FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

Module 03 Converged Detection Engineering

Question set

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 03 Converged Detection Engineering, 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, 17 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 3 context checkpoint

Q1 Day 3 context checkpoint worked in the classroom

What did Day 2 hand you to work from today?

a. A finished set of detection signatures already written for the command path
b. The Day-1 CONOPS, handed forward a second time for structural revision
c. Four AN-THR threats, each anchored by its TOE to one platform element
d. A coverage-gap register inherited from the Security Operations Center

Q2 Day 3 context checkpoint

What is your job on Day 3?

a. Trace how an adversary would move to realize each threat, and name what would see it
b. Write the detection signatures and response playbooks that fire on each threat’s TOE
c. Shrink the attack surface that the catalogued threats keep relying on to succeed
d. Enumerate the services and assets that each catalogued threat targets

Q3 Day 3 context checkpoint worked in the classroom

The paths and the required sources they carry feed which mandate requirement?

a. The 24-hour early-warning clock the NIS2 Directive sets for incident reporting
b. The machine-to-machine sharing channel Kestrel Orbital opens with Space ISAC
c. The vendor attestations the procurement team collects at contract renewal
d. The detection methods Executive Order 14144 requires on the command path

Q4 Day 3 context checkpoint

Satellite Design & Engineering opens six artifacts today. What do they provide?

a. The threat intelligence sources that cite each adversary and its tradecraft
b. The build knowledge of how the platform moves data and commands
c. The detection sources already onboarded in the Security Operations Center
d. The regulatory scope that bounds the telecommand path for Day 1

Q5 Day 3 context checkpoint

Why does Satellite Design & Engineering lead the working session on Day 3?

a. It owns the budget for the new detection tooling the paths will need
b. It is the department both regulators name as accountable for the platform
c. It holds the deepest knowledge of how the platform moves data and commands
d. It operates the platform day to day and watches every pass in real time

Converged detection engineering method checkpoint

Q6 Converged detection engineering method checkpoint

An AN-ATT element names an attack path. What are its waypoints?

a. The services the path crosses, listed in build order
b. Only the final element the adversary is trying to reach
c. The intel sources that cite the path in public reporting
d. Entry, pivot and objective: the points where a detection can fire

Q7 Converged detection engineering method checkpoint

An attack path carries two source fields, RDS and RSS. What separates them?

a. RDS covers the ground segment; RSS covers the link and space segments
b. RDS is what the SOC already receives; RSS is what it has asked for
c. RDS is what must be received as a record; RSS is what must be measured
d. RDS is written on Day 3; RSS is added by Day 4 once signatures exist

Q8 Converged detection engineering method checkpoint worked in the classroom

Where do the required sources live?

a. On the attack-path element, as its RDS and RSS fields
b. In a separate inventory document filed beside the path
c. In the DESCRIPTION, written into the waypoint prose
d. On the AN-THR threat the path realizes, one field each

Q9 Converged detection engineering method checkpoint

A path is anchored to SVC:CP:Control Plane:09 and its objective waypoint is AST:SW:Software:03. This path is:

a. Valid: the anchor names what the path is about, the objective is where it lands
b. Invalid: the objective waypoint has to be the anchor element
c. Invalid: an anchor may not be a service when the objective is an asset
d. Valid only if a fourth waypoint is added to return to the anchor

Q10 Converged detection engineering method checkpoint

You read a path whose waypoints run entry to objective. What do the two ends tell you?

a. The threat's first public reporting date and its source confidence
b. The departments that own each end of the path
c. Where the adversary gets in, and where the route lands
d. The segments the path crosses, in order

Q11 Converged detection engineering method checkpoint

A required source is one nobody on the platform collects. You record it as:

a. A record with the state Gap, carrying what would close it
b. A record with the state unassessed, until someone asks
c. Nothing, since a source that does not exist cannot be enumerated
d. A note in the path description, so the field stays clean

Q12 Converged detection engineering method checkpoint

AN:THR:Threat:00 names SVC:CP:Control Plane:09. What ordinal and what TOE does the path that realizes it carry?

a. Ordinal 00, and TOE SVC:CP:Control Plane:09
b. The next free ordinal, and TOE SVC:CP:Control Plane:09
c. Ordinal 00, and a TOE listing every element the route crosses
d. The next free ordinal, and the TOE of whichever element the route ends on

Attack-path catalogue checkpoint

Q13 Attack-path catalogue checkpoint

How many attack paths did you enumerate, and how do they split by segment?

a. 10; spread evenly across the three segments
b. 4; Ground 2, Link 1, Space 1
c. 44; one path per enumerated element
d. 1; one path per working-session artifact

Q14 Attack-path catalogue checkpoint

What separates a grounded path from a hypothesis in this set?

a. The number of departments that reviewed it
b. Its length in waypoints alone
c. Whether the SOC already has a signature for it
d. Waypoints through real elements, and a cited source

Q15 Attack-path catalogue checkpoint

How do the RDS and RSS records feed Day 4?

a. Day 4 writes the signatures that fire on those sources
b. Day 4 re-enumerates them as fresh threats against the CONOPS
c. They are filed for the auditor and reopened at course end
d. They are shared to Space ISAC before any signature exists

Q16 Attack-path catalogue checkpoint

An AN-ATT element is marked DRIVEN BY AN:THR:Threat:03. What does that tell you?

a. The segment the path terminates in
b. The confidence level assigned to the path’s source
c. Which Day-2 threat this path realizes
d. The required source watched at its objective

Q17 Attack-path catalogue checkpoint

A path’s RDS field is empty because the activity leaves no records anywhere. You write:

a. Nothing; a field with no entries is left blank

b. A placeholder record so the field is never empty

c. The empty field as empty; an empty list is a valid value

d. The RSS records again, copied across, so both fields agree

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

c. Four AN-THR threats, each anchored by its TOE to one platform element Day 2 produced 4 anchored threats, each naming exactly one element as its TOE. Today you walk each one into the path an adversary would take to realize it, and the path takes that same element as its anchor.

Q2

a. Trace how an adversary would move to realize each threat, and name what would see it Converged Detection Engineering traces each threat into an attack path and enumerates the data and signal sources needed to detect every step.

Q3

d. The detection methods Executive Order 14144 requires on the command path EO 14144 requires detection on command and control; the attack paths and the RDS and RSS records that would reveal them are what those detections are built on.

Q4

b. The build knowledge of how the platform moves data and commands SD&E owns the deepest knowledge of how data and commands move; the six artifacts show where an attacker could enter, pivot, and what they would touch.

Q5

c. It holds the deepest knowledge of how the platform moves data and commands Walking a threat into a real path needs the build knowledge of the platform, which SD&E owns; that is why the pen passes to them today.

Q6

d. Entry, pivot and objective: the points where a detection can fire Three waypoints, four at most, each an element where the adversary must act in a way a detection can observe. They are written in the DESCRIPTION; the path’s target field is the anchor TOE, one element.

Q7

c. RDS is what must be received as a record; RSS is what must be measured RDS is the required data source, a log, audit stream, inventory or telemetry feed. RSS is the required signal source, a noise floor, carrier-to-noise ratio, lock status or received power. They stay apart because they are different kinds of observable: jamming is seen in the noise floor and never in a log.

Q8

a. On the attack-path element, as its RDS and RSS fields They are fields on the element, which is what makes them countable, ownable and auditable. Each record carries a sub-ordinal from 00, the one element it is observed on, and its state. The sub-ordinal is its own counter and has nothing to do with the element's ordinal.

Q9

a. Valid: the anchor names what the path is about, the objective is where it lands That is path 00 exactly: anchored to the ground command-acceptance service its threat names, landing on the patch deployment pipeline the wiper rides. The anchor answers what the path is about; the objective answers where the route ends. They may differ.

Q10

c. Where the adversary gets in, and where the route lands Entry is first access, the objective is where the route lands, and the pivot sits between. The anchor element is a separate field, and it need not be either end.

Q11

a. A record with the state Gap, carrying what would close it It still takes a sub-ordinal, an element and a state, and the state is Gap. That is what makes a gap countable rather than a sentence in a chapter. unassessed is different: it means the owning department has not answered yet, not that the source is absent.

Q12

a. Ordinal 00, and TOE SVC:CP:Control Plane:09 The path takes the threat's ordinal and names the same one element. That is the chain: one number, one element, carried without translation. The route it crosses is waypoints and description, never a second target and never a new ordinal.

Q13

b. 4; Ground 2, Link 1, Space 1 The set is 4 paths, one per Day-2 threat, split Ground 2, Link 1, Space 1.

Q14

d. Waypoints through real elements, and a cited source Every path in the set walks three or four real enumerated elements and cites a source. Nothing hypothetical is in the active set.

Q15

a. Day 4 writes the signatures that fire on those sources The required sources are the day's second deliverable, carried on the path element itself. Incident Response Preparation reads them to write the signatures and the playbooks behind them, one signature per required source.

Q16

c. Which Day-2 threat this path realizes DRIVEN BY names the threat the path realizes. The path also takes that threat's ordinal, 03, and its one TOE element, AST:FW:Firmware:01, as its own anchor.

Q17

c. The empty field as empty; an empty list is a valid value An empty field is an answer, not an omission. Path 02, the jamming campaign, is exactly this: no RDS records at all and three RSS records, because jamming is measured and never logged. Both fields empty would mean the path cannot be detected, which is itself a finding.