ONE LOGIC SOURCE

INTELLIGENCE SERVICES

OUTLINE OF SERVICES

SOCIAL MEDIA / OPEN-SOURCE INTELLIGENCE / PROTECTIVE MONITORING

Analyst-driven intelligence to identify emerging risk, contextualize threats, and inform timely action.

PREPARED FOR ORGANIZATIONS, INSTITUTIONS & PROTECTIVE TEAMS

2026 • NATIONAL INTELLIGENCE MONITORING CAPABILITIES

ABOUT ONE LOGIC SOURCE

Intelligence with purpose

A disciplined intelligence capability built around people, context, and decisions.

One Logic Source (OLS) provides social media and open-source intelligence (OSINT) monitoring for organizations, institutions, executives, and individuals exposed to evolving digital and physical risks. Our work begins with a client-specific assessment and translates online activity into relevant, actionable reporting.

OUR MISSION

Identify meaningful indicators early, assess what they represent, and support informed protective and operational decisions.

OUR DIFFERENCE

Persistent technology-enabled collection is paired with active analyst validation, documentation, and appropriate escalation.

OUR PRINCIPLES

- Analysis before amplification: not every mention is a threat.
- Structured reporting: verified facts, assessed implications, and next steps.
- Client-defined priorities: people, places, events, and operating risks.
- Lawful collection, confidentiality, and evidence-handling discipline.

SERVICES AT A GLANCE

A connected intelligence program

Each service can reinforce a wider protective, investigative, or enterprise security strategy.

01 Continuous digital risk monitoring

Persistent collection across configured public social and open sources.

02 Protective & executive intelligence

Threat awareness around people, brands, workplaces, and travel.

03 Schools, campuses & institutions

Digital indicators, incident support, and threat-assessment intelligence.

04 Events, facilities & critical infrastructure

Location-aware visibility into disruption, protests, and security concerns.

05 Targeted OSINT research & assessments

Focused inquiries, source corroboration, and structured findings.

06 Intelligence alerts, reports & briefings

Secure notifications, weekly reporting, and monthly strategic analysis.

07 Monitoring plans & implementation

Flexible coverage tiers with tailored priorities and escalation protocols.

THE CASE FOR MONITORING

Threats often leave digital signals

An evidence-informed approach recognizes both the opportunities and limits of online indicators.

46.5%

PRE-ATTACK COMMUNICATION

A 2021 study of 170 U.S. mass shooters found that 46.5% communicated intent before the attack. Among those who leaked intent, 13% did so online.

Online threat signals may include explicit threats, hostile fixation, doxxing, impersonation, suspicious account activity, event planning, or location-specific chatter. These indicators warrant context, corroboration, and proportional responses—not automatic assumptions of dangerousness.

Signals, not predictions

Research establishes potential warning indicators, not certainty that a particular act will occur.

Volume is not credibility

Threat-related chatter often includes hoaxes, repetition, satire, or unrelated discussion.

A human review layer matters

Trained analysts separate activity requiring escalation from content that belongs in general awareness.

Research context: Peterson et al., JAMA Network Open (2021); RAND, Developing Practical Responses to Social Media Threats Against K–12 Schools (2024). See Research & Sources.

SERVICE 01 — MONITORING

Continuous digital risk monitoring

A persistent listening layer with active review during the contracted monitoring windows.

OLS configures monitoring aligned to a client’s priority intelligence requirements. A persistent OSINT platform collects and flags potentially relevant public activity. During staffed coverage, analysts assess alerts, conduct further research, validate details, and route significant findings for action.

Keyword & narrative monitoring

References to protected people, organizations, grievances, threats, incidents, and emerging narratives.

Geographic & location monitoring

Activity associated with facilities, campuses, venues, communities, public gatherings, and travel locations.

Presence & impersonation monitoring

Suspicious or unauthorized profiles, identity misuse, and reputation-related risk indicators.

Open-source signal discovery

Public social platforms, forums, news, blogs, public records, and other authorized sources.

SERVICE 02 — PROTECTIVE INTELLIGENCE

Executive & protective intelligence

Risk visibility for individuals and organizations operating in the public eye.

Protective intelligence helps security leaders move from reactive information-gathering to anticipatory awareness. Monitoring frameworks may be oriented around a principal, executive team, high-profile individual, brand, or identifiable exposure tied to scheduled activities.

- Direct or indirect threats against a protected person or their associates.
- Doxxing, hostile attention, stalking-related public indicators, and impersonation.
- Location or event-related chatter bearing on public appearances or travel.
- Escalating grievances, targeted harassment, or reputation-linked security concerns.
- Coordination with client-designated executive protection or security personnel.

CLIENT OUTCOME

A defined monitoring picture, fewer unfiltered alerts, better documentation, and timely notice of indicators that may affect a principal’s safety or operational plans.

Scope is tailored to approved targets and sources. OLS intelligence supports—not replaces—on-site protective services, emergency response, or law enforcement assessment.

SERVICE 03 — EDUCATION & INSTITUTIONS

Schools, campuses & institutions

OSINT support for multidisciplinary teams navigating complex safety concerns.

Schools, universities, and private institutions face online rumor cycles, threatening language, harassment, and incidents that can disrupt operations even when activity is not credible. OLS can assist with open-source information collection and contextual analysis for authorized school safety or security teams.

Campus & community monitoring

Public online activity relevant to specific campuses, locations, events, and institutional risks.

Incident-specific digital research

Focused research into publicly available posts, aliases, narratives, and relevant digital context.

School-related threat review

Documentation of concerning content and referral of significant findings to designated officials.

Trend briefs & situational awareness

Recurring observations concerning threat patterns, public events, and developing local concerns.

OLS does not substitute for a school’s threat assessment process, mental-health evaluation, emergency intervention procedures, or multidisciplinary decision-making.

SERVICE 04 — OPERATIONAL RISK

Events, facilities & infrastructure

Location-aware intelligence for changing operating environments.

An online incident may have real operational consequences: a facility closure, reputational disruption, security incident, or fast-moving public gathering. OLS can develop focused monitoring around places, timelines, and organizational exposures.

Events & public gatherings

Monitor public posts related to planned demonstrations, disruptions, threatened actions, and developing conditions.

Facility & site monitoring

Track public mentions of company sites, venues, offices, and other protected locations.

Critical infrastructure & energy

Follow public risk narratives and threats relevant to infrastructure operators and essential services.

Travel & hospitality operations

Monitor events and locations affecting guest safety, operational continuity, or public-facing activity.

SERVICE 05 — TARGETED RESEARCH

Targeted OSINT investigations

Focused research to answer specific operational and investigative questions.

Not every intelligence requirement calls for an ongoing subscription. Scoped OSINT research can help clarify actors, timelines, public digital footprints, online claims, and activity surrounding an incident. OLS brings investigative discipline to identifying relevant information and documenting its source.

- Digital footprint and publicly available social media research.
- Entity, account, and public-profile corroboration when lawful and appropriate.
- Incident, event, or threat-related source collection and timeline development.
- Online narrative, reputation, and public-risk assessments.
- Evidence capture with clear separation of observed facts and analyst judgments.

DELIVERABLES

Engagements may result in targeted intelligence assessments, documented findings, source references, an incident chronology, or a decision-oriented briefing. Specific deliverables, timelines, and fees are defined during scoping.

OUR METHOD

From signal to actionable intelligence

OLS combines technology-enabled awareness with structured human judgment.

01

CONSULT & DEFINE

Identify client risk priorities, authorized targets, relevant locations, and decision-makers.

02

CONFIGURE & COLLECT

Establish platform feeds, keywords, watchlists, geographic criteria, and response contacts.

03

TRIAGE & VALIDATE

Review activity, confirm relevance, assess credibility, and corroborate where possible.

04

DOCUMENT & CLASSIFY

Capture available evidence, record assessments, and assign an alert level.

05

NOTIFY & REPORT

Send significant findings through approved channels; document trend and shift activity.

06

REFINE & REASSESS

Adjust monitoring parameters and escalation thresholds as client risks evolve.

ANALYTIC ENVIRONMENT

Dashboard-enabled analysis

A representative view of how analysts can organize large volumes of online risk activity.



ILLUSTRATIVE ANALYTICS VIEW • PROVIDED SCREENSHOT • NOT CLIENT DATA

Risk pattern visibility

Explore volume trends, source distribution, and the relative prevalence of risk categories.

Prioritization & workflow

Use filtered queues and risk classifications to determine where analyst attention is needed.

Evidence-led reporting

Translate observed patterns and specific findings into contextualized client intelligence.

NOTIFICATIONS & ESCALATION

A clear escalation framework

Four classifications align intelligence delivery with significance and urgency.

EMERGENCY

Imminent danger to life, safety, or critical operations; immediate escalation.

IMMINENT

Clear and developing threat requiring immediate awareness and likely action.

POTENTIAL

Emerging indicators warranting further monitoring and documentation.

GENERAL AWARENESS

Background or contextual information supporting situational awareness.

HOW CLIENTS RECEIVE INTELLIGENCE

Significant alerts are delivered through Signal or another client-authorized secure channel. Notifications are designed to identify the classification, detection time, source, relevant facts, assessment, recommended next action when appropriate, and analyst attribution.

Emergency procedures, recipient lists, escalation methods, and after-hours responsibilities are established at onboarding. OLS is not an emergency dispatch service.

REPORTING & BRIEFINGS

Reporting that supports decisions

Daily signals become structured intelligence for both immediate action and longer-term planning.

SECURE ALERT NOTIFICATIONS

Timely, relevant notifications when monitored activity meets documented escalation criteria; includes contextual assessment rather than unfiltered raw hits.

WEEKLY BRIEFING REPORT

Analyst summary of significant activity, notable developments, watch items, and actions taken during the coverage period.

MONTHLY INTELLIGENCE BRIEFING

Broader analysis of trends, actors, geographies, event-driven risks, and recommendations to refine feeds, priorities, and monitoring scope.

Intelligence products may be tailored for executive leadership, safety and security teams, event operators, institutional administrators, or investigations personnel.

MONITORING PLANS

Flexible coverage plans

Pricing and staffing windows are based on the supplied November 2026 OLS service overview.

TIER 01

DAILY MONITORING

5 days/week • 8 staffed hours/day

$2,000 / month

$24,000 annually

TIER 02

ENHANCED COVERAGE

5 days/week • 16 staffed hours/day

$4,000 / month

$48,000 annually

TIER 03

PREMIUM 24/7

7 days/week • 24 staffed hours/day

$10,000 / month

$120,000 annually

ADDITIONAL COVERAGE

Tier 1: an additional 8-hour monitoring day is listed at $200/month. Tier 2: an additional 16-hour monitoring day is listed at $400/month. Coverage times can be customized by agreement.

Persistent platform collection and active human monitoring are distinct. Human review and response occur during contracted staffed hours unless 24/7 coverage is selected or alternate terms are agreed.

ENGAGEMENT & STANDARDS

Building your monitoring framework

A practical onboarding process aligns collection, review, and escalation with operational needs.

01 INITIAL CONSULTATION

Discuss current concerns, protected interests, operating context, and the client’s primary intelligence requirements.

02 MONITORING DESIGN

Define monitored entities, locations, keywords, exclusions, priority risk indicators, and reporting recipients.

03 ESCALATION PROTOCOL

Agree on notification channels, alert categories, action owners, and responsibilities outside staffed coverage.

04 REPORTING CADENCE

Set briefing audiences, preferred output format, monitoring review frequency, and quality-control expectations.

LEGAL & ETHICAL DISCIPLINE

Collection is limited to authorized and lawful sources. Analysts distinguish fact from inference, preserve relevant material where appropriate, protect confidential client information, and avoid unsupported conclusions. No monitoring service can guarantee detection or prevention of every threat.

RESEARCH, SOURCES & CONTACT

Research-informed. Client-specific.

Public research informs our approach; each client engagement is separately designed and scoped.

- Peterson, J. et al. (2021). Communication of Intent to Do Harm Preceding Mass Public Shootings in the United States, 1966–2019. JAMA Network Open.
- RAND Corporation (2024). Developing Practical Responses to Social Media Threats Against K–12 Schools.
- U.S. Secret Service, National Threat Assessment Center (2023). Mass Attacks in Public Spaces: 2016–2020.
- Arcila-Calderón, C. et al. (2024). Online violent speech and offline violent crime. Humanities & Social Sciences Communications.
- Müller, K. & Schwarz, C. (2021). Social media and violent crime. Journal of the European Economic Association.
- OLS service overview (November 19, 2026) and OLS Social Media & OSINT Monitoring White Paper (provided materials).

START WITH A CONSULTATION

Describe the people, places, assets, and risks you need to monitor. OLS can recommend a tailored program, reporting approach, and coverage schedule.

onelogicsource.com/intelligence-services