SpikeTrendWatch

Global event intelligence

Source-backed updates for readers, teams, and the systems they use.

What changed since the first report?

A headline starts the clock. Teams still need to establish scope, assess exposure, and brief the next shift.

Fragmented evidence

Provider notices, agency statements, and reporting arrive on different clocks.

Operational relevance

A regional disruption matters when it touches a service someone depends on.

Accountability

A team needs to reconstruct what it knew when it acted.

One event record serves four products

A shared record connects evidence, geography, revisions, and delivery.

SpikeTrendWatch

Public desks, event timelines, and source links.

My Spike

Personal workspace for saved interests and watchlists.

Spike Pro

Monitoring and alerts for individuals and teams, in free beta.

Spike Intel Cloud

Incident records, a change feed and signed delivery for enterprise systems, offered through pilots.

Global coverage, local consequences

Spike connects developments across desks when the evidence supports a relationship.

Cyber Watch	Advisories, known-exploited catalog updates, and unverified ransomware claim aggregates.
Markets & global affairs	Follow developments by organization, sector, and geography.
Weather, transport & real estate	Planned: a flood warning and a road closure mapped to a property portfolio.

The NSA network disruption

Spike grouped news reports into one event record. An NSA spokesperson told news organizations that some internal systems were affected during scheduled routine maintenance and that mission-critical capabilities remained operational.

Published record

The event page and its API both list the United States. An earlier mismatch, an empty places field in the API, was found and fixed.

Attribution

The record links the NSA's own statement, as given to CBS, AP and Newsweek, and labels it as the agency's account.

Open questions

The record lists what the statement leaves open: duration, affected systems and cause beyond maintenance.

The second and third updates drive decisions

Illustrative example: a regional identity-provider disruption.

01 Initial observation

An early signal opens an incident. Scope remains uncertain.

02 Provider confirmation

The provider confirms regional impact. Operations checks the affected business service.

03 Material scope change

The provider expands the affected region. Spike delivers the revision to newly relevant teams and updates prior recipients.

Minute monitoring, hourly reconciliation

Provider status pages are read every minute. Source publication and observation times are kept for every change.

Minute loop

Capture meaningful changes and retain source publication and observation times.

Hour loop

Revisit open incidents, reconcile conflicting claims, and check recovery or stale feeds.

Corrections

Publish reviewed corrections promptly and preserve the superseded record.

Publication Analysis & Intelligence Review

Each review ties a publication decision to its evidence and delivery record.

Before publication

Record the sources, uncertainty, and exact claims Spike will publish.

After publication

Check for missing primary evidence, duplicated signals, and mismatches across web, API, and alerts.

Proof

Measure time to a useful update, correction lag, and recoverability after a missed delivery.

The API behind the incident record

The API supports integrations that need updates, audit history and recovery after an interruption.

Record

Stable incident IDs, claim-level evidence, revisions, and machine-readable changes.

Deliver

Filtered change feeds, signed webhooks, retries, and replay from a cursor.

Protect

Per-workspace API keys, tenant isolation, audit logs and documented source rights.

Every buyer uses the record differently

Operational resilience is the first design-partner profile.

Banks & regulated enterprises	Match external incidents against private vendor and business-service inventories.
Newsrooms & platforms	Embed sourced event data and propagate corrections to downstream consumers.
Public-sector teams	Follow affected services and official statements by jurisdiction.

Public event pages lead into monitoring

Every source-backed event page is a useful entry point, and a reason to come back.

Discover

Searchable incident timelines and partner embeds introduce readers to Spike.

Return

Saved interests and relevant updates bring readers back to My Spike.

Go further

Spike Pro (free beta) serves individual and team monitoring. Enterprise pilots bring the data into existing workflows.

A paid pilot starts with one watchlist

Scope the first offer around a buyer-approved set of critical cloud, identity, payment, or telecom dependencies.

Pilot package	Historical replay, live watchlist, and a delivery path into the buyer’s operations.
How success is measured	Measure useful alert speed, relevance, missed incidents, and correction delivery against the buyer’s baseline.
Getting started	Pilots are scoped with each team. Write to contact@spiketrendwatch.com.

A record you can check

Every change is kept, every claim links to its source, and corrections travel with the record.

Revision history

Each incident keeps every numbered revision, so a team can see what it knew and when.

Corrections

Reviewed corrections reach everyone who received the earlier version, and can be replayed.

What comes next

Vendor disruption first. Planned: geographic disruption for weather, transport and real estate.

Explore today, discuss a pilot

Explore and Monitor are live on spiketrendwatch.com today. Pilots are scoped with each enterprise team.

Explore

Event timelines, Cyber Watch, the Outages desk, and the public API and change feed. Free.

Monitor

Spike Pro, in free beta: watched services and alerts by email, Slack, Teams or signed webhook.

Pilot

Enterprise teams can scope a vendor-disruption pilot: one watchlist, historical replay, and delivery into their own tools.

Explore SpikeTrendWatch

spiketrendwatch.com

Readers can explore Cyber Watch and public event timelines.

Enterprise teams can discuss a scoped vendor-disruption pilot.

Developers can start with the public API at spiketrendwatch.com/developers.