vehere

DATASHEET

Vehere Lawful Interception Monitoring Center

Vehere Lawful Interception Monitoring Center

Purpose-built for Law Enforcement Agencies to accelerate investigations and enable evidence-led prosecution

The Vehere Lawful Interception Monitoring Center (LIMC) is specifically designed to address the complex operational requirements of law enforcement agencies worldwide. Built with a user-centric approach, it delivers a unified view of intercepted data across diverse communication sources and networks. Its flexible and scalable architecture enables secure, reliable, and fully auditable monitoring while ensuring compliance with regulatory requirements.

It offers end-to-end coverage across mobile or cellular networks (5G/4G/3G/2G), IPLC, fixed networks (PSTN), IP networks as well as satellite links including both circuit-switched and packet data. It simplifies target pursuit in complex cases by providing a centralized suite of advanced analytical capabilities that empowers analysts to overcome the challenges of encrypted communications and correlation of information from multiple platforms.

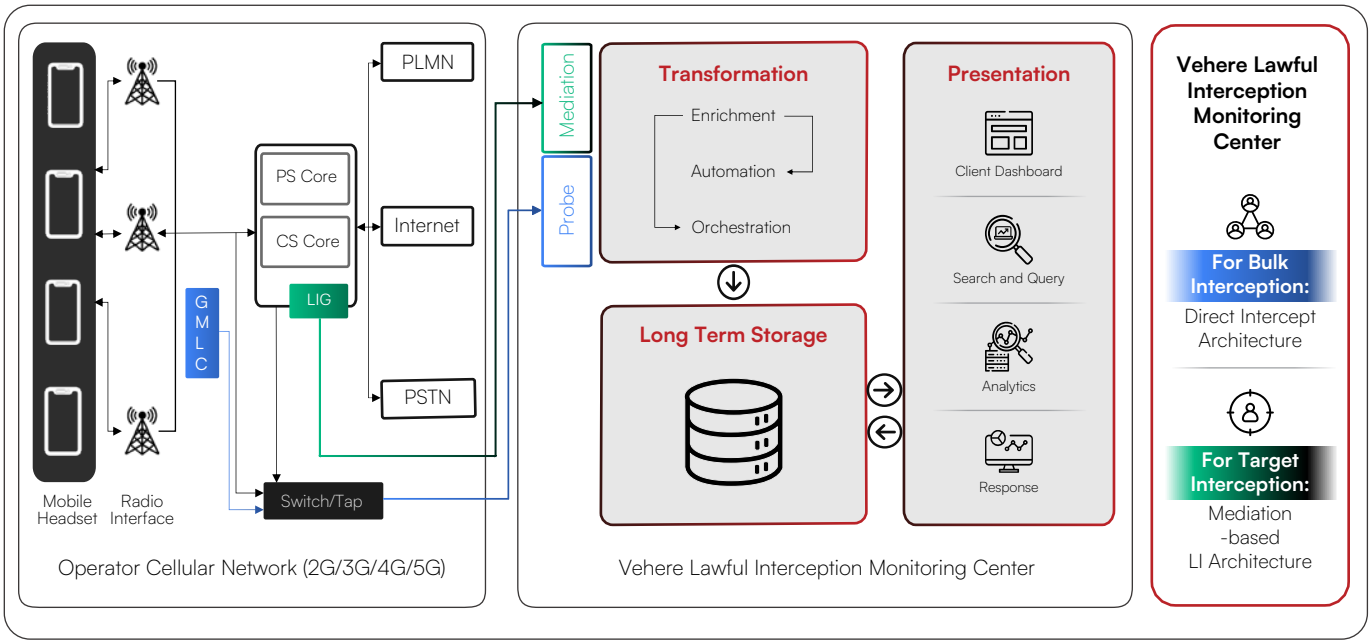


Fig. Architecture of Vehere Lawful Interception Monitoring Center

Key Highlights

- Comprehensive interception and analytics across voice, SMS, fax, email, web, video, VoIP, and IP-based communications
- Advanced target profiling through communication correlation, event analysis, subscriber intelligence, and intercepted data enrichment
- Geo-spatial intelligence and target tracking across 2G/3G/4G/5G, PSTN, and IP network environments
- AI-powered pattern analysis, anomaly detection, and intelligence generation for high-volume investigations
- Role-based access control, flexible architecture, and compliance with global lawful interception standards and regulatory requirements
- Scalable evidence management with long-term retention, customizable reporting, and efficient analyst workflows

Core Capabilities of Vehere Lawful Interception Monitoring Center

AI-powered Analytics

- AI-powered voice analysis delivers seamless language identification, translation, transcription, and speaker identification and diarization.
- AI-powered email analysis automates category classification and spam detection to significantly reduce operational workload.
- AI-powered behavior profiling to identify suspicious domain and communication patterns by detecting abnormal SIP activities and high-volume data transfers.
- AI-powered SMS Analysis for language identification, keyword extraction, and multilingual translation to accelerate intelligence analysis and investigative workflows.

Encrypted Traffic Analysis

Identifies both communication endpoints(IP) in encrypted application call sessions, including WhatsApp, Signal, Telegram, and Viber, through advanced network metadata analysis. Detects a broad range of encrypted applications and infers user activities such as calls, chats, and file transfers (uploads/ downloads), accelerating intelligence analysis and investigative workflows

Visual Link Analysis

Helps identify connections between targets and groups by revealing complex network structures up to 6 layers.

IM Analytics

Automated classification of IM applications and session activity (VoIP). Correlates session metadata to establish relational mapping between targets and behavioral patterns across encrypted communication channels.

Geospatial Analysis

Drives actionable intelligence by visualizing intercepted data points on interactive maps for accurate target location tracking, geofencing, and heatmap generation.

Crypto Transactions

Detects and analyzes cryptocurrency activity by extracting blockchain-related data from network traffic, delivering detailed insights into transaction metadata and currency types to uncover illicit financial flows.

Additional Features

Audit Trail

Maintains a granular audit trail of all user interactions, including logins, data access, modifications, and exports to provide complete operational visibility, internal accountability, and regulatory compliance.

Target and Case Management

Streamlines investigations with a centralized Target Management System to track and correlate target activities, coupled with a Case Management System for dynamic case assignment and focused team inquiry.

User-specific Dashboard

Accelerates decision-making with an intuitive, user-specific dashboard that converts complex network traffic into real-time visual analytics and actionable data insights.

Use Cases

- Organized Crime
- Illicit financial transactions
- Kidnapping and trafficking
- Narcotics and smuggling operations
- Terrorism
- Fraud

Objectives

- Uncover hidden patterns and detect unlawful activities
- Anticipate and prevent crimes
- Enable timely action and gather evidence for prosecution
- Support national security, peace, and public safety

Why is Vehere trusted by Law Enforcement Agencies?

- Terabit-speed packet capture with petabyte retrieval in seconds
- Protocol-agnostic architecture supporting 5000+ protocols
- AI-powered Network Intelligence for language and speaker identification, text translation and summarization and email analysis.
- 400+ metadata attributes help analyze encrypted IP traffic
- Custom PCAP ingestion and analysis
- Seamless integration with lawful interception gateway and third-party platforms
- Data fusion capabilities for better correlation
- Granular forensic analysis to uncover evidence, timelines, associations, and anomalies
- Fully on-premise deployment for the highest level of security
- Tailored IT support and services
- Intuitive and easy-to-use interface
- Supports wide range of law enforcement use-cases

Vehere Lawful Interception Monitoring Center—Specialized to Your Investigation Needs

Deep Network Intelligence

Represents internet and packet-based intelligence capabilities.

- Cryptocurrency analysis
- Application leak
- Deep Packet Inspection

Comprehensive Analytics

Provides analytical capabilities to derive actionable intelligence from collected data.

- Geospatial Analysis
- Visual Link Analysis
- Tracking and Correlation

Compliance

Focuses on maintaining legal and procedural integrity during investigations.

- Evidence and reporting
- Case and target management
- Audit trails

Investigation

Provides operational tools used by analysts during investigations.

- Transcription and labelling
- Product queries
- Rules and alerts
- Enrichment engines

Integrated AI/ML Analytics

Leverage advanced AI/ML-driven analytics to enhance investigative efficiency.

- Language Identification
- Transcription and Translation
- Speaker Identification
- Speaker Diarization
- Spam Detection in Emails
- Email Category Classification
- Behavior Profiling
- Generative AI-based Q&A application

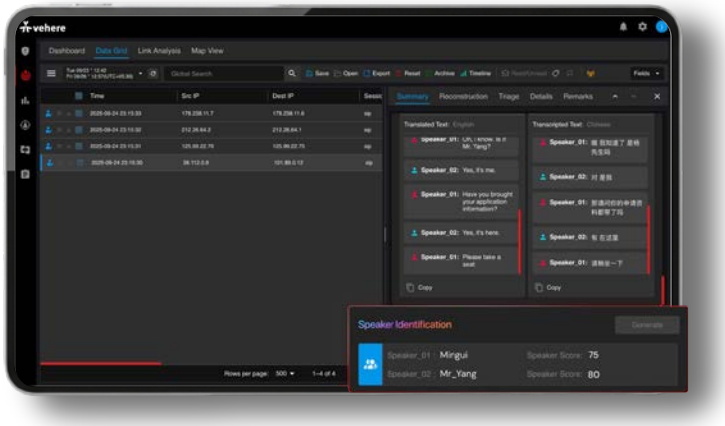
Open Architecture

Integrates with:

- Centralized Target Management using TAXII Protocol
- Phone directory, Identity Databases, Subscriber Databases
- AD/LDAP
- TIP Platform

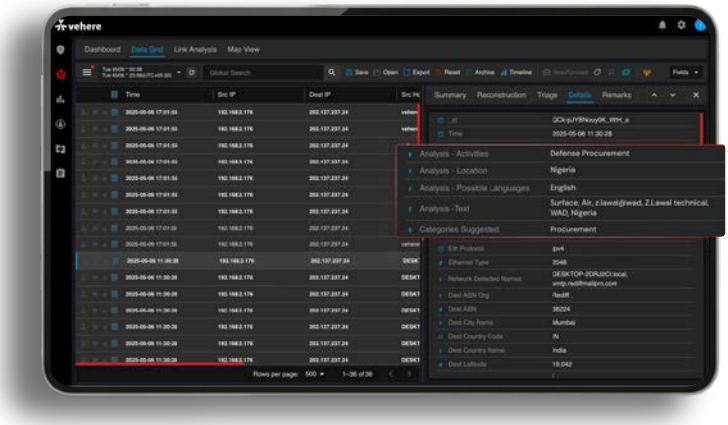
Integrates via:

- SNMP
- SysLog



AI-powered Speaker Identification

AI-powered Email Analysis



Geospatial Analysis

About Vehere

Vehere is an AI cyber defense company operating at the intersection of national security and enterprise security. Our AI-powered Network Intelligence platform processes petabytes of network data at terabit speed, empowering government agencies with real-time intelligence, advanced analytics, and actionable insights. From preventing emerging threats to accelerating investigations, Vehere helps governments and law enforcement agencies protect national sovereignty and strengthen public safety.