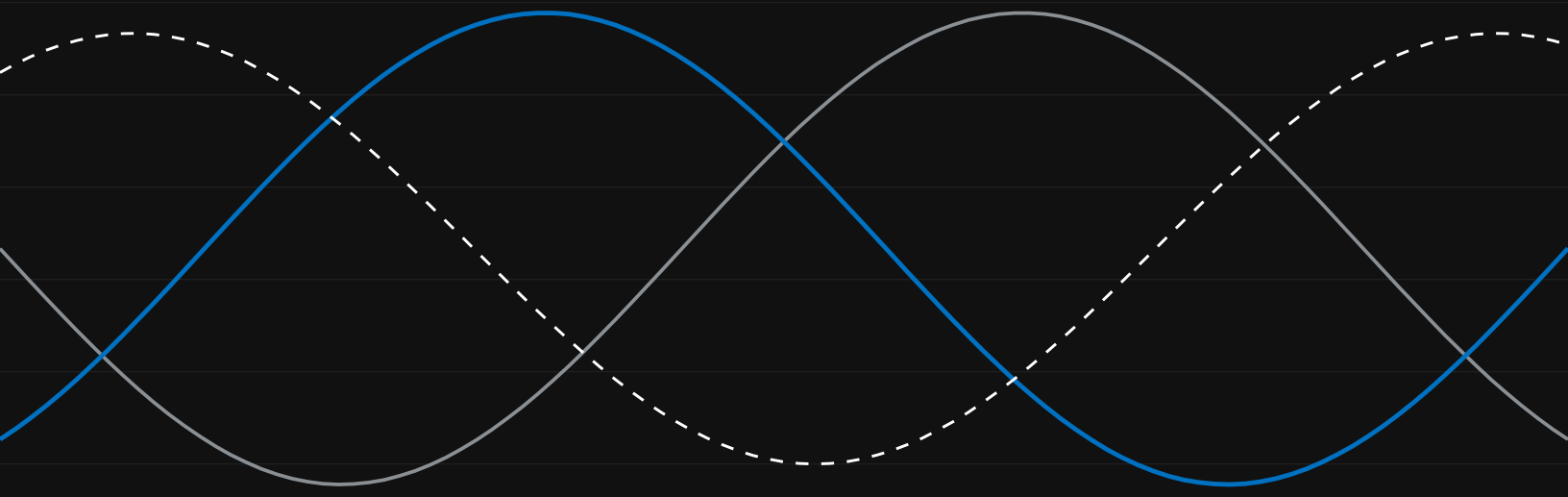
Module 05 · Question set · Student edition

Adversary Management

Every checkpoint question for Module 05, with the answer key.



ethicallyHackingspace (eHs)®
TLP:AMBER

Copyright and legal notices

© 2026 ethicallyHackingspace (eHs)®. All rights reserved.

> **Printing.** To save toner, print from page 2. The cover is a dark full-page plate and carries nothing the pages after it do not.

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. Sharing beyond what that marking permits, and any resale, is not authorized.

Verbatim sources. Every taxonomy definition quoted in this document is the published METEORSTORM taxonomy text, quoted exactly and never abbreviated, paraphrased or reworded. Where the course explains an element in its own words, the explanation is not presented as the definition. One typographical error in the published file, a doubled period, is corrected.

Trademarks. ethicallyHackingspace (eHs)® is the copyright holder of this publication; D2 Team CORP is its publisher. 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 2026-11-19
Contact	www.d2teamcorp.org

What this document is and how to use it

What it is. The checkpoint questions for Module 05, Adversary Management, each with four options, followed by the answer key. Every question is about Kestrel Orbital, the fictional satellite operator this course uses as its example.

How to use it. Tick one option for each question, with the Module 05 workbook beside you, before you open the key. The key repeats each question, so it can be read on its own.

What goes with it. The questions test the method the workbook teaches. Blank record sheets, for your own use, are in the METEORSTORM desk pack on the course downloads page.

Contents

QS **Question Set** 4

Module 05 context checkpoint 4

Adversary management method checkpoint 5

Resilience catalog checkpoint 7

KEY **Answer Key** 9

© 2026 ethicallyHackingspace (eHs)®

QS Question Set

Every checkpoint question for this module, 19 in all, with its options. Answer each one before opening the key, and if your answer differs, trace which chapter rule it breaks before reading the reason.

Module 05 context checkpoint

Q1 Module 05 context checkpoint

Counted across the four attack paths, one element appears in two of them: SVC:CP:Control Plane:09, on Path 00 and Path 01. Every other element appears in one. What does that count tell you to do?

- ☐ **a.** Protect AST:FW:Firmware:01 first, since it carries the gap declared on Day 3
- ☐ **b.** Hold every measure back until a later pass finds more elements that recur
- ☐ **c.** Write one measure for chains 00 and 01 whose TRE names both anchors, since the paths meet
- ☐ **d.** Put SVC:CP:Control Plane:09 first, keep one measure per anchor, and rerun the count

Q2 Module 05 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 cataloged threat to the elements the new detections observe

Q3 Module 05 context checkpoint

Which two departments hold the pen together on Day 5?

- ☐ **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.** SCOR and the Security Operations Center, as on Day 2

© 2026 ethicallyHackingspace (eHs)®

Q4 Module 05 context checkpoint

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 Module 05 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 running
- ☐ **d.** The element the measure's resiliency goal is assigned against

© 2026 ethicallyHackingspace (eHs)®

Q8 Adversary management method checkpoint

Measure 01 puts a second approver on every high-impact command, so one compromised credential cannot release a high-impact sequence alone. Which one goal does it serve?

- ☐ **a.** Anticipate, because it stops the credential from being stolen in the first place
- ☐ **b.** Withstand, because high-impact commanding continues safely while a credential is compromised
- ☐ **c.** Recover, because it restores a known-good command state after the compromise
- ☐ **d.** Adapt, because it changes the platform so the same path cannot work twice

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 records which department owns each measure after acceptance
- ☐ **c.** It generates the adversary scenarios the threat set is drawn from
- ☐ **d.** It is the test bench where a measure is tried before it touches the platform

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 implemented on what is flying
- ☐ **b.** A detection signature, since only observation is possible on a fixed element
- ☐ **c.** Invalid, because a measure must be implementable 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

© 2026 ethicallyHackingspace (eHs)®

Q12 Adversary management method checkpoint

A draft measure for chain 01 reads: TRE AST:SW:Software:04 and SVC:CP:Control Plane:13; goals Withstand and Recover; owner Both; cadence in-force. What must change before it is accepted?

- ☐ **a.** Nothing: every field the method asks for is present, and both elements and both goals are true of it
- ☐ **b.** Only the cadence, which must read phased while the dual-control workflow is still being built
- ☐ **c.** One TRE, AST:SW:Software:04, with the console service moved to the description; one goal; the owner split written out
- ☐ **d.** Split it into an operations entry and an engineering entry, one per owner, each with its own goal

Resilience catalog checkpoint

Q13 Resilience catalog 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 catalog 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 element in the catalog
- ☐ **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 catalog 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

© 2026 ethicallyHackingspace (eHs)®

Q16 Resilience catalog checkpoint

Completing the resilience set finishes what?

- ☐ **a.** The five METEORSTORM functions: 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 catalog 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 catalog 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

Q19 Resilience catalog checkpoint

In MISP, the event for AN:RES:Resilience Measure:00 carries the tags meteorstorm:AN="AN-RES" and meteorstorm:SVC="SVC-CP" and three text attributes: the measure identifier, GOAL and TRE. Where do you read the one element the measure protects?

- ☐ **a.** In the tag meteorstorm:SVC="SVC-CP", which names the one element protected
- ☐ **b.** In the GOAL attribute, which names the element the goal is set against
- ☐ **c.** In the ordinal 00, which is the protected element’s own ordinal
- ☐ **d.** In the TRE attribute, SVC:CP:Control Plane:09, the element Threat 00 targets

Work every question before you read on. The answer key begins on the next page.

© 2026 ethicallyHackingspace (eHs)®

KEY Answer Key

Each entry repeats the question, gives the answer on its own line, then the reason it is the answer. If yours differs, trace which chapter rule it breaks before reading on.

Q1 Counted across the four attack paths, one element appears in two of them: SVC:CP:Control Plane:09, on Path 00 and Path 01. Every other element appears in one. What does that count tell you to do?

> **d. Put SVC:CP:Control Plane:09 first, keep one measure per anchor, and rerun the count**

One element recurs on this first pass: SVC:CP:Control Plane:09 is on Path 00 and Path 01, so it is the element the count names, and it is the anchor Measure 00 protects. No anchor is shared between chains, so each of the four measures still protects its own anchor, a TRE holds exactly one element, and the count is run again every time the catalog grows. Choosing by a declared gap is hardening by conviction (workbook Chapter 5, What recurs, and what to protect next).

Q2 What is your job on Day 5?

> **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, on the flying platform where the element can be reached and as a next-build requirement where it cannot. That is the job as the method states it. On this first pass the count finds one element on two paths, SVC:CP:Control Plane:09, and each anchor keeps its own measure (workbook Chapter 5, What recurs, and what to protect next).

Q3 Which two departments hold the pen together on Day 5?

> **a. Satellite Operations and Satellite Design and Engineering**

A resilience measure has two halves, something built and something done differently every day after, so Satellite Design and Engineering and Satellite Operations commit it together. Security Operations does not hold the pen (workbook Chapter 1; Chapter 2 gives the two halves).

Q4 Why is Day 5 the right time to remove attack surface, and not earlier?

> **d. Because only now do you know which elements recur across the week's findings**

Only after threats, paths, and detections are enumerated can recurrence be counted at all, so only now can the count say which elements the adversary leans on repeatedly. On this first pass it finds one, SVC:CP:Control Plane:09, on Path 00 and Path 01, a result that could not be had before the paths were written (workbook Chapter 1, Why resilience comes last).

© 2026 ethicallyHackingspace (eHs)®

Q5 A proposed change hardens an element that no threat or path touches. How should you weigh it?

> **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 elements the threats and paths name.

Q6 In which layer does an AN-RES element sit, and what is its TAG?

> **c. The Analytic layer; TAG RES**

AN-RES is an analytic-layer element with TAG RES, one of the six analytic elements alongside IOC, IOA, THR, ATT, and DET.

Q7 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**

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 Measure 01 puts a second approver on every high-impact command, so one compromised credential cannot release a high-impact sequence alone. Which one goal does it serve?

> **b. Withstand, because high-impact commanding continues safely while a credential is compromised**

Choose the goal by what the measure changes about the attack. Dual control does not stop the theft; it lets the mission continue while a stolen credential is in use, which is the Withstand test. One measure, one of the four NIST SP 800-160 Volume 2 goals (workbook Chapter 4, Measure 01).

Q9 What role does the digital twin play in Day 5?

> **d. 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 they touch the flying vehicle, so changes are proven safe first.

© 2026 ethicallyHackingspace (eHs)®

Q10 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 implemented 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 implemented on what is flying.

Q11 A measure's cadence is recorded as phased rather than in force. What must the entry also carry?

> **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 implement is not coverage, and an entry that reads as covered while nothing is implemented is worse than one that admits the gap.

Q12 A draft measure for chain 01 reads: TRE AST:SW:Software:04 and SVC:CP:Control Plane:13; goals Withstand and Recover; owner Both; cadence in-force. What must change before it is accepted?

> **c. One TRE, AST:SW:Software:04, with the console service moved to the description; one goal; the owner split written out**

The TRE holds exactly one element, the TOE of Threat 01, and the reach goes in the description. A measure serves one goal. Both on its own is a measure nobody owns, so the split is written out. Splitting into two entries would put two measures on one ordinal (workbook Chapter 3, The six steps; Chapter 2, The Owner field).

Q13 How large is the Day-5 resilience set?

> **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 How does a resilience measure reduce attack surface?

> **d. By shrinking, hardening or removing that element, or hardening the path to it**

Each measure targets the element its chain names. The recurrence count says which element to protect first; on this first pass it names SVC:CP:Control Plane:09, which is on two paths. 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.

© 2026 ethicallyHackingspace (eHs)®

Q15 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**

Integration happened before launch, so the measure cannot be implemented 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 Completing the resilience set finishes what?

> **a. The five METEORSTORM functions: 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 Why does anchoring every measure to an element matter to the departments?

> **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 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?

> **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.

© 2026 ethicallyHackingspace (eHs)®

Q19 In MISP, the event for AN:RES:Resilience Measure:00 carries the tags meteorstorm:AN="AN-RES" and meteorstorm:SVC="SVC-CP" and three text attributes: the measure identifier, GOAL and TRE. Where do you read the one element the measure protects?

> **d. In the TRE attribute, SVC:CP:Control Plane:09, the element Threat 00 targets**

The tags classify the event: AN-RES says it is a resilience measure, and SVC-CP names the kind of element, not which Control Plane service it is. The attribute TRE = SVC:CP:Control Plane:09 names the one element, and its comment reads "Target of resilience enhancement. Equals the TOE it counters." The TOE it counters is the element AN:THR:Threat:00 names. GOAL = Anticipate is a goal, not an element; its comment reads "One of four: Anticipate, Withstand, Recover, Adapt. Exactly one per measure." The ordinal 00 numbers the chain, not the element, which is ordinal 09 (workbook Chapter 6, The record in MISP).

© 2026 ethicallyHackingspace (eHs)®