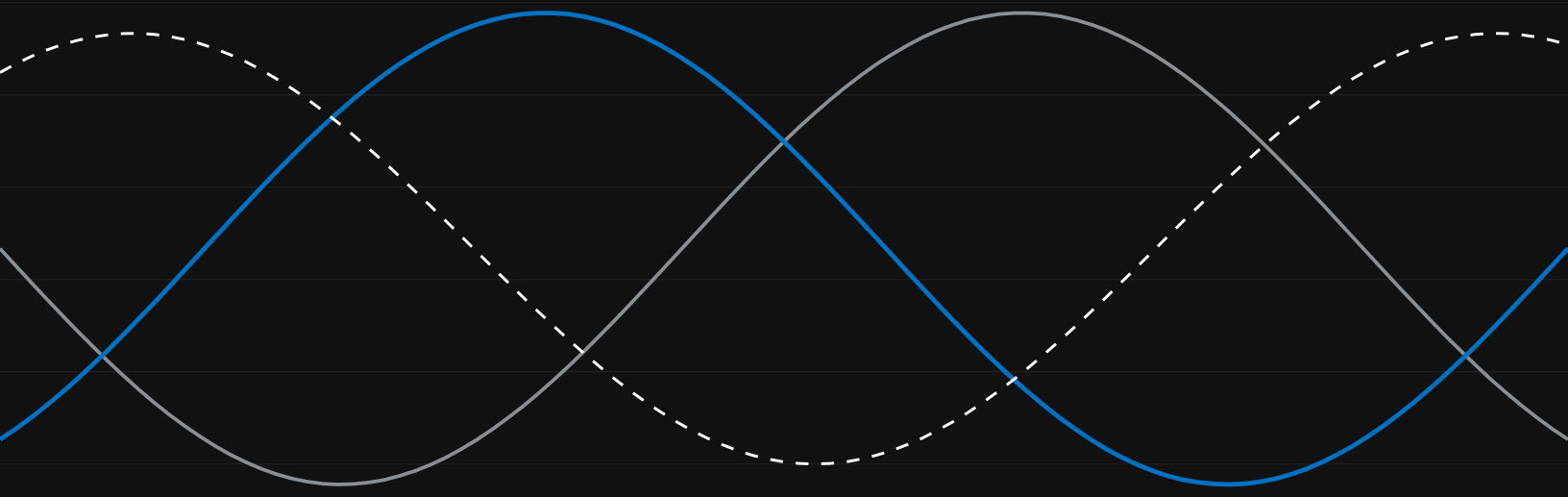
Module 04 · Question set · Student edition

Incident Response Preparation

Every checkpoint question for Module 04, 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 04 Incident Response Preparation, 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 04, Incident Response Preparation, 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 04 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 04 context checkpoint 4

Detection engineering method checkpoint 5

Detection catalog checkpoint 7

KEY **Answer Key** 9

© 2026 ethicallyHackingspace (eHs)®

QS Question Set

Every checkpoint question for this module, 19 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 04 context checkpoint

Q1 Module 04 context checkpoint

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 anchored to it
- ☐ **c.** A coverage-gap register for the Security Operations Center, with no paths behind it
- ☐ **d.** The four attack paths, with the required sources each one carries

Q2 Module 04 context checkpoint

What is your job on Day 4?

- ☐ **a.** Decompose the platform into its PCE, SEG, SVC, and AST elements
- ☐ **b.** Write a signature on each path's sources, and the playbook behind it
- ☐ **c.** Anchor newly reported threats to the one platform element each targets
- ☐ **d.** Remove the attack surface the adversary keeps relying on to reach the platform

Q3 Module 04 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

© 2026 ethicallyHackingspace (eHs)®

Q4 Module 04 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 to the regulation clause it serves
- ☐ **d.** So Satellite Operations knows which subsystems to watch during a pass

Q5 Module 04 context checkpoint

Signature 00 fires at 02:14 UTC on a Saturday. The incident response plan, the rule that fired and the on-call roster are all in hand. Why can no response action run yet?

- ☐ **a.** The rule fired at medium severity, below the threshold the plan sets for action
- ☐ **b.** The roster names nobody from Security Operations on shift that Saturday night
- ☐ **c.** None of the three records who may authorize any of the available actions
- ☐ **d.** The incident response plan has not yet been approved by the regulator

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 between operators
- ☐ **c.** A playbook template for structuring incident response
- ☐ **d.** A vendor-neutral detection format, so one rule ports across tooling

© 2026 ethicallyHackingspace (eHs)®

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 exploited element
- ☐ **c.** The confidence level assigned by the intelligence source
- ☐ **d.** The name of the on-call analyst who owns the alert

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 catalog
- ☐ **c.** You record the detection gap and name the collection that closes it
- ☐ **d.** You lower the confidence on the signature and ship it to production anyway

Q10 Detection engineering method checkpoint

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.** An executor from the action's domain, with Mission Lead as the decider
- ☐ **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

© 2026 ethicallyHackingspace (eHs)®

Q12 Detection engineering method checkpoint

PB-00 halts the patch deployment pipeline. Halting it costs mission time and is recoverable. At what level does it run, and what happens before it is executed?

- ☐ **a.** Solo: Security Operations halts it alone and informs Mission Lead after
- ☐ **b.** Escalated: the Mission Lead approves in writing before execution
- ☐ **c.** Whatever level the on-shift lead chooses, since the ladder is a guide
- ☐ **d.** Collaborative: Satellite Operations co-signs, then Security Operations acts

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: one ordinal, two elements
- ☐ **c.** The threat should be renumbered to match the signature
- ☐ **d.** The signature should be promoted to a second attack path

Detection catalog checkpoint

Q14 Detection catalog 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 catalog checkpoint

PB-01 radiates the Kiruna uplink only for commanding sessions released under two-person review, an action taken on a ground element. What is the action's domain, and who executes it?

- ☐ **a.** Space, by Satellite Operations: it changes what the live uplink may carry
- ☐ **b.** Cyber, by Security Operations: it is taken on a ground-segment element
- ☐ **c.** Cyber, executed by the Mission Lead: it needs a two-person review
- ☐ **d.** Space, executed by Security Operations: it follows a cyber signature

© 2026 ethicallyHackingspace (eHs)®

Q16 Detection catalog checkpoint

Signature 01 watches command-authority usage against a baseline. What does the shipped rule baseline, and where do its known benign causes sit?

- ☐ **a.** Nothing: it keeps only the peer-review tag check, with no shift condition
- ☐ **b.** Each named operator's own working hours, with benign causes left to the analyst
- ☐ **c.** A high-confidence threshold, so a night shift can never trip the rule alone
- ☐ **d.** The role and shift, not the person, with the known benign causes in the rule's details

Q17 Detection catalog 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 catalog checkpoint

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

- ☐ **a.** The SOC runs the rules, each role executes its actions, engineering closes gaps
- ☐ **b.** Only the Security Operations Center reads the set, in its daily monitoring
- ☐ **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 naming first

Q19 Detection catalog checkpoint

Signature 00 is held in MISP as event 30. Which reading of that event is correct?

- ☐ **a.** Tagged meteorstorm:AN="AN-ATT"; TDM AST:SW:Software:03, where the route lands; playbook PB-00
- ☐ **b.** Tagged meteorstorm:AN="AN-DET"; TDM SVC:CP:Control Plane:08, the entry step; no playbook attribute
- ☐ **c.** Tagged meteorstorm:AN="AN-DET"; TDM SVC:CP:Control Plane:09, its threat's TOE; playbook PB-00
- ☐ **d.** Tagged meteorstorm:AN="AN-THR"; TDM chosen by the analyst; playbook named in the description only

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 3 hand you that Day 4 builds on?

> **d. The four attack paths, with the required sources each one carries**

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 What is your job on Day 4?

> **b. Write a signature on each path's sources, and the playbook behind it**

Incident response preparation turns each attack path into one AN-DET signature, written on the path's required sources, and a response playbook.

Q3 Which department leads Day 4's working session?

> **c. The Security Operations Center, which runs the detections**

Day 4 runs in the Security Operations Center, the team that writes and tunes the detections and triggers the playbooks. Each playbook action is then executed by the role its domain names, Security Operations for cyber and Satellite Operations for space.

Q4 Why does every detection trace back to an attack path?

> **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.

© 2026 ethicallyHackingspace (eHs)®

Q5 Signature 00 fires at 02:14 UTC on a Saturday. The incident response plan, the rule that fired and the on-call roster are all in hand. Why can no response action run yet?

> **c. None of the three records who may authorize any of the available actions**

Each document answers a different question: the plan says who to notify, the rule says what fired, the roster says who is on call. None records who may take any of the available actions, so each department holds part of the answer and nothing can run until somebody senior is found. The playbook closes that gap by recording each approved action with its executor and its decider in advance (workbook Chapter 3, Why this is enforced rather than encouraged).

Q6 What does the TDM field on an AN-DET element name?

> **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 What is RootA, and why write signatures in it?

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

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

> **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.

© 2026 ethicallyHackingspace (eHs)®

Q10 What runs when a signature fires?

> **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 Who executes an approved action, and who decides it?

> **a. An executor from the action's domain, with Mission Lead as the decider**

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 PB-00 halts the patch deployment pipeline. Halting it costs mission time and is recoverable. At what level does it run, and what happens before it is executed?

> **d. Collaborative: Satellite Operations co-signs, then Security Operations acts**

Costs mission time and is recoverable is the disruptive class, and the ladder reads disruptive as collaborative: the other operating role co-signs before execution, as the Consulted party. PB-00 ACT:02 is executed by Security Operations, with Satellite Operations consulted and Mission Lead accountable. The level is read off reversibility, never chosen.

Q13 A signature carries ordinal 00 but its TDM names a different element from the TOE of AN:THR:Threat:00. What has happened?

> **b. The chain is broken: one ordinal, two elements**

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

> **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.

© 2026 ethicallyHackingspace (eHs)®

Q15 PB-01 radiates the Kiruna uplink only for commanding sessions released under two-person review, an action taken on a ground element. What is the action's domain, and who executes it?

> **a. Space, by Satellite Operations: it changes what the live uplink may carry**

The effect test asks what the action changes, not where it is taken. Holding the uplink to reviewed commands changes what the live uplink may carry, which is mission operational state, so the domain is space and Satellite Operations executes it, with a why line because the element is a ground one. The element records where, not what (workbook Chapter 3, The effect test sets the domain). Mission Lead decides and never executes.

Q16 Signature 01 watches command-authority usage against a baseline. What does the shipped rule baseline, and where do its known benign causes sit?

> **d. The role and shift, not the person, with the known benign causes in the rule's details**

Workbook Chapter 4, The worked rule in full: the rule detects command-authority usage outside the role and shift baseline, not outside one operator's hours, and its known benign causes, operator travel filed with notice and a documented emergency override carrying an incident ticket, are written into details, because RootA has no falsepositives field. The source state is Partial because the peer-review tag stream depends on workflow adoption.

Q17 What does Day 5 do with what recurs across today's detections and the earlier paths?

> **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 on the flying platform, or writes them into the next build where the element cannot be changed.

Q18 Once written, how do the three departments use the detection set?

> **a. The SOC runs the rules, each role executes its actions, engineering closes gaps**

Because each detection names its element and its gap, the three departments work from one catalog: Security Operations runs the signatures and executes the cyber actions, Satellite Operations executes the space actions, and Satellite Design and Engineering closes the collection gaps the rules exposed.

Q19 Signature 00 is held in MISP as event 30. Which reading of that event is correct?

> **c. Tagged meteorstorm:AN="AN-DET"; TDM SVC:CP:Control Plane:09, its threat's TOE; playbook PB-00**

Workbook Chapter 6, The record in MISP: the signature is one event tagged meteorstorm:AN="AN-DET". Its TDM attribute names SVC:CP:Control Plane:09, the same element AN:THR:Threat:00 names as its TOE, inherited rather than chosen, and its PLAYBOOK attribute names PB-00, the response the signature authorizes.

© 2026 ethicallyHackingspace (eHs)®