



Monitoring the great value in your Big Data

HANDS-ON WALKTHROUGH · PART 3

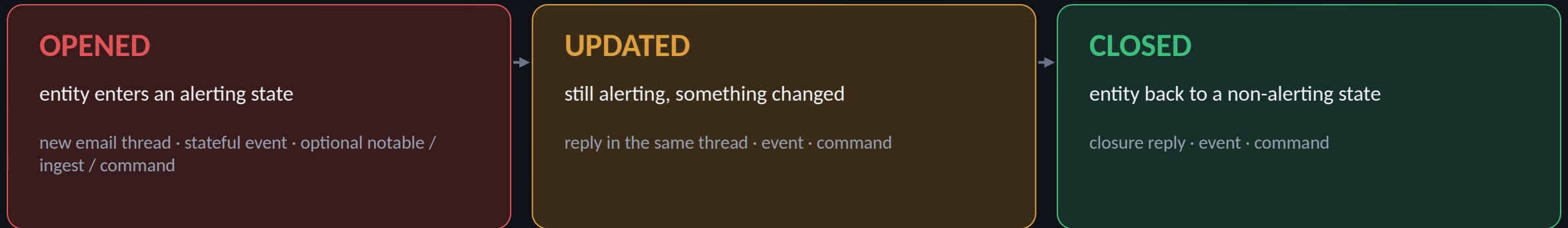
Stateful alerting

One alert on the tenant, scoped to critical and high. Then we break one entity on purpose and follow the incident: opened, emailed, recorded, closed.



Stateful alerting in a nutshell — one incident per problem

Classic alerts fire every cycle an entity is red. TrackMe keeps one incident record per problem and only speaks on transitions — with the whole context attached.



What feeds it

- **trackme:flip** state transitions — the source of opened / closed
- **trackme:state** each cycle's state and score per entity
- **trackme:notable** the notable events TrackMe writes for anomalies
- **trackme:sla_breaches** SLA breaches, when SLA classes are used

Persisted, keyed, threaded

Each incident has an `incident_id`, lives in the KV Store with its embedded charts, and writes `trackme:stateful_alerts` events to the summary index. The email carries a Message-ID; updates and closure are In-Reply-To — one thread per incident in your mailbox or ticketing tool. Suppression (60 min on `event_id` by default) stops repeats within an incident.

Where — Tracking Alerts → Actions → Create a new alert

The alert lives in the Splunk scheduler as a saved search named “TrackMe alert tenant_id:<tenant> - <name>” — visible in Settings → Searches, reports and alerts like any other.

1 Tracking Alerts tab

Fourth tab of Tenant Home — alerts are tenant-scoped like everything else.

2 Two counters

Enabled alerts · triggered in the past 24 h. Both 0 on a fresh tenant.

3 Alert details table

Cron, schedule window, suppress fields / period, actions, next scheduled time.

4 Actions → Create a new alert

Opens the assisted alert wizard. AI Routines also live here.

Step 1 — Pick the alert type, name it

Alert tracking definition - Use this interface to create a custom alert in assisted mode.

Choose the type of alert to be tracked:

1 KME STATEFUL ALERTS NOTABLE EVENTS SPLK-DSM (DATA SOURCES) SLA BREACHES

> About TrackMe Stateful Alerting

2 Alert name

Enter the unique identifier of the new alert. The prefix "TrackMe alert tenant_id: <tenant>" will be added automatically.

Alert identifier:

stateful-alert

Full alert name: TrackMe alert tenant_id:secops - stateful-alert

2 Stateful main features

3 Acknowledgement

3 Various

Cancel Add this new alert

1 Four alert types

TrackMe stateful alerts (the modern path, used here) · Notable events (classic ES-style) · SPLK-DSM data sources · SLA breaches.

2 About TrackMe stateful alerting

The expander explains the model in the product — worth opening once in a session.

3 Alert identifier

stateful-alert → full name "TrackMe alert tenant_id:secops - stateful-alert". Four wizard steps: name, stateful features, acknowledgement, various.

One alert per tenant is usually enough: the priority filter and suppression do the routing. Several alerts make sense when different teams want different recipients or channels.

Step 2 — Delivery mode and email configuration

Alert tracking definition - Use this interface to create a custom alert in assisted mode.

Choose the type of alert to be tracked:

TRACKME STATEFUL ALERTS NOTABLE EVENTS SPLK-DSM (DATA SOURCES) SLA BREACHES

> About TrackMe StateFul Alerting

1 Alert name

2 Stateful main features

1 Acknowledgement

4 Various

2

3

4

Delivery Mode

Mode:

Emails and Ingest

Email Configuration

Select an account:

ovh

Environment name (added to the email header):

Splunk

* List of Recipients: (type an email and press Enter to add)

xxxxx@mydomain.com X

Send update emails if entity Ack is active?

Yes

Send emails notifications for all priority levels?

Select priority levels that should trigger email notifications. Leave empty to send emails for all priority levels.

Cancel Add this new alert

1 Mode: Emails and Ingest

Deliver by email and write the stateful event to the summary index. Other modes: emails only, ingest only, plus notable / command actions.

2 Email account

An SMTP account configured once in TrackMe. Environment name goes in the subject / header.

3 Recipients

Chips — type and press Enter. A distribution list or a ticketing inbox is typical.

4 Update emails if ACK is active

Whether an acknowledged entity keeps sending updates.

Step 2 — Who gets emailed, charts, AI status report

Alert tracking definition - Use this interface to create a custom alert in assisted mode.

1 Send update emails if entity Ack is active?

Yes

2 Send emails notifications for all priority levels?

Select priority levels that should trigger email notifications. Leave empty to send emails for all priority levels.

Critical X High X

Selected: critical, high

Charts Generation

2 Generate charts?

Yes

Charts theme:

Dark

Charts time window:

24h

AI Status Report

3 Include AI status report in emails?

When enabled, an AI-generated entity status summary will be included in email notifications.

Yes

AI Provider:

Default (first available)

Cancel Add this new alert

1 Priority levels for email

Critical + High. Everything is still tracked and ingested; only these priorities generate email. This is where Part 2's classification pays off — no policy, no filter.

2 Charts generation

Yes · dark theme · 24 h window. Latency, delay, volume, hosts, incidents, flipping and state charts are rendered and embedded in the email.

3 AI status report

Optional LLM summary in the email, using the configured AI provider — entirely opt-in; the alert works without it.

Steps 3 (acknowledgement) and 4 (various: cron, suppression, throttling) were left on their defaults.

The alert exists — a scheduled search with TrackMe actions

Virtual Tenants

Topology Studio

Configuration

Artificial Intelligence

Maintenance

Search

API & tooling

Collections

Audit & troubleshoot

License, Help & support

TrackMe

Messages

Settings

Activity

Help

Find

TrackMe - Tenant Home

Monitoring the great value in your Big Data

AI assistant

Last updated: 2026-09-08 17:16:45

Next refresh in 04:39 - cadence 5m

Tenant: secops - Security Operations

Data source monitoring (DSM)

Investigate Status Flipping

Investigate Audit Changes

Tracking Alerts

1

ENABLED ALERTS

0

TRIGGERED ALERTS IN THE PAST 24h

Alert details

Filter by title...

Actions	Alert...	title +	cron_schedule	schedule_window	suppress_fields	suppress_period	actions	disabled	next_scheduled_time
		TrackMe alert tenant_id:secops - stateful-alert	2	auto	3	60m	4	0	2026-09-08 16:21:00 UTC

1

1 enabled alert
Green status dot. Triggered in the past 24 h still 0 — nothing critical or high is red yet.

2

cron 1-56/5 * * * *
Every 5 minutes, offset from the trackers so it evaluates fresh state.

3

suppress event_id · 60m
Splunk-side throttling on the incident event id — a safety net on top of the stateful logic.

4

actions
add_to_triggered + trackme_stateful_alert — the TrackMe alert action that opens, updates and closes incidents.

The pencil / ⋮ in the Actions column edits or disables the alert; the same definition is editable in Splunk's alert page.

TrackMe for Splunk · Hands-on: stateful alerting

docs.trackme-solutions.com

Provoke an incident — manually influence the score

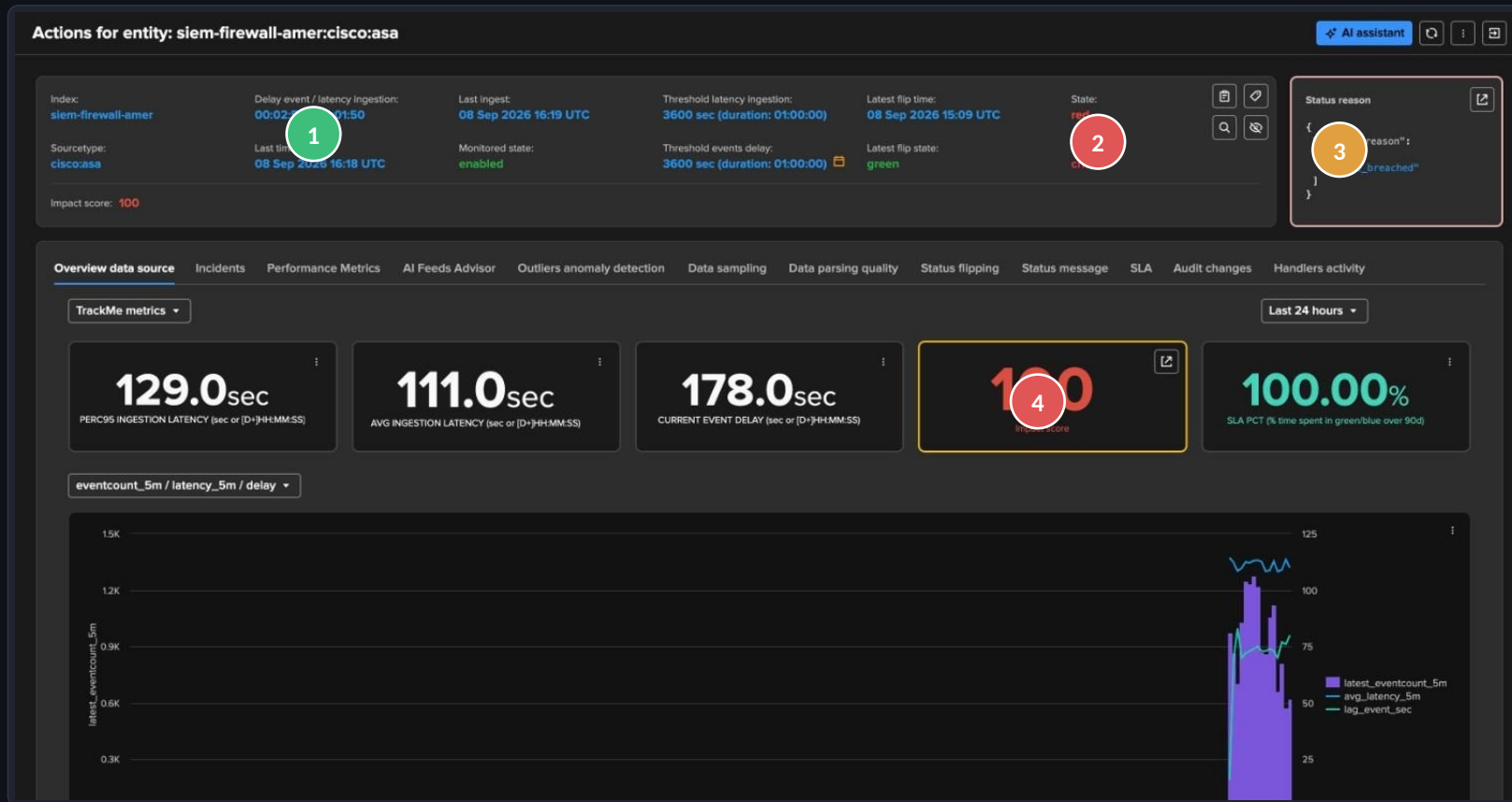
The screenshot displays the 'Actions for entity: siem-firewall-amer:cisco:asa' page. The entity status is 'green' with an impact score of 0. A modal titled 'Manually influence the Score' is open, showing options to 'Add to score (increase)' with a value of 100. A comment box contains the text: 'Force this entity to turn red, for the validation of stateful alerting'. The modal also includes a 'Confirm' button.

- Entity : menu**
Manually influence the score, false positive, disruption queue, lagging classes, priority, maintenance...
- A healthy critical entity**
siem-firewall-amer:cisco:asa — green, score 0, priority critical from the CMDB policy.
- Add 100 to the score**
With a comment. Audited as a manual_score event; a score_breached anomaly is recorded.

Why this is a good demo device

It shows a real feature — operators use score influence to force attention on an entity, or to soften one — and it produces a deterministic red state on a healthy feed without touching data or thresholds. Because the entity is critical, it passes the alert's email filter. Every step is in the entity's audit trail, and the AI status report will even say it was a manual override.

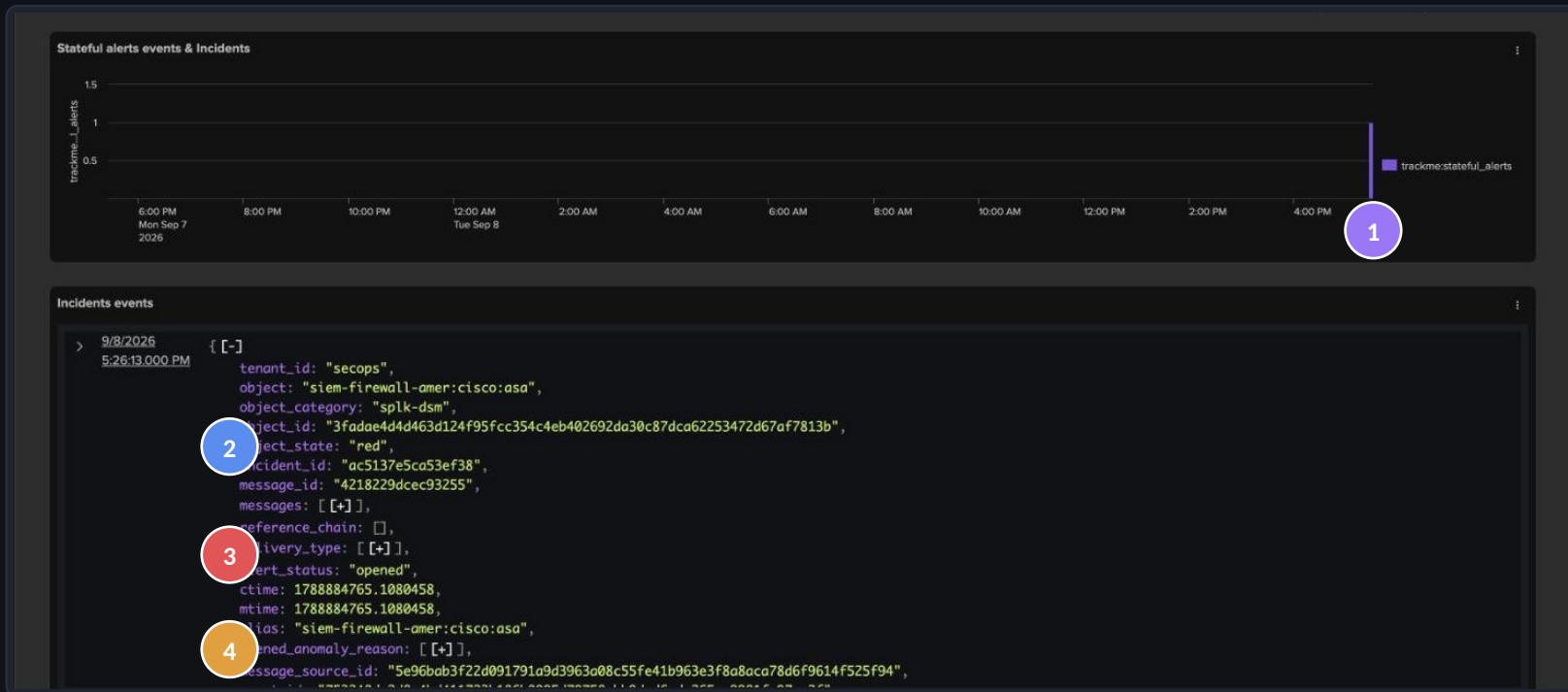
Red by decision, not by data — score_breached



- Metrics still healthy**
Delay 02:59, latency 01:50, thresholds 3600 — nothing wrong with the feed.
- State: red**
Latest flip 16:24 UTC, priority critical.
- anomaly_reason: score_breached**
The status reason names the manual influence — no false “delay” story.
- Impact score 100**
= manual component. score_definition in the Status message tab shows it.

The next alert run (every 5 minutes) sees a critical entity in red with no open incident — and opens one.

Incident opened — the Incidents tab of the entity



1 Stateful alerts events

One bar at 17:26 — the alert run that opened the incident.

2 incident_id · message_id

ac5137e5ca53ef38 is the incident key; message_id is the email Message-ID.

3 alert_status: opened

With object_state red, ctime = mtime, delivery_type listing email + ingest.

4 opened_anomaly_reason

score_breached — what was wrong when the incident opened, kept for the closure.

Everything on this tab is the trackme:stateful_alerts event — the same document that is in the KV Store and the summary index.

The email — opened, with the reason and 24 h of context

✓ TrackMe Notification

Environment: Splunk

Detection Time: Tue Sep 8 16:46:07 2026 UTC

Alert Status: closed

Tenant: secops

Alias: siem-firewall-amer:cisco:asa

Object: siem-firewall-amer:cisco:asa

Priority: critical

[Drilldown Link](#)

Status: green

Impact score: 0

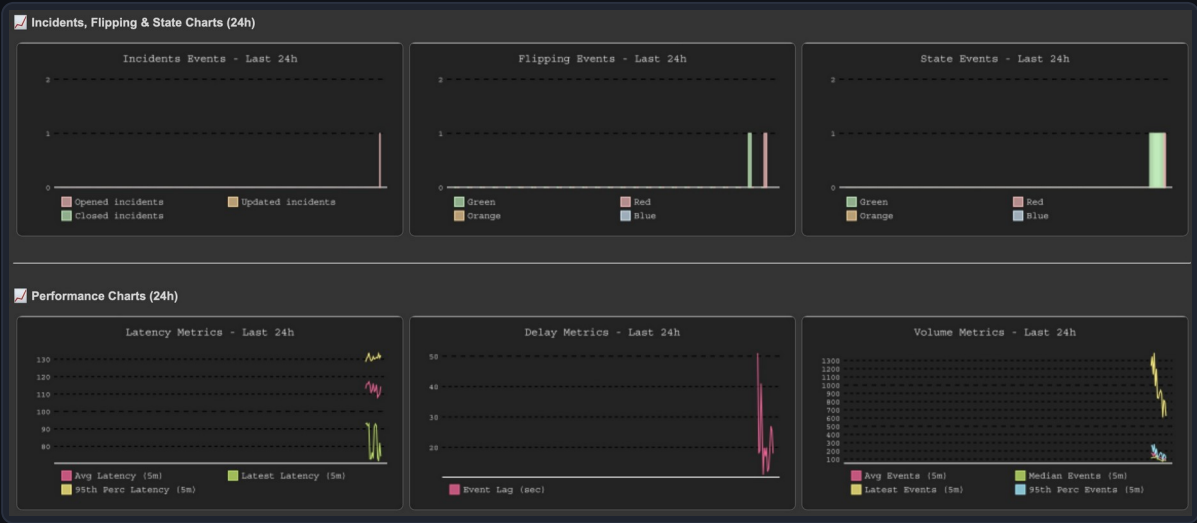
Incident ID: ac5137e5ca53ef38

📁 Detailed Information:

✓ The entity has received an incident closure update and is now in a non-alerting state:

- Alias: siem-firewall-amer:cisco:asa
- Object: siem-firewall-amer:cisco:asa
- Object ID: 3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b
- Category: splk-dsm
- Anomaly Reason(s):
 - score_breached
- Message(s):
 - 08/09/2026 16:43:27, object="siem-firewall-amer:cisco:asa" has flipped from previous_state="red" to previous_anomaly_reason="score_breached", disruption_time="17.33"
 - monitoring conditions for event delay are met. Event delay is 76.0 seconds (duration: 00:01:16), wh (duration: 01:00:00), latest event available (_time) for this entity: 08 Sep 2026 16:43 UTC
 - monitoring conditions for ingest latency are met. Ingestion latency is approximately 108.667 seconds (duration: 01:00:00), latest event indexed (_indextime) for this entity: 08 Sep 2026 16:44
- Message source: trackme:flip
- Message source ID: ccb90ba677534585f51792318c461057d111b5bf7a9a081329e57034bcddd0fe

Header, status, detailed information (closure email shown — the opened email has the same layout with status opened / red / 100)



Incidents, flipping and state charts + latency, delay, volume and hosts — last 24 h, rendered by TrackMe

Subject “[TrackMe Incident-ID: <id>] Entity <object>” · environment, detection time, alert status, tenant, alias, priority, drilldown link · status, impact score, incident id · the flip message and the score explanation verbatim · then the AI status report and the charts. Replies land in the same thread.

The AI status report — optional, and honest about the cause

🤖 AI Status Report (AI-generated content):

Alert Summary: siem-firewall-amer:cisco:asa

Current Status

Entity State: Red (Alert)

Entity Type: Data Source Monitoring (DSM)

Priority: Critical

SLA Class: Silver

Last Updated: Just now

What Is Happening

This Cisco ASA firewall data source is currently in a **red alert state** due to a **manual score influence** that has been applied to the entity without any underlying technical anomaly detected. The entity's health score has been manually set to 100 (maximum alert severity), overriding the normal automated health assessment.

Key Metrics (Current):

- Last event received: ~39 seconds ago
- Event delay: ~39 seconds (within threshold)
- Ingestion latency: ~114 seconds (within threshold)
- Active hosts reporting: 25 (5-minute average)
- Total events in last ~18 minutes: 22,610

The data flow itself appears healthy — events are arriving regularly, latency is acceptable, and host count is stable.

Why This Alert Was Triggered

The red state reflects a **manual override** rather than a detected data delivery problem. This typically occurs when:

- An operator manually adjusted the entity's score for administrative reasons (e.g., planned maintenance acknowledgment, temporary suppression, or policy enforcement)
- A priority or policy rule was applied that forces alert status independent of actual data health

Current Acknowledgment Status:

- The entity is currently acknowledged
- Acknowledgment expires in approximately 24 hours

What to Investigate First

1. Review the Manual Score Reason

Check the entity's notes and recent activity log in the TrackMe UI to understand why the manual score was applied. Look for any maintenance windows, policy changes, or operator comments that explain the override.

1. Verify Data Delivery Health

The actual data metrics are healthy:

- Event delay is ~39 seconds (well within the 3600-second threshold)
- Ingestion latency is ~114 seconds (acceptable)
- Host count is stable at 25 active hosts

If no underlying issue exists, consider whether the manual score is still necessary.

1. Check Acknowledgment Expiration

The current acknowledgment will expire in ~24 hours. Decide whether to:

- Extend the acknowledgment if the manual override should remain in place
- Remove the manual score influence if the issue has been resolved
- Investigate the root cause if this was triggered by an unexpected event

1. Review Recent Changes

Look at the entity's modification history to see if any threshold changes, policy updates, or configuration adjustments were made recently that might have triggered this alert.

Next Steps

1

Current status

State, entity type, priority, SLA class, last updated — structured header.

2

What is happening

Identifies the manual score influence as the cause and confirms the data flow itself is healthy: delay ~39 s, latency ~114 s, 25 hosts.

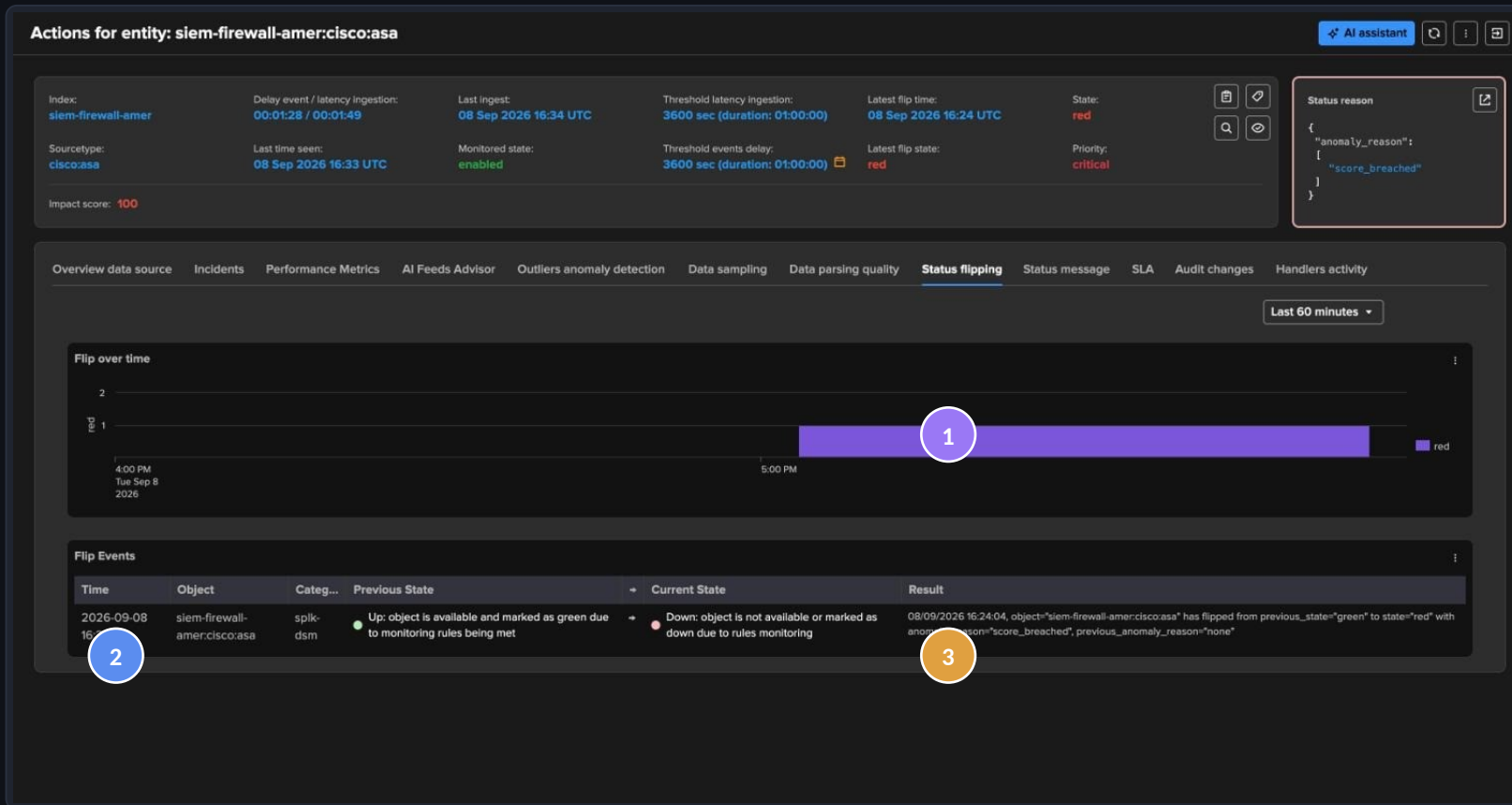
3

What to investigate first

Ordered steps: review the manual score reason, verify delivery health, check the acknowledgment, review recent changes.

Grounded in TrackMe's data, not free prose: the report reads the entity's metrics and audit context through the same tools the AI Assistant uses. Opt-in per alert, provider configured once.

Status flipping — every state change is recorded



1 Flip over time

Red since 16:24 — the timeline of the entity's states.

2 Flip events

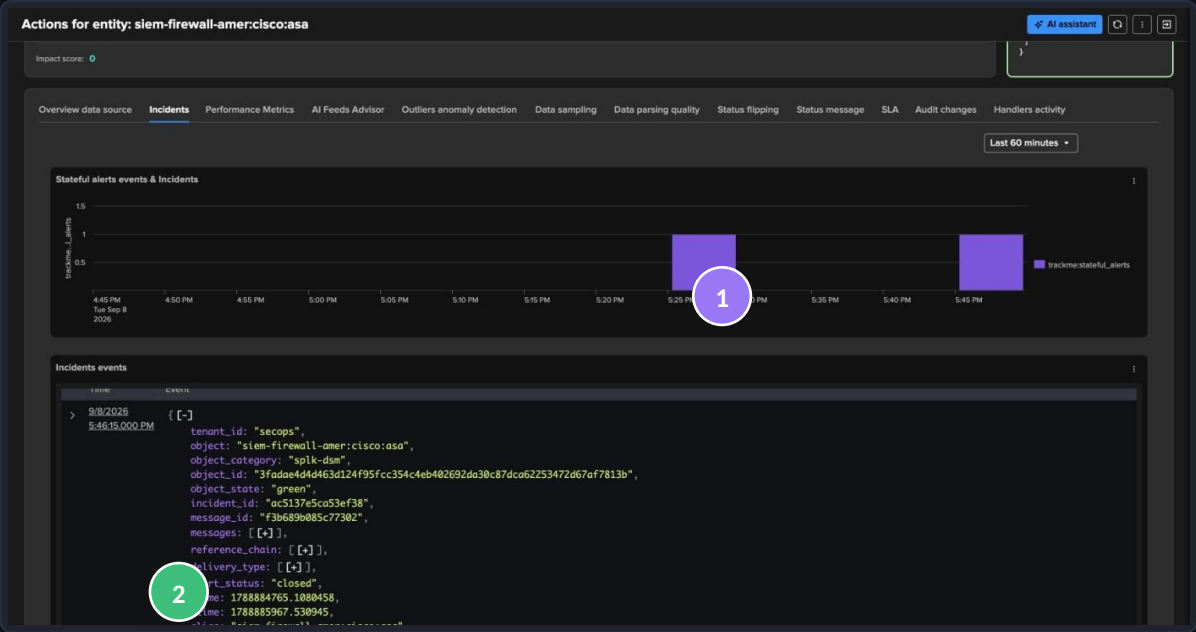
16:24:04 · previous state green (Up) → current state red (Down).

3 Result

"has flipped from previous_state=green to state=red with anomaly_reason=score_breached, previous_anomaly_reason=none" — the trackme:flip event.

Flip events are the raw material of stateful alerting: the incident opened because of this flip, and will close on the next one. They are also what the Investigate Status Flipping tab of Tenant Home aggregates.

Incident closed — score removed, entity green, one closure email



TrackMe Notification

Environment: Splunk

Detection Time: Tue Sep 8 16:46:07 2026 UTC

Alert Status: closed

Tenant: secops

Alias: siem-firewall-amer:cisco:asa

Object: siem-firewall-amer:cisco:asa

Priority: Critical

Drift: 0.0

Status: green

Impact score: 0

Incident ID: ac5137e5ca53ef38

Detailed Information:

The entity has received an incident closure update and is now in a non-alerting state:

Alias: siem-firewall-amer:cisco:asa

Object: siem-firewall-amer:cisco:asa

Object ID: 3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b

Category: splk-dsm

Entity Reason(s): score_breached

Message(s):

- 08/08/2026 16:43:27, object="siem-firewall-amer:cisco:asa" has flipped from previous_state="red" to previous_anomaly_reason="score_breached", disruption_time="17.33"
- monitoring conditions for event delay are met. Event delay is 76.0 seconds (duration: 00:01:16), with (duration: 01:00:00), latest event available (time) for this entity: 08 Sep 2026 16:43 UTC
- monitoring conditions for ingest latency are met. Ingestion latency is approximately 108.667 seconds (duration: 01:00:00), latest event indexed (indextime) for this entity: 08 Sep 2026 16:44

Message source: trackme:flip

Message source ID: ccb90ba677534585f51792318c461057d111b5bf7a9a081329e57034bcddd0fe

1 Two stateful events

17:26 opened, 17:46 closed — same incident_id ac5137e5ca53ef38, alert_status closed, object_state green.

2 Closure record

mtime updated, new message_id — the closure email is a reply in the original thread.

3 Closure email

green header, status closed, impact score 0; the flip message red → green with disruption_time 17.33 min, delay and latency back within thresholds.

Under the hood — it is all Splunk events

splunk>Enterprise

New Search SPL Convert to SPL2 Save As Create Table View Close

(index=trackme_summary sourcetype=trackme:stateful_alerts tenant_id="secops" object_category=splk-dsm (object="sien-firewall-amer:cisco:asa" OR object_id="3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b" OR keyid="3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b")) OR (index=trackme_notable tenant_id="secops" object_category=splk-dsm (object="sien-firewall-amer:cisco:asa" OR object_id="3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b" OR keyid="3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b"))

Time range: Last 60 minutes Q +

✓ 2 events (08/09/2026 15:48:00.000 to 08/09/2026 16:48:27.000) No Event Sampling Job || ↶ ↷ ⬇ Smart Mode

Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection x Deselect 1 minute per column

Format Show: 20 Per Page View: List

i	Time	Event
>	08/09/2026 16:46:15.000	{ [-] alert_status: closed alias: sien-firewall-amer:cisco:asa cti: 14765.1080458 detection_time: [[+]] detection_time: Tue Sep 8 16:46:07 2026 UTC drilldown_link: https://prd2-standalone.trackme-limited.com/splunk/app/trackme/TenantHome?tenant_id=secops&component=dsn&keyid=3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b event_id: 7dd86f138d447ab258aedf11d59f555d789070b07afdb6f3f926879977a5d893 incident_id: ac5137e5ca53ef38 message_id: f3b689b085c77382 message_source: trackme:flip message_source_id: ccb90ba677534585f51792318c461057d111b5b77a9a081329e57034bcd09fe messages: [[+]] mtime: 178885967.530945 object: sien-firewall-amer:cisco:asa object_category: splk-dsm object_id: 3fadae4d4d463d124f95fcc354c4eb402692da30c87dca62253472d67af7813b object_state: green named_splk_category: f f3f

SELECTED FIELDS
a host 1
a index 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a alert_status 2
a alias 1
ctime 1
a delivery_type[] 2
a detection_time 2
a drilldown_link 1
a event_id 2
a incident_id 1
linecount 1
a message_id 2
a message_source 2
a message_source_id 2
a messages[] 4
mtime 2

1 Open in search

From the entity's Incidents panel — the SPL over `index=trackme_summary sourcetype=trackme:stateful_alerts` (and `trackme_notable`) for this object.

2 2 events

opened and closed, in the last 60 minutes.

3 Fields

`alert_status`, `detection_time`, `drilldown_link`, `event_id`, `incident_id`, `message_id`, `message_source`, `object_state`... ready for a dashboard, a ticketing integration, or a report on incidents per team.

Because incidents are events, anything Splunk can do with events applies: MTTR by priority, incidents per tag, forwarding to ITSM, correlation in ES.

Where we are

In this part

● Created

one stateful alert: emails + ingest, critical & high only, charts, AI report

● Provoked

a red state on a healthy critical entity with a manual score influence

● Followed

the incident: opened → email with reason and charts → flip recorded → closed with disruption time

● Verified

the trail as Splunk events — two trackme:stateful_alerts events with every id

What made it work

One incident per problem

opened, updated, closed — one record and one email thread, speaking only on transitions

Classification pays off

the priority filter from the policies decides who gets emailed; every incident is still recorded

Everything is a Splunk event

incidents are searchable, reportable and forwardable — MTTR, dashboards, ITSM, Enterprise Security