

FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

The Pentagon of Pain

Detect, disrupt, deter space threats. The mindset that judges security work by what it costs the adversary, its five mastery areas, and the exercises that make you apply it. Stands alone, inside or outside the course.

COPYRIGHT AND LEGAL NOTICES

© 2026 D2 Team CORP, a 501(c)(3) nonprofit. All rights reserved.

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. Redistribution outside the cohort and those bodies is not authorized.

Verbatim sources. Every taxonomy definition in this document is the published METEORSTORM taxonomy text, quoted exactly. Definitions are never abbreviated, paraphrased, or reworded in this publication.

Trademarks. ethicallyHackingspace (eHs)® is a brand of D2 Team CORP, not a separate legal entity. 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	The Pentagon of Pain, question set, student edition
EDITION	Student edition · revised 2026-09-24
CONTACT	www.d2teamcorp.org

STUDENT EDITION

Every exercise, with the answer and the reason it is the answer. Work them before you read the key.

CONTENTS

- 01 EX Exercises
- 02 KEY Answer Key

EX EXERCISES

Work these on paper or in your notes before opening the answer key. Every exercise is answerable from this guide alone, and each names the chapter it draws on. Every scenario is the Viasat case or a hypothetical operator: nothing here asks about your own organization.

RECALL

RECALL 1

Ch. 1

State what the Pentagon of Pain is and what it is not, and give the one-sentence relationship between the mindset and the framework in the order this guide states it.

RECALL 2

Ch. 1, 10

Name the five mastery areas in order and, beside each, the framework function it is judged against. One pair carries different names on each side: which, and why is the function not renamed?

RECALL 3

Ch. 2.4

In a Pain Index, which column is a measure of performance and which is a measure of effectiveness? Which one does the Pain score summarize, and who is never allowed to score it?

RECALL 4

Ch. 3.3

Name the four stages of the arc, and state what a department at the third stage asks for the first time.

RECALL 5

Ch. 6.4

Converged Detection Engineering has two deliverables. Name both, and explain in one sentence why the required-source inventory has two fields rather than one.

RECALL 6

Ch. 2.3, 8.2

Where does a civilian operator's adversary management end, according to JP 3-12, and through which artifact does the evidence leave the organization?

APPLICATION

APPLICATION 1

Ch. 2.4, 9

A draft status report reads: “Our new detection platform raises adversary cost.” Rewrite it so the cost is concrete, using the Viasat management path. Name the element, the mastery area with the function it is judged against, and what the adversary must now do.

APPLICATION 2

Ch. 5.4

A threat-modeling session for a hypothetical operator produces this candidate: “Solar activity degrades the uplink during the northern ground station’s pass.” Apply the gate. Does it enter the threat catalogue? If not, state whether either exclusion reason applies, or whether it belongs somewhere else in the model, and where, and what adversary threat it points to.

APPLICATION 3

Ch. 6, 7

In the Viasat case, the fleet-wide modem lock status at the gateway would have shown the wipe as it propagated, but no defensive cyber operator was holding it. Record it as a required source: which of the two kinds is it, what state would it have carried before the attack, which department would own closing it, and what does the next function do with a Gap it cannot close in time?

APPLICATION 4

Ch. 8.4

A hypothetical operator’s catalogue shows the ground command-acceptance service named by three of its five threats and four of its five attack paths. Using the recurrence count and the coverage walk, state what the first resilience measure should protect, which NIST SP 800-160 Volume 2 goal a segmentation measure on it would serve, and what the catalogue must record for each of the paths it does not cover.

EXTENSION SCENARIO

EXTENSION

All chapters

An operator’s executive team reads this guide and proposes adopting the Pain Index as a quarterly maturity score, with each department self-assessing its level from Low to Very High. Argue, in the register of this guide, why that proposal would equip without transforming. Then propose what the quarterly measure should be instead, derived from the deliverables of the five functions, and state which of the three departments would carry each number.

WORK EVERY EXERCISE BEFORE YOU READ ON. THE ANSWERS BEGIN ON THE NEXT
PAGE.

KEY ANSWER KEY

Answers with the reasoning, not just the result. If your answer differs, trace which chapter rule it breaks before reading on.

RECALL 1

The Pentagon of Pain is a mindset: a way of judging security work by what it costs the adversary. It is not a framework, a process, a set of controls, a maturity model or a checklist. Transform the mindset, then equip with the framework: the METEORSTORM functions produce the artifacts; the Pentagon judges them. A mindset with no framework is a poster; a framework with no mindset is compliance work with better filing.

RECALL 2

Master Decomposition, Concept of Operations. Master Contextualized Threat Modeling, Contextualized Threat Modeling. Master Converged Detection Engineering, Converged Detection Engineering. Master Exposure Management, Incident Response Preparation. Master Adversary Management, Adversary Management. **The fourth pair differs.** The function is what the framework defines and produces, a signature and a playbook per path; the mastery area is the judgment held over it. Renaming the function would make the mindset contradict the framework it is meant to judge. The bridge is honest: a declared blind spot is exposure, and the signature with its authorized response is the trap at the end of the path.

RECALL 3

The left column, the state of the deliverable, is the **measure of performance**. The Adversary Impact column is the **measure of effectiveness**. The Pain score summarizes the Adversary Impact column only, and it is never self-scored: the left column names a deliverable that can be inspected, and the right column names what the adversary must now do.

RECALL 4

Compliance, Friction, Cost, Ownership. At Cost, a department asks for the first time **what the adversary pays** rather than what the auditor wants. That is the turn, and the point at which the Pain Index starts to mean something.

RECALL 5

The path catalogue, attack paths anchored to the threat's element, and the required-source inventory carried on each path with a state per record. Two fields because a record received and a quantity measured are two kinds of observable, and on a space platform that line decides whether a path is detectable at all: jamming is seen in the noise floor and never in a log.

RECALL 6

It ends at **attribution-quality evidence and its delivery**; response actions outside the defended network (DCO-RA) are reserved to authorized forces. The evidence leaves through the **report stage of the response playbook**, to trusted channels such as Space ISAC and national agencies.

APPLICATION 1

One acceptable rewrite: "A signature on management command volume, timing and scope now fires on the management service that releases commands to the modem fleet, and its playbook isolates the management interface and rate-limits management actions with a named executor. An adversary who reaches the management plane must now push the wipe without tripping the command record, or accept that the first mass command ends the campaign." That is Master Exposure Management judged against Incident Response Preparation. Mark it Proficient if it names an element, a function or its artifact, and a concrete action the adversary must now take. Mark it Developing if the cost is still an adjective.

APPLICATION 2

It does not enter the catalogue. Neither exclusion reason applies, because it is not a threat: there is no adversary. It belongs in the **Primary Capability Environment**, the environment the uplink element lives in. The adversary threat it points to is one that produces the same symptom on purpose, a jamming or interference campaign anchored to the uplink signal element, and the question the mindset then asks is whether the platform holds the signal sources to tell the two apart.

APPLICATION 3

It is a **required signal source**: a lock status is measured in the physical layer, not received as a record. Before the attack its state would have been **Gap** if it had been assessed and nothing was collected, or **unassessed** if nobody had asked; the two are different findings and must not be conflated. Closing it is owned by Satellite Operations, which holds the gateway telemetry, with Engineering if the gateway must be changed to emit it. A Gap that cannot be closed in time becomes a **compensating action in the playbook** of Incident Response Preparation, such as a rate limit or hold on management pushes, with a named owner, until the source is Available and a signature can be written on it.

APPLICATION 4

The first measure protects the **ground command-acceptance service**, because the recurrence count from the catalogues, three of five threats and four of five paths, says a measure there closes the most routes at once. Segmentation of it with attestation on access serves **Anticipate**: it removes the high-impact route before it is taken. For each path the measure does not cover, the catalogue must record either another measure or a **consciously accepted residual risk with an owner and a date**; a residual risk with neither is an omission wearing a label.

EXTENSION

Why it equips without transforming. A self-assessed level is a measure of performance scored by the people who performed it. It tells the executive team what each department did, in the auditor's terms, which is the Compliance stage by definition. It also turns the Pentagon of Pain into a maturity model, which the mindset rules out: a maturity ladder is a set of steps, and the mindset is a way of judging. Nothing in the proposal asks what the adversary now has to do.

What to measure instead. Numbers derived from the deliverables, never self-reported: the count of enumerated elements and the stated scope, from the Concept of Operations, held by Satellite Design and Engineering; the count of anchored threats and recorded exclusions, held by Security Operations; the required-source inventory by state, Available, Partial, Gap and unassessed, with the unassessed count driven to zero, held jointly by Security Operations and Satellite Operations with each Gap's owner named; the count of paths with a signature and a resolvable playbook, held by Security Operations with Satellite Operations sign-off on every action that touches the vehicle; and the coverage walk, every path covered or carrying an owned, dated residual risk, held by Engineering for the rebuilds and by Satellite Operations for the procedures that carry a measure until the rebuild flies. Beside each number, the Adversary Impact column in one sentence: what the adversary must now do that they did not have to do last quarter. Mark Proficient if the answer derives every number from a catalogue and names a department for each; mark Developing if any number is a rating rather than a count.

The Pentagon of Pain Guide · Full Spectrum Space Cybersecurity Professional

Five mastery areas · one question · five functions