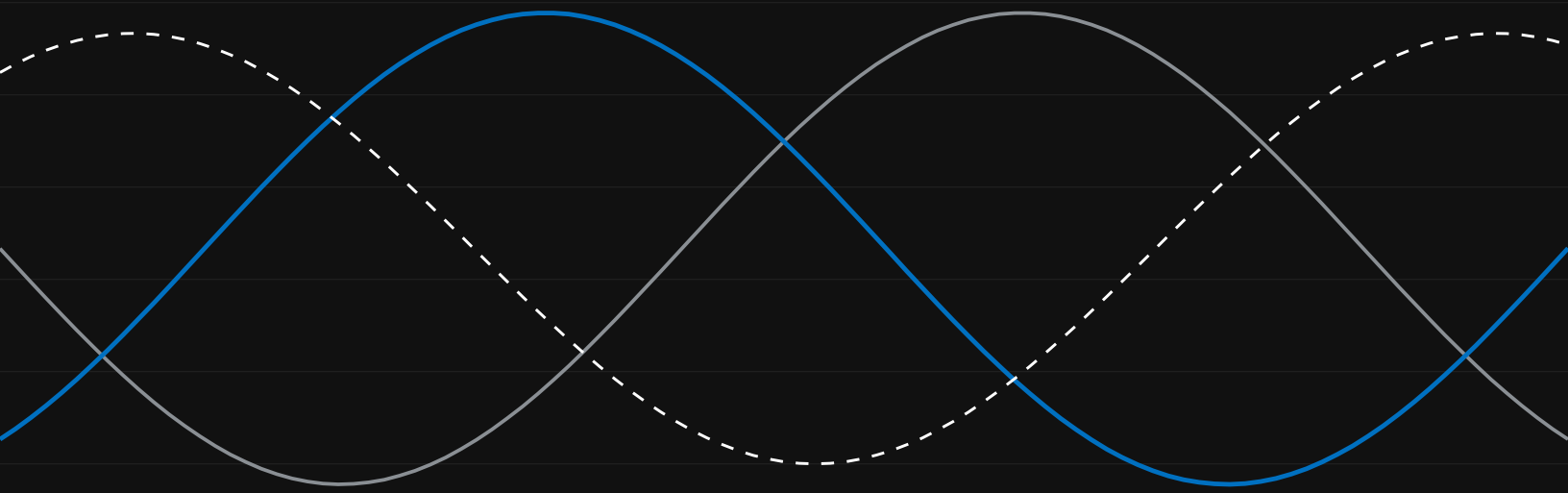
Work center templates

METEORSTORM desk pack

The quick reference, a method card and blank record sheets for each of the five functions, the Pentagon of Pain card, the Pain Index review sheet and the completion checklist.

For use on your own platform. The sheets start on page 4, and each one prints alone.



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	METEORSTORM desk pack
Edition	First edition · version 1.0 · revised 2026-11-19
Contact	www.d2teamcorp.org

What this is and how to use it

1. **For use on your own platform.** Print the sheets you need, write on them, and pin them up at your work center. Each sheet starts on its own page, so any one prints alone.
2. **Framework templates you keep.** The blank sheets carry the fields of the METEORSTORM method in the framework's order, with no platform named.
3. **Nothing is returned to the course.** What you write on a sheet stays with you and your organization.
4. **Kestrel Orbital appears only as the worked example in the course documents.** The one filled identifier on sheet 01 is taken from that example and marked.
5. **Where the definitions come from.** Every definition in quotation marks is the published METEORSTORM taxonomy (MISP, version 2), quoted exactly. The steps and rules are those of the METEORSTORM normative reference and the five module workbooks. The Pentagon of Pain content is from the Pentagon of Pain guide.

The sheets

01 **Quick reference: the four structural layers** 4
02 **Quick reference: the analytic layer** 5
03 **Function 01 Concept of Operations: method card** 6
04 **Function 01: element record sheet** 7
05 **Function 01: element register and enumeration checklist** 8
06 **Function 02 Contextualized Threat Modeling: method card** 9
07 **Function 02: threat record sheet** 10
08 **Function 03 Converged Detection Engineering: method card** 11
09 **Function 03: attack path sheet** 12
10 **Function 04 Incident Response Preparation: method card** 13
11 **Function 04: detection signature record and playbook acceptance checklist** 14
12 **Function 04: blank playbook** 15
13 **Function 05 Adversary Management: method card** 16
14 **Function 05: resilience measure record** 17
15 **Function 05: recurrence tally** 18
16 **Function 05: twin run sheet** 19
17 **Pentagon of Pain card** 20
18 **Pain Index review sheet, page 1 of 3** 21
19 **Pain Index review sheet, page 2 of 3** 22
20 **Pain Index review sheet, page 3 of 3** 23
21 **Completion checklist across the chain** 24

© 2026 ethicallyHackingspace (eHs)®

01 Quick reference: the four structural layers

The four structural layers, in decomposition order

Layer	Published definition (METEORSTORM taxonomy, MISP, version 2)	PARENT names
PCE Primary Capability Environment	"Operational zone in which a capability primarily exists or is exercised."	None. PCE is the root.
SEG Segment	"Service and asset enclaves that compose the system across environments."	One or more PCE
SVC Service	"Functional planes that organize control and data responsibilities."	One or more SEG
AST Asset	"Asset classes composing the system and its interfaces."	One or more SVC

The 24 structural tags and labels

PCE 5 tags		**SEG** 10 tags				**SVC** 3 tags		**AST** 6 tags	
Tag	Label	Tag	Label	Tag	Label	Tag	Label	Tag	Label
TE	Terrestrial	**LA**	Launch	**LO**	Low Altitude	**CP**	Control Plane	**HW**	Hardware
AQ	Aquatic	**LI**	Link	**HI**	High Altitude	**DP**	Data Plane	**FW**	Firmware
AE	Aerial	**GR**	Ground	**NE**	Near Space	**HY**	Hybrid	**SW**	Software
OR	Orbital	**US**	User	**SP**	Space			**DA**	Data
DS	Deep Space	**AQ**	Aquatic	**DE**	Deep Space			**SI**	Signal
								HY	Hybrid

The identifier grammar

TEN
names a type

LAYER-TAG-LABEL-Definition Hyphens, no ordinal. Read from the published taxonomy, never invented.

SEG-GR-Ground-Surface-based services and assets for primary platform operations, serving as the primary locus of control plane activity.

ETEN
names one real element

LAYER:TAG:LABEL:ORDINAL:Description Colons. Layer, tag and label from the TEN; ordinal and description for the instance.

LAYER	TAG	LABEL	ORDINAL	Description
SEG	GR	Ground	00	The Reston, Virginia mission-operations enclave: the control, crypto, access-control, patch, and console services that command the constellation.

Filled example from the course's worked platform, Kestrel Orbital. Its PARENT is PCE:TE:Terrestrial:00.

Fields that govern the record

Field	Rule
ORDINAL	Two digits from 00, counted per tag. Ordinals are scoped to the (LAYER, TAG) pair, continue across segments rather than restarting, and are never re-used.
PARENT	Every parent is enumerated before the child that names it. The parent is linked at Step 06 and governs the record without printing inside the five fields.
DISTRIBUTED services	Y when PARENT lists two or more segments, N when the service runs on a single segment. A cross-segment service lists every participating segment and stays one element, not duplicates.
SUBSYSTEM assets	Optional: a short free-text group name reused verbatim on every asset in one coherent group. Otherwise leave blank.

© 2026 ethicallyHackingspace (eHs)®

02 Quick reference: the analytic layer

The six analytic element types

Tag and label	Published definition (METEORSTORM taxonomy, MISP, version 2)	Target field
AN-THR Threat	"Confirmed and active threat against a converged space system."	**TOE** Target of Exploitation
AN-ATT Attack Path	"Confirmed attack path for a converged space system."	**TOE** Target of Exploitation
AN-DET Detection Signature	"Validated and operational pattern, signal, or logic that triggers on contextualized threat behavior for a converged space system."	**TDM** Target of Detection Method
AN-RES Resilience Measure	"Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats."	**TRE** Target of Resilience Enhancement
AN-IOC Indicator of Compromise	"Confirmed indication that a converged space system has been compromised."	**TOE** Target of Exploitation
AN-IOA Indicator of Attack	"Confirmed indication that a converged space system has been attacked."	**TOE** Target of Exploitation

> **One element in the target field.** One element, never a list, and never a "primary" among several. An analytic element has no parent; it anchors to a structural element through its target field instead.

SOURCE, declared on every analytic entry

observable Built on a real-world report: a signal or data captured from a system.

synthetic Authored data for system resilience engineering and operational exercises.

Required sources on an attack path

RDS The required data source: what must be received as a record.

RSS The required signal source: what must be measured in the physical layer.

RDS and RSS count independently of each other. Nothing to hold: the field reads *none*.

The four states of a required source

Available Collected; the record names the source identifier.

Partial Collected with limits; the record names the reason and the owner.

Gap Assessed and absent; the record names the reason and the owner.

unassessed The owning department has not yet returned a state. Never counts as coverage, and is never a Gap.

Playbook: four stages

assess Is this real, and is it aimed at us?

contain What stops it getting worse?

recover What restores a known-good state?

report Who is told, on what clock?

Effect test: what the action changes sets the domain

cyber Information-system state. Responsible: Security Operations.

space Mission operational state. Responsible: Satellite Operations.

Reversibility ladder: the level is read off, never chosen

reversible: solo. The Responsible role acts alone. Mission Lead is Accountable and Informed.

disruptive: collaborative. The other operating role co-signs before execution, as the Consulted party.

irreversible: escalated. Mission Lead approves before execution, and the approval and its justification are written down before, not after.

Resilience goal, one per measure

Anticipate It removes the opportunity before the adversary acts.

Withstand The mission continues while the attack is under way.

Recover It restores a known-good state afterwards.

Adapt It changes the platform so the same path does not work twice.

Lifecycle of the protected element

reachable Changeable now.

through Fixed in itself, but reachable through something you do control.

fixed Fixed for its service life.

Cadence the measure holds at

in-force Implemented, or implementable this quarter.

phased Part is implementable now, part belongs to the next build.

next-build Cannot be implemented on the flying platform at all.

© 2026 ethicallyHackingspace (eHs)®

Function 01 · method card · For your own use. Not returned to the course.

03 Function 01 Concept of Operations: method card

The gate

The gate is the layer's published definition. An element is enumerated at a layer only when it passes that layer's gate.

Layer	Published definition	The gate
PCE Primary Capability Environment	"Operational zone in which a capability primarily exists or is exercised."	You are naming a zone, not a thing in it.
SEG Segment	"Service and asset enclaves that compose the system across environments."	You are naming a grouping of services and assets, not the zone it sits in and not the hardware inside it.
SVC Service	"Functional planes that organize control and data responsibilities."	You are naming a functional responsibility, what the platform does, not what it is built from.
AST Asset	"Asset classes composing the system and its interfaces."	You are naming a concrete element, a real component the platform is built from.

PCE or SEG? Ask: am I naming a zone, or a group of services and assets? Zone means PCE; group means SEG.

The ETEN process: eight steps, fixed order, repeated for every element

01 **Set the scope.** From the resilience objective and the requirements that drive the decomposition. An element outside the scope is not enumerated.

02 **Select the layer.** Work top down through the taxonomy's structural layers, and confirm the element passes that layer's definition gate before proceeding. An element that fails its layer's gate is not enumerated at that layer; reclassify it and re-enter at Step 02.

03 **Select the tag.** From the taxonomy for that layer. Never invent one.

04 **Write the label.** For that tag, exactly as the quick reference prints it: the short form of the published name.

05 **Assign the ordinal.** Two digits from 00, counted per tag.

06 **Link the parent.** One layer up. This link is the ontology: every child names its parent, PCE is the root, and no element is an orphan. A segment names one or more environments, a service names one or more segments, and an asset names one or more services, never zero.

07 **Set the optional fields.** A service marks DISTRIBUTED when it spans more than one segment; an asset may carry a SUBSYSTEM grouping.

08 **Write the description.** One plain sentence stating what this exact instance is on this platform, at its own layer: a zone for an environment, an enclave of services and assets for a segment, a responsibility for a service, a concrete element for an asset. An instance described at the wrong layer is non-compliant.

The rules

- Eight steps, fixed order, at every layer.
- An element that fails the gate is reclassified, not forced through.
- One identifier carries exactly one description, everywhere it appears.
- Physical units that share an owner, a build and a patch path are one element; where any of those diverge, the element splits and takes the next ordinal.
- The Step 02 gate is applied twice: once selecting the layer, again writing the description.
- A service description begins "The service that …". An asset description is one plain sentence beginning with the element class.

© 2026 ethicallyHackingspace (eHs)®

Function 01 · blank record sheet

04 Function 01: element record sheet

For your own use. Not returned to the course. A framework template you keep.	**Platform**	**Date**	**Sheet** of

1	**LAYER** PCE, SEG, SVC or AST	**TAG**	**LABEL** as published	**ORDINAL** two digits from 00
	Description one plain sentence, at its own layer			
	PARENT one layer up, already enumerated; one or more, never zero; a PCE writes none, root			
	DISTRIBUTED services ☐ Y ☐ N	**SUBSYSTEM** assets, optional		**Reference**

2	**LAYER** PCE, SEG, SVC or AST	**TAG**	**LABEL** as published	**ORDINAL** two digits from 00
	Description one plain sentence, at its own layer			
	PARENT one layer up, already enumerated; one or more, never zero; a PCE writes none, root			
	DISTRIBUTED services ☐ Y ☐ N	**SUBSYSTEM** assets, optional		**Reference**

3	**LAYER** PCE, SEG, SVC or AST	**TAG**	**LABEL** as published	**ORDINAL** two digits from 00
	Description one plain sentence, at its own layer			
	PARENT one layer up, already enumerated; one or more, never zero; a PCE writes none, root			
	DISTRIBUTED services ☐ Y ☐ N	**SUBSYSTEM** assets, optional		**Reference**

4	**LAYER** PCE, SEG, SVC or AST	**TAG**	**LABEL** as published	**ORDINAL** two digits from 00
	Description one plain sentence, at its own layer			
	PARENT one layer up, already enumerated; one or more, never zero; a PCE writes none, root			
	DISTRIBUTED services ☐ Y ☐ N	**SUBSYSTEM** assets, optional		**Reference**

© 2026 ethicallyHackingspace (eHs)®

Function 01 · blank register sheet

05 Function 01: element register and enumeration checklist

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

One row per element. Identifier is LAYER:TAG:LABEL:ORDINAL. Where an element has more than one parent, write each one.

Identifier	Element	Canonical description	Parent	Reference

Enumeration checklist

- ☐ Every parent was enumerated before the child that names it.
- ☐ No element is an orphan: every segment, service and asset names at least one parent, never zero.
- ☐ Every tag and label is read from the published taxonomy. None is invented.
- ☐ Every ordinal is two digits from 00, counted per tag, issued once and never reused.
- ☐ One identifier carries exactly one description, everywhere it appears.
- ☐ Every description passes its layer gate.
- ☐ A service that spans segments is one element, DISTRIBUTED Y, with every segment in PARENT.
- ☐ Every asset names every service it carries.

© 2026 ethicallyHackingspace (eHs)®

Function 02 · method card · For your own use. Not returned to the course.

06 Function 02 Contextualized Threat Modeling: method card

The gate

The published definition of a threat is "Confirmed and active threat against a converged space system." (METEORSTORM taxonomy, MISP, version 2, AN-THR). 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.

> **Excluded on the record.** A threat enters the catalog only when it can name an enumerated target. When it cannot, it is excluded on the record with one of two reasons: the element is not enumerated yet, which is a reason for the next decomposition pass to run, or the platform has no such element.

The AN-THR process: six steps, fixed order, repeated for every threat

01	**Enumerate the LAYER.** AN (fixed).
02	**Confirm the source.** The threat-intelligence provider report, government advisory, peer-shared adversary profile, open-source intelligence, or internal hunt the threat is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
03	**Set the TAG to THR.** With its label, Threat: AN:THR:Threat.
04	**Assign an ORDINAL.** Two digits from 00, one per distinct threat.
05	**Enumerate the TOE.** One enumerated platform element (PCE, SEG, SVC, or AST) the source states the threat is directed against. Concrete, not broad, at the lowest layer the source resolves.
06	**Write the DESCRIPTION.** The threat actor or threat class, the assessed capability, plus the source citation. The line a peer operator or peer machine acts on.

The five source types

Type	Origin	Cite as
TI provider	External	vendor + advisory ID
Government	External	agency + advisory reference
Peer-shared	External	peer org + retro ID
OSINT (open-source intelligence)	External	publication + URL or DOI
Internal hunt	Internal	internal hunt ticket + analyst

The rules

- One element, not a list: the blast radius is real but it is description, not target.
- 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.
- An ordinal is issued once and never renumbered.
- Confidence is stated with its reason, including where it is low.
- An entry with no source is not a threat; it is a worry.
- An exclusion is a deliverable. A catalog with no exclusions has almost certainly forced something in.

Catalog check

- ☐ Every TOE resolves to one enumerated element.
- ☐ Each TOE sits at the lowest layer its source resolves.
- ☐ Every threat cites its source and declares SOURCE.
- ☐ Every ordinal was issued once.
- ☐ Reach is in the description, never in the target field.
- ☐ Every candidate that failed the gate is excluded on the record with its reason.

© 2026 ethicallyHackingspace (eHs)®

Function 02 · blank record sheet

07 Function 02: threat record sheet

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

	LAYER	TAG	LABEL	ORDINAL from 00	SOURCE
1	AN	THR	Threat		☐ observable ☐ synthetic

Target of exploitation (TOE) one enumerated element, not a list, at the lowest layer the source resolves

Description: threat actor or threat class

Description: assessed capability

Description: source citation

Source type

☐ TI provider ☐ Government ☐ Peer-shared ☐ OSINT ☐ Internal hunt

Confidence and reason

	LAYER	TAG	LABEL	ORDINAL from 00	SOURCE
2	AN	THR	Threat		☐ observable ☐ synthetic

Target of exploitation (TOE) one enumerated element, not a list, at the lowest layer the source resolves

Description: threat actor or threat class

Description: assessed capability

Description: source citation

Source type

☐ TI provider ☐ Government ☐ Peer-shared ☐ OSINT ☐ Internal hunt

Confidence and reason

Excluded on the record

Candidate	Reason	Date
	☐ the element is not enumerated yet ☐ the platform has no such element	
	☐ the element is not enumerated yet ☐ the platform has no such element	
	☐ the element is not enumerated yet ☐ the platform has no such element	

© 2026 ethicallyHackingspace (eHs)®

Function 03 · method card · For your own use. Not returned to the course.

08 Function 03 Converged Detection Engineering: method card

The gate

The published definition of an attack path is “Confirmed attack path for a converged space system.” (METEORSTORM taxonomy, MISP, version 2, AN-ATT). 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. An element the adversary only passes through, with nothing to see, is dropped rather than listed.

The AN-ATT process: eight steps, fixed order, repeated for every path

01	**Enumerate the LAYER.** AN (fixed).
02	**Identify the source.** The confirmed exposure, red-team report, adversary-behavior catalog entry (ATT&CK, SPARTA, ATLAS), or peer-shared documentation the path is drawn from. The source defines the TOE. SOURCE is observable or synthetic.
03	**Set the TAG to ATT.** With its label, Attack Path: AN:ATT:Attack Path.
04	**Assign the ORDINAL.** Each path keeps the ordinal of the threat it realizes.
05	**Enumerate the TOE.** One enumerated platform element: the element the path is anchored to, the same element the related AN-THR names.
06	**Write the DESCRIPTION.** The traversal, entry to objective, in enough detail for another analyst to evaluate it against their own platform, plus the source citation.
07	**Enumerate the RDS.** At each step where the adversary’s action would leave a record, name the one data source a defensive cyber operator must hold to see it, as an RDS record counted from 00, each carrying its OBSERVED ON element and its STATE of Available, Partial, Gap or unassessed. Where the path leaves no records at all, write *none*.
08	**Enumerate the RSS.** Walk the same traversal for observables that exist in the physical layer rather than in a record, as RSS records counted from 00, carrying the same four fields. If both fields read *none*, the path as written is not detectable, and that is a finding to record.

The four states of a required source

State	What it obliges
Available	Record the source identifier.
Partial	Record what is short: the field, the retention window, or the subset of hosts covered.
Gap	Record what would have to be collected to close it, and name the owner.
unassessed	Chase the owner. It is not a coverage state and never counts as one.

The rules

- **Waypoints.** Entry, pivot, objective. A fourth is earned only by a second pivot crossing a trust boundary the first did not. The objective is where the route lands, and it need not be the anchor.
- **One record.** A sub-ordinal: Two digits counted from 00, per field, per path. A name: Specific enough that a defensive cyber operator could requisition it. The element it is observed on: One enumerated platform element, never a list. A state.
- **Choosing the source when a step emits several.** Closest to the adversary’s action. Hardest for the adversary to suppress. Already onboarded over newly collected. One required source per observable step is the deliverable.

Path review checklist

- ☐ The path names its driving threat and carries that threat’s TOE as its anchor.
- ☐ The anchor is one element, never a list and never the route.
- ☐ Three waypoints, four at most, each a fully qualified element a detection can observe.
- ☐ RDS and RSS are each written, or read none.
- ☐ Every record names one element and one state.
- ☐ Every Partial and Gap names what is short and an owner.

© 2026 ethicallyHackingspace (eHs)®

Function 03 · blank record sheet

09 Function 03: attack path sheet

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

Identifier AN:ATT:Attack Path:	Driving threat AN:THR:Threat:	SOURCE ☐ observable ☐ synthetic
Anchor (TOE) one enumerated element: the same element the driving threat names		
Entry	**Pivot**	
Second pivot optional	**Objective**	
Source citation		
Confidence and reason High where the pattern is directly reported, Medium where it is technically grounded but per-operator or on-orbit specifics are not public. ☐ High ☐ Medium		

Required data sources (RDS): what must be received as a record

Sub-ordinal	Name of the data source	Observed-on element	State	Identifier or owner
RDS:				
RDS:				
RDS:				
RDS:				

Required signal sources (RSS): what must be measured in the physical layer

Sub-ordinal	Name of the signal source	Observed-on element	State	Identifier or owner
RSS:				
RSS:				
RSS:				

State is one of Available, Partial, Gap, unassessed. Write the source identifier where the state is Available; the reason and the owner where it is Partial or Gap.

☐ RDS empty by answer ☐ RSS empty by answer Both empty: the path as written cannot be detected. Record that as a finding.

© 2026 ethicallyHackingspace (eHs)®

10 Function 04 Incident Response Preparation: method card

The gate

The published definition of a detection signature is “Validated and operational pattern, signal, or logic that triggers on contextualized threat behavior for a converged space system.” (METEORSTORM taxonomy, MISP, version 2, AN-DET). Two ways to fail it. Not a complete rule: a bare SPL, KQL or EQL query, or a bare Sigma rule, with no RootA wrapper and no METEORSTORM anchor block. Not anchored to one element: a TDM that is empty, or that holds a list.

The AN-DET process: seven steps, fixed order, repeated for every signature

01	**Enumerate the LAYER.** AN (fixed).
02	**Verify the format.** The signature must be a complete RootA rule (SOC Prime RootA specification v1.0.0): the mandatory name and detection fields, the optional fields the source supports, and the METEORSTORM anchor block.
03	**Set the TAG to DET.** With its label, Detection Signature: AN:DET:Detection Signature.
04	**Assign an ORDINAL.** Two digits from 00, one per distinct signature.
05	**Enumerate the TDM.** One enumerated platform element the signature observes, the same element the related AN-THR names in its TOE.
06	**Write the DESCRIPTION.** The complete RootA rule: every required field (name, detection language and body), the supporting fields (severity, class, mitre-attack, logsource, correlation, references), and the METEORSTORM block anchoring the rule to the target element and its parent chain.
07	**Name the PLAYBOOK.** The authorized response this signature triggers, as meteorstorm.playbook on the rule and a playbook file beside it. A signature whose playbook does not resolve is not accepted into the layer.

The playbook: four stages, one executor and one decider per action

Stages. assess: Is this real, and is it aimed at us?; **contain**: What stops it getting worse?; **recover**: What restores a known-good state?; **report**: Who is told, on what clock? An action needing two executors is two actions. The level is derived, never chosen.

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

The effect test: the action changes	Domain	Responsible
Information-system state: an identity, a credential, an access path, a host, a network route, a pipeline, a rule	**cyber**	Security Operations
Mission operational state: what the vehicle does, what the link carries, what is commanded, when a contact window opens, which side of a redundant pair is live	**space**	Satellite Operations

The ladder	Undoing the action	Level	At execution time
reversible	Undone without mission impact.	**solo**	The Responsible role acts alone. Mission Lead is Accountable and Informed.
disruptive	Costs mission time, capability or availability, and is recoverable: safe mode, for example.	**collaborative**	The other operating role co-signs before execution, as the Consulted party.
irreversible	Cannot be undone by deciding differently: a filed regulatory change, a filed Space ISAC Exchange entry, destroyed volatile evidence.	**escalated**	Mission Lead approves before execution, and the approval and its justification are written down before, not after.

© 2026 ethicallyHackingspace (eHs)®

Function 04 · blank record sheet

11 Function 04: detection signature record and playbook acceptance checklist

For your own use. Not returned to the course. A framework template you keep.	**Platform**	**Date**	**Sheet** of

Identifier **AN:DET:Detection Signature:**	**Name of the signature**	**SOURCE** ☐ observable ☐ synthetic

Target of detection method (TDM) one enumerated element: the element the threat it covers names as its TOE

Covers the attack path and threat entries this signature covers

Rule format and file a complete RootA rule carrying the METEORSTORM anchor block

Source state as Function 03 recorded it

☐ Available ☐ Partial ☐ Gap ☐ unassessed

Source identifier, or what the rule cannot see, or the collection that would close the gap and its owner

Corroborating streams named in the description, never in the TDM

Known benign causes

Bound playbook the playbook identifier, and the playbook file beside the rule

A threat or attack path with no matching signature is a detection gap, and the gap is itself an enumerable analytic product.

Playbook acceptance checklist: the nine-point minimum

A playbook is not complete, and its signature does not ship, until all of these hold.

- ☐ At least one approved action in each of the four stages.
- ☐ Every action carries a complete record, plus the why wherever the domain departs from the element's expectation.
- ☐ Exactly one Accountable per action, and it is Mission Lead.
- ☐ Exactly one Responsible per action, and it is never Mission Lead.
- ☐ The Responsible role matches the domain.
- ☐ Level matches reversibility by the ladder.
- ☐ Every collaborative action names its co-signer as Consulted.
- ☐ At least one action names the signature's TDM.
- ☐ At least one report action names a regulatory clock and who starts it.

> **The field is element, never on.** In YAML 1.1 the bare key on parses as the boolean true, so a playbook written with on: silently loses every element and validates as if no action named anything.

© 2026 ethicallyHackingspace (eHs)®

Function 04 · blank record sheet

12 Function 04: blank playbook

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

Playbook identifier	Signature AN:DET:Detection Signature:	**Trigger** the entry condition, not an action: the signature and the element it watches
Confidence threshold		Why that threshold and not a higher one

id	stage	domain	action	element	reversibility	level	Responsible	Accountable	Consulted	Informed
ACT:										
ACT:										
ACT:										
ACT:										
ACT:										
ACT:										
ACT:										
ACT:										

stage assess, contain, recover, report: at least one action in each. **domain** cyber or space, by the effect test. **element** one enumerated element. **reversibility and level** reversible is solo; disruptive is collaborative; irreversible is escalated. **Responsible** exactly one, matching the domain. **Accountable** exactly one. Where the domain departs from the element's expectation, write the why under the action.

© 2026 ethicallyHackingspace (eHs)®

13 Function 05 Adversary Management: method card

The gate

The published definition of a resilience measure is “Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats.” (METEORSTORM taxonomy, MISP, version 2, AN-RES). Every element carries exactly one TRE element, names its resiliency goal and names its owner. A measure with no target, no goal or no owner is decoration, not resilience. Every element also declares the lifecycle of the element it protects and the cadence the measure holds at, because a measure that cannot be implemented is not a control in force.

The AN-RES process: six steps, fixed order, repeated for every measure

01	**Enumerate the LAYER.** AN (fixed).
02	**Identify the resiliency goal.** One of Anticipate, Withstand, Recover, or Adapt, per NIST SP 800-160 Volume 2. SOURCE is observable or synthetic.
03	**Set the TAG to RES.** With its label, Resilience Measure: AN:RES:Resilience Measure.
04	**Assign an ORDINAL.** Two digits from 00, one per distinct measure.
05	**Enumerate the TRE.** One enumerated platform element: the element the measure protects, the same element the related AN-THR targets. TRE, not TOE or TDM: the element made more resilient.
06	**Write the DESCRIPTION.** The measure, the resiliency goal it serves, the AN-ATT or AN-THR entries it counters, plus the source citation: internal engineering, control-framework guidance, peer-shared pattern, or post-incident lesson.

Choosing among the four goals

Goal	Working test
Anticipate	It removes the opportunity before the adversary acts.
Withstand	The mission continues while the attack is under way.
Recover	It restores a known-good state afterwards.
Adapt	It changes the platform so the same path does not work twice.

Cadence	What the organization holds today
in-force	Implemented, or implementable this quarter.
phased	Part is implementable now, part belongs to the next build.
next-build	Cannot be implemented on the flying platform at all.

The goals are those of NIST SP 800-160 Volume 2. The test is the course’s working test, not the publication’s wording.

The lifecycle test: where the protected element sits in its life

Lifecycle	The protected element	So the measure is
reachable	Changeable now.	Applied to the element directly.
through	Fixed in itself, but reachable through something you do control.	A compensating control on the path to it.
fixed	Fixed for its service life.	A requirement for the next build. It cannot be implemented on what is flying.

The rules

- Anything not in force must name a compensating control or a recorded residual risk. Coverage you cannot implement is not coverage. A compensating control names the element it is applied to. A residual risk names its owner and what closes it. Where the cadence is in force, both fields are empty, and that emptiness is a statement rather than an omission.
- A measure recorded as Both must name the split. One element, never a list, and never a “primary” among several.
- There are only two honest answers per attack path: a measure on its anchor element, or a recorded residual risk with an owner.

© 2026 ethicallyHackingspace (eHs)®

Function 05 · blank record sheet

14 Function 05: resilience measure record

For your own use. Not returned to the course. A framework template you keep.	**Platform**	**Date**	**Sheet** of

Identifier **AN:RES:Resilience Measure:**	**Name of the measure**	**SOURCE** ☐ observable ☐ synthetic

Target of resilience enhancement (TRE) one enumerated element: the element the threat it counters names as its TOE

Counters the attack path or threat entries this measure counters

Goal one

☐ Anticipate ☐ Withstand ☐ Recover ☐ Adapt

Why this goal

Owner where two departments own it, name the split

Lifecycle of the protected element ☐ reachable ☐ through ☐ fixed	**Cadence** ☐ in-force ☐ phased ☐ next-build

Compensating control required where the cadence is not in force	**The element it is applied to**

Residual risk required where the cadence is not in force	**Owner of the risk**	**What closes it**

Source citation

© 2026 ethicallyHackingspace (eHs)®

Function 05 · blank tally sheet

15 Function 05: recurrence tally

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

The counting rule. That count compares exact identifiers and does not roll an asset up to its parent. The count covers waypoints and required-source elements only. The method publishes no rule for counting by parent. The count is run again every time the catalog grows.

Write each attack path ordinal across the top and each element once down the side. Tick a cell where the element is a waypoint of that path, or the element one of its required sources is observed on. An element in two or more paths is where the adversary keeps having to go.

Element, by exact identifier	Path	Path	Path	Path	Path	Path	Paths it appears in

Function 05 · blank run sheet

16 Function 05: twin run sheet

For your own use. Not returned to the course. A framework template you keep.	Platform	Date	Sheet of

Measure validated	Attack path replayed
AN:RES:Resilience Measure:	**AN:ATT:Attack Path:**

Nothing reaches the platform before the digital twin. Run the scenario twice, once with the measure applied and once without.

Question what the run has to answer, and what the measure costs

Scenario the attack path profile replayed on the twin, run twice: once with the measure applied and once without

Without the measure

With the measure

Cost the effect of the measure on mission capability while it is active

Abuse case how an adversary who learns the measure could turn it against the platform

Rejection criterion the result on which the measure is rejected on the evidence

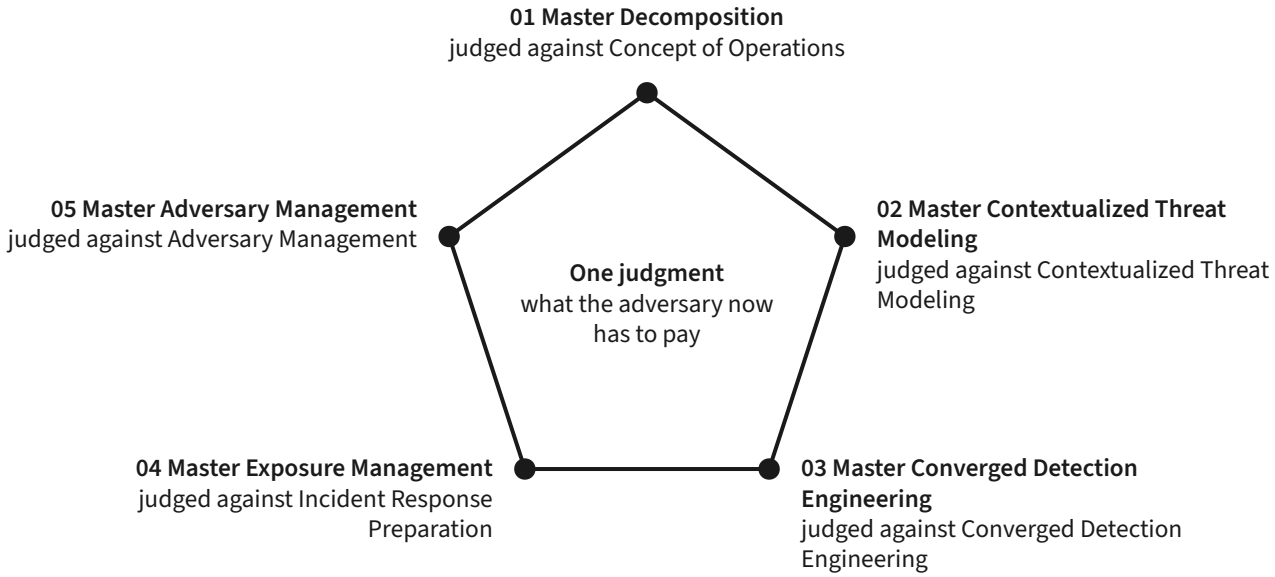
© 2026 ethicallyHackingspace (eHs)®

Pentagon of Pain · For your own use. Not returned to the course.

17 Pentagon of Pain card

The single test, for every hour and every dollar

Does this raise the adversary's cost?



#	Mastery area	The adversary suffers when	Judged against
01	**Master Decomposition**	"The adversary suffers when you know your platform better than they ever can."	Function 01 Concept of Operations
02	**Master Contextualized Threat Modeling**	"The adversary suffers when every strike they imagine is already prepared for."	Function 02 Contextualized Threat Modeling
03	**Master Converged Detection Engineering**	"The adversary suffers when they cannot hide, and every move is seen."	Function 03 Converged Detection Engineering
04	**Master Exposure Management**	"The adversary suffers when every path they take ends in a trap."	Function 04 Incident Response Preparation
05	**Master Adversary Management**	"The adversary suffers when their plans are known, broken, and turned against them."	Function 05 Adversary Management

> Cost must be concrete. "Raises adversary cost" is filler; name what the adversary must now do: hold access longer, burn a second capability, move where telemetry sees them, or beat three departments instead of one.

© 2026 ethicallyHackingspace (eHs)®

Pentagon of Pain · reviewer's record

18 Pain Index review sheet, page 1 of 3

A reviewer's record. It is never self-scored. Write the evidence you inspected beside the state it supports. For your own use. Not returned to the course.	**Reviewer**	**Work reviewed**	**Date**

01 Master Decomposition judged against Concept of Operations				
State of the decomposition	**Adversary impact**	**Pain**	**Evidence inspected**	**What the adversary must now do**
Basic system diagrams exist but lack operational traceability or cross-functional ownership.	Attackers exploit undocumented interfaces and data paths, maintaining stealth and mobility.	**1**		
The in-scope platform is enumerated across the four layers, every element with a parent and a description, agreed by the three departments.	Attackers lose stealth; a deviation from baseline on a named element raises a question all three departments can read.	**2**		
Threats, attack paths, detections and resilience measures are anchored to the enumerated elements.	Lateral movement and command injection on the mapped platform are flagged and constrained against a named element.	**3**		
The decomposition is re-run as a pass, extended where earlier exclusions said it should be, and the measures feed the next platform design.	Campaigns collapse mid-operation; attackers must retool and re-infiltrate under significantly greater risk each pass.	**4**		

02 Master Contextualized Threat Modeling judged against Contextualized Threat Modeling				
State of the threat catalog	**Adversary impact**	**Pain**	**Evidence inspected**	**What the adversary must now do**
Threat modeling is ad hoc and focused on listing possible threats without alignment to the decomposed platform.	Attackers face minimal disruption; threat models are too generic to anticipate or constrain actions.	**1**		
Known threats are anchored by METEORSTORM contextualized threat modeling, one enumerated element each, with source and confidence stated and exclusions recorded.	Attackers must vary tools or timing; reused techniques and AI-generated steps land on a named element the defensive cyber operator has already read.	**2**		
Every anchored threat carries an attack path, a detection and a resilience measure on the same element.	Adversary campaign variants become predictable and less effective; the strike they imagined is the one the platform prepared for.	**3**		
The catalog is refreshed as reporting arrives and the exclusions drive the next decomposition pass.	Automated campaigns break under real-time counterplay; adversaries are forced into improvisation.	**4**		

© 2026 ethicallyHackingspace (eHs)®

Pentagon of Pain · reviewer's record

19 Pain Index review sheet, page 2 of 3

A reviewer's record. It is never self-scored. Write the evidence you inspected beside the state it supports. For your own use. Not returned to the course.

Reviewer	Work reviewed	Date

03 Master Converged Detection Engineering judged against Converged Detection Engineering				
State of the path catalog and source inventory	**Adversary impact**	**Pain**	**Evidence inspected**	**What the adversary must now do**
Detection relies on default signatures or generic anomaly rules written before any path exists; no source inventory; space and cyber observables live in separate programs.	Attackers bypass detection by blending into noise or mimicking routine activity.	**1**		
Each threat has a path anchored to its element, with the required data and signal sources named and their states recorded, gaps included.	Known techniques cross at least one step where a source is Available; simple replay or automation attempts begin to break down.	**2**		
The gaps are being closed by the owning department, and the inventory is what the detection signatures are written against.	Tradecraft is exposed quickly; the attacker must sacrifice stealth, use untested techniques, or withdraw.	**3**		
The inventory is re-assessed with every pass and the unassessed count is driven to zero.	Dwell time is crushed; attackers face immediate loss of cover and rapid exposure.	**4**		

04 Master Exposure Management judged against Incident Response Preparation				
State of the signatures and playbooks	**Adversary impact**	**Pain**	**Evidence inspected**	**What the adversary must now do**
Exposure is managed via static policy and periodic review; signatures are vendor-locked with no paired response; responses are invented on the day.	Attackers exploit long-lived weaknesses and a predictable architecture without time pressure.	**1**		
Each path has a signature on its required source and a playbook naming who decides and who executes, but some sources are still Partial.	Automated tools and known exploits begin failing on the instrumented routes; attackers must adapt tools or pivot to a route not yet instrumented.	**2**		
Every recorded gap has a compensating action in a playbook and an owner closing it.	Intrusions lose persistence quickly; the blind spot they counted on is now a hold, a review or a rate limit with a named executor.	**3**		
Signatures and playbooks are rehearsed and refreshed as the source inventory changes.	Attackers are expelled mid-operation and forced to rebuild access repeatedly at escalating cost, inside positive control.	**4**		

© 2026 ethicallyHackingspace (eHs)®

Pentagon of Pain · reviewer's record

20 Pain Index review sheet, page 3 of 3

A reviewer's record. It is never self-scored. Write the evidence you inspected beside the state it supports. For your own use. Not returned to the course.	**Reviewer**	**Work reviewed**	**Date**

05 Master Adversary Management judged against Adversary Management				
State of the resilience portfolio	**Adversary impact**	**Pain**	**Evidence inspected**	**What the adversary must now do**
Response ends at containment; the same flaw stays exposed; no recurrence is counted; attribution is ad hoc and sharing happens after the fact if at all.	Attackers retain plausible deniability and can reuse infrastructure or tactics without consequence.	**1**		
Recurrence is counted from the catalogs and each measure protects one element for one goal with an owner and a cadence; some sharing occurs after containment.	Attackers begin to lose the element they reused most, and suffer exposure across intelligence-sharing communities.	**2**		
Every path is either covered or carries an owned, dated residual risk, and attribution-quality evidence goes out on a confirmed attack.	Campaigns become traceable; attacker playbooks degrade quickly, and the residual path has an expiry date.	**3**		
The residual risks close in the next platform design and the portfolio and the evidence are portable across operators.	Adversaries are identified and tracked in near real time; reuse becomes a liability and deniability collapses.	**4**		

Reviewer's summary

> The left column names the state of a deliverable that can be inspected; the right column names what the adversary must now do that they did not have to do before. Cost must be concrete. "Raises adversary cost" is filler; name what the adversary must now do: hold access longer, burn a second capability, move where telemetry sees them, or beat three departments instead of one.

Mastery area	**Pain, from the adversary impact**	**What the adversary must now do**
01 Master Decomposition	☐ 1 ☐ 2 ☐ 3 ☐ 4	
02 Master Contextualized Threat Modeling	☐ 1 ☐ 2 ☐ 3 ☐ 4	
03 Master Converged Detection Engineering	☐ 1 ☐ 2 ☐ 3 ☐ 4	
04 Master Exposure Management	☐ 1 ☐ 2 ☐ 3 ☐ 4	
05 Master Adversary Management	☐ 1 ☐ 2 ☐ 3 ☐ 4	

© 2026 ethicallyHackingspace (eHs)®

All five functions

21 Completion checklist across the chain

For your own use. Not returned to the course. A framework template you keep.	**Platform**	**Date**	**Sheet** of

One column per chain: write the ordinal that carries the chain from threat to attack path to detection signature to resilience measure, then tick each line that holds for it.

Function	Check	Chain	Chain	Chain	Chain	Chain
01	**No orphan.** Every segment, service and asset names at least one enumerated parent. Only a PCE writes none.					
01	**Every description passes its layer gate.** A zone for an environment, an enclave for a segment, a responsibility for a service, a concrete element for an asset.					
02 to 05	**Every target names one enumerated element.** TOE, TDM and TRE each hold one element, never a list, and it is the same element down the chain.					
02 to 05	**SOURCE is declared.** Every analytic entry reads observable or synthetic. The citation is in the description.					
03	**Both required-source fields are written, or read none.** RDS and RSS each carry their records, or the answer none.					
03, 04	**Every gap has an owner.** Each Partial and Gap names what is short or missing and who owns closing it. A signature that cannot fire is still enumerated.					
05	**Every measure not in force names a compensating control or a residual risk.** The control names the element it is applied to. The risk names its owner and what closes it.					

Checked by	**Date**	**Next review**
Open items, each with an owner		

© 2026 ethicallyHackingspace (eHs)®