

FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE 05 • MEETING MINUTES • SIMULATED RECORD

Module 05 Meeting Minutes

Day 5, Adversary Management

How the week's findings became four funded measures

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

COPYRIGHT AND LEGAL NOTICES

© 2026 D2 Team CORP, a 501(c)(3) nonprofit. All rights reserved.

TLP:AMBER. Limited disclosure. Recipients may share this document only within their own organization and its clients, on a need-to-know basis, and only to the extent necessary to act on the information.

This document is part of the Full Spectrum Space Cybersecurity Professional program. It is provided to enrolled learners and to the credentialing bodies it is submitted to. Redistribution outside the cohort and those bodies is not authorized.

Verbatim sources. Every taxonomy definition in this document is the published METEORSTORM taxonomy text, quoted exactly. Definitions are never abbreviated, paraphrased, or reworded in this publication.

Trademarks. ethicallyHackingspace (eHs)® is a brand of D2 Team CORP, not a separate legal entity. Other names appearing in this document are the property of their respective owners and are used for identification only.

No warranty. This publication is provided for education. It is not legal, regulatory, or engineering advice for any specific system.

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 05 meeting minutes, Day 5, Adversary Management
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 resilience measure has to name; Item 03, Measure 01, dual-control commanding, and the cost of it; Item 05, Measure 03, and closing the gap the week has been carrying: 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 5, Adversary Management · SCOR Minutes

HOW THE WEEK'S FINDINGS BECAME FOUR FUNDED MEASURES

This is the meeting where the week pays off. The clearest moment in it is Measure 03: a detection gap that Dana declared on Wednesday, rather than hiding, becomes a funded engineering program on Friday.

FIELD	RECORD
Meeting	Day 5, Adversary Management
Function	Function 05, Adversary Management
Date	Friday 07 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	Find the platform elements that recur across the threats and paths, and build measures that shrink, harden or remove them.
Output	Four AN-RES measures, each with a target, an objective and a named owner.

The gate. A measure is accepted only if its **Target of Resilience Enhancement** names the same elements the threat it counters targets, if it names one objective from NIST SP 800-160 volume 2, and if it has a named owner. No target, no objective or no owner means no measure.

01 DECISIONS TAKEN

01 What a resilience measure has to name

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

Set the gate. A measure that does not name the element it protects is a budget line, not a control. It must name its Target of Resilience Enhancement, and that target must be the same element the threat targets.

Maya Reyes · Analyst Lead, Security Operations Center

Added a second requirement: each measure names which of the four objectives from NIST SP 800-160 volume 2 it serves, anticipate, withstand, recover or adapt. Otherwise every measure gets described as making us more secure.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Asked that ownership be explicit, including where it is shared, because a control owned by everyone is owned by nobody.

RULING Every measure names its target elements, the path it counters, one objective, and a named owner. Where ownership is genuinely shared the split is written out rather than left as both.

Owner. SCOR holds the gate. Each measure has a departmental owner.

02 Measure 00, zero-trust segmentation of the device management plane

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Proposed segmenting the device management plane from external networks, requiring hardware-rooted attestation for any access to it, and gating firmware pushes behind a dual-approval workflow inside a maintenance window.

Theo Lindgren · Senior Controller, Satellite Operations Center

Accepted the maintenance-window enforcement but warned it removes the ability to push an emergency fix at will, and asked that the emergency path be designed rather than left as an exception people will invent under pressure.

Maya Reyes · Analyst Lead, Security Operations Center

Noted that this measure removes the highest-impact ground path entirely rather than making it easier to spot.

RULING **AN:RES:Resilience Measure:00** accepted against Attack Path 00. Objective: **anticipate**, because it raises the barrier to management-plane access rather than waiting to detect the abuse. Theo's emergency-path condition is recorded as a design requirement.

Owner. Shared. Satellite Design and Engineering owns the segmentation and dual-approval rebuild; Satellite Operations owns the maintenance-window discipline.

03 Measure 01, dual-control commanding, and the cost of it

Maya Reyes · Analyst Lead, Security Operations Center

Proposed that high-impact commands require a second operator to approve before transmission.

Theo Lindgren · Senior Controller, Satellite Operations Center

Objected on timing. A pass is a fixed window. A second approver who is not at the console when the window opens means a missed pass, and a missed pass has its own operational cost.

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

Held the line on the principle and moved on the implementation. Dual control applies to high-impact actions only, not to every command, and the pre-pass briefing puts the second approver in the room before the window opens.

Theo Lindgren · Senior Controller, Satellite Operations Center

Accepted, and noted this is the control he asked for on Day 2: it protects the controller who is impersonated rather than watching the controller who is not.

RULING **AN:RES:Resilience Measure:01** accepted against Attack Path 01. Objective: **withstand**, because a single insider cannot act alone on a high-impact sequence. Per-operator behavior baselines and pre-pass briefings make out-of-pattern actions visible.

Owner. Shared. Satellite Design and Engineering owns the dual-control workflow in the commanding software; Satellite Operations owns the peer-review discipline.

04 Measure 02, frequency-agile link with a backup band

Theo Lindgren · Senior Controller, Satellite Operations Center

Proposed automatic band switching when the noise floor exceeds threshold, so a pass survives interference instead of being lost to it.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Accepted ownership of the frequency-agile waveform and flagged that it is the longest lead item in the set.

Maya Reyes · Analyst Lead, Security Operations Center

Noted the detection interaction: Signature 02 still has to fire, because switching bands silently would hide a sustained campaign from the analysts.

RULING **AN:RES:Resilience Measure:02** accepted against Attack Path 02. Objective: **withstand**, because communications continue under sustained interference. Band switching raises an alert; it does not suppress one.

Owner. Shared. Satellite Design and Engineering owns the agility waveform; Satellite Operations owns the switching procedure.

05 Measure 03, and closing the gap the week has been carrying

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Proposed measured-boot firmware attestation with a signed vendor manifest, supply-chain provenance verification at integration, and quarantine of any component whose hash does not match.

Maya Reyes · Analyst Lead, Security Operations Center

Pointed out what this does beyond the threat. It is the missing source from Day 3 and the dependency on Day 4. Building it arms a signature that has been written but unarmed all week.

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

Recorded that as the clearest demonstration of the method in the whole week. A gap declared honestly on Wednesday became a funded measure on Friday, because it was named rather than hidden.

Theo Lindgren · Senior Controller, Satellite Operations Center

Asked that it be validated on the digital twin before it goes near the flying platform.

RULING AN:RES:Resilience Measure:03 accepted against Attack Path 03. Objective: **anticipate**, because tampered firmware never reaches an operational role. It closes the Day 3 detection gap and upgrades the coverage of Signature 03.

Owner. Satellite Design and Engineering owns the measured-boot architecture, the signing pipeline and supply-chain verification.

06 Validate on the twin before the platform

Theo Lindgren · Senior Controller, Satellite Operations Center

Insisted that nothing in this set touches the flying platform until it has been applied to the digital twin and the second-order effects observed.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Agreed and listed what the twin has to show: mission capability, duty cycle, downlink margin and power budget.

Maya Reyes · Analyst Lead, Security Operations Center

Added that the Day 3 paths should be replayed against the twin with each measure in place, to see how far an adversary still gets and whether the Day 4 detections still fire.

RULING Every measure is validated on the digital twin before it reaches the operational platform, and each attack path is replayed against the twin with the measure applied. Decisions move from opinion to evidence.

Owner. Satellite Operations runs the twin campaigns. Security Operations Center confirms detections still fire.

07 What the week actually bought

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

Closed the week by naming the point. The four measures do not make Kestrel unbreakable. They make the platform expensive to attack, and they make the three departments describe it the same way while doing it.

Maya Reyes · Analyst Lead, Security Operations Center

Noted that the adversary now has to beat three departments who know the platform better than they do, which is the first point of the Pentagon of Pain.

Theo Lindgren · Senior Controller, Satellite Operations Center

Noted the operational version: the paths that remain are slower, noisier and harder to finish inside a pass.

Dana Whitfield · Systems Engineer, Satellite Design and Engineering

Noted the engineering version: two of the four measures remove a path rather than detect it.

RULING Week one closes with four threats anchored, four paths mapped, four signatures written, one playbook worked and four measures funded, all tied to the same 44 enumerated elements. The mindset is what changed; the framework is what made it repeatable.

Owner. SCOR. The same procedure runs on the next scope.

02 DECISION REGISTER

ELEMENT	COUNTERS	OBJECTIVE	OWNER
AN:RES:Resilience Measure:00	Attack Path 00	Anticipate	Shared, Engineering and Operations
AN:RES:Resilience Measure:01	Attack Path 01	Withstand	Shared, Engineering and Operations
AN:RES:Resilience Measure:02	Attack Path 02	Withstand	Shared, Engineering and Operations
AN:RES:Resilience Measure:03	Attack Path 03	Anticipate	Satellite Design and Engineering

03 ACTIONS

ACTION	OWNER	DUE
Design the emergency firmware-push path rather than leaving it as an exception	Satellite Design and Engineering	Four weeks
Stand up measured boot and re-rate the coverage of Signature 03	Satellite Design and Engineering	Program, quarterly review
Validate all four measures on the digital twin before the platform	Satellite Operations	Before any live change
Replay each Day 3 path against the twin with the measure applied	Security Operations Center	With each validation
Open the next enumeration scope from the Day 1 backlog	SCOR	Week two

Scope note. Four measures against four paths is one countermeasure per path. A mature program layers several and accepts that some paths are reduced rather than removed. Two of these four remove a path outright and two make it survivable, and the minutes say which is which instead of implying all four are equally strong.

04 CARRIED FORWARD

Week two reopens Function 01 on the next scope from the Day 1 backlog. The procedure does not change; only the part of the platform it runs on does.