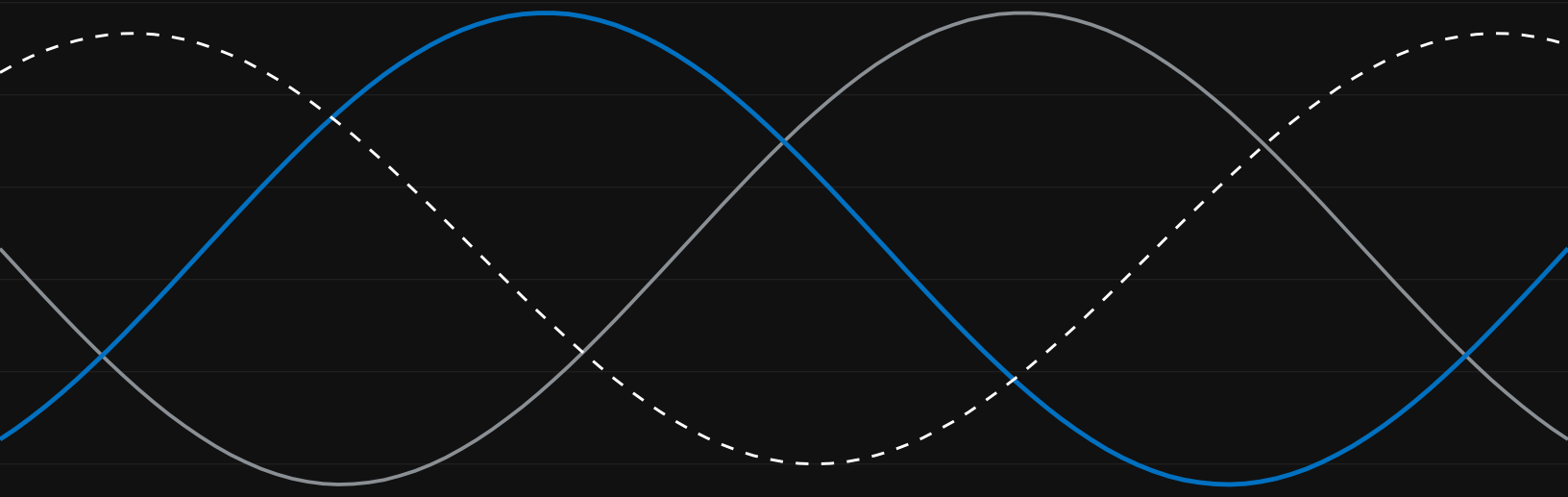
Module 01 · Question set · Student edition

Concept of Operations

Every checkpoint question for Module 01, with the answer key.



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 01 Concept of Operations, 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 01, Concept of Operations, 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 01 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

Context checkpoint 4
Data model checkpoint 5
PCE checkpoint 7
Segment checkpoint 8
Service checkpoint 9
Asset checkpoint 10
Enumeration checkpoint 12

KEY **Answer Key** 14

© 2026 ethicallyHackingspace (eHs)®

QS Question Set

Every checkpoint question for this module, 38 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.

Context checkpoint

Q1 Context checkpoint

You were hired into Kestrel Orbital to establish which new department?

- ☐ **a.** SCOR, Space Cybersecurity Operations and Resilience
- ☐ **b.** A second Security Operations Center for the space side
- ☐ **c.** The Satellite Operations Center, newly stood up
- ☐ **d.** A compliance office reporting to the regulators

Q2 Context checkpoint

SCOR works across which three existing departments to drive them toward resilient cyber operations?

- ☐ **a.** Mission Assurance, Launch Services, and Ground Network Operations
- ☐ **b.** Security Operations, Satellite Operations, and Satellite Design & Engineering
- ☐ **c.** Flight Dynamics, Mission Planning, and Spacecraft Health Monitoring
- ☐ **d.** Launch Operations, Payload Engineering, and Recovery Services

Q3 Context checkpoint

What is the core problem SCOR was created to solve?

- ☐ **a.** The satellite hardware keeps failing on orbit without warning
- ☐ **b.** There are not enough detection rules written for the platform’s command path
- ☐ **c.** The three departments defend one platform but describe it differently
- ☐ **d.** The regulators require a dedicated cyber department by name

© 2026 ethicallyHackingspace (eHs)®

Q4 Context checkpoint

Day 1 starts by decomposing the telecommand path. Why that part of the platform first?

- ☐ **a.** It is the command-and-control path that all three mandates bind
- ☐ **b.** It is the newest part of the platform, so it has no documentation yet
- ☐ **c.** It is the only part of the platform that flies on orbit
- ☐ **d.** It is the only path Satellite Operations does not already monitor

Q5 Context checkpoint

Three mandates set the Day 1 scope. One is the Space ISAC sharing duty. Which are the other two?

- ☐ **a.** SPD-5 and the Outer Space Treaty of 1967
- ☐ **b.** ISO 27001 and the SOC 2 audit standard
- ☐ **c.** The Outer Space Treaty and the ITAR export rules
- ☐ **d.** Executive Order 14144 and the NIS2 Directive

Q6 Context checkpoint

How is the Space ISAC mandate scoped for SCOR?

- ☐ **a.** Share everything the SOC sees with Space ISAC members in real time
- ☐ **b.** A redacted alert on a confirmed command-and-control attack, shared machine to machine
- ☐ **c.** Space ISAC membership alone satisfies it, with no alert and no machine-to-machine channel
- ☐ **d.** It is scoped to an annual membership report and nothing else

Data model checkpoint

Q7 Data model checkpoint

The data model you bring the three departments has two halves. Its taxonomy is:

- ☐ **a.** The controlled set of names: the shared names every element is given
- ☐ **b.** The rules for how the named elements relate to each other, layer to layer
- ☐ **c.** The catalog of threats the Analytic layer records
- ☐ **d.** The per-instance descriptions the enumeration adds

© 2026 ethicallyHackingspace (eHs)®

Q8 Data model checkpoint

The second half of that model, the ontology, is:

- ☐ **a.** The controlled list of element names the published taxonomy defines
- ☐ **b.** The catalog of detection signatures the SOC will run
- ☐ **c.** The enumeration procedure walked once for every element
- ☐ **d.** The rules for how the named elements relate, the parent chain

Q9 Data model checkpoint

You decompose Kestrel Orbital's platform into elements across which four layers?

- ☐ **a.** TCP, IP, DNS, TLS
- ☐ **b.** People, Process, Technology
- ☐ **c.** PCE, SEG, SVC, AST
- ☐ **d.** Confidentiality, Integrity, Availability

Q10 Data model checkpoint

The four layers form a strict parent chain. Which layer is the root that every element you enumerate resolves to through the parent chain?

- ☐ **a.** AST (Asset), the concrete element layer
- ☐ **b.** SVC (Service), the delivered function layer
- ☐ **c.** SEG (Segment), the operational enclave layer
- ☐ **d.** PCE (Primary Capability Environment)

Q11 Data model checkpoint

Which of these is a correctly formed ETEN for Kestrel Orbital's Kiruna ground enclave?

- ☐ **a.** SEG-GR-Ground-01-The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.
- ☐ **b.** SEG:GR:Ground:1:The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.
- ☐ **c.** SEG:GR:Ground:01:The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.
- ☐ **d.** SEG:GR:Kiruna:01:The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.

© 2026 ethicallyHackingspace (eHs)®

PCE checkpoint

Q12 PCE checkpoint

What does the Primary Capability Environment (PCE) layer add that an inventory starting at the asset cannot give you?

- ☐ **a.** The concrete assets that implement each named service
- ☐ **b.** The list of software vulnerabilities on the platform
- ☐ **c.** The enclaves the platform is distributed into, one per role
- ☐ **d.** The operating environment, named as a first-class element

Q13 PCE checkpoint

Every SEG, SVC, and AST element resolves to a PCE element through the parent chain. Why does that matter?

- ☐ **a.** So the environment can be patched like an asset
- ☐ **b.** So detections can fire at the environment layer instead of at the asset layer below
- ☐ **c.** Because regulators require five layers
- ☐ **d.** So every downstream element inherits the same environment context automatically

Q14 PCE checkpoint

Kestrel Orbital's Day-1 CONOPS populates how many of the five PCE environments, and which?

- ☐ **a.** All five
- ☐ **b.** One: Orbital only
- ☐ **c.** Two: Terrestrial and Orbital
- ☐ **d.** Three: Terrestrial, Aerial, and Orbital

Q15 PCE checkpoint

PCE records the environment, the where. What does it deliberately NOT name?

- ☐ **a.** The orbital regime the platform flies in
- ☐ **b.** The spacecraft and equipment operating there
- ☐ **c.** The atmospheric region the platform crosses
- ☐ **d.** The maritime domain a tracking vessel works in

© 2026 ethicallyHackingspace (eHs)®

Q16 PCE checkpoint

Why does naming the environment matter to Satellite Design & Engineering?

- ☐ **a.** It reduces the number of elements you have to enumerate on the platform at all
- ☐ **b.** It moves detection work from the SOC to Satellite Operations
- ☐ **c.** The same hardware behaves differently on the ground than on orbit
- ☐ **d.** Space platforms cannot be modeled at the asset layer at all

Segment checkpoint

Q17 Segment checkpoint

As you decompose the platform for the three departments, what does the Segment (SEG) layer name?

- ☐ **a.** The self-contained enclaves the platform is distributed into
- ☐ **b.** The orbital regime the platform flies in, which is the environment
- ☐ **c.** The concrete assets that implement each named service
- ☐ **d.** The function an enclave delivers to the wider platform

Q18 Segment checkpoint

For Kestrel Orbital's satellite-control scope, which three SEG TAGs do you enumerate (across its four SEG elements)?

- ☐ **a.** Launch, Aquatic, Deep Space
- ☐ **b.** Space, Link, Ground
- ☐ **c.** Space, Ground, User
- ☐ **d.** Launch, Link, Ground

Q19 Segment checkpoint

Every SEG element you enumerate names what in its PARENT field?

- ☐ **a.** One or more PCE (environment) elements above it
- ☐ **b.** One or more SVC elements below it
- ☐ **c.** Nothing; SEG is the top layer
- ☐ **d.** The Analytic elements that reference it

© 2026 ethicallyHackingspace (eHs)®

Q20 Segment checkpoint

Why does naming the segment matter to the departments you are aligning?

- ☐ **a.** Regulators require segment names in every incident filing
- ☐ **b.** It fixes which orbital regime the platform actually flies in, for the record
- ☐ **c.** It lets each department keep its own segment names locally
- ☐ **d.** Adversaries pick an enclave, so naming it names what you defend

Q21 Segment checkpoint

How many SEG taxonomic elements does the published taxonomy define?

- ☐ **a.** Four
- ☐ **b.** Six
- ☐ **c.** Ten
- ☐ **d.** Fifty-four

Service checkpoint

Q22 Service checkpoint

What does the Service (SVC) layer record for the three departments?

- ☐ **a.** The enclave the platform is distributed into
- ☐ **b.** The physical hardware in a rack
- ☐ **c.** The orbit the platform flies in
- ☐ **d.** The function an enclave delivers, what it actually does

Q23 Service checkpoint

The three SVC values you tag services with are:

- ☐ **a.** Hardware, Software, Firmware
- ☐ **b.** Control Plane, Data Plane, Hybrid
- ☐ **c.** Space, Link, Ground
- ☐ **d.** Read, Write, Execute

© 2026 ethicallyHackingspace (eHs)®

Q24 Service checkpoint

Command and Data Handling (C&DH) is which SVC value?

- [ ] **a.** Control Plane
- [ ] **b.** Data Plane
- [ ] **c.** Hybrid
- [ ] **d.** Signal

Q25 Service checkpoint

A service that would run across more than one segment is recorded how? (None of Kestrel's fifteen services does; this is the rule for one that would.)

- [ ] **a.** As duplicate service elements, one per segment
- [ ] **b.** With DISTRIBUTED set to Y and every participating SEG listed in PARENT
- [ ] **c.** It anchors to the Ground segment alone, as the controlling enclave for it
- [ ] **d.** With a SUBSYSTEM tag naming each segment it crosses

Q26 Service checkpoint

Why would the Security Operations Center write a detection rule against a service rather than against the device that runs it?

- [ ] **a.** Because SVC elements carry the platform's IP addresses and service ports
- [ ] **b.** Because regulators require every rule to cite a named service
- [ ] **c.** Because the segment layer is far too broad to alert against
- [ ] **d.** So the rule fires on the function and survives a hardware refresh

Asset checkpoint

Q27 Asset checkpoint

The Asset (AST) layer is where your three departments converge. What does it name?

- [ ] **a.** The concrete elements that implement a service
- [ ] **b.** The operating environment the platform runs in
- [ ] **c.** The function an enclave delivers to the platform
- [ ] **d.** The enclaves the platform is distributed into

© 2026 ethicallyHackingspace (eHs)®

Q28 Asset checkpoint

The six AST values you tag assets with are:

- ☐ **a.** Control Plane, Data Plane, Hybrid, Space, Link, Ground
- ☐ **b.** Hardware, Firmware, Software, Data, Signal, Hybrid
- ☐ **c.** Read, Write, Execute, Delete, Modify, Own
- ☐ **d.** PCE, SEG, SVC, AST, AN, TEN

Q29 Asset checkpoint

Each AST element you enumerate names what in its PARENT field?

- ☐ **a.** A PCE directly
- ☐ **b.** The Analytic elements that target it
- ☐ **c.** One or more SVC (service) parents
- ☐ **d.** Another asset

Q30 Asset checkpoint

Why is AST the layer where the work actually happens?

- ☐ **a.** It is the only layer the SOC can see in the telemetry feed
- ☐ **b.** Patching, monitoring and replacing act on assets, not on services
- ☐ **c.** It is the first layer the enumeration procedure visits
- ☐ **d.** It is the only layer that carries a description

Q31 Asset checkpoint

What optional tag can an AST element carry, and why?

- ☐ **a.** A DISTRIBUTED tag, because assets can span segments
- ☐ **b.** A PARENT tag, because naming a parent is optional at the asset layer
- ☐ **c.** No optional tags are allowed at the asset layer
- ☐ **d.** A SUBSYSTEM tag, to group several assets into one physical group

© 2026 ethicallyHackingspace (eHs)®

Enumeration checkpoint

Q32 Enumeration checkpoint

The Day-1 deliverable is a CONOPS of how many elements, split how?

- [ ] **a.** 44 = 4 PCE + 4 SEG + 15 SVC + 21 AST
- [ ] **b.** 44 = 2 PCE + 4 SEG + 16 SVC + 22 AST
- [ ] **c.** 40 = 4 PCE + 4 SEG + 15 SVC + 17 AST
- [ ] **d.** 44 = 4 PCE + 2 SEG + 17 SVC + 21 AST

Q33 Enumeration checkpoint

An element that falls outside the scope the enumeration declared is:

- [ ] **a.** Enumerated with a SUBSYSTEM tag
- [ ] **b.** Enumerated but left without a parent
- [ ] **c.** Not enumerated
- [ ] **d.** Moved to the Analytic layer

Q34 Enumeration checkpoint

In the Module 01 story film, Dana Whitfield wants a complete decomposition before anything else. How is it ruled, and what happens to her objection?

- [ ] **a.** Overruled and erased; the whole platform is enumerated first
- [ ] **b.** The telecommand path is the first pass; the objection is recorded and Dana holds the backlog
- [ ] **c.** Upheld; enumeration waits until Design and Engineering has confirmed every asset on the platform
- [ ] **d.** Deferred to the Security Operations Center, which owns the scope of every pass

Q35 Enumeration checkpoint

Every parent chain you enumerate terminates at a PCE, because PCE is the root. What does that buy the departments?

- [ ] **a.** Any element named can be traced to a physical place and a jurisdiction
- [ ] **b.** It keeps the element count balanced evenly across all four of the layers
- [ ] **c.** It lets an asset be counted under more than one parent service
- [ ] **d.** It gives the Analytic layer a parent element to inherit from

© 2026 ethicallyHackingspace (eHs)®

Q36 Enumeration checkpoint

Which pair are both PCE elements in the Day-1 deliverable?

- ☐ **a.** The Reston site and the GEO regime
- ☐ **b.** The Ground segment and the Link segment
- ☐ **c.** Telecommand and C&DH
- ☐ **d.** The OBC and the OBDH bus

Q37 Enumeration checkpoint

MISP event 27 (workbook Chapter 7) carries the tag meteorstorm:SVC="SVC-CP" and the attribute SVC:CP:Control Plane:09, whose comment carries PARENT: SEG:GR:Ground:00. What does each one tell you?

- ☐ **a.** The tag names the one real element; the attribute repeats its type so that the whole event can be searched
- ☐ **b.** The tag records the element's parent segment; the attribute records the element's ordinal alone
- ☐ **c.** The tag names the type, Control Plane; the attribute names one real element and its comment its parent
- ☐ **d.** The tag and the attribute are two copies of one identifier, kept so a partner can pick either

Q38 Enumeration checkpoint

In the Module 01 story film, Maya Reyes asks why her analysts should learn a second taxonomy when they have used MITRE ATT&CK for years. What is the answer?

- ☐ **a.** ATT&CK is retired, and every detection is rewritten against METEORSTORM before Module 03
- ☐ **b.** ATT&CK stays and keeps describing what an adversary does; METEORSTORM names the platform element it lands on
- ☐ **c.** The objection is upheld, and METEORSTORM is used by Satellite Design and Engineering only
- ☐ **d.** Both are set aside for a new platform that SCOR procures and stands up for all three departments

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 You were hired into Kestrel Orbital to establish which new department?

> **a. SCOR, Space Cybersecurity Operations and Resilience**

You lead SCOR, Kestrel Orbital's new Space Cybersecurity Operations and Resilience department. Its mission is to evolve the existing departments toward resilient cyber operations; aligning them onto one shared data model is how it gets there.

Q2 SCOR works across which three existing departments to drive them toward resilient cyber operations?

> **b. Security Operations, Satellite Operations, and Satellite Design & Engineering**

SCOR's mission is to evolve these three departments toward resilient cyber operations. One shared description of the platform is the means: it lets enrichment cross their handoffs without re-translation.

Q3 What is the core problem SCOR was created to solve?

> **c. The three departments defend one platform but describe it differently**

SCOR's mission is to evolve the three departments into one resilient cyber operation, able to anticipate, withstand, and recover from attacks together. With no centralized taxonomy, ontology, or enumeration process, each names the platform its own way, so a threat moving from the Ground segment onto the Link is re-explained at every handoff and detection and recovery lag. The centralized taxonomy, ontology, and enumeration process are the means to that resilience.

Q4 Day 1 starts by decomposing the telecommand path. Why that part of the platform first?

> **a. It is the command-and-control path that all three mandates bind**

The telecommand path runs from the operator console to the spacecraft. Executive Order 14144 sets the protections Kestrel Orbital adopts as binding by company directive on that command and control, encrypt the commands, guarantee their integrity, authenticate the source, and reject unauthorized commands, and the NIS2 Directive puts the ground-based infrastructure that carries it under mandatory risk-management and incident-reporting obligations. The third mandate, Space ISAC, is a redacted alert on a confirmed command-and-control attack, so it lands on the same path (workbook Chapter 1). You decompose it first because that is where all three obligations land and where you have to be able to show they are met.

© 2026 ethicallyHackingspace (eHs)®

Q5 Three mandates set the Day 1 scope. One is the Space ISAC sharing duty. Which are the other two?

> **d. Executive Order 14144 and the NIS2 Directive**

Executive Order 14144 in the United States sets the command-and-control protections required of civil space systems, which Kestrel Orbital adopts as binding by company directive; the NIS2 Directive in Europe places the ground-based infrastructure that carries it under mandatory risk-management and incident-reporting obligations. Together they make the telecommand path a standing obligation, not a choice, which is why you decompose it first. The third mandate that sets the scope, Space ISAC, is the sharing duty: a redacted alert on a confirmed command-and-control attack, shared machine to machine (workbook Chapter 1).

Q6 How is the Space ISAC mandate scoped for SCOR?

> **b. A redacted alert on a confirmed command-and-control attack, shared machine to machine**

Space ISAC sharing is not open-ended. SCOR shares a redacted alert on a confirmed command-and-control attack, machine to machine (workbook Chapter 1). The detections themselves are the Executive Order 14144 duty and the reporting clocks are the NIS2 duty; the sharing is scoped to the confirmed attack.

Q7 The data model you bring the three departments has two halves. Its taxonomy is:

> **a. The controlled set of names: the shared names every element is given**

The taxonomy is the published set of taxonomic elements: every element takes its TAG and LABEL from it, so Security Operations, Satellite Operations, and Satellite Design & Engineering record the same element under the same TEN.

Q8 The second half of that model, the ontology, is:

> **d. The rules for how the named elements relate, the parent chain**

The ontology is the relationships: the four layers form a strict parent chain, so any element the departments name carries its full context up to the environment.

Q9 You decompose Kestrel Orbital's platform into elements across which four layers?

> **c. PCE, SEG, SVC, AST**

Primary Capability Environment (PCE), Segment (SEG), Service (SVC), and Asset (AST): the four structural layers every enumerated element belongs to.

© 2026 ethicallyHackingspace (eHs)®

Q10 The four layers form a strict parent chain. Which layer is the root that every element you enumerate resolves to through the parent chain?

> **d. PCE (Primary Capability Environment)**

PCE is the root; every SEG, SVC, and AST element resolves to a PCE through the parent chain, so every enumerated element carries its environment context.

Q11 Which of these is a correctly formed ETEN for Kestrel Orbital's Kiruna ground enclave?

> **c. SEG:GR:Ground:01:The Kiruna, Sweden polar TT&C ground-station enclave: the ground terminal service and its antenna and RF front end that radiate the command path into the link.**

Five colon-delimited fields: LAYER, TAG and LABEL copied from the published TEN (SEG, GR, Ground), a two-digit ORDINAL counted per tag (01, because Reston is 00), and the one canonical description. The hyphenated form is the TEN type form and takes no ordinal; a one-digit ordinal is malformed; and the LABEL is never invented, so Kiruna cannot replace Ground.

Q12 What does the Primary Capability Environment (PCE) layer add that an inventory starting at the asset cannot give you?

> **d. The operating environment, named as a first-class element**

PCE names the environment, the where, as the root of the parent chain. Most models start at the asset and never model the environment the platform operates in.

Q13 Every SEG, SVC, and AST element resolves to a PCE element through the parent chain. Why does that matter?

> **d. So every downstream element inherits the same environment context automatically**

Parent anchoring means an asset resolves up through its service and segment to its environment, so every element carries its operating context for free.

Q14 Kestrel Orbital's Day-1 CONOPS populates how many of the five PCE environments, and which?

> **c. Two: Terrestrial and Orbital**

The telecommand path spans the ground complex and the orbit, so Terrestrial and Orbital are enumerated, held as 4 PCE elements: Reston, Kiruna, GEO, and MEO. The other three environments stay reference.

© 2026 ethicallyHackingspace (eHs)®

Q15 PCE records the environment, the where. What does it deliberately NOT name?

> **b. The spacecraft and equipment operating there**

PCE names only the environment. The spacecraft and equipment that operate in it are named later at the Segment, Service, and Asset layers, keeping the where separate from the what.

Q16 Why does naming the environment matter to Satellite Design & Engineering?

> **c. The same hardware behaves differently on the ground than on orbit**

Workbook Chapter 3.1: Satellite Design & Engineering reads PCE because the same hardware behaves differently on the ground than on orbit. PCE is also the layer that deconflicts nature from adversary: naming the environment keeps a natural anomaly from being chased as an attack and an attack from being written off as weather.

Q17 As you decompose the platform for the three departments, what does the Segment (SEG) layer name?

> **a. The self-contained enclaves the platform is distributed into**

SEG names the enclaves, Space, Link, Ground, User and the rest, the parts an adversary picks to operate against and the parts your three departments defend.

Q18 For Kestrel Orbital's satellite-control scope, which three SEG TAGs do you enumerate (across its four SEG elements)?

> **b. Space, Link, Ground**

Kestrel's telecommand scope enumerates 4 SEG elements across three TAGs: Space (the spacecraft), Link (the uplink and downlink), and Ground (two enclaves: the Reston command authority and the Kiruna TT&C station). The telecommand path runs Ground to Link to Space. SEG-US, the User segment, is a fourth taxonomic element in the published taxonomy, but the customer edge is out of scope for this platform, so it is not enumerated.

Q19 Every SEG element you enumerate names what in its PARENT field?

> **a. One or more PCE (environment) elements above it**

A segment is an enclave inside an environment, so each SEG names one or more PCE parents in the parent chain.

Q20 Why does naming the segment matter to the departments you are aligning?

> **d. Adversaries pick an enclave, so naming it names what you defend**

Nobody attacks 'the satellite'. The Security Operations Center scopes a hunt to a segment, anything on the Link, and that shared boundary is the line all three departments defend.

© 2026 ethicallyHackingspace (eHs)®

Q21 How many SEG taxonomic elements does the published taxonomy define?

> **c. Ten**

Ten segments are published (Launch, Link, Ground, User, Aquatic, Low Altitude, High Altitude, Near Space, Space, Deep Space); Kestrel's telecommand scope uses three (Space, Link, Ground) across 4 SEG elements, the Ground TAG holding the Reston and Kiruna enclaves, and teaches SEG-US, the User segment, as a taxonomic element that is out of scope for this platform.

Q22 What does the Service (SVC) layer record for the three departments?

> **d. The function an enclave delivers, what it actually does**

Two enclaves tagged the same can do different jobs. SVC records the function so the departments can say what is actually at risk, not just which asset is involved.

Q23 The three SVC values you tag services with are:

> **b. Control Plane, Data Plane, Hybrid**

Control Plane commands the platform, Data Plane moves mission product, and Hybrid does both.

Q24 Command and Data Handling (C&DH) is which SVC value?

> **c. Hybrid**

C&DH both commands the bus and routes mission data, so it is a Hybrid service.

Q25 A service that would run across more than one segment is recorded how? (None of Kestrel's fifteen services does; this is the rule for one that would.)

> **b. With DISTRIBUTED set to Y and every participating SEG listed in PARENT**

A cross-segment service stays one element: set DISTRIBUTED to Y and list every participating SEG in PARENT. On Kestrel all fifteen services run inside a single segment, so DISTRIBUTED is N for each.

© 2026 ethicallyHackingspace (eHs)®

Q26 Why would the Security Operations Center write a detection rule against a service rather than against the device that runs it?

> **d. So the rule fires on the function and survives a hardware refresh**

Targeting the function, not the device, means the detection still fires after Satellite Design & Engineering swaps the hardware behind it. A detection names the one element it observes, in whichever layer that element sits: a service when the behavior belongs to the function, an asset when it belongs to one concrete element (workbook Chapter 3.3 and 3.4).

Q27 The Asset (AST) layer is where your three departments converge. What does it name?

> **a. The concrete elements that implement a service**

AST is the concrete layer where the departments meet: the actual hardware, code, data, and signals a patch lands on, and the layer a detection resolves to when it names one concrete element.

Q28 The six AST values you tag assets with are:

> **b. Hardware, Firmware, Software, Data, Signal, Hybrid**

Hardware, Firmware, Software, Data, Signal, and Hybrid are the six asset classes.

Q29 Each AST element you enumerate names what in its PARENT field?

> **c. One or more SVC (service) parents**

An asset implements a service, so every AST names at least one SVC parent and its parent chain reads straight up through that service to the segment and the environment. Where one physical asset carries several services, it names all of them: the flight computer that runs command handling, attitude control and attack detection is one asset with three service parents, and an adversary who takes it takes all three.

Q30 Why is AST the layer where the work actually happens?

> **b. Patching, monitoring and replacing act on assets, not on services**

Satellite Design & Engineering does not patch ’the control plane’; they patch a specific firmware image on a specific device. A patch lands at AST resolution, and so does a detection that names one concrete element; that is where all three departments converge.

© 2026 ethicallyHackingspace (eHs)®

Q31 What optional tag can an AST element carry, and why?

> **d. A SUBSYSTEM tag, to group several assets into one physical group**

An AST element takes one or more SVC parents and an optional SUBSYSTEM tag that groups several assets into one physical group, such as the spacecraft bus group workbook Chapter 6.4 recommends; the Day 1 inventory does not record a SUBSYSTEM value yet. Units inside one asset, like the sensors in AST:HW:Hardware:00, need no tag: they are already one element.

Q32 The Day-1 deliverable is a CONOPS of how many elements, split how?

> **a. 44 = 4 PCE + 4 SEG + 15 SVC + 21 AST**

The telecommand-path CONOPS holds 44 elements: 4 environments, 4 segments, 15 services, and 21 assets, every parent link populated below the root.

Q33 An element that falls outside the scope the enumeration declared is:

> **c. Not enumerated**

The scope constraint is absolute: an element outside the Step 01 scope is not enumerated. SEG-US, the User segment, is the worked example, real in the taxonomy, out of scope on this platform.

Q34 In the Module 01 story film, Dana Whitfield wants a complete decomposition before anything else. How is it ruled, and what happens to her objection?

> **b. The telecommand path is the first pass; the objection is recorded and Dana holds the backlog**

Module 01 story film: the first pass is the telecommand path, from the operator console to execution on board. Dana's objection is recorded, and she holds the backlog. Workbook Chapter 6 states the same boundary: a complete, parented decomposition of the telecommand path, not a complete model of Kestrel Orbital.

Q35 Every parent chain you enumerate terminates at a PCE, because PCE is the root. What does that buy the departments?

> **a. Any element named can be traced to a physical place and a jurisdiction**

A root is what makes the parent chain terminate, and a chain that terminates somewhere physical is what lets three departments argue about the same thing. Name any asset and you can walk up to the site or the orbit regime it lives in, which is what pins the regulator, the owner and the environment to it. The other three are real ideas in the wrong place: layer counts are never balanced and are not meant to be; shared assets are a cardinality rule, not a root rule; and the Analytic layer has no parent at all, it anchors through a target field instead.

© 2026 ethicallyHackingspace (eHs)®

Q36 Which pair are both PCE elements in the Day-1 deliverable?

> **a. The Reston site and the GEO regime**

The four PCE elements are the Reston and Kiruna terrestrial sites plus the GEO and MEO orbital regimes; segments, services, and assets live in the lower layers.

Q37 MISP event 27 (workbook Chapter 7) carries the tag meteorstorm:SVC="SVC-CP" and the attribute SVC:CP:Control Plane:09, whose comment carries PARENT: SEG:GR:Ground:00. What does each one tell you?

> **c. The tag names the type, Control Plane; the attribute names one real element and its comment its parent**

A layer tag classifies the event by type: meteorstorm:SVC="SVC-CP" says a Control Plane service is involved, and it is identical in every organization. The attribute is the ETEN, the one Kestrel element, SVC:CP:Control Plane:09, ACA (Ground), and its comment carries PARENT: SEG:GR:Ground:00, the Reston enclave it resolves through to PCE:TE:Terrestrial:00. Five tags classify the event; five attributes carry the records (workbook Chapter 7; the elements are in the Chapter 6 tables).

Q38 In the Module 01 story film, Maya Reyes asks why her analysts should learn a second taxonomy when they have used MITRE ATT&CK for years. What is the answer?

> **b. ATT&CK stays and keeps describing what an adversary does; METEORSTORM names the platform element it lands on**

Module 01 story film: ATT&CK stays. It describes what an adversary does, and it was never designed to name a part of a space platform. Adoption is not a purchase: the taxonomy is published openly as a MISP taxonomy, and Kestrel already runs MISP.

© 2026 ethicallyHackingspace (eHs)®