FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE 03 · MEETING MINUTES · SIMULATED RECORD

Module 03 Meeting Minutes Day 3, Converged Detection Engineering

How each threat was traced to a path, and where the platform cannot see

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 03 meeting minutes, Day 3, Converged Detection Engineering
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, What a path has to prove; Item 06, Records and measurements do not line up; Item 05, Path 03, and the gap the room chose to declare: 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 3, Converged Detection Engineering · SCOR Minutes

HOW EACH THREAT WAS TRACED TO A PATH, AND WHERE THE PLATFORM CANNOT SEE

This is the meeting that turns four assertions into four routes a stranger can check. It is also the meeting where the room ran into the problem nobody solves by writing a better rule: the records live in one department's systems, the measurements live in another's, and nothing in either one points at the other. What the room decided about that is item 06, and it is the decision the rest of the week depends on.

FIELD	RECORD
Meeting	Day 3, Converged Detection Engineering
Function	Function 03, Converged Detection Engineering
Date	Wednesday 05 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	Trace how an adversary would move through the platform to realize each cataloged threat, and enumerate the data and signal sources needed to see each step.
Output	Four AN-ATT attack paths, twelve waypoints, and thirteen required sources: nine data, four signal, of which nine are unassessed, one partial and one a declared gap.

The gate. A path is accepted only if it names **one** target element, the same element the threat it realizes named, and only if it carries the sources a defensive cyber operator must hold to see it, each naming the one element it is collected from and its coverage state. Where a source does not exist, the path declares the gap rather than assuming the step is visible.

01 DECISIONS TAKEN

01 What a path has to prove

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Set the requirement. A path is not a story about an adversary. It is a sequence of named elements, and it is about exactly one of them: the Target of Exploitation the threat named yesterday.

Maya Reyes · Analyst Lead, Security Operations Center
Asked the obvious question. If the path is about the threat's target, does it have to end there?

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Ruled that it does not. The target says what the path is about; the objective says where the traversal lands. Path 00 is about ground command acceptance and ends on the patch deployment pipeline, and forcing those to be the same element would have meant writing a false route.

Maya Reyes · Analyst Lead, Security Operations Center
Added the detection requirement. A path nobody can see is not testable, so each path has to carry the sources a defensive cyber operator must already hold, or Function 04 has nothing to write a rule against.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Asked what happens when a step produces nothing to hold.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Ruled that the gap is written down as a gap. A path with an honest hole is more useful than a path with an invented sensor.

RULING Every path carries three waypoints, entry, pivot and objective, and names **one** target element, equal to the Target of Exploitation of the threat it realizes. The objective is where the traversal ends and is not required to be that element. Required sources are carried on the path, each naming the one element it is collected from and its coverage state.
Owner. Security Operations Center authors paths. SCOR holds the gate that the path's target equals the threat's target.

02 Path 00, mass modem firmware wipe through management-plane abuse

Maya Reyes · Analyst Lead, Security Operations Center
Walked the path: unexpected remote access reaching the management network, then an anomalous firmware push on the management plane, ending in mass terminal drop-off and firmware-hash mismatch.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Confirmed each waypoint maps to an enumerated element: ground crypto at entry, ground command acceptance at the pivot, the patch deployment pipeline as the objective.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Confirmed the anchor separately, because it is the field that joins the week. The path is about ground command acceptance, the same element Threat 00 named, which is what lets Day 4 and Day 5 attach to it without anyone re-deciding what the scenario was.

Maya Reyes · Analyst Lead, Security Operations Center
Recorded confidence as medium. KA-SAT is public, but the per-operator detail is not, so the middle of the path is reconstructed rather than observed.

RULING AN:ATT:Attack Path:00 is accepted with three waypoints, anchored to SVC:CP:Control Plane:09, and its required sources carried on the element: three required data sources and one required signal source, each naming the element it is collected from and its state. Confidence medium, with the reason recorded on the path rather than in a footnote. **Owner.** Security Operations Center. Satellite Design and Engineering confirms the element mapping.

03 Path 01, compromise of command authority

Theo Lindgren · Senior Controller, Satellite Operations Center
Walked this one himself, because it runs through his console. Entry is a console access anomaly, a new host or an off-hours sign-in. The pivot is anomalous use of command authority. The objective is an unauthorized or unreviewed command reaching the control plane.

Maya Reyes · Analyst Lead, Security Operations Center
Noted the awkward part: every one of those steps is a legitimate action performed at the wrong time or by the wrong person. There is no malicious binary to find.

Theo Lindgren · Senior Controller, Satellite Operations Center
Said that is exactly why it needs a path. If the model cannot describe it, the detection will never be written.

Maya Reyes · Analyst Lead, Security Operations Center
Flagged one source as partial rather than available. The command-authority record only carries the peer-review tag where the workflow has been adopted, and adoption is not complete, so the record exists but does not answer the question everywhere.

RULING AN:ATT:Attack Path:01 is accepted with three required data sources and **no signal sources at all**. The room records explicitly that this path has no malware artifact and nothing to measure in the physical layer, so detection has to be behavioral, which sets the constraint Function 04 inherits. The peer-review tag is recorded as partial, with the reason. **Owner.** Satellite Operations walks it, Security Operations Center authors it.

04 Path 02, sustained radio frequency noise injection

Theo Lindgren · Senior Controller, Satellite Operations Center
Described it from experience: a power spike on the uplink band, then a noise-floor anomaly across the link, ending in outage and loss of lock, sometimes timed to overhead passes.

Maya Reyes · Analyst Lead, Security Operations Center
Recorded this at high confidence. Radio frequency interference against satellite communications is well documented and what it does to the link is unambiguous.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Confirmed the hybrid services carrying received power and noise floor are the elements that would see it first, and the signal asset is where loss of lock shows.

Maya Reyes · Analyst Lead, Security Operations Center
Stopped on what this path does not have. It carries three signal sources and **not one data source**. Nothing in this path writes a log, so every tool her team runs today would show this platform as healthy right up to the outage.

Theo Lindgren · Senior Controller, Satellite Operations Center
Confirmed it from the other side. His controllers see it on a spectrum display, in a system her analysts do not have accounts on.

RULING `AN:ATT:Attack Path:02` is accepted at high confidence, with three required signal sources and no data sources. The absence is recorded as a property of the path, not an omission: this is the path that proves a record-only detection strategy would miss an entire class of attack on a space system.
Owner. Satellite Operations, with Security Operations Center authoring.

05 Path 03, and the gap the room chose to declare

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Walked the path: an anomalous update push through the thermal control service, a signed-manifest mismatch at the electrical power service, ending in a firmware-hash mismatch at boot on the on-board computer.

Maya Reyes · Analyst Lead, Security Operations Center
Stopped at the last waypoint and asked the question that mattered. Where does the boot hash come from?

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Answered honestly: the platform does not currently perform measured boot, so there is no attestation to compare against. The observable is correct in principle and unavailable in practice.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Ruled that the gap is declared on the path, not quietly dropped. It becomes a known limit that Function 04 must state and Function 05 must close.

RULING `AN:ATT:Attack Path:03` is accepted with a **declared gap** on its required boot-time measurement and attestation record: measured boot is not flown, so there is nothing to compare against. The gap is carried forward by name, with an owner.
Owner. Satellite Design and Engineering owns the gap and carries it to Day 5.

06 The part the room found hardest: records and measurements do not line up

Maya Reyes · Analyst Lead, Security Operations Center
Put the problem on the table with Path 00, because it is the only path in the set that needs both kinds of source at once. The firmware push leaves a record on the management plane. The consequence, tens of thousands of terminals dropping, is a measurement at the gateway. Nothing in either one names the other.

Theo Lindgren · Senior Controller, Satellite Operations Center
Said the practical version. His side sees carrier and demodulator lock as a continuous quantity sampled at the gateway. Her side sees discrete events written by whichever host produced them. There is no shared identifier, and asking his controllers to eyeball a spectrum display against her event list at three in the morning is not a detection strategy.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Added the time problem. The two sides do not share a clock discipline, and a record is stamped when the writing host says it happened, not when the effect appeared on the link. So the honest correlation is a window, not a match, and nobody had written down how wide.

Maya Reyes · Analyst Lead, Security Operations Center
Named the failure mode that follows. A fleet-wide loss of lock caused by wiped modems and one caused by weather look the same in the measurement. Only the record side separates them, and on this path that record sits on an element nobody has assessed yet.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Refused the tempting fix, which was to invent a correlation identifier and require every source to carry it. Nothing on this platform emits one today, so that would have produced a design nobody could implement and a coverage claim that was not true.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Ruled the approach instead. Correlate on the **element**, because the model already forces every source to name exactly one, so the element is the join and time is the filter applied after it, not the thing doing the joining.

Theo Lindgren · Senior Controller, Satellite Operations Center
Accepted on the condition that each source states the time base it is stamped in and the offset where it is known, so a window can be computed rather than argued about.

Maya Reyes · Analyst Lead, Security Operations Center
Asked for one more thing on paths that carry both kinds: name which record is expected to explain which measurement, so an analyst inherits the pairing instead of rediscovering it. On Path 00 that is the management-plane firmware-push record explaining the fleet-wide loss of lock at the gateway.

RULING Correlation is anchored on the **enumerated element**, not on a timestamp and not on an invented shared key. Three consequences are recorded. First, every required source names the one element it is collected from, and that element is the join. Second, each source states its time base and known offset, so cross-source comparison is a stated window rather than an assumption of simultaneity. Third, where a path carries both a data source and a signal source, the path names the expected pairing: on Path 00, `RDS:01`, the management-plane firmware-push record, is what explains `RSS:00`, fleet-wide loss of carrier and demodulator lock. Paths carrying only one kind say so, because it changes what Function 04 can write.
Owner. Security Operations Center owns the data sources. Satellite Operations owns the signal sources and the time bases. SCOR owns the pairing statements and reviews them at the Day 4 open.

07 What the tagged path actually buys, and what it costs

Maya Reyes · Analyst Lead, Security Operations Center
Said the benefit plainly, because the room had spent a day on it. Yesterday she had four targets and a paragraph each. Today she has four routes, each written as elements in order, which means she can hand one to somebody who has never seen this platform and they can check it step by step instead of believing her.

Theo Lindgren · Senior Controller, Satellite Operations Center
Gave the operational version. A route tells him which pass matters and which element to watch, which a threat name never did.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Gave the engineering version. A route ends on something she owns and can change, so the path is a work order rather than a warning.

Maya Reyes · Analyst Lead, Security Operations Center
Added the mechanical benefit. The analytic tag separates a route from the threat it realizes and the signature that

watches it, so three of us can work the same scenario at the same time without overwriting each other, and one query returns every path that crosses a control-plane service.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Named the external benefit and the entry condition together. The attack path is one of the element types the exchange memorandum approves for sharing, defined as a confirmed attack path for a converged space system, so confirmed is the condition of leaving the building. Unconfirmed work stays in the register. And the channel runs both ways: a path arriving in the same vocabulary is routed to whoever owns the element it names.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Recorded the cost, and asked that it not be buried. Writing routes this way produced thirteen required sources, and nine of them are marked unassessed. The method did not create those blind spots, it surfaced them, and now somebody has to answer for each one.

RULING The benefit is recorded on the register rather than asserted in prose: the path is checkable step by step, queryable by element, separable from the threat and the signature, and shareable once confirmed. The cost is recorded beside it: **thirteen required sources, of which nine are unassessed, one is partial and one is a declared gap**. Both go to Day 4 together.
Owner. SCOR. Security Operations Center holds the register.

08 Recording confidence rather than smoothing it

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Asked that confidence be written on every path, including where it is weak.

Maya Reyes · Analyst Lead, Security Operations Center
Agreed, and noted the professional reason. An analyst who inherits this map in six months needs to know which parts are evidence and which are inference.

Theo Lindgren · Senior Controller, Satellite Operations Center
Added the operational reason. A high-confidence path and a medium-confidence path do not deserve the same response posture.

RULING Every path carries a confidence rating and the reason for it. Three of the four are medium, and the minutes say so.
Owner. Security Operations Center.

02 DECISION REGISTER

ELEMENT	DRIVES FROM	ENTRY, PIVOT, OBJECTIVE	DATA, SIGNAL	CONFIDENCE
AN:ATT:Attack Path:00	Threat 00	Ground crypto, ground command acceptance, patch deployment pipeline	3 data, 1 signal, pairing named	Medium
AN:ATT:Attack Path:01	Threat 01	Console hardware, console software, console operations	3 data, 0 signal, 1 partial	Medium
AN:ATT:Attack Path:02	Threat 02	Error correction, tracking and telemetry, waveforms	0 data, 3 signal	High
AN:ATT:Attack Path:03	Threat 03	Thermal control, electrical power, on-board firmware	3 data, 0 signal, 1 gap	Medium, gap declared

03 ACTIONS

ACTION	OWNER	DUE
Declare the measured-boot gap on Path 03 and carry it by name	Satellite Design and Engineering	Day 4 and Day 5
Confirm each path names one target element, equal to the driving threat's target	SCOR	Day 3 close
Return a coverage state for every required source still marked unassessed, nine of thirteen, so the gaps are countable rather than assumed	Security Operations Center	Day 4 open
State the time base and known offset for every signal source, so a correlation window can be computed	Satellite Operations Center	Day 4 open
Write the expected record-to-measurement pairing on every path that carries both kinds	SCOR	Day 4 open
Give Security Operations read access to the gateway measurement streams, or state why not	Satellite Operations Center	Day 4
Record the behavioral-only constraint on Path 01, and the record-free constraint on Path 02, for the detection meeting	Security Operations Center	Day 4

Scope note. Four paths, one per threat, is deliberately one route each. A real adversary has more than one way to reach a target and a mature map carries several paths per threat. One per threat is enough to prove the method and to produce a first detection portfolio, and the room recorded that limit rather than implying the map is complete. The same honesty applies to the correlation decision in item 06: joining on the element is what this platform can do today with the sources it actually has. It is not a claim that record and measurement have been correlated, only that the model says where the join goes and who owes the missing halves.

04 CARRIED FORWARD

Function 04 writes the signatures that fire on these sources and the playbooks that run when they do. Three things travel with them and none may be quietly rounded up: the Path 03 gap, which has to appear in a coverage rating rather than in a footnote; the nine unassessed sources, which are the difference between a portfolio that fires and one that only reads well; and the pairing on Path 00, because a signature that watches the record without the measurement will not know the scale of what it has just caught.