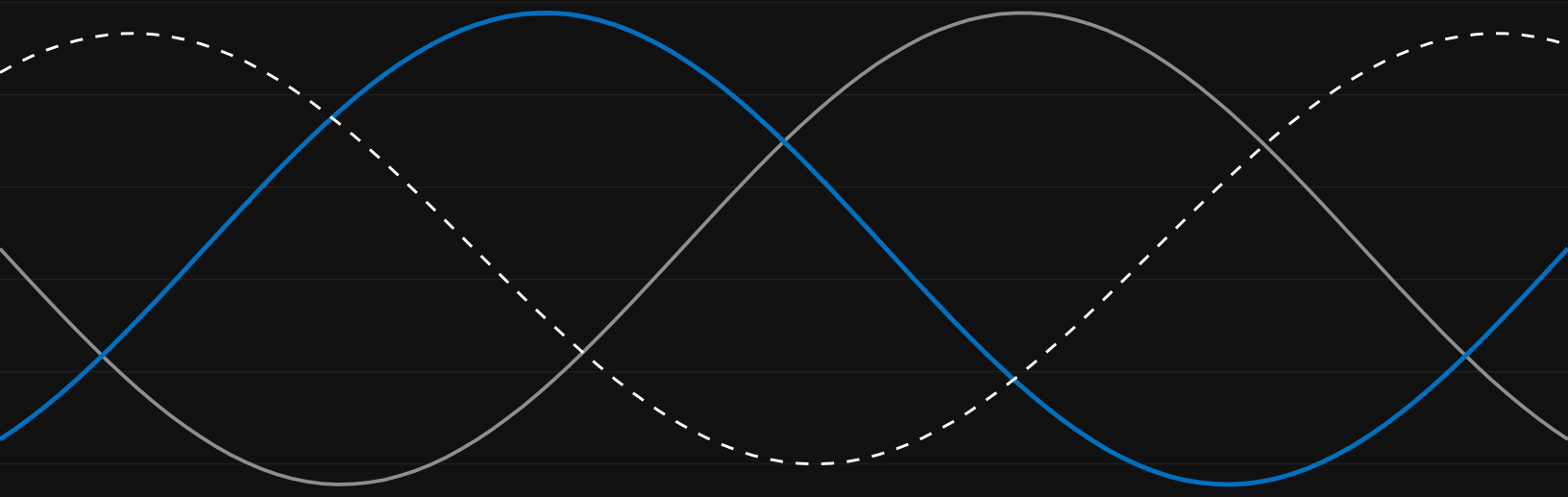
Module 03 · Question set · Student edition

Converged Detection Engineering

Every checkpoint question for Module 03, 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 03 Converged Detection Engineering, 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 03, Converged Detection Engineering, 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 03 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 03 context checkpoint 4

Converged detection engineering method checkpoint 5

Attack-path 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 03 context checkpoint

Q1 Module 03 context checkpoint

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 enumerated platform element
- ☐ **d.** A coverage-gap register inherited from the Security Operations Center

Q2 Module 03 context checkpoint

During the Kiruna uplink outage, Satellite Operations sees the spacecraft's uplink noise floor rise in telemetry while Security Operations sees a healthy event stream. Why can neither settle the cause?

- ☐ **a.** Both observations are valid, and no shared identifier joins the two
- ☐ **b.** The spectrum display is sampled too slowly to show a jamming campaign
- ☐ **c.** Security Operations lacks a log source on the Kiruna ground station
- ☐ **d.** Weather data is held by a third department that was not in the room

Q3 Module 03 context checkpoint

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-and-control path

© 2026 ethicallyHackingspace (eHs)®

Q4 Module 03 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 Module 03 context checkpoint

AN:ATT:Attack Path:03 carries its first required data source. What is that record's sub-ordinal?

- ☐ **a.** RDS:03, because it takes the path's ordinal
- ☐ **b.** RDS:00, counted from 00 in its own field
- ☐ **c.** RSS:00, because the sub-ordinal is shared across both fields
- ☐ **d.** RDS:01, because 00 is reserved for the anchor

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 the order they were built
- ☐ **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 only; RSS covers the link and space segments
- ☐ **b.** RDS is what the SOC already receives; RSS is what it still has to ask 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

© 2026 ethicallyHackingspace (eHs)®

Q8 Converged detection engineering method checkpoint

Path 01's entry step leaves an operator console session record on AST:HW:Hardware:04, and Security Operations has not yet said whether it receives it. Which record is written correctly?

- ☐ **a.** RSS:00, console session record, AST:HW:Hardware:04, unassessed
- ☐ **b.** RDS:00, console session record, AST:HW:Hardware:04, unassessed
- ☐ **c.** RDS:00, console session record, AN:ATT:Attack Path:01, unassessed
- ☐ **d.** RDS:01, console session record, AST:HW:Hardware:04, Gap

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 says what it is about, the objective where it lands
- ☐ **b.** Invalid: the objective waypoint has to be the same element as the anchor
- ☐ **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

A noise-floor measurement and a host record have to be compared, and nothing on the platform emits a key they share. What does the method join them on?

- ☐ **a.** A correlation identifier, added to every source and then required
- ☐ **b.** The timestamp, matched to the second across both time bases
- ☐ **c.** The enumerated element each names, with time as a filter after it
- ☐ **d.** The ticket number the duty officer opens when the alert first fires

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 about it
- ☐ **c.** Nothing, since a source that does not exist cannot be enumerated
- ☐ **d.** A note in the path description, so the field stays clean

© 2026 ethicallyHackingspace (eHs)®

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 catalog checkpoint

Q13 Attack-path catalog 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, one per Day-2 threat
- ☐ **c.** 44; one path per enumerated element
- ☐ **d.** 1; one path per working-session artifact

Q14 Attack-path catalog checkpoint

What grounds each path 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 written for it
- ☐ **d.** Waypoints through real elements, and a cited source

Q15 Attack-path catalog checkpoint

How do the RDS and RSS records feed Day 4?

- ☐ **a.** Day 4 writes the detection 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

© 2026 ethicallyHackingspace (eHs)®

Q16 Attack-path catalog 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 catalog 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

Q18 Attack-path catalog checkpoint

AN:ATT:Attack Path:00 is held in MISP as one event. Which reading of that event is correct?

- ☐ **a.** Tagged meteorstorm:AN=AN-THR; target AST:SW:Software:03, where the route lands; sources as attributes
- ☐ **b.** Tagged meteorstorm:AN=AN-ATT; target AST:SW:Software:03, chosen by the path; sources in the description
- ☐ **c.** Tagged meteorstorm:AN=AN-DET; target SVC:CP:Control Plane:08, the entry; sources as separate events
- ☐ **d.** Tagged meteorstorm:AN=AN-ATT; target SVC:CP:Control Plane:09, from its threat; sources as attributes

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 2 hand you to work from today?

> **c. Four AN-THR threats, each anchored by its TOE to one enumerated 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 During the Kiruna uplink outage, Satellite Operations sees the spacecraft's uplink noise floor rise in telemetry while Security Operations sees a healthy event stream. Why can neither settle the cause?

> **a. Both observations are valid, and no shared identifier joins the two**

Each side holds a true observation of one outage: a continuously sampled measurement, and records stamped by whichever host wrote them. Nothing carries a key both sides share, and Path 02 carries three measurements and no record, so nothing on the record side says whether it was jamming or weather, and neither side alone can say which it was. The scene is in workbook Chapter 5, One outage, two observations; Path 02 is in Chapter 4; the ruling that follows is in Chapter 5, The join.

Q3 The paths and the required sources they carry feed which mandate requirement?

> **d. The detection methods Executive Order 14144 requires on the command-and-control path**

Executive Order 14144 sets the command-and-control protections required of civil space systems, and Kestrel Orbital adopts them as binding by company directive; SCOR writes a detection for each protection it requires (Module 01 workbook, Chapter 1). The attack paths and the RDS and RSS records that would reveal them are what those detections are built on: Module 04 writes one signature per path and reads its required sources (workbook Chapter 3, Choosing the required source when a step emits several).

Q4 Satellite Design & Engineering opens six artifacts today. What do they provide?

> **b. The build knowledge of how the platform moves data and commands**

Satellite Design and Engineering 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.

© 2026 ethicallyHackingspace (eHs)®

Q5 AN:ATT:Attack Path:03 carries its first required data source. What is that record's sub-ordinal?

> **b. RDS:00, counted from 00 in its own field**

The sub-ordinal is a separate counter from the element's ordinal: two digits from 00, per field, per element. Path 03's first required data source is RDS:00. The 03 belongs to the chain; the 00 counts records inside one field of one element (workbook Chapter 3, What one record carries).

Q6 An AN-ATT element names an attack path. What are its waypoints?

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

> **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 Path 01's entry step leaves an operator console session record on AST:HW:Hardware:04, and Security Operations has not yet said whether it receives it. Which record is written correctly?

> **b. RDS:00, console session record, AST:HW:Hardware:04, unassessed**

A session record is received as a record, so it belongs in RDS, and as the first record in that field it is RDS:00. Its element is the one platform element it is observed on, never the path that carries it. Nobody has answered for it, so its state is unassessed; Gap would claim somebody looked and found nothing. This is Path 01's RDS:00 exactly (Chapter 3, What one record carries; Chapter 4).

Q9 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 says what it is about, the objective 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 pushed image rides. The anchor answers what the path is about; the objective answers where the route ends. They may differ.

© 2026 ethicallyHackingspace (eHs)®

Q10 A noise-floor measurement and a host record have to be compared, and nothing on the platform emits a key they share. What does the method join them on?

> **c. The enumerated element each names, with time as a filter after it**

Workbook Chapter 5, The join. A shared identifier was refused because nothing on the platform emits one today, so requiring it would produce a design nobody could implement. The model already forces every required source to name exactly one element (workbook Chapter 3, What one record carries), so the element is the join. Each source states its time base and known offset, and time is the window applied after the join, not the thing doing the joining.

Q11 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**

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 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**

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

> **b. 4; Ground 2, Link 1, Space 1, one per Day-2 threat**

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

Q14 What grounds each path in this set?

> **d. Waypoints through real elements, and a cited source**

Every path in the set walks three real enumerated elements and cites the reporting or framework reference it is anchored to, with its confidence stated beside it (workbook Chapter 1, What you build; Chapter 4).

© 2026 ethicallyHackingspace (eHs)®

Q15 How do the RDS and RSS records feed Day 4?

> **a. Day 4 writes the detection 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 path.

Q16 An AN-ATT element is marked DRIVEN BY AN:THR:Threat:03. What does that tell you?

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

> **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.

Q18 AN:ATT:Attack Path:00 is held in MISP as one event. Which reading of that event is correct?

> **d. Tagged meteorstorm:AN=AN-ATT; target SVC:CP:Control Plane:09, from its threat; sources as attributes**

Workbook Chapter 6, and MISP event 29: the path is one event tagged meteorstorm:AN=AN-ATT. It inherits the one element its threat named, SVC:CP:Control Plane:09, rather than choosing one, and its three required data sources are attributes on the event. AST:SW:Software:03 is the objective waypoint, where the route lands, not the target.

© 2026 ethicallyHackingspace (eHs)®