FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

REFERENCE WORKBOOK

Kestrel Orbital Day 1-5 Analytic Layer

The Analytic Layer Enumerated Taxonomic Element Nomenclature (ETEN) reference. The threats, attack paths, detection signatures, and resilience measures enumerated across the five functions, each anchored to one platform element.

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Kestrel Orbital Day 1-5 Analytic Layer, ETEN reference workbook
EDITION	First edition · version 1.0 · revised 2026-09-24
CONTACT	www.d2teamcorp.org

SCOPE AND STANDING OF THIS WORK · READ BEFORE JUDGING THE ENUMERATION

What this is. Kestrel Orbital's first application of the METEORSTORM framework, produced by three departments who had never used it before, in five working days. It is a deliberately scoped first pass over the telecommand path: the command-and-control chain from the operator console to execution on orbit.

Why that scope, and not more. The mandates chose it. Executive Order 14144 puts the command and control of an operational platform first, and the NIS2 Directive places a duty of care and a reporting clock on the ground operator. The fleet is already flying, so the first pass ran on the part that would end the mission if an adversary took it. Enumerating everything else first would have been thorough and useless.

What it is not, stated plainly. It is not an exhaustive model of the platform and does not claim to be. Elements off the telecommand path are not enumerated. Some assets group several physical units where those units share an owner, a build and a patch path. Gaps in the ordinal sequence mark elements the register tracks outside this scope. Every one of those is a recorded decision taken at the enumeration meeting, not an oversight discovered later.

How it grows. Ordinals are issued once and never renumbered, so everything enumerated here keeps its identifier as the register expands. The same eight-step procedure runs on the next scope, and the one after that. A first pass that names its boundary can be extended. One that hides its boundary has to be rebuilt.

The standard we hold ourselves to. A scope choice is stated openly. A defect is fixed, never narrated. If you find an element misnamed, a parent wrong, or a count that does not add up, that is a defect and we want to hear about it. If you find something outside the telecommand path missing, that is the scope, it was chosen deliberately, and it is on the roadmap. The two are not the same criticism, and this work is built so you can tell them apart.

CONTENTS

An analytic Enumerated Taxonomic Element Nomenclature (ETEN) names one enrichment element on a platform, in five fields. 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.

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.

ETEN EXAMPLE

LAYER	**AN**
TAG	**THR**
LABEL	**Threat**
ORDINAL	**02**
SOURCE	**observable**
TOE	**SVC:CP:Control Plane:09**
DESCRIPTION	**State-sponsored actor with demonstrated capability to gain persistent access to SATCOM management networks and abuse the provider-to-customer trust relationship to push malicious modem updates (KA-SAT / AcidRain class). Source: composite OSINT threat assessment read against the peer-reviewed research paper.**
ETEN	**AN:THR:Threat:00:State-sponsored actor targeting the ground ACA management plane to push malicious modem updates.**

THE ANALYTIC LAYER, OVERVIEW

ENRICHMENT	The four structural layers (PCE, SEG, SVC, AST) enumerate the platform. The Analytic Layer enriches that decomposition: each AN entry is an enrichment element recording what the analyst knows about specific platform elements. It takes no PARENT; it is not part of the platform.
TAXONOMY	Each entry is classified by LAYER, TAG, and LABEL: six elements, AN-IOC, AN-IOA, AN-ATT, AN-THR, AN-DET, AN-RES.
ONTOLOGY	Where structural elements bind upward through PARENT, an enrichment element binds through its target reference: TOE for IOC, IOA, ATT, and THR; TDM for DET; TRE for RES. The target is fixed by the tag. The anchor is machine-readable, so an entry enumerated against an AST is reachable from queries against the SVC, SEG, and PCE above it. An anchor names a platform element, never another enrichment element.

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.

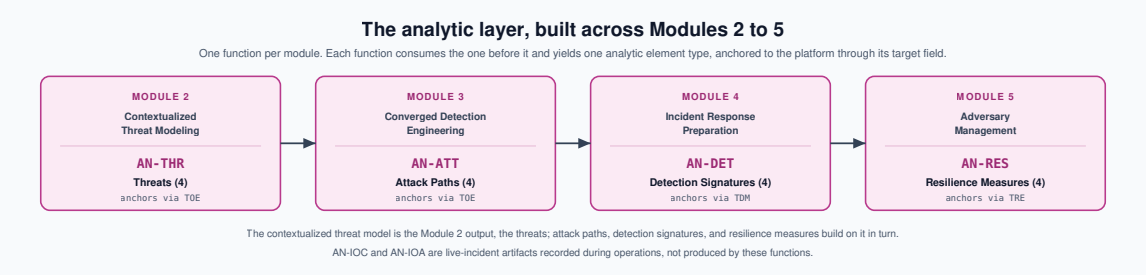
OBSERVABLE	**Built on a real-world report:** a signal or data captured from a system. The standard for IOC, IOA, ATT, THR.
SYNTHETIC	**Authored data** for system resilience engineering and operational exercises.

Collective defense. Under the Space ISAC Exchange sharing mandate (Space Information Sharing and Analysis Center), every finding relevant to Executive Order 14144 or the NIS2 Directive is shared: the indicators, the tactics and techniques, the affected ETENs, and the detection signatures in an open format, so peer operators defend before they are hit. An incoming peer finding enters this catalogue only after peer validation, normalized with its provenance recorded: source framework, source id, source name.

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 six-step process in its section.

THE KESTREL ENUMERATION

The analytic layer is built across Modules 2 to 5, one function per module, against the Day-1 CONOPS: 4 threats in Module 2, 4 attack paths in Module 3, 4 detection signatures in Module 4, and 4 resilience measures in Module 5, 16 enumerated elements in four chains. The contextualized threat model is the Module 2 output, the threats; each later function builds on it. AN-IOC and AN-IOA are live-incident artifacts recorded during operations, not produced by these functions. The platform elements every entry anchors to are in the structural ETEN reference; the analytic element definitions are in the analytic TEN reference.



The analytic layer across Modules 2 to 5. Contextualized Threat Modeling yields the AN-THR threats; Converged Detection Engineering the AN-ATT attack paths; Incident Response Preparation the AN-DET detection signatures; Adversary Management the AN-RES resilience measures. Each anchors to the platform through its target field, TOE, TDM, or TRE.

THE FOUR CHAINS

Every entry in this catalog belongs to a chain, and every chain is one scenario carried through all four analytic elements under one ordinal: the threat names its target element in its TOE field, the attack path traces how that threat moves through the platform, the detection signature fires on that behavior with its TDM equal to the threat's TOE, and the resilience measure counters it with its TRE equal to the same element. One number, one anchor element, end to end.

```
AN:THR:Threat:NN → AN:ATT:Attack Path:NN → AN:DET:Detection Signature:NN → AN:RES:Resilience Measure:NN
```

CHAIN	ANCHOR ELEMENT	SCENARIO, AS THE THREAT STATES IT
00	SVC:CP:Control Plane:09	State-sponsored actor targeting the ground ACA management plane to push malicious modem updates.
01	AST:SW:Software:04	Cleared operator misusing the console software to issue unauthorized telecommands.
02	AST:SI:Signal:00	RF actor jamming the uplink and downlink waveforms to deny command and telemetry.
03	AST:FW:Firmware:01	Adversary pushing a backdoored firmware image to the on-board computer over the update path.

The chapters that follow present the catalog by element type: every threat, then every attack path, then every detection signature, then every resilience measure. Read a chain horizontally by following its ordinal through the four chapters. The anchor equality is what makes coverage auditable: every threat in this catalog is either covered end to end or would carry a recorded gap.

L5 AN-THR · THREATS (4)

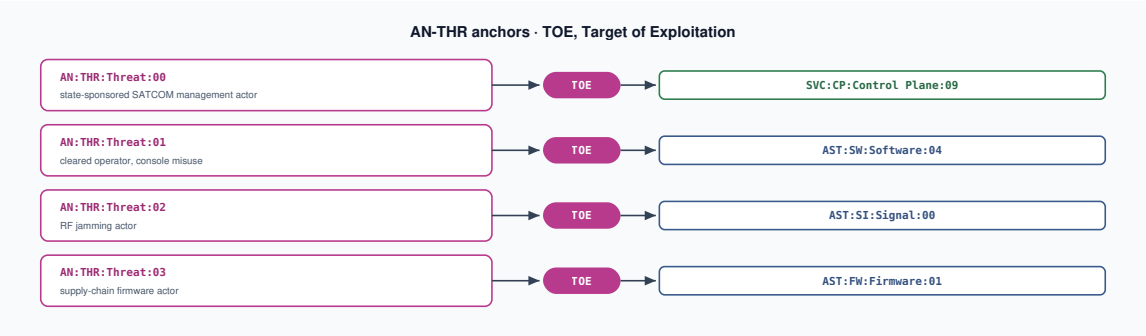
Definition: “Known adversarial threat to the platform” (METEORSTORM:AN=THR)

A Threat is the targeted statement: a known adversary capability or campaign directed at the platform or its class of systems. Where an Attack Path records what the platform exposes, a Threat records who or what is likely to exercise that exposure. The two work as a pair: a path with no threat is a hypothetical, and a threat with no path is unmoored from the architecture. Every entry is built on attributed adversary activity: threat-intelligence reporting, government attribution, or a peer-shared adversary profile, so the community reads every threat as evidenced, not assumed.

The three departments, at the table. SCOR runs Function 02, Contextualized Threat Modeling, with all three departments. The Security Operations Center brings the threat intelligence and attribution; the Satellite Operations Center brings the operational picture, what normal commanding and passes look like, so each threat anchors to the right element; Satellite Design and Engineering brings the architecture, confirming which enumerated element a threat can actually reach. The output is the contextualized threat model: every AN-THR anchored by TOE to the platform element it targets.

AN-THR ETEN PROCESS

STEP 01	**Enumerate the LAYER.** AN (fixed).
STEP 02	**Confirm the source.** The threat-intelligence report, government attribution statement, peer-shared adversary profile, or open-source intelligence the threat is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
STEP 03	**Set the TAG to THR.** AN:THR.
STEP 04	**Assign an ORDINAL.** Two digits from 00, one per distinct threat.
STEP 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.
STEP 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.



Each AN-THR entry with its one TOE target, the enumerated platform element from its catalogue entry, in the layer colours of the structural ETEN reference.

EXAMPLES, FIELD BY FIELD (4)

FIELD	VALUE
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	00
SOURCE	observable
TOE	SVC:CP:Control Plane:09
DESCRIPTION	State-sponsored actor with demonstrated capability to gain persistent access to SATCOM management networks and abuse the provider-to-customer trust relationship to push malicious modem updates (KA-SAT / AcidRain class). Source: composite OSINT threat assessment read against the peer-reviewed research paper.
ETEN	AN:THR:Threat:00:State-sponsored actor targeting the ground ACA management plane to push malicious modem updates.

FIELD	VALUE
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	01
SOURCE	observable
TOE	AST:SW:Software:04
DESCRIPTION	Cleared operator with command authority misuses the commanding console software to issue unauthorized telecommands to the vehicle. Source: insider-threat reporting, MITRE ATT&CK T1078 Valid Accounts.
ETEN	AN:THR:Threat:01:Cleared operator misusing the console software to issue unauthorized telecommands.

FIELD	VALUE
LAYER	AN
TAG	THR

LABEL	Threat
ORDINAL	02
SOURCE	observable
TOE	AST:SI:Signal:00
DESCRIPTION	RF actor sustains noise injection across the uplink and downlink bands to deny command and telemetry to the vehicle. Source: ITU interference reporting, documented SATCOM jamming campaigns.
ETEN	AN:THR:Threat:02:RF actor jamming the uplink and downlink waveforms to deny command and telemetry.

FIELD	VALUE
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	03
SOURCE	observable
TOE	AST:FW:Firmware:01
DESCRIPTION	Adversary subverts the flight-software update supply chain and pushes a backdoored firmware image to the on-board computer over the command-and-update path. Source: NIST SP 800-193, SolarWinds supply-chain reporting.
ETEN	AN:THR:Threat:03:Adversary pushing a backdoored firmware image to the on-board computer over the update path.

L5 AN-ATT · ATTACK PATHS (4)

Definition: “Known attack path for a converged space system” (METEORSTORM:AN=ATT)

An Attack Path is a conditional statement: a documented sequence of adversary actions that could traverse the platform from entry to impact. Attack Paths are exposures, not observations; they record what is reachable given the architecture. Each one is drawn from real-world reporting: a confirmed exposure observed against the platform or a trusted partner, or documented adversary tradecraft, so the community reads every path as grounded, not guessed.

Two source fields, kept separate. An attack path states what a defensive cyber operator must hold to see it, in two fields. **RDS**, the required data source, is what must be received as a record: a log, an audit stream, an inventory, a telemetry feed. **RSS**, the required signal source, is what must be measured in the physical layer: a noise floor, a carrier-to-noise ratio, a lock status, a received power level. They are two fields because they are two kinds of observable, the same line the structural taxonomy draws between AST-DA Data and AST-SI Signal. On a converged space platform that line decides whether a path is detectable at all: jamming is seen in the noise floor, and it is never seen in a log. The word that does the work is *required*. The field states what a defensive cyber operator must hold, not what the organization happens to hold today, which is what makes coverage computable instead of asserted: required against available, and the difference is the gap.

The three departments, converged. SCOR runs Function 03, Converged Detection Engineering, across the same three. The Security Operations Center traces how an adversary moves to realize each threat; the Satellite Operations Center confirms which moves are visible in operations; Satellite Design and Engineering names the data and signal sources on each element. The output is the AN-ATT attack paths, each anchored to the same element as the threat it realizes, with the pivot in its description.

AN-ATT ETEN PROCESS

STEP 01 **Enumerate the LAYER.** AN (fixed).

STEP 02 **Confirm the source.** The confirmed exposure, red-team report, adversary-behavior catalogue entry (ATT&CK, SPARTA, ATLAS), or peer-shared documentation the path is drawn from. The source defines the TOE. SOURCE is observable or synthetic.

STEP 03 **Set the TAG to ATT.** AN:ATT.

STEP 04 **Assign an ORDINAL.** Two digits from 00, one per distinct path.

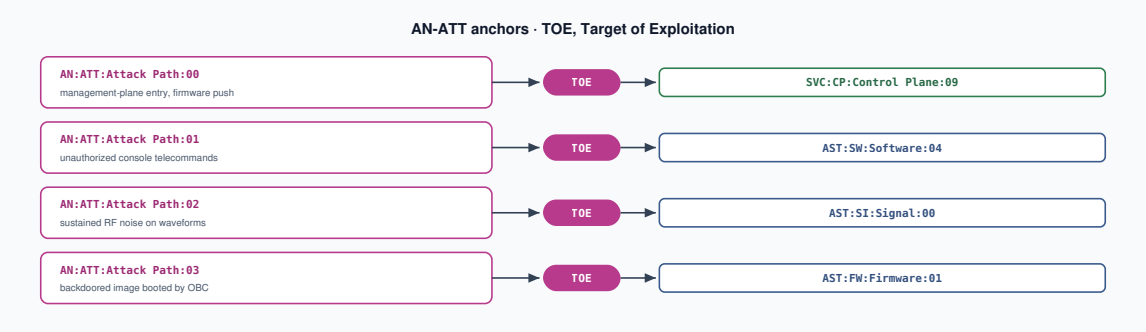
STEP 05 **Enumerate the TOE.** One enumerated platform element: the element the path is anchored to, the same element the related AN-THR names. Concrete, at the lowest layer the source resolves.

STEP 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.

STEP 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 or Gap. Where the path leaves no records at all, write `none`.

STEP 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 three 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.

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.



Each AN-ATT entry with its one TOE target, the enumerated platform element from its catalogue entry, in the layer colours of the structural ETEN reference.

EXAMPLES, FIELD BY FIELD (4)

FIELD	VALUE
LAYER	AN
TAG	ATT

LABEL	Attack Path
ORDINAL	**00**
SOURCE	**observable**
TOE	**SVC:CP:Control Plane:09**
RDS	RDS:00 Management-plane firmware-push operation record · observed on SVC:CP:Control Plane:09 · **Available**, `src-ground-aca-010`. Records for the entry and objective steps are required by this path and are not yet enumerated.
RSS	Not yet enumerated. The objective step's observable, mass terminal drop-off, is physical and belongs in this field.
DESCRIPTION	Anchored to the ground ACA management plane, SVC:CP:Control Plane:09. Pivot: entry through the external VPN appliance into the management network, abuse of the ground ACA (SVC:CP:Control Plane:09), through the ACA software (AST:SW:Software:02) and credential store (AST:DA:Data:01) onto the patch path (SVC:CP:Control Plane:12), objective a wiper pushed as a firmware update, modems bricked. Source: Space ISAC advisory, KA-SAT / AcidRain reporting.
ETEN	**AN:ATT:Attack Path:00:Management-plane entry pivoting through the ground ACA onto the patch path to push a wiper as a firmware update.**

FIELD	VALUE
LAYER	**AN**
TAG	**ATT**
LABEL	Attack Path
ORDINAL	**01**
SOURCE	**observable**
TOE	**AST:SW:Software:04**
RDS	RDS:00 Command-authority usage record carrying the peer-review tag · observed on AST:SW:Software:04 · **Partial**, the peer-review tag stream depends on workflow adoption. Records for the entry and objective steps are required by this path and are not yet enumerated.
RSS	none

DESCRIPTION	Anchored to the console operator software, AST:SW:Software:04. Pivot: authenticated operator on the console software issues unauthorized telecommands through the satellite console service (SVC:CP:Control Plane:13), bypassing single-operator review at the ground ACA (SVC:CP:Control Plane:09), objective an out-of-profile command to the vehicle. Source: insider-threat reporting.
ETEN	AN:ATT:Attack Path:01:Authenticated operator issuing unauthorized telecommands from the console, bypassing single-operator review.

FIELD	VALUE
LAYER	AN
TAG	ATT
LABEL	Attack Path
ORDINAL	02
SOURCE	observable
TOE	AST:SI:Signal:00
RDS	none
RSS	RSS:00 Receiver radio-frequency measurement, carrying received power and noise floor · observed on AST:SI:Signal:00 · **Available**, `src-rx-rf-024`. Records for the entry and pivot steps are required by this path and are not yet enumerated.
DESCRIPTION	Anchored to the uplink and downlink waveforms, AST:SI:Signal:00. Pivot: RF actor injects sustained noise onto the waveforms, overwhelming forward-error correction (SVC:HY:Hybrid:01) and tracking and telemetry (SVC:HY:Hybrid:02), objective denial of command and telemetry. May be paired with timing knowledge of overhead passes. Source: documented jamming campaigns.
ETEN	AN:ATT:Attack Path:02:Sustained RF noise on the waveforms overwhelming FEC and tracking to deny command and telemetry.

FIELD	VALUE
LAYER	AN
TAG	ATT
LABEL	Attack Path
ORDINAL	03
SOURCE	observable

TOE	**AST:FW:Firmware:01**
RDS	RDS:00 Boot-time firmware measurement and attestation record · observed on AST:FW:Firmware:01 · **Gap**, measured boot is not flown; owner Satellite Design and Engineering. A required source that does not exist still takes a sub-ordinal and a state. That is what makes this gap countable rather than a sentence in a chapter.
RSS	none
DESCRIPTION	Anchored to the on-board computer boot firmware, AST:FW:Firmware:01. Pivot: backdoored image staged in the patch pipeline (AST:SW:Software:03), pushed over the command-and-update path (SVC:CP:Control Plane:12), booted by the on-board computer, objective persistent control of the OBC. Source: NIST SP 800-193.
ETEN	**AN:ATT:Attack Path:03:Backdoored image staged in the patch pipeline and booted by the on-board computer for persistent control.**

L5 AN-DET · DETECTION SIGNATURES (4)

Definition: “Pattern, signal, or logic that triggers on contextualized threat behavior, expressed in RootA format” (METEORSTORM:AN=DET)

A Detection Signature is the coverage statement: the written commitment to see a specific behavior when it produces observable activity. A threat or attack path with no matching signature is a detection gap, and the gap is itself an enumerable analytic product. Every entry is a complete RootA rule (SOC Prime RootA specification v1.0.0), the open, vendor-neutral wrapper over the native query language it was authored in, extended with a METEORSTORM block that anchors the rule to its enumerated platform element, so a signature written by one operator deploys and routes in another operator’s stack without translation. In the ontology, AN-DET binds through TDM, Target of Detection Method: the one element the signature watches, and it is the same element the AN-THR it serves named in its TOE.

The three departments, engineering coverage. SCOR runs Function 04, Incident Response Preparation, as a joint product. The Security Operations Center authors the RootA signature; the Satellite Operations Center validates it against real telemetry so it fires without drowning operations in false positives; Satellite Design and Engineering confirms the source is instrumented on the element. Each AN-DET binds by TDM to the element its threat targets and ships in RootA so it crosses to peer operators.

Every signature names its authorized response. The rule says the platform will see the behavior. The playbook says what the organization is already authorized to do about it, who executes, and who decides. They ship side by side, same directory, same stem, bound through `meteorstorm.playbook`, so a peer operator receives the response with the detection. Approved actions run across assess, contain, recover and report, and the authority level of each is read off what undoing it would cost, never chosen: `solo`, `collaborative`, `escalated`. Mission Lead is accountable for every action and executes none.

AN-DET ETEN PROCESS

STEP 01 **Enumerate the LAYER.** AN (fixed).

STEP 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, Sigma) with no RootA wrapper is not accepted into the layer. SOURCE is observable or synthetic.

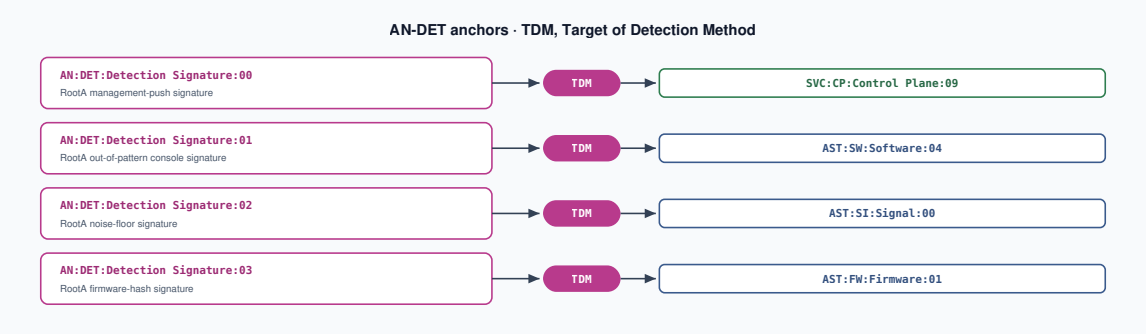
STEP 03 **Set the TAG to DET.** AN:DET.

STEP 04 **Assign an ORDINAL.** Two digits from 00, one per distinct signature.

STEP 05 **Enumerate the TDM.** One enumerated platform element the signature observes, the same element the related AN-THR targets. TDM, not TOE: the element scanned, not the element exploited.

STEP 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. See the roota authority for the full field set.

STEP 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.



Each AN-DET entry with its one TDM target, the enumerated platform element from its catalogue entry, in the layer colours of the structural ETEN reference.

EXAMPLES, FIELD BY FIELD (4)

FIELD	VALUE
LAYER	AN
TAG	DET
LABEL	Detection Signature

ORDINAL	00
SOURCE	observable
TDM	SVC:CP:Control Plane:09
PLAYBOOK	PB-00
DESCRIPTION	Full RootA rule, base fields plus the METEORSTORM anchor block: Covers AN:ATT:Attack Path:00 and AN:THR:Threat:00. Source: SOC detection engineering.
ETEN	AN:DET:Detection Signature:00:RootA signature for the chain-00 behavior on SVC:CP:Control Plane:09.

```
name: KO-DET-ACA-MGMT-PUSH-000
title: Firmware push from ground ACA management interface outside maintenance window
severity: high
type: query
class: behavioral
date: 2026-07-26
mitre-attack:
  - t1195.002
detection:
  language: splunk-spl-query
  body: index=ground_aca sourcetype=mgmt action=firmware_push | where
in_maintenance_window=false OR vpn_auth_anomaly=true
logsource:
  product: ground-aca
  service: management-plane
references:
  - AN:ATT:Attack Path:00
  - AN:THR:Threat:00
tags: KO-DET-ACA-MGMT-PUSH-000, acidrain, ground-aca
license: DRL 1.1
version: 1
uuid: a1b2c3d4-0000-4a00-8a00-000000000000
meteorstorm:
  pce: PCE:TE:Terrestrial:00
  seg: SEG:GR:Ground:00
  svc: SVC:CP:Control Plane:09
  an:
    eten: AN:DET:Detection Signature:00
    tdm: SVC:CP:Control Plane:09
```

FIELD	VALUE
LAYER	AN
TAG	DET
LABEL	Detection Signature
ORDINAL	01
SOURCE	observable

TDM	**AST:SW:Software:04**
PLAYBOOK	**PB-01**

DESCRIPTION	Full RootA rule, base fields plus the METEORSTORM anchor block:
	`name: KO-DET-CONSOLE-OOP-001`
	`title: Out-of-pattern commanding from the operator console`
	`severity: high`
	`type: query`
	`class: behavioral`
	`date: 2026-07-26`
	`mitre-attack:`
	`  - t1078`
	`detection:`
	`  language: splunk-spl-query`
	`  body: index=console sourcetype=command | where hour_of_day NOT IN (operator_shift) OR peer_review_tag=null OR off_mission_profile=true`
	`logsource:`
	`  product: console-ops`
	`  service: command-audit`
	`references:`
	`  - AN:ATT:Attack Path:01`
	`  - AN:THR:Threat:01`
	`tags: KO-DET-CONSOLE-OOP-001, insider, console`
	`license: DRL 1.1`
	`version: 1`
	`uuid: a1b2c3d4-0001-4a00-8a00-000000000000`
	`meteorstorm:`
	`  pce: PCE:TE:Terrestrial:00`
	`  seg: SEG:GR:Ground:00`
	`  svc: SVC:CP:Control Plane:13`
	`  ast: AST:SW:Software:04`
	`  an:`
	`  eten: AN:DET:Detection Signature:01`
	`  tdm: AST:SW:Software:04`
	Covers AN:ATT:Attack Path:01 and AN:THR:Threat:01. Source: SOC detection engineering.

ETEN	**AN:DET:Detection Signature:01:RootA signature for the chain-01 behavior on AST:SW:Software:04.**

FIELD	VALUE
LAYER	**AN**
TAG	**DET**
LABEL	Detection Signature
ORDINAL	**02**
SOURCE	**observable**
TDM	**AST:SI:Signal:00**

PLAYBOOK	**PB-02**

DESCRIPTION	Full RootA rule, base fields plus the METEORSTORM anchor block:
	`name: KO-DET-RF-NOISE-002`
	`title: Sustained noise-floor anomaly on the uplink and downlink bands`
	`severity: high`
	`type: query`
	`class: behavioral`
	`date: 2026-07-26`
	`detection:`
	`  language: splunk-spl-query`
	`  body: index=rf_metrics | stats avg(noise_floor_db) as nf by band, _time span=5m |`
	`where nf > env_threshold_db AND sustained_minutes > 10`
	`logsource:`
	`  product: rf-frontend`
	`  service: snr-telemetry`
	`references:`
	`  - AN:ATT:Attack Path:00`
	`  - AN:THR:Threat:00`
	`tags: KO-DET-RF-NOISE-002, jamming, rf`
	`license: DRL 1.1`
	`version: 1`
	`uuid: a1b2c3d4-0002-4a00-8a00-000000000000`
	`meteorstorm:`
	`  pce: PCE:TE:Terrestrial:01`
	`  seg: SEG:LI:Link:00`
	`  svc: SVC:HY:Hybrid:02`
	`  ast: AST:SI:Signal:00`
	`  an:`
	`  eten: AN:DET:Detection Signature:00`
	`  tdm: AST:SI:Signal:00`
	Covers AN:ATT:Attack Path:00 and AN:THR:Threat:00. Source: SOC detection engineering.

ETEN	**AN:DET:Detection Signature:02:RootA signature for the chain-02 behavior on AST:SI:Signal:00.**

FIELD	VALUE
LAYER	**AN**
TAG	**DET**
LABEL	Detection Signature
ORDINAL	**03**
SOURCE	**observable**
TDM	**AST:FW:Firmware:01**
PLAYBOOK	**PB-03**

DESCRIPTION

Full RootA rule, base fields plus the METEORSTORM anchor block:

```
name: KO-DET-FW-HASH-003
title: Firmware hash mismatch at boot on the on-board computer
severity: high
type: query
class: behavioral
date: 2026-07-26
mitre-attack:
  - t1542
detection:
  language: splunk-spl-query
  body: index=obc_boot sourcetype=attestation | where measured_hash !=
signed_expected_hash
logsource:
  product: obc
  service: boot-attestation
references:
  - AN:ATT:Attack Path:03
  - AN:THR:Threat:03
tags: KO-DET-FW-HASH-003, supply-chain, firmware
license: DRL 1.1
version: 1
uuid: a1b2c3d4-0003-4a00-8a00-000000000000
meteorstorm:
  pce: PCE:OR:Orbital:00
  seg: SEG:SP:Space:00
  svc: SVC:HY:Hybrid:00
  ast: AST:FW:Firmware:01
  an:
    eten: AN:DET:Detection Signature:03
    tdm: AST:FW:Firmware:01
```

Covers AN:ATT:Attack Path:03 and AN:THR:Threat:03. Source: SOC detection engineering.

ETEN

AN:DET:Detection Signature:03:RootA signature for the chain-03 behavior on AST:FW:Firmware:01.

L5 AN-RES · RESILIENCE MEASURES (4)

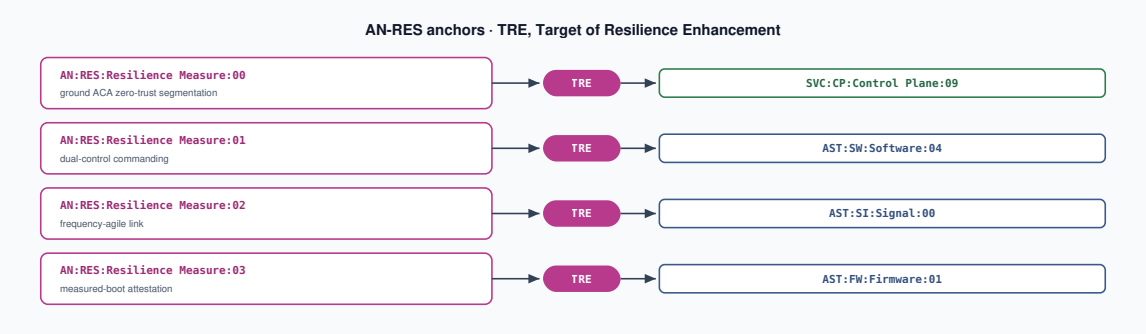
Definition: “Protective capability ensuring resistance or recovery from threats, for either immediate implementation or as feedback for future platform engineering efforts” (METEORSTORM:AN=RES)

A Resilience Measure is the forward-looking statement: what the organization changes to alter its posture. Each entry serves one of the four cyber-resiliency goals of NIST SP 800-160 Volume 2: Anticipate, Withstand, Recover, Adapt. Measures are enumerated prospectively, before they are exercised, which makes completeness auditable: a reviewer walks the attack paths and checks that each has a corresponding measure or a consciously accepted residual risk. Accessible technologies apply the measure in place at the cadence they support; for a vehicle on orbit, the same entry becomes input to the next generation of platform design. In the ontology, AN-RES binds through TRE, Target of Resilience Enhancement: the element the measure protects.

The three departments, hardening the platform. SCOR runs Function 05, Adversary Management, across the three. The Security Operations Center names the elements that recur across many threats and paths; Satellite Design and Engineering builds or specifies the measure; the Satellite Operations Center runs it at the cadence the platform supports. Each AN-RES binds by TRE to the element its threat targets, with one resiliency goal.

AN-RES ETEN PROCESS

STEP 01	**Enumerate the LAYER.** AN (fixed).
STEP 02	**Identify the resiliency goal.** One of Anticipate, Withstand, Recover, or Adapt, per NIST SP 800-160 Volume 2. SOURCE is observable or synthetic.
STEP 03	**Set the TAG to RES.** AN:RES.
STEP 04	**Assign an ORDINAL.** Two digits from 00, one per distinct measure.
STEP 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.
STEP 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.



Each AN-RES entry with its one TRE target, the enumerated platform element from its catalogue entry, in the layer colours of the structural ETEN reference.

EXAMPLES, FIELD BY FIELD (4)

FIELD	VALUE
LAYER	AN
TAG	RES
LABEL	Resilience Measure
ORDINAL	00
SOURCE	observable
TRE	SVC:CP:Control Plane:09
DESCRIPTION	Zero-trust segmentation of the ground ACA management plane from external networks, with hardware-rooted attestation and dual-approval on every management-plane action. Protects SVC:CP:Control Plane:09. Goal: Withstand. Counters AN:ATT:Attack Path:00 and AN:THR:Threat:00. Source: internal engineering, KA-SAT / AcidRain lesson.
ETEN	AN:RES:Resilience Measure:00:Zero-trust segmentation and dual-approval on the ground ACA management plane.

FIELD	VALUE
LAYER	AN
TAG	RES
LABEL	Resilience Measure
ORDINAL	01
SOURCE	observable
TRE	AST:SW:Software:04
DESCRIPTION	Dual-control commanding for high-impact actions, a second operator approving before transmission, with per-operator behavior baselines and pre-pass briefings enforced in the console software. Protects AST:SW:Software:04. Goal: Withstand. Counters AN:ATT:Attack Path:01 and AN:THR:Threat:01. Source: internal engineering.
ETEN	AN:RES:Resilience Measure:01:Dual-control commanding and per-operator baselines in the console software.

FIELD	VALUE
LAYER	AN
TAG	RES

LABEL	Resilience Measure
ORDINAL	**02**
SOURCE	**observable**
TRE	**AST:SI:Signal:00**
DESCRIPTION	Frequency-agile, spread-spectrum link operation with a pre-arranged backup band; Satellite Operations switches bands automatically when the noise floor exceeds threshold; Satellite Design and Engineering owns the agility waveform. Protects AST:SI:Signal:00. Goal: Withstand. Counters AN:ATT:Attack Path:02 and AN:THR:Threat:02. Source: internal engineering.
ETEN	**AN:RES:Resilience Measure:02:Frequency-agile spread-spectrum link with automatic band switch on noise threshold.**

FIELD	VALUE
LAYER	**AN**
TAG	**RES**
LABEL	Resilience Measure
ORDINAL	**03**
SOURCE	**observable**
TRE	**AST:FW:Firmware:01**
DESCRIPTION	Measured-boot firmware attestation with a signed-vendor manifest, supply-chain provenance verification at integration, and quarantine of any image whose hash does not match the signed expected value. Protects AST:FW:Firmware:01. Goal: Anticipate. Counters AN:ATT:Attack Path:03 and AN:THR:Threat:03. Source: internal engineering, NIST SP 800-193.
ETEN	**AN:RES:Resilience Measure:03:Measured-boot attestation with signed-vendor manifest and hash-mismatch quarantine.**

L5 INDICATORS · AN-IOC AND AN-IOA (0)

Indicators of compromise and indicators of attack are live-incident artifacts, recorded during operations, not produced by the five-function build. They were not the primary focus of this course, which teaches the enumeration of threats, attack paths, detection signatures, and resilience measures across Modules 2 to 5. Their processes and worked examples are kept here in full for completeness.

L5 AN-IOC · INDICATOR OF COMPROMISE

Definition: “Verifiable indication that the platform has been compromised” (METEORSTORM:AN=IOC)

An Indicator of Compromise is backward-looking evidence anchored to a real-world observation: a file hash recovered from a host, a command-and-control domain reached by a beacon, a registry key left behind by a known tool. It answers the first question of any unfolding situation: has something already happened here?

AN-IOC is the highest priority analytic element. It indicates a confirmed platform breach, and every entry is traceable to an actual incident or live operator telemetry. That confirmation is what a peer operator acts on immediately, without further analysis.

AN-IOC ETEN PROCESS

STEP 01	**Enumerate the LAYER.** AN (fixed).
STEP 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.
STEP 03	**Set the TAG to IOC.** AN:IOC.
STEP 04	**Assign an ORDINAL.** Two digits from 00, one per distinct indicator.
STEP 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.
STEP 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.

EXAMPLE, FIELD BY FIELD

FIELD	VALUE
LAYER	AN
TAG	IOC
LABEL	Indicator of Compromise
ORDINAL	00
SOURCE	observable
TOE	AST:SW:Software:02
DESCRIPTION	Wiper binary hash 4f8e…c21a recovered from the ground ACA software host. Source: incident report KO-IR-2026-003.
ETEN	AN:IOC:Indicator of Compromise:00:Wiper binary hash recovered from the ground ACA software host.

L5 AN-IOA · INDICATOR OF ATTACK

Definition: “Verifiable indication that the platform has been targeted” (METEORSTORM:AN=IOA)

An Indicator of Attack is present-tense evidence that adversary activity is in progress: a reconnaissance pattern against a public interface, a credential-spraying sequence against an authentication service, an anomalous command pattern arriving at a control plane. Where AN-IOC establishes that a breach has occurred, AN-IOA establishes that the attempt is live. The compromise may or may not have completed; the response window is open.

The framework keeps the past and the present as separate analytic elements so the analyst answers two questions independently: did something already happen, and is something happening right now. Two questions, two elements, two decision paths.

AN-IOA ETEN PROCESS

STEP 01 **Enumerate the LAYER.** AN (fixed).

STEP 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.

STEP 03 **Set the TAG to IOA.** AN:IOA.

STEP 04 **Assign an ORDINAL.** Two digits from 00, one per distinct indicator.

STEP 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.

STEP 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.

EXAMPLE, FIELD BY FIELD

FIELD	VALUE
LAYER	AN
TAG	IOA
LABEL	Indicator of Attack
ORDINAL	00
SOURCE	observable
TOE	SVC:CP:Control Plane:09
DESCRIPTION	Credential-spraying sequence against the ground ACA authentication interface, sustained at one attempt per 30 seconds across 40 accounts, ongoing in live SOC telemetry. Source: SOC alert KO-AL-2026-117.

ETEN	**AN:IOA:Indicator of Attack:00:Credential-spraying sequence in progress against the ground ACA authentication interface.**