DemandFlow Monitoring and SIEM

DEMANDFLOW®

Events from every network source, matched to the asset, service and customer behind them

DATA SHEET

A telco's events land in a monitoring stack that sits apart from the estate. The log line names a host; nothing connects it to the platform it belongs to, the service it carries or the customer who will ring. A full security operations platform fixes that at a price: expensive to license, slow to fill with asset context and dependent on a specialist team.

DemandFlow® ingests events from the network, security and application sources you already have, normalises them, stamps each one with the device, platform, site, interface and link it concerns, evaluates rules every minute and routes alerts to the places your teams work. Because it runs inside the platform that holds the assets, services and customers, an alert on an OLT already knows the service and the customers behind it.

What it is

Log collection, search, alerting and triage for operators and service providers: one HTTPS ingest endpoint with per-source keys; parsers for JSON, syslog, CEF and vendor formats; a normalised envelope with asset and network context added at ingest; a per-tenant store with hot retention and an archive you can search; source health and volume metrics; threshold, pattern, absence and correlation rules; an alert workflow with cooldown, auto-close and incident folding; routing to Slack, Teams, email and webhooks through integration flows; tickets raised by hand or by rule; dashboards on the designer; and a service impact console that maps open alerts to services and customers.

It sits inside DemandFlow, so the collector's own command audit arrives as a source, a link alert carries the circuits and customers that ride on it, outage impact from a link alarm traces the fibre beneath, and the Sense audit chain and the network change calendar use the same records.

What an operator gets

- **Every event in context.** Matched at ingest to the device, RAN node, IT asset or site, and for network events to the interface and link, so the alert names the platform, service and owner.
- **One endpoint, many formats.** JSON, syslog RFC 5424 and 3164, CEF, and vendor syslog for Nokia SR OS, Juniper Junos, Arista EOS and Cisco IOS XR; IP Fabric intent findings too.
- **Rules that understand the network.** Threshold, pattern, absence and correlation, scoped to a platform or a set of sources, evaluated every minute.
- **Alerts that do not flood.** Cooldown, auto-close when the condition clears, and folding of alerts on the same link or interface into one incident whose count grows and severity rises.
- **Routed where people are.** Slack, Teams, email and webhooks through a flow, drawn on the rule so you can see where an alert goes and what the last delivery did.
- **Tickets with the asset attached.** Raised from an alert or an event by hand, or automatically per rule, with the asset linked and the ticket reference written back.
- **Impact, not just noise.** Open alerts mapped through the dependency graph to services and customers, grouped by probable root cause, with maintenance windows suppressed.
- **Retention you control.** Hot retention per tenant, archive to your own bucket as compressed NDJSON, and archive search with the same syntax.

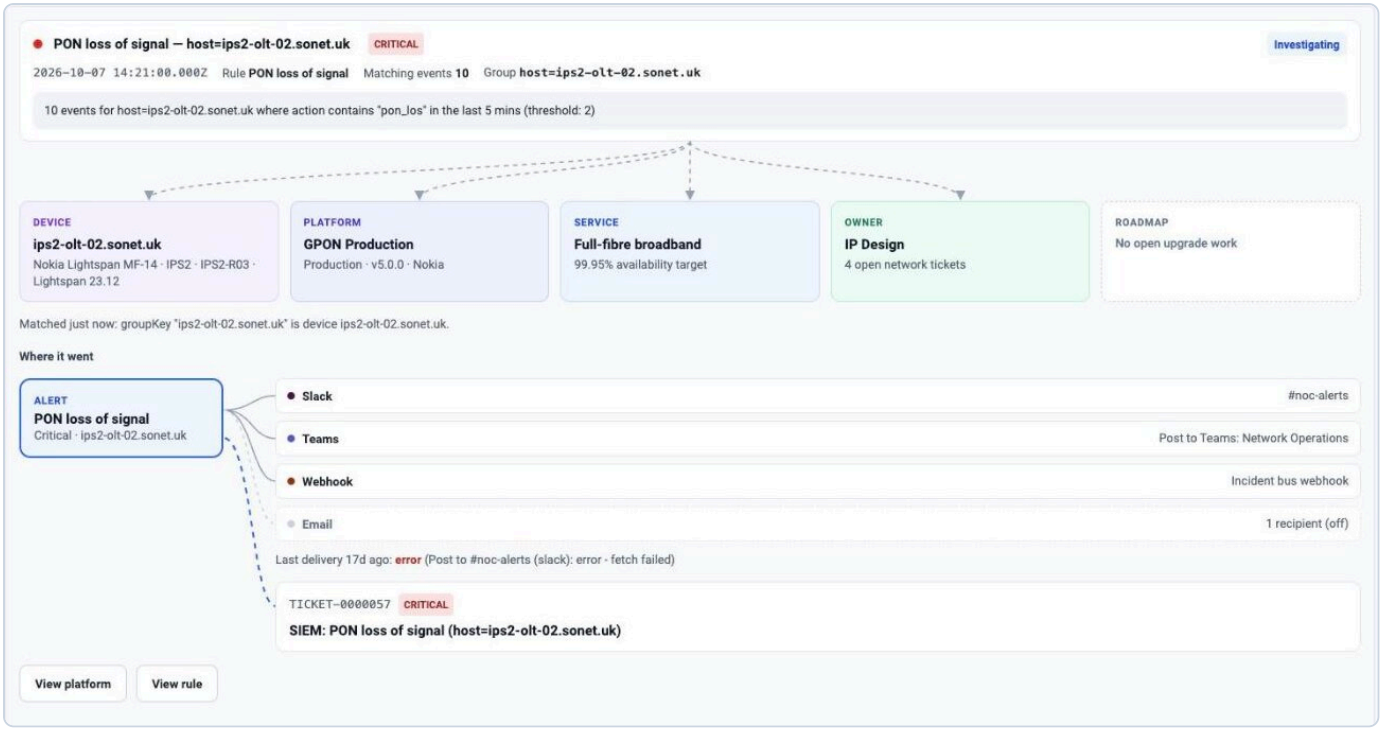

FIGURE 1. A PON LOSS OF SIGNAL ALERT: THE OLT, ITS PLATFORM, THE FULL-FIBRE BROADBAND SERVICE AND ITS OWNER, THE ROUTE THE ALERT TOOK TO SLACK, TEAMS, THE WEBHOOK AND EMAIL, AND THE TICKET RAISED AUTOMATICALLY

Ingest and the event

Sources send newline-delimited JSON to one HTTPS endpoint with their source key in a header: up to 500 events and 1 MB per request, answered with accepted and rejected counts and the reasons, or 401 on a bad key. Keys are generated, rotated and revoked by an administrator, shown once and kept in the tenant vault; the source id is an immutable slug. Each source carries a heartbeat interval so silence can be detected. Devices that only speak syslog post through a lightweight relay or their own HTTPS export.

Each event is normalised to one envelope: timestamp and ingest time, severity from debug to critical, category (auth, network, app, system, audit or other), host, user, action, outcome, a message up to 2,000 characters, up to 20 tags, the raw event up to 100 KB, and a country from the bundled GeoIP data. CEF severities are mapped; vendor syslog is parsed for the four platforms named above.

Asset context. A tenant host index of hostnames, management addresses, OSS node names and site codes matches each event to a device, RAN node, IT asset or site and stamps it with the asset, platform, site and OS version. Network events are recognised by kind (port down and up, LAG member, adjacency, BFD, BGP, optical low) and matched to the interface and link they concern.

Store. Events live in a per-tenant table with a hot retention you set from 1 to 3,650 days (90 by default). On expiry they are archived to the tenant's own bucket as gzipped NDJSON by source and date, kept for 365 days by default (up to 3,650, or forever), and the archive is searchable with the same field and value syntax up to 1,000 results. Search within the hot window is a case-insensitive contains, not a full-text index.

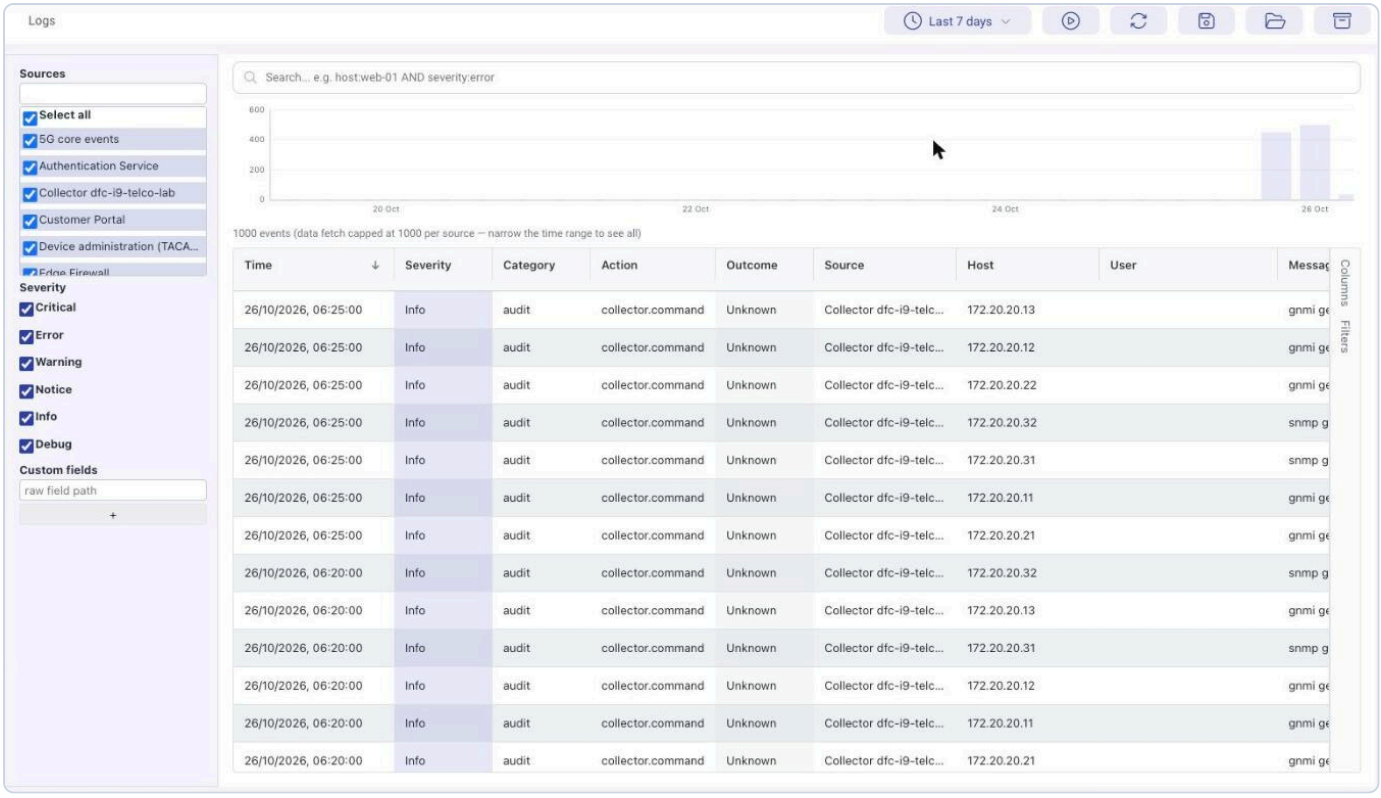

FIGURE 2. THE LOGS SCREEN: SOURCES AND SEVERITIES AS FACETS, A SEARCH BAR WITH FIELD AND VALUE SYNTAX, THE SEVERITY HISTOGRAM OVER SEVEN DAYS WITH BRUSH SELECTION, AND THE COLLECTOR'S OWN COMMAND AUDIT ARRIVING AS A SOURCE

Rules, alerts and routing

Rules run every minute. A **threshold** rule counts events over a window (more than five in five minutes by default) with a field filter and grouping by host, user, action, source, interface or link. A **pattern** rule matches a substring on an envelope field or a raw path over the last two minutes. An **absence** rule fires when a source is silent longer than its heartbeat. A **correlation** rule fires when two other rules both alert within a window (ten minutes by default), optionally only when the two share a site, platform, asset, interface or link. Scope is a platform (which includes sources added later), a set of sources or everything, with a severity filter and an active switch.

Alerts move through open, acknowledged, investigating, resolved and false positive, with assignment, stamps, notes and a resolution (fixed, transient, expected, duplicate, rule adjusted, not reproducible). Each carries a summary, the match count and up to ten sample events. A cooldown (60 minutes by default) stops a rule re-firing; auto-close resolves the alert once the condition has cleared for a grace period (15 minutes by default).

Incident folding. Alerts on the same link or interface fold into the open alert for 24 hours: the count grows, the severity rises and "Also matched" lists the rules. A link alert carries impact text naming the carriers, platforms, services, LSPs, VRFs, redundancy and customers affected.

Routing. A rule names an integration flow that is invoked with the alert payload on a new alert. Flows have native Slack and email steps and post to Teams or any webhook over HTTP. The "Where an alert goes" panel draws the route and reports the last delivery. Folded fires and status changes do not re-notify.

Tickets. Create ticket from an alert or an event sets the priority from severity, links the asset and writes the ticket reference back; a network ticket is raised from the context panel; a rule can raise a ticket automatically (network or IT, chosen by the asset) with critical mapped to P1, error to P2, warning to P3 and the rest to P4.

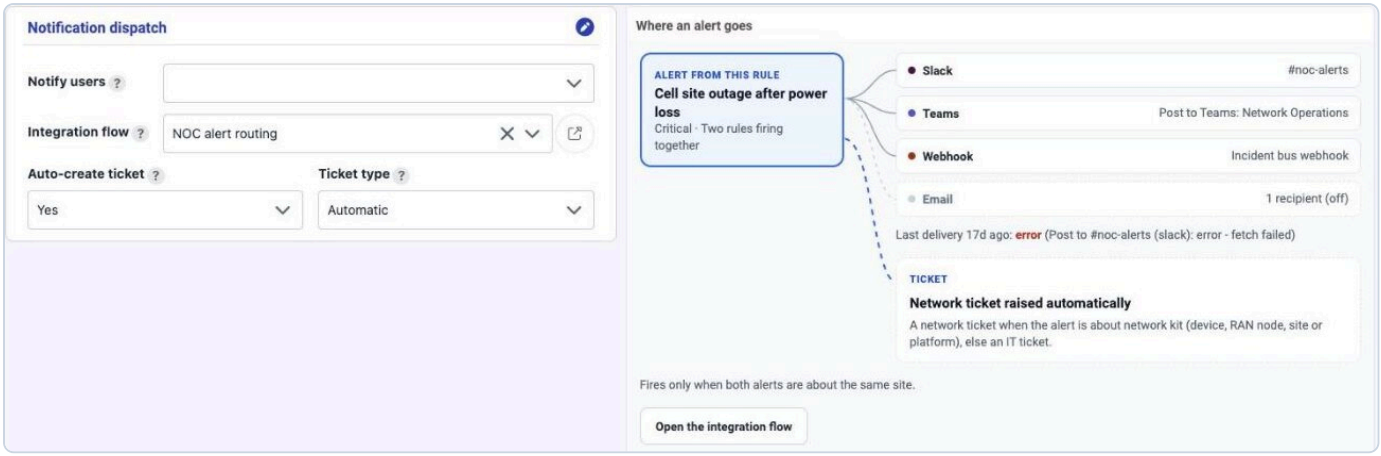

FIGURE 3. A CORRELATION RULE'S DISPATCH: THE INTEGRATION FLOW, AUTOMATIC TICKET TYPE, AND THE DRAWN ROUTE TO SLACK, TEAMS, THE INCIDENT WEBHOOK AND EMAIL, WITH THE LAST DELIVERY RESULT

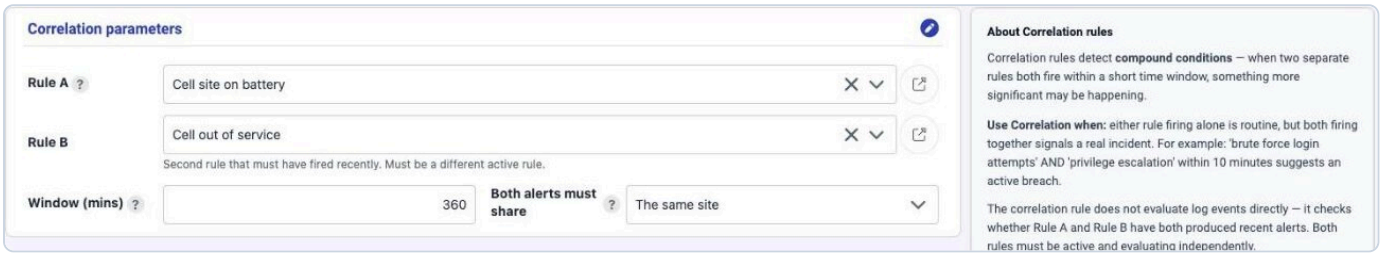

FIGURE 4. CORRELATION PARAMETERS: CELL SITE ON BATTERY AND CELL OUT OF SERVICE WITHIN SIX HOURS AT THE SAME SITE

Health, volume, dashboards and impact

Source health shows every source as healthy, silent, inactive or never used, with last seen, events in the last hour, day and week and a trend. The Connection panel on a source reports receiving, silent, waiting for first event, no ingest key or inactive, the rate per minute, a 24-hour trend and the share of events matched to a device, refreshing every 15 seconds.

Volume metrics over 24 hours, 7 or 30 days: events per day, total against the previous period, active sources, peak bucket, a stacked area by severity and the top eight sources and hosts with country.

Logs. Ranges of 15 minutes, 1 hour, 24 hours and 7 days; facets for sources, severity and custom fields; search with field and value terms joined by AND and OR plus bare words, with autocomplete; a stacked severity histogram with brush selection; live refresh from 5 seconds to 15 minutes; an event record with a context panel (device, platform, services, owner, upgrade work), raw JSON and notes; saved views per user; a daily digest from a saved view through a flow; export to CSV, Excel and NDJSON.

Dashboards are built on the dashboard designer from log source and event datasets, with six templates: AWS Health, Authentication Overview, Network Security, Error and Incident Tracker, Source Health Summary and Executive Summary.

Service impact maps open alerts through the dependency graph to the services and customers that depend on the affected device, link or platform, groups them into incidents by probable root cause, suppresses alerts that fall inside a maintenance window, and draws the affected path on the topology, by customer, service or alert. Outage impact from a link alarm traces the fibre beneath it to the circuits and premises affected.

Audit sources. The DemandFlow collector uploads one audit line per device command it issues, and the Sense service keeps a hash-chained audit trail; both arrive as sources alongside your own.

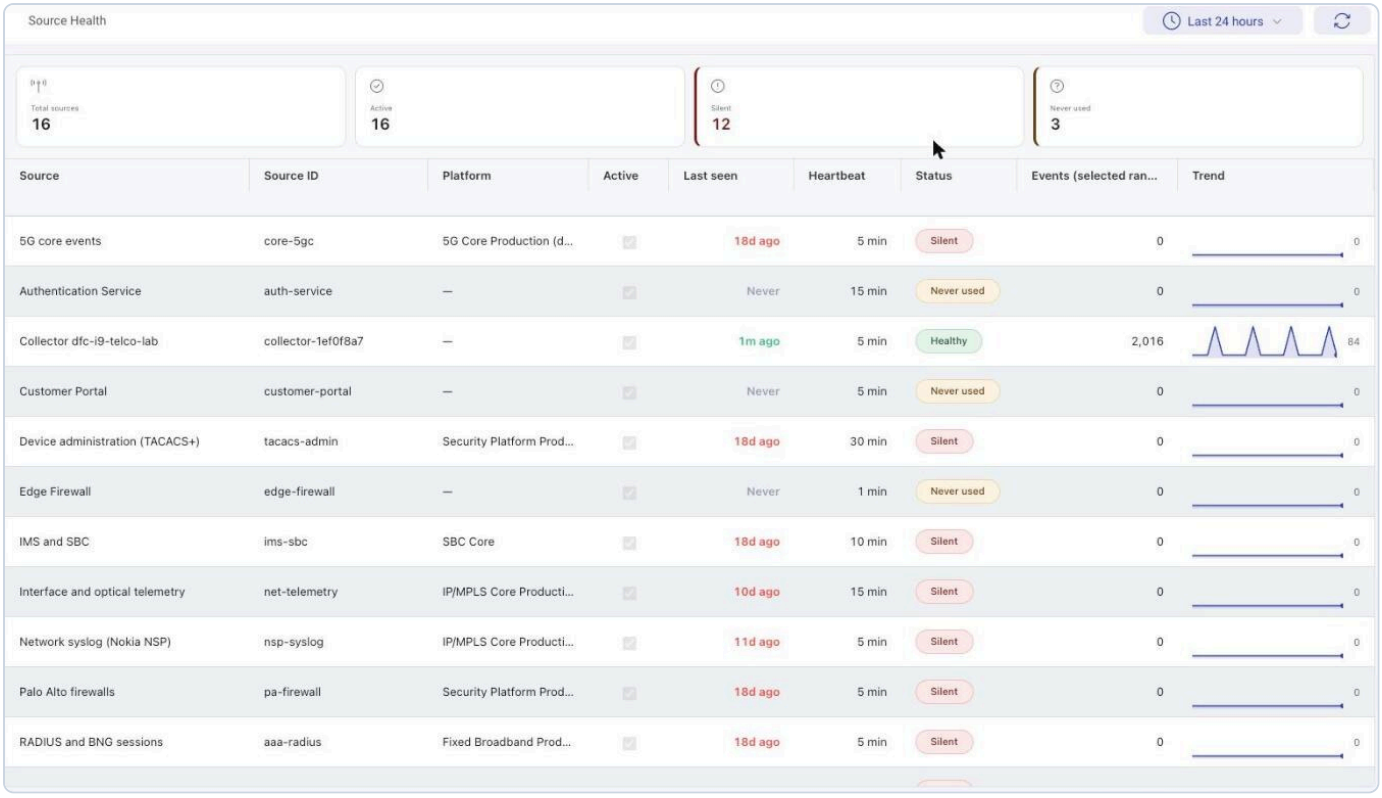

FIGURE 5. SOURCE HEALTH: SIXTEEN SOURCES WITH PLATFORM, HEARTBEAT, LAST SEEN, STATUS AND TREND, WITH SILENT AND NEVER-USED SOURCES COUNTED AT THE TOP

Summary of specifications

Item	Detail
Ingest	One HTTPS endpoint; NDJSON; 500 events and 1 MB per request; per-source keys (shown once, rotated, revoked); heartbeat per source 0 to 1,440 minutes; no syslog listener or agents
Formats	Generic JSON; syslog RFC 5424 and 3164; CEF; vendor syslog for Nokia SR OS, Juniper Junos, Arista EOS, Cisco IOS XR; IP Fabric intent JSON
Envelope	Timestamp, ingested at, severity (debug to critical), category, host, user, action, outcome, message 2,000 chars, 20 tags, raw 100 KB, GeoIP country; asset, platform, site, OS version; interface, link and event kind for network events
Store and archive	Per-tenant table; hot retention 1 to 3,650 days (default 90); archive to the tenant bucket as gzipped NDJSON by source and date, 365 days default (0 forever, max 3,650); archive search up to 1,000 results; 1,000 events per source per load
Rules	Every minute; threshold (count over window, group by), pattern (substring, 2-minute lookback), absence (per source heartbeat), correlation (two rules within a window, default 10 minutes, optional shared site, platform, asset, interface or link); scope by platform, sources or all
Alerts	Open, acknowledged, investigating, resolved, false positive; cooldown default 60 minutes; auto-close grace 15 minutes; folding on link or interface for 24 hours; 10 sample events; link impact text
Routing and tickets	Integration flow per rule; Slack, email, Teams and webhook steps; route drawn with last delivery; manual and automatic tickets, network or IT; P1 to P4 from severity
Screens	Logs (15 min to 7 days, facets, search, histogram, live refresh 5 s to 15 min, context panel, saved views, digest, CSV, Excel, NDJSON); source health; volume metrics (24 h, 7 d, 30 d); dashboards with six templates; service impact

Item	Detail
Impact	Alerts mapped through the dependency graph to services and customers; incidents by probable root cause; maintenance windows suppressed; path on topology; fibre outage impact from link alarms

www.demandflow.com

Book a demo: www.demandflow.com/intelligent-siem/

DemandFlow® is a registered trademark of TOCLOCO LTD. Registered in England No. 09950859. 71-75 Shelton St, London, WC2H 9JQ. © TOCLOCO LTD. All rights reserved.