FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE WORKBOOK · STUDENT EDITION

Module 04 Incident Response Preparation

The method behind the Day-4 detection signatures, and every rule it produced, complete and anchored, with the response playbook that runs when it fires.

COPYRIGHT AND LEGAL NOTICES

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 04 Incident Response Preparation, module workbook, student edition
EDITION	Student edition · revised 2026-09-24
CONTACT	www.d2teamcorp.org

STUDENT EDITION

The teaching chapters and the complete worked deliverable. Your instructor holds the instructor edition, which adds the session plan and the marking guidance.

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

PART I

Orientation

What the day produces, and what each department brings to the table before any of it can be written.

CH 1 THE DAY IN ONE PAGE

Three days in, the platform has a shared decomposition, an anchored threat catalogue, and four attack paths, each with a data or signal source named at every waypoint and marked Available, Partial or Gap. Today the Security Operations Center opens its own working reality, and every one of those paths gets something that fires: a detection signature, and the playbook that runs when it does.

IN THE CLASSROOM

This module runs as slides, then a classroom of three parts. Have this workbook, the question set and the day's meeting minutes open. The classroom does this, in this order:

THE WORKBOOK	Chapter 3, The RACI, and Chapter 4, The Playbooks. Take Playbook 04. For two of its actions write who decides, who executes, and the authority level, solo, collaborative or escalated, with the reason that sets it: whether the action can be undone.
THE QUESTION SET	Questions 1, 5 and 10 are worked and marked in the classroom, each answer given with its reason. The rest are yours.
LESSONS LEARNED FROM THE MINUTES	Open the Day 4 minutes at the decision register and read Item 01, Choosing a rule format the organization can live with; Item 03, Signature 01, and the argument about baselining people; Item 05, Signature 03, written against a source that does not exist yet. The rule, the objection and the decision are taken from the record, not from the slide.

The chain, four days in. One number carries a chain across the week, and Day 4 is where it pays off. Element `AST:SW:Software:04`, the operator console software, was enumerated on Day 1. `AN:THR:Threat:01` named it as its TOE on Day 2. `AN:ATT:Attack Path:01` anchored to that same element on Day 3 and traced a route to it. Today `AN:DET:Detection Signature:01` takes it as its `TDM`, and **PB-01** says what happens when the watch fires. Four tags, one element, one number. Any of the three departments can follow that chain in either direction without a lookup table.

The TDM is not chosen. It is inherited. The `TDM` on an AN-DET holds exactly one enumerated platform element, and it is the same element the AN-THR this signature covers named as its TOE, carried across unchanged. There is no list, no “full TDM”, and no “primary” target with extras behind it. A signature reads more than one stream in practice, and those corroborating streams are named in the description, because they are description and not target. If you find yourself picking a fresh element, either the signature covers a different threat than you think, or the threat was anchored wrong, and that is a Day 2 defect to raise.

What you build. Four AN-DET elements, each a complete RootA rule: 2 Ground, 1 Link, 1 Space, each holding one TDM element, carrying forward the source state Function 03 assigned, and each bound to the response playbook it authorizes. Where the source is Available, the signature ships

and fires. Where it is a Gap, the signature and the playbook are still written and the gap is recorded as an enumerable product with the collection that would close it. Chapter 4 prints the whole deliverable.

What a playbook is. Not a description of what a competent team would do. It is the list of actions the organization has *already approved*, each with a named executor and a named decider. One **trigger**, the entry condition, then approved actions across four stages: **assess**, **contain**, **recover**, **report**. An action that is not on the list is not available, and adding one is a decision taken deliberately, in daylight, rather than at three in the morning.

The clocks. A playbook is not finished when the threat is contained; it is finished when the report is filed. The NIS2 Directive sets an early warning within 24 hours of becoming aware of a significant incident, a fuller notification within 72 hours, and a final report within one month. Every report action in chapter 4 names the clock it starts and who starts it, because an on-call analyst at 02:00 should not have to look it up.

What tomorrow consumes. Day 5, Adversary Management, reads the whole accumulated set and asks which platform elements keep recurring across threats, paths, and detections, then builds the resilience measures that shrink or harden them.

CH 2 WHAT THE SOC BRINGS TO THE TABLE

> "Six artifacts on the table. Security Operations runs the detections and acts on the alerts, and today the center lays its working reality on the table."
>
> DEEP DIVE DECK, SLIDE 4 · DAY-4 SECURITY OPERATIONS CENTER WORKING SESSION

ARTIFACT	WHAT IT HOLDS	WHAT IT CONSTRAINS
01 Telemetry sources	What data streams the SOC actually has visibility into: auth logs, network flow, endpoint detection and response (EDR) telemetry, tracking RF metrics, attestation.	Whether a hook can be watched at all.
02 RootA templates	The vendor-neutral detection format. One rule deploys to Splunk, Elastic, or Microsoft Sentinel without rewrite.	The form every signature must take.
03 Playbook library	The IR playbooks Security Operations already runs, written against a class of incident rather than one rule.	Which actions the organization has already approved, and which it has not.
04 Alert queue	Current alert volume and triage practice.	The false-positive budget a new rule may spend.
05 On-call context	What an on-call analyst can actually do in real time during a contact window.	Which contain actions are realistic at 02:00, and which need a co-signer.
06 Known gaps	Telemetry blind spots already documented.	Which signatures cannot ship until engineering closes a gap.

WHAT A LIBRARY PLAYBOOK LOOKS LIKE, AND HOW A SIGNATURE HOOKS INTO IT

The slide names the playbook library and moves on, which leaves the most important question unanswered: what is already in there, and what does hooking into it actually mean? A library playbook is generic by design. It is written against a class of incident, not against one rule, and it looks like this:

LIB-GROUND-CRED · Suspected credential misuse on a ground service (existing library entry)

Trigger: any alert indicating credential use inconsistent with the owning operator's pattern on a ground service.
assess: check the filed travel, the shift roster and the change record for the operator.
contain: suspend the credential at the authorizing service, and fail the function over to the alternate site if the service is single-homed.
recover: rotate the credential, replay the affected audit log against the authorized plan of record, confirm end state.
report: duty officer and CISO; assess reportability and start the regulatory clock if the incident is significant.

No element resolved, no executor named, no decider named, no authority level set. That is what generic means, and it is exactly the four things a signature supplies.

Hooking a signature into it means four concrete edits, not a filing action. First, the signature identifier is named in the trigger, with the confidence at which the playbook runs and why that threshold and not a higher one, so the generic trigger becomes specific. Second, every "authorizing service" and "alternate site" is replaced by an exact enumerated element, so the on-call analyst does not have to work out which service is meant. Third, the report action names the concrete clock and who starts it, rather than "assess reportability". Fourth, and this is the edit teams skip, every action gets its authorization: one Responsible executor, Mission Lead as the Accountable decider, and an authority level read off how reversible the action is.

One of those edits splits an action in two. The library's contain line contains two different acts. Suspending a credential changes information-system state, which makes it a cyber response Security Operations executes. Failing commanding over to the second ground site changes which site holds live commanding authority, which is mission operational state, so it is a space response Satellite Operations executes, even though it is taken on a ground element. One sentence, two domains, two executors, and therefore two actions. PB-01 in chapter 4 is LIB-GROUND-CRED with those edits made, and its contain stage carries `ACT:01` and `ACT:02` where the library carried one line. Prose hides that split; the action list cannot. That is why writing a playbook per signature is a day's work rather than a month's, and why the day is worth spending: most of the procedure already exists, and detection engineering makes it precise enough to run.

PART II

The method and the catalogue

The process for producing one entry correctly, then the complete catalogue this day produced, entry by entry.

CH 3 THE AN-DET METHOD, AND ROOTA

> "Six steps, fixed order. Every signature is a complete RootA rule, and its TDM is the one element its threat already named."
>
> DEEP DIVE DECK, SLIDES 7 AND 8 · AN-DET ENUMERATION PROCESS · ROOTA, OPEN DETECTION LANGUAGE

Inputs. Yesterday's attack-path catalogue and its data and signal source inventory, plus a working session with Security Operations, building the detect-report-recover capability Executive Order 14144 requires inside the NIS2 reporting deadlines.

Output. One `AN-DET` element per attack path, written as a complete RootA rule. The response playbook is the module's **second deliverable**, written alongside the signature rather than as a field on it.

The Gate. "Pattern, signal, or logic that triggers on contextualized threat behavior, expressed as a complete RootA rule." Two ways to fail it. **Not a complete rule**: a bare SPL, KQL, EQL or Sigma query with no RootA wrapper and no METEORSTORM anchor block. It cannot travel, so it cannot be shared, reviewed, or ported when the tooling changes. **Not anchored to one element**: a `TDM` that is empty, or that holds a list. If the field holds two elements it cannot say which one the signature is about, and Day 5 reads that field to decide what to harden.

THE SIX STEPS, FIXED ORDER

1. **Enumerate the LAYER.** LAYER = `AN`, fixed. A signature is the Security Operations Center's own instrument, not a part of the platform.
2. **Verify the format.** The signature must be a complete RootA rule, SOC Prime RootA specification v1.0.0, carrying the METEORSTORM anchor block. The native query you already know rides inside `detection.body`; RootA is the wrapper around it, not a replacement for it. SOURCE is `observable` or `synthetic`, and those are the only two values it takes. A citation is evidence, not a SOURCE value.
3. **Set the TAG to DET.** A Detection-Signature element within the Analytic Layer.
4. **Assign an ORDINAL.** Two digits from 00, taken from the path the signature covers. Today's four are 00, 01, 02, 03. Ordinals come from the running register that also tracks work outside today's scope, so a scoped set is legitimately non-consecutive, and an ordinal issued once is never renumbered.
5. **Enumerate the TDM.** Target of Detection Method: **one** enumerated platform element, the element this signature observes, and it is the same element the `AN-THR` it covers named as its TOE. TDM, not TOE: the element scanned, not the element exploited. Any structural layer may be named, environment included; the old restriction to services and assets is retired.
6. **Write the DESCRIPTION.** The complete RootA rule, every required field plus the anchor block, the AN-IOC, AN-IOA, AN-ATT or AN-THR entries it covers, and the source citation. The covered entries ride in `references`, so coverage is reviewable from the rule itself rather than from a side table.

Repeat for the next signature. When every catalogued attack path has a detection enumerated, whether it can fire yet or not, the AN-DET coverage matrix is current.

> **TDM is not TOE, but it holds the same element.** The two names answer different questions about one element. TOE, Target of Exploitation, says the adversary acts here; it belongs to threats and paths. TDM, Target of Detection Method, says the signature watches here. On a worked chain they are the same element seen twice, which is the whole point: threat, path, signature and measure all name `AST:SW:Software:04` on chain 01, so nobody has to negotiate what the signature is for. What differs is the verb, not the element.

THE SECOND DELIVERABLE: THE RESPONSE PLAYBOOK

The six steps produce the element. They do not produce the playbook, and that is deliberate: a playbook is not a field on the ETEN, it is the module's other output, the way the source inventory was Module 03's. It ships beside its rule, same directory, same stem, `.playbook.yml`, and the rule binds to it through `meteorstorm.playbook`. A signature with no playbook field, or with one that does not resolve to a file beside it, is not accepted into the analytic layer.

Why this is enforced rather than encouraged. On a converged space platform the cost of an unrehearsed response is not symmetric. Revoking a ground credential is reversible in minutes. Placing a spacecraft in safe mode costs mission time and cannot be undone by deciding differently later. Switching bands touches spectrum coordination and a regulatory filing. An organization that

has not decided in advance which of those an analyst may reach for will decide it under pressure, badly, and will discover afterwards that nobody held the authority they assumed they had. So the playbook is a list of already-approved actions with a named executor and a named decider, not a description of what a competent team would do.

One trigger, four stages

A playbook carries **one trigger** and approved actions in four stages. The trigger is the entry condition, not an action: it names the signature, the element it watches, the confidence at which the playbook runs, and why that threshold and not a higher one. A playbook that runs on every low-confidence hit will be ignored by the third week.

STAGE	ANSWERS	WHY IT IS HERE, ON THIS PLATFORM
assess	Is this real, and is it aimed at us?	The stage teams skip. Acting on an unverified signal is expensive on a space platform, and some effects, interference and atmospheric loss among them, look identical to an attack until a second source is consulted.
contain	What stops it getting worse?	Where the cyber and space split is sharpest, and where the authority level does most of its work.
recover	What restores a known-good state?	Frequently spans both domains, so frequently splits into paired actions.
report	Who is told, on what clock?	Not optional. **This is the leg teams drop, and it is the one the regulator reads.** Under the NIS2 Directive: an early warning within 24 hours of becoming aware of a significant incident, a fuller notification within 72 hours, a final report within one month. The 24-hour clock starts on awareness, not on resolution, which is why the report action is written before the incident rather than during it.

A playbook is not finished when the threat is contained; it is finished when the report is filed. A signature with no playbook is not shippable, and neither is a playbook with no signature. Detection without a response is an alert nobody owns.

Who executes, and who decides

The roles and the authority levels are Module 7's, inherited here without change, under the rule Module 7 states: **every commanded action maps to one role at one level.**

ROLE	HOLDS	NEVER
Mission Lead	The objective, the escalation thresholds, and the go / no-go call. Accountable for every action in every playbook, without exception and without sharing.	Executes an action. The decider does not also do the work.
Security Operations	Responsible for cyber responses: identity, access, network, host, credential, signature, log, pipeline.	Executes an action that changes mission operational state.
Satellite Operations	Responsible for space responses: commanding, vehicle state, link configuration, band selection, pass scheduling, safe mode, redundancy switching.	Executes an action that changes information-system state only.

The separation is the point. One role decides, another executes. A single person holding both is the failure mode this structure exists to prevent, which is why Mission Lead is Accountable on every action and Responsible on none. Accountable means owning the outcome, not standing over the console: on a `solo` action the Mission Lead is Accountable and Informed, not present. Module 7's third mission-simulation role, Payload Operations, takes no part in a Function 04 playbook.

LETTER	MEANS	HOW MANY
R, Responsible	Executes the action.	Exactly one, never Mission Lead.
A, Accountable	Owns the decision and the outcome.	Exactly one, always Mission Lead.
C, Consulted	Two-way, before the action is taken. On a `collaborative` action this is the co-signer.	Zero or more.
I, Informed	One-way, after the action is taken.	Zero or more.

An action needing two executors is two actions. Not one action with two Responsible roles. That is Module 7's rule, one role at one level, and splitting is what makes the sequence auditable and what stops each department assuming the other did it. It is the most common defect in an inherited playbook, because prose hides it and an action list cannot.

The effect test sets the domain

Ask what the action **changes**, not where it is taken and not what verb it uses.

THE ACTION CHANGES	DOMAIN	RESPONSIBLE
Information-system state: an identity, a credential, an access path, a host, a network route, a pipeline, a rule	`cyber`	Security Operations
Mission operational state: what the vehicle does, what the link carries, what is commanded, when a contact window opens, which side of a redundant pair is live	`space`	Satellite Operations

The element records where, not what. The segment an element sits in is a useful expectation, not the answer. The ground segment carries both kinds: a credential on the ground command-acceptance service is information-system state, while failing commanding over to the second ground site is mission operational state, and both are taken on ground elements. Reading the domain off the segment gets the second one wrong. Where an action departs from its element's expectation it carries a one-line `why` naming the mission effect that makes it a space response. That is the only conditional field in the record, and it exists because the ambiguity is real and belongs on the page rather than in someone's head.

The reversibility ladder sets the level

Each action declares what undoing it costs. That class, and nothing else, determines its authority level. **The level is derived, never chosen.**

REVERSIBILITY	MEANS	LEVEL	AT EXECUTION TIME
`reversible`	Undone without mission impact.	`solo`	The Responsible role acts alone. Mission Lead is Accountable and Informed.
`disruptive`	Costs mission time, capability or availability, and is recoverable.	`collaborative`	The other operating role co-signs before execution, as the Consulted party.
`irreversible`	Cannot be undone by deciding differently: safe mode, a filed regulatory change, destroyed volatile evidence.	`escalated`	Mission Lead approves before execution, and the approval and its justification are written down before, not after.

Solo does not mean unaccountable. It means the decision was made in advance, when there was time to think, and recorded in this playbook. And if an action feels over-gated, the reversibility class is wrong: that is the conversation to have, not a quiet downgrade of the level.

One action record

FIELD	HOLDS
`id`	`ACT:00`. Two digits from 00, counted within the playbook, consecutive, issued once, never renumbered. The `ACT` sub-ordinal bears no relation to the signature's ordinal.
`stage`	`assess`, `contain`, `recover`, or `report`.
`domain`	`cyber` or `space`, set by the effect test.
`action`	The approved action as an imperative a duty officer can execute without interpretation. "Revoke the pushing identity's command-release authority", not "authority should be reviewed".
`element`	One enumerated platform element the action is taken on. Never a category, never a system name that is not an ETEN.
`why`	Required only where `domain` departs from the element's expectation. One line naming the mission effect.
`reversibility`	`reversible`, `disruptive`, or `irreversible`.
`level`	`solo`, `collaborative`, or `escalated`. Read off the ladder, never chosen.
`raci`	`r`, `a`, `c`, `i` per the cardinality rules above.

> **The field is `element`, never `on`.** In YAML 1.1 the bare key `on` parses as the boolean true, so a playbook written with `on:` silently loses every element and validates as if no action named anything. This is not a style preference; it is a defect that hides itself.

The minimum. A playbook is not complete, and its signature does not ship, until all of these hold. (1) At least one approved action in **each** of the four stages. (2) Every action carries a complete record, plus `why` wherever the domain departs from the element's expectation. (3) Exactly one Accountable per action, and it is Mission Lead. (4) Exactly one Responsible per action, and it is never Mission Lead. (5) The Responsible role matches the domain. (6) `level` matches `reversibility` by the ladder. (7) Every `collaborative` action names its co-signer in `c`. (8) At least one action names the signature's TDM. (9) At least one report action names a regulatory clock and who starts it. A playbook that cannot meet the minimum is a finding, recorded as such. It is never met by writing a vaguer action.

WHAT FUNCTION 03 HANDS OVER, AND WHAT YOU DO WITH EACH STATE

Every waypoint in yesterday's inventory carries one named source with one of three states. The state is not a grade on the analyst; it is a statement about the platform, and each one has a different instruction attached.

STATE	WHAT IT MEANS	WHAT YOU DO TODAY
Available	The stream exists, is onboarded, and carries a source identifier.	Author now, against the named source identifier. Put that identifier in `logsource`.
Partial	The stream exists but its fidelity is limited, or it depends on something outside collection such as a workflow people may not follow.	Author what the fidelity supports, and record in `details` exactly what the rule cannot see. Do not round Partial up to Available.
Gap	The stream does not exist. Nothing can be authored against it today.	Record the DETECTION GAP as an enumerable product: enumerate the AN-DET anyway, name the collection that would close the gap, give it an owner, and write the playbook so the response exists the day the collection lands.

> **The detection-gap rule.** A threat or attack path with no matching signature is a detection gap, and the gap is itself an enumerable analytic product. It is never a silent omission and never rounded up to coverage. One of today's four sits here: Signature 03 cannot fire, because Kestrel does not fly measured boot. It is enumerated anyway, the missing collection is named in the rule's own `logsource.audit.enable` field, Satellite Design and Engineering owns it, and PB-03 is written in full. When Day 5 proposes measured boot, the justification is already enumerated instead of argued from scratch.

ROOTA, IN MORE DETAIL

RootA is an open public-domain detection-engineering language created by the SOC Prime team and released in 2023. It is a YAML wrapper that carries a native SIEM, EDR, extended detection and response (XDR), or data lake query plus the metadata a defensive cyber operator needs to share that query: MITRE ATT&CK mapping, log-source declaration, references, threat-actor and campaign timeline, and tags. The companion tool Uncoder.IO converts a RootA rule into 65 query dialects across 45 technologies, including Splunk, Elastic, Microsoft Sentinel, Google Chronicle, CrowdStrike, QRadar, and Sumo Logic.

Two consequences matter for this course. A SIEM migration becomes a translation pass over the detection portfolio rather than a rewrite of every rule from scratch. And a rule you write today is a rule a peer operator, such as a fellow Space ISAC member, can pull tomorrow and run on different tooling with no rewrite, which is what makes the sharing mandate practical rather than aspirational.

WHY THE MANDATES ARE TIGHTENING

Updated CNSS policy for national security space systems (CNSSP No. 12 and CNSSI 1200, August 2025) now requires real-time on-board intrusion detection and prevention, and patch management for on-board and ground-segment software, written into procurement contracts. As Aerospace Corporation's Brandon Bailey put it at CyberSat 2025: "if you build services or capabilities that support national security missions, [these requirements] apply to you." A detection

portfolio anchored to enumerated elements is how an operator demonstrates that requirement is met rather than asserted. (Source: Air and Space Forces Magazine, 19 November 2025.)

CH 4 THE CATALOGUE, COMPLETE

> "One signature per path, one playbook per signature, one element per signature, and one executor and one decider per action."
>
> DEEP DIVE DECK, SLIDE 15 · SIGNATURES AND PLAYBOOKS · DAY-4 ENUMERATED SIGNATURES AND PLAYBOOKS

How to read each entry. The first row of every table is the **TDM anchor**: the one enumerated element the signature observes, inherited from the threat the signature covers. Everything below it is description. Covers links the signature to the AN-ATT it serves. Source state is what Function 03 assigned to the stream behind it, **Available**, **Partial** or **Gap**. Corroborating streams lists the other places the analyst looks on a hit; they are printed here so the difference between the anchor and the streams is visible, which the deck cannot show at a glance. Each signature is followed by the playbook it authorizes: one trigger, then the approved actions as a RACI table, one row per action, with the element it is taken on, its reversibility class and the level that class produces. Read the level column as a claim about cost, not about seniority. The full rule files and their playbooks live in `module4/rules/`, side by side with the same stem; the worked rule is printed in full below.

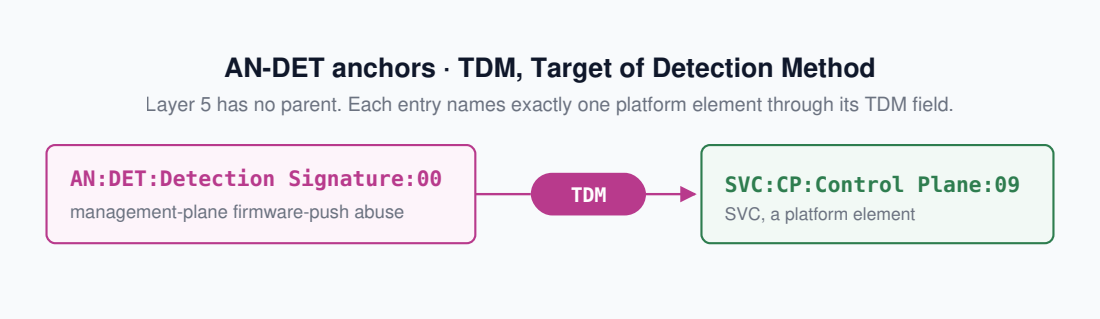
GROUND · 2 AN-DET + 2 playbooks

AN:DET:Detection Signature:00 · Management-plane abuse

Detects firmware-push operations from the modem management interface outside maintenance windows, or following a VPN-appliance authentication anomaly.

FIELD	VALUE
TDM (anchor)	`SVC:CP:Control Plane:09`
What that element is	The ground command-acceptance service. The one element this signature observes, taken unchanged from the TOE of `AN:THR:Threat:00`. Day 3 anchored its path here; Day 5 hardens it.
Covers	`AN:ATT:Attack Path:00 (KA-SAT class)`
Format	Complete RootA rule (`an-det-00-mgmt-plane-abuse.yml`), severity critical
Source state	**Available, src-ground-aca-010**
Corroborating streams	Patch binary store hash audit (`AST:DA:Data:02`) and patch pipeline execution log (`AST:SW:Software:03`). Pulled on a hit, named in the rule's `details`, not in the TDM.
Source	CISA / FBI AA22-076 and the Viasat post-incident report (30 March 2022), with SentinelLabs' AcidRain analysis as supporting

AN-DET ANCHORS · 1 OF 4 ENTRIES · AFTER AN:DET:DETECTION SIGNATURE:00



One signature, one anchor. The detection sits in Layer 5 and names one platform element through its `TDM` field, exactly as its threat and its path did through `TOE`. The streams it reads for corroboration are in the entry table above, not in this figure, because streams are description and the anchor is the target.

Why this looks like yesterday's figure. It is yesterday's figure with a different tag. That is the chain working: `AN:DET:Detection Signature:00` names the element `AN:THR:Threat:00` named, so the box on the right has not moved since Day 2.

PB-00 · Management-plane firmware-push abuse

Trigger. AN:DET:Detection Signature:00 fires on an out-of-window firmware push at SVC:CP:Control Plane:09, at any confidence. The threshold is any confidence and not higher because the blast radius is the whole modem fleet.

APPROVED ACTION	R EXECUTES	A DECIDES	C CONSULTED	I INFORMED
ACT:00 ASSESS · CYBER Check the change record for a documented emergency change reference or an authorized red-team exercise covering this push window, the two benign causes the rule names. SVC:CP:Control Plane:09 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:01 CONTAIN · CYBER Revoke the pushing identity's command-release authority on the ground command-acceptance service. SVC:CP:Control Plane:09 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:02 CONTAIN · CYBER Halt the patch deployment pipeline carrying the image. AST:SW:Software:03 DISRUPTIVE → COLLABORATIVE	Security Operations	Mission Lead	Satellite Operations	none
ACT:03 RECOVER · CYBER Inventory which terminals received the push and compare each deployed firmware hash against the signed expected value. AST:SW:Software:03 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:04 RECOVER · SPACE Sequence the rollback of affected terminals against the maintenance window, confirming operational impact before each batch. AST:SW:Software:03 *Why space: Changes what the terminal fleet is running and when, a mission operational state change taken on a ground element.* DISRUPTIVE → COLLABORATIVE	Satellite Operations	Mission Lead	Security Operations	none
ACT:05 REPORT · CYBER Notify the duty officer and the CISO immediately, and start the NIS2 clocks on awareness, 24-hour early warning, 72-hour notification, one-month final report. A fleet-wide firmware event is significant on its face, so significance is pre-determined here and does not wait on a call. SVC:CP:Control Plane:09 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:06 REPORT · CYBER File the redacted Space ISAC Exchange entry. SVC:CP:Control Plane:09 IRREVERSIBLE → ESCALATED	Security Operations	Mission Lead	Satellite Operations	none

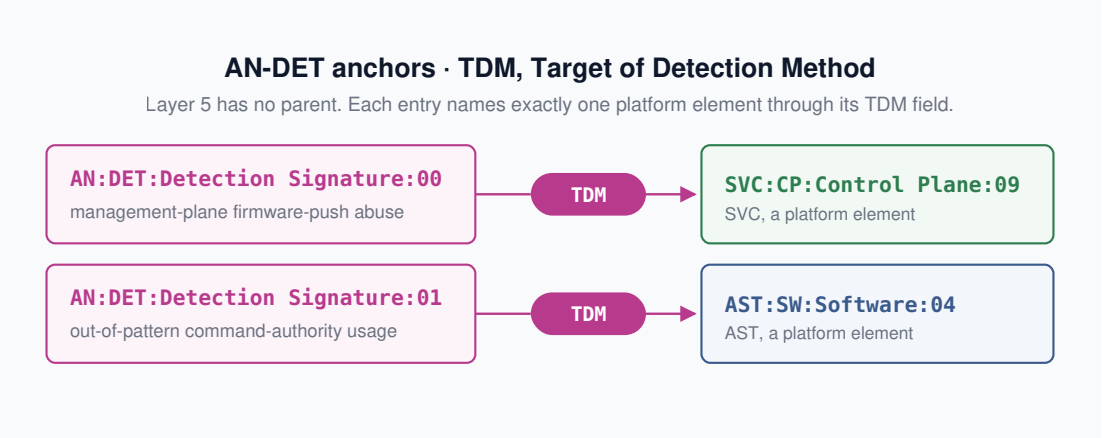
Accountable is Mission Lead on every action and Responsible on none. Cyber responses are Security Operations's, space responses are Satellite Operations's, and every level is read off the reversibility class rather than chosen.

AN:DET:Detection Signature:01 · Out-of-pattern command-authority usage

Detects commanding workstation usage outside the operator's normal hours, commands issued without peer-review tags, or sequences inconsistent with the active mission profile.

FIELD	VALUE
TDM (anchor)	`AST:SW:Software:04`
What that element is	The operator console software, the ground command-and-control suite. The one element this signature observes, taken unchanged from the TOE of `AN:THR:Threat:01`.
Covers	`AN:ATT:Attack Path:01`
Format	Complete RootA rule (`an-det-01-out-of-pattern-command.yml`), severity high
Source state	**Partial: the peer-review tag stream depends on workflow adoption, so a command from a team that has not adopted the tag is indistinguishable from one that skipped review. Recorded in the rule's `details`.**
Corroborating streams	Operator console workstation usage stream (`AST:HW:Hardware:04`) and satellite console command audit (`SVC:CP:Control Plane:13`). Pulled on a hit, not the anchor.
Source	MITRE ATT&CK T1078.003; NIST SP 800-53 PS-7

AN-DET ANCHORS · 2 OF 4 ENTRIES · AFTER AN:DET:DETECTION SIGNATURE:01



The second signature anchors to an asset, so it draws in the asset colour. Two signatures, two structural layers, and in both cases the anchor was inherited rather than chosen.

The tempting error. This rule reads the console workstation usage stream and the console command audit, so a first draft naturally lists all three elements. That draft is wrong. A field holding three elements cannot say which one the signature is about, and Day 5 reads that field to decide what to harden. One element in the field, the other two in the description.

PB-01 · Out-of-pattern command-authority usage

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.

APPROVED ACTION	R EXECUTES	A DECIDES	C CONSULTED	I INFORMED
ACT:00 ASSESS · CYBER Check the filed travel, the shift roster and the change record for this operator, the benign causes the rule names. AST:SW:Software:04 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:01 CONTAIN · CYBER Suspend the operator credential on the ground command-acceptance service. SVC:CP:Control Plane:09 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:02 CONTAIN · SPACE Fail commanding over to the second ground site. SVC:HY:Hybrid:03 *Why space: Changes which site holds live commanding authority, a mission operational state change taken on a ground element.* DISRUPTIVE → COLLABORATIVE	Satellite Operations	Mission Lead	Security Operations	none
ACT:03 RECOVER · CYBER Rotate the ground command-acceptance service credentials. SVC:CP:Control Plane:09 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:04 RECOVER · SPACE Replay the command log against the flight plan and confirm the vehicle state matches the last authorized command. SVC:CP:Control Plane:13 *Why space: Confirms vehicle state against the flight plan, a mission operational judgment taken on a ground element.* REVERSIBLE → SOLO	Satellite Operations	Mission Lead	none	Security Operations
ACT:05 REPORT · CYBER Notify the duty officer and the CISO, and start the NIS2 clocks, 24-hour early warning, 72-hour notification, one-month final report. AST:SW:Software:04 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:06 REPORT · CYBER File the redacted Space ISAC Exchange entry. AST:SW:Software:04 IRREVERSIBLE → ESCALATED	Security Operations	Mission Lead	Satellite Operations	none

Accountable is Mission Lead on every action and Responsible on none. Cyber responses are Security Operations's, space responses are Satellite Operations's, and every level is read off the reversibility class rather than chosen.

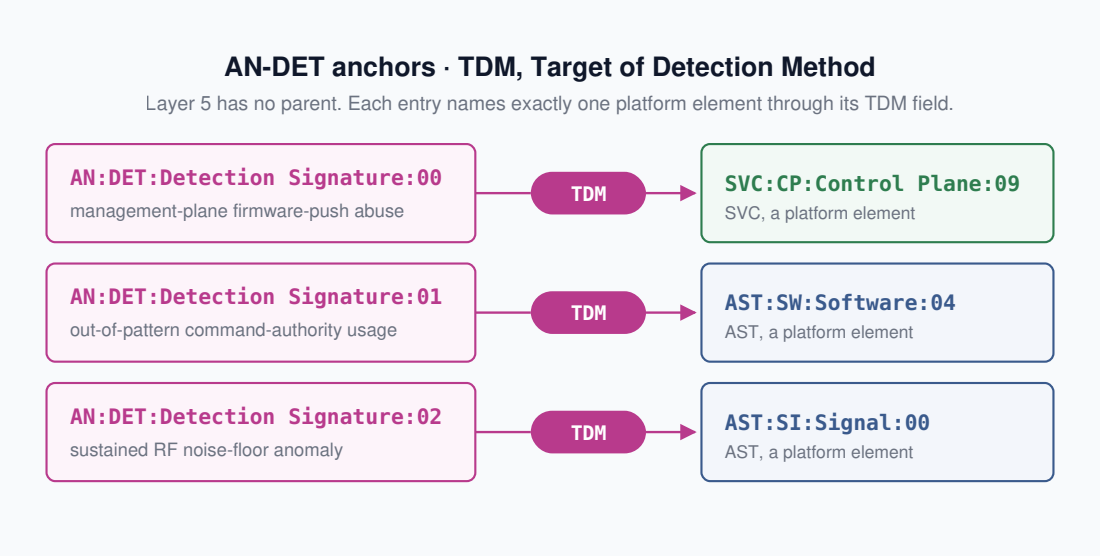
LINK · 1 AN-DET + 1 playbook

AN:DET:Detection Signature:02 · Sustained RF noise-floor anomaly

Detects elevated noise across the uplink or downlink bands beyond expected environmental thresholds, sustained for longer than incidental atmospheric events.

FIELD	VALUE
TDM (anchor)	`AST:SI:Signal:00`
What that element is	The uplink and downlink waveforms. The one element this signature observes, taken unchanged from the TOE of `AN:THR:Threat:02`.
Covers	`AN:ATT:Attack Path:02`
Format	Complete RootA rule (`an-det-02-rf-noise-floor-anomaly.yml`), severity high
Source state	**Available, src-rx-rf-024, per-band SNR and BER telemetry already streaming**
Corroborating streams	Tracking and telemetry noise-floor stream (`SVC:HY:Hybrid:02`, src-tnt-noise-025) and the link access-control authority failure-rate stream (`SVC:CP:Control Plane:05`, src-link-aca-026).
Source	ITU interference-reporting guidance; SPARTA SPACE-T1429

AN-DET ANCHORS · 3 OF 4 ENTRIES · AFTER AN:DET:DETECTION SIGNATURE:02



The link signature joins. Its anchor is the waveform itself, which on Day 3 was also where the route landed. That coincidence is common on RF paths and is not a rule.

Any structural layer is a legal anchor. Nothing stops a TDM naming a segment or an environment where that is where the source resolves. The earlier restriction to services and assets is retired. What the rule does require is that the layer be the lowest one the source actually resolves to: here the noise is measured on the waveform, so the waveform is the anchor rather than the link segment above it.

PB-02 · Sustained RF noise-floor anomaly

Trigger. AN:DET:Detection Signature:02 fires on a noise-floor anomaly at AST:SI:Signal:00 beyond the environmental threshold, at medium confidence or higher. The threshold is medium and not any, because atmospheric loss and local interference produce the same reading and the assess stage separates them.

APPROVED ACTION	R EXECUTES	A DECIDES	C CONSULTED	I INFORMED
ACT:00 ASSESS · SPACE Confirm through a secondary ground station that the elevated noise on the waveform is platform-targeted rather than local. AST:SI:Signal:00 REVERSIBLE → SOLO	Satellite Operations	Mission Lead	none	Security Operations
ACT:01 CONTAIN · SPACE Switch the link to the backup band or to spread-spectrum mode. AST:SI:Signal:00 DISRUPTIVE → COLLABORATIVE	Satellite Operations	Mission Lead	Security Operations	none
ACT:02 RECOVER · SPACE File the geolocation request with the interference-mitigation team. AST:SI:Signal:00 REVERSIBLE → SOLO	Satellite Operations	Mission Lead	none	Security Operations
ACT:03 RECOVER · SPACE Adjust pass scheduling around the affected windows while the interference persists, and confirm link margin returns to baseline. SVC:HY:Hybrid:02 DISRUPTIVE → COLLABORATIVE	Satellite Operations	Mission Lead	Security Operations	none
ACT:04 REPORT · SPACE File the ITU interference report through the regulatory liaison. AST:SI:Signal:00 IRREVERSIBLE → ESCALATED	Satellite Operations	Mission Lead	Security Operations	none
ACT:05 REPORT · CYBER Notify the duty officer and the CISO and start the NIS2 24-hour early warning, which runs on a sustained denial of the command link even when no data is lost, with the 72-hour notification and one-month final report behind it. AST:SI:Signal:00 *Why cyber: Reporting is an information act carried out by Security Operations; the element names what the report concerns, not where the action lands.* REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations

Accountable is Mission Lead on every action and Responsible on none. Cyber responses are Security Operations's, space responses are Satellite Operations's, and every level is read off the reversibility class rather than chosen.

FIELD NOTE PB-02 is the shape a link-layer incident takes: every action is a space response except the reporting one, because nothing in a log sees jamming. Note the assess action in particular. It is the whole reason the assess stage exists on this platform: elevated noise on the waveform looks identical whether it is a solar scintillation event, local interference, or somebody aiming at you, and the only way to tell is a second ground station. A playbook that opened with the band switch would burn mission time on the weather.

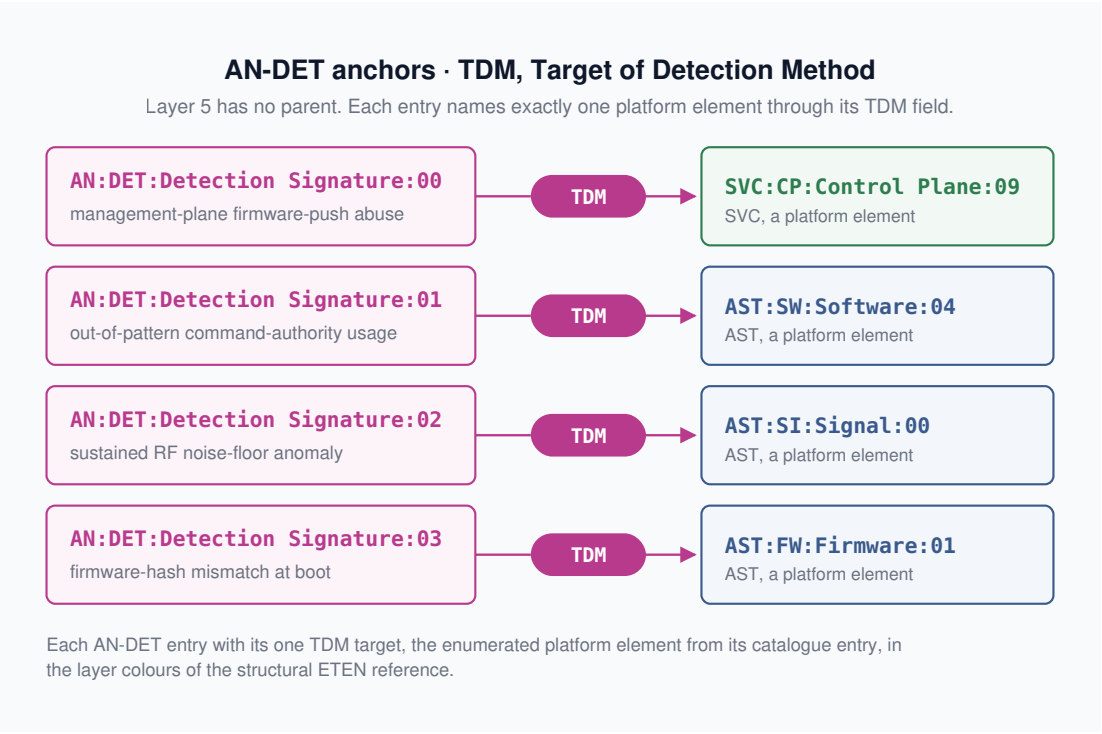
SPACE · 1 AN-DET + 1 playbook

AN:DET:Detection Signature:03 · Firmware-hash mismatch at boot

Detects firmware images whose measured hash does not match the signed expected value at boot or after an update.

FIELD	VALUE
TDM (anchor)	**AST:FW:Firmware:01**
What that element is	The on-board computer boot firmware, the root of trust that runs first at power-on. The one element this signature observes, taken unchanged from the TOE of AN:THR:Threat:03.
Covers	**AN:ATT:Attack Path:03**
Format	Complete RootA rule (an-det-03-firmware-hash-mismatch.yml), severity critical
Source state	**Gap. Kestrel does not fly measured boot, so the stream this rule reads does not exist. Collection that would close it: on-board measured boot with hardware-rooted attestation reported over the telemetry path. Owner: Satellite Design and Engineering. Named in the rule at logsource.audit.enable.**
Corroborating streams	Vendor signed-manifest and provenance attestation checked at acceptance (SVC:CP:Control Plane:02, src-obc-supply-040) and the repeater firmware attestation record (AST:FW:Firmware:02, src-pl-supply-041).
Source	NIST SP 800-193; SPARTA SPACE-T1041; SolarWinds (2020) post-incident retrospectives

AN-DET ANCHORS · 4 OF 4 ENTRIES · THE COMPLETE DAY-4 DETECTION ANCHOR MAP



Four signatures, four anchors, and the same four elements Day 2 produced and Day 3 kept. This figure and the Module 02 and Module 03 figures are identical on the right-hand side, which is what a working chain looks like three days in.

A gap still draws. Signature 03 appears on this map even though it cannot fire, because the entry exists and the anchor is real. That is the visible form of the detection-gap rule: an empty row would let the platform look better covered than it is.

PB-03 · Firmware-hash mismatch at boot

> **Status: gap-blocked.** Measured boot is not flown, so the signature cannot fire. Owner: Satellite Design and Engineering. The playbook ships anyway, complete and held to every check, so the authorized response exists the day the source arrives rather than being written under pressure then. The status records why the signature is dormant; it waives nothing.

Trigger. AN:DET:Detection Signature:03 fires on a measured-hash mismatch at AST:FW:Firmware:01 at boot or after an update, at any confidence. The threshold is any confidence because an unauthorized image running on the on-board computer admits no benign cause. Dormant until measured boot ships.

APPROVED ACTION	R EXECUTES	A DECIDES	C CONSULTED	I INFORMED
ACT:00 ASSESS · SPACE Compare the measured hash against the signed expected value in the vendor manifest. AST:FW:Firmware:01 REVERSIBLE → SOLO	Satellite Operations	Mission Lead	none	Security Operations
ACT:01 CONTAIN · SPACE Hold the boot firmware in its current state and keep it out of an operational role. AST:FW:Firmware:01 DISRUPTIVE → COLLABORATIVE	Satellite Operations	Mission Lead	Security Operations	none
ACT:02 CONTAIN · SPACE Switch to the redundant on-board computer where one exists. AST:HW:Hardware:06 IRREVERSIBLE → ESCALATED	Satellite Operations	Mission Lead	Security Operations	none
ACT:03 RECOVER · CYBER Engage the flight-software build team on the source of the discrepancy and audit the patch deployment pipeline for the image's provenance. AST:SW:Software:03 REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:04 RECOVER · SPACE Re-establish a known-good image before the component resumes its role. AST:FW:Firmware:01 IRREVERSIBLE → ESCALATED	Satellite Operations	Mission Lead	Security Operations	none
ACT:05 REPORT · CYBER Notify the duty officer and the CISO. A confirmed unauthorized on-orbit image is a significant incident, so the NIS2 24-hour early warning starts on confirmation, with the 72-hour notification and one-month final report following. AST:FW:Firmware:01 *Why cyber: Reporting is an information act carried out by Security Operations; the element names what the report concerns, not where the action lands.* REVERSIBLE → SOLO	Security Operations	Mission Lead	none	Satellite Operations
ACT:06 REPORT · CYBER Engage the supply-chain lead upstream and file the redacted Space ISAC Exchange entry. AST:SW:Software:03 IRREVERSIBLE → ESCALATED	Security Operations	Mission Lead	Satellite Operations	none

Accountable is Mission Lead on every action and Responsible on none. Cyber responses are Security Operations's, space responses are Satellite Operations's, and every level is read off the reversibility class rather than chosen.

FIELD NOTE This playbook is written against a signature that cannot yet fire, because the platform does not fly measured boot. That is deliberate, and it is why the status field exists. The gap was declared on Day 3 with an owner; writing the playbook now means the day measured boot ships, the response already exists, and Day 5's resilience measure has a documented justification rather than an argument. Note also what a space-heavy playbook looks like: two of its seven actions are `escalated`, because switching to the redundant on-board computer and re-flashing a known-good image cannot be undone by deciding differently later. That is the ladder doing its job, not caution.

THE WORKED RULE IN FULL

The deck walks `an-det-01-out-of-pattern-command.yml` field by field on screen. Here it is complete, so the walkthrough survives off-screen. Every other AN-DET carries the same field set; only the values change. Field names, order and casing follow the SOC Prime RootA specification v1.0.0, and the `meteorstorm` block is appended last.

```
name: Out-of-pattern command authority usage on the operator console software
details: |
  Detects command-authority usage outside the per-operator behavioral baseline: off-hours
  commanding, high-impact commands issued with no peer-review tag, and command sequences
  inconsistent with the active mission profile. Corroborating streams the analyst should
pull
  on a hit, which are not the target of this rule: the operator console workstation usage
  stream and the satellite console command audit. Source state Partial: the peer-review tag
  stream depends on workflow adoption. Known benign causes: operator travel filed with
notice,
  and a documented emergency override carrying an incident ticket.
author: Kestrel Orbital SOC
severity: high
type: query
class: behavioral
date: 2026-08-04
mitre-attack:
    - t1078.003
detection:
    language: splunk-spl-query
    body: index=sat_command sourcetype=command_audit origin_device="operator-console"
command_class IN ("fts_arm","thruster_burn","ranging_off","encryption_disable") AND
(peer_review_tag=false OR date_hour<8 OR date_hour>17)
logsource:
    product: satellite_command_pipeline
    service: command_audit
    audit:
        source: Console operator software command audit
        enable: Enable per-command auditing on the console C2 application, including the
          peer-review tag and the issuing operator identity.
correlation:
    timeframe: 24h
    functions: count(command) by operator
references:
    - AN:ATT:Attack Path:01
    - AN:THR:Threat:01
    - https://attack.mitre.org/techniques/T1078/003/
    - https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
tags: KO-DET-CONSOLE-CMD-001, command-authority, operator-console
license: DRL 1.1
version: 1.0
uuid: 2b7c9d14-6f3a-4c58-9e21-7a0d5b3c8f46
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
```

Read the last block first. The `meteorstorm` block is what makes this an AN-DET rather than a saved query. `pce`, `seg`, `svc` and `ast` carry the parent chain of the target element straight out of the

Day-1 CONOPS, so a peer's machine querying at any layer above the console software reaches this rule without knowing it exists. `an.eten` names the analytic entry the rule implements. Exactly one of `an.toe`, `an.tdm` and `an.tre` is populated, matching the entry's tag: TDM for a signature, and one element in it. That single field is what lets a coverage review ask "which enumerated elements have no rule watching them" and get an answer from the rule pack itself.

And `playbook` is the other half of the deliverable. It names the authorized response, which ships beside this file as `an-det-01-out-of-pattern-command.playbook.yml`, same directory, same stem, so neither can be read or shipped without the other. The binding lives inside the METEORSTORM extension block rather than at the top level of the rule, which is where platform extensions belong so the base RootA field set stays conformant for a peer operator. A signature with no `meteorstorm.playbook`, or with one that does not resolve to a playbook file beside it, is not accepted into the analytic layer.

> **Two fields people expect and will not find.** There is no `status` field and no `falsepositives` field: neither is in the RootA specification, so known benign causes are written into `details` where the on-call analyst reads them anyway. And there is no second target field. A rule that reads three streams still names one element, because the field answers "what is this signature about", not "what does it read".

> **The User segment.** `SEG-US-User` is a real type in the METEORSTORM data model, the enclave of end users and operators who consume the delivered service. On the Kestrel reference platform it is out of scope, owned and operated elsewhere, so it is not enumerated and carries no AN-DET signatures. The operator-facing attack surface that does touch Kestrel is enumerated inside Ground, Link, and Space.

PART III

Putting it to work

Who reads what you wrote, and how it leaves the room as machine-readable intelligence rather than a document a partner has to re-key.

CH 5 WHO READS THE CATALOGUE

> "The signature, its path, its threat, and the element it watches now share one identifier chain any of the three departments can follow unaided."
>
> DEEP DIVE DECK, SLIDES 15 AND 21 · SIGNATURES AND PLAYBOOKS · DAY 4 COMPLETE

The three readings. The Security Operations Center deploys the rules and executes the actions it is Responsible for. Satellite Operations reads the actions it is Responsible for and the ones it co-signs, so it knows in advance what will be done to a live system during a contact window and has already agreed to it. Satellite Design and Engineering reads the source states as a work queue: every Partial names a dependency, and every Gap names the collection that would close it and the owner who will build it. The RACI is what makes those three readings possible from one document: each department can find its own rows without reading the other two.

Sharing. Every signature is a complete RootA rule, so it ports across detection tooling and is runnable by a peer operator: the form the organization's policy-gated Space ISAC contributions ride on. A peer receives the rule, the one element its TDM anchors to, its source state, and the playbook it authorizes, and can deploy it on different tooling without a rewrite. What the peer does with the RACI is their business: our role names are ours, but the stages, the effect test and the reversibility ladder travel with the file and are what let them work out who in their organization holds each row.

YOUR ROLE IN FUNCTION 04

Incident-response preparedness is the fourth of the five functions where a Full Spectrum professional drives change, and you do not have to be the security operations analyst, the detection author, or the spacecraft engineer to lead it. Security Operations, Satellite Operations, and Satellite Design and Engineering can sometimes be provided by separate organizations, and an incident crosses every one of them at once. Your job is to build the cross-functional team and agree the signatures and playbooks before the incident, so each organization knows its part. That is what makes this function a deliberate point of insertion for transforming how those organizations respond together.

CH 6 TAG AND SHARE

> "Tag your four signatures so the detection portfolio is readable by any peer operator."
>
> DEEP DIVE DECK, SLIDE 19 · TAG THE SIGNATURES

TAG `meteorstorm:AN="AN-DET"`

The tag round-trips against the live METEORSTORM MISP taxonomy, and the machine-readable anchor travels inside the rule itself, in the `meteorstorm` block, where `an.tdm` names the one element the rule watches and the structural fields above it carry that element's parent chain. That is what turns a pile of rules into a reviewable portfolio: coverage is queried by element, not counted by rule, and a query at the segment or environment layer still reaches a rule anchored to an asset three layers down. What a peer operator receives is the complete rule, the element it watches, the source state with any dependency named, and the playbook that runs when it fires.
