FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

Module 04 Incident Response Preparation

Question set

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 04 Incident Response Preparation, 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, 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 4 context checkpoint

Q1 Day 4 context checkpoint worked in the classroom

What did Day 3 hand you that Day 4 builds on?

a. A finished set of resilience measures for the recurring elements
b. The Day-1 CONOPS on its own, with no analytic elements attached
c. A coverage-gap register with no paths behind it yet
d. The four AN-ATT paths plus the required sources carried on the elements they name

Q2 Day 4 context checkpoint

What is your job on Day 4?

a. Decompose the platform into its PCE, SEG, SVC, and AST elements
b. Write the signatures that fire on those sources, and the playbooks behind them
c. Anchor newly reported threats to the elements they target
d. Remove the attack surface the adversary keeps relying on

Q3 Day 4 context checkpoint

Which department leads Day 4’s working session?

a. Satellite Design and Engineering, which drew the paths yesterday
b. Satellite Operations, which flies the platform each pass
c. The Security Operations Center, which runs the detections
d. All three departments jointly, with no single lead

Q4 Day 4 context checkpoint

Why does every detection trace back to an attack path?

a. So coverage is measured against the paths, and a Gap source is recorded
b. So each signature can be priced against the tooling budget it needs
c. So the auditor can trace each rule back to a regulation clause
d. So Satellite Operations knows which subsystems to watch during a pass

Q5 Day 4 context checkpoint worked in the classroom

Before you can write a single detection, what has to exist?

a. A resilience measure covering the element the path ends on
b. A finished playbook the signature can hook into on arrival
c. A vendor query already written in the SIEM’s native dialect
d. An attack path with a named data or signal source behind it

Detection engineering method checkpoint

Q6 Detection engineering method checkpoint

What does the TDM field on an AN-DET element name?

a. The tooling the signature was authored in and ported from
b. The one platform element the signature observes
c. Every element the signature reads a stream from, listed in order
d. The team that owns the alert when the signature fires

Q7 Detection engineering method checkpoint

What is RootA, and why write signatures in it?

a. A single-vendor SIEM query language maintained by one platform
b. A threat-intelligence feed format for sharing indicators
c. A playbook template for structuring incident response
d. A vendor-neutral detection format, so one rule ports across tooling

Q8 Detection engineering method checkpoint

Besides its TDM anchor, what else must every AN-DET carry?

a. A reference to the AN-ATT attack path the signature covers
b. A second TOE field naming the element the adversary exploits
c. The confidence level assigned by the intelligence source
d. The segment the observed element belongs to

Q9 Detection engineering method checkpoint

Function 03 marked a path’s source Gap. Under the method, what happens?

a. You author the signature against the nearest observable neighbor
b. You drop the whole attack path from the Day-3 catalogue
c. You record the detection gap and name the collection that closes it
d. You lower the confidence on the signature and ship it anyway

Q10 Detection engineering method checkpoint worked in the classroom

What runs when a signature fires?

a. The next signature in the register, linked by ordinal
b. The response playbook the signature is bound to
c. The Day-5 resilience measure for the element it watches
d. The redacted Space ISAC contribution, sent automatically

Q11 Detection engineering method checkpoint

Who executes an approved action, and who decides it?

a. One Responsible executor from the action’s domain, with Mission Lead Accountable
b. Whoever holds the on-call phone, who both decides and executes at 02:00
c. Security Operations executes and decides, since it owns the signature
d. Mission Lead executes, because accountability means doing the work

Q12 Detection engineering method checkpoint

What sets an action’s authority level?

a. The seniority of whoever happens to be on shift when it fires
b. The segment the element sits in, Ground, Link or Space
c. How reversible the action is: reversible, disruptive or irreversible
d. The severity the RootA rule assigned to the signature

Q13 Detection engineering method checkpoint

A signature carries ordinal 00 but its TDM names a different element from the TOE of AN:THR:Threat:00. What has happened?

a. Nothing; a signature may watch whichever element emits the best telemetry
b. The chain is broken, and the ordinal no longer describes one thing
c. The threat should be renumbered to match the signature
d. The signature should be promoted to a second attack path

Detection catalogue checkpoint

Q14 Detection catalogue checkpoint

How large is the Day-4 set, and how does it split across segments?

a. 10 detections, split evenly across the three enumerated segments
b. 44 detections, one for every enumerated element in the CONOPS
c. 4 detections and 4 playbooks: Ground 2, Link 1, Space 1
d. 5 detections, one for each of the intel source types briefed

Q15 Detection catalogue checkpoint

Why write every signature in vendor-neutral RootA?

a. So one rule ports across tooling and a peer operator can run it
b. So the signatures stay readable only inside the Security Operations Center
c. So the rule count satisfies the NIS2 Article 21(2)(a) risk analysis
d. So each rule can be priced against the detection tooling budget

Q16 Detection catalogue checkpoint

What happens to a path whose source Day 3 marked Gap?

a. It is detected with a lower-confidence signature instead
b. It is deleted from the Day-3 attack-path catalogue
c. It becomes a playbook entry rather than a signature
d. It is recorded as a detection gap with the collection that closes it

Q17 Detection catalogue checkpoint

What does Day 5 do with what recurs across today’s detections and the earlier paths?

a. Discards it and re-enumerates the platform from scratch
b. Finds the elements that recur, and shrinks or hardens them
c. Turns the accumulated set directly into the end-of-course exam
d. Shares the full unredacted set with the Space ISAC membership

Q18 Detection catalogue checkpoint

Once written, how do the three departments use the detection set?

a. The SOC runs the signatures and playbooks while engineering closes the gaps
b. Only the Security Operations Center reads the set in its day-to-day work
c. The set is filed for the auditor and reopened at the end of the course
d. Satellite Operations rewrites the set into its own console vocabulary first

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

d. The four AN-ATT paths plus the required sources carried on the elements they name Day 3, Converged Detection Engineering, produced the 4 attack paths and the required-source inventory behind them: RDS and RSS records carried on the element each is observed on, marked Available, Partial, Gap or unassessed. Day 4 writes the signatures that fire on those sources.

Q2

b. Write the signatures that fire on those sources, and the playbooks behind them Incident response preparation turns each attack-path step into an AN-DET signature and a response playbook.

Q3

c. The Security Operations Center, which runs the detections Day 4 runs in the Security Operations Center, the team that writes and tunes detections and runs the playbooks.

Q4

a. So coverage is measured against the paths, and a Gap source is recorded Each AN-DET references the AN-ATT it covers and carries the same ordinal, so coverage is read off the number rather than a lookup table, and a path whose source is a Gap shows up as a recorded gap rather than a silent hole.

Q5

d. An attack path with a named data or signal source behind it A signature is authored against a source Function 03 named on a path. With no path and no named source, there is nothing for the rule to read.

Q6

b. The one platform element the signature observes TDM (Target of Detection Method) holds exactly one enumerated element, and it is the same element the AN-THR this signature covers named as its TOE. Corroborating streams belong in the description, not in the field.

Q7

d. A vendor-neutral detection format, so one rule ports across tooling RootA is vendor-neutral, so each signature runs across different detection tools rather than being locked to one product.

Q8

a. A reference to the AN-ATT attack path the signature covers The RootA references field names the AN-ATT and AN-THR entries the rule covers, so coverage is reviewable from the rule itself. There is no separate TOE on an AN-DET: the TDM already holds that element.

Q9

c. You record the detection gap and name the collection that closes it A Gap is an enumerable analytic product, not an omission. You record it, name the collection that would close it, give it an owner, and still write the playbook so the response exists the day the collection lands.

Q10

b. The response playbook the signature is bound to The playbook is the module’s second deliverable, one per signature, bound to it through meteorstorm.playbook and shipping beside it. It carries one trigger and approved actions across assess, contain, recover and report, and the report stage is where the NIS2 clocks are met or missed.

Q11

a. One Responsible executor from the action’s domain, with Mission Lead Accountable Every action names exactly one Responsible executor, Security Operations for a cyber response and Satellite Operations for a space response, and exactly one Accountable decider, always Mission Lead. Mission Lead is Responsible on nothing: the decider does not also do the work, and one person holding both is the failure this structure exists to prevent.

Q12

c. How reversible the action is: reversible, disruptive or irreversible The level is derived from the reversibility class and never chosen. Reversible gives solo, disruptive gives collaborative and the other operating role co-signs, irreversible gives escalated and Mission Lead approves in writing beforehand. If an action feels over-gated, the reversibility class is wrong, and that is the conversation to have.

Q13

b. The chain is broken, and the ordinal no longer describes one thing Within a chain the AN-THR TOE, the AN-ATT TOE, the AN-DET TDM and the AN-RES TRE are all the same element. Break that equality anywhere and one ordinal no longer holds one account, which is the whole property the framework exists to produce. Fix the TDM, do not renumber the threat.

Q14

c. 4 detections and 4 playbooks: Ground 2, Link 1, Space 1 The set is 4 detections and 4 playbooks, split Ground 2, Link 1, Space 1, mirroring the 4 attack paths they cover.

Q15

a. So one rule ports across tooling and a peer operator can run it Vendor-neutral rules run across different tools and are the form the organization’s policy-gated Space ISAC contributions ride on, so detections are portable and shareable.

Q16

d. It is recorded as a detection gap with the collection that closes it One of today’s four sits here: the firmware-hash signature cannot fire until measured boot flies. It is enumerated anyway, with the missing collection named and Satellite Design and Engineering as its owner, and its playbook ships marked gap-blocked, complete and held to every check, so the authorized response exists the day measured boot arrives.

Q17

b. Finds the elements that recur, and shrinks or hardens them Day 5, Adversary Management, targets the elements that keep reappearing and shrinks, hardens, or removes them before launch.

Q18

a. The SOC runs the signatures and playbooks while engineering closes the gaps Because each detection names its element and its gap, the SOC operates the set while engineering fixes the blind spots, working from the same catalogue.