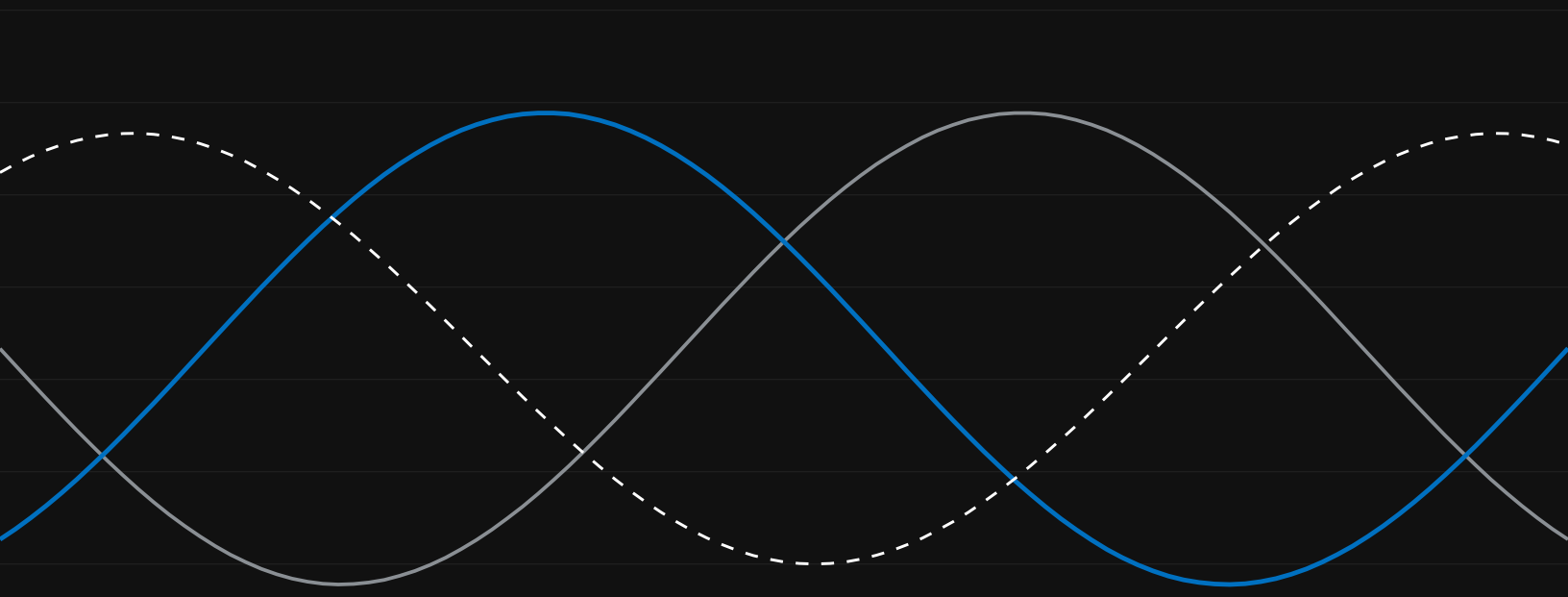
Module 02 · Question set · Student edition

Contextualized Threat Modeling

Every checkpoint question for Module 02, 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 02 Contextualized Threat Modeling, 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 02, Contextualized Threat Modeling, 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 02 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 02 context checkpoint 4

Contextualized threat modeling method checkpoint 5

Threat catalog checkpoint 7

KEY **Answer Key** 9

© 2026 ethicallyHackingspace (eHs)®

QS Question Set

Every checkpoint question for this module, 18 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 02 context checkpoint

Q1 Module 02 context checkpoint

What did Day 1 hand you that today's work builds on?

- ☐ **a.** The Day-2 threat research report on command-and-control attacks
- ☐ **b.** The Day-1 CONOPS: the 44-element shared decomposition of the telecommand path
- ☐ **c.** A finished set of detection signatures
- ☐ **d.** A completed threat catalog, already shared with Space ISAC

Q2 Module 02 context checkpoint

What is your job on Day 2?

- ☐ **a.** Rebuild the platform decomposition the prior day produced, from scratch
- ☐ **b.** Write the detection signatures for the SOC to run
- ☐ **c.** Present the Day-1 CONOPS to the NIS2 regulators
- ☐ **d.** Enumerate adversary threats against the elements they target

Q3 Module 02 context checkpoint

Of the three mandates that set the scope, which two are regulatory, and which NIS2 provision does the enumerated threat set feed?

- ☐ **a.** EO 14144 and the NIS2 Directive; the Article 21(2)(a) risk analysis
- ☐ **b.** SPD-5 and the Outer Space Treaty; the Article IX due-regard consultation
- ☐ **c.** ITAR and the EAR; the Annex B export-control list
- ☐ **d.** SOC 2 and ISO 27001; the Clause 6 information security planning requirement

© 2026 ethicallyHackingspace (eHs)®

Q4 Module 02 context checkpoint

Workbook Chapter 2 names five intelligence source types. They are:

- ☐ **a.** Firewall logs, intrusion detection alerts, SIEM correlation rules, endpoint telemetry, SOAR case notes
- ☐ **b.** Spacecraft telemetry, beacons, pass schedules, TLEs, and ground station logs
- ☐ **c.** Vendor or Space ISAC feed, government advisory, peer operator, open source, internal hunting
- ☐ **d.** Classified government reporting only, with no open-source or peer input

Q5 Module 02 context checkpoint

A candidate threat has no target among the elements in your CONOPS. What happens to it?

- ☐ **a.** It is added to the set anyway, with the TOE left empty
- ☐ **b.** It stays out of the set; the platform has nothing for it to target
- ☐ **c.** It replaces the closest existing threat already in the set
- ☐ **d.** It is anchored to the whole platform instead of one element

Contextualized threat modeling method checkpoint

Q6 Contextualized threat modeling method checkpoint

An AN-THR element sits in which METEORSTORM layer, and what does TOE stand for?

- ☐ **a.** The Segment layer; Type of Element
- ☐ **b.** The Asset layer; Total Operational Exposure
- ☐ **c.** The Analytic layer; Target of Exploitation
- ☐ **d.** The Service layer; Time of Entry

Q7 Contextualized threat modeling method checkpoint

How many enumerated elements does a valid AN-THR name in its TOE?

- ☐ **a.** One element from every layer
- ☐ **b.** Exactly one
- ☐ **c.** At least one service and one asset
- ☐ **d.** As many as the adversary crosses

© 2026 ethicallyHackingspace (eHs)®

Q8 Contextualized threat modeling method checkpoint

Which is the correct order for enumerating an AN-THR element?

- ☐ **a.** Source, then ORDINAL, then LAYER (AN), TAG (THR), TOE, Description
- ☐ **b.** TOE first, then LAYER (AN) and TAG (THR) taken from what it names
- ☐ **c.** TAG (THR), LAYER (AN), TOE, Description, ORDINAL last, no source
- ☐ **d.** LAYER (AN), source, TAG (THR), ORDINAL, TOE, Description

Q9 Contextualized threat modeling method checkpoint

You read AN:THR:Threat:00 with TOE naming SVC:CP:Control Plane:09. What does that one identifier tell you?

- ☐ **a.** The intel source the threat was first cited from, and the date it was assessed
- ☐ **b.** The parent environment of the targeted segment, and nothing below it
- ☐ **c.** The detection signature that will eventually cover it on Day 4
- ☐ **d.** The one platform element this threat targets

Q10 Contextualized threat modeling method checkpoint

A new threat targets ground command authorization. Which TOE is correct?

- ☐ **a.** The Ground segment element, because that is where the service sits
- ☐ **b.** The ground ACA service element on its own
- ☐ **c.** The ground ACA service and the asset it runs on, both named
- ☐ **d.** Nothing; threats do not carry a TOE

Q11 Contextualized threat modeling method checkpoint

You assign ordinal 00 to a threat. What have you just opened?

- ☐ **a.** A parent chain, which will terminate at an environment
- ☐ **b.** A register entry that Day 3 will renumber to keep the set consecutive
- ☐ **c.** A chain: one ordinal that Days 3, 4 and 5 reuse, all naming the same element
- ☐ **d.** A placeholder, until the detection engineer confirms the threat is real

© 2026 ethicallyHackingspace (eHs)®

Q12 Contextualized threat modeling method checkpoint

A candidate reads: solar activity degrades the uplink during the northern ground station's pass. Apply the gate. What happens to it?

- ☐ **a.** It enters the catalog, anchored to the telecommand uplink waveform
- ☐ **b.** It does not enter: there is no adversary, so it is not a threat; the environment is an element, not a threat
- ☐ **c.** It is excluded because its target is not enumerated, and held in the open-source register
- ☐ **d.** It enters as intelligence, with no target

Threat catalog checkpoint

Q13 Threat catalog checkpoint

How many AN-THR threats did you enumerate, and how do they split across the segments?

- ☐ **a.** 10; spread evenly across the three segments
- ☐ **b.** 5; one per intel source type
- ☐ **c.** 44; one per CONOPS element
- ☐ **d.** 4; Ground 2, Link 1, Space 1

Q14 Threat catalog checkpoint

Once the set is written, how does each department use the TOE targets?

- ☐ **a.** The SOC hunts, Satellite Operations tracks, Satellite Design & Engineering hardens
- ☐ **b.** Only the SOC reads them; Satellite Operations and Engineering wait for tickets
- ☐ **c.** They are filed for the NIS2 Article 21(2)(a) report and not used day to day
- ☐ **d.** Each department re-translates them into its own tracker and naming

Q15 Threat catalog checkpoint

Why does writing every threat as an ETEN in the five-field syntax Module 01 taught matter?

- ☐ **a.** It satisfies the ordinal numbering rule in the published taxonomy
- ☐ **b.** It lets the SOC keep the set in its own private tracking format
- ☐ **c.** Any department can pick the set up and act on it without re-translation
- ☐ **d.** It shortens the NIS2 Article 21(2)(a) risk-analysis filing

© 2026 ethicallyHackingspace (eHs)®

Q16 Threat catalog checkpoint

Threat 00's TOE is SVC:CP:Control Plane:09. Which segment does that element's PARENT chain resolve to?

- ☐ **a.** Ground
- ☐ **b.** Space
- ☐ **c.** Link
- ☐ **d.** No single segment

Q17 Threat catalog checkpoint

What does Day 3 do with today's threat set?

- ☐ **a.** Walks each threat's TOE into an attack path the adversary would take
- ☐ **b.** Discards it and starts the whole threat enumeration over again from scratch
- ☐ **c.** Writes the detection signatures for it immediately, skipping the paths
- ☐ **d.** Shares the full set with Space ISAC unredacted, with no attack paths

Q18 Threat catalog checkpoint

MISP event 28 carries the tags meteorstorm:AN="AN-THR", SVC-CP, SEG-GR and PCE-TE, and the attributes AN:THR:Threat:00, TOE = SVC:CP:Control Plane:09 and SOURCE = observable. Which one element does the threat anchor to, and where on the event do you read it?

- ☐ **a.** SEG:GR:Ground:00, read from the meteorstorm:SEG tag carried on the event
- ☐ **b.** SVC:CP:Control Plane:09, read from the TOE attribute; the tags only classify
- ☐ **c.** All the elements the layer tags name together: Control Plane, Ground and Terrestrial
- ☐ **d.** AN-THR itself, read from the analytic tag, since the tag is the threat's target

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 What did Day 1 hand you that today's work builds on?

> **b. The Day-1 CONOPS: the 44-element shared decomposition of the telecommand path**

Module 01 produced the CONOPS, 44 enumerated elements across PCE, SEG, SVC, AST. Today you enumerate threats against those exact elements.

Q2 What is your job on Day 2?

> **d. Enumerate adversary threats against the elements they target**

Contextualized Threat Modeling names, in each threat's TOE, the exact CONOPS element it would target, so the threat picture is grounded in the platform.

Q3 Of the three mandates that set the scope, which two are regulatory, and which NIS2 provision does the enumerated threat set feed?

> **a. EO 14144 and the NIS2 Directive; the Article 21(2)(a) risk analysis**

EO 14144 protects command and control and NIS2 binds the ground infrastructure; the enumerated catalog is the documented risk basis NIS2 Article 21(2)(a) requires. The third mandate, Space ISAC, is a sharing duty rather than a regulation: the catalog is written ready for the Space ISAC Exchange, and a confirmed command-and-control attack is shared as a redacted alert, machine to machine.

Q4 Workbook Chapter 2 names five intelligence source types. They are:

> **c. Vendor or Space ISAC feed, government advisory, peer operator, open source, internal hunting**

Four sources come from outside (feed, government advisory, peer operator, open source) and one from inside (the center's own hunting). Every threat is cited to one of the five.

Q5 A candidate threat has no target among the elements in your CONOPS. What happens to it?

> **b. It stays out of the set; the platform has nothing for it to target**

A threat with no CONOPS target names nothing on your platform to attack, so it stays out of the set, excluded on the record with its reason, until an element exists for it to target.

© 2026 ethicallyHackingspace (eHs)®

Q6 An AN-THR element sits in which METEORSTORM layer, and what does TOE stand for?

> **c. The Analytic layer; Target of Exploitation**

AN-THR is an analytic-layer element. Its TOE (Target of Exploitation) names the one structural element the threat would target.

Q7 How many enumerated elements does a valid AN-THR name in its TOE?

> **b. Exactly one**

The TOE holds exactly one enumerated element, at the lowest layer the source resolves. That element becomes the anchor the chain reuses on Days 3, 4 and 5. Everything else the adversary crosses is description content, never a second target.

Q8 Which is the correct order for enumerating an AN-THR element?

> **d. LAYER (AN), source, TAG (THR), ORDINAL, TOE, Description**

The six-step order is fixed: LAYER, source, TAG, ORDINAL, TOE, Description. The TOE target and the source are mandatory.

Q9 You read AN:THR:Threat:00 with TOE naming SVC:CP:Control Plane:09. What does that one identifier tell you?

> **d. The one platform element this threat targets**

The TOE is the exact identifier of the one element the threat targets. All three departments point at it with no re-translation, and Days 3, 4 and 5 name it again under TOE, TDM and TRE.

Q10 A new threat targets ground command authorization. Which TOE is correct?

> **b. The ground ACA service element on its own**

Name the one element the threat is directed against, at the lowest layer the source resolves: the ground ACA service. The asset it runs on is reachable through it and belongs in the description.

Q11 You assign ordinal 00 to a threat. What have you just opened?

> **c. A chain: one ordinal that Days 3, 4 and 5 reuse, all naming the same element**

A chain is one ordinal carried across Functions 02 to 05, where the threat, the attack path, the detection signature and the resilience measure all name the same platform element. Ordinal 00 opens chain 00, and it is never renumbered.

© 2026 ethicallyHackingspace (eHs)®

Q12 A candidate reads: solar activity degrades the uplink during the northern ground station's pass. Apply the gate. What happens to it?

> **b. It does not enter: there is no adversary, so it is not a threat; the environment is an element, not a threat**

A threat is adversary activity: an adversarial capability or intent. Solar activity has no adversary, so neither exclusion reason applies: it is not a threat at all. The environment is not a threat; it was enumerated on Day 1, as an element.

Q13 How many AN-THR threats did you enumerate, and how do they split across the segments?

> **d. 4; Ground 2, Link 1, Space 1**

The set is 4 threats: Ground 2, Link 1, Space 1, each with a TOE naming exactly one Day 1 CONOPS element.

Q14 Once the set is written, how does each department use the TOE targets?

> **a. The SOC hunts, Satellite Operations tracks, Satellite Design & Engineering hardens**

Because every threat targets exact elements, all three departments act on the same set: hunt, operate, and harden against the same named elements.

Q15 Why does writing every threat as an ETEN in the five-field syntax Module 01 taught matter?

> **c. Any department can pick the set up and act on it without re-translation**

LAYER:TAG:LABEL:ORDINAL:Description is the same form every Day 1 element carries, with SOURCE and TOE added. One shared form is what lets a threat written by one department be read and used by the others without re-translation, the point of the shared data model.

Q16 Threat 00's TOE is SVC:CP:Control Plane:09. Which segment does that element's PARENT chain resolve to?

> **a. Ground**

SVC:CP:Control Plane:09, the ground command-acceptance service, names SEG:GR:Ground:00, the Reston enclave, as its PARENT. The TOE names one element; the segment is read off the Day 1 CONOPS through the parent chain, never written into the threat.

Q17 What does Day 3 do with today's threat set?

> **a. Walks each threat's TOE into an attack path the adversary would take**

Day 3, Converged Detection Engineering, takes each threat's one anchor element and writes an attack path anchored to it, a traversal from entry through pivot to objective, recording the required sources at each step. Today's threats become tomorrow's paths.

© 2026 ethicallyHackingspace (eHs)®

Q18 MISP event 28 carries the tags meteorstorm:AN="AN-THR", SVC-CP, SEG-GR and PCE-TE, and the attributes AN:THR:Threat:00, TOE = SVC:CP:Control Plane:09 and SOURCE = observable. Which one element does the threat anchor to, and where on the event do you read it?

> **b. SVC:CP:Control Plane:09, read from the TOE attribute; the tags only classify**

The tags classify the event: AN-THR says it is a threat, and SVC-CP, SEG-GR and PCE-TE name the taxonomic elements along the target's parent chain. The anchor is the TOE attribute, one enumerated element, SVC:CP:Control Plane:09, the ground command-acceptance service. A tag never names an element and an analytic entry never targets another analytic element (Module 02 workbook, Chapters 3 and 6).

© 2026 ethicallyHackingspace (eHs)®