rule nobody else can run is a rule nobody else benefits from.

Maya Reyes · Analyst Lead, Security Operations Center
Proposed RootA on that basis: open and vendor neutral, a wrapper around whatever native query language the team already writes, with the ATT&CK techniques as a first-class field, translatable across systems.

RULING Detection signatures are authored in **RootA**. The native query stays in whatever dialect the team writes; the wrapper carries the name, severity, log source, ATT&CK techniques, references and the METEORSTORM tags. A platform migration becomes a translation pass rather than a rewrite.
Owner. Security Operations Center owns the rule portfolio and its format.

02 Signature 00, abuse of firmware push on the management plane

Maya Reyes · Analyst Lead, Security Operations Center
Wrote it against the Path 00 hooks: a firmware-push operation from the modem management interface outside a maintenance window, or following an authentication anomaly on the virtual private network appliance.

Theo Lindgren · Senior Controller, Satellite Operations Center
Confirmed maintenance windows are already published and enforced, so the outside-the-window condition is meaningful rather than theoretical.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Confirmed the deployment log and the execution log both exist and are retained.

RULING `AN:DET:Detection Signature:00` accepted at **full coverage**. Its Target of Detection Method names one element, the same one the driving threat named. The audit, deployment and execution records are the sources it fires on, not additional targets.
Owner. Security Operations Center, with Satellite Operations owning the maintenance-window discipline it depends on.

03 Signature 01, and the argument about baselining people

Maya Reyes · Analyst Lead, Security Operations Center
Proposed detecting commanding-workstation use outside the operator's normal hours, commands issued without peer-review tags, and sequences inconsistent with the active mission profile.

Theo Lindgren · Senior Controller, Satellite Operations Center
Objected, hard. He read the first condition as surveillance of his controllers and said he would not sign up to a rule that treats a night shift as suspicious.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Proposed the compromise. Baseline the role and the shift pattern, not the individual, and pair the rule with false positives written up front so an on-call analyst is not guessing.

Maya Reyes · Analyst Lead, Security Operations Center
Accepted and wrote the false positives into the rule itself: operator travel filed with notice, and authorized red-team exercise.

Theo Lindgren · Senior Controller, Satellite Operations Center
Agreed on that basis.

RULING `AN:DET:Detection Signature:01` accepted at **partial coverage**, because it depends on per-operator baselines that do not exist yet. The coverage rating states the dependency rather than claiming full. Known false positives ship with the rule.
Owner. Security Operations Center authors it. Satellite Operations owns the baselines and the peer-review tagging it relies on.

04 Signature 02, sustained noise-floor anomaly

Theo Lindgren · Senior Controller, Satellite Operations Center
Set the threshold discussion. Atmospheric events raise the noise floor routinely, so a rule that fires on any elevation will be ignored within a week.

Maya Reyes · Analyst Lead, Security Operations Center
Wrote it to require elevation beyond environmental thresholds sustained longer than an incidental event, using the tracking and telemetry noise-floor stream and the receiver telemetry.

RULING `AN:DET:Detection Signature:02` accepted at **full coverage**. Duration, not amplitude alone, is what separates interference from weather.
Owner. Security Operations Center, with Satellite Operations owning the environmental thresholds.

05 Signature 03, written against a source that does not exist yet

Maya Reyes · Analyst Lead, Security Operations Center
Wrote the rule as it should be: a firmware image whose measured hash does not match the signed expected value at boot or after an update.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Restated the Day 3 gap. Without measured boot there is no attestation to compare, so the rule is correct and currently unarmed.

Theo Lindgren · Senior Controller, Satellite Operations Center
Asked whether it should therefore be held back until the platform can feed it.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Ruled that it ships now with its coverage stated as dependent on measured boot. Writing the rule is what makes the missing capability visible as a cost rather than an abstraction.

RULING AN:DET:Detection Signature:03 accepted with coverage recorded as **dependent on measured boot, the declared Day 3 gap**. The rule is real, the source is not yet, and the document says so.
Owner. Security Operations Center authors it. Satellite Design and Engineering owns the missing capability.

06 Playbook 04, worked end to end

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Asked for one playbook worked fully, on the grounds that a signature with no response is an alert nobody can act on.

Theo Lindgren · Senior Controller, Satellite Operations Center
Chose Path 01, because it is the one where a controller has to act inside a pass.

Maya Reyes · Analyst Lead, Security Operations Center
Drafted the trigger and containment: suspend the operator credential on ground command authorization and fail commanding over to the second ground site.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Added recovery: rotate the access-control credentials, replay the command log against the flight plan, and confirm the vehicle state matches the last authorized command.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Added the reporting leg. Notify the duty officer and the chief information security officer, start the NIS2 clock at 24 hour early warning, 72 hour notification and one month final report, and prepare the redacted Space ISAC entry.

RULING Playbook PB-01 is accepted with its trigger and approved actions across all four stages, assess, contain, recover and report, each naming one executor and Mission Lead as the decider. The Kiruna failover in the containment stage is the reason Day 1 insisted on two ground segments rather than one, and it is the action that shows the split: Security Operations suspends the credential alone, Satellite Operations fails commanding over with a co-sign.
Owner. Satellite Operations runs it. Security Operations Center triggers it. SCOR owns the reporting leg.

02 DECISION REGISTER

ELEMENT	COVERS	COVERAGE	PLAYBOOK
AN:DET:Detection Signature:00	Attack Path 00	Full	PB-00
AN:DET:Detection Signature:01	Attack Path 01	Partial, depends on per-operator baselines	PB-01, worked in full
AN:DET:Detection Signature:02	Attack Path 02	Full	PB-02
AN:DET:Detection Signature:03	Attack Path 03	Dependent on measured boot, the declared Day 3 gap	PB-03

03 ACTIONS

ACTION	OWNER	DUE
Build per-role, per-shift baselines so Signature 01 can move off partial	Satellite Operations	Four weeks
Carry the measured-boot dependency into the resilience meeting	Satellite Design and Engineering	Day 5
Rehearse PB-01 against the digital twin before it is used live	Satellite Operations	Two weeks
Prepare the redacted Space ISAC entry template for the reporting leg	SCOR	Two weeks

Scope note. One playbook is worked end to end rather than four. The other three are paired to their signatures and scheduled. Working one fully in the room, with all three departments arguing over the containment step, taught more than four written alone afterwards, and the minutes record which is which.

04 CARRIED FORWARD

Function 05 looks across all four threads for the elements that keep reappearing, and builds the measures that shrink them. The measured-boot gap arrives there as a named debt.