FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE 02 · MEETING MINUTES · SIMULATED RECORD

Module 02 Meeting Minutes Day 2, Contextualized Threat Modeling

How four threats were chosen and anchored to real elements

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 02 meeting minutes, Day 2, Contextualized Threat Modeling
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, How the day was going to be run, agreed before any evidence was opened; Item 02, What counts as a threat we can act on; Item 04, Threat 01, compromise of command authority: 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 2, Contextualized Threat Modeling · SCOR Minutes

HOW FOUR THREATS WERE CHOSEN AND ANCHORED TO REAL ELEMENTS

The value of this meeting is not the four threats. It is that a threat can now be written down in a form the whole organization, and the wider sector, can act on. Yesterday gave the room a published taxonomy and a parented model of the telecommand path. Today that root does its first real work: every threat attaches to a named element, in a nomenclature that MISP already understands and the Space ISAC exchange already accepts. The room agreed the rule before it looked at any evidence, so the rule chose the set rather than the set choosing the rule. One working day, three departments in one room, and a deliberately small first pass whose job is to get the method running, not to survey the threat landscape.

FIELD	RECORD
Meeting	Day 2, Contextualized Threat Modeling
Function	Function 02, Contextualized Threat Modeling
Date	Tuesday 04 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	Anchor known adversarial threats to the specific enumerated elements they would target.
Output	Four AN-THR elements, each naming a Target of Exploitation from the Day 1 model.

The gate. A threat enters the catalogue only if its **Target of Exploitation** names **exactly one** element enumerated on Day 1. No target, no entry, and the exclusion is written down with its reason. This is what makes a threat catalogue reviewable instead of a reading list, and it is the same gate every later function inherits.

01 DECISIONS TAKEN

01 How the day was going to be run, agreed before any evidence was opened

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Opened by naming the constraint rather than discovering it at 16:00. One working day, and the mandates do not extend for a department that wants to be thorough. Asked the room to agree the method first and let the method decide the size of the set.

Maya Reyes · Analyst Lead, Security Operations Center
Pushed back on the day, not the method. Her open-source list ran to dozens of campaigns and she could defend most of them; working one day means most of that work does not land today.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Answered that the list is not lost, it is queued. What a day can buy is a method that holds, and a small set produced by it that the next pass extends. What a quarter buys is a longer document nobody has used yet.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Asked why all three departments had to sit through it rather than the Security Operations Center writing the catalogue and circulating it. Answered by working an example: intelligence names the behavior, operations knows what the platform does under load, engineering knows what is actually built. A threat none of the three can corroborate is not ready.

Theo Lindgren · Senior Controller, Satellite Operations Center
Agreed on the condition that the room records what was left out, so nobody later reads a short catalogue as a claim that the platform faces four threats.

RULING The day runs as a joint working session, and the method is agreed before the evidence is opened. The set is deliberately small: **the deliverable is the method running end to end**, not a survey of the threat landscape. Everything not enumerated today is held in the register with the reason recorded.
Owner. SCOR chairs. All three departments attend for the whole session.

02 What counts as a threat we can act on

Maya Reyes · Analyst Lead, Security Operations Center
Arrived with a long open-source list: dozens of reported campaigns against space and satellite communications operators.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Applied the gate before any of them were discussed. A threat that cannot name an element from yesterday's model is not a threat we can act on, it is background reading.

Maya Reyes · Analyst Lead, Security Operations Center
Accepted the gate and re-sorted the list against it. Most items did not survive, not because they are untrue, but because they target parts of the platform this pass has not enumerated.

Theo Lindgren · Senior Controller, Satellite Operations Center
Asked that the discarded items not be thrown away. They are the argument for widening the scope in the next pass.

RULING Four threats pass the gate on the telecommand path. Everything else is held in the open-source register against the parts of the platform not yet enumerated. Each surviving threat names its Target of Exploitation in enumerated identifiers, not in prose.
Owner. Security Operations Center owns the threat register. SCOR owns the gate.

03 Threat 00, intrusion into the satellite communications management network

Maya Reyes · Analyst Lead, Security Operations Center
Presented the KA-SAT case from February 2022 and AcidRain, the wiper it ended with: an actor reached the management network, abused the provider-to-customer trust relationship and pushed a malicious modem update that disabled tens of thousands of terminals across Europe.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Challenged the relevance. Kestrel's modems are not that vendor's modems, so the specific exploit does not transfer.

Maya Reyes · Analyst Lead, Security Operations Center
Answered that the modem was not the target. The trust relationship was. Kestrel has the same relationship, a patch pipeline that is trusted by everything downstream of it.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Withdrew the objection and confirmed the pipeline is enumerated as `SVC:CP:Control Plane:12` with staged binaries at `AST:DA:Data:02`.

RULING `AN:THR:Threat:00` enters the catalogue. Target of Exploitation names ground crypto and ground access control, the patch pipeline software and the staged patch binaries. Recorded as the highest-impact ground threat in the pass.
Owner. Security Operations Center authors it. Satellite Design and Engineering confirms the target elements.

04 Threat 01, compromise of command authority

Maya Reyes · Analyst Lead, Security Operations Center
Raised the case where an adversary holds valid command authority, whether stolen or coerced, and issues unauthorized telecommands.

Theo Lindgren · Senior Controller, Satellite Operations Center
Was uncomfortable. His controllers are the people this describes, and he said so plainly: this reads as an accusation against my team.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)
Reframed it. The threat is against the authority, not against the person holding it. A model that cannot describe misuse of a valid credential cannot protect the operator who is impersonated.

Theo Lindgren · Senior Controller, Satellite Operations Center
Accepted on that basis and asked that the eventual control be built so it protects controllers rather than watching them.

RULING AN:THR:Threat:01 enters the catalogue, targeting ground access control and console operations together with the console hardware and software. Theo's condition is recorded and carried to Function 05.
Owner. Security Operations Center authors it. Satellite Operations holds the condition on how it is countered.

05 Threat 02, sustained jamming

Theo Lindgren · Senior Controller, Satellite Operations Center
Raised it as the threat his controllers have actually seen. Radio frequency interference against satellite communications is routine, documented and does not require a sophisticated actor.

Maya Reyes · Analyst Lead, Security Operations Center
Agreed and noted this is the one item on the list with high confidence rather than medium.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Confirmed the affected elements are the link access control, the forward error correction and error-correcting code service, the tracking and telemetry service and the waveforms themselves.

RULING AN:THR:Threat:02 enters the catalogue targeting the link services and AST:SI:Signal:00. Recorded at high confidence, which is unusual in this set and is stated rather than smoothed over.
Owner. Satellite Operations raises it, Security Operations Center authors it.

06 Threat 03, malicious firmware update on orbit

Dana Whitfield · Systems Engineer, Satellite Design and Engineering
Raised the one that worries engineering most. The update path is the road to the satellite. An adversary who subverts the flight-software supply chain does not need to break anything on the ground, because the platform will install the payload itself.

Theo Lindgren · Senior Controller, Satellite Operations Center
Noted the operational consequence: a bad firmware image on orbit is not something a controller can simply undo on the next pass.

Maya Reyes · Analyst Lead, Security Operations Center
Confirmed there is no publicly disclosed on-orbit case, so this is recorded at medium confidence on technical grounds rather than incident evidence.

RULING AN:THR:Threat:03 enters the catalogue targeting the thermal control and electrical power services and the on-board computer and repeater firmware. Confidence recorded as medium, with the reason stated.
Owner. Satellite Design and Engineering raises it, Security Operations Center authors it.

07 Why one ordinal carries the whole chain

Theo Lindgren · Senior Controller, Satellite Operations Center
Asked why the four threats are not simply numbered one to four.

Maya Reyes · Analyst Lead, Security Operations Center
Explained that the ordinals come from the Security Operations Center's running threat register, which is one sequence across every threat the organization tracks, not a per-project count.

You · Lead, Space Cybersecurity Operations and Resilience (SCOR)

Ruled that they stay as issued. Renumbering to make a document look tidy would break every reference from this meeting onward, and the gaps are informative: they are the threats that did not pass the gate.

RULING Ordinals are register-issued and are never renumbered. This register opened this week, so the first four it issues read 00 to 03. The same number then carries the scenario into the attack path, the signature and the measure, and an ordinal issued once is never renumbered.
Owner. Security Operations Center owns the register and issues ordinals.

02 DECISION REGISTER

ELEMENT	THREAT	TARGET OF EXPLOITATION, ONE ELEMENT	CONFIDENCE
AN:THR:Threat:00	SATCOM management-network intrusion	SVC:CP:Control Plane:09, ground command acceptance	Medium
AN:THR:Threat:01	Command-authority compromise	AST:SW:Software:04, the operations console software	Medium
AN:THR:Threat:02	Jamming campaign	AST:SI:Signal:00, the telecommand uplink waveform	High
AN:THR:Threat:03	Malicious on-orbit firmware update	AST:FW:Firmware:01, the on-board computer boot firmware	Medium

03 ACTIONS

ACTION	OWNER	DUE
Hold the discarded open-source items against the unenumerated scope	Security Operations Center	Rolling
Confirm every named target element exists in the Day 1 inventory	SCOR	Before Day 3
Carry Theo's condition on Threat 01 to the resilience meeting	SCOR	Day 5
Record confidence and source for each threat, including where evidence is absent	Security Operations Center	Day 2 close

Scope note. Four threats is not the threat landscape, and nobody in the room pretended otherwise. Three things bound this set, and all three were chosen rather than suffered. **One working day.** The mandates carry clocks and a department that spends a quarter cataloguing has delivered nothing; a day buys a working method and a set the next pass extends. **Three departments at one table.** Security Operations holds the intelligence, Satellite Operations knows what the platform does under load, and Satellite Design and Engineering knows what is actually built, so a threat none of them can corroborate is not ready to enter. That is slower than one analyst writing alone, and it is the reason each entry survives challenge. **A first pass whose job is the method.** The set is small on purpose, because the point of Day 2 is to prove that a threat can be anchored, tagged and shared at all, not to be exhaustive. Threats against parts of the platform not yet enumerated are held in the register, not dismissed, and enter when their elements do. Four entries that name their target beat forty that nobody can act on, and the forty are still there when the model grows.

04 CARRIED FORWARD

Function 03 has to show how an adversary would actually reach each of these targets. A threat without a path is an assertion, and the same ordinal carries the work forward, so tomorrow extends today rather than restarting it.