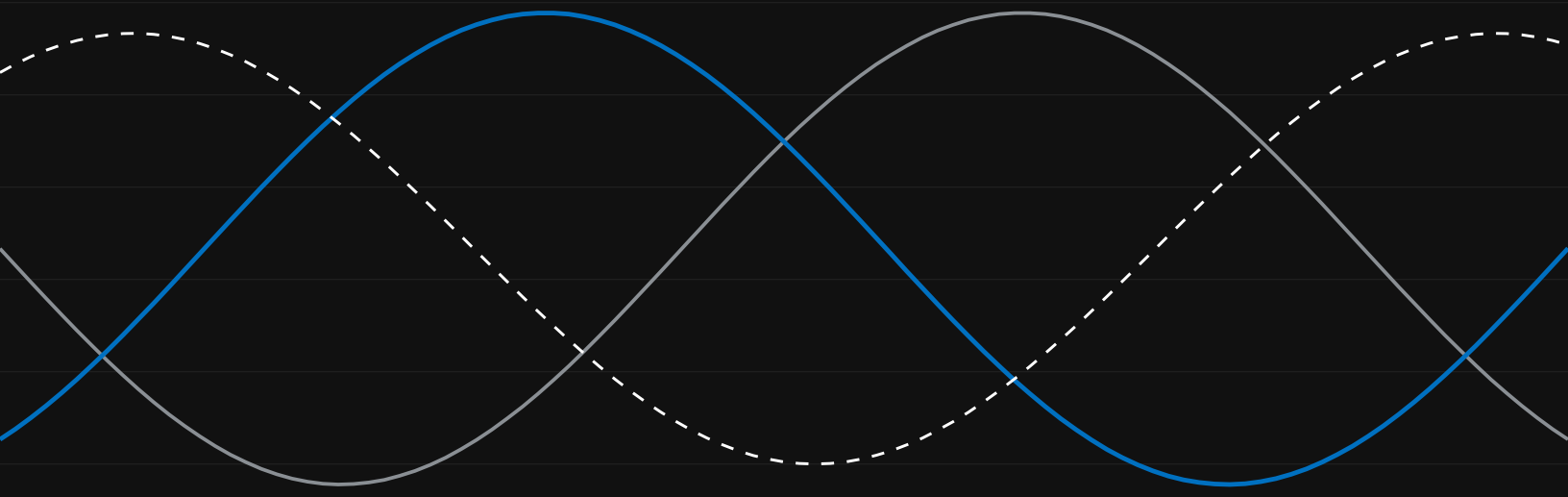
Question Set · Student edition

The Pentagon of Pain

The exercises for the Pentagon of Pain guide, with the answer key, and five questions to ask of any piece of security work. Every exercise draws on a chapter of the guide; read the guide first.



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	The Pentagon of Pain, question set, student edition
Edition	Student edition · revised 2026-11-19
Contact	www.d2teamcorp.org

Student edition

Every exercise, with its keyed or model answer and the reason. Work them before you read the key.

Contents

EX **Exercises** 4

KEY **Answer Key** 7

ASK **Five Questions to Ask of Any Piece of Security Work** 10

© 2026 ethicallyHackingspace (eHs)®

EX Exercises

Work these before opening the answer key. Every exercise is answerable from the Pentagon of Pain guide alone, and each names the guide chapter it draws on.

Recall 1 to 6 are select or match questions with one keyed answer each. Application 1 and the Extension are worked examples: write your answer, then compare it with the model answer in the key. They are not marked. Every scenario is a hypothetical operator: nothing here asks about your own organization.

Recall: select or match, one keyed answer each

Recall 1 Ch. 1

Which option states what the Pentagon of Pain is, what it is not, and the relationship between the mindset and the framework, as the guide states them?

a. A framework, not a mindset. It tells an organization what to produce. Equip with the framework, then transform the mindset.
b. A mindset, not a framework. It tells the organization how to judge what it produces. Transform the mindset, then equip with the framework.
c. A set of steps, not a way of judging. Its five points are five stages of a process, and the framework judges each stage.
d. An engineering specification, not a thought model. It replaces the framework that produces the work.

Recall 2 Ch. 1, 7.4, 10

Match each mastery area to the framework function it is judged against. Each function is used once.

_____	01 Master Decomposition	**A**	Adversary Management
_____	02 Master Contextualized Threat Modeling	**B**	Concept of Operations
_____	03 Master Converged Detection Engineering	**C**	Contextualized Threat Modeling
_____	04 Master Exposure Management	**D**	Converged Detection Engineering
_____	05 Master Adversary Management	**E**	Incident Response Preparation

Recall 3 Ch. 2.4

In a Pain Index, which column does the Pain score summarize, what kind of measure is that column, and what does the guide rule about who scores the index?

a. The Adversary Impact column, a measure of effectiveness. The index is never self-scored.
b. The left column, a measure of performance. The index is never self-scored.
c. The Adversary Impact column, a measure of performance. Each department scores its own column.
d. The left column, a measure of effectiveness. Each department scores its own column.

© 2026 ethicallyHackingspace (eHs)®

Recall 4 Ch. 3.3

Which option gives the four stages of the arc in order, and the stage at which a department first asks what the adversary pays rather than what the auditor wants?

a. Compliance, Cost, Friction, Ownership. The department first asks it at Friction.
b. Friction, Compliance, Ownership, Cost. The department first asks it at Cost.
c. Compliance, Friction, Cost, Ownership. The department first asks it at Cost.
d. Compliance, Friction, Cost, Ownership. The department first asks it at Ownership.

Recall 5 Ch. 2.3

As the guide reads JP 3-12, where does every action in the guide sit, and what crosses the line?

a. Outside the defended network, once an attack is confirmed. The evidence stays inside the organization.
b. Inside the defended network. Attribution-quality evidence crosses, delivered through trusted channels such as Space ISAC.
c. Inside the defended network. Nothing crosses the line.
d. At containment. The evidence is kept inside the organization.

Recall 6 Ch. 2.1

The model's reasoning is borrowed most directly from three published documents. Match each document to what the guide takes from it. Each is used once.

_____	Air Force Doctrine Publication 3-60, *Targeting*	**A**	The target system concept: a target is composed of components, and components are composed of elements.
_____	Joint Publication 3-60, *Joint Targeting*	**B**	The joint targeting cycle, which runs through six phases.
_____	Air Force Pamphlet 14-210, *USAF Intelligence Targeting Guide*	**C**	Targeting described as effects-based, interdisciplinary, anticipatory, systematic and integrated with other processes.

Application: worked examples, compared with a model answer

Application 1 Ch. 2.4, 4.7

A draft status report reads: "Our new detection platform raises adversary cost." Rewrite it so the cost is concrete, using a hypothetical operator's management path: the ground service that decides which commands are released to the link. Name the element, the mastery area with the function it is judged against, and what the adversary must now do.

© 2026 ethicallyHackingspace (eHs)®

Extension scenario: a worked example, compared with a model answer

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 score from 1 to 4. 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.

© 2026 ethicallyHackingspace (eHs)®

KEY Answer Key

Recall 1 to 6 have one keyed answer each, given with the reason it is the answer. Application 1 and the Extension have a model answer to compare yours against; they are not marked. If your answer differs, trace which chapter rule it breaks before reading on.

Recall 1 · keyed answer b

b. A mindset, not a framework. The Pentagon of Pain is a way of judging security work by what it costs the adversary. It does not tell an organization what to produce; it tells the organization how to judge what it produces. Transform the mindset, then equip with the framework: the METEORSTORM functions produce the artifacts; the Pentagon judges them. Option c reverses Chapter 1, which calls it a way of judging, not a set of steps; option d reverses it too, because the guide is a thought model, not an engineering specification, and the mindset does not replace the framework.

Recall 2 · keyed answer 01 B, 02 C, 03 D, 04 E, 05 A

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 first and fourth pairs differ in name.** The function is what the framework defines and produces; the mastery area is the judgment held over it. The function is not renamed to match (7.4): the guide names each function exactly as the framework defines it, so that the two never contradict each other (Chapter 1). For the fourth pair, whose function produces a signature and a playbook per path, 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 · keyed answer a

a. The Adversary Impact column, a measure of effectiveness; never self-scored. The left column, the state of the deliverable, is the measure of performance. The Adversary Impact column is the measure of effectiveness, and the Pain score summarizes that column only. The index is never self-scored, and it is not a maturity model. The left column names a deliverable that can be inspected, and the right column names what the adversary must now do.

Recall 4 · keyed answer c

c. Compliance, Friction, Cost, Ownership; at Cost. 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. At Ownership the department applies that reasoning to its own work without being asked.

© 2026 ethicallyHackingspace (eHs)®

Recall 5 · keyed answer b

b. Inside the defended network; attribution-quality evidence crosses. JP 3-12 defines internal defensive measures (DCO-IDM) as authorized defense actions within the defended portion of cyberspace, and response actions (DCO-RA) as deliberate, authorized measures taken outside the defended network. Every action in the guide sits on the DCO-IDM side of that line. What crosses is attribution-quality evidence, delivered through trusted channels such as Space ISAC to the governments and coalitions that hold the authority to act (2.3).

Recall 6 · keyed answer C, B, A in the order the documents are listed

Air Force Doctrine Publication 3-60, *Targeting*, C: targeting as effects-based, interdisciplinary, anticipatory, systematic and integrated with other processes, and assessment that measures whether desired effects were created. **Joint Publication 3-60, *Joint Targeting*, B**: the joint targeting cycle, six phases from commander's objectives and intent to combat assessment. **Air Force Pamphlet 14-210, *USAF Intelligence Targeting Guide*, A**: the target system concept, the structure borrowed most directly, which read against your own platform is a parent chain and a blast radius. Because the model is borrowed rather than invented, it can be checked against these sources.

Application 1 · model answer

One acceptable rewrite, drawn from the Pain Index in 4.7: "The ground service that decides which commands are released to the link is now an enumerated element, with a parent and a description agreed by the three departments. An adversary on that path loses stealth: a deviation from baseline on that service now raises a question all three departments can read." That is Master Decomposition judged against Concept of Operations. Compare yours with it: a sound rewrite names an element, a function or its artifact, and a concrete action the adversary must now take. If the cost in yours is still an adjective, rewrite it (2.4).

© 2026 ethicallyHackingspace (eHs)®

Extension · model answer

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 the three departments, Operations supplying normal, Security the technique and Engineering which interfaces can emit the source (6.6), 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. Compare yours with it: a sound answer derives every number from a catalog and names a department for each, and no number in it is a rating rather than a count.

© 2026 ethicallyHackingspace (eHs)®

ASK Five Questions to Ask of Any Piece of Security Work

Use this page at work. Each question is about the piece of work in front of you: a design change, a detection, a playbook, a resilience measure. None of them asks what an organization has or lacks. There is one question per mastery area, and each is taken from the Adversary Impact column of that area's Pain Index in the guide.

Mastery area	Ask of the work	The Adversary Impact wording it is taken from
01 Master Decomposition	**Does this work mean a deviation from baseline on a named element raises a question all three departments can read?**	Guide 4.7, Pain 2: "Attackers lose stealth; a deviation from baseline on a named element raises a question all three departments can read."
02 Master Contextualized Threat Modeling	**Does this work make reused techniques and AI-generated steps land on a named element the defensive cyber operator has already read?**	Guide 5.7, Pain 2: "Attackers must vary tools or timing; reused techniques and AI-generated steps land on a named element the defensive cyber operator has already read."
03 Master Converged Detection Engineering	**Does this work make known techniques cross at least one step where a source is Available?**	Guide 6.7, Pain 2: "Known techniques cross at least one step where a source is Available; simple replay or automation attempts begin to break down."
04 Master Exposure Management	**Does this work make attackers adapt tools or pivot to a route not yet instrumented?**	Guide 7.7, Pain 2: "Automated tools and known exploits begin failing on the instrumented routes; attackers must adapt tools or pivot to a route not yet instrumented."
05 Master Adversary Management	**Does this work mean attackers begin to lose the element they reused most?**	Guide 8.7, Pain 2: "Attackers begin to lose the element they reused most, and suffer exposure across intelligence-sharing communities."

Reading the answer. The guide's rule in 2.4 applies to every answer: cost must be concrete. "Raises adversary cost" is filler; name what the adversary must now do. Work that has changed nothing about adversary behavior has performed without being effective. The Pain Index review sheet in the METEORSTORM desk pack (meteorstorm-desk-pack.pdf) gives the five indexes with blank columns for a reviewer's record.

© 2026 ethicallyHackingspace (eHs)®