



Monitoring the great value in your Big Data

HANDS-ON WALKTHROUGH · PART 1

Your first DSM tenant

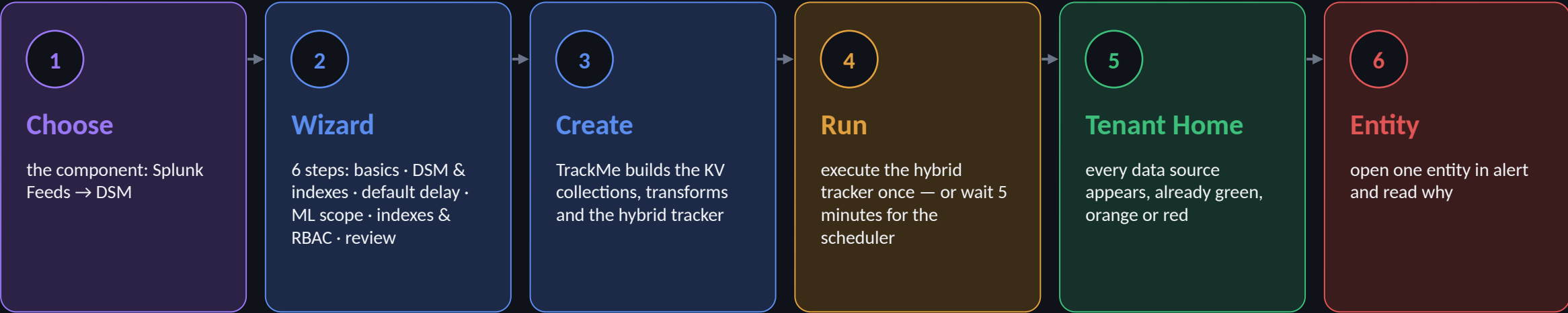
From an empty TrackMe to monitored data sources — create a Virtual Tenant, let the hybrid tracker discover the feeds, and read the first entity in alert and why.

Captured live on TrackMe 2.4.18 · Splunk Cloud



What we are going to do

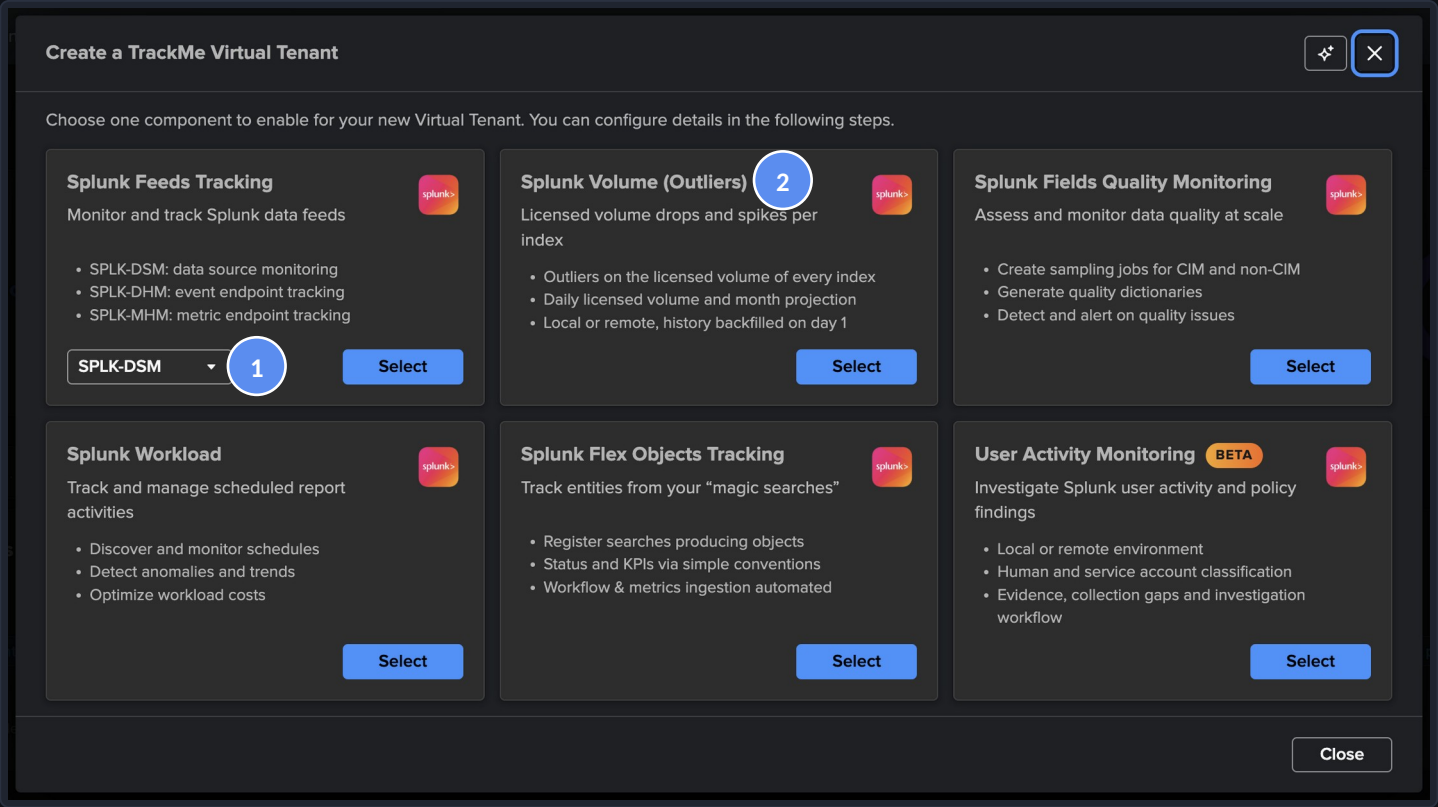
One tenant, one component, one tracker. The wizard asks six questions; the tracker does the rest.



Our example tenant

Tenant id	Alias	Component	Index scope	Everything else
secops	Security Operations	DSM — Data Source Monitoring	siem-*	wizard defaults

Step 0 — choose the component



1 Splunk Feeds Tracking

Bundles the three feeds components. The selector picks which one this tenant starts with — SPLK-DSM here. DHM and MHM can be enabled later from “Manage components”.

2 One tenant, one starting component

The wizard configures a single component; a tenant can run several. The other tiles start Volume (Outliers), Fields Quality, Workload, Flex Objects or User Activity Monitoring (Beta) tenants.

Why DSM first

It answers the question every Splunk team has — is my data still arriving? — and it is auto-discovered: nothing to declare, nothing to maintain.

Step 1 — Basics: identity that cannot change

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

1 Basics 2 Configure DSM 3 Default delay 4 ML Outliers 5 Indexes & RBAC 6 Review

Provide an identifier for your Virtual Tenant. This cannot be changed later.

Tenant id

secops 1

Lowercase, numbers and hyphens only, max 20 characters.

✓ This tenant id is available

Tenant alias (optional)

Security Operations 2

Tenant description (optional)

Security Operations feeds - DSM on business data and SIEM sources 3

> Impact score configuration 4

> Help - concepts & tips

> Advanced tenant options

< Back Next >

1 Tenant id — immutable

Lowercase, digits, hyphens, max 20 chars. It is stamped as an indexed field on every event and metric the tenant produces. Choose it like a hostname.

2 Alias

Human-readable display name — editable any time. Cards are ordered by alias, so “01 - SecOps” style prefixes work well.

3 Description

Free text shown on the tenant card.

4 Expanders

Impact score configuration, concepts & tips, advanced options — defaults are fine for a first tenant.

The banner confirms the id is available. Try a taken id and the wizard refuses before you spend time on the next steps.

Step 1 — the impact-score weights live at tenant level

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

✓ This tenant id is available

Tenant alias (optional): Security Operations

Tenant description (optional): Security Operations feeds - DSM on business data and SIEM sources

▼ Impact score configuration **1**

Configure impact scores (0-100) for different anomaly types. An entity is green if the accumulated score is 0, orange if >0 and <100, red if ≥100.

Outliers - Default Impact Score

0 100 Current value: 36

The default impact score (0-100) applied when new outlier models are created. Once a model exists, its score weight is persisted individually and can be updated via bulk edit or on a per-model basis.

DSM - Data Sampling Anomaly Impact Score

0 100 Current value: 36

Impact score (0-100) assigned when data sampling anomalies are detected.

DSM - Delay Threshold Breach Impact Score **2**

0 100 Current value: 100

Impact score (0-100) assigned when delay threshold is breached.

DSM - Latency Threshold Breach Impact Score

0 100 Current value: 48

Impact score (0-100) assigned when latency threshold is breached.

DSM - Min Hosts Dcount Breach Impact Score

0 100 Current value: 100

Impact score (0-100) assigned when minimum host count threshold is breached.

DSM - Future Tolerance Breach Impact Score

0 100 Current value: 36

Impact score (0-100) assigned when future tolerance threshold is breached.

> Help – concepts & tips

< Back Next >

1 Impact score configuration

The weights from the introduction — outliers, data sampling, delay breach, latency breach, min hosts, future tolerance — are set here per tenant, 0–100 each.

2 Delay breach = 100

A delay-threshold breach alone reaches the red threshold (≥ 100). Latency is 48, outliers 36: on their own they only make an entity orange.

Remember

$\text{total_score} = \sum \text{weights of active anomalies}$
 0 → green · < 100 → orange · ≥ 100 → red

The tenant default cascades to every entity and can be overridden per entity or in bulk. We keep the defaults.

Step 2 — Configure DSM: the hybrid tracker is born here

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

Progress: 1 Basics 2 **Configure DSM** 3 Default delay 4 ML Outliers 5 Indexes & RBAC 6 Review

Configure Data Source Monitoring (SPLK-DSM) options for this tenant.

Create tracker now? Yes Splunk deployment **1**

Indexes discovery (optional) - allow only these Index patterns

siem-* Test **2**

Resulting search root constraint for this tracker:

`index=siem-*` **3**

Simulation successful **4**

ENTITIES **92** INDEXES **35**

siem-cloud-amer siem-cloud-apac siem-cloud-emea siem-cloud-latam siem-firewall-amer siem-firewall-apac siem-firewall-emea siem-firewall-latam siem-identity-amer siem-identity-apac
siem-identity-emea siem-identity-latam siem-infra-amer siem-infra-apac siem-infra-emea siem-infra-latam siem-osnx-amer siem-osnx-apac siem-osnx-emea siem-osnx-latam +15 more

• siem-cloud-amer.aws:cloudtrail
 • siem-cloud-amer.aws:config

< Back Next >

1 Create tracker now = Yes

The wizard creates the DSM hybrid tracker for you — a scheduled search that runs every 5 minutes against the local deployment (or a remote one).

2 Index patterns

Chips, wildcards allowed: siem-* covers every SIEM index family. Leave empty to discover every index the tracker's owner can read.

3 Resulting root constraint

index=siem-* — this is the SPL the tracker will start from.

4 Test now = simulation

Before creating anything: the entities and indexes the tracker will discover, listed. No surprises after creation.

Step 3 — Default delay: what “late” means for this tenant

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

Thresholds accept seconds or with unit suffix (m/h/d/w), for example: 3600, 15m, 1h, 2d.

business_hours

01:00:00

(1h)

1

Remove

Days: Select all

MonTueWedThuFriSatSun

Hours: Select all

01234567891011121314151617181920212223

business_nights

04:00:00

(4h)

2

Remove

Days: Select all

MonTueWedThuFriSatSun

Hours: Select all

01234567891011121314151617181920212223

This slot spans midnight in the server's time; its weekday stays on the server's calendar.

weekends

1+00:00:00

(1d)

3

Remove

Days: Select all

MonTueWedThuFriSatSun

Hours: Clear all

01234567891011121314151617181920212223

This slot spans midnight in the server's time; its weekday stays on the server's calendar.

Default threshold (fallback): 01:00:00

Applies when no slot

4

< Back

Next >

- business_hours — 1h**
Mon–Fri, 09–20: a feed silent for more than an hour is late.
- business_nights — 4h**
Mon–Fri, 21–08: more tolerance while batch jobs and low traffic are expected.
- weekends — 1 day**
Sat–Sun, all hours.
- Fallback — 1h**
Applies when no slot matches.

Static vs variable

Static: one limit, always. Variable: limits by day and hour. The quick template “Business hours vs. off-hours” pre-fills three slots; hours are shown in your browser time and stored in server time. This is the tenant default — every entity inherits it and can override it.

Step 4 — ML Outliers: off by default, volume belongs to VOL

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

✓ Basics

✓ Configure DSM

✓ Default delay

4 ML Outliers

5 Indexes & RBAC

6 Review

☐ Outliers detection disabled for this tenant

1

i

Recommended: volume outliers per index

We recommend detecting volume outliers at the level of indexes, with the Splunk Volume (Outliers) component in a separate tenant: it models the licensed volume of every index. You can still enable outliers detection on the data sources of this tenant as well.

Outliers detection scope

Restrict which entities the ML Outliers detection trains on for this tenant. Both filters apply to every component eligible for outliers detection; the Volume KPI override below is consumed by dsm and dhm only. Leave them at their defaults to train every entity.

Priority filter

2

☒ Critical

☒ High

☐ Medium

☐ Low

Only entities whose priority is selected here will be trained. Leaving all four selected disables the priority filter.

< Back

Next >

1 Disabled for this tenant

Outliers detection on data sources starts off. The banner recommends volume outliers per index with the Splunk Volume (Outliers) component, in its own tenant.

2 If you enable it: the scope

A priority filter (critical + high by default) and a filter expression in the Virtual Groups DSL narrow training to the feeds where anomalies are meaningful.

Why this default

VOL models the licensed volume of every index — the right grain for drops and spikes. Per-feed models cost search time and add 36 to the score per breach: a focused opt-in, not a fleet-wide switch.

Step 5 — Indexes & RBAC: where the tenant writes, who can see it

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

✓ Basics

✓ Configure DSM

✓ Default delay

✓ ML Outliers

5 Indexes & RBAC

6 Review

Choose indexes for TrackMe objects and assign ownership and roles.

Summary index

1 trackme_summary

Audit index

trackme_audit

Metric index

trackme_metrics

Notable index

trackme_notable

Splunk owner for created objects

2 nobody

Admin roles

3 trackme_admin

Power roles

trackme_power

Readonly roles

trackme_user

< Back

Next >

1 Four indexes

summary (state events), audit (who changed what), metrics (KPIs over time), notable (alert output). Defaults are the trackme_* indexes; large estates often dedicate indexes per tenant.

2 Owner

The Splunk user the tenant's objects belong to and its trackers run as — “nobody” keeps them app-scoped.

3 Roles

Admin, power and read-only roles per tenant. This is how team A never sees team B's entities.

RBAC is per tenant and enforced at the REST boundary — the UI, the API and the AI Assistant all go through it.

Step 6 — Review, then watch TrackMe build the tenant

Create a new TrackMe Virtual Tenant: Splunk Feeds - DSM

Progress bar: Basics (checked), Configure DSM (checked), Default delay (checked), ML Outliers (checked), Indexes & RBAC (checked), **Review (6)**

1 Please review the configuration before confirmation.

Update comment (optional)

SecOps data sources - DSM tenant for the SIEM index families

2 Action Progress Events (auto-refresh 15s)

Time	Event
> 9/29/2026 6:54:47.052 AM	2026-09-29 05:54:47,052 INFO trackme.rest.splk_hybrid_trackers_admin trackme_libs.py trackme_create_report 3159 tenant_id="secops", action="success", report_name="trackme_dsm_hybrid_tracker-prss3i9_wrapper_tenant_secops" with kwargs={"owner": "nobody", "sharing": "app", "perms.write": "trackme_admin", "perms.read": "trackme_user,trackme_power"} index = <u>_internal</u> source = /opt/splunk/var/log/splunk/trackme_rest_api_splk_hybrid_trackers_admin.log sourcetype = trackme:rest_api
> 9/29/2026 6:54:47.009 AM	2026-09-29 05:54:47,009 INFO trackme.rest.splk_hybrid_trackers_admin trackme_libs.py trackme_create_report 3154 tenant_id="secops", attempting to update report_name="trackme_dsm_hybrid_tracker-prss3i9_wrapper_tenant_secops" with kwargs={"owner": "nobody", "sharing": "app", "perms.write": "trackme_admin", "perms.read": "trackme_user,trackme_power"} index = <u>_internal</u> source = /opt/splunk/var/log/splunk/trackme_rest_api_splk_hybrid_trackers_admin.log sourcetype = trackme:rest_api

< Back Close >

1 Update comment

Free text stored in the audit trail with this creation — useful months later.

2 Action progress events

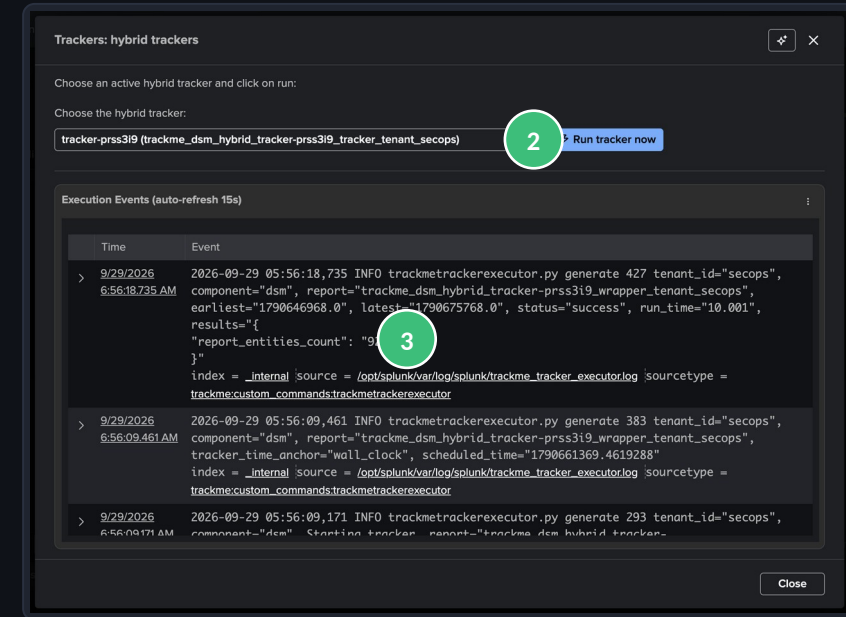
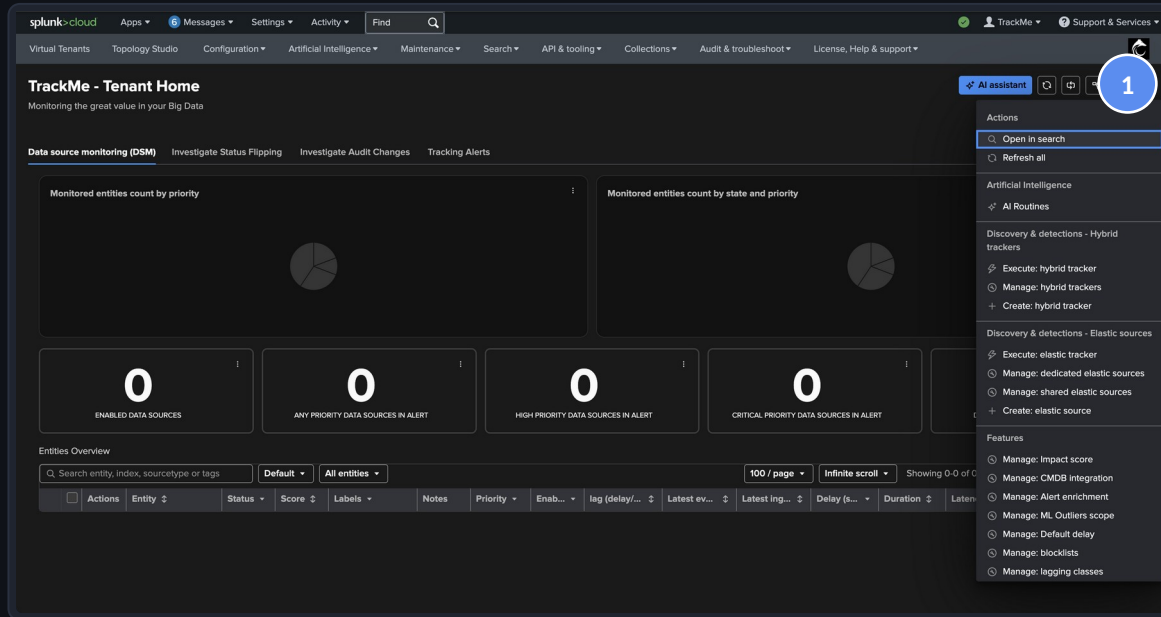
The wizard streams the REST log live: KV collections and transforms created per feature (outliers, sampling...), then the hybrid tracker report with its ACL — owner nobody, sharing app, write trackme_admin, read trackme_user + trackme_power.

What now exists

- the tenant record and its per-tenant KV Store
- a scheduled report: trackme_dsm_hybrid_tracker-
<id>_tracker_tenant_secops
- the wrapper report the tracker executor calls

...and zero entities, until the tracker runs.

Run the hybrid tracker once — or wait five minutes



1 Tenant Home → Actions

The  menu at the top right of Tenant Home groups everything tenant-scoped: hybrid trackers, elastic sources, impact score, CMDB, alert enrichment, ML scope, default delay, blocklists, lagging classes.

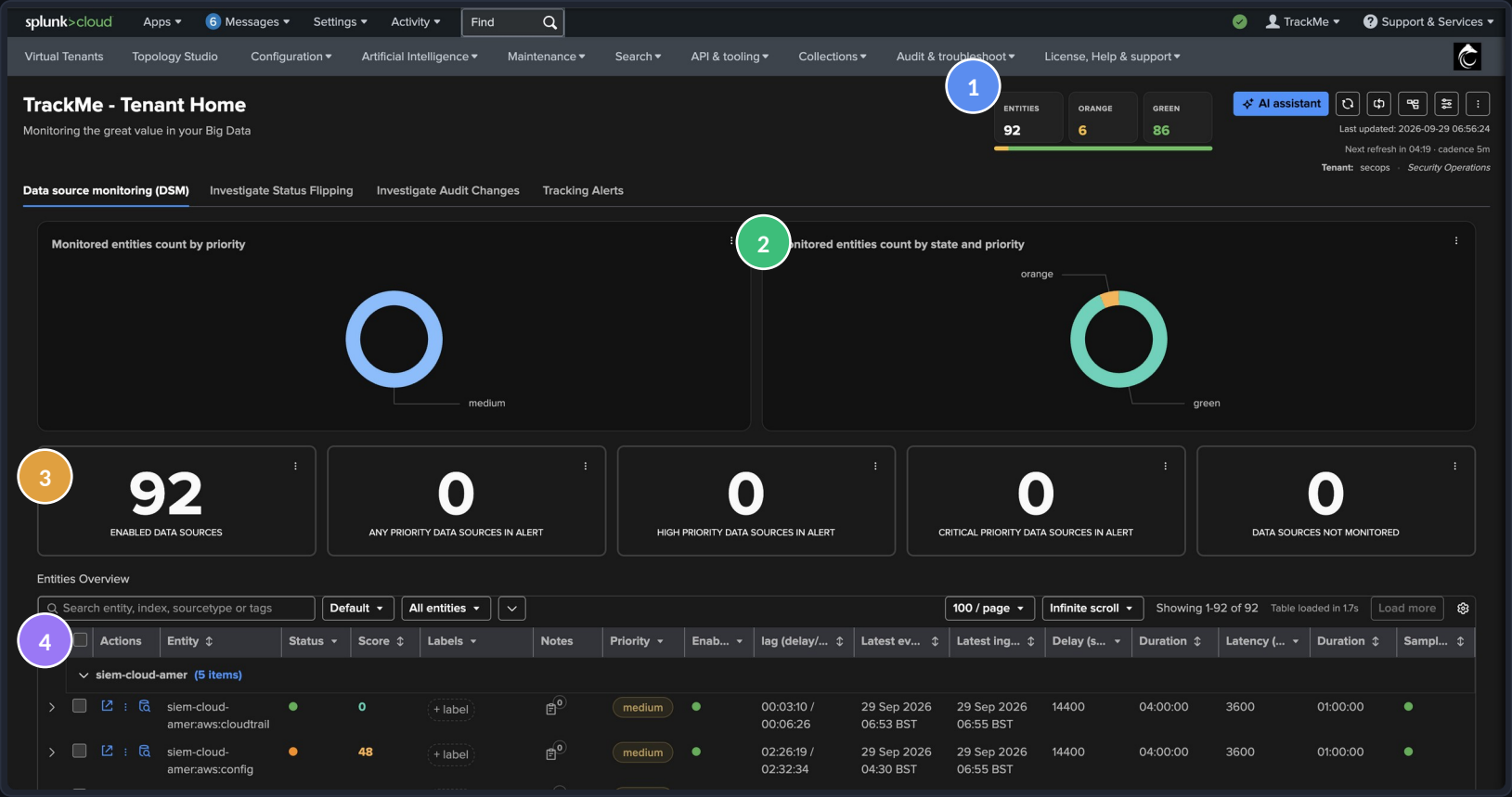
2 Execute: hybrid tracker

Pick the tracker created by the wizard and “Run tracker now”. The same modal streams the executor log.

3 One run, every data source

report_entities_count over earliest/latest of the last 8 hours. From here on the scheduler runs it every 5 minutes.

Tenant Home — every data source, already scored



- 1 Health strip**
Entities per state — computed by the decision maker on the tracker run we just made.
- 2 State x priority donut**
Everything is medium priority for now: discovery does not know what matters yet — that is what policies bring.
- 3 Single-stat drilldowns**
Click a tile — or a state in the health strip — and the table filters. Every number on the page is a filter.
- 4 Entities table**
One row per (index, sourcetype): state, score, labels, priority, lag (delay / latency), last event, last ingest, thresholds, outliers, sampling.

Reading the table — why are these orange?

92
ENABLED DATA SOURCES

0
ANY PRIORITY DATA SOURCES IN ALERT

0
HIGH PRIORITY DATA SOURCES IN ALERT

0
CRITICAL PRIORITY DATA SOURCES IN ALERT

0
DATA SOURCES NOT MONITORED

Entities Overview

Q Search entity, index, sourcetype or tags

Default

All entities

100 / page

Infinite scroll

Showing 1-6 of 6

Table loaded in 17s

Load more

Actions	Entity	Status	Score	Labels	Notes	Priority	Enab...	lag (delay/...	Latest ev...	Latest ing...	Delay (s...	Duration	Latency (...	Duration	Sampl...
4	siem-cloud-amer (1 items)		48	1		medium		2	2026	29 Sep 2026	14400	04:00:00	3600	01:00:00	
	siem-cloud-amer:aws.config		48			medium		02:26:19 / 02:32:34	2026	29 Sep 2026 06:55 BST	14400	04:00:00	3600	01:00:00	
	siem-cloud-apac (1 items)		48			medium									
	siem-cloud-apac:google:gcp:pubsub:message		48			medium		01:04:31 / 01:42:36	29 Sep 2026 05:51 BST	29 Sep 2026 06:55 BST	14400	04:00:00	3600	01:00:00	
	siem-cloud-emea (1 items)		48			medium									
	siem-cloud-emea:google:gcp:pubsub:message		48			medium		02:03:58 / 02:01:56	29 Sep 2026 04:52 BST	29 Sep 2026 06:54 BST	14400	04:00:00	3600	01:00:00	
	siem-cloud-latam (1 items)		48			medium									
	siem-cloud-latam:google:gcp:pubsub:message		48			medium		03:19:34 / 03:26:09	29 Sep 2026 03:36 BST	29 Sep 2026 06:55 BST	14400	04:00:00	3600	01:00:00	
	siem-identity-amer (1 items)														

- 1

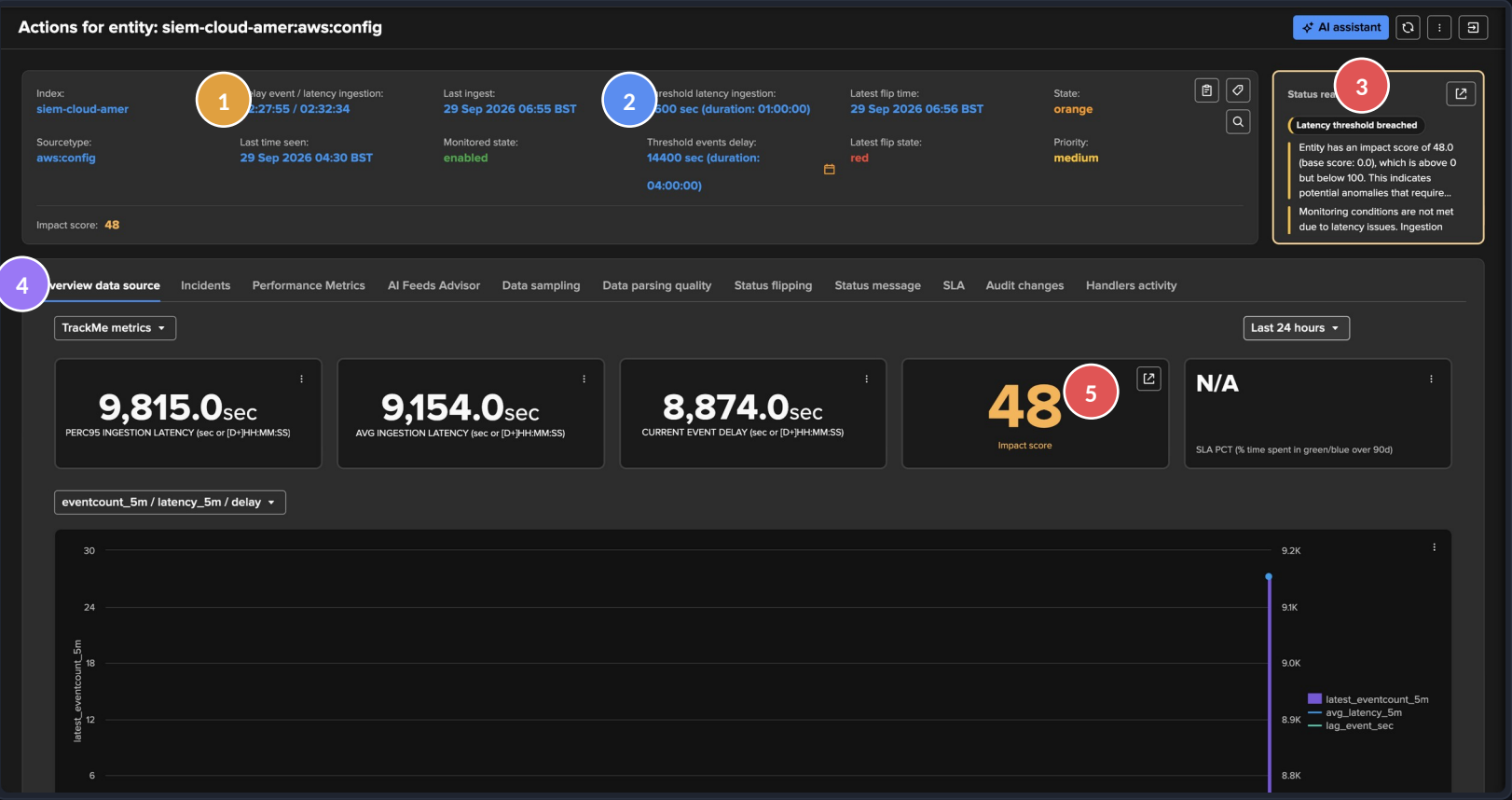
Score 48 = latency only
48 is below 100: orange. Add a delay breach (100) and the same entity turns red at 148 — additive, exactly as configured in step 1.
- 2

lag = delay / latency
02:26:19 / 02:32:34: last event 2h26 ago, indexed 2h32 after its timestamp. Latency is what breached.
- 3

Thresholds inline
Delay 14400 · duration 04:00:00 — the business_nights slot applied at run time. Latency 3600.
- 4

Grouped by index
The default grouping folds rows per index; here the table is filtered on orange from the health strip.

One entity — everything TrackMe knows about it



- 1 Delay 02:27:55 / latency 02:32:34
Last event seen 04:30, last ingest 06:55 — the events arrive, but late.
- 2 Thresholds
Latency 3600 s, delay 14400 s — the calendar icon opens the variable-delay editor for this entity.
- 3 Status reason
Latency threshold breached, with the score explained. No guessing.
- 4 Tabs
Overview, incidents, performance, AI Feeds Advisor, sampling, parsing quality, flipping, status message, SLA, audit, handlers.
- 5 Impact score 48
KPIs over 24 h: p95/avg latency, current delay, score, SLA % — one chart per metric.

Explainable by design — the status message

Actions for entity: siem-cloud-amer:aws:config

Index:
siem-cloud-amer

Delay event / latency ingestion:
02:27:55 / 02:32:34

Source type:
aws:config

Impact score: 48

Last ingest:
29 Sep 2026 06:55 BST

Last time seen:
29 Sep 2026 04:30 BST

Monitored state:
enabled

Threshold latency ingestion:
3600 sec (duration: 01:00:00)

Latest flip time:
29 Sep 2026 06:56 BST

State:
orange

Threshold events delay:
14400 sec (duration: 04:00:00)

Latest flip state:
red

Priority:
medium

Status reason

Latency threshold breached

Entity has an impact score of 48.0 (base score: 0.0), which is above 0 but below 100. This indicates potential anomalies that require...

Monitoring conditions are not met due to latency issues. Ingestion

Overview data sourceIncidentsPerformance MetricsAI Feeds AdvisorData samplingData parsing qualityStatus flippingStatus messageSLAAudit changesHandlers activity

Last 7 days

Status Message

Latency threshold breached

Entity has an impact score of 48.0 (base score: 0.0), which is above 0 but below 100. This indicates potential anomalies that require attention but do not yet warrant a critical alert status.

Monitoring conditions are not met due to latency issues. Ingestion latency is approximately 9153.875 seconds (duration: 02:32:33), which is higher than the maximum allowed latency of 3600 seconds (duration: 01:00:00), latest event available (_time) for this entity: 29 Sep 2026 04:30 BST, latest event indexed (_indextime) for this entity: 29 Sep 2026 06:55 BST, this indicates that the source is receiving delayed events only

IMPACT SCORE BREAKDOWN

Contribution	Detail	Score
Base score	Score events over the last 24 hours	0
Latency threshold breach	Latency threshold breached	+48
Total impact score		48

3Raw JSON

1 Status message

“Monitoring conditions are not met due to latency issues. Ingestion latency is approximately 9153 seconds (02:32:33), higher than the maximum allowed latency of 3600 seconds.” Human-readable, and what goes into the alert email.

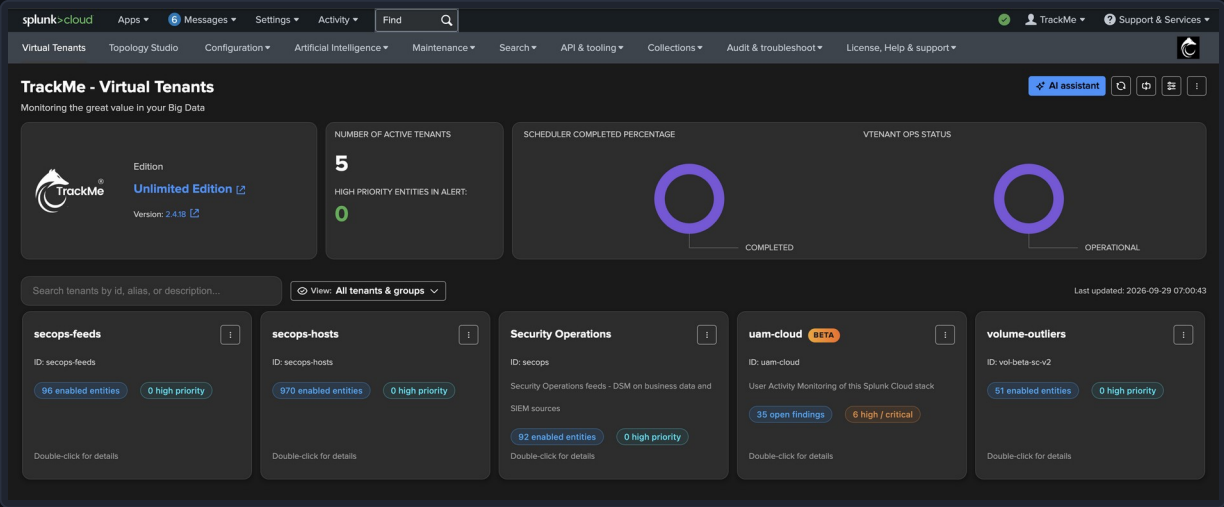
2 Impact score breakdown

Base score 0 + latency threshold breach 48 = total 48. The arithmetic behind the colour, per entity, per cycle.

3 Raw JSON

One toggle shows the structured status behind the view — the same document the AI Assistant and the alerts consume.

Where we are



In this part

- Created** the secops tenant with DSM and its hybrid tracker, in one wizard
- Discovered** every data source of the SIEM index families — no manual list
- Decided** a state, a score and a reason for every entity, from the first run
- Read** one entity end to end: latency vs threshold, score breakdown, status message

What made it work

Auto-discovery

The hybrid tracker finds every index × sourcetype pair in scope — nothing to declare, nothing to maintain.

Tenant defaults

Impact weights and variable delay are set once in the wizard, inherited by every entity, overridable per entity.

Explainable state

Every colour carries a score, a breakdown and a sentence — the same text an alert will use.