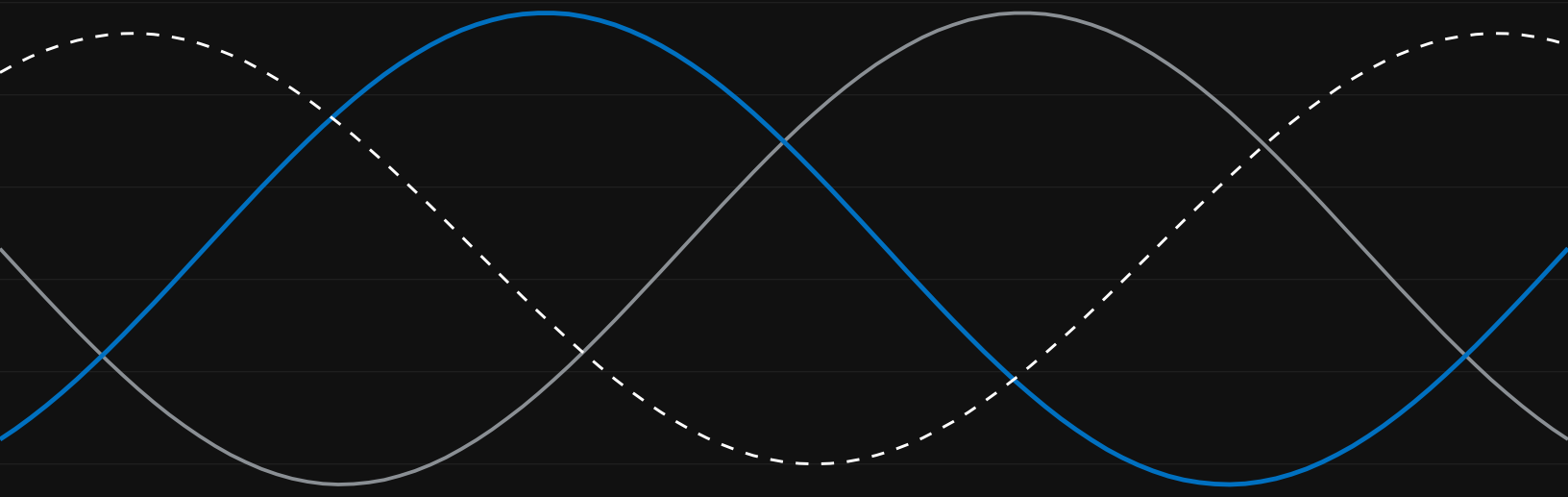
Module 02 · Workbook · Student edition

Contextualized Threat Modeling

The method behind the Day-2 threat catalog, and every entry it produced, each anchored to the one element it targets.



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 02 Contextualized Threat Modeling, 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 02 workbook for Contextualized Threat Modeling, METEORSTORM Function 02: 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 02 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 02 question set is a separate download; the answers to its questions are printed in it.

How to use this workbook

The Module 02 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 Contextualized Threat Modeling at Kestrel Orbital
Video 1	A report that names no element
Video 2	The gate
Part A	Run the gate
Video 3	Writing the threat record
Video 4	Four threats, four anchors
Part B and C	One element in the field
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** 5

CH 2 **Where Threat Intelligence Comes From** 6

The five source types 6

How to read an incoming report 7

CH 3 **The AN-THR Method** 7

CH 4 **The Catalog, Complete** 9

CH 5 **Who Reads the Catalog** 16

Presenting it back 16

CH 6 **Tag and Share** 17

CH 7 **Use This at Work** 18

Ten things to do at your work center 18

Desk pack sheets for Function 02 19

Where the method is in this workbook 20

What you will be able to do

We will be looking at threat anchoring so you can turn open threat reporting into a catalog of threats that each name the one platform element they would target.

O1	State why a threat report that names no element produces no work
O2	Apply the gate: one element in the TOE, or an exclusion with its reason
O3	Write an AN-THR record: the five ETEN fields, plus SOURCE and TOE
O4	State the Day 2 rulings and why an ordinal is never renumbered
O5	Read a threat entry in MISP and resolve it to its one element

The detail behind those objectives:

KNOWLEDGE

K1	The analytic layer and how an analytic element differs from a structural one: a finding anchored to a structural element, not an element of the platform.
K2	The Target of Exploitation field: it holds exactly one enumerated element, the one the threat is directed against, at the lowest layer the source resolves, and detection and resilience inherit it later.
K3	The five source types threat reporting arrives in, and what each is and is not good evidence for.
K4	The anchoring gate: a threat enters the catalog only when it can name an enumerated target, and is excluded on the record when it cannot.
K5	Register-issued ordinals, and the chain: one number carries a chain from threat to attack path to detection signature to resilience measure, and an ordinal issued once is never renumbered.

© 2026 ethicallyHackingspace (eHs)®

K6	Confidence and its reason: why a stated confidence with weak evidence is more useful than an unstated one.

SKILLS

S1	Read an incoming threat report and extract the behavior rather than the headline.
S2	Write a well-formed AN-THR identifier with a description that names the adversary behavior.
S3	Populate the Target of Exploitation with the one enumerated element the threat is directed against, and write the rest of its reach into the description.
S4	Apply the anchoring gate to a candidate threat and record the exclusion with its reason.
S5	State a confidence level and the evidence that sets it.
S6	Check a catalog for segment coverage and name where it is thin.

ABILITIES

A1	Turn a body of open reporting into an anchored catalog another department can act on, unprompted.
A2	Defend an exclusion to a department that wanted its threat in the catalog.
A3	Present the catalog back to the departments that supplied the platform inventory, in their terms.

TASKS

T1	Produce a threat catalog in which every entry names one enumerated target.
T2	Record at least one excluded candidate with the reason it failed the gate.
T3	Hand the catalog to detection engineering as the input its attack paths trace from.

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

Day 2 opens in the Security Operations Center (SOC), and this time the department is presenting, not being sold. Yesterday Satellite Operations and Satellite Design & Engineering reconciled their views into one Concept of Operations (CONOPS) of forty-four enumerated elements: 4 PCE, 4 SEG, 15 SVC, 21 AST. Today the SOC steps forward with the threat picture, and you enumerate adversary threats, cyber and electronic warfare, against those same elements. The environment is the PCE, not a threat.

What arrives. A composite open-source intelligence (OSINT) threat assessment of command-and-control attacks against the platform you defend lands on your desk. It walks the three operational enclaves (Space, Link, Ground), names the potential attacks each one currently faces, and lists the platform subsystems each attack would touch. More sources follow: the four external types in Chapter 2 and the SOC's own hunting.

What you build. Four AN-THR elements: 2 Ground, 1 Link, 1 Space, every one with a Target of Exploitation (TOE) naming exactly one element from yesterday's decomposition. No free-floating threats; nothing in the set that the platform is not actually exposed to. Chapter 4 prints the whole deliverable.

© 2026 ethicallyHackingspace (eHs)®

Why it matters to the mandates. The catalog feeds the risk analysis the NIS2 Directive requires under Article 21(2)(a), across the command-and-control scope Executive Order 14144 protects, and because every element is written as an ETEN in the five-field syntax Module 01 taught, with SOURCE and TOE added, it is ready for the policy-gated contribution to the Space ISAC Exchange the organization's own mandate requires.

What tomorrow consumes. Day 3, Converged Detection Engineering, picks up each threat's TOE and walks it into concrete attack paths and the data and signal sources that would reveal each step. A clean TOE today is a traceable path tomorrow: that is why the targeting step is the strictest of the six.

CH 2 Where Threat Intelligence Comes From

> "Threat intel comes from a range of sources."

The sourcing discipline. The exact mix of sources depends on the organization; every threat is sourced and cited to where it came from, which moves the organization off assumption-based defense and onto intelligence-driven, resilient operations. An uncited threat cannot be re-checked when the intelligence changes, cannot be weighed against a peer's report of the same activity, and cannot be defended in the risk analysis the mandates require. The source is what makes a threat citable and reproducible, which is why identifying it is step 02 of the method, before the threat even has an ordinal.

The five source types

Type	Origin	What it looks like	Cite as
TI provider	External	A commercial threat-intel vendor feed, or the Space ISAC feed the organization's own mandate requires. That channel is live; consuming from it starts today.	vendor + advisory ID
Government	External	A federal advisory or attribution bulletin from a national cyber-defense agency.	agency + advisory reference
Peer-shared	External	An adversary profile or incident retrospective shared by another satellite operator.	peer org + retro ID
OSINT (open-source intelligence)	External	An open-source publication, peer-reviewed paper, or public threat database. Today's working source is the composite OSINT threat assessment of attacks on satellite command and control, cited by its title.	publication + URL or DOI
Internal hunt	Internal	A threat your own Security Operations Center surfaced through in-house hunting on this platform.	internal hunt ticket + analyst

© 2026 ethicallyHackingspace (eHs)®

How to read an incoming report

Intel arrives. A credible research report on command-and-control threats lands on your desk: segment-by-segment narrative of potential attacks, with the subsystems each one would touch.

You assess it. Review each segment's narrative for the situational picture, then walk its table of potential attacks. Plausibility is judged with the departments: Satellite Operations weighs each threat against the platform as flown, Satellite Design & Engineering against the platform as built, the same two views that produced the CONOPS. Match each plausible threat to the platform subsystems named in the report; set aside threats that have nothing to match.

> **Working rule.** The report proposes; the departments dispose. A finding enters the working list only after the two platform views agree it is plausible against this platform as flown and as built, and only if its targets resolve to enumerated CONOPS elements.

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-THR Method

> "Six steps, fixed order: every threat's TOE naming the exact element it targets."

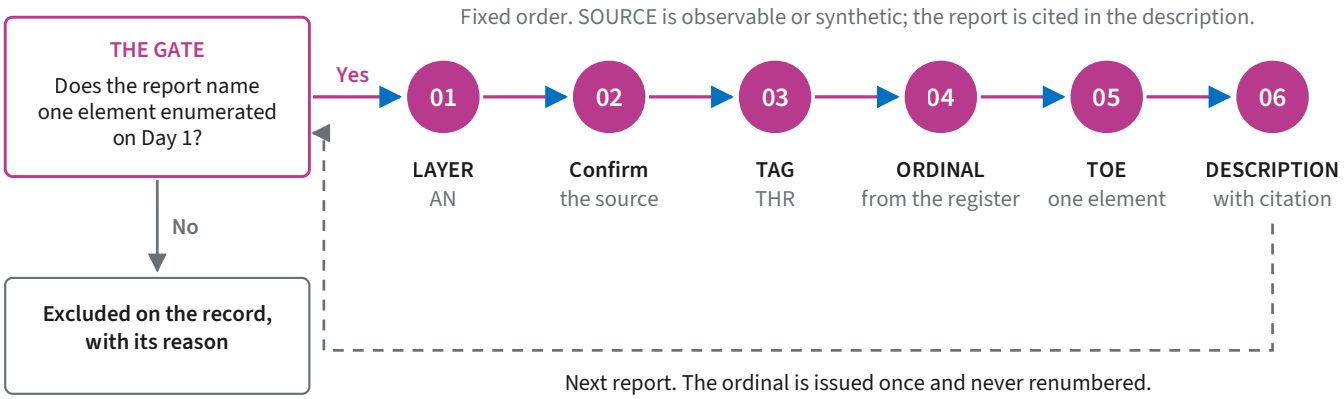
Inputs. Yesterday's decomposition: 44 ETENs of the telecommand path, the command-and-control scope the three mandates set, Executive Order 14144, the NIS2 Directive and the Space ISAC alert on a confirmed command-and-control attack. Threat intelligence cited to the five source types in Chapter 2; today it is the Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite, a document on the course site under Module 02.

Output. One AN-THR ETEN per threat you add to the enumerated set, each one targeting one decomposed element via its TOE.

> **The Gate.** The published definition of a threat is "Confirmed and active threat against a converged space system." (MISP meteorstorm taxonomy v2, AN-THR). In this course it is written against the platform: a threat targeting one enumerated platform element. THR admits an adversarial capability or intent. If it names an actor with no element it would act on, it is intelligence, not an enumerated threat: name the TOE or leave it out. A threat with no target stays out of the enumerated set until either the target is decomposed or the threat is scoped out.

© 2026 ethicallyHackingspace (eHs)®

Figure 1 The Gate, then the AN-THR process: six steps in fixed order, repeated for every report



The six steps, fixed order

1. **Enumerate the LAYER.** LAYER = AN, fixed. These are not platform parts, they are the SOC's findings about the platform, so every element sits in the Analytic Layer. Unlike a PCE, SEG, SVC, or AST, an analytic element has no parent; it anchors to a structural element through its target field instead.
2. **Confirm the source.** Threat-intelligence provider, government attribution statement, peer-shared adversary profile, OSINT, or the SOC's own hunting: one of the five types in Chapter 2. The source defines the TOE. The SOURCE field records only whether the entry is **observable**, built on a real-world report, or **synthetic**, authored for an exercise; the report itself is cited in the description at step 06. All four Kestrel threats are observable.
3. **Set the TAG to THR.** The element is a Threat within the Analytic Layer (AN-THR): an adversarial capability the organization must enumerate, not an attack path or a detection. The LABEL comes with the tag and is fixed: Threat, so the entry reads AN:THR:Threat.
4. **Assign the ORDINAL.** Two digits starting at **00**, one ordinal per distinct threat. Ordinals are issued by the Security Operations Center's running threat register, one sequence across every threat the organization tracks. This register opened this week, so today's four threats are the first four it has issued and they read 00, 01, 02, 03. They will not stay consecutive: as the register takes in threats outside this scope, and as entries retire, gaps appear, and the rule that makes those gaps safe is that an ordinal is issued once and never renumbered.
5. **Enumerate the TOE.** Target of Exploitation: **one** enumerated platform element the source states the threat is directed against. Concrete, not broad, at the lowest layer the source resolves. One element, not a list: the blast radius is real but it is description, not target. This element is the shared anchor of the chain, so the attack path on Day 3, the detection signature on Day 4 and the resilience measure on Day 5 all name it too.
6. **Write the DESCRIPTION.** Identify the threat actor or threat class, describe the assessed capability, and cite the source. This is the line a peer operator will read to act on the element. Confidence is stated with its reason, including where it is low.

© 2026 ethicallyHackingspace (eHs)®

Repeat for the next threat. When the enumerated set covers the three departments' priority threat list, the AN-THR enumeration is current. The TOE is the seam Functions 03, 04 and 05 read next, so it must resolve to CONOPS elements that already exist.

CH 4 The Catalog, Complete

> "Four threats enumerated: Ground 2, Link 1, Space 1, every TOE naming one CONOPS element."

How to read each entry. Each record prints its fields in order: the identifier read whole, then LAYER, TAG, LABEL, ORDINAL, SOURCE, TOE, what that element is, and DESCRIPTION, then the source citation that step 06 writes into the description, and last the confidence and its reason. The TOE holds **one** enumerated platform element, at the lowest layer the source resolves. That element is the one Day 3 anchors the attack path to, the element Day 4 watches, and the element Day 5 hardens, so one identifier carries the whole chain. Everything else the threat would touch on its way through is in the description, where it belongs: a target field with four elements in it cannot tell a reader which one the finding is actually about. The element's parents are not repeated here; they are read off the Day-1 CONOPS whenever they are needed. Source for every Day-2 entry: OSINT, the Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite. The assessment is a document on the course site, under Module 02.

Watch the anchors accumulate. After each entry below you get the anchor figure: one row per threat, the threat on the left, its TOE field in the middle, and on the right the one platform element that field names, labeled with its own layer and drawn in that layer's color. By the end of the chapter the figure is the contextualized threat model: four findings, four anchors, four elements.

The analytic layer is drawn by a target edge, never by containment, because an AN element has no parent. The card on the left is labeled AN · Layer 5 and drawn in magenta. The card on the right is labeled with the structural layer the element belongs to, SVC · Service or AST · Asset, and drawn in that layer's color. The change of label across the arrow is the anchor crossing layers.

© 2026 ethicallyHackingspace (eHs)®

GROUND · 2 AN-THR

AN:THR:Threat:00 · Ground command-acceptance abuse through the management plane

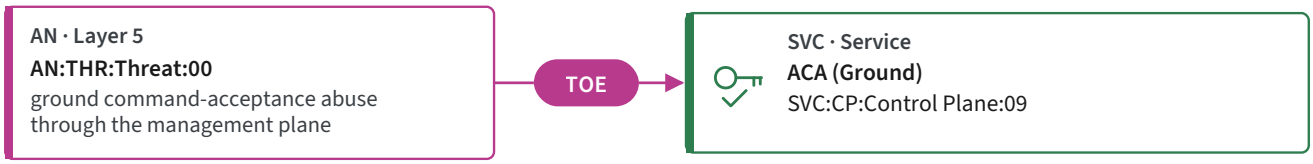
Field	Value
ETEN	AN:THR:Threat:00
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	00
SOURCE	observable
TOE	**SVC:CP:Control Plane:09**
What that element is	the ground command-acceptance service
DESCRIPTION	Adversary reaches the ground management plane through the ground crypto service, abuses the ground command-acceptance service that decides which commands are released to the link, and pushes unauthorized firmware through the patch deployment pipeline.
Source citation	OSINT: Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite
Confidence and reason	Medium

Why this element. The ground command-acceptance service decides who may command and which commands are released to the link. The threat is that authority, turned to release what was never authorized: which is why the TOE names **SVC:CP:Control Plane:09**, the ground command-acceptance service, and nothing else. The ground crypto service and the patch deployment pipeline are how the actor gets there and what the damage rides on, and both are in the description.

> **Field note**
>
> The management network and the commanding consoles ride different Control Plane services: the ground command-acceptance service holds the ACA credential store, **AST:DA:Data:01**, and the console service holds the operator console and its software, **AST:HW:Hardware:04** and **AST:SW:Software:04**. Ruling: two ordinals, 00 and 01, each with its own TOE. First win: Day 3 traces two distinct attack paths, each anchored to the one element it abuses, instead of one blurred ground intrusion.

© 2026 ethicallyHackingspace (eHs)®

Figure 2 AN-THR anchors · 1 of 4 entries · after AN:THR:Threat:00



One finding, one anchor. The threat sits in Layer 5 on the left and names one element on the right, and the arrow through the **TOE** pill is the only link the two have. Nothing is nested, because an analytic element has no parent.

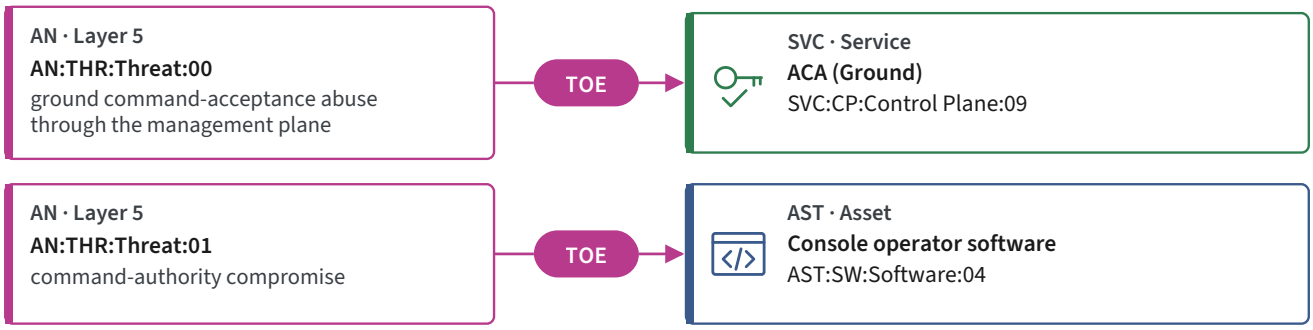
Why the card on the right reads SVC · Service. The label names the structural layer the element belongs to. Its color is green, the Service layer color **SVC:CP:Control Plane:09** already has in the Day-1 decomposition. The card on the left reads AN · Layer 5, in magenta, which is the analytic layer and nothing else. The change of label across the arrow is the anchor crossing layers, which is the one thing this figure exists to show.

AN:THR:Threat:01 · Command-authority compromise

Field	Value
ETEN	AN:THR:Threat:01
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	01
SOURCE	observable
TOE	**AST:SW:Software:04**
What that element is	the console operator software
DESCRIPTION	Adversary with stolen or coerced command authority issues unauthorized telecommands to the on-orbit satellite.
Source citation	OSINT: Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite
Confidence and reason	Medium

© 2026 ethicallyHackingspace (eHs)®

Figure 3 AN-THR anchors · 2 of 4 entries · after AN:THR:Threat:01



The second row anchors to an asset, not a service, so its card reads AST · Asset, in the asset color, blue. Two findings, two different layers, one figure: the target field does not care which layer the element sits at, only that the source resolves to exactly one.

Why these two threats stayed apart. Both reach the ground commanding chain. They are two entries because they resolve to different elements, and an entry that resolves to two elements cannot be detected or hardened as one thing on Days 4 and 5.

LINK · 1 AN-THR

AN:THR:Threat:02 · Jamming campaign

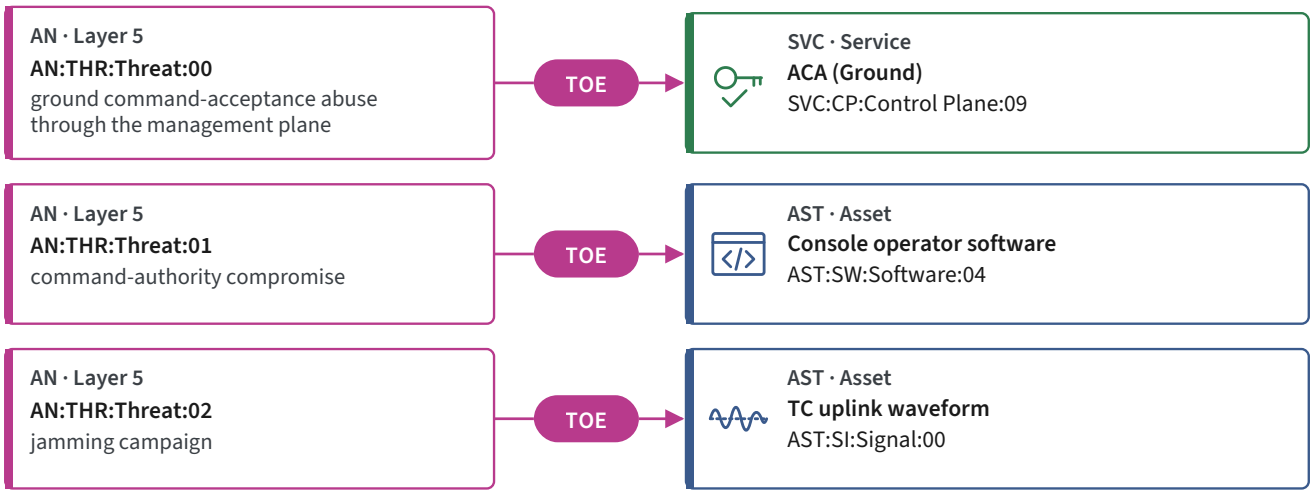
Field	Value
ETEN	AN:THR:Threat:02
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	02
SOURCE	observable
TOE	**AST:SI:Signal:00**
What that element is	the telecommand uplink waveform
DESCRIPTION	RF actor sustains noise injection on the telecommand uplink waveform to deny communications.
Source citation	OSINT: Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite
Confidence and reason	High

© 2026 ethicallyHackingspace (eHs)®

Field note

The one test the framework gives is whether the threat names one enumerated element, and this one does: **AST:SI:Signal:00**, the telecommand uplink waveform. Ruling: the TOE decides scope, not the attack medium, so jamming is enumerated. First win: the receiver lock status and link-outage measurement, already available, is now pinned to **AST:SI:Signal:00**, ready to become a required signal source on Day 3 and the source a Day 4 signature fires on. A jamming threat is seen in the noise floor and never in a log, which is why Day 3 records data sources and signal sources as two separate fields.

Figure 4 AN-THR anchors · 3 of 4 entries · after AN:THR:Threat:02



The link enters the catalog. The waveform asset is the element the jammer acts on, so it is the TOE; the error-correction and tracking services that carry the waveform are reach, not target, and they stay out of the field.

Why the services are not in the field. They would be more identifiers with no way for a reader to tell which one the finding is about. The field answers one question, what is this threat directed at, and it answers it once.

© 2026 ethicallyHackingspace (eHs)®

SPACE · 1 AN-THR

AN:THR:Threat:03 · Malicious on-orbit firmware update

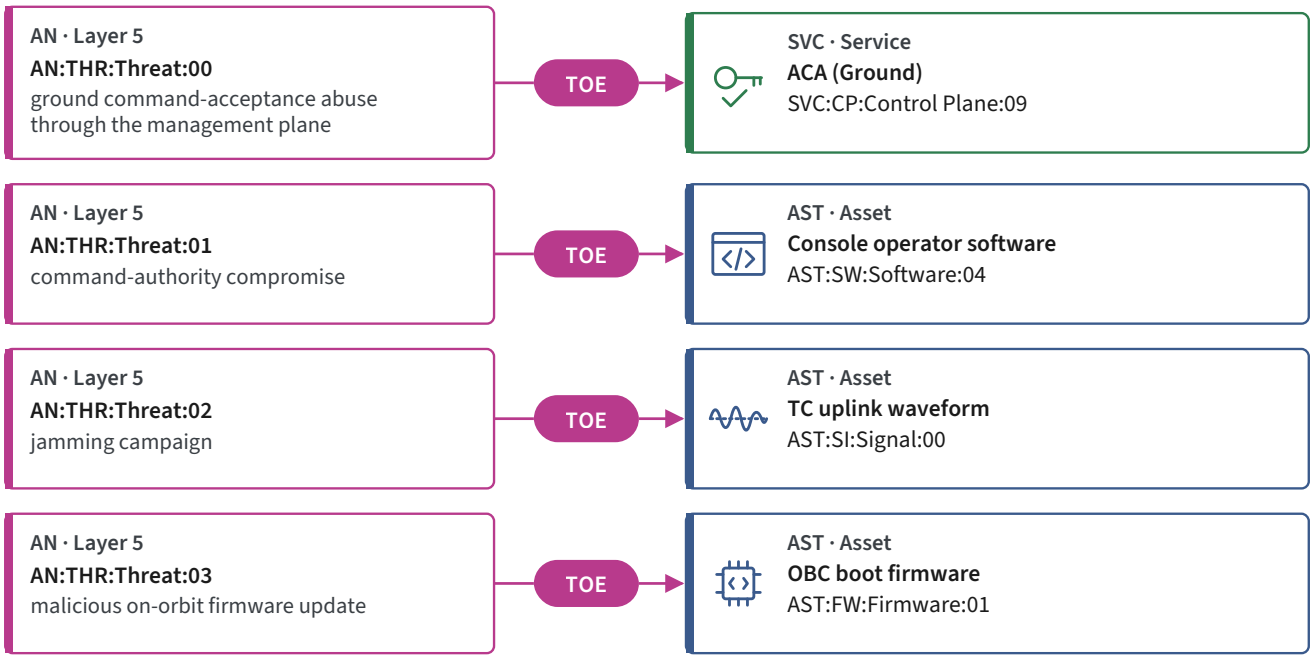
Field	Value
ETEN	AN:THR:Threat:03
LAYER	AN
TAG	THR
LABEL	Threat
ORDINAL	03
SOURCE	observable
TOE	**AST:FW:Firmware:01**
What that element is	the on-board computer boot firmware
DESCRIPTION	Adversary subverts the flight-software update supply chain and pushes a backdoored firmware update to the operational satellite over the command-and-update path.
Source citation	OSINT: Composite OSINT Threat Assessment, Potential Attacks Against the Reference Satellite
Confidence and reason	Medium: there is no publicly disclosed on-orbit case

Field note

Ruling: a Space-segment threat whose TOE names one element, the on-board computer boot firmware; the update supply chain and the command-and-update path that deliver the image are in the description. First win: when Day 5 authors the measured-boot measure, the element it protects is already the right one, the firmware in orbit, not the pipeline on the ground.

© 2026 ethicallyHackingspace (eHs)®

Figure 5 AN-THR anchors · 4 of 4 entries · the complete Day-2 contextualized threat model



Four findings, four anchors, four elements: one service and three assets, reaching the ground, the link and the space segments. This figure is the deliverable Day 3 consumes, and every attack path it draws is anchored to one of these four elements.

What four anchors do and do not claim. They do not claim the rest of the platform is safe. They claim that four threats, enumerated in one day from the evidence available, resolve to these four elements. The boundary is stated so a reader can hold it, and the register is built so the fifth entry costs nothing to add.

> **Scope note.** The User segment (SEG-US-User) is a taxonomic element in the METEORSTORM data model, but it is out of scope on this platform's Day-1 CONOPS, so it is not enumerated and carries no AN-THR threats here.

© 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

> "One shared threat picture: three departments acting on the same enumerated set."

The three readings. All three departments pick this set up in the same form. The Security Operations Center turns each element into a hunt priority against its TOE elements. Satellite Operations reads TOE to know which active subsystems carry which threats during operations. Satellite Design & Engineering reads TOE to plan hardening at the exact elements being targeted.

Three translations become one form. You can now stand in front of Security Operations, Satellite Operations, and Satellite Design & Engineering with one shared threat picture. You do not have to be the threat expert for every domain; you convene them and give them one contextualized picture to act on. Before this engagement that reading took three translations; now it takes one shared form.

The sharing seam. Because every element is written as an ETEN in the shared five-field syntax, the set is ready for the policy-gated contribution to Space ISAC that the organization's own mandate requires: comparable, citable, and machine-readable. Chapter 6 shows the tag that carries it.

Presenting it back

The catalog is enumerated; now you present it. You walk the three departments through the threat picture the same way you walked them through the CONOPS: the whole platform first, then each segment exploded with its threats targeting its own services and assets, then the full picture. The work is contiguous: CONOPS grounds threats, and what the departments confirm in this presentation is what tomorrow's work builds on.

© 2026 ethicallyHackingspace (eHs)®

CH 6 Tag and Share

> “Your work ships as machine tags the whole community can read.”

The METEORSTORM taxonomy the Security Operations Center deployed on Day 1 is published openly as a MISP machine-tag namespace. Tagging the four threats with the Analytic-layer threat entry turns today’s intel into machine-readable threat intelligence instead of a document a partner must re-key:

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

The tag rides on the MISP event, and the TOE travels as an attribute naming the one structural element the threat targets, so a peer operator reads your threat intel in the shared data model, with no translation. What a peer receives is exactly what chapter 4 prints: the five-field ETEN with its cited description, SOURCE, and the TOE naming one enumerated element, comparable against their own platform’s decomposition of the same taxonomic elements.

© 2026 ethicallyHackingspace (eHs)®

CH 7 Use This at Work

This workbook teaches Function 02 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 02 anchors every threat to one enumerated element of the platform, which gives three departments one shared threat picture to act on. 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 one incoming report against the platform as flown and as built.** Review each segment's narrative, then walk its table of potential attacks. A finding enters the working list only after both platform views agree it is plausible, and only if its targets resolve to enumerated elements.

What you gain: Nothing enters the set that the platform is not actually exposed to.

Chapter 2, How to read an incoming report · desk pack sheet 06, Function 02 Contextualized Threat Modeling: method card

02 **Apply the gate to each candidate threat.** Ask whether it names one enumerated element. If it names an actor with no element it would act on, it is intelligence, not an enumerated threat: name the TOE or leave it out, and record the exclusion with its reason.

What you gain: No free-floating threats: every entry in the set has a target on the platform.

Chapter 3, The Gate · desk pack sheets 06 and 07

03 **Enumerate the LAYER as AN.** A threat is a finding about the platform, not a platform part, so it sits in the Analytic Layer. It has no parent.

What you gain: The finding stays apart from the platform parts and anchors to a structural element through its target field.

Chapter 3, step 01 · desk pack sheet 07, Function 02: threat record sheet

04 **Confirm the source of each threat.** Place it in one of the five source types and cite it the way that type is cited. Set SOURCE to observable, built on a real-world report, or synthetic, authored for an exercise.

What you gain: A cited threat can be re-checked when the intelligence changes, weighed against a peer's report of the same activity, and defended in the risk analysis.

Chapter 2, The five source types; Chapter 3, step 02 · desk pack sheets 06 and 07

05 **Set the TAG to THR.** The LABEL comes with the tag and is fixed, so the entry reads **AN:THR:Threat**. It records an adversarial capability, not an attack path or a detection.

What you gain: A peer operator reads the entry in the shared data model, with no translation.

Chapter 3, step 03; Chapter 6 · desk pack sheet 07, Function 02: threat record sheet

© 2026 ethicallyHackingspace (eHs)®

06 **Assign the ORDINAL from one running threat register.** Two digits starting at 00, one ordinal per distinct threat, one sequence across every threat tracked. An ordinal is issued once and never renumbered.

What you gain: The gaps that appear as entries retire are safe, because no ordinal is ever renumbered.

Chapter 3, step 04 · desk pack sheet 07, Function 02: threat record sheet

07 **Enumerate the TOE as one element, not a list.** Name the one enumerated element the source states the threat is directed against, at the lowest layer the source resolves. The blast radius goes in the description, not the target.

What you gain: One shared anchor that the attack path, the detection signature and the resilience measure all name too. A clean TOE is a traceable path.

Chapter 1, What tomorrow consumes; Chapter 3, step 05 · desk pack sheets 06 and 07

08 **Write the DESCRIPTION.** Identify the threat actor or threat class, describe the assessed capability, and cite the source.

What you gain: This is the line a peer operator reads to act on the element.

Chapter 3, step 06 · desk pack sheet 07, Function 02: threat record sheet

09 **Check the catalog, then present it whole platform first.** Repeat the six steps for each threat. Then walk the catalog through the whole platform, then each segment with the threats targeting its own services and assets, then the full picture.

What you gain: One shared threat picture in one form, where the reading used to take three translations.

Chapter 3, Repeat for the next threat; Chapter 5, Presenting it back · desk pack sheet 06, Function 02 Contextualized Threat Modeling: method card

10 **Tag each threat for the shared data model.** Put `meteorstorm:AN="AN-THR"` on the MISP event and carry the TOE as an attribute naming the one structural element the threat targets.

What you gain: Machine-readable threat intelligence instead of a document a partner must re-key.

Chapter 6

Desk pack sheets for Function 02

Sheet	Use it to
Sheets 01 and 02, Quick reference	Read the layers, the tags and the identifier syntax without opening a workbook.
Sheet 06, Function 02 Contextualized Threat Modeling: method card	Apply the gate to each report, then run the six steps in order.
Sheet 07, Function 02: threat record sheet	Write one threat per record, in field order, with its one TOE.
Sheet 06, Catalog check, and sheet 21, Completion checklist across the chain	Check a threat catalog before you present it.

© 2026 ethicallyHackingspace (eHs)®

Where the method is in this workbook

You need	Chapter and heading
The five source types, and how to cite each	Chapter 2, The five source types.
How to read an incoming report	Chapter 2, How to read an incoming report, and the working rule under it.
The gate	Chapter 3, The Gate, and the figure under it.
The six steps	Chapter 3, The six steps, fixed order.
The rules	Chapter 3, steps 02, 04, 05 and 06: SOURCE is observable or synthetic, an ordinal is issued once and never renumbered, and the TOE holds one element at the lowest layer the source resolves. Step 06: Confidence is stated with its reason, including where it is low.
Four complete worked records	Chapter 4, each in field order.
The tag that carries a threat to a peer	Chapter 6.

Module 02 Contextualized Threat Modeling Workbook · Full Spectrum Space Cybersecurity Professional

4 AN-THR · Ground 2 + Link 1 + Space 1 · 4 of 44 elements targeted

© 2026 ethicallyHackingspace (eHs)®