

METEORSTORM

One data model for the platform, the adversary and the response.

The method
MISP taxonomy v2
d2teamcorp.org

meteorstorm · Multiple Environment Threat Evaluation of Resources Space Threats and Operational Risk to Missions: a taxonomy for modeling space, cyber, and multi-domain threats and resilience across five layers. Published in the MISP taxonomy repository, version 2, October 2025.

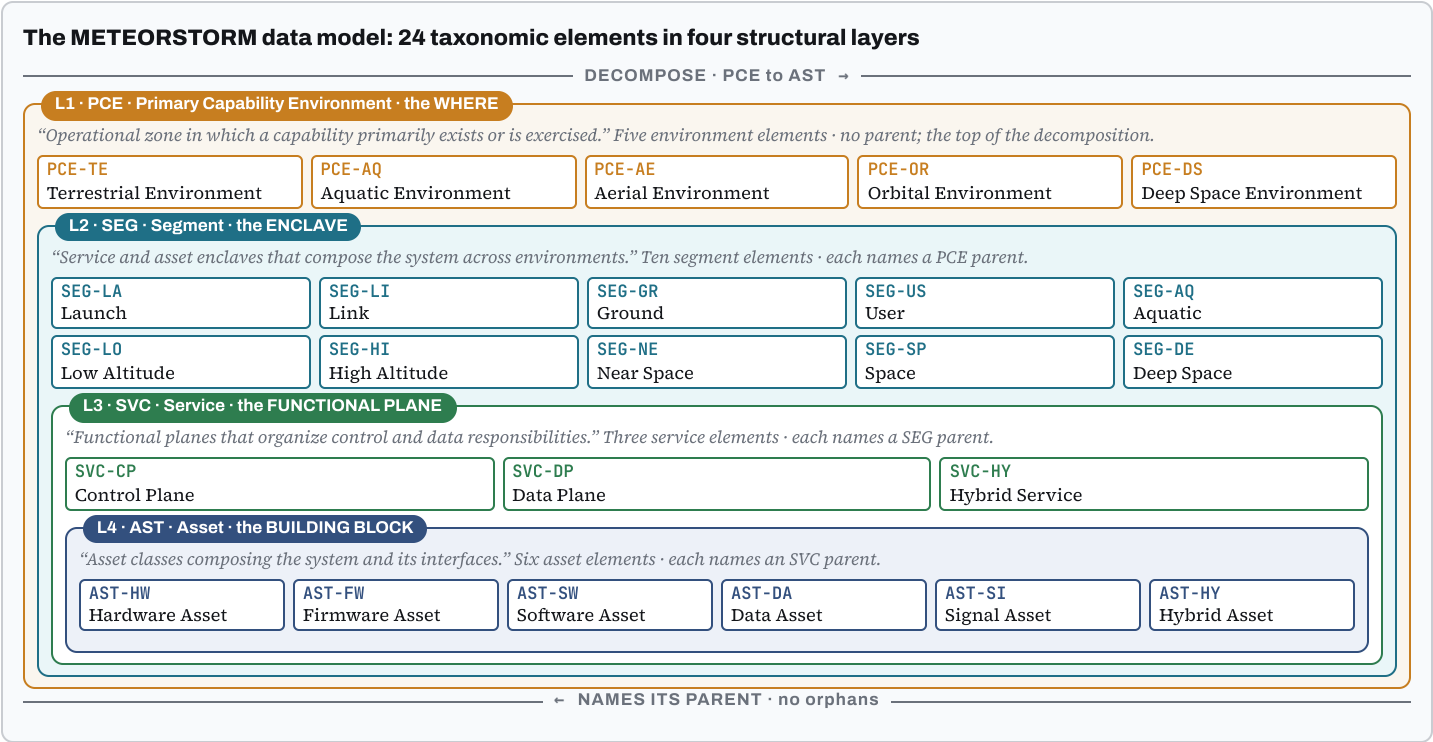


Figure 1. Every component of a platform in scope is recorded as exactly one enumerated element, in one of these four layers, and every element names its parent.

1 FIVE FUNCTIONS, RUN IN ORDER

F01	Concept of Operations	Decompose the platform tailored to your requirements.	PCE SEG SVC AST
F02	Contextualized Threat Modeling	Anchor every threat to the platform you just decomposed.	AN-THR
F03	Converged Detection Engineering	Enumerate attack paths and the data and signals needed to detect each step.	AN-ATT
F04	Incident Response Preparation	Write the detection signatures and the response playbooks.	AN-DET
F05	Adversary Management	Shrink the attack surface the threats keep using.	AN-RES

2 ONE MODEL, EVERY ENVIRONMENT

METEORSTORM covers the ground, user, link, and space segments, and also the aquatic, aerial, and deep space environments. When a merger, an acquisition, or a new market strategy takes your organization toward cislunar, maritime, or drone operations, your staff and your data model come with you: no expensive re-upskilling, no framework migration.

And you do not have to choose METEORSTORM over other frameworks: the analytic layer normalizes past, present, and future frameworks into the same standardized taxonomy and ontology, without building a new taxonomy for each. The reverse shows the layer and the sources it normalizes today.

The Analytic layer

What the analyst knows about the platform, in a form every participating organization reads identically.

METEORSTORM

Layer 5 · AN

3 SIX ELEMENTS, THREE TARGET FIELDS

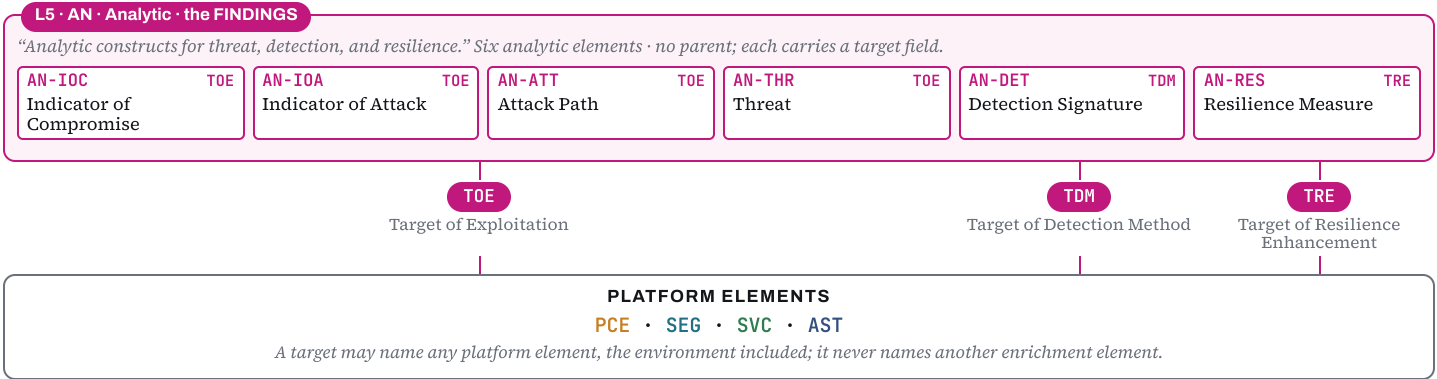


Figure 2. Six elements, three target fields, one destination. Read left to right, they answer the questions an analyst asks as a situation unfolds. Every entry declares its SOURCE before enumeration: observable, or synthetic.

4 WHERE FINDINGS COME FROM: THE ANALYTICS CATALOG

FRAMEWORK	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						•

Table 1. 14 sources and the analytic elements each most naturally supplies; recommendations, not restrictions. METEORSTORM does not replace these frameworks or compete with them: their content normalizes into the same six elements.

5 NAMING ONE REAL INSTANCE: THE ETEN

LAYER	TAG	LABEL	ORDINAL	DESCRIPTION
SEG	GR	Ground	00	<i>what it is, where it is, what role it plays</i>

Tags come from the published list, never invented. Ordinals start at 00 and are never re-used. One identifier carries exactly one description, everywhere it appears.

6 MACHINE-READABLE FROM DAY ONE

The data model is a published taxonomy in the MISP taxonomy repository, namespace meteorstorm, version 2, integrated in October 2025. A partner’s threat intelligence platform reads the tags unchanged, so findings move machine to machine in one shared vocabulary.