

# OSAVUL SERVICE DEFINITION DOCUMENT

**Service type: Software as a Service (SaaS)**
**Framework: G-Cloud (Lot 2b)**

# Content

1. Introduction.....3
2. Services Overview.....4
3. Service Features and Capabilities.....5
4. Operational Value and Outcomes.....6
5. How We Deliver Our Services.....7
6. Customer Support and Technical Assistance Framework.....12
7. Case study.....12

**INTRODUCTION**

## Company overview

Osavul was created with a singular ambition: to bring clarity, speed, and confidence to decision-making in the most complex information environments faced by governments and security institutions.

In a world influenced by hybrid conflicts, influence operations, and rapidly evolving cyber threats, timely, trustworthy intelligence is a strategic necessity. Narrative intelligence, OSINT, and situational awareness form the foundation of any effective national or institutional security posture. Without them, early warning, threat detection, and response remain fragmented and reactive. Intelligence should empower institutions, not overwhelm them. It should transform complexity into operational advantage, enabling governments and security organisations to act decisively rather than defensively.

Osavul is a cloud-based intelligence and analytics platform designed to meet these needs. Delivered as a secure, browser-based SaaS solution requiring no local installation, Osavul supports public sector organisations and enterprises in detecting, analysing, and responding to information, hybrid, and cyber threats in real time.

The Osavul platform combines automated global data collection, AI-powered analytics, and intuitive visualisation to surface emerging risks, public opinion trends, and malicious activity across multiple domains, languages, and platforms. It strengthens awareness of the information environment, supports strategic communications, policy coordination, hybrid and cyber security activities through early identification of information, cyber and physical risks, and delivers actionable cyber and hybrid threat intelligence by analysing hostile actors' intent, capabilities, and behavioural patterns — within a single, interoperable system.

While many providers bolt analytics onto existing services, Osavul was built natively around intelligence as a core government capability — purpose-designed to link analytical outputs directly to security, policy, and operational outcomes across departments.

Osavul exists to ensure government institutions are not only informed — but prepared.

## Services Overview

Osavul delivers a comprehensive set of intelligence capabilities designed to support UK public sector organisations in countering information, hybrid, and cyber threats through a single, secure platform.

At its core, Osavul enables **narrative intelligence and tracking**, allowing users to **identify, monitor, and analyse the evolution of harmful narratives, hybrid threats, influence campaigns, and strategic messaging in real time**. This is underpinned by automated global OSINT data collection across social media, news outlets, forums, and online communities worldwide, ensuring continuous visibility across the digital information environment.

The platform provides **multi-domain strategic situational awareness** by integrating information, cyber, and hybrid threat data into a unified operational picture. Through advanced detection and analysis mechanisms, Osavul supports **the identification of hostile activity, including coordinated information operations, cyber-enabled influence, and hybrid threat patterns**. This also includes the detection of bot networks, inauthentic behaviour, and high-risk sources, helping users distinguish genuine public discourse from manipulated or hostile activity.

Using Osavul's SaaS platform, analysts can **conduct investigations and research** to develop **situational awareness and deliver strategic intelligence** to relevant stakeholders. Osavul's situational awareness and strategic intelligence capabilities can be applied to the analysis of the global information environment across multiple languages.

To support operational decision-making and cross-government coordination, Osavul offers rich data visualisation tools, including dashboards, charts, timelines, and network views, enabling analysts and policy teams to rapidly interpret complex datasets and communicate findings effectively.

The platform also includes robust reporting and export tools, allowing users to generate OSINT-based analytical outputs suitable for briefings, policy development, and operational reporting.

Osavul delivers its services through a secure public cloud **Software-as-a-Service (SaaS) model**, complemented by ongoing analytical and technical consultation to ensure that the platform is configured and used in line with customer operational requirements. This includes expert support on the correct use and integration of APIs, configuration of data ingestion parameters, optimisation of visualisation and dashboards, and the design of reporting workflows aligned with policy, operational, and communications needs.

Through this combined delivery model, Osavul ensures that customers not only access advanced analytical capabilities but are also supported in translating platform outputs into actionable intelligence and decision-ready products.

## Service Features and Capabilities

Public sector organisations require intelligence systems that move faster than adversaries and operate across multiple domains. Osavul was built to meet this challenge. Osavul is a cloud-based AI-powered intelligence and analytics platform that delivers a comprehensive set of interoperable capabilities for monitoring, analysing, and responding to threats across the information environment.

Osavul provides the following core features:

| |
|---|
| **Narrative intelligence and tracking, enabling continuous monitoring of influence campaigns and strategic messaging** |
| **Automated global OSINT data collection across social media, news outlets, and online communities worldwide** |
| **Multi-domain strategic situational awareness spanning information, hybrid, and cyber threat environments** |
| **Detection and analysis of information, hybrid, and cyber threats in near real time** |
| **Predictive threat intelligence to anticipate emerging information, hybrid, and cyber risks** |
| **AI-powered big data analytics for large-scale content processing and pattern detection** |
| **Detection of bot activity, coordinated inauthentic behaviour, and high-risk or state-affiliated sources** |
| **Monitoring of social media, news, and online communities worldwide across multiple languages and platforms** |

| |
|---|
| **Advanced data visualisation through dashboards, charts, timelines, and network views** |
| **Integrated reporting and export tools for OSINT and analytical outputs** |
| **Secure, browser-based SaaS platform access with no local installation required** |

## Operational Value and Outcomes

Osavul is designed not only to collect and analyse data, but to convert complex information environments into operational advantage for government and security institutions.

Using Osavul, organisations can:

- Quickly detect and investigate information, hybrid, and cyber threats before escalation
- Identify and analyse foreign malicious interference and hostile influence operations
- Track public opinion and narratives across languages, regions, and digital platforms
- Monitor global OSINT data in near real time to maintain continuous situational awareness
- Detect coordinated inauthentic behaviour and automated bot networks
- Predict and proactively prevent emerging threats through AI-powered intelligence
- Deliver strategic intelligence to support policy, communications, and operational decision-making
- Visualise complex data through dashboards, charts, and analytical reports

By integrating advanced analytics, AI, and scalable OSINT collection into a single secure platform, Osavul enables public sector organisations to move from reactive monitoring to proactive threat management — strengthening national resilience, protecting democratic institutions, and supporting evidence-based decision-making.

## How We Deliver Our Services

Osavul delivers its service through a secure public cloud SaaS platform, providing customers with immediate access to advanced intelligence and analytical capabilities. Alongside platform access, Osavul supports customers through structured onboarding, training, and continuous technical and analytical assistance to ensure effective operational use of the service.

In addition to providing access to the platform, Osavul actively supports customers in configuring data collection, designing analytical workflows, and applying the platform to real-world operational needs. This includes advisory support on API usage and system integration, optimisation of dashboards and visualisations, and the development of reporting formats aligned with policy, operational, and communications objectives.

At the core of this delivery model is a structured, data-driven operational workflow.
Osavul platform usage is structured around **5 core operational steps**, described below.

### Step 1: Data Onboarding, Platform Configuration, and Client Engagement

Based on the customer's requests and objectives, Osavul configures its proprietary ingestion framework, Data Pipelines, to collect publicly available information at scale and in near real time. Data ingestion is aligned to defined analytical parameters, including topic areas, geographic focus, language coverage, actor groups, and platform relevance.

New sources are continuously identified, validated, and integrated into the platform, ensuring that collection coverage evolves in line with emerging threats, shifting policy priorities, and changes in the information environment. This enables Osavul to operate as a continuously adaptive collection ecosystem rather than a fixed, one-size-fits-all source inventory.

Through this approach, Osavul ensures that data availability, platform capabilities, and analytical focus remain tightly aligned with customer requirements throughout the lifecycle of service delivery.

### Step 2: Data Enrichment, Attribution, and Advanced Analytical Querying

Once collected, data within Osavul is systematically enriched and structured to enhance analytical value and operational relevance for public sector users.

This includes comprehensive **source classification and risk profiling**, enabling the identification of bots, coordinated inauthentic behaviour, high-risk actors, and state-affiliated or proxy accounts. Osavul performs **actor attribution** by mapping locations, affiliations, and behavioural patterns, alongside **relationship and network analysis** to identify connections between actors, channels, and information flows.

Additional **metadata enhancement** is applied, including language, geolocation, platform, and content typologies, enabling prioritisation and targeted filtering aligned with operational needs.

Osavul supports precision data retrieval through advanced keyword querying and a robust set of Boolean logical operators. To support user proficiency, the platform includes an integrated written search guide directly within the interface. In addition, Osavul provides an **AI-powered Query Assistant**, allowing users to describe their research intent in natural language. The system automatically converts this input into structured queries, identifying relevant synonyms and contextual relationships without requiring manual Boolean construction.

Users can perform targeted searches across both content and metadata, supported by:

- **Multilingual search**, enabling simultaneous analysis across multiple languages
- **Advanced filtering**, including security-specific filters to isolate inauthentic behaviour, high-risk accounts, and state-affiliated actors
- **Actor Group (Actor Collection) segmentation**, allowing users to create custom actor sets for inclusion or exclusion in analysis
- **AI-powered fuzzy search**, which infers semantic meaning, slang, indirect references, and contextual variations to return a more exhaustive and relevant result set

This enrichment and querying layer enables analysts to move beyond surface-level content monitoring, supporting a deeper understanding of who is driving activity, how it is coordinated, and why it is operationally relevant for public sector decision-making.

## Step 3: Case Creation, Threat Investigation, and Narrative Analysis

Osavul enables users to organise relevant data into structured cases, supporting in-depth investigation, collaboration across teams, and alignment with government investigative, policy, and communications workflows.

Within each case, users can **track how specific messages, narratives, or campaigns evolve over time,** identify key amplifiers and originators, and detect coordinated behaviour and campaign orchestration. The platform supports actor-based analysis to assess influence, reach, and intent, as well as correlation of information activity with **real-world events, operational developments, or policy timelines**.

Osavul provides continuous monitoring of key operational metrics within each case, including:

- The volume of messages associated with the case
- The number and characteristics of actors involved
- The evolution of content and dominant sentiments over time

Where analytical scope becomes too broad, Osavul applies **AI-powered functions to extract and decompose sub-narratives from the dataset.** This enables users to group content "by stories", breaking complex narratives into smaller, analytically coherent components for targeted examination and comparison.

This case-based and narrative-centric approach ensures that analysts move beyond static monitoring to conduct structured, evidence-driven investigations that directly support public sector decision-making and operational response.

## Step 4: Narrative Decomposition, Topic Modelling, and Sentiment Analysis

Osavul applies advanced AI to decompose complex information environments into analytically coherent narratives, topics, and sentiment patterns, enabling both tactical counter-disinformation activity and strategic situational awareness for public sector organisations.

The platform automatically disaggregates large volumes of content into distinct narratives and sub-narratives, allowing users to separate individual news events from broader strategic narratives, identify recurring themes, framing techniques, and influence patterns, and assess narrative velocity, reach, and audience penetration. Osavul supports the analysis of how narratives mutate, converge, or diverge across platforms, languages, and regions.

Osavul provides **AI-powered Topic Modelling and Narrative Tracking**, enabling the analysis of large datasets across multiple platforms and content formats, including articles, videos, and comments.

Datasets can be defined by combinations of keywords and filters representing specific segments of the information environment, thematic areas, or geographical focus.

Topic detection supports multiple analytical modes, including:

- Event-based clustering, whereby the system automatically identifies key events triggering publications and groups content around central developments
- Opinion and narrative detection, grouping content by dominant viewpoints or messages expressed within it, including conversational content such as comments and messages

For each identified topic or narrative, **Osavul calculates engagement and impact metrics**, including total volume of posts, views, and reactions. The platform enables actor-based analysis, allowing users to identify which actors — including state-affiliated, high-risk, or inauthentic accounts — are driving coverage of specific topics.

Geographical analysis provides insight into how topics are covered across countries and regions, while temporal analysis tracks how discussions evolve over time. All topics and narratives are fully grounded in underlying content. Users can access the source material directly, analyse it independently, export it, and provide feedback on content relevance, which is used to improve model accuracy over time.

Osavul features **Aspect-Based Sentiment Analysis**, significantly enhancing the precision of sentiment measurement. Unlike basic sentiment analysis, which assesses overall tone, this capability evaluates sentiment toward specific entities, organisations, or concepts based on contextual meaning. This enables precise sentiment estimation towards user-defined entities such as the UK, Russia, Ukraine, or China, even in cases of semantic ambiguity.

The platform includes specialised capabilities for analysing sentiment in short-form and conversational content, including comments and threads. To achieve this, Osavul extracts and incorporates additional contextual information, such as surrounding discussions or referenced articles, into the analysis.

Sentiment results are visualised through dashboards and trend views, enabling users to understand sentiment dynamics over time or in response to specific topics and events.

## Step 5: Visualisation, Reporting, Sharing, and API Integration

Osavul provides a comprehensive suite of visualisation, reporting, and data-sharing capabilities designed to support operational analysis, policy development, and cross-government collaboration.

The platform delivers three core analytical dashboards — **Case View, Case Comparison, and Topic Dashboard** — each tailored to support distinct analytical and operational use cases. These dashboards incorporate a wide range of visualisation tools, including charts, graphs, and time-series displays, enabling users to assess trends, distributions, and relationships within the data effectively.

All visual elements within Osavul are fully data-transparent. Users can access the underlying source content directly through integrated pop-up views and may save selected datasets as separate cases for deeper investigation. This ensures traceability, auditability, and analytical integrity, consistent with public sector evidence standards.

Dashboards are fully configurable, allowing users to select analytical widgets, adjust parameters, and annotate elements with rich-text notes to provide operational and policy context. Reports can be exported in PDF format or shared securely via platform-generated links, enabling controlled dissemination across teams and partner organisations.

Osavul supports comprehensive data export in multiple operational formats, including PDF, CSV, DOCX, JSON, and XML, ensuring compatibility with a wide range of analytical, reporting, and archival workflows. In addition to direct file export, data can be shared securely within the customer environment via platform-generated access links or delivered in JSON format through a REST API, enabling integration with external systems, mission-specific analytical tools, and downstream data platforms.

Through this combination of visualisation, reporting, and system integration capabilities, Osavul ensures that analytical outputs are not only generated efficiently but can be operationalised across public sector workflows and digital ecosystems.

## Customer Support and Technical Assistance Framework

Osavul offers a comprehensive customer support framework to ensure smooth platform usage from day one.

Our support structure includes:

- Onboarding & Training: A dedicated team provides tailored training to ensure your team is fully equipped to leverage the platform.
- Ongoing Support based on the applied SLA

Our team of experts, including senior analysts with deep experience in media intelligence, provides ongoing technical assistance throughout the project. Whether troubleshooting issues or refining analytical queries, Osavul's support team is available to ensure the platform is optimally utilized.

As part of our commitment to data privacy and security, Osavul adheres strictly to privacy laws and other relevant regulations. Our platform and processes are fully compliant with EU data protection laws, ensuring the highest standards of privacy for all stakeholders.

## Case study

Below you may see a short case study providing an example of deployment of Osavul's SaaS platform.

**Customer Type**

Public sector institution operating in a high-risk information and hybrid threat environment.

**Service Model**

Software as a Service (SaaS), Public Cloud.

**Customer Challenge**

The customer faced sustained hybrid threats, including hostile information activity and foreign state-linked influence operations. These threats created operational risk, reputational exposure, and significant analyst workload.

The organisation required a capability to:

- Identify hostile infrastructure as early as possible

- Maintain continuous situational awareness across the information environment
- Monitor known hostile actors and networks over time
- Analyse foreign state-affiliated actors, their narratives, and operational agendas
- Support analysts with scalable, evidence-based intelligence outputs aligned with public sector standards

Existing tooling was fragmented, reactive, and insufficient for persistent monitoring and early warning.

**Osavul's Solution**

Osavul delivered a secure, browser-based SaaS intelligence platform configured to the customer's operational priorities.

1. Continuous Data Pipelines for Situational Awareness
Osavul implemented adaptive OSINT data pipelines collecting publicly available information in near real time across social media, news, and online communities. Collection was tailored by topic, geography, language, and actor group to ensure relevance and proportionality.

2. Early Threat Identification and Alerting
AI-powered analytics and risk profiling enabled early identification of hostile signals, including coordinated inauthentic behaviour, emerging narratives, and activity linked to known high-risk or state-affiliated actors.

3. Persistent Monitoring of Hostile Infrastructure
Osavul enabled continuous monitoring of previously identified hostile sources and networks. Analysts tracked behavioural changes, narrative evolution, and coordination patterns to understand adversary intent and tactics over time.

4. Analysis of Foreign State-Affiliated Actors
The platform supported attribution, network analysis, and narrative tracking of foreign state-affiliated actors operating in the relevant information environment, enabling monitoring of their activity, messaging strategies, and agendas.

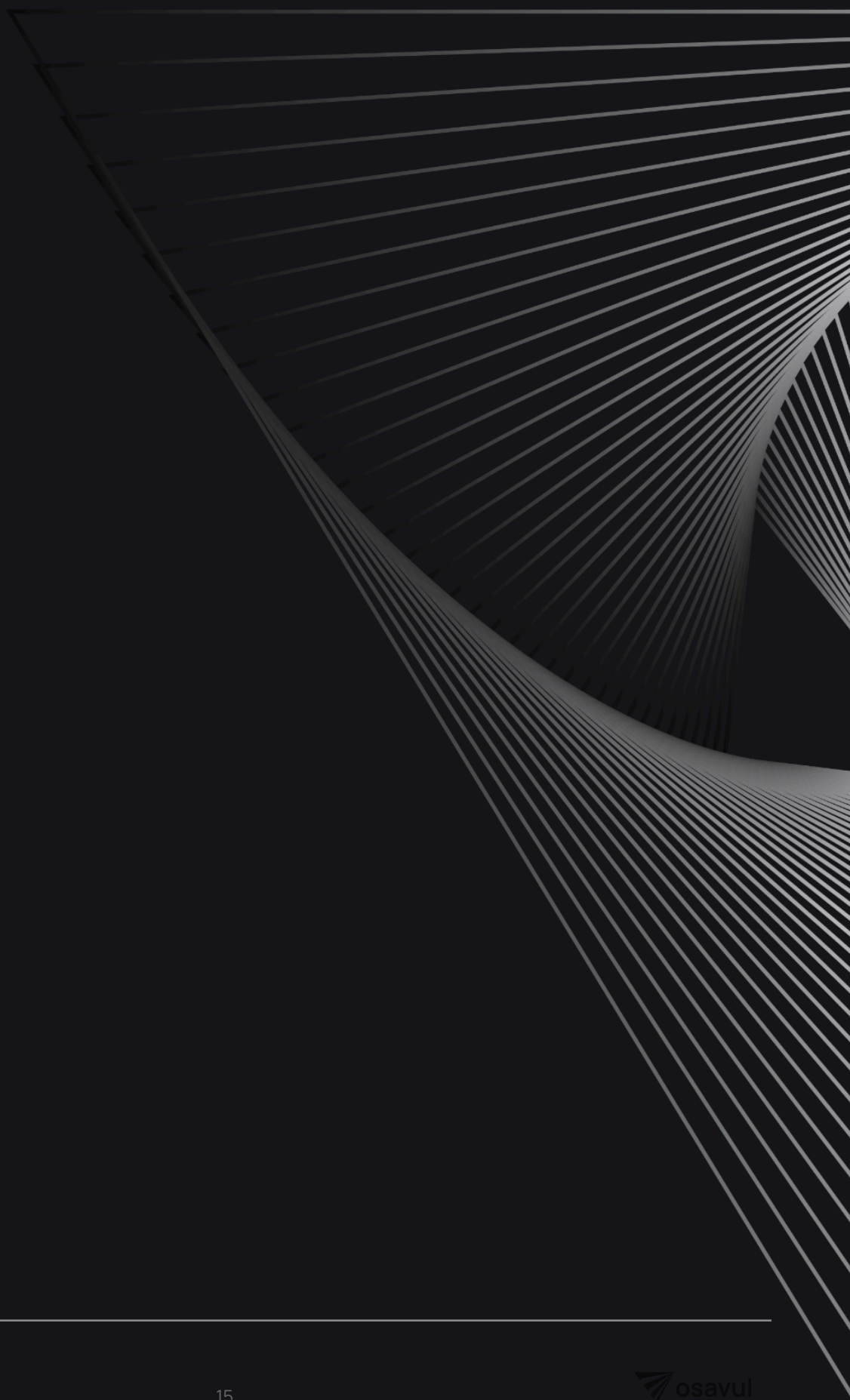
5. Decision-Ready Outputs
Osavul provided dashboards, case-based investigations, and exportable reports aligned with public sector evidence, auditability, and reporting requirements.

**Outcomes and Benefits**

As a result of deploying Osavul, the customer achieved:

- 50–70% reduction in time to identify emerging threats, enabling earlier intervention
- Continuous situational awareness across priority platforms, languages, and regions
- Improved analyst efficiency, reducing manual data collection and triage by approximately 40–60%
- Persistent visibility of hostile infrastructure, supporting long-term threat understanding rather than reactive response
- Clear, evidence-based intelligence products to support operational, policy, and strategic decision-making

Overall, the customer transitioned from reactive monitoring to proactive hybrid threat management, strengthening institutional resilience and decision confidence.



Contact us
info@osavul.cloud