softserve

ARCHITECTURE VISION

Disinformation Security & Validation Engine (Public Sector)

Version 0.1

For

<CLIENT>

[mm/dd/yyyy]

Contents

Revision History

Date	Version	Description	Author
10/15/2025	0.1	Filled in the Architectural Drivers section of the document.	Bohdan Boretskyi
10/15/2025	<x.x>	Approved	<name>

1 Introduction

1.1 Purpose

This Architecture Vision elicits the significant architecture drivers such as business, functional, nonfunctional requirements and constraints, defines architecture, and develops a roadmap for Single Entry implementation. The document is intended as a primary technical guidance into solution implementation for the development team.

The solution architecture is designed following the guiding principles outlined in Appendix A – Architecture Design Methodology.

1.2 Scope

The document describes the proposed Single Entry architecture towards development of the solution that will satisfy business, functional, non-functional requirements and constraints provided by the Client. This Architecture Vision covers the following information:

- Significant architectural drivers for the Solution
- Proposed software architecture of the solution based on these drivers
- Technology stack and environment definitions
- Operations specific perspectives
- Development road map and high level estimates for effort, team size and skill sets.

1.3 Definitions

The Definitions section lists the acronyms and terms used in this document which might possess lesser familiarity or double meaning to the reader.

(Fill the table if you have definitions)

#	Term	Definition
1.	NLP	Natural Language Processing - a branch of artificial intelligence that enables computers to understand, interpret, and analyze human language text to extract meaning and classify content
2.	OSINT	Open-Source Intelligence - publicly available information collected from open sources such as news outlets, public forums, and social media platforms used for intelligence gathering

#	Term	Definition
3.	SSO	Single Sign-On - an authentication mechanism that allows users to access multiple applications or systems with one set of login credentials
4.	LDAP	Lightweight Directory Access Protocol - an industry-standard protocol for accessing and maintaining distributed directory information services, commonly used for centralized authentication
5.	TLS	Transport Layer Security - a cryptographic protocol that provides secure communication over a computer network by encrypting data in transit between client and server
6.	API	Application Programming Interface - a set of protocols and tools that allows different software applications to communicate and exchange data with each other
7.	F1 Score	A statistical measure of a model's accuracy that combines precision and recall into a single metric, ranging from 0 to 1, where 1 represents perfect precision and recall
8.		

1.4 References

The References section provides a complete list of all the documents referenced elsewhere in this document.

(Fill the table if you have references)

#	Version	Date	Document Name	Published by
1.	<x.x>	<mm/dd/yyyy>	<Document Name>	<Publishing Organization>
2.				
3.				
4.				
5.				

1.5 Documentation Roadmap

This section guides into the Architecture Vision document structure to help find the information of interest.

- Executive Summary speaks about the proposed architecture on the highest level and covers:
    - Key Decisions about the architectural and operational choices made for the solution
    - Key Risks and Open Issues detected with the analysis of the available context, requirements, and proposed decisions
- Architectural Drivers elicits the known essential requirements and constraints for the solution to design which play key role in forming archectural decisions and overall architecture.
    - Business Case describes the solution from the business standpoint including major features
    - Service Level Agreement defines the important technical constraints and guarantees under which the solution will be serviced to its clients
    - Use Case Model lists the key Use Cases for the designed solution
    - Domain Model shows the key business entities with attributes and relationships between them.
    - Design Constraints include business, resource, technical and other constraints accounted for in the architecture of the solution.
    - Quality Attribute Scenarios are a set of the testable scenarios clarifying non-functional requirements for the system quality attributes such as performance, maintainability, and others.
- Solution Architecture defines the proposed architecture as a set of architectural views in the format defined in Appendix C – How View is Documented.
    - Big Picture shows the solution architectural context, high level decomposition into components, and followed reference architecture.
    - Development Technology Stack selects the tools, frameworks, libraries, external services and other technologies the solution implementation will rely on.
- Implementation Roadmap proposes the plan for solution implementation including:
    - Implementation Deliverables expected to be implemented and delivered at the implementation phase.
    - Implementation Milestones tied to the project timeline

- Estimate of complexity/size, effort, schedules for the implementation
- Team skillset and structure based on the technology, competence, and schedule requirements

2 Executive Summary

The section Executive Summary highlights key architectural decisions made for the solution described in Business Case. These decisions are defined and discussed in depth in Solution Architecture while Implementation Roadmap lays out the proposed milestones, estimates, and team to implement the provided architecture vision.

This section also summarizes the key business and technical risks related to the solution implementation. These risks are uncovered in depth in the rest of the document.

2.1 Key Decisions

The section outlines key design decisions about the solution including the architecture big picture and most essential technologies and external services to rely on.

(provide a short description of the main decisions you've made solutioning the architecture)

The solution will be implemented as a cloud based Java web service and deployed to the Cloud Platform Provider XYZ using it's A, B, C services. The structured data will be stored in the scalable cloud RDBMS storage provided by the Cloud Platform Provider with multy-AZ replication to ensure data availability and backup as required by the solution's SLA. The solution will be integrated as a REST-ful client with the third-party service ABC to store and retrieve the unstructured blob data.

2.2 Key Risks and Open Issues

The section lists the key risks related to the solution design and implementation. It also lists key open issues where architectural decisions have not been made yet or are likely to change.

(add identified risks and a mitigation strategy for them in the table below)

Risk Description	Mitigation Strategy
Solution relies on the third-party services to implement its functionality under SLA. As a result the solution service performance and availability can be at risk	▪ Enter into the business agreement with the third-party service provider. ▪ Select the backup provider ▪ Implement the fail-over strategy
<risk description>	<mitigation strategy description>

3 Architectural Drivers

The section captures significant requirements driving the solution architecture and road map. The requirements which are not influencing the solution architecture in major ways and low level requirement details and scenarios are typically excluded from this section and can be found in the requirement specification or the product backlogs.

3.1 Business Case

The section lays out the business case for the solution Disinformation Security & Validation Engine (Public Sector).

(insert your business view diagram here)

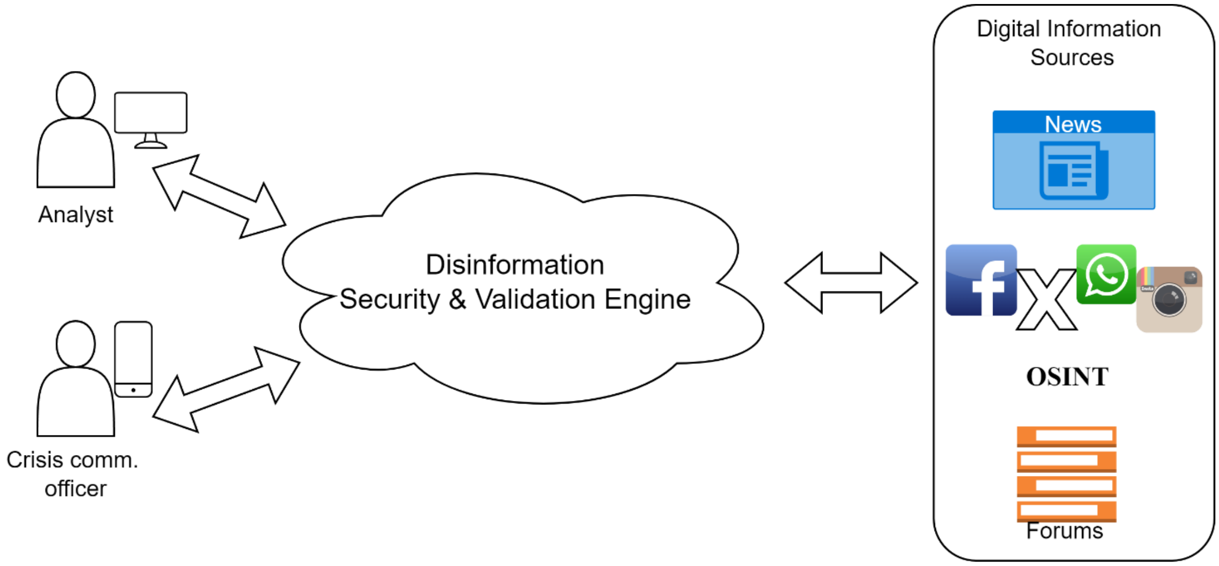

Analyst
Crisis comm. officer
Disinformation Security & Validation Engine
Digital Information Sources
News
OSINT
Forums

Figure 1. Business level view of Disinformation Security & Validation Engine (Public Sector)

(Provide a short description of the business view diagram)

The business view illustrates the Disinformation Security & Validation Engine as a cloud-based centralized platform serving government stakeholders in combating disinformation campaigns.

Government analysts use the system through web browser-based access to investigate disinformation sources, track narrative evolution, and validate information across digital channels. Crisis communication officers utilize mobile access for rapid field response to emerging threats.

The system continuously monitors diverse digital information sources—including social media platforms, news outlets, public forums, and open-source intelligence (OSINT)—

automatically identifying, scoring, and validating potential disinformation narratives using advanced natural language processing and behavioral analytics.

This transforms the agency's operational model from manual, reactive monitoring to automated, proactive threat detection, reducing the average time required to identify high-risk narratives from 72 hours to under 4 hours, and decreasing exposure to validated high-risk disinformation sources by 50% within the first year of operation.

3.1.1 Business Goals

The section enumerates essential business goals for the solution

(Add identified business goals in the table below)

#	Description
BG-1	Protect governmental stability and public trust from targeted disinformation campaigns
BG-2	Enable proactive situational awareness and information ecosystem management during elections and other high-engagement events
BG-3	Reduce risk of civil unrest, electoral interference, and emergency resource misallocation by providing early detection and validated insights on disinformation narratives
BG-4	Build long-term institutional resilience and response capability against coordinated digital influence operations

3.1.2 Major Features

The section enumerates solution major features.

(add identified major features in the table below, at least 5)

#	Description
F-1	Real-time monitoring and ingestion of digital content from social media, news outlets, public forums, and open-source intelligence (OSINT) feeds
F-2	Advanced NLP-based analysis and scoring engine evaluating narrative veracity, sentiment, source credibility, and predicted reach
F-3	Automated identification and tracking of disinformation narratives, including origin, evolution, and propagation vectors

#	Description
F-4	Web-based analytical dashboard providing government analysts with detailed investigation, visualization, and reporting tools
F-5	Mobile access module for crisis communication officers with push notifications and field response capabilities
F-6	Secure authentication and role-based access control integrated with enterprise identity management (SSO via LDAP)

3.2 Use Case Model

3.2.1 Use Case View - User Interactions

3.2.1.1 View Context

This view illustrates the primary interactions between system users (Government Analysts and Crisis Communication Officers) and the Disinformation Security & Validation Engine, covering functional scenarios derived from features F-1 through F-6 defined in section 3.1.2.

3.2.1.2 Representation

(Add your Use Case diagrams here. They should cover all major cases of the system usage (at least 5 use cases). You could have a few separate diagrams to cover all the use cases)

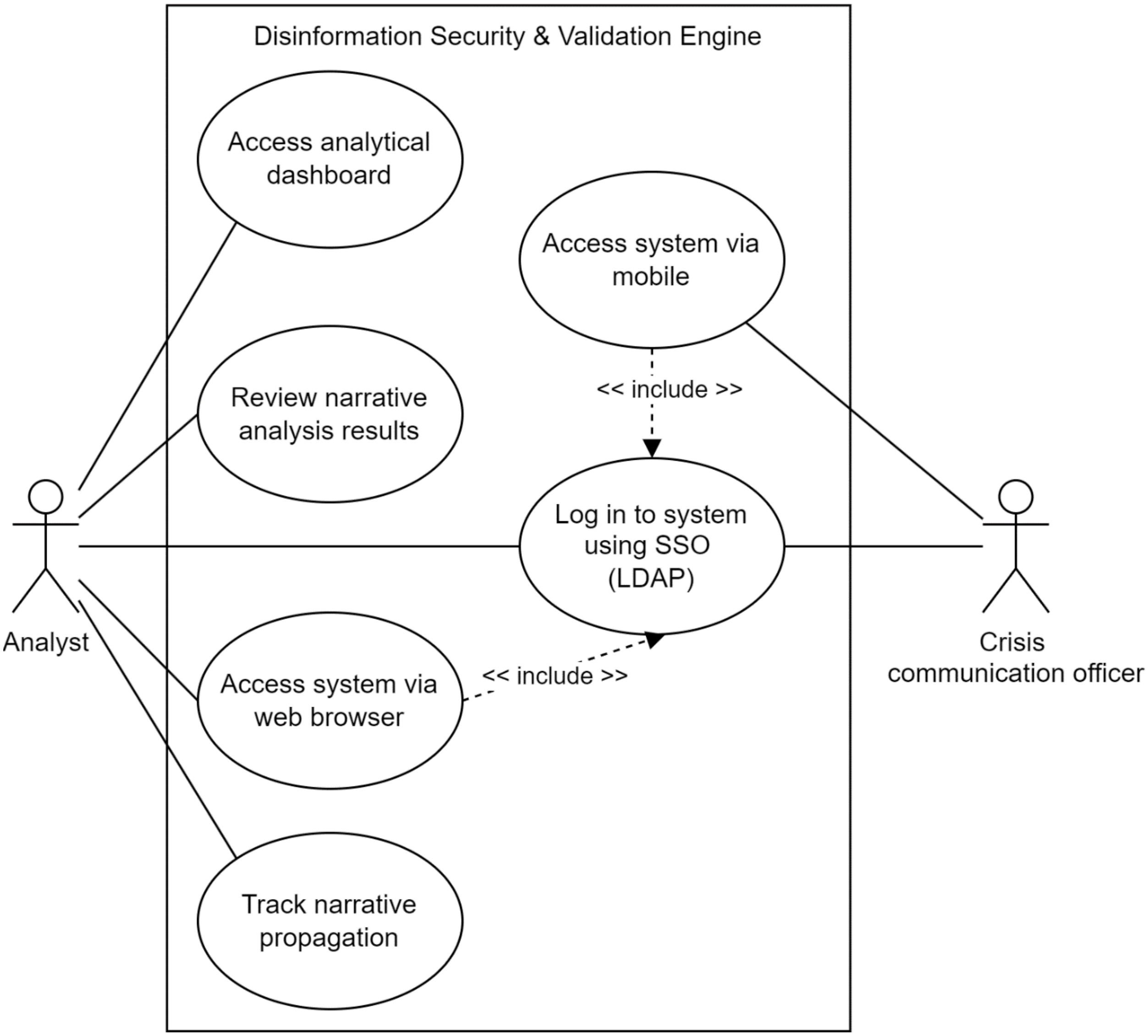

Disinformation Security & Validation Engine
Access analytical dashboard
Access system via mobile
Review narrative analysis results
<< include >>
Log in to system using SSO (LDAP)
Analyst
Crisis communication officer
Access system via web browser
<< include >>
Track narrative propagation

Figure 2. Use Case diagram – User Interactions

(add description for your diagrams here, refer to features using IDs you defined in 3.1.2.)

This use case view defines six primary use cases representing the key user interactions with the Disinformation Security & Validation Engine.

Government Analysts interact with the system primarily through secure web browser-based access (UC-4, Feature F-4) to open the analytical dashboard (UC-1, Feature F-4), review automatically generated narrative analysis results including sentiment and credibility scores (UC-2, Feature F-2), and track the origin and propagation of disinformation narratives (UC-5, Feature F-3).

Crisis Communication Officers utilize mobile access (UC-3, Feature F-5) for real-time monitoring and field response during crisis situations.

All users must authenticate through enterprise single sign-on integration (UC-6, Feature F-6) before accessing any functionality, as indicated by the <<include>> relationships. The authentication mechanism leverages LDAP-based SSO integrated with existing corporate security infrastructure.

3.2.1.3 Element Catalog

(Describe your actors and use cases in the table below)

#	Name	Description
ACT-1	Government Analyst	Agency personnel responsible for monitoring, investigating, and validating disinformation narratives using web-based analytical tools.
ACT-2	Crisis Communication Officer	Agency personnel responsible for rapid field response to emerging disinformation threats using mobile access.
UC-1	Access analytical dashboard	The analyst accesses the main analytical dashboard to view summary metrics, visualizations, and system alerts related to ongoing disinformation narratives.
UC-2	Review narrative analysis results	The analyst reviews automatically generated narrative analysis, including sentiment classification, source credibility, and predicted reach, to assess threat level and accuracy.
UC-3	Access system via mobile	The crisis communication officer accesses system capabilities through a secure mobile interface for real-time monitoring and on-site response during crisis situations.
UC-4	Access system via web browser	The analyst connects to the system through a secure web browser interface to utilize full analytical and investigative capabilities.
UC-5	Track narrative propagation	The analyst investigates and tracks identified disinformation narratives to determine their origin, trace their evolution across platforms, and assess their impact and spread patterns.
UC-6	Log in to system using SSO (LDAP)	The user authenticates to the system using enterprise single sign-on credentials via LDAP integration, which grants role-based access to authorized system functions.

3.3 Design Constraints

The section lists the constraints accounted for in the designed solution. These can be of business, technical, resource, and other types.

(list identified constraints in the table below)

#	Description
CONST-1	The solution shall be deployed on an infrastructure platform certified for use by national security and intelligence agencies, meeting stringent data handling and access-control requirements (e.g., ISO 27001, FedRAMP Moderate/High).
CONST-2	The solution shall utilize containerized deployment (Docker + Kubernetes) to enable rapid horizontal scaling during peak disinformation events such as elections or emergencies.
CONST-3	The platform shall provide secure, web-browser-based access for analyst teams, ensuring TLS 1.2+ encryption and session management aligned with organizational security policy.
CONST-4	The system shall support mobile access for crisis communication officers with equivalent authentication and authorization mechanisms.
CONST-5	Integration with existing corporate security and communications platforms is mandatory, requiring standard API documentation and single sign-on (SSO) integration via LDAP
CONST-6	The NLP models must achieve a minimum F1 score of 0.90 in classifying and scoring narrative veracity and intent
CONST-7	The organization must secure necessary legal permissions and API access from major social media and public data providers for data ingestion
CONST-8	The internal security team must approve the use of external cloud-based NLP models, provided data anonymization is guaranteed

3.4 Quality Attribute Scenarios

A Quality Attribute Scenario is an unambiguous and testable requirement for one or more Solution Quality Attributes such as Performance, Usability, Maintainability and others. The scenario consists of six parts: Source of Stimulus, Stimulus, Environment, Artifact, Response, testable and accurate Response Measure.

This section lists and prioritizes the scenarios pertinent to the designed solution.

(List your quality attributes in the table below (at least 5))

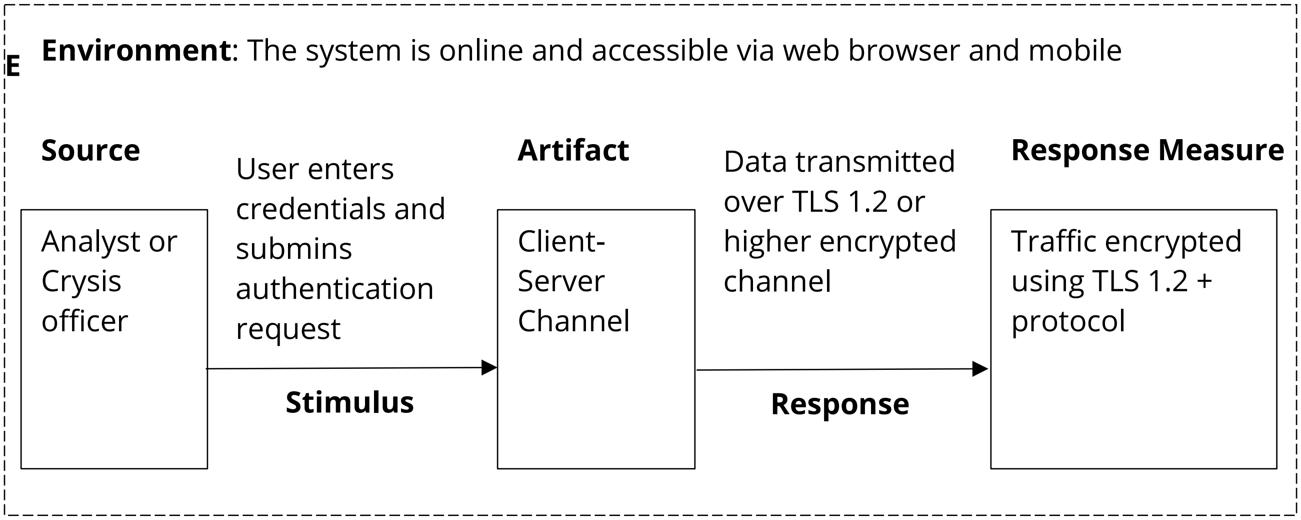
#	Quality Attribute	Scenario	Business Priority	Related To
QA-1	Performance (Real-time Processing)	When new digital content is ingested from social media or OSINT sources during normal operations, the system shall complete ingestion, analysis, and narrative scoring within 4 hours for at least 95% of content	High	F-1, F-2, BG-2
QA-2	Accuracy (NLP Model Performance)	During normal operation, NLP models shall classify and score narrative veracity and intent with a minimum F1 score of 0.90.	High	F-2, CONST-6
QA-3	Scalability (Peak Load Handling)	During peak disinformation events, the system scales horizontally using containerized deployment to handle increased content volume with no more than 10% degradation in average analysis time or model accuracy.	High	F-1, CONST-2
QA-4	Security (Data Transmission)	At all times, all user and narrative data transmitted between clients and the system shall be encrypted using TLS 1.2 or higher.	High	UC-6, CONST-3
QA-5	Availability (System Uptime)	Under normal and peak operating conditions, the system shall maintain at least 99.5% service availability on a monthly basis.	High	F-1, BG-2

#	Quality Attribute	Scenario	Business Priority	Related To
QA-6	Usability (Mobile Access)	Crisis communication officers shall be able to authenticate and access critical threat information via mobile device within 30 seconds, regardless of device, assuming a minimum network connection of 3G (1 Mbps downlink / 256 Kbps uplink) or better.	Medium	UC-3, F-5
QA-7	Interoperability (SSO Integration)	When a user attempts to log in, authentication via existing corporate LDAP infrastructure using SSO shall complete within 3 seconds in 98% of the cases, without requiring separate credentials.	Medium	UC-6, F-6, CONST-5
QA-8	Maintainability (Model Updates)	When NLP models require updates to counter evolving disinformation tactics, authorized data scientists shall deploy new models to production with zero downtime using the existing containerized deployment pipeline.	Medium	F-2, CONST-2

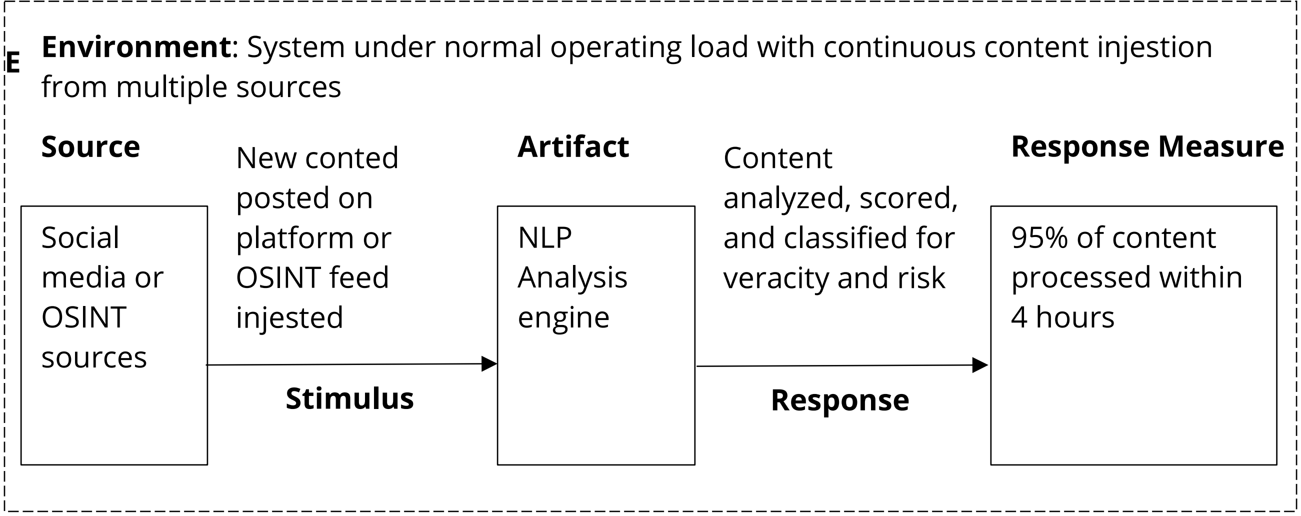
(At least one QA from the table above should be documented in the graphic format as below)

Scenario: QA-4
Quality Attributes: Security (Data Transmission)
Business Priority: High
Related To: UC-6, CONST-3, F-6

Description: All data transmitted between clients (analysts, crisis officers) and the system is encrypted using TLS 1.2 or higher at all times.


E
Environment: The system is online and accessible via web browser and mobile
Source
Analyst or Crysis officer
User enters credentials and submins authentication request
Stimulus
Artifact
Client-Server Channel
Data transmitted over TLS 1.2 or higher encrypted channel
Response
Response Measure
Traffic encrypted using TLS 1.2 + protocol

Scenario: QA-1
Quality Attributes: Performance (Real-time Processing)
Business Priority: High
Related To: F-1, F-2, BG-2
Description: When new digital content is ingested from social media or OSINT sources during normal operations, the system shall complete ingestion, analysis, and narrative scoring within 4 hours for at least 95% of content.


E
Environment: System under normal operating load with continuous content injestion from multiple sources
Source
Social media or OSINT sources
New conted posted on platform or OSINT feed injested
Stimulus
Artifact
NLP Analysis engine
Content analyzed, scored, and classified for veracity and risk
Response
Response Measure
95% of content processed within 4 hours

4 Solution Architecture

The section Solution Architecture is primary for the Architecture Vision document. It defines and reasons about the solution architecture design based on requirements and constraints identified in the section Architectural Drivers.

4.1 Big Picture

The section includes a list of architectural views covering the designed solution along with the context it runs in on the high level.

4.1.1 Solution Context

4.1.1.1 Intent

The view defines the primary solution components collaborating with the external systems and services. It is driven by the Business Case.

4.1.1.2 Representation

(add your C4 context diagram below)

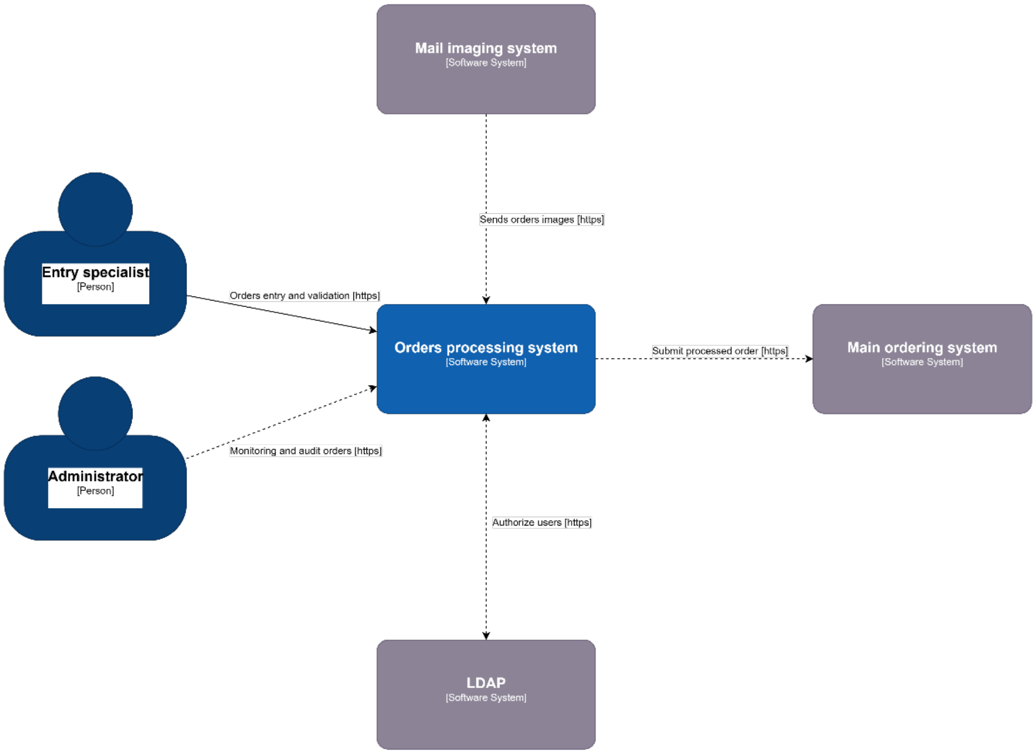


Figure 4. Solution Context diagram

(explain your context diagram)

4.1.1.3 Element Catalog

Table of annotated elements

(annotate elements from your diagram in the table below)

Name	Description
Cloud Based Solution	Responsible for implementing the REST API to serve data on request from the mobile and web clients
Element2	Responsible for a, b, c
Element3	Responsible for a, b, c
<element name>	<element description and responsibilities>

4.1.2 Solution Decomposition

4.1.2.1 Intent

The view defines the runtime decomposition of the server-side part of the solution. It is driven by the Business Case and the architecture best practices applicable to the cloud-based applications.

4.1.2.2 Context

The view context is defined by the view Solution Context where this section represents the decomposition of the system using the Containers view.

4.1.2.3 Representation

(add your container diagram below)

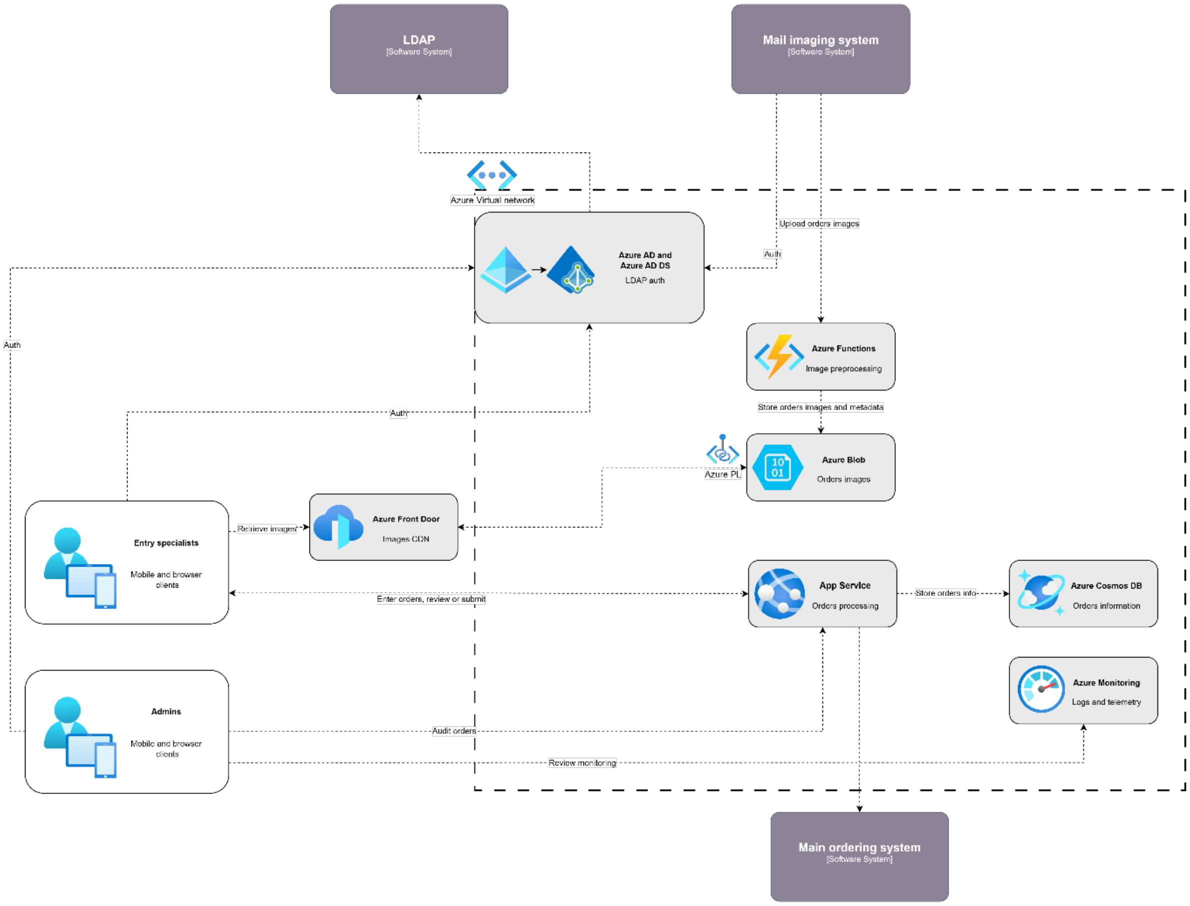


Figure 5. Cloud Solution Container view

(explain your container diagram)

The cloud based part of the solution is decomposed into several parts documented below combining several standard architectural patterns applicable to the highly loaded cloud based SaaS applications: Load Balancer, Data Cache, Background Process, Shared Storage, and Static Content Provider. The subsection resoning provides detailed discussion of these choices.

4.1.2.4 Element Catalog

Table of annotated elements

(annotate elements from the container diagram here)

#	Description
Element1	Responsible for a, b, c
Element2	Responsible for a, b, c
Element3	Responsible for a, b, c
<element name>	<element description and responsibilities>

4.2 Design Concerns

The section lists the concerns defined for the solution.

(list your design concerns/ architecturally significant requirements in the table below)

#	Description
CONC-1	<concern description>
CONC-2	<concern description>
CONC-3	<concern description>
CONC-4	<concern description>
<concern id>	<concern description>

4.3 Development Technology Stack

The section includes a list of decisions on tech stack, frameworks, libs, tools, external services, etc.

4.3.1 Development Languages, Frameworks, and Libraries

4.3.1.1 Intent

The view lists the set of programming languages, frameworks, and libraries the solution implementation will depend on.

4.3.1.2 Context

The context is provided by the view Solution Context.

4.3.1.3 Element Catalog

Table of annotated elements

(list all technologies, frameworks, libraries that have to be used in the solution in the table below)

Name	Version	Description
Framework1	x.x	Responsible for a, b, c
Library2	3.0-RC1	Responsible for a, b, c
Library3	x.x.x.x	Responsible for a, b, c
<name>	<version>	<description and responsibilities>

4.3.2 Development Tools

4.3.2.1 Intent

The view lists the set of tools the development team will rely upon in solution implementation.

4.3.2.2 Context

The context is provided by the view Solution Context.

4.3.2.3 Element Catalog

Table of annotated elements

(list all the tools, like IDEs, SAAS, plugins, etc that will be used during the development)

Name	Version	Description
Framework1	x.x	Responsible for a, b, c
Library2	3.0-RC1	Responsible for a, b, c
Library3	x.x.x.x	Responsible for a, b, c
<name>	<version>	<description and responsibilities>

4.3.3 External Integration Points

4.3.3.1 Intent

The view lists the set of programming languages, frameworks, and libraries the solution implementation will depend on.

4.3.3.2 Context

The context is provided by the view Solution Context.

4.3.3.3 Element Catalog

(list all the integration points if you have any 3-rd party integration in the table below)

Name	Version	Description
Framework1	x.x	Responsible for a, b, c
Library2	3.0-RC1	Responsible for a, b, c
Library3	x.x.x.x	Responsible for a, b, c
<name>	<version>	<description and responsibilities>

5 Implementation Roadmap

Implementation Roadmap defines the solution implementation road map including list of implementation deliverables, major milestones, effort estimates, and recommended team skillset, structure, and size.

5.1 Implementation Deliverables

The implemented solution will include the following parts as deliverables:

(list your deliverables in the table below)

Name	Refer to Requirements	Refer to Design
Application 1		
Service 2		
Mobile Client 3		
Production Deployment 4		

5.2 Implementation Milestones

The section proposes the major milestones to guide the solution implementation.

(decide and list main milestones for your project in the table below)

Milestone	Description	Outcomes
M0	Project bootstrap	▪ Dev Team ramped up ▪ Dev and Testing Environment set up ▪ Project Skeleton built
M1	Main application with web front-end development	▪ Alpha version of the web application ▪ Deployment to the staging
M2	Development and stabilization of the web application, development of the deployment and monitoring procedures, release	▪ Release 1.0 of the application prepared and stable ▪ DevOps framework functional ▪ Release 1.0 goes to production

5.3 Estimate

The Estimate section provides the estimates for the solution implementation based on the proposed architecture and selected estimation methodology.

5.3.1 Assumptions and Limitations

This section describes the known limitations imposed by selected platform, technology, hardware, operating system, third party components, etc. which might affect implementation effort and schedule estimates.

(Describe assumptions and possible limitations that could affect delivery timelines in the table below)

#	Description	Responsible
A1	Assumption 1	<Client Name>
A2	Assumption 2	SoftServe Team
L1	Limitation 1	<Third Party Name>

5.3.2 Estimate

The Estimate section provides effort and, optionally, schedule estimates for the implementation based on the architecture proposed in this Vision document using the WBS approach.

(list delivery items and estimation for these items to be ready)

#	Item	Complexity	Min Effort	Max Effort
1.				
2.				
3.				
4.				
5.				
Total:				

5.4 Team

The Team section outlines the proposed team skillset and structure based on the proposed technology stack and estimates.

5.4.1 Team Skillset

The section defines skills required from the different team member roles to implement the solution.

(describe team roles and required skillsets for these roles)

Role	Skillset
Business Analyst	▪ Business domain 1 ▪ Business domain 2
Backend Developer	▪ Programming Language 1 ▪ Technology 2 ▪ Framework 3 ▪ Tool 4 ▪ Standard 5
UI Developer	▪ Programming Language 1 ▪ Technology 2 ▪ Framework 3 ▪ Tool 4 ▪ Standard 5
DevOps Engineer	▪ Programming Language 1 ▪ Technology 2 ▪ Framework 3 ▪ Tool 4 ▪ Standard 5

5.4.2 Team Structure

The section proposes a team/sub-team structure and work allocation for the implementation phase.

(describe teams and their responsibilities)

5.4.2.1 Core Team

The core team is responsible for:

- Development of <Component 1>
- Development of <Component 2>
- Support of <Application 1>

Role	Responsibility	Count	FTE
Project Manager	▪ Project management (coordinate the team, status reporting, communications with the Client team) ▪ Gap analysis	1	0.5
Business Analyst	▪ Business analysis ▪ Business requirements specification ▪ Software requirements specification	1	1.0
Solutions Architect	▪ System analysis and design ▪ System requirements specification	1	0.2
Technical Leader	▪ Technical leadership and communication ▪ SCRUM Master ▪ Code Reviews ▪ Backend implementation	1	1.0
Sr. Backend Developer	▪ Technical communication ▪ Code reviews ▪ Backend implementation	2	1.0
Jr. Backend Developer	▪ Backend implementation	3	1.0
Int. UI Developer	▪ Web frontend design and implementation ▪ UX prototyping	3	1.0

5.4.2.2 DevOps Team

The DevOps team is responsible for:

- Configuration of <Environment 1>
- Configuration of <Environment 2>
- Deployment and runtime monitoring of <Application 1>

Role	Responsibility	Count	FTE
DevOps Architect	▪ Operations analysis and design	1	0.2
Int. DevOps Engineer	▪ System deployment ▪ Environment setup ▪ Production operations support	3	1.0