

The Pentagon of Pain

Detect, disrupt, deter space threats: five mastery areas and one question.

The mindset

October 2026

d2teamcorp.org

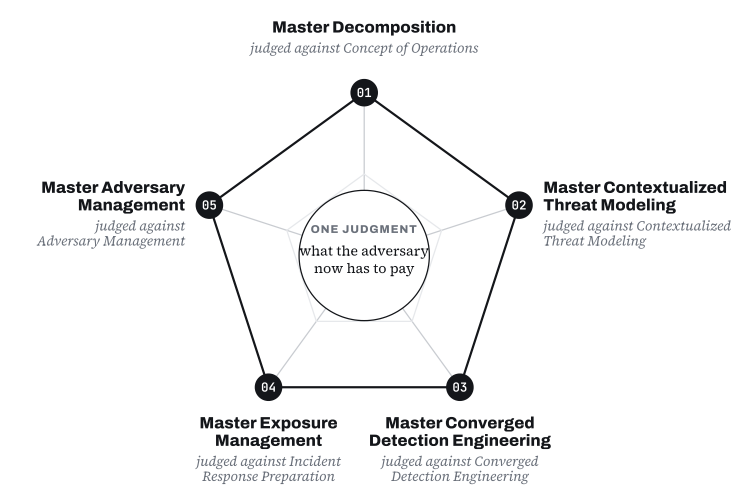


Figure 1. Read it as five points of one judgment, not five stages of a process. Point 04 is judged against Incident Response Preparation: a mastery area and a function are different things, so the names differ.

1 THE QUESTION

Most security programs judge their work by what they have put in place. The Pentagon of Pain changes the question to what the adversary now has to pay. It is a way of judging, not a set of steps.

It gives the engineers, the operators and the security analysts who defend one platform a single test for every hour and every dollar: **does this raise the adversary's cost?**

2 MINDSET AND METHOD

The Pentagon of Pain is a mindset, not a framework. It does not tell an organization what to produce; it tells the organization how to judge what it produces. The method is the METEORSTORM cyber resilience framework, whose five functions produce the artifacts the judgment is applied to.

Transform the mindset, then equip with the framework. A mindset with no framework is a poster. A framework with no mindset is compliance work with better filing.

3 THE FIVE MASTERY AREAS

MASTERY AREA	THE ADVERSARY SUFFERS WHEN	ADVERSARY PAIN
01 Master Decomposition	<i>“The adversary suffers when you know your platform better than they ever can.”</i>	Adversary must invest more time and resources to discover undocumented pathways, losing stealth and meeting hardened chokepoints.
02 Master Contextualized Threat Modeling	<i>“The adversary suffers when every strike they imagine is already prepared for.”</i>	Adversary must constantly adapt, as reused tactics land on a named element the defensive cyber operator has already read.
03 Master Converged Detection Engineering	<i>“The adversary suffers when they cannot hide, and every move is seen.”</i>	Adversary dwell time is cut sharply; attempts to blend into noise or exploit phase changes are rapidly exposed.
04 Master Exposure Management	<i>“The adversary suffers when every path they take ends in a trap.”</i>	Adversary finds fewer viable attack paths, and persistent footholds are disrupted mid-operation.
05 Master Adversary Management	<i>“The adversary suffers when their plans are known, broken, and turned against them.”</i>	Adversary loses anonymity and operational continuity, facing exposure, tool and infrastructure loss, and real-world consequences.

4 BORROWED FROM DOCTRINE

A defensive cyber operator’s model whose reasoning is borrowed from an established military discipline: targeting, as described in Air Force Doctrine Publication (AFDP) 3-60 and Joint Publication (JP) 3-60. Air Force Pamphlet (AFPAM) 14-210 holds that a target is composed of components, and components of elements. Read against a satellite platform, that is a parent chain and a blast radius. It does not ask civilian operators to conduct targeting.

5 THE BOUNDARY

Every action sits on the side of the line JP 3-12 draws for defensive cyberspace operations, internal defensive measures (DCO-IDM): within the defended network. Consequences mean attribution-quality evidence delivered through trusted channels, such as the Space Information Sharing and Analysis Center (Space ISAC), to the governments and coalitions that hold the authority to act.

6 MEASURED BY THE PAIN INDEX

Each mastery area ends with a Pain Index. Its left column is a measure of performance: the state of what the organization has produced. Its Adversary Impact column is a measure of effectiveness. The Pain score summarizes the second, not the first.

The index is not a maturity model. It is never self-scored.