

FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

Module 05

Adversary Management

Question set

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 Adversary Management, question set, student edition
EDITION	Student edition · revised 2026-09-24
CONTACT	www.d2teamcorp.org

SCOPE AND STANDING OF THIS WORK · READ BEFORE JUDGING THE ENUMERATION

What this is. Kestrel Orbital's first application of the METEORSTORM framework, produced by three departments who had never used it before, in five working days. It is a deliberately scoped first pass over the telecommand path: the command-and-control chain from the operator console to execution on orbit.

Why that scope, and not more. The mandates chose it. Executive Order 14144 puts the command and control of an operational platform first, and the NIS2 Directive places a duty of care and a reporting clock on the ground operator. The fleet is already flying, so the first pass ran on the part that would end the mission if an adversary took it. Enumerating everything else first would have been thorough and useless.

What it is not, stated plainly. It is not an exhaustive model of the platform and does not claim to be. Elements off the telecommand path are not enumerated. Some assets group several physical units where those units share an owner, a build and a patch path. Gaps in the ordinal sequence mark elements the register tracks outside this scope. Every one of those is a recorded decision taken at the enumeration meeting, not an oversight discovered later.

How it grows. Ordinals are issued once and never renumbered, so everything enumerated here keeps its identifier as the register expands. The same eight-step procedure runs on the next scope, and the one after that. A first pass that names its boundary can be extended. One that hides its boundary has to be rebuilt.

The standard we hold ourselves to. A scope choice is stated openly. A defect is fixed, never narrated. If you find an element misnamed, a parent wrong, or a count that does not add up, that is a defect and we want to hear about it. If you find something outside the telecommand path missing, that is the scope, it was chosen deliberately, and it is on the roadmap. The two are not the same criticism, and this work is built so you can tell them apart.

Contents

- 01 QS Question Set
- 02 KEY Answer Key

QS

Question Set

Every checkpoint question for this module, 18 in all, with its options. Three are worked and marked in the classroom; the rest are yours to work on your own. Answer each one before opening the key, and if your answer differs, trace which chapter rule it breaks before reading the reason.

Day 5 context checkpoint

Q1 Day 5 context checkpoint worked in the classroom

What have Days 1 through 4 accumulated that Day 5 acts on?

- a. The Day-1 CONOPS on its own, with none of the analytic elements attached to it
- b. The CONOPS, the threat set, the attack-path map, and the detection set
- c. The detection set alone, since it is the most recent deliverable of the week
- d. The threat set and the detections, but not the structural model underneath

Q2 Day 5 context checkpoint

What is your job on Day 5?

- a. Re-decompose the platform against everything the week's work has now accumulated
- b. Write further detection signatures for the path steps that remain uncovered
- c. Find the parts that recur across threats and paths, and shrink or harden them
- d. Re-anchor each catalogued threat to the elements the new detections observe

Q3 Day 5 context checkpoint

Which departments share Day 5's working session?

- a. Satellite Operations and Satellite Design and Engineering
- b. The Security Operations Center on its own, as on Day 4
- c. Satellite Design and Engineering with the Security Operations Center
- d. All three departments, with the SOC leading as on Day 2

Q4 Day 5 context checkpoint worked in the classroom

Why is Day 5 the right time to remove attack surface, and not earlier?

- a. Because hardening always follows detection in the framework's fixed order of work
- b. Because the NIS2 continuity duties only take effect once the detections are running
- c. Because the digital twin is unavailable until the full detection set has been written
- d. Because only now do you know which elements recur across the week's findings

Q5 Day 5 context checkpoint

A proposed change hardens an element that no threat or path touches. How should you weigh it?

- a. Top priority, since an unmodeled element is the least understood on the whole platform
- b. Low priority: with nothing modeled against it, the change buys little resilience
- c. It must run first, to close the exposure before any adversary can reach it
- d. It replaces the detection currently covering the nearest modeled element

Adversary management method checkpoint

Q6 Adversary management method checkpoint

In which layer does an AN-RES element sit, and what is its TAG?

- a. The Segment layer; TAG SEG
- b. The Asset layer; TAG AST
- c. The Analytic layer; TAG RES
- d. The Service layer; TAG SVC

Q7 Adversary management method checkpoint

The TRE field holds exactly one enumerated platform element. Which element is it?

- a. The element the AN-THR this measure counters already names as its TOE
- b. The element at the deepest point the measure's protection reaches
- c. The element the department that owns the measure is responsible for
- d. The element the measure's resiliency goal is assigned against

Q8 Adversary management method checkpoint

The four cyber resiliency goals, per NIST SP 800-160 v2, are:

- a. Detect, Deny, Disrupt, Deceive
- b. Plan, Do, Check, Act
- c. Confidentiality, Integrity, Availability, Safety
- d. Anticipate, Withstand, Recover, Adapt

Q9 Adversary management method checkpoint

What role does the digital twin play in Day 5?

- a. It replaces the CONOPS as the shared model once measures are written
- b. It is the test bench where a measure is tried before it touches the platform
- c. It generates the adversary scenarios the threat set is drawn from
- d. It records which department owns each measure after acceptance

Q10 Adversary management method checkpoint

The element a measure protects is fixed for its service life. What does that make the measure?

- a. A requirement for the next build, not a control installed on what is flying
- b. A detection signature, since only observation is possible on a fixed element
- c. Invalid, because a measure must be installable on the element it protects
- d. Unchanged, since where the element sits in its life does not reach the measure

Q11 Adversary management method checkpoint

A measure's cadence is recorded as phased rather than in force. What must the entry also carry?

- a. A second ordinal, so the two halves can be tracked as separate work
- b. A compensating control or a recorded residual risk with its owner
- c. A waiver from the department that cannot deliver its half this year
- d. Nothing further, because phased is a complete statement on its own

Q12 Adversary management method checkpoint worked in the classroom

What must an AN-RES anchor to before its logic is written?

- a. The threat actor the measure is intended to frustrate
- b. The attack path whose objective the measure removes
- c. A structural element, named in the TRE field
- d. The resiliency goal the measure is assigned

Resilience catalogue checkpoint

Q13 Resilience catalogue checkpoint

How large is the Day-5 resilience set?

- a. 44 measures, one for every element enumerated in the Day-1 CONOPS
- b. Four resilience measures, one countering each attack path
- c. 5 measures, one for each resiliency goal plus a spare
- d. 10 measures, spread evenly across the enumerated segments

Q14 Resilience catalogue checkpoint

How does a resilience measure reduce attack surface?

- a. By adding a further alert on the element the adversary keeps relying on
- b. By enumerating an additional threat against that same platform element
- c. By re-decomposing the platform around the exposure that keeps recurring
- d. By shrinking, hardening or removing that element, or hardening the path to it

Q15 Resilience catalogue checkpoint

AN:RES:Resilience Measure:03 specifies attestation at integration, and the firmware it protects is already in orbit. What does the entry record?

- a. Cadence next-build, plus a compensating control and a residual risk
- b. Cadence in-force, since the measure is written, owned and specified
- c. Nothing extra: it counters path 03, so the exposure reads as covered
- d. A second TRE naming the ground element the interim control is applied to

Q16 Resilience catalogue checkpoint

Completing the resilience set finishes what?

- a. The five-function METEORSTORM week: CONOPS, threats, paths, detections, resilience
- b. Adversary management alone, which stands apart from the four functions before it
- c. The Day-1 decomposition, which these resilience measures finally bring to completion
- d. The intel briefing cycle that the Security Operations Center opened back on Day 2

Q17 Resilience catalogue checkpoint

Why does anchoring every measure to an element matter to the departments?

- a. It sets the order in which the measures are implemented before the next launch
- b. It satisfies the element-citation requirement that NIST SP 800-160 v2 imposes
- c. Each department sees which part changes and who owns the change
- d. It lets the measure cross to Space ISAC with no redaction step required

Q18 Resilience catalogue checkpoint

AN:THR:Threat:00, AN:ATT:Attack Path:00, AN:DET:Detection Signature:00, and AN:RES:Resilience Measure:00 all share an ordinal. What does that chain tell you?

- a. Ordinal 00 recurs at every layer because the running register restarts at the top of each working day
- b. Threat, path, signature, and measure share ordinal 00: one exposure, traced from Function 02 to Function 05
- c. Only the detection and the measure share an ordinal, because threats and paths are numbered on a separate register
- d. The shared ordinal marks those four analytic elements as belonging to the Ground segment of the platform

WORK EVERY QUESTION BEFORE YOU READ ON. THE ANSWERS BEGIN ON THE NEXT
PAGE.

KEY Answer Key

The answer with the reason it is the answer. If yours differs, trace which chapter rule it breaks before reading on.

Q1

b. The CONOPS, the threat set, the attack-path map, and the detection set

Day 5 stands on all four prior outputs: the 44-element CONOPS, 4 AN-THR threats, 4 AN-ATT paths, and 4 AN-DET detections.

Q2

c. Find the parts that recur across threats and paths, and shrink or harden them Adversary management reduces attack surface by targeting the elements the adversary keeps relying on, before launch.

Q3

a. Satellite Operations and Satellite Design and Engineering Day 5 runs with Satellite Operations and Satellite Design & Engineering, the teams who operate the platform and own its design changes.

Q4

d. Because only now do you know which elements recur across the week's findings Only after threats, paths, and detections are enumerated can you see which elements the adversary leans on repeatedly, and target those.

Q5

b. Low priority: with nothing modeled against it, the change buys little resilience Resilience effort follows the evidence; an element with no threat or path behind it yields little return compared with the recurring ones.

Q6

c. The Analytic layer; TAG RES AN-RES is an analytic-layer element with TAG RES, the fifth analytic category alongside THR, ATT, and DET.

Q7

a. The element the AN-THR this measure counters already names as its TOE TRE (Target of Resilience Enhancement) is inherited, not chosen: the measure names the same element the threat it counters named, so threat, path, signature, and measure all point at one thing. The wider chain the protection touches is description, never a second target.

Q8

d. Anticipate, Withstand, Recover, Adapt Every AN-RES maps to one of the four goals, Anticipate, Withstand, Recover, Adapt, from NIST SP 800-160 v2.

Q9

b. It is the test bench where a measure is tried before it touches the platform The digital twin is a test bench: measures are validated against a model of the platform before launch, so changes are proven safe first.

Q10

a. A requirement for the next build, not a control installed on what is flying The lifecycle test decides what the measure can be. Reachable means apply it to the element directly. Through means protect the element with a compensating control on the path to it. Fixed means the measure is a requirement for the next build and cannot be installed on what is flying.

Q11

b. A compensating control or a recorded residual risk with its owner Anything not in force must name the interim control or the residual risk with its owner. Coverage you cannot install is not coverage, and an entry that reads as covered while nothing is installed is worse than one that admits the gap.

Q12

c. A structural element, named in the TRE field As with every analytic element, you anchor first: name the structural element the measure protects, then write what it does.

Q13

b. Four resilience measures, one countering each attack path The week closes with four resilience measures, each anchored to one platform element and countering one of the four attack paths.

Q14

d. By shrinking, hardening or removing that element, or hardening the path to it Each measure targets a recurring element. Where the element can be changed, the measure shrinks, hardens or removes it. Where it cannot, because it is flying and fixed for its service life, the measure becomes a compensating control on the path the adversary has to cross, and the entry records the residual risk that remains.

Q15

a. Cadence next-build, plus a compensating control and a residual risk Integration happened before launch, so the measure cannot be installed on the element it protects. Lifecycle fixed, cadence next-build. The entry therefore carries a ground-side compensating control on the patch pipeline and a residual risk owned by Satellite Design & Engineering, and the TRE still holds exactly one element.

Q16

a. The five-function METEORSTORM week: CONOPS, threats, paths, detections, resilience AN-RES is the fifth and final function's output; with it the platform is described once and defended across all five functions.

Q17

c. Each department sees which part changes and who owns the change Because each AN-RES names its element via TRE, Operations and Engineering read the same anchor and know precisely what is being hardened and by whom.

Q18

b. Threat, path, signature, and measure share ordinal 00: one exposure, traced from Function 02 to Function 05 One exposure, followed end to end: the threat named SVC:CP:Control Plane:09, the path walked to it, the signature watches it, and the measure hardens it. All four name that one element, and ordinal 00 is issued once and never renumbered, which is what makes the chain followable without a cross-reference table.