FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

MODULE WORKBOOK · STUDENT EDITION

# Module 03 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.

## COPYRIGHT AND LEGAL NOTICES



| | |
|---|---|
| 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 2026-09-24 |
| CONTACT | www.d2teamcorp.org |

STUDENT EDITION

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

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

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

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

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

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

---

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

CONTENTS

PART I

# Orientation

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

## CH 1 THE DAY IN ONE PAGE

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 TOE to the elements 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.

IN THE CLASSROOM

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

| | |
|---|---|
| **THE WORKBOOK** | Chapter 3, The Source Records, and Chapter 4, The Four Paths. Take one of the four paths in Chapter 4. Walk three of its steps. At each step name the single source a defensive cyber operator must hold to see it, its kind, a record or a measurement, and its state: available, partial, gap, or not assessed. |
| **THE QUESTION SET** | Questions 1, 3 and 8 are worked and marked in the classroom, each answer given with its reason. The rest are yours. |
| **LESSONS LEARNED FROM THE MINUTES** | Open the Day 3 minutes at the decision register and read Item 01, What a path has to prove; Item 06, Records and measurements do not line up; Item 05, Path 03, and the gap the room chose to declare. The rule, the objection and the decision are taken from the record, not from the slide. |

**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 uplink command 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 FEC/ECC service where an RF power spike first shows, 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.

## 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."
>
> DEEP DIVE DECK, SLIDE 4 · DAY-3 SATELLITE DESIGN AND ENGINEERING WORKING SESSION

| 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 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: 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 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 vocabulary they helped build, and Day 2 produced a threat set written in that vocabulary rather than in security jargon. The artifacts open because the team asking already speaks the platform's language.

PART II

# The method and the catalogue

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

## CH 3 THE AN-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."
>
> DEEP DIVE DECK, SLIDE 7 · AN-ATT ENUMERATION PROCESS

**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 `RDS` and `RSS` fields carry the sources a defensive cyber operator must hold to see that traversal.

**The Gate.** "An attack path traversing enumerated platform elements toward a threat objective." ATT admits a traversal: three waypoints, 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.
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. Ordinals come from the running register that also tracks work outside today's scope, which is why a scoped set carries non-consecutive numbers.
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.
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 with a sub-ordinal counted from `00`, 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 three 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 catalogued 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 rooms drop: the path catalogue, 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: that path leaves no records at all, and everything that would reveal it is a measurement.

#### What one record carries

- **The sub-ordinal.** `RDS:00`, `RDS:01`, `RSS:00`. Two digits from 00, counted per field, per element. **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: path 00 requires a lock-status measurement on `AST:SI:Signal:00`, which its route never touches.
- **The state.** One of four, below.

**The four states**

| STATE | MEANS | WHAT IT OBLIGES |
|---|---|---|
| **Available** | The Security Operations Center 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.

There is no separate exhaustive per-step inventory. One required source per observable step is the deliverable, because Day 4 writes one signature per required source. 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

DHS Science and Technology reports an on-board detection gap: most satellite detection today is telemetry-based, and many cyberattacks cannot be seen through telemetry alone. DHS and Aerospace Corporation built an on-board intrusion-detection prototype, SpaceCOP, around malware-agnostic Indicators of Behavior to close it. Converged detection engineering targets exactly this gap, which is why the method forces every waypoint to declare whether it can be seen at all. (Source: Air and Space Forces Magazine, 19 November 2025.)

## CH 4 THE CATALOGUE, 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."
>
> DEEP DIVE DECK, SLIDES 10 THROUGH 13 · ATTACK PATHS: GROUND, LINK, SPACE · DAY-3 ENUMERATED ATTACK PATHS

**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, which the deck cannot show at a glance. 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. Thirteen 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 nine are waiting on an owner, and they are written that way rather than guessed.

GROUND · 2 AN-ATT

### AN:ATT:Attack Path:00 · Mass modem firmware-wipe via management-plane abuse

A state-sponsored actor reaches the SATCOM management network, abuses the legitimate modem management interface and the provider-to-customer trust relationship, and pushes a wiper as a firmware update, bricking the modem fleet (KA-SAT / AcidRain class).

| 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 | The management plane, where the firmware push is issued. Also the anchor. |
| Objective | AST:SW:Software:03 | The patch deployment software the wiper rides to the fleet. |

| 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 | Terminal-fleet firmware inventory and deployed-hash record | AST:SW:Software:03 | **unassessed** |
| RSS:00 | Fleet-wide carrier and demodulator lock status at the gateway | AST:SI:Signal:00 | **unassessed** |

**Read the RSS row twice.** RSS:00 is observed on AST:SI:Signal:00, an element this path never walks. A wiped modem fleet stops transmitting, and the fastest confirmation that the fleet is down is a measurement at the gateway, not a record on the ground. A required source names the element it is measured or received on, which is often a waypoint and is not required to be one.

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 box on the right has not moved.

**Driven by** AN:THR:Threat:00 (SATCOM management-network intrusion). **Source** CISA / FBI AA22-076 (KA-SAT / AcidRain) and the Viasat post-incident report of 30 March 2022; supporting public analysis in SentinelLabs' AcidRain write-up. **Confidence** Medium: KA-SAT is public, per-operator details are not.

**Full traversal behind the waypoints.** Compromise of an external VPN appliance facing the management network (SEG:GR:Ground:00), pivot into ground crypto with VPN-derived credentials, ACA issues subscriber-modem privileges, patch-deployment software stages the wiper, the patch binary store (AST:DA:Data:02) holds the payload, and the patch deployment software (AST:SW:Software:03) pushes it to the fleet as a firmware image. The VPN appliance and the binary store were not made waypoints: they are corridor, not chokepoint, for this path, so no required source is enumerated against them here.

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.

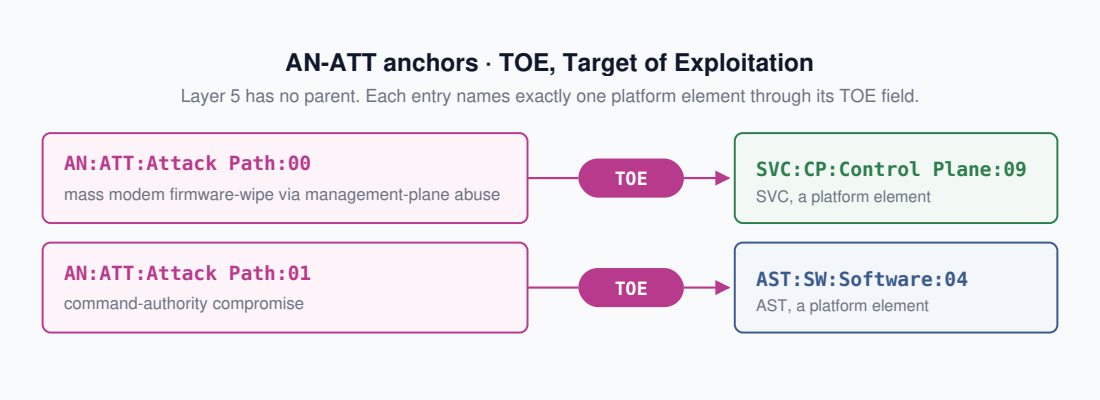
### AN:ATT:Attack Path:01 · Command-authority compromise

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 operator console 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:13 | The console service, where the unreviewed command is released. |

| 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:13 | **unassessed** |
| RSS | *none.* Everything that would reveal this path arrives as a record. Nothing about a legitimate operator issuing a legitimate command is visible in the physical layer, so the field is an empty list, which is an answer rather than an omission. | | |

AN-ATT ANCHORS · 2 OF 4 ENTRIES · AFTER AN:ATT:ATTACK PATH:01




The second path anchors to an asset, so it draws in blue. 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.

**Driven by** `AN:THR:Threat:01` (Command-authority compromise). **Source** MITRE ATT&CK (valid accounts, T1078.003) and SPARTA, with insider-threat reporting and NIST SP 800-53 PS-7 for the personnel control. **Confidence** Medium: the pattern is widely reported, per-operator specifics are not.

LINK · 1 AN-ATT

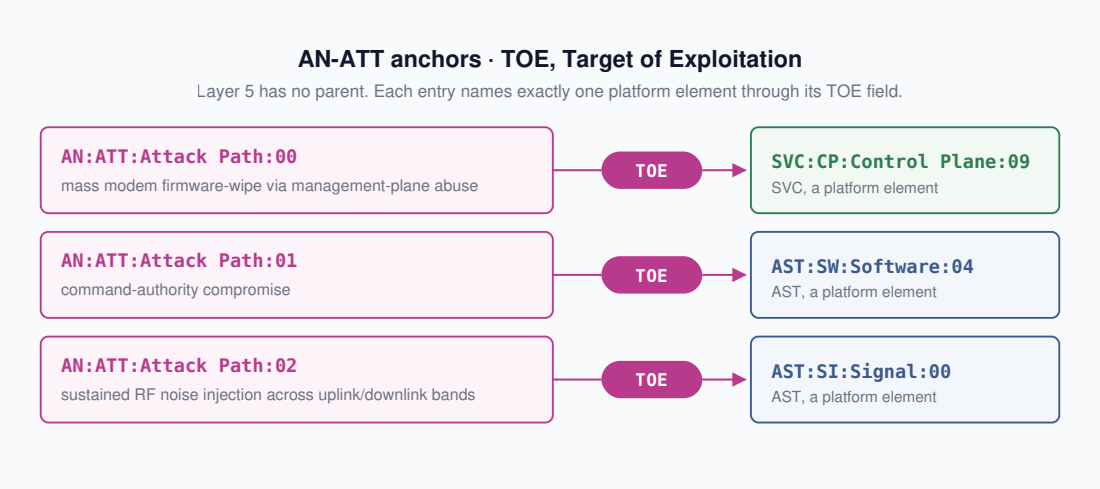
### AN:ATT:Attack Path:02 · Sustained RF noise injection across uplink and downlink bands

Sustained RF noise injection across the uplink and downlink bands to deny communications.

| WAYPOINT | ELEMENT | WHAT IT IS ON THIS PATH |
|---|---|---|
| **TOE (anchor)** | AST:SI:Signal:00 | the uplink and downlink waveforms. 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: the uplink band. |
| 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.* A jamming campaign writes nothing anywhere. 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 in a vocabulary it does not live in. | | |
| RSS:00 | Uplink-band received power 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** |

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. An earlier draft of this course taught that the objective must equal the anchor, and its own catalogue broke that rule twice. The rule is gone.

**Driven by** `AN:THR:Threat:02` (Jamming campaign). **Source** SPARTA and public RF-interference reporting, including reported jamming during the Russia and Ukraine conflict (2022 to 2024) and ITU interference reports. **Confidence** High: RF interference against SATCOM is well documented and directly reported.

**Also touched, not a waypoint.** The link access control authority (`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 power spike on the uplink band. 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 nothing here is ever going to appear in a log.

SPACE · 1 AN-ATT

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

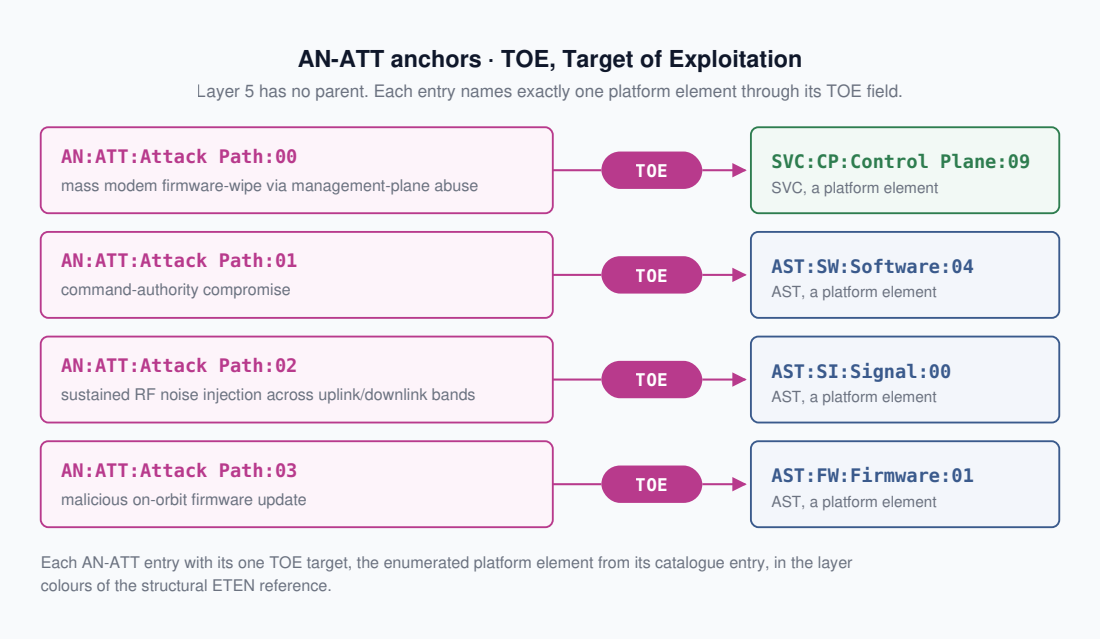
An adversary subverts the flight-software update supply chain and pushes a backdoored firmware update to the operational satellite over the command-and-update path, where it runs in orbit.

| 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:04 | The service the tampered update is pushed through. |
| Pivot | SVC:CP:Control Plane:02 | Where the signed manifest is checked at acceptance. |
| 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 thermal control service | SVC:CP:Control Plane:04 | **unassessed** |
| RDS:01 | Signed-manifest verification record | SVC:CP:Control Plane:02 | **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. | | |

**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 catalogue.

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 box on the right. No lookup, no cross-reference table, no negotiation about what the signature is for.

**Driven by** `AN:THR:Threat:03` (Malicious on-orbit firmware update). **Source** SPARTA (SPACE-T1041) and software-supply-chain security guidance, with the SolarWinds (2020, CISA AA20-352A) and CCleaner (2017) compromises as the terrestrial precedent. **Confidence** Medium: technically grounded, but no on-orbit incident of this class is 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.

### 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 a ground jump host, pivots into the management network, and then, using management-plane access to the modulator configuration, reaches the uplink chain to inject crafted frames at the waveform. That crosses two distinct trust boundaries: the office-to-management boundary and the ground-to-link boundary. The path is:

| WAYPOINT | ELEMENT | BOUNDARY CROSSED |
|---|---|---|
| Entry | `AST:HW:Hardware:04` | into the operational enclave |
| Pivot 1 | `SVC:CP:Control Plane:09` | into the management plane |
| Pivot 2 | `SVC:HY:Hybrid:01` | from ground into the link |
| Objective | `AST:SI:Signal:00` | none; this is the threat's TOE |

The second pivot is earned because the first did not cross the ground-to-link boundary, and that crossing 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.

PART III

# Putting it to work

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

## CH 5 WHO READS THE CATALOGUE

> "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."
>
> DEEP DIVE DECK, SLIDES 13 AND 19 · DAY-3 ENUMERATED ATTACK PATHS · DAY 3 COMPLETE

**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, and owes a state on every record still marked `unassessed`.

**Sharing the analysis.** Written in the shared form, the paths read the same to all three departments, and the strongest of them, like the KA-SAT reconstruction, are exactly the kind of runnable 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, and can line it up against its own decomposition without a translation step.

**Presenting it back.** You walk the three departments through the catalogue 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.

### 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.”
>
> DEEP DIVE DECK, SLIDE 17 · TAG THE ATTACK PATHS

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

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 reconstruction of a public incident or a technically grounded projection.

---