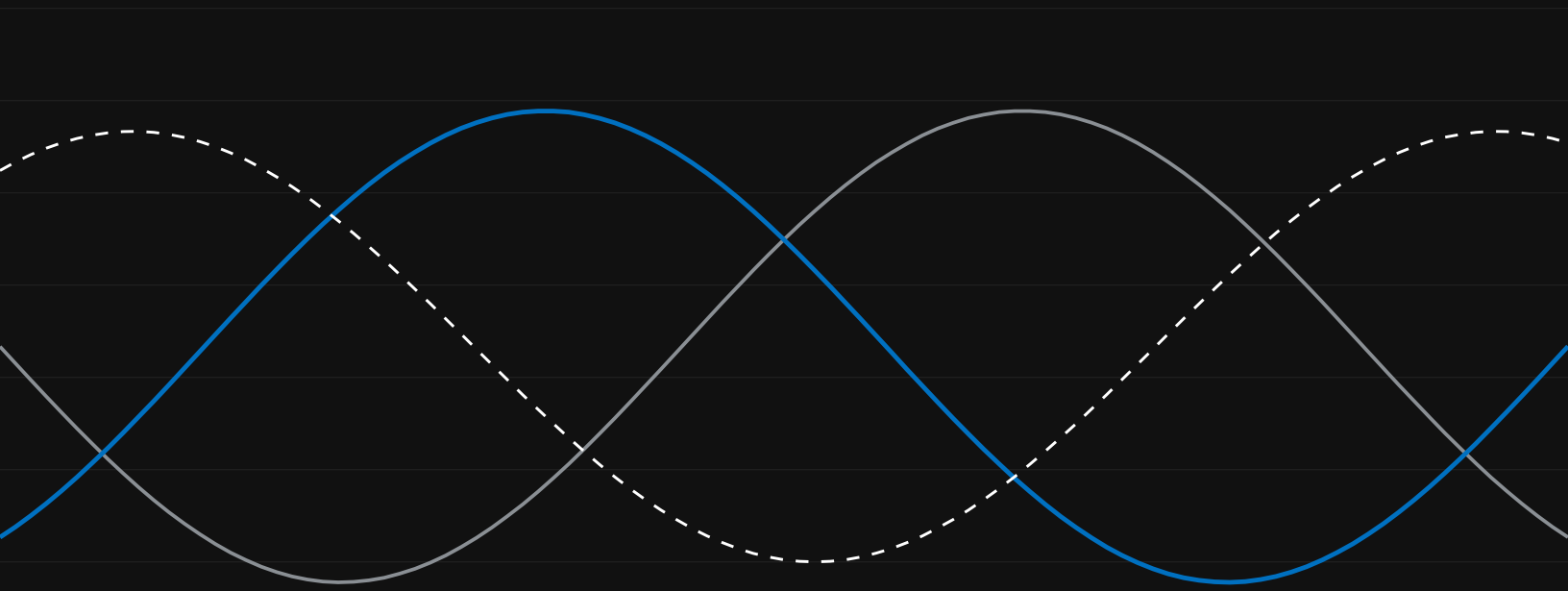
Module 03 · Workbook · Student edition

Converged Detection Engineering

The method behind the Day-3 attack paths, and every path it produced, each anchored to the element its threat names, with the required source inventory that goes with it.



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 03 Converged Detection Engineering, 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 03 workbook for Converged Detection Engineering, METEORSTORM Function 03: 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 03 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 03 question set is a separate download; the answers to its questions are printed in it.

How to use this workbook

The Module 03 lesson on the course site runs in the order below. This workbook is the reference for every step. The lettered parts are worked on the lesson page, not in this workbook.

Story film	Master Converged Detection Engineering at Kestrel Orbital
Video 1	One outage, two true pictures
Video 2	Record or signal: the required-source record
Part A	Build and check the required-source record
Video 3	Walking the four paths
Part B	Walk the paths and count what must be collected
Video 4	The element is the join
Part C	Join each detection to its path
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** 6

CH 2 **What Engineering Brings to the Table** 7

CH 3 **The AN-ATT Method** 8

The second deliverable: the required-source inventory 9

Choosing the required source when a step emits several 10

Why converged detection engineering exists 11

CH 4 **The Catalog, Complete** 11

A four-waypoint path, worked 20

CH 5 **Who Reads the Catalog** 21

Your role in Function 03 22

CH 6 **Tag and Share** 22

CH 7 **Use This at Work** 23

Ten things to do at your work center 23

Desk pack sheets for Function 03 25

Where the method is in this workbook 25

What you will be able to do

We will be looking at route tracing and source enumeration so you can turn an anchored threat into a traced route and a list of the things a defensive cyber operator must watch to see it.

O1	State why an outage that no shared record explains cannot be resolved
O2	Separate a required data source from a required signal source
O3	Write a required-source record: sub-ordinal, name, element and state
O4	State the Day 3 rulings, including how two sources are joined
O5	Read an attack path in MISP and the element it inherits

The detail behind those objectives:

KNOWLEDGE

K1	An attack path is an exposure, not an observation: it records what is reachable given the architecture, and is drawn from documented tradecraft or a confirmed exposure.
K2	The anchor is inherited: a path takes the one element its AN-THR names, so threat, path, signature and measure all name the same thing.
K3	Anchor and objective are different questions. The anchor is what the path is about; the objective is where the route lands, and they need not be the same element.

© 2026 ethicallyHackingspace (eHs)®

K4	Waypoints are description content: entry, pivot and objective, three or four, each an element where the adversary must act in a way a detection could observe.
K5	The module has two deliverables, the path catalog and the required-source inventory, and the required sources are fields on the attack-path element: RDS for what must be received as a record, RSS for what must be measured in the physical layer.
K6	A coverage gap is an enumerable product. A required source that does not exist still takes a sub-ordinal, an element and the state Gap, and unassessed is kept distinct from it because nobody has looked yet.

SKILLS

S1	Trace a route from entry to objective across enumerated elements, dropping pass-through elements that emit nothing.
S2	Inherit the anchor correctly from the driving threat rather than choosing a fresh element.
S3	Choose the one required source to record where a step emits several candidates, and say which field it belongs in.
S4	Give every required source its state honestly: Available with the source identifier, Partial with what is short, Gap with what would close it, or unassessed where the owning department has not yet returned one.
S5	Justify a fourth waypoint by naming the trust boundary the second pivot crosses.
S6	State confidence in a path and the evidence that sets it.

ABILITIES

A1	Take an unfamiliar threat and produce a path another analyst can evaluate against their own platform, unprompted.
A2	Defend a recorded gap to a department that would rather it were marked Partial.
A3	Hand the source inventory to detection engineering in a form it can author against without re-analysis.

TASKS

T1	Produce attack paths whose anchor is inherited and whose traversal is written as observable waypoints.
T2	Populate the RDS and RSS fields on every attack path, each record carrying a sub-ordinal, the one element it is observed on, and its state.
T3	Record every coverage gap as an enumerated finding rather than an omission.

© 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

Two days in, the department you are building has a foundation: one shared data model of 44 enumerated elements, and four **AN-THR** threats each anchored by its Target of Exploitation (TOE) to the one element it targets. Today Satellite Design and Engineering takes the lead and opens its build knowledge, because walking a threat into a real route needs the platform as it was actually built.

What you do. For each Day-2 threat you enumerate an attack path: the ordered elements an adversary traverses to realize it, expressed as three or four detectable waypoints, then you record on that same element the data sources and the signal sources a defensive cyber operator must hold to see the traversal happen.

The chain, three days in. One chain is one number carried across the week. Day 1 enumerated **AST:SI:Signal:00**, the telecommand uplink waveform. Day 2 anchored **AN:THR:Threat:02**, the jamming campaign, to that waveform. Day 3 walks it as **AN:ATT:Attack Path:02**, entering at the error-handling service, forward error correction and error-correcting code (FEC/ECC), where corrected bit errors first climb, pivoting through tracking as the noise floor rises, and ending on the waveform itself, which on this path is also its anchor, where the link loses lock. Every path in chapter 4 is walked the same way.

What you build. Four **AN-ATT** elements: 2 Ground, 1 Link, 1 Space, one per threat, each anchored to public reporting or a framework reference with an honestly stated confidence. Chapter 4 prints the whole deliverable with every waypoint and every required source.

What tomorrow consumes. Day 4, Incident Response Preparation, reads the required sources one record at a time and turns each into a detection signature and the playbook that runs when it fires. A required source that is only a guess today is a signature that never fires tomorrow, which is why steps 07 and 08 are the strictest of the eight.

© 2026 ethicallyHackingspace (eHs)®

CH 2 What Engineering Brings to the Table

> "Six artifacts on the table. Satellite Design and Engineering owns the deepest knowledge of how the platform actually moves data and commands, and today the department lays that knowledge open."

Artifact	What it holds	The question it answers
01 Architecture	System block diagrams: what subsystem connects to what, over which bus, with which authentication boundary.	Where are the trust boundaries a path would have to cross?
02 Command flows	How a single telecommand actually moves from operator console through Command and Data Handling (C&DH) to the receiving subsystem.	What is the real route a command takes, hop by hop?
03 Data flows	How mission data moves on-board, where it is buffered, where it is signed, where it is downlinked.	Where does evidence exist, and where does it never leave the vehicle?
04 Interface specs	Wire-level protocol specs: Consultative Committee for Space Data Systems (CCSDS) framing, MIL-STD-1553 bus traffic, SpaceWire, internal handshakes.	What can be observed at the wire, and in what format?
05 Flight software	What runs on the on-board computer (OBC), how commands are parsed and dispatched, what behaviors are hard-coded versus reconfigurable.	What would an adversary have to change, and would it be logged?
06 Supply chain	Vendor provenance for each firmware and hardware item: who built it, when, with which signing pipeline.	Where could a tampered component enter before the platform ever flew?

> **There is no one-size-fits-all artifact set.** These six carry Kestrel Orbital's own document numbers and branding; another operator would open a different stack. What stays constant is the question each artifact answers, not the document itself. When you run this session at a different organization, bring the six questions and find whichever documents answer them.

Why the ask worked. Engineering documentation of this depth is rarely handed to a security function on request. It was handed over here because two days of shared work earned it: Day 1 gave the departments one taxonomy they helped build, and Day 2 produced a threat set enumerated against that taxonomy rather than written in security jargon. The artifacts open because the team asking already speaks the platform's language.

© 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-ATT Method

> "Eight steps, fixed order. Every path anchors to the one element its driving threat already names, and states on that element what a defensive cyber operator must hold to see it."

Inputs. Yesterday's enumerated threat set, four threats anchored to the telecommand path, and a working session with Satellite Design and Engineering.

Output. One AN-ATT element per attack path. Its description carries three or four detectable waypoints (entry, pivot, objective). Its required data source (RDS) and required signal source (RSS) fields carry the sources a defensive cyber operator must hold to see that traversal.

> **The Gate.** The published definition of an attack path is "Confirmed attack path for a converged space system." (MISP meteorstorm taxonomy v2, AN-ATT). In this course it is written as a traversal: three waypoints, four at most, each observable, anchored to the driving threat's TOE and stating what a defensive cyber operator must hold to see it. An element the adversary only passes through, with nothing to see, is dropped rather than listed. A path that cannot name its anchor is not landing on its threat, and a path whose two source fields are both empty cannot be detected at all.

The eight steps, fixed order

1. **Enumerate the LAYER.** LAYER = AN, fixed. An attack path is analysis about the platform, not a part of it.
2. **Identify the source.** Adversary-behavior catalog (MITRE ATT&CK, MITRE ATLAS, SPARTA), internal red-team report, architecture review, or peer-shared attack-path documentation. Record confidence honestly alongside it: High where the pattern is directly reported, Medium where it is technically grounded but per-operator or on-orbit specifics are not public. The SOURCE field itself records only observable or synthetic; all four Kestrel paths are observable, and the reporting is cited in the description.
3. **Set the TAG to ATT.** These are the routes that realize the threats, not the threats themselves and not yet detections.
4. **Assign the ORDINAL.** Each path keeps the ordinal of the threat it realizes: 00, 01, 02, 03. One number carries one chain from threat to path to Day 4's signature and Day 5's measure. The register opened this week, so today's paths 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 TOE.** One enumerated platform element: the element this path is anchored to, and it is the same element the AN-THR this path realizes names. One element, never a list, never the route. The anchor says what the path is about; where the adversary goes is the next step. The chain then holds: Day 4 watches this element and Day 5 hardens it.

© 2026 ethicallyHackingspace (eHs)®

6. **Write the DESCRIPTION.** The traversal, entry to objective, as three waypoints, four at most: each a fully qualified element where the adversary must act in a way a detection can observe. A fourth is earned only by a second pivot crossing a trust boundary the first did not, such as a hop from the ground enclave into the link. Elements passed through with nothing observable are dropped. **The objective is where the route lands, and it need not be the anchor**: path 00 is anchored to the ground command-acceptance service its threat names and lands on the patch pipeline. Close with the source citation.
7. **Enumerate the RDS, the required data sources.** Walk the traversal again. Wherever the adversary's action would leave a record, name the one data source a defensive cyber operator must hold to see it. Each becomes an RDS record of four fields: a sub-ordinal counted from **00**, a name, the one element it is observed on, and a state. Where the path leaves no records at all, the field is an empty list, which is an answer.
8. **Enumerate the RSS, the required signal sources.** Walk the same traversal for observables that live in the physical layer rather than in a record: noise floor, carrier-to-noise ratio, lock status, received power. Each becomes an RSS record carrying the same four fields, counted from **00** in its own sequence. Where the path produces no physical observable, the field is an empty list. If both fields are empty, the path as written cannot be detected, and that is a finding to record rather than a blank to leave.

Repeat for the next attack path. When every cataloged threat has at least one realizable path enumerated, with both source fields answered, the AN-ATT enumeration is current.

The second deliverable: the required-source inventory

Function 03 has two deliverables and the second is the one teams drop: the path catalog, and the inventory of what a defensive cyber operator must be holding to see each path. The inventory is not a separate document traveling beside the element. Steps 07 and 08 put it **on** the element, in two fields, which is what makes it countable, ownable and auditable instead of a paragraph somebody wrote once.

Field	What it holds	Why it is its own field
RDS	The required **data** source: what must be received as a record. A log, an audit stream, an inventory, a telemetry feed.	Records are written by something that can be turned off, filtered or never onboarded. The field states what must be received, not what happens to arrive today.
RSS	The required **signal** source: what must be measured in the physical layer. A noise floor, a carrier-to-noise ratio, a lock status, a received power level.	A physical measurement is not a record and never becomes one. Jamming is seen in the noise floor and is never seen in a log.

The two fields stay separate because they are separate kinds of observable, the same line the structural taxonomy draws at the asset layer between AST-DA Data and AST-SI Signal. One generic "source" field cannot express attack path 02 honestly: its RDS field is empty, and everything the inventory lists to reveal it is a measurement.

© 2026 ethicallyHackingspace (eHs)®

What one record carries

- **The sub-ordinal.** RDS:00, RDS:01, RSS:00. Two digits counted from 00, per field, per path. **It is a separate counter from the element's own ordinal and never increments with it**: AN:ATT:Attack Path:03 carries RDS:00, and the 03 and the 00 are unrelated numbers. RDS and RSS count independently of each other.
- **The name.** Specific enough that a defensive cyber operator could requisition it. "Signed-manifest verification record", not "logs".
- **The one element it is observed on.** One enumerated platform element, never a list. It is usually a waypoint, and it does not have to be: a source is recorded on whichever element emits it, even one the route only passes beside.
- **The state.** One of four, below.

The four states

State	Means	What it obliges
Available	The Security Operations Center (SOC) already receives or measures it.	Record the source identifier, so Day 4 can author against it immediately.
Partial	Held, but not at the fidelity, retention or coverage the path needs.	Record what is short: the field, the retention window, or the subset of hosts covered.
Gap	Assessed, and absent. Nothing is being collected or measured that would show this.	Record what would have to be collected to close it, and name the owner.
unassessed	The owning department has not yet returned a state.	Chase the owner. It is not a coverage state and never counts as one.

> **unassessed is not Gap, and the difference is the point.** Gap means somebody looked and there is nothing there. unassessed means nobody has looked yet. Collapse the two and you report a platform as blind where nobody has checked, and as covered where nobody has answered. Most of the Day-3 record is still unassessed at close of day, and printing it that way is the honest state of the work, not a defect in it.

Choosing the required source when a step emits several

Real services emit more than one candidate source, so the selection rule matters as much as the step. In order:

- **Closest to the adversary's action.** Prefer the source that records or measures the act itself over one that shows a downstream consequence.
- **Hardest for the adversary to suppress.** A log the adversary controls once they hold the host is worth less than one written elsewhere.
- **Already onboarded over newly collected.** A source the Security Operations Center already receives can carry a signature tomorrow; one that needs new collection cannot.

© 2026 ethicallyHackingspace (eHs)®

There is no separate exhaustive per-step inventory. One required source per observable step is the deliverable, because Day 4 writes one signature per path and reads its required sources to decide what that signature watches and what its analyst corroborates. A list of every candidate means the choice has not been made.

> **Coverage gaps are recorded, not hidden.** A step whose required source does not exist is a declared coverage gap: it still takes a sub-ordinal, an element and the state Gap, it is assigned an owner, and it is handed to engineering as work to close. That is what makes a gap countable rather than a sentence in a chapter. An element the adversary only passes through, with nothing observable and nothing to gain from watching, is dropped from the route instead. The difference is whether the platform should be able to see it: a chokepoint you cannot see is a gap, a corridor you do not need to see is noise.

Why converged detection engineering exists

CNSSI 1200 (Committee on National Security Systems, August 2025), implementing CNSSP No. 12, requires on-board intrusion detection and prevention capable of real-time monitoring for space systems used to support national security missions. A detection built on records alone cannot see a path like 02, whose required sources are all measurements; that is why the method forces every waypoint to declare whether it can be seen, and in which field.

CH 4 The Catalog, Complete

> "Four attack paths walked: one per threat, each naming the entry, pivot, and objective the attacker would cross, each citing the reporting it is anchored to."

How to read each entry. Each path prints twice over. The first table is the element: its anchor, then the three waypoints in order, which are description content. The second table is the required-source inventory carried on that same element, one row per RDS or RSS record, with the element it is observed on and its state. Read the two together: the first says where the adversary goes, the second says what you must be holding to see them go there. Where a paragraph names the full traversal, it lists the further elements the adversary crosses that were dropped as unobservable or unnecessary to watch, so the difference between the traversal and the waypoints is visible. Source and confidence carry the honest limit of the public record.

> **Most states here read unassessed, and that is the record.** Day 3 enumerates what a defensive cyber operator *must* hold. Whether Kestrel holds it is a question for the department that owns each element, and at close of day most of those answers have not come back. Twelve required sources are enumerated across the four paths. Four are assessed: two Available with their source identifiers, one Partial with the reason, one Gap with its owner. The other eight are waiting on an owner, and they are written that way rather than guessed.

© 2026 ethicallyHackingspace (eHs)®

GROUND · 2 AN-ATT

AN:ATT:Attack Path:00 · Unauthorized firmware push through ground command acceptance

An adversary enters at the ground crypto service, pivots through the ground command-acceptance service, and pushes unauthorized firmware through the patch deployment pipeline.

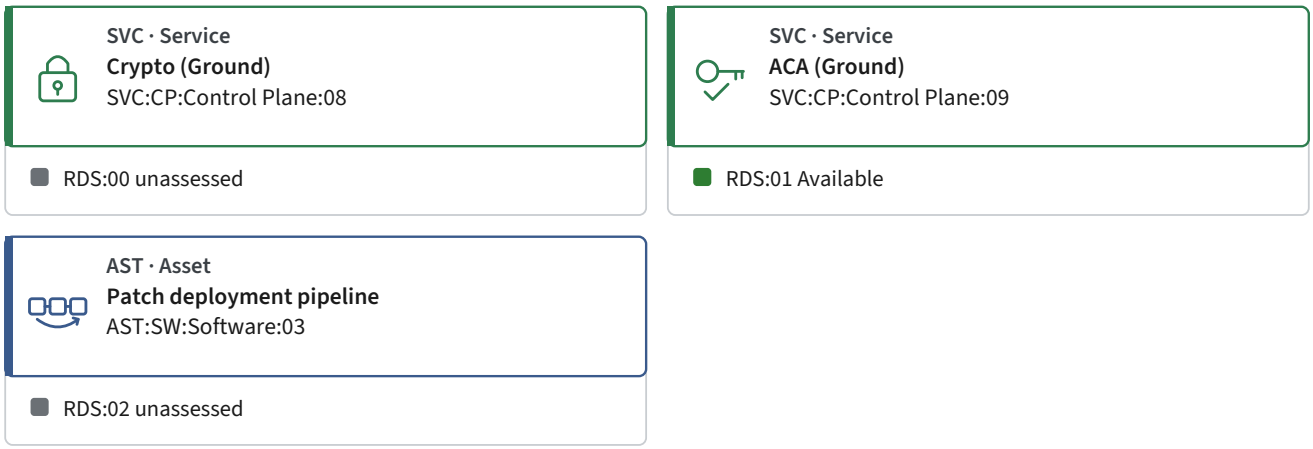
Waypoint	Element	What it is on this path
TOE (anchor)	**SVC:CP:Control Plane:09**	The ground command-acceptance service. The one element this path is anchored to, taken from AN:THR:Threat:00. Day 4 watches it and Day 5 hardens it.
Entry	**SVC:CP:Control Plane:08**	Ground crypto, reached from the management network.
Pivot	**SVC:CP:Control Plane:09**	Ground command acceptance, where the firmware push is released through the management plane. Also the anchor.
Objective	**AST:SW:Software:03**	The patch deployment pipeline that builds, signs, distributes, and installs the pushed image.

Record	Required source	Observed on	State
RDS:00	Management-network remote-access record	**SVC:CP:Control Plane:08**	unassessed
RDS:01	Management-plane firmware-push operation record	**SVC:CP:Control Plane:09**	Available, src-ground-aca-010
RDS:02	Patch deployment pipeline deployed-image hash record	**AST:SW:Software:03**	unassessed

> **Field note**
>
> The SOC opened with full kill chains, every host and hop an adversary would touch. Satellite Design and Engineering pushed back: most of those hops log nothing, so a path written that way cannot be watched. Ruling: three waypoints, four at most, and the required sources go on the element as RDS and RSS records rather than into the prose beside it. First win: Day 4 authors signatures against a short list of named records instead of a route no sensor covers.

© 2026 ethicallyHackingspace (eHs)®

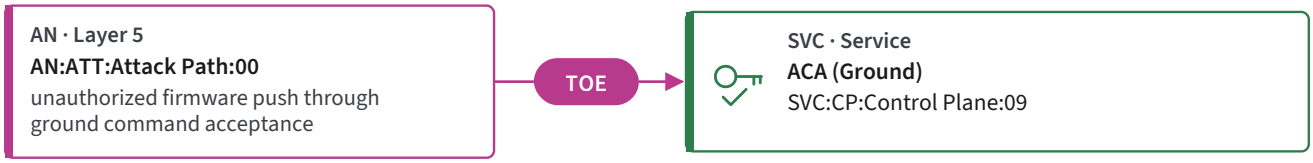
Figure 1 The required sources as icons, by the element each is observed on



Each platform element with the required sources observed on it, and each source's state.

Read the empty RSS field. This path carries no required signal source. Every step it takes is a ground operation, and each one leaves a record, so the field is empty by answer, not by omission. A required source names the element it is measured or received on, which is often a waypoint and is not required to be one.

Figure 2 AN-ATT anchors · 1 of 4 entries · after AN:ATT:Attack Path:00



One path, one anchor. The attack path sits in Layer 5 and names one platform element through its **TOE** field, exactly as its threat did. The route it traces is in the entry table above, not in this figure, because the route is 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 point of the chain: AN:ATT:Attack Path:00 names the same element AN:THR:Threat:00 named, so the element on the right has not moved.

Driven by AN:THR:Threat:00 (Ground command-acceptance abuse through the management plane). **Source** Day-2 composite OSINT threat assessment, through AN:THR:Threat:00. **Confidence** Medium: the route is reconstructed from the Day-1 inventory; per-operator specifics are non-public.

Full traversal behind the waypoints. Entry into the ground segment (**SEG:GR:Ground:00**) through the ground crypto service, release of a firmware push through the ground command-acceptance service, the patch binary store (**AST:DA:Data:02**) holding the staged image, and the patch deployment pipeline (**AST:SW:Software:03**) installing it. The binary store was not made a waypoint: it is corridor, not chokepoint, for this path, so no required source is enumerated against it here.

© 2026 ethicallyHackingspace (eHs)®

AN:ATT:Attack Path:01 · Command-authority compromise

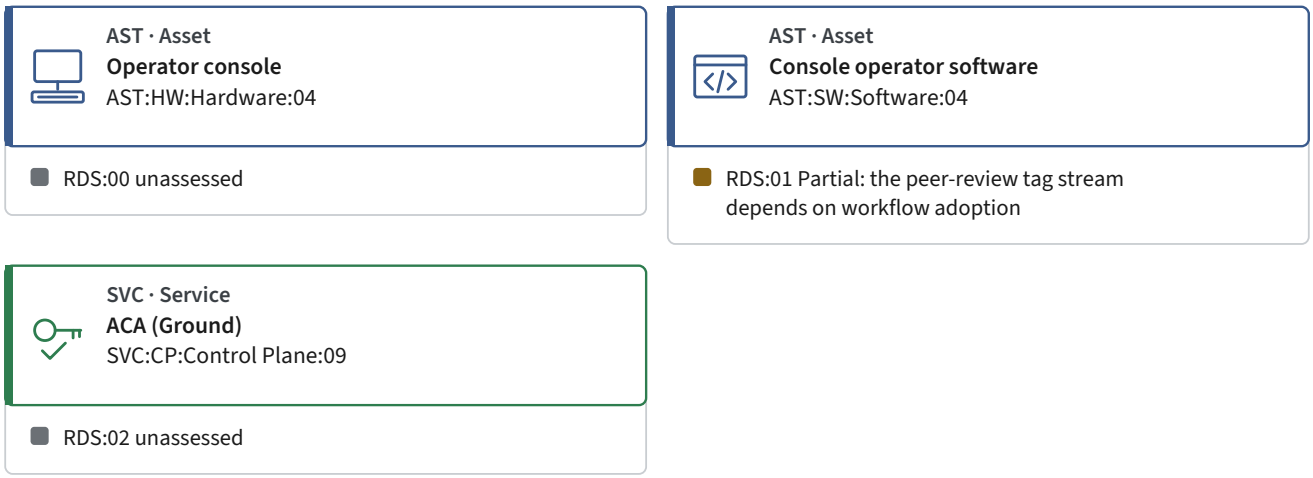
An adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite directly from a commanding workstation, bypassing peer review.

Waypoint	Element	What it is on this path
TOE (anchor)	**AST:SW:Software:04**	The console operator software. The one element this path is anchored to, taken from AN:THR:Threat:01. Day 4 watches it and Day 5 hardens it.
Entry	**AST:HW:Hardware:04**	The commanding workstation the adversary signs in at.
Pivot	**AST:SW:Software:04**	The console software, where command authority is exercised. Also the anchor.
Objective	**SVC:CP:Control Plane:09**	Ground command acceptance, where the unreviewed command is released to the link.

Record	Required source	Observed on	State
RDS:00	Operator console session record, host and sign-in time	**AST:HW:Hardware:04**	unassessed
RDS:01	Command-authority usage record carrying the peer-review tag	**AST:SW:Software:04**	**Partial: the peer-review tag stream depends on workflow adoption**
RDS:02	Control-plane command release record with review state	**SVC:CP:Control Plane:09**	unassessed
RSS	*none.* Everything that would reveal this path arrives as a record. Nothing about an unauthorized telecommand issued under stolen or coerced command authority is visible in the physical layer, so the field is an empty list, which is an answer rather than an omission.		

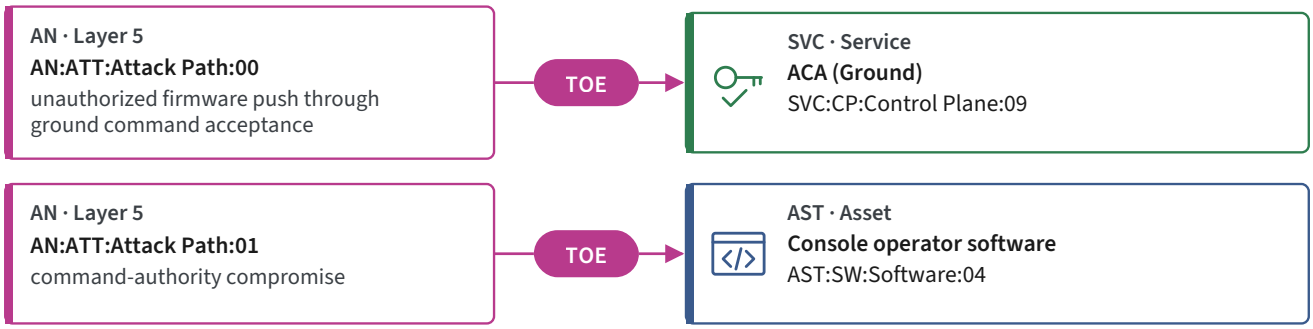
© 2026 ethicallyHackingspace (eHs)®

Figure 3 The required sources as icons, by the element each is observed on



Each platform element with the required sources observed on it, and each source's state.

Figure 4 AN-ATT anchors · 2 of 4 entries · after AN:ATT:Attack Path:01



The second path anchors to an asset, so its card reads AST · Asset, in the asset color. Two paths, two layers, and in both cases the anchor is inherited from the threat rather than chosen fresh.

What you do not choose. The anchor is not an authoring decision on Day 3. It is fixed by Day 2. If you find yourself picking a different element, either the path realizes a different threat than you think, or the threat was anchored wrong and that is a Day 2 defect to raise.

One element, two paths. SVC:CP:Control Plane:09 is the pivot and anchor of Path 00 and the objective of this path, and it carries a required data source on each. It is the one element that appears on more than one path in this catalog.

Driven by AN:THR:Threat:01 (Command-authority compromise). **Source** MITRE ATT&CK T1078 (Valid Accounts); SPARTA; insider-threat reporting. **Confidence** Medium: the pattern is widely reported, per-operator specifics are not.

© 2026 ethicallyHackingspace (eHs)®

LINK · 1 AN-ATT

AN:ATT:Attack Path:02 · Sustained RF noise injection on the telecommand uplink waveform

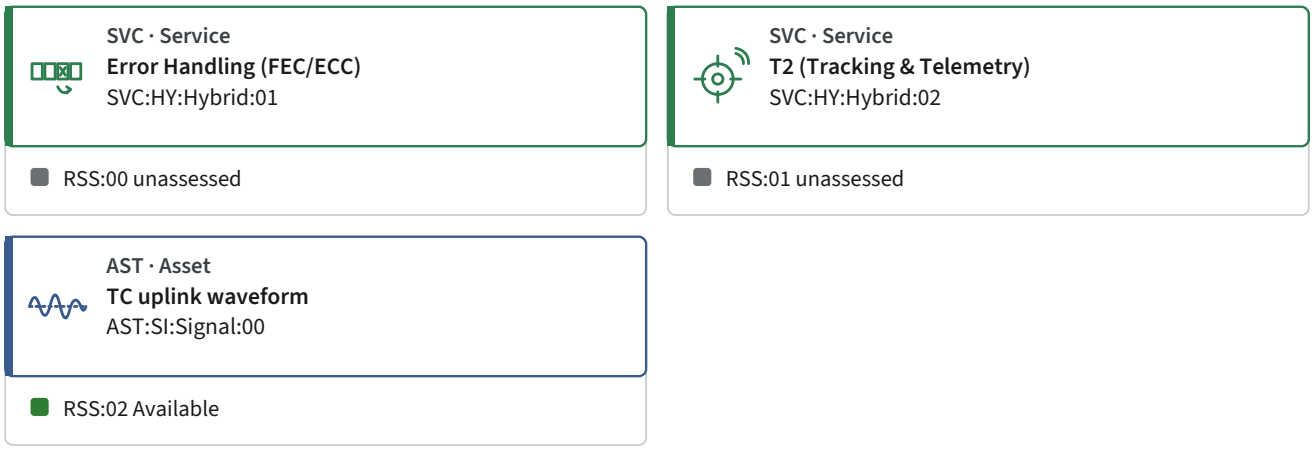
Sustained RF noise injection on the telecommand uplink waveform to deny communications, optionally timed to overhead passes.

Waypoint	Element	What it is on this path
TOE (anchor)	**AST:SI:Signal:00**	The telecommand uplink waveform. The one element this path is anchored to, taken from AN:THR:Threat:02. Day 4 watches it and Day 5 hardens it.
Entry	**SVC:HY:Hybrid:01**	The first place the platform can see the attack: corrected bit and frame errors climbing on the uplink.
Pivot	**SVC:HY:Hybrid:02**	Tracking, as the noise floor rises across the link.
Objective	**AST:SI:Signal:00**	The waveform itself, where the link loses lock. Also the anchor.

Record	Required source	Observed on	State
RDS	*none.* The inventory lists no record for this path. There is no login, no command, no file. An empty RDS field is the honest answer here, and it is the reason the two source fields are kept apart: a single generic source field would force this path to be described as a record source it does not have.		
RSS:00	Uplink corrected bit-error and frame-error rate measurement	**SVC:HY:Hybrid:01**	unassessed
RSS:01	Link noise-floor and carrier-to-noise measurement	**SVC:HY:Hybrid:02**	unassessed
RSS:02	Receiver lock status and link-outage measurement	**AST:SI:Signal:00**	Available, src-rx-rf-024

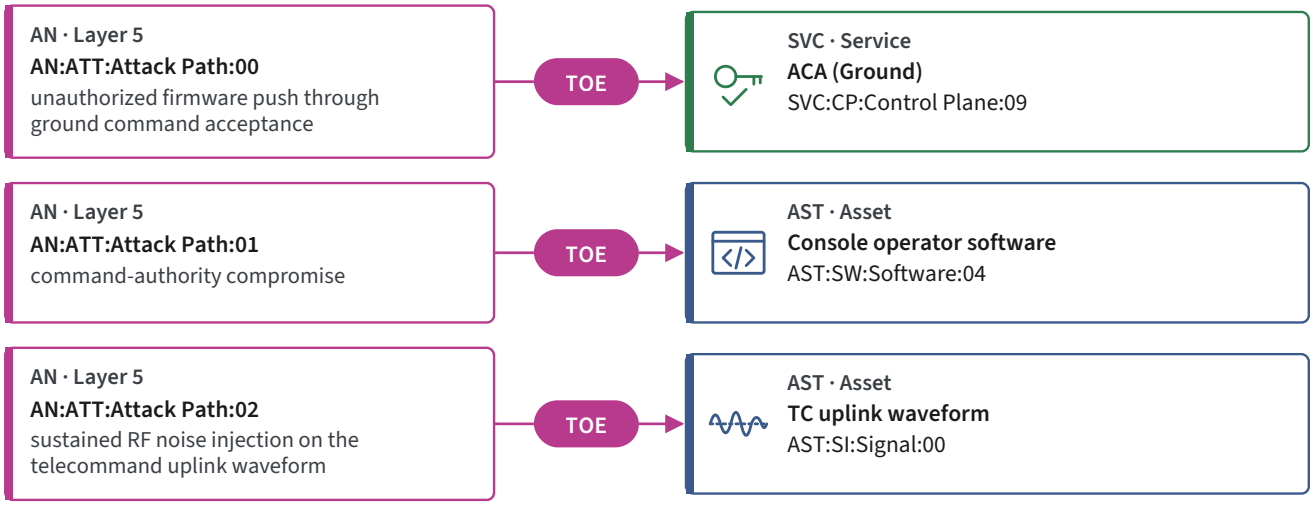
© 2026 ethicallyHackingspace (eHs)®

Figure 5 The required sources as icons, by the element each is observed on



Each platform element with the required sources observed on it, and each source's state.

Figure 6 AN-ATT anchors · 3 of 4 entries · after AN:ATT:Attack Path:02



The link path joins. Its objective waypoint and its anchor happen to coincide here, which is common and is not a rule.

Coincidence, not constraint. On paths 02 and 03 the route ends on the anchor. On paths 00 and 01 it does not. The objective is where the route lands, and it need not be the anchor.

Where the three measurements are observed. The inventory places each on one enumerated element: RSS:00 on the error-handling service (**SVC:HY:Hybrid:01**), RSS:01 on the tracking and telemetry service (**SVC:HY:Hybrid:02**), and RSS:02 on the telecommand uplink waveform (**AST:SI:Signal:00**). All three are Link elements on the Day-1 CONOPS. The inventory names the element and goes no further: it does not say on which side of the link a reading is taken.

Driven by AN:THR:Threat:02 (Jamming campaign). **Source** SPARTA; public RF-interference reporting. **Confidence** High: RF interference is well documented against SATCOM.

© 2026 ethicallyHackingspace (eHs)®

Also touched, not a waypoint. The link Access Control and Authentication service, ACA (Link) (**SVC:CP:Control Plane:05**) sees authentication outcomes degrade as the link deteriorates. That is a consequence of the jamming rather than the jamming itself, and the selection rule prefers the source closest to the act, so it is not enumerated as a required source on this path.

> **Field note**
>
> There is no door to walk through on an RF path, so "entry" was argued. Satellite Operations settled it: the entry is the first place the platform can see the attack, the climb in corrected bit errors on the uplink. Ruling: waypoints are defined by observability, not by where the adversary stands. Second ruling, the one that carried the day: this path has an empty RDS field and three RSS records, and writing it any other way would have hidden the fact that no required source on this path is a log.

SPACE · 1 AN-ATT

AN:ATT:Attack Path:03 · Malicious on-orbit firmware update

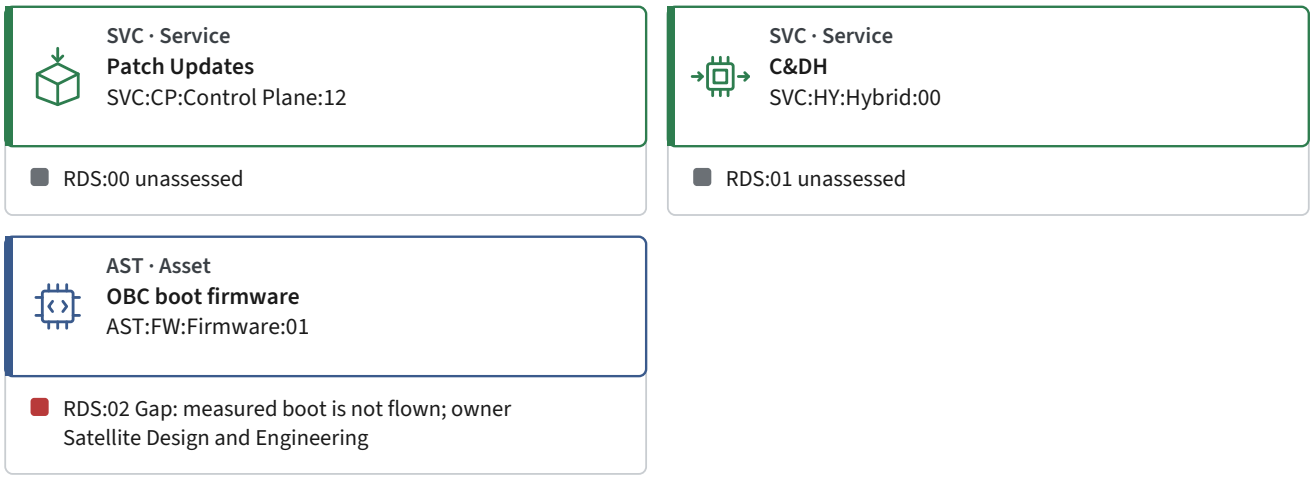
An adversary subverts the flight-software update supply chain and pushes a backdoored firmware update to the operational satellite over the command-and-update path, where it runs in orbit.

Waypoint	Element	What it is on this path
TOE (anchor)	**AST:FW:Firmware:01**	The on-board computer boot firmware. The one element this path is anchored to, taken from AN:THR:Threat:03. Day 4 watches it and Day 5 hardens it.
Entry	**SVC:CP:Control Plane:12**	The patch update service the tampered image is pushed through.
Pivot	**SVC:HY:Hybrid:00**	C&DH on board, where the signed manifest is checked when the update is accepted.
Objective	**AST:FW:Firmware:01**	The boot firmware, where the backdoored image runs in orbit. Also the anchor.

Record	Required source	Observed on	State
RDS:00	Update-push activity record on the patch update service	**SVC:CP:Control Plane:12**	unassessed
RDS:01	On-board signed-manifest verification record	**SVC:HY:Hybrid:00**	unassessed
RDS:02	Boot-time firmware measurement and attestation record	**AST:FW:Firmware:01**	**Gap: measured boot is not flown; owner Satellite Design and Engineering**
RSS	*none.* A firmware image running in orbit changes nothing a radio can measure. The path is entirely a records problem, and the record that matters most is the one the platform does not produce.		

© 2026 ethicallyHackingspace (eHs)®

Figure 7 The required sources as icons, by the element each is observed on



Each platform element with the required sources observed on it, and each source's state.

The sub-ordinal is not the element's ordinal. This is AN:ATT:Attack Path:03 and its first required source is RDS:00. The 03 belongs to the chain, threat to path to signature to measure. The 00 counts records inside one field of one element. They never move together, and a reader who assumes they do will misread every path in this catalog.

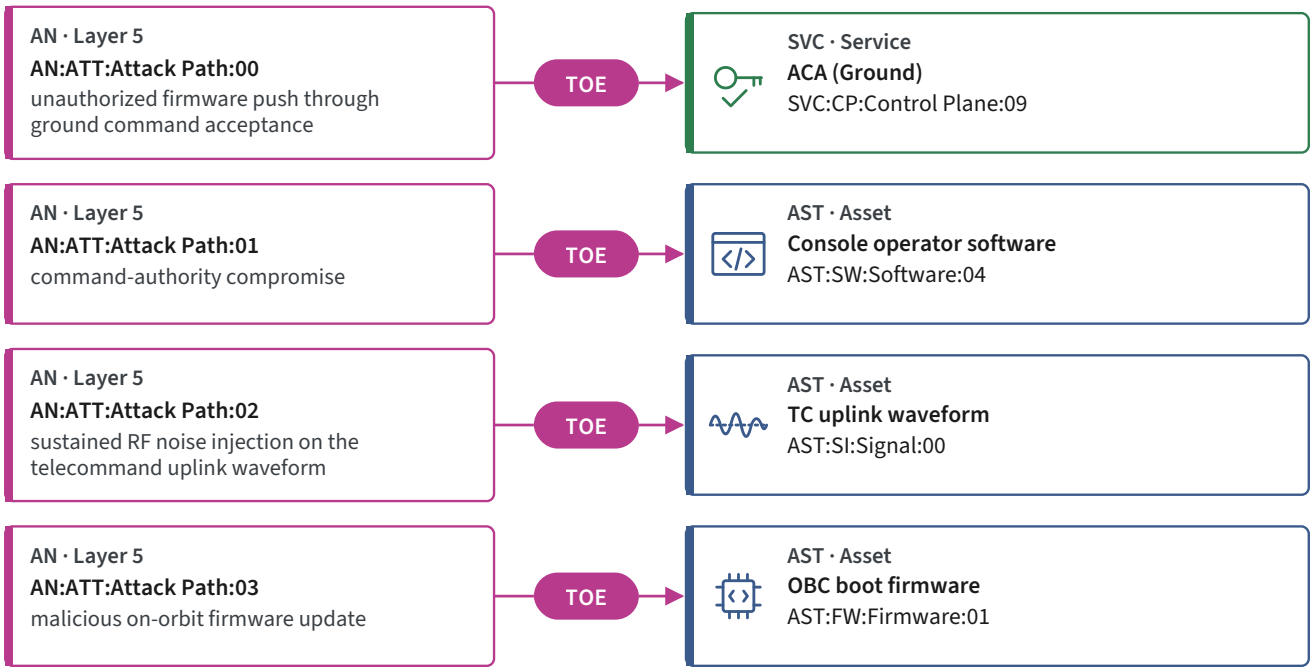
Driven by AN:THR:Threat:03 (Malicious on-orbit firmware update). **Source** SPARTA IA-0001 (Compromise Supply Chain); software-supply-chain security guidance. **Confidence** Medium: technically grounded; specific on-orbit incidents not publicly disclosed.

Also touched, not a waypoint. The same command-and-update path can deliver a tampered image to the repeater firmware (**AST:FW:Firmware:02**). The on-orbit objective was set at the OBC firmware because that is the element the Day-2 threat names, so the repeater carries no required source on this path.

> **Field note**
>
> RDS:02, a boot-time firmware measurement, assumes attestation the platform does not yet fly. The easy move was leaving the field short; Satellite Design and Engineering refused to let the path end on nothing. Ruling: the required source is enumerated anyway, given a sub-ordinal, an element and the state Gap, with Satellite Design and Engineering as its owner. First win: when Day 5 proposes measured boot, the justification is already a counted record instead of an argument made from scratch.

© 2026 ethicallyHackingspace (eHs)®

Figure 8 AN-ATT anchors · 4 of 4 entries · the complete Day-3 attack-path anchor map



Four paths, four anchors, and the same four elements Day 2 produced. This figure and the Module 02 figure are identical on the right-hand side, which is what a working chain looks like.

What the chain buys Day 4. Tomorrow you write one signature per path, and you already know which element each one watches: the element on the right. No lookup, no cross-reference table, no negotiation about what the signature is for.

A four-waypoint path, worked

All four paths today need three waypoints, so the fourth-waypoint rule is easy to misread as decoration. Here is what earns one. Suppose an adversary compromises the operator workstation, pivots into the ground command-acceptance service, and then, using that release authority, reaches the Kiruna ground terminal to inject crafted frames into the uplink waveform. That crosses two distinct trust boundaries: from the console into command release, and out of the Reston enclave to the Kiruna ground terminal that radiates into the link. The path is:

Waypoint	Element	Boundary crossed
Entry	**AST:HW:Hardware:04**	into the operator console
Pivot 1	**SVC:CP:Control Plane:09**	into command release
Pivot 2	**SVC:HY:Hybrid:03**	from the Reston enclave into the Kiruna enclave, at the ground terminal that radiates
Objective	**AST:SI:Signal:00**	none; this is where the route lands

© 2026 ethicallyHackingspace (eHs)®

The second pivot is earned because the first stayed inside the Reston enclave, and the crossing to the Kiruna terminal is separately observable. Two pivots inside the same enclave would not earn it: they would be one pivot with extra detail, and the extra detail belongs in the traversal, not the waypoints. The example shows a route only. It realizes none of the four Day-2 threats, so it carries no anchor: before it could be enumerated as an **AN-ATT**, Function 02 would have to enumerate the threat it realizes, and the path would take that threat's TOE.

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

> "Satellite Design and Engineering spent the day writing in the language it helped build, and the other two departments can read every path without a briefing."

The three readings. The Security Operations Center reads the **RDS** and **RSS** records to know what to collect, what to measure and what it is still waiting on an answer for. Satellite Operations reads the waypoints to know which live services carry a traced route during a contact window. Satellite Design and Engineering reads the **Gap** records as engineering work with an owner and a date. A state on each record still marked **unassessed** is owed by the department that owns the element it is observed on.

One outage, two observations. The module opens on one outage seen two ways. Satellite Operations sees the spacecraft's uplink noise floor rise and its receiver lock fall in telemetry, each sampled continuously. Security Operations sees a healthy event stream, because Path 02 carries no record at all. Both observations are valid, and no shared identifier joins them. The two sides do not share a clock discipline either: a record is stamped when the writing host says it happened, not when the effect appeared on the link. Jamming and weather produce the same reading in a single sample, and no record on this path separates them.

The join. The tempting fix was to invent a correlation identifier and require every source to carry it. It was refused, because nothing on this platform emits one today, so requiring it would produce a design nobody could implement. The ruling is to correlate on the enumerated element: every required source already names exactly one, so the element is the join, and time is a filter applied after it. Each source states its time base and known offset, so a comparison across sources is a stated window. Where a path carries both a data source and a signal source, it names the expected pairing. On this pass none does: Paths 00, 01 and 03 carry records only and Path 02 carries measurements only.

Sharing the analysis. Written in the shared form, the paths read the same to all three departments, and they are the kind of analysis the organization's Space ISAC channel exists to exchange. A peer operator receiving Attack Path 00 gets the anchor, the waypoints, the required sources with their states, the source, and the confidence, which for Path 00 is Medium because the route is reconstructed from the Day-1 inventory, and can line it up against its own decomposition without a translation step.

Presenting it back. You walk the three departments through the catalog segment by segment: the platform first, then each segment with its paths, then the full picture. What the departments confirm in that session is what Day 4 builds on.

© 2026 ethicallyHackingspace (eHs)®

Your role in Function 03

Detection engineering is the third of the five functions where a Full Spectrum professional drives change, and you do not have to be the detection expert or the spacecraft engineer to lead it. Security Operations, Satellite Operations, and Satellite Design and Engineering can sometimes be provided by separate organizations, so your job is to build the cross-functional team and converge their data and signals into shared detections. That is what makes this function a deliberate point of insertion for transforming how those organizations defend the platform together.

CH 6 Tag and Share

> “The taxonomy is already deployed and your threats are already tagged. Today you tag your four attack paths.”

> **TAG** `meteorstorm:AN="AN-ATT"`

In MISP the path is held as one event carrying that tag, and each required source is an attribute on the event, with the element it is observed on and its state written beside it. A peer SOC can follow the chain step by step in the same element names, and line it up against its own platform on sight. What travels with a shared path is the whole record: the identifier, the driving threat, the anchor, the waypoints in order, every **RDS** and **RSS** record with the element it is observed on and its state, the source, and the confidence with its stated limit. Sending the required sources with their states is what lets a peer answer the only question that matters on receipt, whether they could see this happen on their own platform. The confidence field is what makes the exchange honest, because a peer needs to know whether they are receiving a route reconstructed from an enumerated inventory or a technically grounded projection.

© 2026 ethicallyHackingspace (eHs)®

CH 7 Use This at Work

This workbook teaches Function 03 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 03 walks each threat into an attack path and records, on the element the path is anchored to, the data sources and the signal sources a defensive cyber operator must hold to see the traversal happen. 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 **Bring the six questions to engineering.** Find whichever documents answer them; the question each artifact answers stays constant, not the document itself.
What you gain: the platform as it was actually built, which walking a threat into a real route needs.
Chapter 2, the artifact table, third column

02 **Apply the gate to one path before you write it.** It must name its anchor, and at least one of its two source fields must hold a source.
What you gain: a path that cannot name its anchor is not landing on its threat, and a path with both source fields empty cannot be detected at all, so you find both failures before anyone builds on them.
Chapter 3, The Gate · desk pack sheet 08, Function 03 Converged Detection Engineering: method card

03 **Record the source and state the confidence honestly.** High where the pattern is directly reported, Medium where it is technically grounded but the specifics are not public.
What you gain: a reader knows whether the route is reconstructed from an enumerated inventory or is a technically grounded projection.
Chapter 3, step 02, and Chapter 6 · desk pack sheet 09, Function 03: attack path sheet

04 **Anchor the path to one enumerated element.** It is the same element the threat this path realizes names: one element, never a list, never the route.
What you gain: the chain holds, because the detection signature watches this element and the resilience measure hardens it.
Chapter 3, step 05 · desk pack sheet 09, Function 03: attack path sheet

05 **Write the traversal as three waypoints, four at most.** Entry, pivot, objective, each a fully qualified element where the adversary must act in a way a detection can observe. Drop any element passed through with nothing observable.
What you gain: Satellite Operations can read the waypoints to know which live services carry a traced route during a contact window.
Chapter 3, step 06 · desk pack sheet 09, Function 03: attack path sheet

© 2026 ethicallyHackingspace (eHs)®

06 **Name the required data sources.** Walk the traversal again; wherever the adversary's action would leave a record, name the one data source that must be held to see it, with its sub-ordinal, the one element it is observed on and its state.

What you gain: the field states what must be received, not what happens to arrive today, and a known technique that crosses a step where a source is Available is seen.

Chapter 3, step 07, and What one record carries · desk pack sheet 09, Function 03: attack path sheet

07 **Name the required signal sources.** Walk the same traversal for what must be measured in the physical layer: noise floor, carrier-to-noise ratio, lock status, received power. If both fields are empty, record that the path as written cannot be detected.

What you gain: jamming is seen in the noise floor and never in a log, so the adversary cannot hide in the measurements a detection built on records alone would miss.

Chapter 3, step 08, and Why converged detection engineering exists · desk pack sheet 09, Function 03: attack path sheet

08 **Choose one required source for each observable step.** In order: closest to the adversary's action, hardest for the adversary to suppress, already onboarded over newly collected.

What you gain: the choice is made, so the detection signature has one named source to watch, and a log the adversary controls once they hold the host is not the one relied on.

Chapter 3, Choosing the required source when a step emits several · desk pack sheet 08, Function 03 Converged Detection Engineering: method card

09 **Give every record one of the four states, and keep unassessed apart from Gap.** Available, Partial, Gap or unassessed. Gap means somebody looked and nothing is there; unassessed means nobody has looked yet, so chase the owner.

What you gain: you do not report a platform as blind where nobody has checked, or as covered where nobody has answered.

Chapter 3, The four states · desk pack sheets 08 and 09

10 **Record every coverage gap; do not hide it.** A step whose required source does not exist still takes a sub-ordinal, an element and the state Gap, with what would have to be collected to close it and an owner.

What you gain: the gap is countable engineering work with an owner, and as gaps close the attacker must sacrifice stealth, use untested techniques, or withdraw.

Chapter 3, Coverage gaps are recorded, not hidden · desk pack sheet 09, Function 03: attack path sheet

© 2026 ethicallyHackingspace (eHs)®

Desk pack sheets for Function 03

Sheet	Use it to
Sheets 01 and 02, Quick reference	Read the layers, the tags and the identifier syntax without opening a workbook.
Sheet 08, Function 03 Converged Detection Engineering: method card	Apply the gate to each path, then run the eight steps in order.
Sheet 09, Function 03: attack path sheet	Write one attack path per record: its anchor, its waypoints, and its required data and signal sources with their states.
Path review checklist, on sheet 08	Check a path and its required sources before you present them.

Where the method is in this workbook

You need	Chapter and heading
The six questions to bring to engineering	Chapter 2, the artifact table, third column.
The gate	Chapter 3, The Gate.
The eight steps	Chapter 3, The eight steps, fixed order.
The fields of a required source	Chapter 3, The second deliverable: the required-source inventory, and What one record carries.
The four states, and what each obliges	Chapter 3, The four states.
The rules	Chapter 3, Choosing the required source when a step emits several, and Coverage gaps are recorded, not hidden. Chapter 4, A four-waypoint path, worked. Chapter 5, The join.
Four complete worked paths	Chapter 4, each with its waypoints and its required sources.
The tag that carries a path to a peer	Chapter 6.

© 2026 ethicallyHackingspace (eHs)®