FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

Module 02 Contextualized Threat Modeling

Question set

COPYRIGHT AND LEGAL NOTICES

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 2026-09-24
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

QS Question Set

Every checkpoint question for this module, 16 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 2 context checkpoint

Q1 Day 2 context checkpoint worked in the classroom

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. The Space ISAC machine-to-machine channel, already live

Q2 Day 2 context checkpoint

What is your job on Day 2?

a. Rebuild the platform decomposition the prior day produced
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 Day 2 context checkpoint

Which mandates put the telecommand path in scope, 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 IV due-regard clause
c. ITAR and the EAR; the Annex B export-control list
d. SOC 2 and ISO 27001; the Clause 6 planning requirement

Q4 Day 2 context checkpoint worked in the classroom

The Security Operations Center briefing named five intel 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 Day 2 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 worked in the classroom

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

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 one platform element this threat targets
c. The detection signature that will eventually cover it on Day 4
d. The parent environment of the targeted segment, and nothing below it

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

Threat catalogue checkpoint

Q12 Threat catalogue 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

Q13 Threat catalogue 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

Q14 Threat catalogue checkpoint

Why does writing every threat in the same five-field form 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

Q15 Threat catalogue checkpoint

The SATCOM management-network intrusion targets which segment?

a. Space
b. Ground
c. Link
d. No single segment

Q16 Threat catalogue 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 threat enumeration over 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

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 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

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

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 catalogue is the documented risk basis NIS2 Article 21(2)(a) requires.

Q4

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

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 until an element exists for it to target.

Q6

c. The Analytic layer; Target of Exploitation AN-THR is an analytic-layer element. Its TOE (Target of Exploitation) names the structural elements the threat would target.

Q7

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

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

b. 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

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

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.

Q12

d. 4; Ground 2, Link 1, Space 1 The set is 4 threats: Ground 2, Link 1, Space 1, each with a TOE naming CONOPS elements.

Q13

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.

Q14

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

Q15

b. Ground The SATCOM management network and ground ACA live in the Ground segment, so that threat targets the Ground segment.

Q16

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 walks an attack path to it, from first touch to objective, recording the required sources at each step. Today’s threats become tomorrow’s paths.