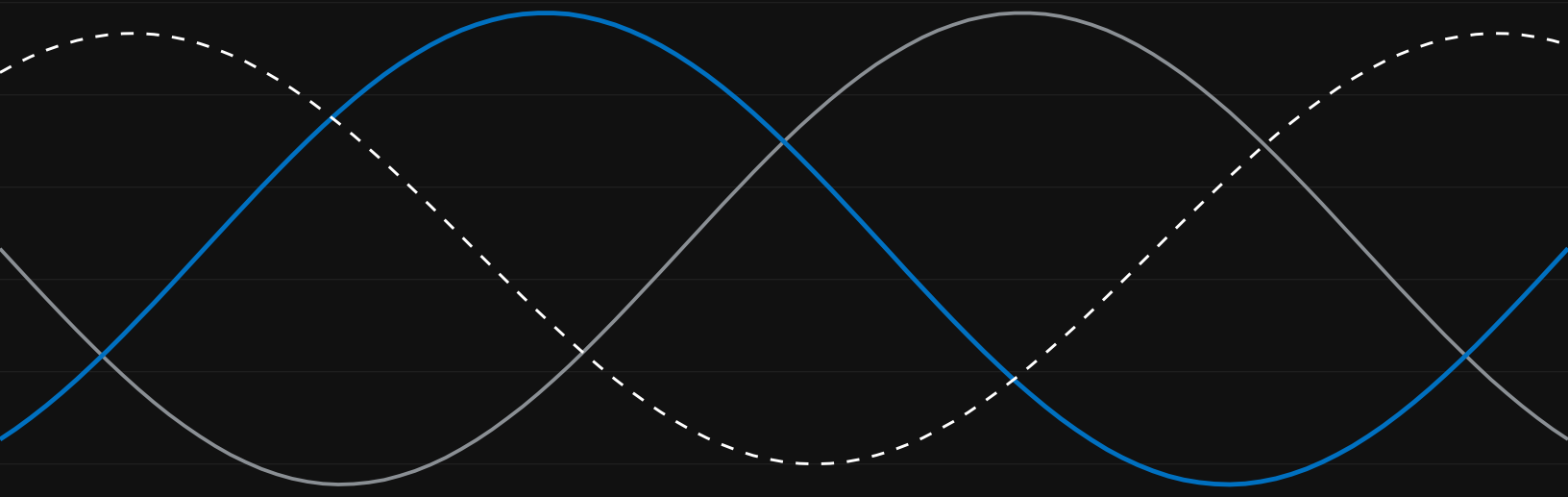
Module 04 · Workbook · Student edition

Incident Response Preparation

The method behind the Day-4 detection signatures: all four entries anchored, one rule printed complete, and the response playbook that runs when each fires.



ethicallyHackingspace (eHs)®
TLP:AMBER

Copyright and legal notices

© 2026 ethicallyHackingspace (eHs)®. All rights reserved.

> **Printing.** To save toner, print from page 2. The cover is a dark full-page plate and carries nothing the pages after it do not.

TLP:AMBER. Limited disclosure. Recipients may share this document only within their own organization and its clients, on a need-to-know basis, and only to the extent necessary to act on the information.

This document is part of the Full Spectrum Space Cybersecurity Professional program. It is provided to enrolled learners and to the credentialing bodies it is submitted to. Sharing beyond what that marking permits, and any resale, is not authorized.

Verbatim sources. Every taxonomy definition quoted in this document is the published METEORSTORM taxonomy text, quoted exactly and never abbreviated, paraphrased or reworded. Where the course explains an element in its own words, the explanation is not presented as the definition. One typographical error in the published file, a doubled period, is corrected.

Trademarks. ethicallyHackingspace (eHs)® is the copyright holder of this publication; D2 Team CORP is its publisher. Other names appearing in this document are the property of their respective owners and are used for identification only.

No warranty. This publication is provided for education. It is not legal, regulatory, or engineering advice for any specific system.

Publisher	D2 Team CORP, a 501(c)(3) nonprofit
Program	Full Spectrum Space Cybersecurity Professional
Document	Module 04 Incident Response Preparation, module workbook, student edition
Edition	Student edition · revised 2026-11-19
Contact	www.d2teamcorp.org

Student edition

The teaching chapters and the complete worked deliverable.

What this document is and how to use it

What it is. The Module 04 workbook for Incident Response Preparation, METEORSTORM Function 04: the method, taught once, and the complete worked result for Kestrel Orbital, the fictional satellite operator this course uses as its example.

How to use it. Read it beside the Module 04 lesson, then keep it as your reference for the method. The contents list every chapter and section with its page.

What goes with it. The Module 04 question set is a separate download; the answers to its questions are printed in it.

© 2026 ethicallyHackingspace (eHs)®

How to use this workbook

The Module 04 lesson on the course site runs in the order below. This workbook is the reference for the story film, Videos 1 to 4 and Parts A to C. Videos 5 to 7 and Parts D and E, the Traffic Light Protocol labels, are taught on the lesson page and are not covered in this workbook.

Story film	Master Exposure Management at Kestrel Orbital
Video 1	The alert nobody may answer
Video 2	The effect test and the level
Video 3	Reading a detection rule
Part A	Read the rule and its signature record
Video 4	From alert to playbook: PB-01
Part B and C	Who may act?
Video 5	Five labels for how far it may go
Video 6	Labeling the Space ISAC entry
Video 7	Writing the label, and receiving one
Part D	Who may receive it?
Part E	Label it
Check	Check your understanding

Use this at work. Blank record sheets, for your own use, are in the METEORSTORM desk pack on the course downloads page.

© 2026 ethicallyHackingspace (eHs)®

Contents

CH 1 **The Day in One Page** 7

CH 2 **What the SOC Brings to the Table** 8

What a library playbook looks like, and how a signature hooks into it 9

CH 3 **The AN-DET Method, and RootA** 10

The second deliverable: the response playbook 11

What Function 03 hands over, and what you do with each state 15

RootA, in more detail 16

Why the mandates are tightening 16

CH 4 **The Catalog, Complete** 17

The worked rule in full 30

CH 5 **Who Reads the Catalog** 32

Your role in Function 04 32

CH 6 **Tag and Share** 33

CH 7 **Use This at Work** 34

Ten things to do at your work center 34

Desk pack sheets for Function 04 36

Where the method is in this workbook 36

What you will be able to do

We will be looking at detection authoring and response readiness so you can author a detection that another operator could deploy without translation, and the response procedure that runs when it fires.

O1	State why a signature with no recorded decider stalls the response
O2	Apply the effect test to set an action's domain and its executor
O3	Write an approved action with its decider, executor and level
O4	State the Day 4 rulings on the rule format and on baselining
O5	Read a signature in MISP and the element it watches
	Sharing what you found, taught on the lesson page only: We will be looking at the Traffic Light Protocol so you can label what Kestrel shares with the Space ISAC Exchange, and apply a label you receive.

The detail behind those objectives:

KNOWLEDGE

K1	A detection signature is a coverage statement: the written commitment to see a specific behavior when it produces observable activity.

© 2026 ethicallyHackingspace (eHs)®

K2	Every AN-DET is a complete RootA rule, SOC Prime specification v1.0.0, carrying the METEORSTORM anchor block. A bare vendor query is not accepted into the layer.
K3	The TDM holds exactly one enumerated element, and it is the TOE of the AN-THR the signature covers. The anchor is inherited, not chosen, and any structural layer may be named.
K4	Streams a signature reads for corroboration are description, not target. A field holding more than one element cannot say what the signature is about.
K5	The module has two deliverables, the signature and the playbook it authorizes. The playbook is not a field on the element: it ships beside the rule and binds to it through meteorstorm.playbook.
K6	A threat or path with no matching signature is a detection gap, and the gap is an enumerable analytic product naming the collection that would close it.
K7	The report stage of a playbook is where the NIS2 clocks are met or missed: 24-hour early warning, 72-hour notification, then a final report one month after the notification. The first two run from awareness.
K8	A playbook carries one trigger and approved actions across assess, contain, recover and report. Assess is the stage teams skip, and on a space platform interference and atmospheric loss look identical to an attack until a second source is consulted.
K9	Every action carries one Responsible executor and one Accountable decider. Mission Lead is Accountable on every action and Responsible on none, because the decider does not also do the work.
K10	The domain comes from the effect test, what the action changes rather than where it happens, and the authority level is derived from the reversibility class rather than chosen.

SKILLS

S1	Author a complete RootA rule: native body inside the wrapper, every mandatory field present, every enum value legal.
S2	Build the METEORSTORM anchor block from the target element's parent chain, with exactly one of toe, tdm and tre populated.
S3	Inherit the TDM correctly from the covered threat rather than assembling it from the streams the rule reads.
S4	Carry the Available, Partial or Gap state forward honestly, and record in the rule what a Partial source cannot see.
S5	Write a playbook carrying at least one approved action in each of assess, contain, recover and report, each action naming one enumerated element and an imperative the on-call analyst can execute at 02:00 without interpretation.
S6	Name the correct reporting clock, its start point and who starts it on a report action, before the incident rather than during it.
S7	Assign the RACI on an action: one Responsible from the domain, Mission Lead Accountable, and the co-signer named on every collaborative action.
S8	Split an action that spans domains into two actions rather than giving one action two Responsible roles.

ABILITIES

A1	Take an unfamiliar path and produce a rule a peer operator can deploy on different tooling without a rewrite.
A2	Defend a recorded Gap to a department that would rather the coverage map read clean.
A3	Refuse a TDM that lists several elements, and explain to its author where the other elements belong.
A4	Hold the line when an action feels over-gated, by treating the reversibility class as the thing to argue about rather than quietly lowering the level.

TASKS

T1	Produce detection signatures as complete RootA rules whose anchor is inherited and singular.
T2	Produce one response playbook per signature, covering all four stages, with an authorization RACI against every action.
T3	Record every detection gap as an enumerated product with its closing collection and owner.

© 2026 ethicallyHackingspace (eHs)®

Part I **Orientation**

What the module 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 catalog, and four attack paths, each carrying its required data and signal sources on the elements they are observed on, every one marked Available, Partial, Gap or unassessed. Today the Security Operations Center (SOC) 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.

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 console operator 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 all four catalog entries and all four playbooks in full, and one of the four rules complete, the worked rule for Signature 01. The other three rule files are not printed here: they are in the machine-readable data and rule files, the download **04-machine-readable.zip** on the course downloads page.

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.

© 2026 ethicallyHackingspace (eHs)®

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 of that notification, each submitted to the CSIRT, the computer security incident response team, or, where applicable, the competent authority (Article 23(4)). 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."

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 required source can be watched at all.
02 RootA templates	The vendor-neutral detection format. One rule moves between Splunk, Elastic and Microsoft Sentinel by a translation pass, not a rewrite.	The form every signature must take.
03 Playbook library	The incident response (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.

© 2026 ethicallyHackingspace (eHs)®

What a library playbook looks like, and how a signature hooks into it

The six artifacts name the playbook library and move 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 chief information security officer (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. Holding the uplink at the Kiruna ground terminal to reviewed commands changes what the live uplink may carry, 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.

© 2026 ethicallyHackingspace (eHs)®

Part II **The method and the catalog**

The process for producing one entry correctly, then the complete catalog it produced, entry by entry.

CH 3 The AN-DET Method, and RootA

> "Seven steps, fixed order. Every signature is a complete RootA rule, and its TDM is the one element its threat already named."

Inputs. Yesterday's attack-path catalog 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.** The published definition of a detection signature is "Validated and operational pattern, signal, or logic that triggers on contextualized threat behavior for a converged space system." (MISP meteorstorm taxonomy v2, AN-DET). In this course it is written as a complete RootA rule. Two ways to fail it. **Not a complete rule**: a bare SPL, KQL or EQL query, or a bare Sigma rule, 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 seven 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. The register opened this week, so today's signatures read 00 to 03; gaps will appear as it takes in work outside this scope, and an ordinal is issued once and 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 layer is not chosen today: Day 2 set the TOE at the lowest layer its source resolves, and the TDM inherits that element unchanged.

© 2026 ethicallyHackingspace (eHs)®

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.
7. **Name the PLAYBOOK.** The authorized response this signature triggers, as **meteorstorm.playbook** on the rule and a playbook file beside it. The step names the playbook; the next section is how you write it.

Repeat for the next signature. When every cataloged 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: 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

Step 07 names the playbook. It does not write it, 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. 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.

© 2026 ethicallyHackingspace (eHs)®

Stage	Answers	Why it is here, on this platform
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 of that notification. 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

Three roles and three authority levels govern every playbook in this course, under one rule: **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.

© 2026 ethicallyHackingspace (eHs)®

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.

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 the one-role-one-level rule, 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 holding the uplink at the Kiruna ground terminal to reviewed commands 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.

© 2026 ethicallyHackingspace (eHs)®

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: safe mode, for example.	**collaborative**	The other operating role co-signs before execution, as the Consulted party.
irreversible	Cannot be undone by deciding differently: a filed regulatory change, a filed Space ISAC Exchange entry, 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.

© 2026 ethicallyHackingspace (eHs)®

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 required source in yesterday's inventory, each RDS record and each RSS measurement, sits on the one element it is observed on and carries one of four states. The state is not a grade on the analyst; it is a statement about the platform, and each one carries a different instruction.

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.
unassessed	The owning department has not returned a state yet. It is not a coverage state.	Do not author against it as if it were Available. Write the signature on the anchor source, name the unassessed stream in **details** as a corroboration still to be confirmed, and chase the owner for a state.

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.

© 2026 ethicallyHackingspace (eHs)®

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 security information and event management (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 translates a RootA rule into the query languages of other platforms, 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 after a translation pass rather than a rewrite, which is what makes the sharing mandate practical rather than aspirational.

Why the mandates are tightening

CNSS policy for national security space systems (CNSSP No. 12, implemented by CNSSI 1200, August 2025) requires on-board intrusion detection and prevention capable of real-time monitoring, detection and response. A detection portfolio anchored to enumerated elements is how an operator demonstrates that requirement is met rather than asserted. (Source: CNSSI 1200, Committee on National Security Systems, August 2025.) These policies bind national security systems and their suppliers. Kestrel Orbital is neither; they are cited as the direction its government customers are moving in, not as duties on Kestrel.

© 2026 ethicallyHackingspace (eHs)®

CH 4 The Catalog, Complete

> “One signature per path, one playbook per signature, one element per signature, and one executor and one decider per action.”

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. 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. One rule, the worked rule for Signature 01, is printed in full below. The four rule files and their playbook files, side by side with the same stem, are in the machine-readable data and rule files, the download **04-machine-readable.zip** on the course downloads page.

GROUND · 2 AN-DET + 2 playbooks

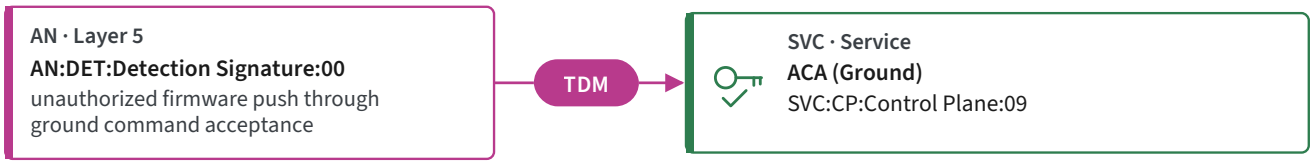
AN:DET:Detection Signature:00 · Unauthorized firmware push through ground command acceptance

Detects firmware-push operations released through the ground command-acceptance service outside maintenance windows. The other two Path 00 sources, the remote-access record at the ground crypto service and the deployed-image hash record, are unassessed and corroborate on a hit.

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**
Format	Complete RootA rule (**an-det-00-mgmt-plane-abuse.yml**), severity critical
Source state	**Available, src-ground-aca-010**
Corroborating streams	The other two required data sources on Attack Path 00: the management-network remote-access record (**SVC:CP:Control Plane:08**, **RDS:00**) and the deployed-image hash record (**AST:SW:Software:03**, **RDS:02**), both still unassessed. Pulled on a hit, named in the rule’s **details**, not in the TDM.
Source citation	Day-2 composite OSINT threat assessment, through AN:THR:Threat:00 and AN:ATT:Attack Path:00

© 2026 ethicallyHackingspace (eHs)®

Figure 1 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 element on the right has not moved since Day 2.

PB-00 · Unauthorized firmware push through ground command acceptance

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 patch deployment pipeline installs to every element downstream of it.

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

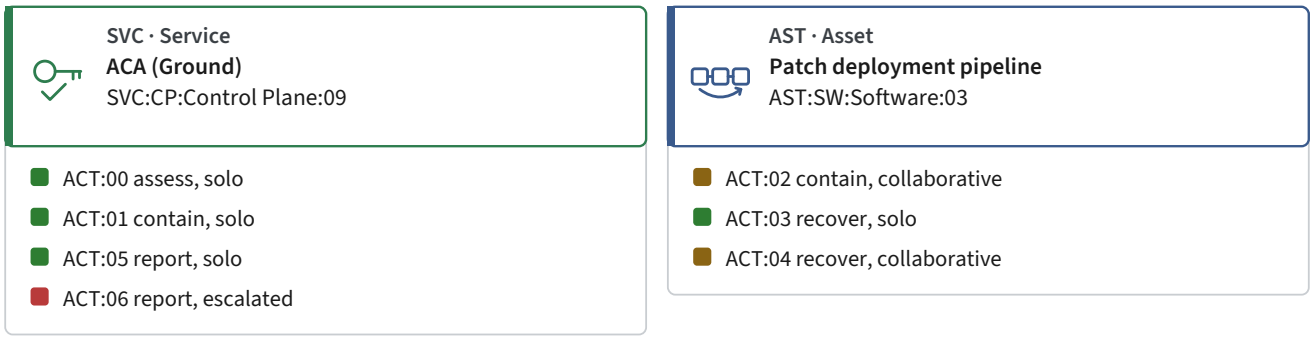
© 2026 ethicallyHackingspace (eHs)®

Approved action	R executes	A decides	C consulted	I informed
ACT:03 recover · cyber Inventory which elements received the push and compare each deployed image 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 the pushed image against the maintenance window, confirming operational impact before each batch. AST:SW:Software:03 *Why space: Changes what the platform 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, who assess significance under NIS2; the clocks run from awareness, 24-hour early warning, 72-hour notification, one-month final report. A firmware push outside any maintenance window 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 belong to Security Operations, space responses to Satellite Operations, and every level is read off the reversibility class rather than chosen.

© 2026 ethicallyHackingspace (eHs)®

Figure 2 The playbook's approved actions as icons, by the element each acts on



Each platform element the playbook acts on, with the approved actions that name it and their authority level.

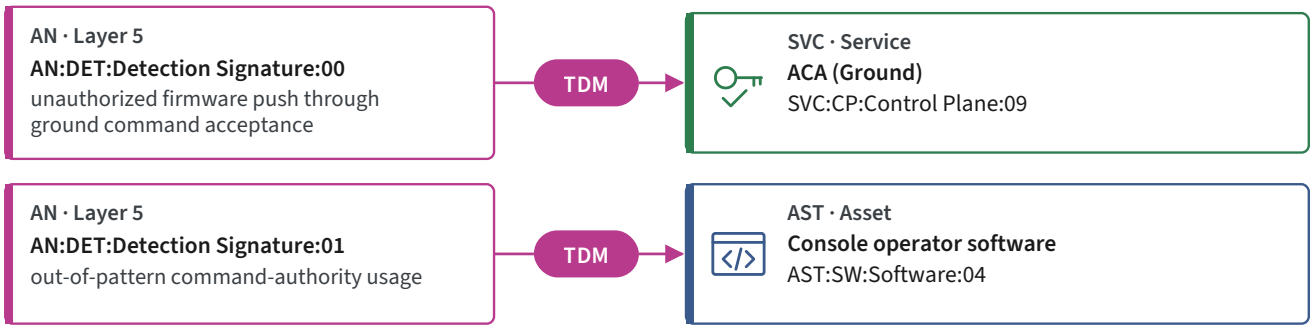
AN:DET:Detection Signature:01 · Out-of-pattern command-authority usage

Detects command-authority usage outside the role and shift baseline, or high-impact commands issued with no peer-review tag.

Field	Value
TDM (anchor)	**AST:SW:Software:04**
What that element is	The console operator 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	The other two required data sources on Attack Path 01: the operator console session record, host and sign-in time (**AST:HW:Hardware:04**, **RDS:00**) and the control-plane command release record with review state (**SVC:CP:Control Plane:09**, **RDS:02**), both still unassessed. Pulled on a hit, named in the rule's **details**, not the anchor.
Source citation	MITRE ATT&CK T1078 (Valid Accounts); NIST SP 800-53 AC-5 (Separation of Duties)

© 2026 ethicallyHackingspace (eHs)®

Figure 3 AN-DET anchors · 2 of 4 entries · after AN:DET:Detection Signature:01



The second signature anchors to an asset, so its card reads AST · Asset, in the asset color. Two signatures, two structural layers, and in both cases the anchor was inherited rather than chosen.

The tempting error. This rule reads the operator console session record and the control-plane command release record, 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. 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 Radiate the Kiruna uplink only for commanding sessions released under two-person review. SVC:HY:Hybrid:03 *Why space: Changes what the live uplink is allowed to carry to the vehicle, a mission operational state change taken on a ground element.* disruptive → collaborative	Satellite Operations	Mission Lead	Security Operations	none

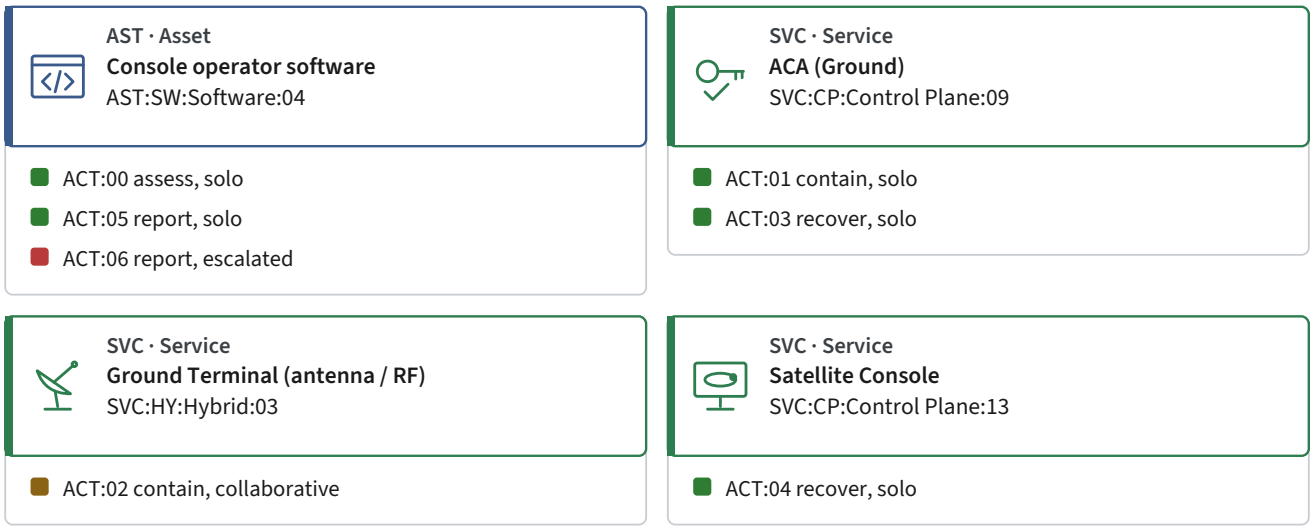
© 2026 ethicallyHackingspace (eHs)®

Approved action	R executes	A decides	C consulted	I informed
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, who assess significance under NIS2; the clocks run from awareness, 24-hour early warning, 72-hour notification, one-month final report. AST:SW:Software:04 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 belong to Security Operations, space responses to Satellite Operations, and every level is read off the reversibility class rather than chosen.

© 2026 ethicallyHackingspace (eHs)®

Figure 4 The playbook's approved actions as icons, by the element each acts on



Each platform element the playbook acts on, with the approved actions that name it and their authority level.

LINK · 1 AN-DET + 1 playbook

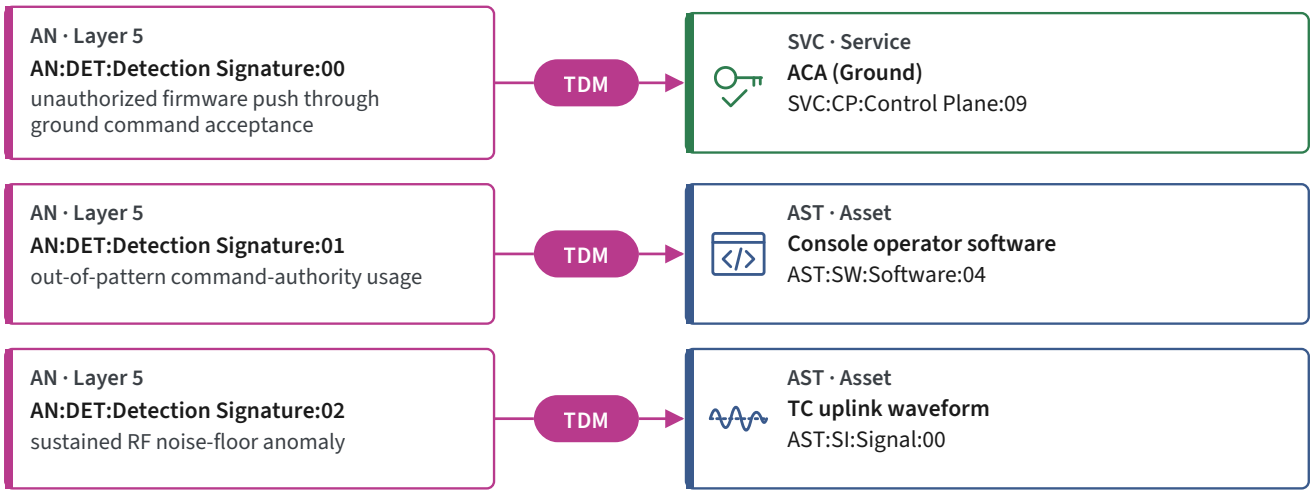
AN:DET:Detection Signature:02 · Sustained RF noise-floor anomaly

Detects elevated noise on the telecommand uplink waveform beyond expected environmental thresholds, sustained for longer than incidental atmospheric events.

Field	Value
TDM (anchor)	**AST:SI:Signal:00**
What that element is	The telecommand uplink waveform. 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, the receiver lock status and link-outage measurement on this element (RSS:02 on Attack Path 02). The rule body as shipped does not yet read this source, and its details says so.**
Corroborating streams	The other two required signal sources on Attack Path 02: the uplink corrected bit-error and frame-error rate measurement (**SVC:HY:Hybrid:01**, **RSS:00**) and the link noise-floor and carrier-to-noise measurement (**SVC:HY:Hybrid:02**, **RSS:01**), both still unassessed. Pulled on a hit, not the anchor.
Source citation	ITU interference-reporting guidance; SPARTA EX-0016 (Jamming)

© 2026 ethicallyHackingspace (eHs)®

Figure 5 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 threat's TOE sits. The layer is not chosen today: Day 2 set the TOE at the lowest layer its source resolves, and the TDM inherits it. Here the TOE of AN:THR:Threat:02 is 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 Compare the spacecraft receiver lock and signal-level telemetry against the Kiruna noise floor to separate interference at the spacecraft from interference local to the ground station. AST:SI:Signal:00 reversible → solo	Satellite Operations	Mission Lead	none	Security Operations
ACT:01 contain · space Switch the uplink to the pre-arranged backup band. AST:SI:Signal:00 disruptive → collaborative	Satellite Operations	Mission Lead	Security Operations	none

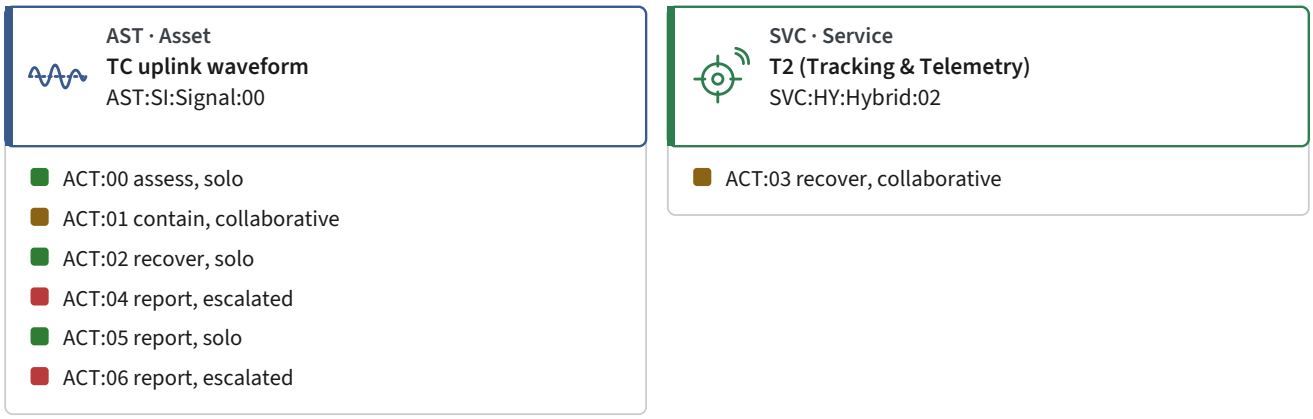
© 2026 ethicallyHackingspace (eHs)®

Approved action	R executes	A decides	C consulted	I informed
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
ACT:06 report · cyber File the redacted Space ISAC Exchange entry. 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.* irreversible → escalated	Security Operations	Mission Lead	Satellite Operations	none

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

© 2026 ethicallyHackingspace (eHs)®

Figure 6 The playbook's approved actions as icons, by the element each acts on



Each platform element the playbook acts on, with the approved actions that name it and their authority level.

Field note

PB-02 is the shape a link-layer incident takes: every action is a space response except the two report actions Security Operations executes, the NIS2 notification, **ACT:05**, and the Space ISAC Exchange entry, **ACT:06**, 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 way to tell is to compare the spacecraft's own receiver telemetry against the Kiruna noise floor. 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

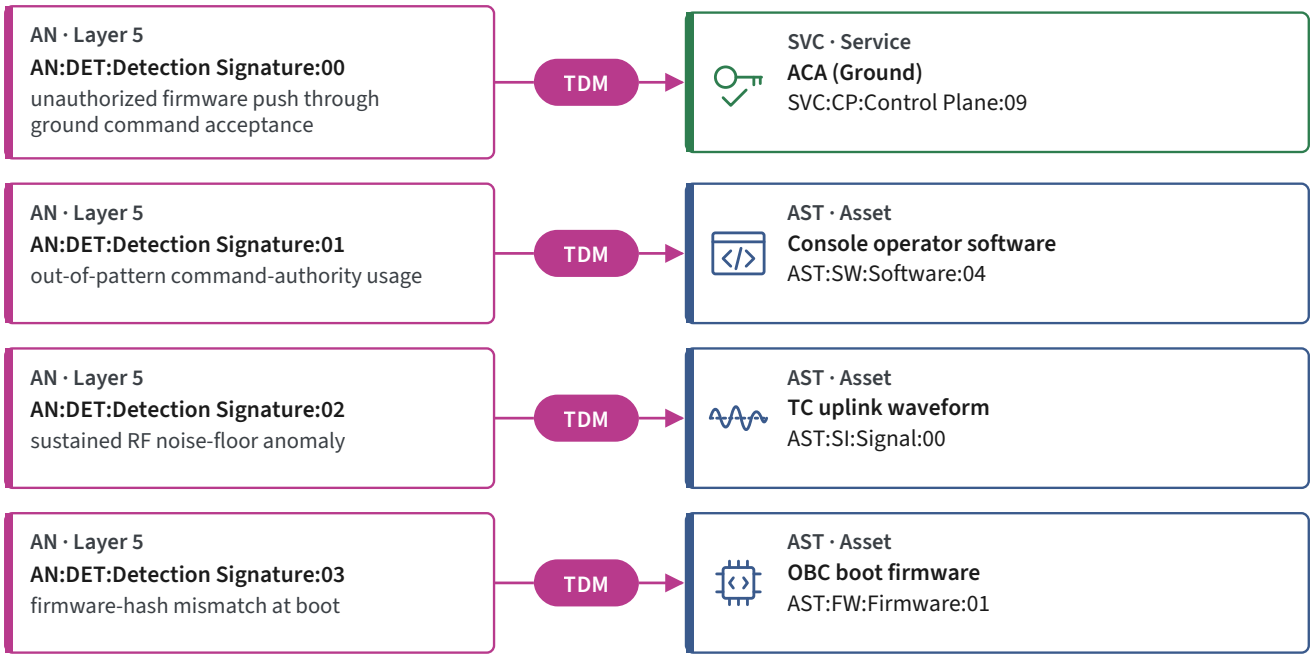
Detects firmware images whose measured hash does not match the signed expected value at boot or after an update.

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.**

© 2026 ethicallyHackingspace (eHs)®

Field	Value
Corroborating streams	The other two required data sources on Attack Path 03: the update-push activity record on the patch update service (**SVC:CP:Control Plane:12**, **RDS:00**) and the on-board signed-manifest verification record (**SVC:HY:Hybrid:00**, **RDS:01**), both still unassessed. Pulled on a hit, not the anchor.
Source citation	NIST SP 800-193; SPARTA IA-0001 (Compromise Supply Chain)

Figure 7 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.

> **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.

© 2026 ethicallyHackingspace (eHs)®

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.

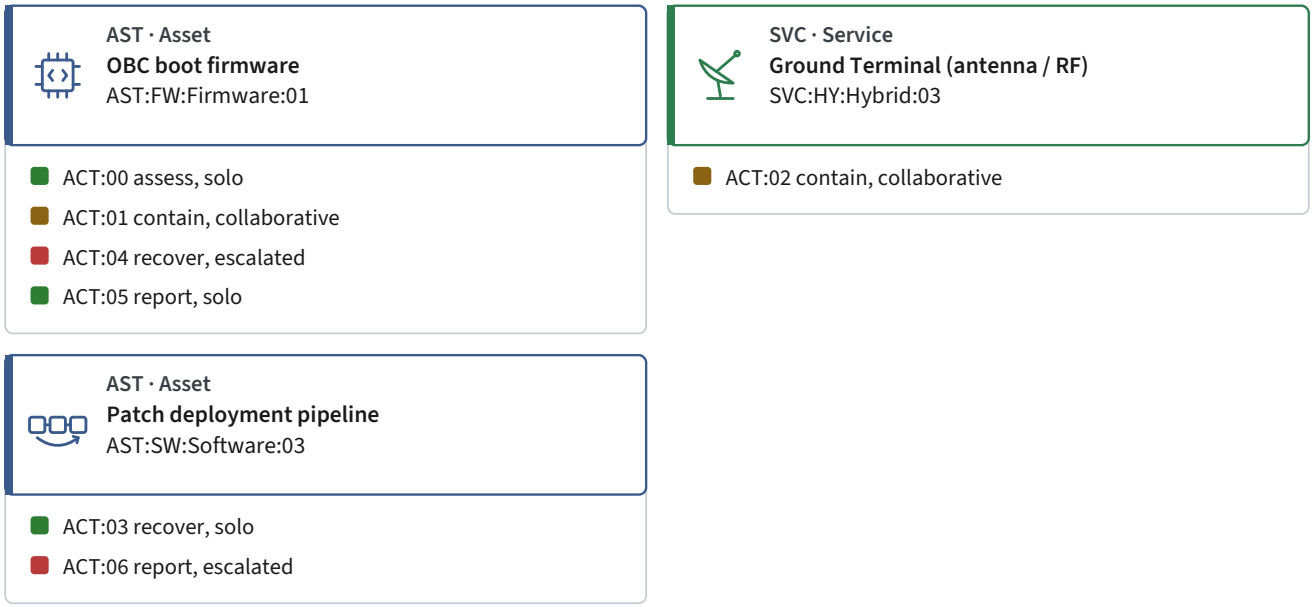
Approved action	R executes	A decides	C consulted	I informed
ACT:00 assess · space Compare the measured hash against the signed expected value in the vendor manifest. AST:FW:Firmware:01 reversible → solo	Satellite Operations	Mission Lead	none	Security Operations
ACT:01 contain · space Hold the boot firmware 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 Radiate the uplink to the affected spacecraft from the Kiruna ground terminal only for commanding sessions released under two-person review, so no further image or command reaches the on-board computer unreviewed. SVC:HY:Hybrid:03 *Why space: Changes what the live uplink is allowed to carry to the vehicle, a mission operational state change taken on a ground element.* disruptive → collaborative	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

© 2026 ethicallyHackingspace (eHs)®

Approved action	R executes	A decides	C consulted	I informed
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 runs from awareness, the moment Security Operations becomes aware of the mismatch, 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 belong to Security Operations, space responses to Satellite Operations, and every level is read off the reversibility class rather than chosen.

Figure 8 The playbook's approved actions as icons, by the element each acts on



Each platform element the playbook acts on, with the approved actions that name it and their authority level.

© 2026 ethicallyHackingspace (eHs)®

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 re-establishing a known-good image and filing the Space ISAC entry cannot be undone by deciding differently later, and the containment holds the Kiruna uplink to reviewed commands rather than switching hardware, because no redundant on-board computer is recorded for this constellation. That is the ladder doing its job, not caution.

The worked rule in full

The rule and its playbook are one product; here is the rule for **an-det-01-out-of-pattern-command.yml** complete, with every field. The other three rules follow the same layout with their own values. Field names, order and casing follow the SOC Prime RootA specification v1.0.0, and the **meteorstorm** block is appended last.

Listing an-det-01-out-of-pattern-command.yml · the complete rule file, from **04-machine-readable.zip**, folder **module4/rules**. In print, a value too long for one line continues on the lines below it, indented under its key.

```
name: Out-of-pattern command-authority usage on the console operator software
details: |
  Detects command-authority usage outside the role and shift baseline: an operator not on
  the shift roster commanding, and high-impact commands issued with no peer-review tag.
  Corroborating streams the analyst should pull on
  a hit, which are not the target of this rule: the other two required data sources on Attack
  Path 01, the operator console session record, host and sign-in time (AST:HW:Hardware:04), and
  the control-plane command release record with review state (SVC:CP:Control Plane:09), both
  still unassessed. Source state Partial: the peer-review tag stream depends
  on workflow adoption, so a command issued by a team that has not adopted the tag will not be
  distinguishable from one that skipped review. 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: 2026-08-06
mitre-attack:
    - t1078
detection:
    language: splunk-spl-query
    body: index=sat_command sourcetype=command_audit origin_device="operator-console" command_class IN
        ("safe_mode_exit","thruster_burn","ranging_off","encryption_disable") | lookup shift_roster
        operator OUTPUT role, shift, on_shift | where peer_review_tag="false" OR
        isnull(peer_review_tag) OR on_shift="false" OR isnull(on_shift)
logsource:
    product: satellite_command_pipeline
    service: command_audit
```

© 2026 ethicallyHackingspace (eHs)®

```
    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 role, shift
references:
    - AN:ATT:Attack Path:01
    - AN:THR:Threat:01
    - https://attack.mitre.org/techniques/T1078/
    - 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. Where an element in the chain has more than one parent, the field lists every parent: the Signature 02 rule lists under **pce** every environment **SEG:LI:Link:00** sits in. **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".

© 2026 ethicallyHackingspace (eHs)®

Part III **Putting it to work**

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

CH 5 Who Reads the Catalog

> "The signature, its path, its threat, and the element it watches now share one identifier chain any of the three departments can follow unaided."

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. What crosses is governed by company directive KO-EXEC-2026-014: redaction before release is mandatory, and only the approved element and the context needed to act on it leaves the company (section 3.4). Within that limit 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 with a translation pass rather than 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.

© 2026 ethicallyHackingspace (eHs)®

CH 6 Tag and Share

> “Tag your four signatures so the detection portfolio is readable by any peer operator.”

> **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 rule, the element it watches, the source state with any dependency named, and the playbook that runs when it fires, each after the redaction described below.

The record in MISP. The signature is the event. **AN:DET:Detection Signature:00** is recorded as one event tagged **meteorstorm:AN="AN-DET"**, with a **TDM** attribute naming **SVC:CP:Control Plane:09**, the same element **AN:THR:Threat:00** names as its TOE, and a **PLAYBOOK** attribute naming PB-00.

The redacted Space ISAC Exchange entry. All four playbooks carry an approved action that files one. What governs it is company directive KO-EXEC-2026-014, section 3, Conditions of Exchange. Every exchanged element carries its METEORSTORM tag and, where it names a specific instance on the platform, its ETEN identifier and parent chain (3.1), which is what the tag above and the **meteorstorm** block supply. Exchange is machine to machine: “structured records over the agreed Space ISAC interface, not free-text email or ad hoc attachments” (3.2). And redaction before release is mandatory: “Mission-sensitive detail, customer identity, and any content restricted under ITAR or EAR is removed or withheld. Only the approved element and the context needed to act on it leaves the company.” (3.4). The directive makes SCOR the owner of the interface and the redaction standard (section 4). It sets no entry template and no handling marking for the entry, and this workbook adds none.

© 2026 ethicallyHackingspace (eHs)®

CH 7 Use This at Work

This workbook teaches Function 04 on Kestrel Orbital. To run it on your own platform, work from the **METEORSTORM desk pack**, a separate course download. Its sheets are blank framework templates. They are for your own use and are not returned to the course.

Ten things to do at your work center

Function 04 gives every attack path something that fires: a detection signature, and the playbook that runs when it does. Each of these can be done with what is already on your desk, in the order given. They are for your own use and are not returned to the course. The sheets named are in the METEORSTORM desk pack.

01 **Read the state of each required source before you write a signature.** Available: author against the named source identifier. Partial: author what the fidelity supports and record exactly what the rule cannot see. Do not round Partial up to Available, and do not author against an unassessed source as if it were Available.
What you gain: the source states read as a work queue: every Partial names a dependency, and every Gap names the collection that would close it and its owner.
Chapter 3, What Function 03 hands over, and what you do with each state; Chapter 5 · desk pack sheet 11, Function 04: detection signature record and playbook acceptance checklist

02 **Apply the gate to one signature.** It passes only as a complete RootA rule carrying the METEORSTORM anchor block, with a TDM that holds exactly one enumerated element. A bare query fails it, and so does a TDM that is empty or holds a list.
What you gain: a rule that can travel, so it can be shared, reviewed, and ported when the tooling changes.
Chapter 3, The Gate · desk pack sheet 10, Function 04 Incident Response Preparation: method card

03 **Run the seven steps on one signature, in the fixed order.** Layer, format, tag, ordinal, TDM, description, playbook. Repeat for the next signature until every cataloged attack path has a detection enumerated, whether it can fire yet or not.
What you gain: a current coverage matrix, in which coverage is queried by element, not counted by rule.
Chapter 3, The seven steps, fixed order; Chapter 6 · desk pack sheet 10, Function 04 Incident Response Preparation: method card

04 **Carry the TDM across; do not choose it.** It is the same element the threat this signature covers named as its TOE. Name the corroborating streams in the description, never in the TDM.
What you gain: threat, path and signature name one element, so nobody has to negotiate what the signature is for.
Chapter 1, and Chapter 3, step 05 and the note after the steps · desk pack sheet 11, Function 04: detection signature record and playbook acceptance checklist

05 **Record one detection gap as a product.** Where the source is a Gap, enumerate the signature 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.
What you gain: the gap is never a silent omission, and the justification for the collection that closes it is already enumerated instead of argued from scratch.
Chapter 3, The detection-gap rule · desk pack sheet 11, Function 04: detection signature record and playbook acceptance checklist

© 2026 ethicallyHackingspace (eHs)®

06 **Hook one library playbook to its signature with the four edits.** Name the signature and its confidence threshold in the trigger, replace every generic service or site with an exact enumerated element, name the concrete clock and who starts it in the report action, and give every action its authorization.
What you gain: most of the procedure already exists, and the edits make it precise enough to run; the on-call analyst does not have to work out which service is meant.
Chapter 2, What a library playbook looks like, and how a signature hooks into it · desk pack sheet 12, Function 04: blank playbook

07 **Set each action's domain by the effect test, and split any action that needs two executors.** Ask what the action changes, not where it is taken and not what verb it uses. An action needing two executors is two actions.
What you gain: a sequence that can be audited, and no department assuming the other did it.
Chapter 3, Who executes, and who decides, and The effect test sets the domain · desk pack sheet 10, Function 04 Incident Response Preparation: method card

08 **Read each action's authority level off the reversibility ladder.** Reversible is solo, disruptive is collaborative, irreversible is escalated. The level is derived, never chosen; if an action feels over-gated, review its reversibility class instead of lowering the level.
What you gain: the decision is made in advance, when there is time to think, and recorded in the playbook, not taken under pressure.
Chapter 3, The second deliverable, and The reversibility ladder sets the level · desk pack sheet 10, Function 04 Incident Response Preparation: method card

09 **Write the report action before the incident.** Every report action names the clock it starts and who starts it. A playbook is not finished when the threat is contained; it is finished when the report is filed.
What you gain: the on-call analyst does not have to look the clock up, and the leg the regulator reads is not dropped.
Chapter 1, The clocks, and Chapter 3, One trigger, four stages · desk pack sheet 12, Function 04: blank playbook

10 **Check one playbook against the nine-point minimum before its signature ships.** A playbook that cannot meet the minimum is a finding, recorded as such. It is never met by writing a vaguer action.
What you gain: no alert without an owner. With a signature and a playbook on each path, automated tools and known exploits begin failing on the instrumented routes, and attackers must adapt tools or pivot to a route not yet instrumented.
Chapter 3, The minimum · Pentagon of Pain guide, section 7.7 · desk pack sheet 11, Function 04: detection signature record and playbook acceptance checklist

© 2026 ethicallyHackingspace (eHs)®

Desk pack sheets for Function 04

Sheet	Use it to
Quick reference, two pages	Read the layers, the tags and the identifier syntax without opening a workbook.
Function 04 method card	Apply the gate to each signature, run the seven steps in order, and set each action's domain and authority level.
Function 04 blank record sheet	Write one detection signature and the playbook it authorizes, one approved action per row.
Checklists	Check a signature and its playbook before the signature ships.

Where the method is in this workbook

You need	Chapter and heading
The gate	Chapter 3, The Gate.
The seven steps	Chapter 3, The seven steps, fixed order.
The playbook stages	Chapter 3, One trigger, four stages.
Who executes and who decides	Chapter 3, Who executes, and who decides: the three roles and the RACI letters.
The domain and the authority level	Chapter 3, The effect test sets the domain, and The reversibility ladder sets the level.
The fields of one action	Chapter 3, One action record.
The rules	Chapter 3, The minimum, nine checks a playbook must pass. Chapter 3, What Function 03 hands over, and what you do with each state, and The detection-gap rule.
Complete worked models	Chapter 4, four signatures with their playbooks, and The worked rule in full.
The tag, and what may be shared	Chapter 6.

© 2026 ethicallyHackingspace (eHs)®