FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

REFERENCE WORKBOOK

METEORSTORM Analytic Layer

The Analytic Layer Taxonomic Element Nomenclature (TEN) reference. Six analytic elements and the Analytics Catalog they produce, each definition carried verbatim.

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	METEORSTORM Analytic Layer, TEN reference workbook
EDITION	First edition · version 1.0 · revised 2026-09-24
CONTACT	www.d2teamcorp.org

CONTENTS

INTRODUCTION

The Analytic Layer is the fifth layer of the METEORSTORM data model, built on the four structural layers that enumerate the platform itself. The layer contributes three mechanisms. Its taxonomy classifies analytic knowledge into six elements, each carrying its published definition verbatim. Its ontology anchors every enumerated analytic element through a fixed target field to the exact platform elements it concerns, so a finding recorded against an asset is reachable from the service, the segment, and the environment above it. Its normalization is the innovation: intelligence and peer-framework content, whatever its origin, is normalized into the same six elements and attaches to the same decomposition in one shared vocabulary, so the catalogue keeps pace with the ecosystem without re-architecting the data model. This card is the taxonomic dictionary for the analytic layer; the organizational enumeration is the companion analytic ETEN reference.

WHY THE ANALYTIC LAYER WAS DEVELOPED

The analytic layer was developed for front-line space collective defense. The intent of the layer: entries move operator to operator as machine-to-machine exchange across a trusted network, and a peer acts on an entry without renegotiating its provenance. Every entry declares its SOURCE at the gate before enumeration.

The four structural layers classify what the platform is. The analytic layer classifies what the analyst knows about it, in a form every participating organization reads identically. Its six elements answer the six questions an analyst asks in the order a situation unfolds: has a platform been compromised, is an attack confirmed, is an attack path active, is a threat confirmed, is a detection signature available, and can the threat be engineered out of the platform. A platform means the organization's own or a trusted community member's.

The six-element structure is also the layer's intake surface. Peer frameworks evolve on their own timelines; their content normalizes into these six elements without changing the data model. The ingestion structure is fixed, the contents refresh continuously, and evolution in the peer ecosystem becomes a taxonomy update, not a re-architecting.

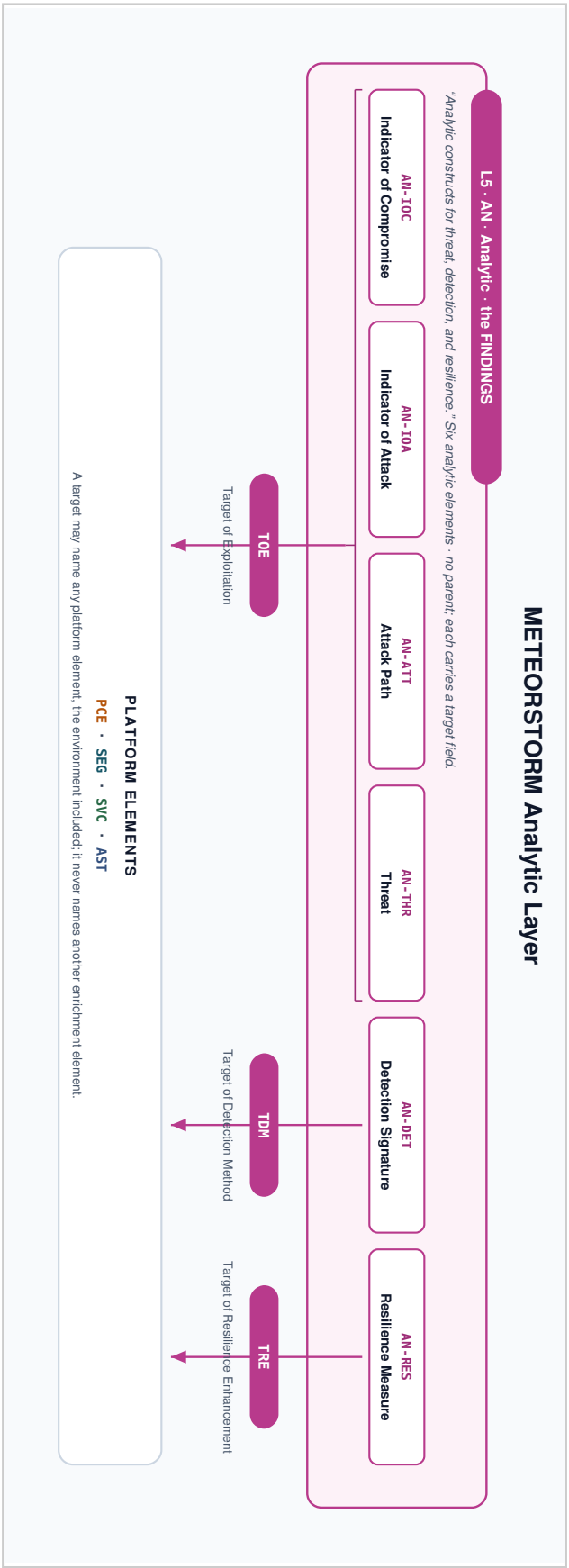
METEORSTORM DATA MODEL FIELDS

LAYER	The layer the element belongs to; every element on this card is **AN**, Analytic (L5).
TAG	The published tag for the element within its layer, for example **THR**.
LABEL	The published name that corresponds to the tag, for example **Threat**.
DEFINITION	The published definition for the element, quoted verbatim.
TARGET	The target field fixed by the element: **TOE**, **TDM**, or **TRE**. It names the platform elements the enumerated element concerns.
SOURCE	Declared at the gate before enumeration: **observable**, a signal or data captured from a system, or **synthetic**, authored data for resilience engineering and exercises.

Every element below carries its published fields. To record one real analytic element on your platform, switch to the colon ETEN nomenclature in the companion analytic ETEN reference.

> **Verbatim rule.** Every definition below is the published METEORSTORM taxonomy text, quoted exactly. On this platform an element definition is never abbreviated, paraphrased, or reworded. When you need to describe how an element applies to your actual system, that is the job of the ETEN, not an edit to the definition.

TLP:AMBER



THE GATE

The analytic layer was developed for front-line space collective defense. The intent of the layer: entries move operator to operator as machine-to-machine exchange across a trusted network, and a peer acts on an entry without renegotiating its provenance. That intent holds only if every entry declares its SOURCE before enumeration:

- `SOURCE=observable` · Built on a real-world report: a signal or data captured from a system. The standard for Indicator of Compromise, Indicator of Attack, Attack Path, and Threat.
- `SOURCE=synthetic` · Authored data for system resilience engineering and operational exercises.

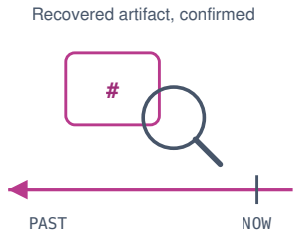
L5 ANALYTIC (AN)

Predicate: “Analytic constructs for threat, detection, and resilience.” The ENRICHMENT layer. Every AN element is an enrichment element; it anchors to the platform element it concerns through its target field.

METEORSTORM DATA MODEL FIELDS

TOE	**Target of Exploitation.** Carried by Attack Path, Indicator of Compromise, Indicator of Attack, and Threat; names the platform elements the adversary activity is directed at.
TDM	**Target of Detection Method.** Carried by Detection Signature; names the platform elements the signature observes.
TRE	**Target of Resilience Enhancement.** Carried by Resilience Measure; names the platform elements the measure protects.

The target field is fixed by the element; it is never chosen freely. It references platform elements in any layer, PCE, SEG, SVC, or AST, so a threat can anchor to the environment itself; it never references another enrichment element.



QUESTION 01 · HAS AN ORGANIZATIONAL OR TRUSTED COMMUNITY MEMBER PLATFORM BEEN COMPROMISED?

Indicator of Compromise

The highest priority analytic element: backward-looking evidence of a confirmed platform breach, traceable to an actual incident or live operator telemetry, and acted on by a peer operator without further analysis.

LAYER	**AN** Analytic (L5)
TAG	**IOC**
LABEL	Indicator of Compromise
DEFINITION	Confirmed indication that a converged space system has been compromised.
TARGET	**TOE** Target of Exploitation

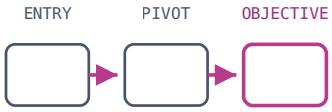
Activity in progress, window open

QUESTION 02 · IS THERE A CONFIRMED ATTACK AGAINST AN ORGANIZATIONAL OR TRUSTED COMMUNITY MEMBER PLATFORM?

Indicator of Attack

Present-tense evidence that adversary activity is in progress against the platform. The compromise may or may not have completed; the response window is open. Past and present stay separate elements so each question gets its own decision path.

LAYER	**AN** Analytic (L5)
TAG	**IOA**
LABEL	Indicator of Attack
DEFINITION	Confirmed indication that a converged space system has been attacked.
TARGET	**TOE** Target of Exploitation



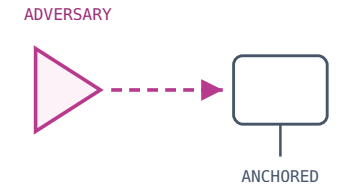
Documented route, entry to impact

QUESTION 03 · IS THERE AN ACTIVE ATTACK PATH AGAINST AN ORGANIZATIONAL OR TRUSTED COMMUNITY MEMBER PLATFORM?

Attack Path

A documented sequence of adversary actions that could traverse the platform from entry to impact. An exposure, not an observation: recorded in enough detail for another analyst to evaluate it against their own platform. Alone among the six, it also states what a defensive cyber operator must hold to see it: the route says where the adversary goes, the required sources say what would witness them there.

LAYER	**AN** Analytic (L5)
TAG	**ATT**
LABEL	Attack Path
DEFINITION	Confirmed attack path for a converged space system.
TARGET	**TOE** Target of Exploitation
SOURCES	**RDS** Required Data Source · **RSS** Required Signal Source



Attributed capability, bearing on one element

QUESTION 04 · IS THERE A CONFIRMED THREAT AGAINST AN ORGANIZATIONAL OR TRUSTED COMMUNITY MEMBER PLATFORM?

Threat

A known adversary capability or campaign directed at the platform, built on attributed activity: threat-intelligence reporting, government attribution, or a peer-shared adversary profile. Where the Attack Path records what the platform exposes, the Threat records who is likely to exercise it.

LAYER	**AN** Analytic (L5)
TAG	**THR**
LABEL	Threat
DEFINITION	Confirmed and active threat against a converged space system.
TARGET	**TOE** Target of Exploitation

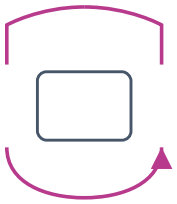
Written logic fires when behavior crosses it

QUESTION 05 · IS THERE A CONFIRMED DETECTION SIGNATURE AVAILABLE FOR A CONFIRMED THREAT?

Detection Signature

The written commitment to see a specific behavior, expressed in the open RootA format so a signature written by one operator deploys in another operator's stack; the native vendor query rides along as enrichment. A threat or attack path with no matching signature is a detection gap, and the gap is itself an enumerable analytic product.

LAYER	**AN** Analytic (L5)
TAG	**DET**
LABEL	Detection Signature
DEFINITION	Validated and operational pattern, signal, or logic that triggers on contextualized threat behavior for a converged space system.
TARGET	**TDM** Target of Detection Method
PLAYBOOK	**PB** the authorized response this signature triggers



Protection around the element, posture restored

QUESTION 06 · IS THERE A MEANS TO ENGINEER THE THREAT OUT OF THE PLATFORM?

Resilience Measure

The forward-looking element: a protective capability serving one of the four resiliency goals of NIST SP 800-160 Volume 2, Anticipate, Withstand, Recover, Adapt. Applied in place at the cadence the technology supports, or captured as input to the next generation of platform design when the vehicle is on orbit.

LAYER	**AN** Analytic (L5)
TAG	**RES**
LABEL	Resilience Measure
DEFINITION	Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats.
TARGET	**TRE** Target of Resilience Enhancement

The target field is mandatory. An analytic element is enumerated only when its target field, the TOE, TDM, or TRE, names a real enumerated platform element on your platform; an element with no populated target is not a valid ETEN and is not entered in the catalogue. The target may name a platform element in any structural layer, the environment included; it never names another enrichment element. That is the value of the analytic layer: every threat, indicator, attack path, detection signature, and resilience measure anchors to the exact platform element it concerns, so any department reads it and acts on it without re-translation.

A signature ships with its authorized response, or it does not ship. A Detection Signature that fires and leaves the on-call analyst to invent a response, and to go looking for someone with the authority to approve it, is half a deliverable. So the signature carries a **Playbook** reference alongside its target, and the playbook carries a minimum set of *approved* actions: at least one in each of assess, contain, recover and report. Each action names one enumerated element, one executor and one decider, on the authority levels the operating roles already use: **solo**, the executing role acts alone; **collaborative**, the other operating role co-signs first; **escalated**, the Mission Lead approves and the approval is recorded before execution. The level is not chosen. It is read off what undoing the action would cost, because on a space platform revoking a ground credential and safing a spacecraft are not the same kind of act. Mission Lead is accountable for every action and executes none of them: the decider never does the work. An entry whose playbook does not resolve is not a valid ETEN.

The Attack Path carries two source fields. Alongside its target, an Attack Path declares what a defensive cyber operator must hold to see it: **RDS**, the required data source, what must be received as a record; and **RSS**, the required signal source, what must be measured in the physical layer. They stay separate because they are separate kinds of observable, the same line drawn at the asset layer between AST-DA Data and AST-SI Signal, and on a converged space platform that line decides whether a path is detectable at all: jamming is seen in the noise floor and the carrier-to-noise ratio, never in a log. Each field holds one or more sub-enumerated records counted from 00, and each record names the element it is observed on and its state, Available, Partial, or Gap. A required source nobody collects still takes a record and a state, which is what makes a gap countable. A field with no required sources reads *none*, never blank.

Enumeration. This card carries the taxonomy of the analytic layer; the target field is its ontology. Enumerating against it produces the analytic ETEN record: each element named with an ordinal and a description, its target populated. The companion analytic ETEN reference applies these six elements to the Kestrel Orbital Day-1 CONOPS with worked examples from Modules 02 through 05.

THE ANALYTICS CATALOG

The Analytics Catalog is how the layer innovates. It is the normalization engine of the model: past, current, and evolving reference frameworks, whatever their origin or vintage, normalize into the same six analytic elements, expressed in one nomenclature and anchored to the structural decomposition of the platform being defended. That normalization is what establishes a solid taxonomy and ontology across every operational environment, from terrestrial to deep space. METEORSTORM does not replace the source frameworks below, and it does not compete with them. It gives organizations one reliable lens through which every framework, including frameworks not yet published, contributes to the same catalog without forcing its vocabulary on the others.

The catalog is therefore not a separate product, and not something the layer simply outputs. It is the running, organized collection of analytic elements that accumulates as an organization enumerates its own intelligence and normalizes peer-framework content through the layer. It keeps pace with the ecosystem by design: when a source framework evolves, its content re-normalizes into the same six elements, so evolution in the peer ecosystem becomes a taxonomy update, never a re-architecting of the data model.

Different source types feed different elements, and the element tags in the SOURCE column are recommendations, not restrictions: they name the elements each source most naturally supplies. Threat-intelligence feeds carrying observations from real incidents feed the two indicators; an indicator entry is never drawn from an architectural framework, because an indicator cannot be theoretical. Adversary-behavior catalogues feed Attack Path and Threat. Control and defensive-technique frameworks feed Detection Signature and Resilience Measure.

FRAMEWORK	PUBLISHER	SOURCE
Trusted threat-intelligence feeds (Space ISAC Exchange, vendor and government reporting, own telemetry)	Various	IOC · IOA · ATT · THR · DET · RES
MITRE ATT&CK	The MITRE Corporation	ATT · THR · RES
MITRE FiGHT	The MITRE Corporation with the U.S. DoD 5G Cross-Functional Team	ATT · THR · RES
MITRE ATLAS	The MITRE Corporation	ATT · THR · RES
MITRE CAPEC	The MITRE Corporation	ATT
Aerospace SPARTA	The Aerospace Corporation	ATT · THR · DET · RES
ESA SPACE-SHIELD	European Space Agency	ATT · THR · RES
MITRE EMB3D	The MITRE Corporation	ATT · THR · RES
MITRE D3FEND	The MITRE Corporation, funded by the NSA	DET · RES
CSA AI Controls Matrix	Cloud Security Alliance	RES
CSA Cloud Controls Matrix	Cloud Security Alliance	RES
CSA Shared Security Responsibility Model	Cloud Security Alliance	RES
NIST SP 800-160 Volumes 1 and 2	National Institute of Standards and Technology	RES
NIST SP 800-53	National Institute of Standards and Technology	RES