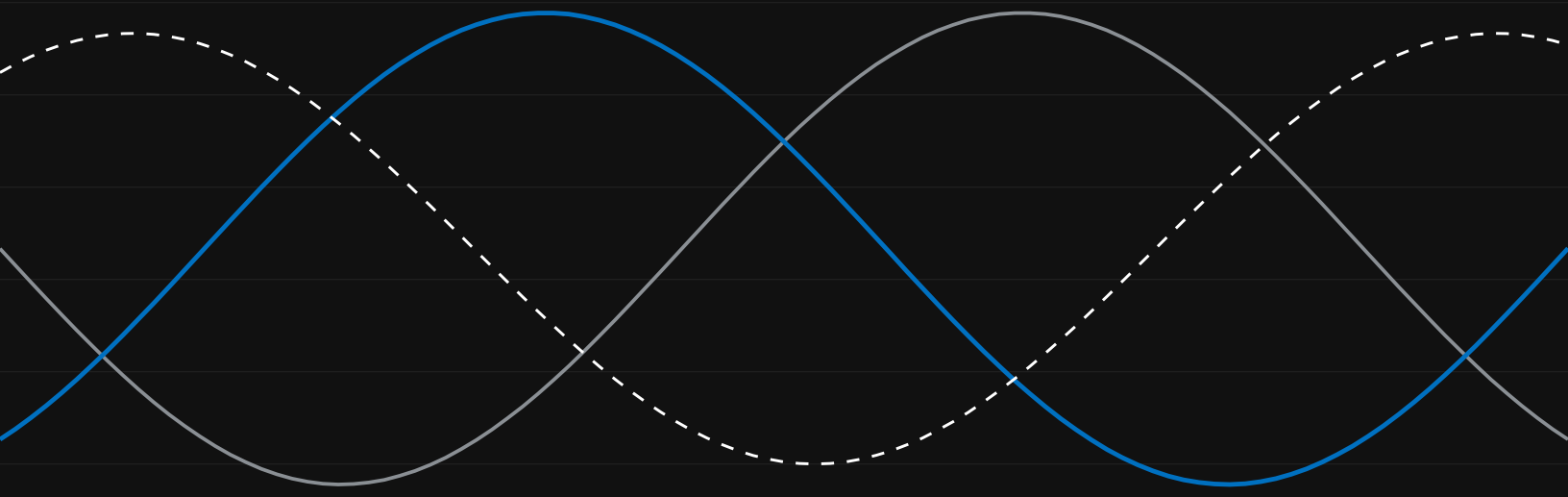
Normative reference

METEORSTORM normative reference

The data model (TEN): five layers and 30 taxonomic elements. The ETEN: the record and the process for enumerating a real platform, structural and analytic.



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	METEORSTORM normative reference
Edition	First edition · version 1.0 · revised 2026-11-19
Contact	www.d2teamcorp.org

Contents

	What this is and how to use it	4
	Introduction	5
L1	Primary Capability Environment (PCE)	7
L2	Segment (SEG)	8
L3	Service (SVC)	10
L4	Asset (AST)	11
L5	Analytic (AN)	13
E1	The ETEN	16
E2	The layer gates	18
E3	The ETEN process	20
A1	The analytic layer	22
A2	The gate	24
A3	The analytic ETEN	25
A4	The analytics catalog	35
	Background	37

© 2026 ethicallyHackingspace (eHs)®

What this is and how to use it

1. This is the normative reference for the METEORSTORM data model: five layers and 30 taxonomic elements, each with its published definition quoted exactly.
2. Chapters L1 to L5 are the data model (the TEN): every element with its tag, its label and its definition.
3. Chapters E1 to E3 are the ETEN: the five-field identifier, the four layer gates and the eight steps that name one real element on a platform.
4. Chapters A1 to A4 are the analytic layer: the SOURCE gate, the numbered process for each of the six analytic elements, required sources, the playbook and the analytics catalog.
5. Look things up in it; it is not written to be read through. Each worked example is marked Kestrel Orbital, the platform of the course scenario. The Background, at the back, is the history of the framework.

Use this at work

The sheets to work from and to write on are in a separate download, the **METEORSTORM desk pack** (meteorstorm-desk-pack.pdf): the two-page quick reference, one method card and one blank record sheet for each function, the Pentagon of Pain card, the Pain Index review sheet and the checklists. This reference does not repeat them. Keep the desk pack on the desk, and open this reference to check a definition, a gate or a step. The pages a practitioner looks up most:

Look up	Where it is in this reference	Page
The tags, on one page	The data model figure, 24 structural tags; the analytic layer figure, six analytic tags	6, 13
The tag tables	Tag, label and published definition of every element, by layer: PCE, SEG, SVC, AST, AN	7, 8, 10, 11, 13
The identifier grammar	The five fields of an ETEN, and one identifier written in full	16, 17
The gates	The four layer gates and what each child names as its parent; the SOURCE gate for an analytic entry	19, 24
The steps	The eight steps of the ETEN process; the six analytic processes compared	20, 26
The target fields	TOE, TDM and TRE, and which analytic element carries each	14
The source states	Available, Partial, Gap and unassessed, for a required source on an attack path	33
The authority levels	Solo, collaborative and escalated, on a playbook action	34
The worked records	Kestrel Orbital: threat, attack path, detection signature with its playbook, resilience measure	27, 28, 29, 31

© 2026 ethicallyHackingspace (eHs)®

Introduction

This is the METEORSTORM TEN data model: five layers defining 30 taxonomic elements, each named by a Taxonomic Element Nomenclature (TEN) of four fields: Layer, Tag, Label and Description. The verbatim rule below governs every description.

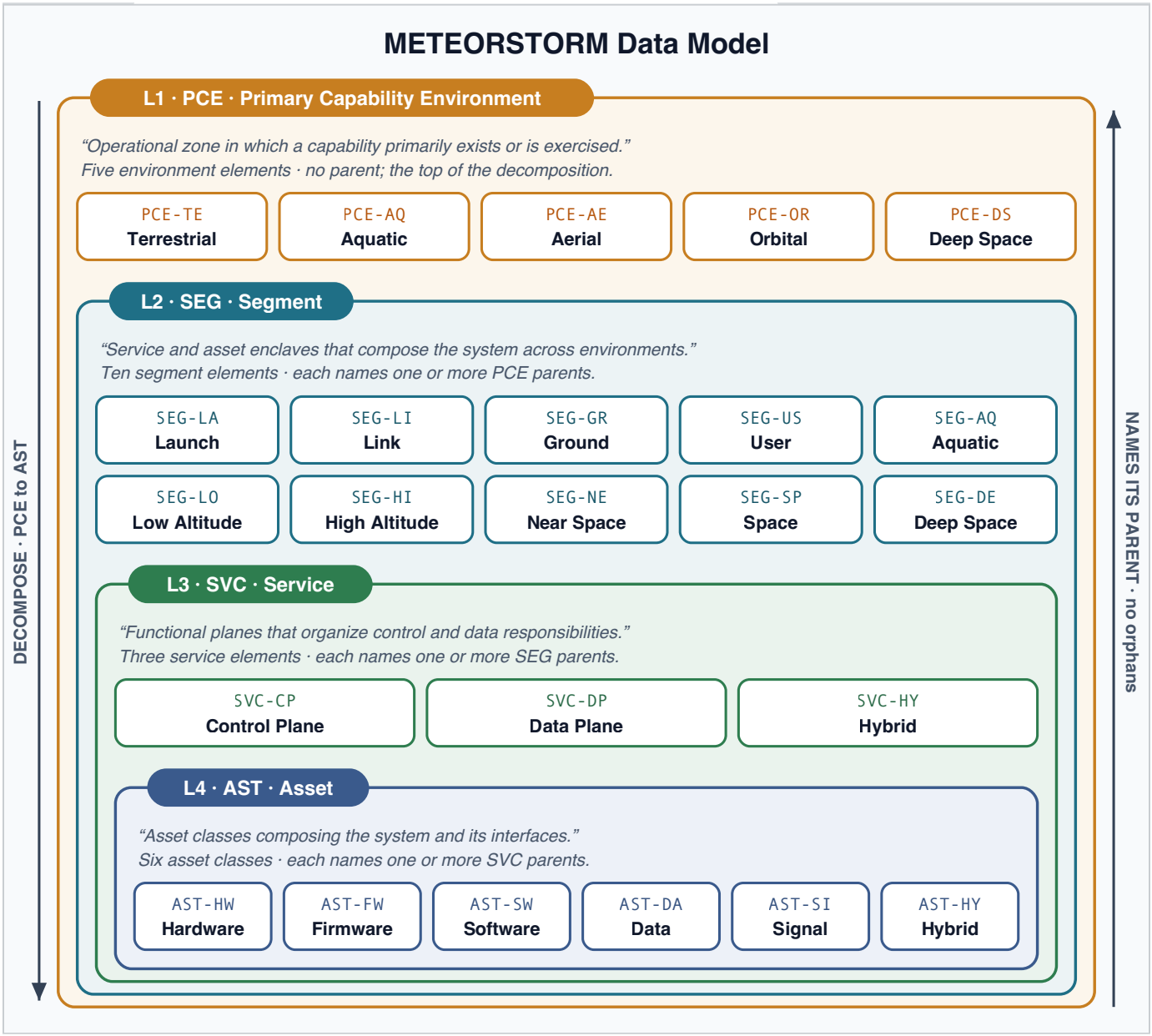
METEORSTORM Data Model Fields

Layer	The layer the element belongs to: **PCE**, **SEG**, **SVC**, **AST**, or **AN**.
Tag	The published tag for the element within its layer, for example **OR**.
Label	The short name that corresponds to the tag: the published name without its layer word (Environment, Service, Asset) or bracketed abbreviation, for example **Orbital** for the published Orbital Environment.
Description	The published description of the element, quoted verbatim.

To name one real occurrence on a platform, use the ETEN, defined in chapter E1 of this reference.

> **Verbatim rule.** Every description in this reference is the published METEORSTORM taxonomy text, quoted exactly. A description 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 description. One typographical error in the published file is corrected here: the published Detection Signature description ends with two periods, and this reference prints one.

© 2026 ethicallyHackingspace (eHs)®



© 2026 ethicallyHackingspace (eHs)®

L1 Primary Capability Environment (PCE)

Why this layer exists

Analysts needed to operationalize the attribution of platform environments during threat intel curation, and no existing framework carried a mechanism for it. Nature can create adverse conditions in every one of the five environments, so the environment must be a first-class attribute of every record, not a footnote.

> *"This layer was crucial as current frameworks simply skipped over mechanisms to operationalize key enrichment sources like Space Domain Awareness (SDA), terrestrial weather, maritime activity, and other environmental dimensions that need to be top of mind for analyst. No environmental context so how would you ever know if it was environmental or cyber physical?"*
>
> The ethicallyHackingspace (eHs) team

Predicate: "Operational zone in which a capability primarily exists or is exercised." A PCE has no parent; it is the top of the decomposition.

Terrestrial

TEN nomenclature **PCE-TE-Terrestrial-Surface-based operational zones on planetary bodies.**

Layer **PCE** Primary Capability Environment (L1) Tag **TE** Label Terrestrial
Description Surface-based operational zones on planetary bodies.

Aquatic

TEN nomenclature **PCE-AQ-Aquatic-Water-based operational zones, including but not limited to Earth's maritime domains.**

Layer **PCE** Primary Capability Environment (L1) Tag **AQ** Label Aquatic
Description Water-based operational zones, including but not limited to Earth's maritime domains.

Aerial

TEN nomenclature **PCE-AE-Aerial-Atmospheric operational zones spanning lower, upper, and near-space regions.**

Layer **PCE** Primary Capability Environment (L1) Tag **AE** Label Aerial
Description Atmospheric operational zones spanning lower, upper, and near-space regions.

Orbital

TEN nomenclature **PCE-OR-Orbital-Operational zones within planetary or satellite orbits.**

Layer **PCE** Primary Capability Environment (L1) Tag **OR** Label Orbital
Description Operational zones within planetary or satellite orbits.

Deep Space

TEN nomenclature **PCE-DS-Deep Space-Operational zones beyond planetary orbital regimes.**

Layer **PCE** Primary Capability Environment (L1) Tag **DS** Label Deep Space
Description Operational zones beyond planetary orbital regimes.

© 2026 ethicallyHackingspace (eHs)®

L2 Segment (SEG)

Why this layer exists

Ten segments, including aquatic, low altitude, high altitude, and near space, modeled before the attack trends that later proved them out. The layer builds a distributed, cyber-physical platform mindset: a platform is not one place, it is services and assets composed across enclaves.

> *"We had considered aerial, aquatic and other less frequently explored segments before the renewed focus on issues like oceanic cable attacks and rogue aerial platforms. These increased attack patterns simply codified that our approach to using the evolving adversary mindset to decompose systems made sense."*
>
> The ethicallyHackingspace (eHs) team

Predicate: "Service and asset enclaves that compose the system across environments." A SEG names one or more PCE parents.

Launch

> TEN nomenclature **SEG-LA-Launch-Surface-based services and assets for primary launch operations.**

Layer **SEG** Segment (L2) Tag **LA** Label Launch
Description Surface-based services and assets for primary launch operations.

Link

> TEN nomenclature **SEG-LI-Link-Services and assets enabling platform communications across signal paths.**

Layer **SEG** Segment (L2) Tag **LI** Label Link
Description Services and assets enabling platform communications across signal paths.

Ground

> TEN nomenclature **SEG-GR-Ground-Surface-based services and assets for primary platform operations, serving as the primary locus of control plane activity.**

Layer **SEG** Segment (L2) Tag **GR** Label Ground
Description Surface-based services and assets for primary platform operations, serving as the primary locus of control plane activity.

User

> TEN nomenclature **SEG-US-User-Services and assets for primary end-user operations.**

Layer **SEG** Segment (L2) Tag **US** Label User
Description Services and assets for primary end-user operations.

© 2026 ethicallyHackingspace (eHs)®

Aquatic

TEN nomenclature **SEG-AQ-Aquatic-Water-based services and assets for primary platform operations, not limited to Earth's maritime domains.**

Layer **SEG** Segment (L2) Tag **AQ** Label Aquatic
Description Water-based services and assets for primary platform operations, not limited to Earth's maritime domains.

Low Altitude

TEN nomenclature **SEG-LO-Low Altitude-Aerial services and assets in the lower atmosphere.**

Layer **SEG** Segment (L2) Tag **LO** Label Low Altitude
Description Aerial services and assets in the lower atmosphere.

High Altitude

TEN nomenclature **SEG-HI-High Altitude-Aerial services and assets above the lower atmosphere but below near space.**

Layer **SEG** Segment (L2) Tag **HI** Label High Altitude
Description Aerial services and assets above the lower atmosphere but below near space.

Near Space

TEN nomenclature **SEG-NE-Near Space-Aerial services and assets above high altitude and below orbital regions.**

Layer **SEG** Segment (L2) Tag **NE** Label Near Space
Description Aerial services and assets above high altitude and below orbital regions.

Space

TEN nomenclature **SEG-SP-Space-Services and assets operating in planetary or satellite orbits.**

Layer **SEG** Segment (L2) Tag **SP** Label Space
Description Services and assets operating in planetary or satellite orbits.

Deep Space

TEN nomenclature **SEG-DE-Deep Space-Services and assets operating beyond planetary orbital regimes.**

Layer **SEG** Segment (L2) Tag **DE** Label Deep Space
Description Services and assets operating beyond planetary orbital regimes.

© 2026 ethicallyHackingspace (eHs)®

L3 Service (SVC)

Why this layer exists

Space systems are too diverse for any fixed catalog of service definitions to survive contact with real platforms. The layer stays deliberately small, three elements, and lets every platform owner nest their own service definitions beneath it, so diversity does not fracture the shared schema.

> *"Space systems are simply too diverse in terms of service definitions and descriptions. Grounding the service decomposition into control plane, data plane, and hybrid while allowing the platform owner to nest their organizational specific service definitions made the most sense."*
>
> The ethicallyHackingspace (eHs) team

Predicate: "Functional planes that organize control and data responsibilities." An SVC names one or more SEG parents.

Control Plane

TEN nomenclature **SVC-CP-Control Plane-Services for managing and orchestrating platform control functions.**

Layer **SVC** Service (L3) Tag **CP** Label Control Plane
Description Services for managing and orchestrating platform control functions.

Data Plane

TEN nomenclature **SVC-DP-Data Plane-Services for managing and orchestrating mission product functions.**

Layer **SVC** Service (L3) Tag **DP** Label Data Plane
Description Services for managing and orchestrating mission product functions.

Hybrid

TEN nomenclature **SVC-HY-Hybrid-Services integrating both control and data plane functionalities.**

Layer **SVC** Service (L3) Tag **HY** Label Hybrid
Description Services integrating both control and data plane functionalities.

© 2026 ethicallyHackingspace (eHs)®

L4 Asset (AST)

Why this layer exists

Six asset classes ground the enormous variety of real components, and the hybrid element is the deliberate bridge to how engineers already think: it aligns the model with the concept of a subsystem while preserving owner-nested definitions beneath the shared classes.

> *"Space systems are simply too diverse in terms of asset definitions and descriptions. Grounding the asset decomposition into data, signal, hardware, firmware, software, and most importantly having a hybrid element to enable alignment with the concept of a 'subsystem' while allowing the platform owner to nest their organizational specific asset definitions made the most sense."*
>
> The ethicallyHackingspace (eHs) team

Predicate: "Asset classes composing the system and its interfaces." An AST names one or more SVC parents.

Hardware

TEN nomenclature **AST-HW-Hardware-Physical components supporting platform operations.**

Layer **AST** Asset (L4) Tag **HW** Label Hardware
Description Physical components supporting platform operations.

Firmware

TEN nomenclature **AST-FW-Firmware-Embedded control code governing hardware functions.**

Layer **AST** Asset (L4) Tag **FW** Label Firmware
Description Embedded control code governing hardware functions.

Software

TEN nomenclature **AST-SW-Software-Applications and logic executing operational tasks.**

Layer **AST** Asset (L4) Tag **SW** Label Software
Description Applications and logic executing operational tasks.

© 2026 ethicallyHackingspace (eHs)®

Data

TEN nomenclature **AST-DA-Data-Information generated, processed, or consumed by the platform.**

Layer **AST** Asset (L4) Tag **DA** Label Data

Description Information generated, processed, or consumed by the platform.

Signal

TEN nomenclature **AST-SI-Signal-Communication channels and transmission frequencies.**

Layer **AST** Asset (L4) Tag **SI** Label Signal

Description Communication channels and transmission frequencies.

Hybrid

TEN nomenclature **AST-HY-Hybrid-Composite elements combining multiple asset types.**

Layer **AST** Asset (L4) Tag **HY** Label Hybrid

Description Composite elements combining multiple asset types.

© 2026 ethicallyHackingspace (eHs)®

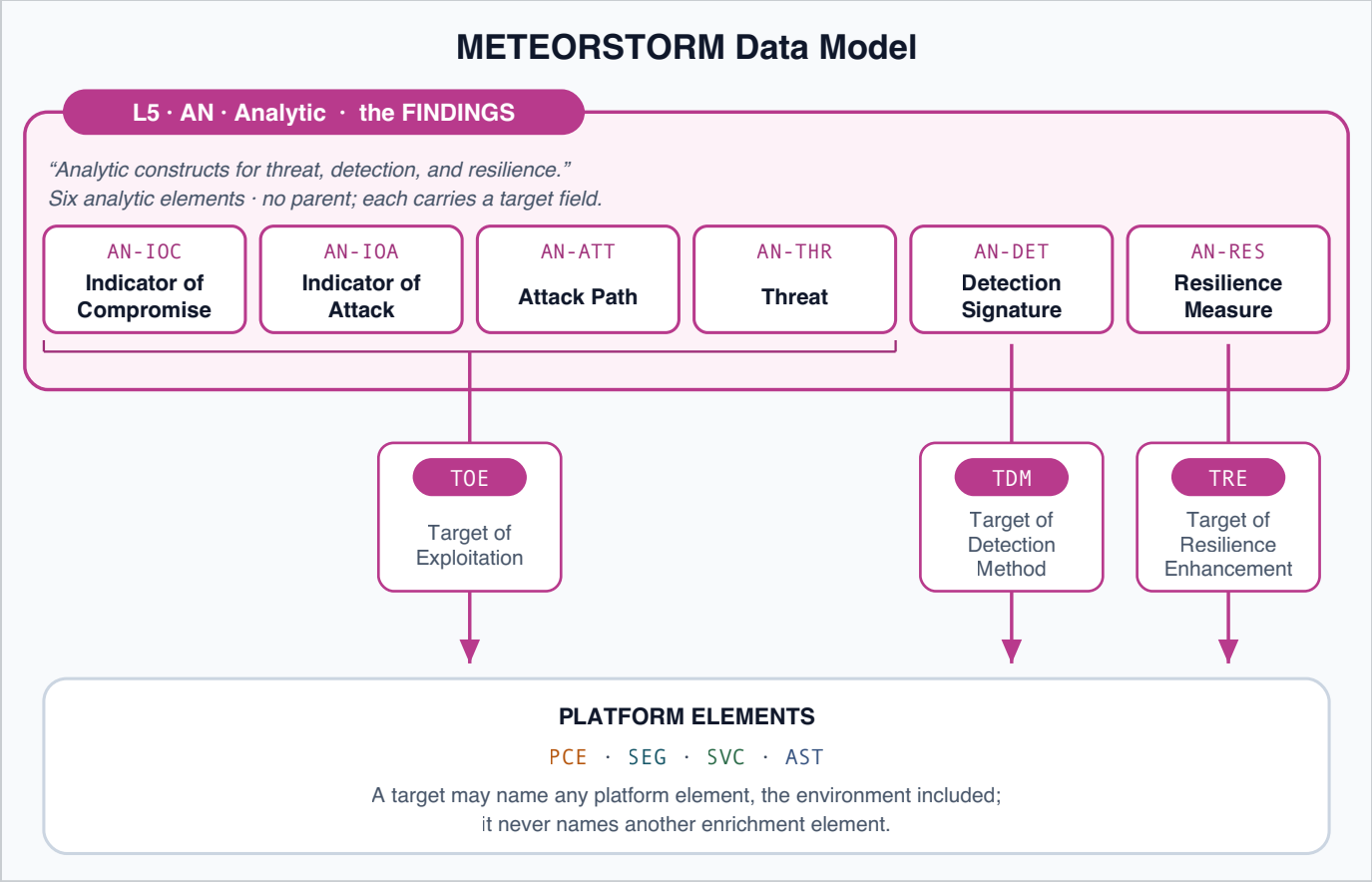
L5 Analytic (AN)

Why this layer exists

Six elements, scoped against analyst fatigue. Each one answers a single operational question an analyst must dispatch quickly: is something compromised, is it under attack, is an attack path known, is a specific threat involved, is a detection signature available, is a resilience measure available.

> *"We had to focus on the key points without inducing analyst fatigue. Is something compromised, under attack, advertising an attack path, related to a specific threat and is there an available detection signature or resilience measure?"*
>
> The ethicallyHackingspace (eHs) team

Predicate: "Analytic constructs for threat, detection, and resilience." Every AN element anchors to one platform element through its target field.



© 2026 ethicallyHackingspace (eHs)®

METEORSTORM Data Model Fields

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

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

Indicator of Compromise

TEN nomenclature **AN-IOC-Indicator of Compromise-Confirmed indication that a converged space system has been compromised.**

Layer **AN** Analytic (L5) Tag **IOC** Label Indicator of Compromise
Description Confirmed indication that a converged space system has been compromised.
Target **TOE** Target of Exploitation

Indicator of Attack

TEN nomenclature **AN-IOA-Indicator of Attack-Confirmed indication that a converged space system has been attacked.**

Layer **AN** Analytic (L5) Tag **IOA** Label Indicator of Attack
Description Confirmed indication that a converged space system has been attacked.
Target **TOE** Target of Exploitation

Attack Path

TEN nomenclature **AN-ATT-Attack Path-Confirmed attack path for a converged space system.**

Layer **AN** Analytic (L5) Tag **ATT** Label Attack Path
Description Confirmed attack path for a converged space system.
Target **TOE** Target of Exploitation Sources **RDS** Required Data Source · **RSS** Required Signal Source

© 2026 ethicallyHackingspace (eHs)®

Threat

TEN nomenclature **AN-THR-Threat-Confirmed and active threat against a converged space system.**

Layer **AN** Analytic (L5) Tag **THR** Label Threat
Description Confirmed and active threat against a converged space system.
Target **TOE** Target of Exploitation

Detection Signature

TEN nomenclature **AN-DET-Detection Signature-Validated and operational pattern, signal, or logic that triggers on contextualized threat behavior for a converged space system.**

Layer **AN** Analytic (L5) Tag **DET** Label Detection Signature
Description 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

Resilience Measure

TEN nomenclature **AN-RES-Resilience Measure-Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats.**

Layer **AN** Analytic (L5) Tag **RES** Label Resilience Measure
Description Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats.
Target **TRE** Target of Resilience Enhancement

Enumeration. Applying this data model to a platform produces the ETEN record: each element named with an ordinal and a description of the real instance. The ETEN chapters that follow define that record.

© 2026 ethicallyHackingspace (eHs)®

E1 The ETEN

An Enumerated Taxonomic Element Nomenclature (ETEN) names one real element on a platform, in five fields. It is the outcome of applying the METEORSTORM data model to a platform: the TEN chapters of this reference supply the layer, the tag and the label; the ETEN adds the ordinal and the description of the real instance.

> **LAYER:TAG:LABEL:ORDINAL:Description**

Hyphens and colons. A TEN is written with hyphens, as chapters L1 to L5 print it, and an ETEN is written with colons, so the two are never mistaken for each other on a page.

Figure E1.1 The five fields: three selected from the taxonomy, two written for the instance



Table 1 The five fields

Field	Content	Source	Step
Layer	The structural layer: PCE, SEG, SVC or AST.	From the taxonomy	02
Tag	The tag the taxonomy publishes for that layer. Never invented.	From the taxonomy	03
Label	The label exactly as this reference prints it for that tag: the short form of the published name.	From the taxonomy	04
Ordinal	Two digits from 00, counted per tag.	For the instance	05
Description	One plain sentence stating what this exact instance is on this platform, at its own layer.	For the instance	08

The parent (Step 06) and the optional fields (Step 07) do not print inside the five fields; they govern the record.

© 2026 ethicallyHackingspace (eHs)®

Kestrel Orbital worked example **one structural identifier, written in full**

> **AST:SW:Software:04:The software C2 application on the operator console, the ground command-and-control suite.**

LAYER	**AST** Asset
TAG	**SW**
LABEL	Software
ORDINAL	**04**
Description	The software C2 application on the operator console, the ground command-and-control suite.
PARENT	**SVC:CP:Control Plane:13** (Satellite Console)
Parent links to the root	**AST:SW:Software:04** names **SVC:CP:Control Plane:13**; **SVC:CP:Control Plane:13** names **SEG:GR:Ground:00**; **SEG:GR:Ground:00** names **PCE:TE:Terrestrial:00**. No element is an orphan.
Working name	Console operator software
The TEN it instantiates	**AST-SW-Software-Applications and logic executing operational tasks.** The TEN is written with hyphens and ends in the published definition; the ETEN is written with colons and ends in the description of this instance.

The enumeration that produces every ETEN is governed by the normative process: the scope bounds what is enumerated, the taxonomy supplies the tag and label, the ontology links the parent, and the description states the instance.

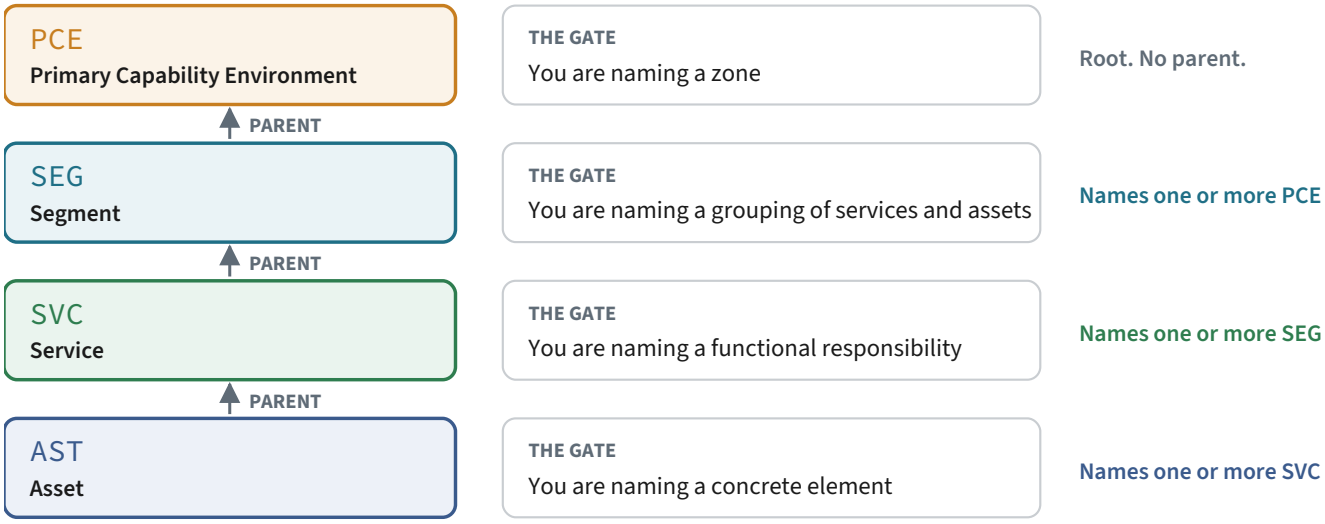
© 2026 ethicallyHackingspace (eHs)®

E2 The layer gates

Each structural layer has a gate, and the gate is the layer's published definition, verbatim. An element is enumerated at a layer only when it passes that layer's gate.

> **Tiebreak for the recurring trap.** PCE and SEG carry similar element names (Orbital and Space, Aquatic, Deep Space) but are different things. Ask: am I naming a zone, or a group of services and assets? Zone means PCE; group means SEG.

Figure E2.1 The four gates, and the PARENT link each child names



Enumerated top down, so every parent exists before its child. Every arrow is one PARENT link; a child that names no parent is an orphan and is not a valid ETEN.

© 2026 ethicallyHackingspace (eHs)®

Table 2 The four gates

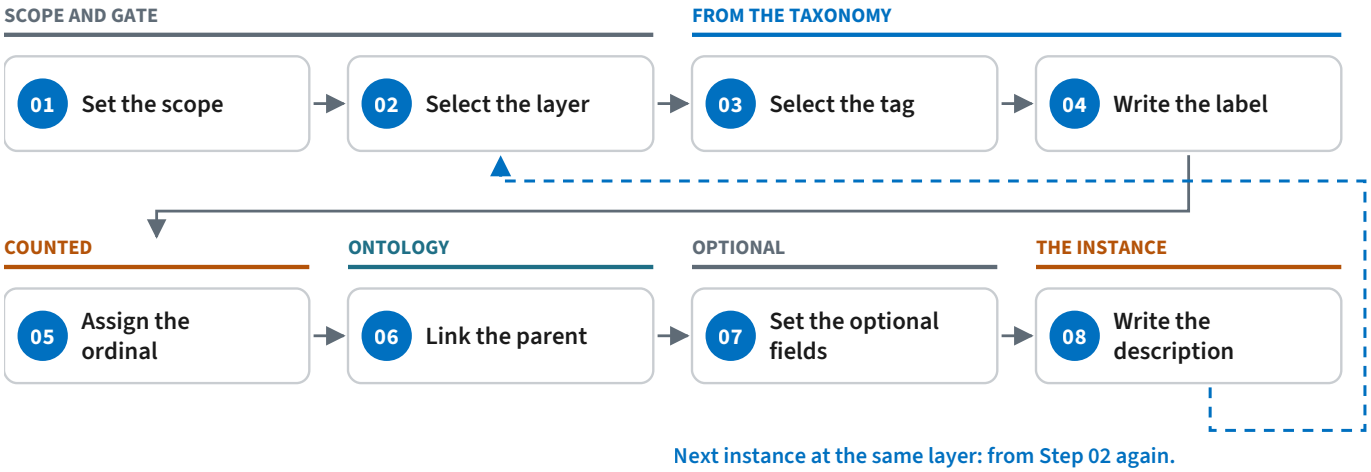
Layer	Published definition	The gate	PARENT names
PCE Primary Capability Environment	*"Operational zone in which a capability primarily exists or is exercised."*	You are naming a zone, not a thing in it.	None. PCE is the root.
SEG Segment	*"Service and asset enclaves that compose the system across environments."*	You are naming a grouping of services and assets, not the zone it sits in and not the hardware inside it.	One or more PCE
SVC Service	*"Functional planes that organize control and data responsibilities."*	You are naming a functional responsibility, what the platform does, not what it is built from.	One or more SEG
AST Asset	*"Asset classes composing the system and its interfaces."*	You are naming a concrete element, a real component the platform is built from.	One or more SVC

© 2026 ethicallyHackingspace (eHs)®

E3 The ETEN process

Eight steps, fixed order. The same steps run at every layer, top down, so parents exist before children.

Figure E3.1 The ETEN process, eight steps in fixed order



When no instance remains, the layer is fully enumerated; the next layer down starts at Step 02.

Table 3 The ETEN process

Step	Name	What the step does	Sets
01	**Set the scope**	From the resilience objective and the requirements that drive the decomposition. An element outside the scope is not enumerated.	Scope
02	**Select the layer**	Work top down through the taxonomy's structural layers, and confirm the element passes that layer's definition gate (Table 2) before proceeding. An element that fails its layer's gate is not enumerated at that layer; reclassify it and re-enter at Step 02.	LAYER
03	**Select the tag**	From the taxonomy for that layer. Never invent one.	TAG
04	**Write the label**	For that tag, exactly as this reference prints it: the short form of the published name.	LABEL
05	**Assign the ordinal**	Two digits from 00, counted per tag.	ORDINAL

© 2026 ethicallyHackingspace (eHs)®

Step	Name	What the step does	Sets
06	**Link the parent**	One layer up. This link is the ontology: every child names its parent, PCE is the root, and no element is an orphan. A segment names one or more environments, a service names one or more segments, and an asset names one or more services, never zero. An analytic element takes no parent; it anchors through its target field.	PARENT
07	**Set the optional fields**	A service marks DISTRIBUTED when it spans more than one segment; an asset may carry a SUBSYSTEM grouping; an analytic element carries its TARGET and SOURCE.	DISTRIBUTED, SUBSYSTEM; TARGET, SOURCE
08	**Write the description**	One plain sentence stating what this exact instance is on this platform, at its own layer: a zone for an environment, an enclave of services and assets for a segment, a responsibility for a service, a concrete element for an asset. The layer gate from Step 02 applies again here: a segment description never describes the hardware inside the enclave; a service description begins “The service that …”; an asset description begins with its element class (“The physical …”, “The embedded …”, “The flight software …”, “The stored …”, “The transmitted …”). An instance described at the wrong layer is non-compliant.	Description

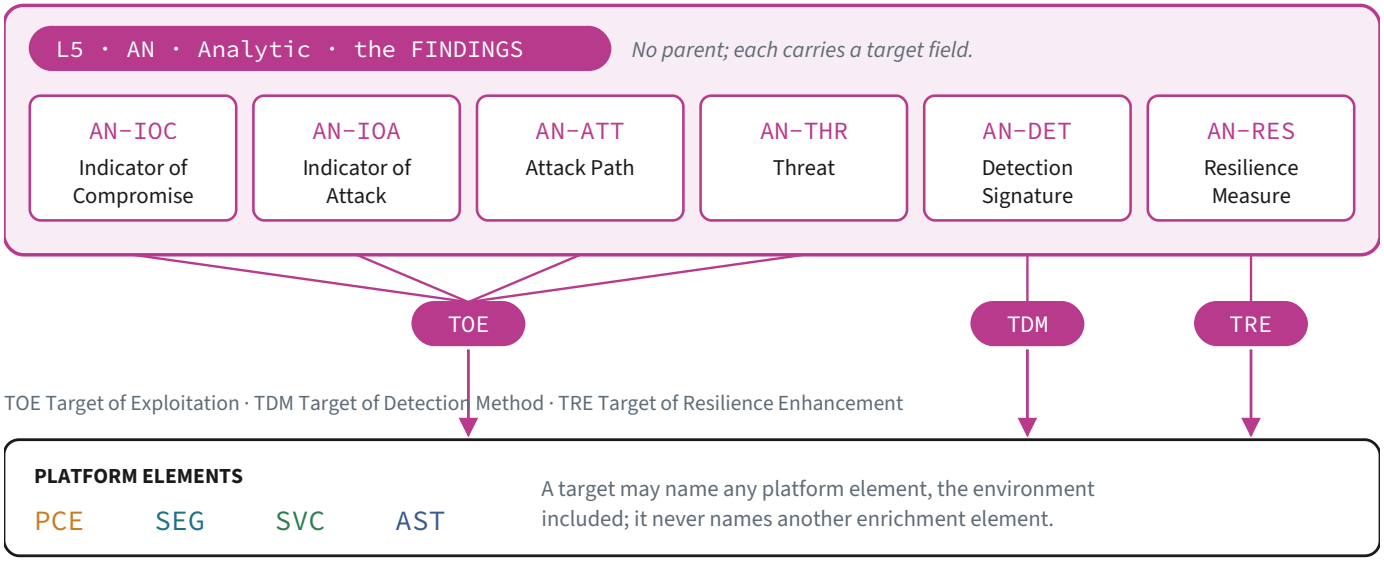
Repeat for the next instance. When no more remain, the layer is fully enumerated.

© 2026 ethicallyHackingspace (eHs)®

A1 The analytic layer

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 description verbatim. Its ontology anchors every enumerated analytic element through a fixed target field to the exact platform element 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 catalog keeps pace with the ecosystem without re-architecting the data model.

Figure A1.1 The analytic layer: six elements, three target fields, one destination



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.

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. A platform means the organization's own or a trusted community member's.

© 2026 ethicallyHackingspace (eHs)®

Table 4 The six questions

#	Element, question and target field	What it records
01	AN-IOC **Indicator of Compromise** Has an organizational or trusted community member platform been compromised? TOE	The highest priority analytic element: backward-looking evidence of a confirmed platform breach, traceable to an actual incident or live operator telemetry, and specific enough that a peer operator can triage and act on it without renegotiating its provenance.
02	AN-IOA **Indicator of Attack** Is there a confirmed attack against an organizational or trusted community member platform? TOE	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.
03	AN-ATT **Attack Path** Is there an active attack path against an organizational or trusted community member platform? TOE	A documented sequence of adversary actions confirmed as able to traverse the platform from entry to impact. Confirmed means the route is shown feasible against this platform, not that it has been observed in an attack: 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.
04	AN-THR **Threat** Is there a confirmed threat against an organizational or trusted community member platform? TOE	A known adversary capability or campaign directed at the platform, built on attributed activity from one of five source types: a threat-intelligence provider, a government advisory, a peer-shared adversary profile, open-source intelligence, or the operator's own hunting. Where the Attack Path records what the platform exposes, the Threat records who is likely to exercise it.
05	AN-DET **Detection Signature** Is there a confirmed detection signature available for a confirmed threat? TDM	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.
06	AN-RES **Resilience Measure** Is there a means to engineer the threat out of the platform? TRE	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.

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.

© 2026 ethicallyHackingspace (eHs)®

A2 The gate

Every analytic entry declares its SOURCE before enumeration. The intent of the layer, entries a peer acts on without renegotiating provenance, holds only if it does.

Figure A2.1 The gate: an entry with no declared SOURCE is not entered

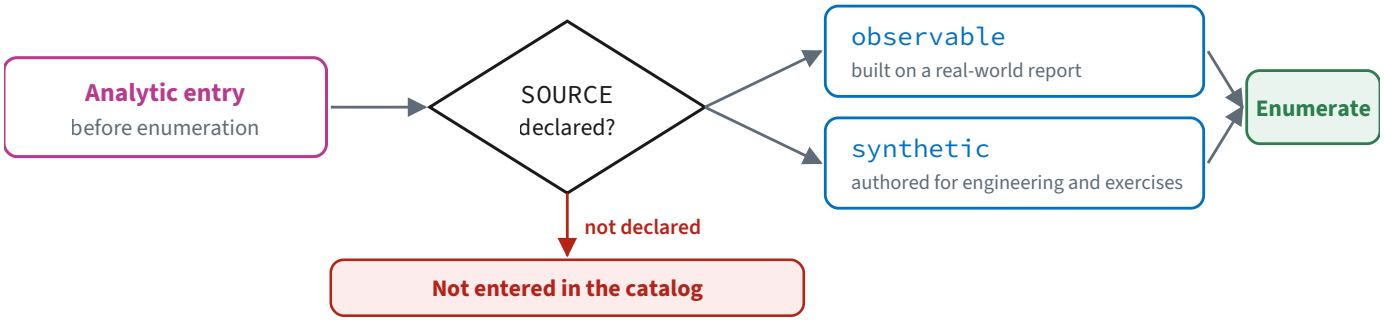


Table 5 SOURCE

Value	Meaning
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.
synthetic	Authored data for system resilience engineering and operational exercises.

Resilient Cyber Operations prioritizes real-world information sharing: by default an indicator of compromise, an indicator of attack, an attack path, or a threat is real world, ideally confirmed with a space collective defense community member. The framework also serves exercises and modeling, with one intent: developing real-world detection signatures and resilience measures from simulated activity.

© 2026 ethicallyHackingspace (eHs)®

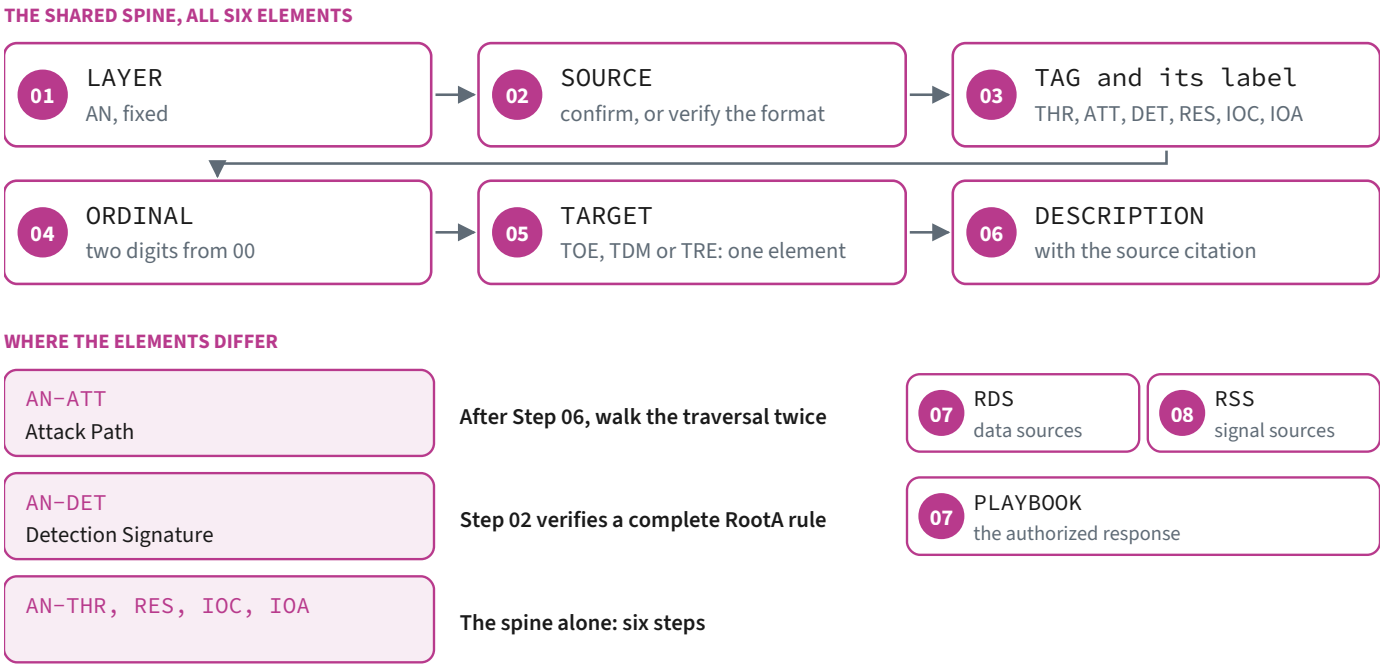
A3 The analytic ETEN

An analytic ETEN names one enrichment element on a platform. An enrichment element is an indicator of compromise, an indicator of attack, an attack path, a threat, a detection signature, or a resilience measure, and it enriches the platform's Resilient Cyber Operations context by anchoring to the platform element it concerns. It takes no PARENT; it is not part of the platform. Where structural elements bind upward through PARENT, an enrichment element binds through its target reference, and the anchor is machine-readable.

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; an element with no populated target is not a valid ETEN and is not entered in the catalog.

The process. The enumeration that produces every analytic ETEN is governed by the normative process: the source is confirmed at the gate, the taxonomy supplies the tag and label, and the target reference anchors the entry to the platform. Each element walks its own numbered process: six steps for a threat, a resilience measure or an indicator, seven for a detection signature, eight for an attack path.

Figure A3.1 One spine of six steps; the attack path and the detection signature add steps



© 2026 ethicallyHackingspace (eHs)®

Table 6 The six analytic processes compared

Element	Step 02	Target field (Step 05)	Steps	Steps beyond the spine
AN-THR **Threat**	Confirm the source	TOE Target of Exploitation	6	none
AN-ATT **Attack Path**	Confirm the source	TOE Target of Exploitation	8	RDS, RSS
AN-DET **Detection Signature**	Verify the format	TDM Target of Detection Method	7	PLAYBOOK
AN-RES **Resilience Measure**	Identify the resiliency goal	TRE Target of Resilience Enhancement	6	none
AN-IOC **Indicator of Compromise**	Confirm the source	TOE Target of Exploitation	6	none
AN-IOA **Indicator of Attack**	Confirm the source	TOE Target of Exploitation	6	none

The Kestrel Orbital worked examples printed after the threat, attack path, detection signature and resilience measure processes below are one chain. Each carries ordinal 01, and each names the same platform element in its target field: AST:SW:Software:04, the element written in full in chapter E1.

AN-THR Threat

Table 7 The Threat (AN-THR) process, the steps that differ

Step	Name	What the step does
02	**Confirm the source**	The threat-intelligence provider report, government advisory, peer-shared adversary profile, open-source intelligence, or internal hunt the threat is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
05	**Enumerate the TOE**	One enumerated platform element (PCE, SEG, SVC, or AST) the source states the threat is directed against. Concrete, not broad, at the lowest layer the source resolves.
06	**Write the DESCRIPTION**	The threat actor or threat class, the assessed capability, plus the source citation. The line a peer operator or peer machine acts on.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to THR, with its label, Threat: AN:THR:Threat; Assign an ORDINAL, two digits from 00, one per distinct threat.

© 2026 ethicallyHackingspace (eHs)®

Kestrel Orbital worked example one threat record

> **AN:THR:Threat:01:adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite.**

Identifier	AN:THR:Threat:01
Name	Command-authority compromise
SOURCE	**observable**
TOE	AST:SW:Software:04 (Console operator software)
Description	adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite.
Source citation	Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite

AN-ATT Attack Path

Table 8 The Attack Path (AN-ATT) process, the steps that differ

Step	Name	What the step does
02	**Confirm the source**	The confirmed exposure, red-team report, adversary-behavior catalog entry (ATT&CK, SPARTA, ATLAS), or peer-shared documentation the path is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
05	**Enumerate the TOE**	One enumerated platform element: the element the path is anchored to, the same element the related AN-THR names. Concrete, at the lowest layer the source resolves.
06	**Write the DESCRIPTION**	The pivot, entry to objective, in enough detail for another analyst to evaluate it against their own platform, plus the source citation.
07	**Enumerate the RDS**	Walk the traversal. At each step where the adversary's action would leave a record, name the one data source a defensive cyber operator must hold to see it, as an RDS record counted from 00, each carrying its OBSERVED ON element and its STATE of Available, Partial, Gap or unassessed. Where the path leaves no records at all, write *none*.
08	**Enumerate the RSS**	Walk the same traversal for observables that exist in the physical layer rather than in a record, as RSS records counted from 00, carrying the same four fields. Where the path produces no physical observable, write *none*. If both fields read *none*, the path as written is not detectable, and that is a finding to record.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to ATT, with its label, Attack Path: AN:ATT:Attack Path; Assign an ORDINAL, two digits from 00, one per distinct path.

The sub-ordinal is a separate counter. It counts within one field of one element and bears no relation to the element's ORDINAL. AN:ATT:Attack Path:07 may carry RDS:00 and RDS:01; the 07 and the 00 are unrelated numbers. RDS and RSS count independently of each other.

© 2026 ethicallyHackingspace (eHs)®

Kestrel Orbital worked example one attack path record

> **AN:ATT:Attack Path:01:An adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite directly from a commanding workstation, bypassing peer review.**

Identifier	AN:ATT:Attack Path:01
Name	Command-authority compromise
SOURCE	**observable**
TOE	AST:SW:Software:04 (Console operator software)
Threat it realizes	AN:THR:Threat:01 Command-authority compromise
Description	An adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite directly from a commanding workstation, bypassing peer review.
Traversal	entry AST:HW:Hardware:04 (Operator console); pivot AST:SW:Software:04 (Console operator software); objective SVC:CP:Control Plane:09 (ACA (Ground)).
RDS	**RDS:00** Operator console session record, host and sign-in time. OBSERVED ON AST:HW:Hardware:04. STATE **unassessed**. **RDS:01** Command-authority usage record carrying the peer-review tag. OBSERVED ON AST:SW:Software:04. STATE **Partial**: the peer-review tag stream depends on workflow adoption. **RDS:02** Control-plane command release record with review state. OBSERVED ON SVC:CP:Control Plane:09. STATE **unassessed**.
RSS	*none*
Source citation	MITRE ATT&CK T1078 (Valid Accounts); SPARTA; insider-threat reporting
Confidence	Medium. Pattern widely reported; per-operator specifics non-public.

© 2026 ethicallyHackingspace (eHs)®

AN-DET Detection Signature

Table 9 The Detection Signature (AN-DET) process, the steps that differ

Step	Name	What the step does
02	**Verify the format**	The signature must be a complete RootA rule (SOC Prime RootA specification v1.0.0): the mandatory name and detection fields, the optional fields the source supports, and the METEORSTORM anchor block. A bare vendor query (Splunk SPL, KQL) or a bare Sigma rule with no RootA wrapper is not accepted into the layer. SOURCE is observable or synthetic.
05	**Enumerate the TDM**	One enumerated platform element the signature observes, the same element the related AN-THR names in its TOE. The field is TDM, not TOE, because it records that element as the one scanned; the element itself does not change.
06	**Write the DESCRIPTION**	The complete RootA rule: every required field (name, detection language and body), the supporting fields (severity, class, mitre-attack, logsource, correlation, references), and the METEORSTORM block anchoring the rule to the target element and its parent chain.
07	**Name the PLAYBOOK**	The authorized response this signature triggers, as meteorstorm.playbook on the rule and a playbook file beside it. It carries at least one approved action in each of assess, contain, recover and report, each naming one element, one executor and one decider at *solo*, *collaborative* or *escalated*. A signature whose playbook does not resolve is not accepted into the layer.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to DET, with its label, Detection Signature: AN:DET:Detection Signature; Assign an ORDINAL, two digits from 00, one per distinct signature.

Kestrel Orbital worked example one detection signature record, with its playbook

Identifier	AN:DET:Detection Signature:01
Name	Out-of-pattern command-authority usage
SOURCE	**observable**
TDM	AST:SW:Software:04 (Console operator software)
Attack path it covers	AN:ATT:Attack Path:01
Source state	Partial, the peer-review tag stream depends on workflow adoption
What it detects	Out-of-pattern command authority usage: detects command-authority usage outside the role and shift baseline, or high-impact commands issued with no peer-review tag.

© 2026 ethicallyHackingspace (eHs)®

Description	The complete RootA rule, file an-det-01-out-of-pattern-command.yml. Its METEORSTORM anchor block:

```
meteorstorm:
  pce: PCE:TE:Terrestrial:00
  seg: SEG:GR:Ground:00
  svc: SVC:CP:Control Plane:13
  ast: AST:SW:Software:04
  playbook: PB-01
  an:
    eten: AN:DET:Detection Signature:01
    tdm: AST:SW:Software:04
```

PLAYBOOK	**PB-01** Out-of-pattern command-authority usage, file an-det-01-out-of-pattern-command.playbook.yml

PB-01 Out-of-pattern command-authority usage: the approved actions

Trigger. AN:DET:Detection Signature:01 fires on out-of-pattern command-authority usage at AST:SW:Software:04, at medium confidence or higher. The threshold is medium and not any, because filed travel and roster changes produce the same pattern and the assess stage separates them.

Action	Stage	Approved action	Element	Executor	Decider	Level
ACT:00	assess	Check the filed travel, the shift roster and the change record for this operator.	AST:SW:Software:04	Security Operations	Mission Lead	*solo*
ACT:01	contain	Suspend the operator credential on the ground command-acceptance service.	SVC:CP:Control Plane:09	Security Operations	Mission Lead	*solo*
ACT:02	contain	Radiate the Kiruna uplink only for commanding sessions released under two-person review.	SVC:HY:Hybrid:03	Satellite Operations	Mission Lead	*collaborative*
ACT:03	recover	Rotate the ground command-acceptance service credentials.	SVC:CP:Control Plane:09	Security Operations	Mission Lead	*solo*
ACT:04	recover	Replay the command log against the flight plan and confirm the vehicle state matches the last authorized command.	SVC:CP:Control Plane:13	Satellite Operations	Mission Lead	*solo*
ACT:05	report	Notify the duty officer and the CISO, who assess significance under NIS2; the clocks run from awareness, 24-hour early warning, 72-hour notification, one-month final report.	AST:SW:Software:04	Security Operations	Mission Lead	*solo*
ACT:06	report	File the redacted Space ISAC Exchange entry.	AST:SW:Software:04	Security Operations	Mission Lead	*escalated*

© 2026 ethicallyHackingspace (eHs)®

AN-RES Resilience Measure

Table 10 The Resilience Measure (AN-RES) process, the steps that differ

Step	Name	What the step does
02	**Identify the resiliency goal**	One of Anticipate, Withstand, Recover, or Adapt, per NIST SP 800-160 Volume 2. SOURCE is observable or synthetic.
05	**Enumerate the TRE**	One enumerated platform element: the element the measure protects, the same element the related AN-THR targets. TRE, not TOE or TDM: the element made more resilient.
06	**Write the DESCRIPTION**	The measure, the resiliency goal it serves, the AN-ATT or AN-THR entries it counters, plus the source citation: internal engineering, control-framework guidance, peer-shared pattern, or post-incident lesson.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to RES, with its label, Resilience Measure: AN:RES:Resilience Measure; Assign an ORDINAL, two digits from 00, one per distinct measure.

Kestrel Orbital worked example one resilience measure record

> **AN:RES:Resilience Measure:01:Dual-control commanding for high-impact actions (a second operator must approve before transmission); role and shift baselines and pre-pass briefings make out-of-pattern actions stand out.**

Identifier	AN:RES:Resilience Measure:01
Name	Dual-control commanding for high-impact actions
SOURCE	**observable**
Resiliency goal	**Withstand**: high-impact commanding continues safely while a credential is compromised, because one credential alone cannot release a high-impact sequence.
TRE	AST:SW:Software:04 (Console operator software)
Counters	AN:ATT:Attack Path:01
Description	Dual-control commanding for high-impact actions (a second operator must approve before transmission); role and shift baselines and pre-pass briefings make out-of-pattern actions stand out.
Owner	**Both**. Satellite Design & Engineering owns the dual-control workflow in the commanding software; Satellite Operations owns the operational discipline of peer review.
Cadence	**in-force**
Source citation	NIST SP 800-53 AC-5 / AC-6 (separation of duties / least privilege); NIST SP 800-160 v2 withstand-goal guidance.

© 2026 ethicallyHackingspace (eHs)®

AN-IOC Indicator of Compromise

Table 11 The Indicator of Compromise (AN-IOC) process, the steps that differ

Step	Name	What the step does
02	**Confirm the source**	The incident report, telemetry stream, or partner report the observation is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
05	**Enumerate the TOE**	One enumerated platform element (PCE, SEG, SVC, or AST) the source states the indicator was observed on. Lowest layer the source resolves.
06	**Write the DESCRIPTION**	The observable (hash, domain, IP, registry key), plus the source citation. The line a peer operator or peer machine acts on.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to IOC, with its label, Indicator of Compromise: AN:IOC:Indicator of Compromise; Assign an ORDINAL, two digits from 00, one per distinct indicator.

Kestrel Orbital worked example: none. The Kestrel Orbital inventories hold no Indicator of Compromise record, so none is printed here.

AN-IOA Indicator of Attack

Table 12 The Indicator of Attack (AN-IOA) process, the steps that differ

Step	Name	What the step does
02	**Confirm the source**	The live telemetry pattern, confirmed alert, or partner incident report the activity is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
05	**Enumerate the TOE**	One enumerated platform element (PCE, SEG, SVC, or AST) the source states is under the in-progress activity. Lowest layer the source resolves.
06	**Write the DESCRIPTION**	The in-progress activity (the pattern, the cadence, the origin where applicable), plus the source citation. The line a peer operator or peer machine acts on.

Steps 01, 03 and 04 are the spine: Enumerate the LAYER, AN (fixed); Set the TAG to IOA, with its label, Indicator of Attack: AN:IOA:Indicator of Attack; Assign an ORDINAL, two digits from 00, one per distinct indicator.

Kestrel Orbital worked example: none. The Kestrel Orbital inventories hold no Indicator of Attack record, so none is printed here.

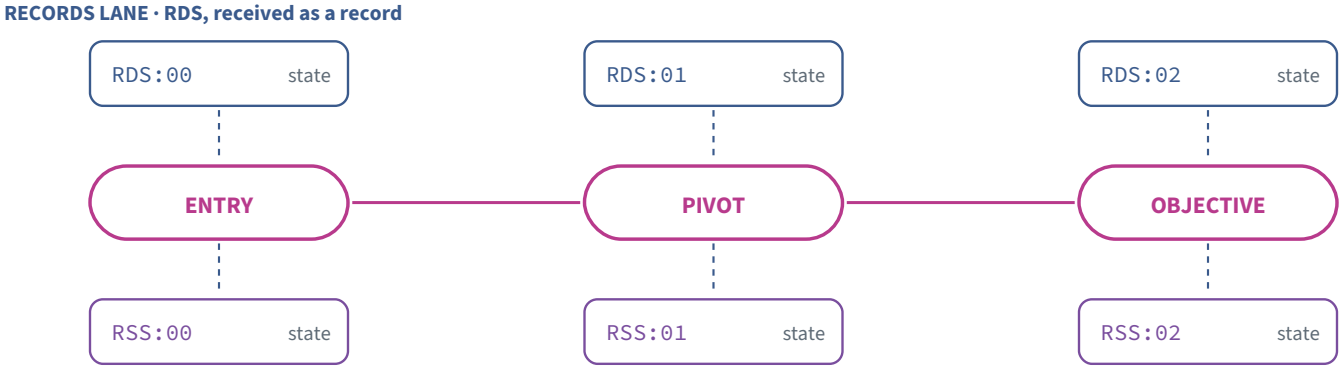
Required sources on an attack path

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, a required signal source and not a required data source. Each record

© 2026 ethicallyHackingspace (eHs)®

names the element it is observed on and its state, Available, Partial, Gap, or unassessed (the owning department has not yet returned a state, which never counts as coverage). A required source nobody collects still takes a record and a state, which is what makes a gap countable.

Figure A3.2 Required sources: a records lane and a signal lane along the traversal



Each record names the one element it is observed on and its state. A step that leaves nothing in a lane writes none; if both fields read none, the path as written is not detectable, and that is a finding.

Table 13 The two required-source fields

	RDS, required data source	RSS, required signal source
What it is	What must be received as a record	What must be measured in the physical layer
Asset-layer line	The AST-DA Data side	The AST-SI Signal side
Counted	RDS:00, RDS:01, from 00 per element	RSS:00, RSS:01, from 00 per element, independently
Each record carries	The OBSERVED ON element and its STATE	
Nothing to hold	The field reads *none*. Both *none*: the path as written is not detectable, a finding to record	

Table 14 The four states of a required source

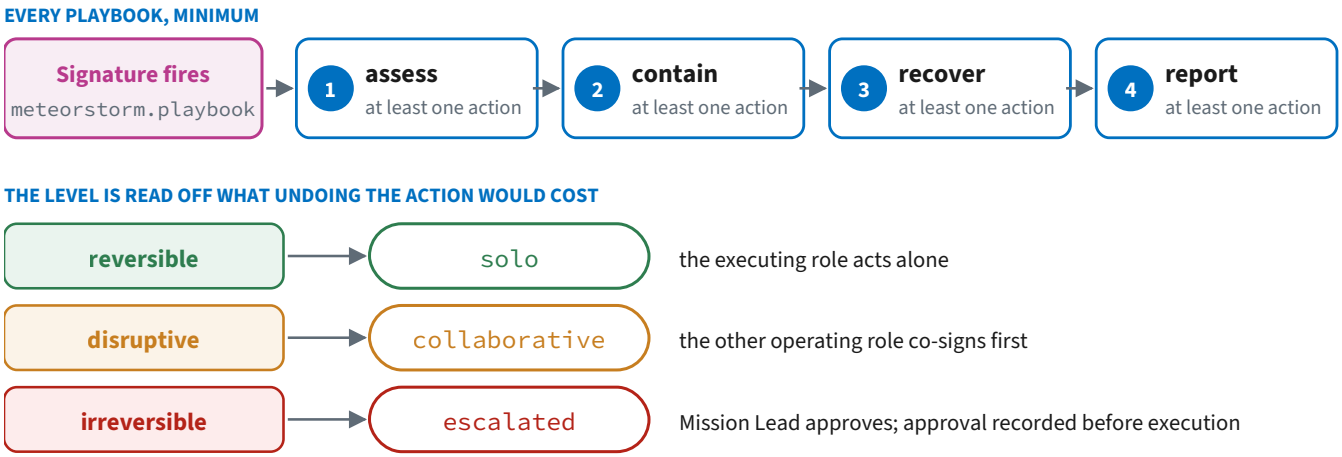
State	Means
Available	Collected; the record names the source identifier.
Partial	Collected with limits; the record names the reason and the owner.
Gap	Assessed and absent; the record names the reason and the owner.
unassessed	The owning department has not yet returned a state. Never counts as coverage, and is never a Gap.

© 2026 ethicallyHackingspace (eHs)®

The playbook on a detection signature

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. Three roles hold them: the Mission Lead is the decider, accountable for every action, and the two operating roles execute, Security Operations the cyber responses and Satellite Operations the space responses. The authority level states what must happen before the executor acts: *solo*, the executing role acts alone and the Mission Lead is informed; *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.

Figure A3.3 The playbook: four stages, and the level read off the cost of undoing



Each action names one element, one executor and one decider. Mission Lead is accountable for every action and executes none of them: the decider never does the work.

© 2026 ethicallyHackingspace (eHs)®

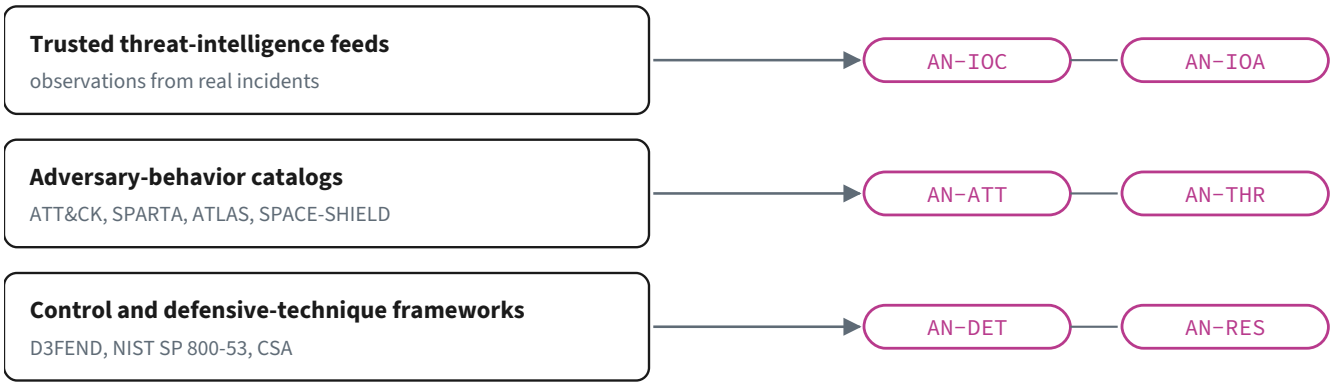
A4 The analytics catalog

The Analytics Catalog 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. 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. 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 elements marked for each source in Table 15 are recommendations, not restrictions: they name the elements each source most naturally supplies. Only 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 catalogs feed Attack Path and Threat. Control and defensive-technique frameworks feed Detection Signature and Resilience Measure.

Figure A4.1 Three source families, and the elements each most naturally feeds



Recommendations, not restrictions: an indicator is never drawn from an architectural framework, because an indicator cannot be theoretical. Table 15 gives every framework and every element it feeds.

© 2026 ethicallyHackingspace (eHs)®

Table 15 Source frameworks and the elements they feed

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

© 2026 ethicallyHackingspace (eHs)®

Background

Who developed it and how it evolved

METEORSTORM comes out of a decade of standing in the middle of the space information sharing problem, not from a whiteboard. It did not begin life as a framework at all. It began as a practical way to generate multi-domain mission scenarios: exercises that had to place realistic adversary activity across terrestrial, aquatic, aerial, orbital, and deep space platforms at once. Building those scenarios kept exposing the same gap. There was no shared vocabulary that could name where on a converged platform something happened, what it touched, and what it meant, in terms every organization at the table could read. The scenario generator's working vocabulary hardened into a data model, the data model proved out in analyst curation workflows, and the result grew into a global framework for converged space platforms.

The author's path runs through the rooms where that gap costs the most:

- Co-Chair, Space ISAC Information Sharing Working Group, and Member Analyst, Space ISAC Analyst Working Group (2020-2022)
- Founder, ethicallyHackingspace (eHs) (2022-2023)
- Technical Editor, IEEE Space Systems Cybersecurity (S2CY) Working Group (2023-present)
- Lead, Space Systems Integration Layer Subgroup, IEEE S2CY Working Group (2026-present)
- Co-Chair, Space Information Sharing and Analysis Center (ISAC) Space System Extended Bill of Material (BOM) Working Group
- MITRE Hardware SIG (2024-present)
- U.S. Air Force from 1993 as a Meteorological and Navigational Systems Specialist, then Instructor of Technology and Military Science at Keesler AFB under Air Education and Training Command until 1997

The meteorology background is not incidental: it is where the environment enters the model. An analyst trained to read weather as an operational force treats the environment as a first-class condition of every record, never as a threat, and that instinct became the model's first layer, the Primary Capability Environment, and the deconfliction question no other framework asked: is this environmental, or is it cyber physical?

The four problems it was built to solve

1. **Fragmented data schema across domains.** Threat and telemetry data from terrestrial, aerial, aquatic, orbital, and deep space systems use incompatible structures, preventing seamless integration or automated cross-correlation.
2. **Incomplete context for threat attribution.** Indicators rarely carry sufficient metadata to distinguish between environmental layer, segment, or service function, making multi-domain attribution inconsistent and error-prone.
3. **Limited machine interpretability of threat indicators.** Existing feeds lack standardized, machine-readable classifications for space-specific threats, constraining automated fusion, enrichment, and detection workflows.
4. **Tagging inconsistency and analytical noise.** Overlapping or ambiguous labels applied by different organizations introduce redundancy and confusion, eroding the reliability of shared threat intelligence.

The framing thesis: the convergence of terrestrial, aquatic, aerial, space, and deep space platforms is both the challenge, keeping pace with AI enabled adversaries, and the opportunity, moving professional skills from non-kinetic to kinetic platforms.

© 2026 ethicallyHackingspace (eHs)®

How it is evolving

The model was formally integrated into MISP in October 2025, and now lives as a published, machine-readable taxonomy in the MISP taxonomy repository, at version 2. That is what lets any organization tag intelligence in the shared vocabulary today and exchange it machine to machine, including with the Space ISAC Exchange. Around the model, a full delivery apparatus has grown: the Full Spectrum Space Cybersecurity Professional program teaches the five functions end to end on a working platform scenario, and its credentials put the framework in the hands of the workforce that has to run it.

The formal debut: CYBERSAT 2025

The model was presented formally at CYBERSAT 2025 in the session Space Collective Defense: Collective Response. The talk laid out the four information sharing problems the model answers, walked all five layers with the design rationale for each, and closed not with a product pitch but with a call to action: three community missions, a Minimum Priority Intelligence Requirements Baseline, a Minimum Converged Detection Engineering Baseline, and a Minimum Telemetry Instrumentation Baseline, with a public entry point at launch.collectivedefense.space. The framing was deliberate. The model was offered to the community as the first big step toward aligning government, commercial, and academic threat intelligence at a global level.

© 2026 ethicallyHackingspace (eHs)®