vehere

HUNT BEFORE BREACH™

AI Counter-Terrorism Software

A unified solution powered by AI and Big Data for Signals Intelligence - collecting and analyzing intelligence from foreign signals, and Cybersecurity - preventing and eradicating cyberthreats to national security systems and critical infrastructure.

Vehere AI Counter-Terrorism Software is a powerful system that is optimized for today's fast-paced digital environments, built for real-time collection and mass analysis of data from a variety of communication network sources.

Vehere enables collection and analysis of mass, wide, and target data from diverse communication network sources, including telephone calls, mobile data, and Internet-based services such as email, voice-over-IP, instant messaging, and others.

Its modular architecture facilitates seamless integration of disparate interfaces, data sources, and tools on a single platform. This empowers investigators to "connect dots" across data from various sources to identify suspicious behavior, uncover hidden connections between entities, find hidden leads, profile objects of interest, and make rapid detections to take action.

Its data fusion capability can ingest and reconstruct large volumes of data, import external data sources, perform highly flexible and intelligent custom queries, and provide location analytics for subjects of interest.

Vehere delivers National and Cross-border Cyber Vigilance for detection and containment of post-breach activities like ransomware, APTs, insider threats or lateral movements using AI and heuristic behavior analytics. It ensures full visibility with lossless packet capture, full digital forensics, next-gen file analysis, AI-powered breach detection and threat hunting.

KEY BENEFITS

Enhanced user management framework incorporating Role-Based Access Control (RBAC) & two-factor authentication to fortify security against unauthorized access

Delivers comprehensive summaries & complete session metadata of raw packet data

Unified view of all intercepted data on a single interface

Configurable data grid for accelerated analysis

Conducts analytic examination of encrypted application data from platforms such as WhatsApp & Signal to identify user activities

KEY HIGHLIGHTS

- Acquire & Decode Voice & IP Communication
- Examine and assess suspect activity via detailed metadata analysis
- An AI-driven intelligence collection system enhanced with Natural Language Processing, featuring capabilities such as spam filtering, language detection, speaker recognition, translation, sentiment analysis, and additional advanced functions
- Designed to manage and monitor millions of subjects effectively
- Comprehensive text search capabilities for thorough intelligence gathering
- Ingestion and assimilation of diverse external data sources, including banking records, passport information, and government ID databases, utilizing a robust ETL (Extract, Transform, Load) engine
- Architecture designed for 100+ Gbps & full duplex scalability and cost-efficiency, with the capacity to manage millions of subjects
- Machine learning and rule-based alert triggering system
- Implementation of two-factor authentication for secure admin entry, complemented by detailed audit logs tracking each user's actions

ABOUT VEHERE

Vehere is a new-age Cybersecurity software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere has been supporting counter-terrorism analysts in Defense & Intelligence communities. Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial Institutions, Smart cities, to protect their critical infrastructure against real-time cyberattacks.

Vehere preserves fundamental principles of privacy and civil liberties. We proactively defend your cyberspace by cross-leveraging our expertise between national security and enterprise security.

DIFFERENTIATORS

100% Capture, 100% Visibility, 100% Intelligence
High speed and real-time passive interception platforms for lossless data extractions with DPI engine

Port agnostic protocol detection of thousands of protocols

Open Architecture which is scalable, secure, and standards-based

AI/ML-based advanced analytics for data analysis and cyber threat detection

Deployment adaptability: Available for installation on customer-provided hardware or on Vehere-certified hardware systems

Supports complex and high-volume networks

Centralized monitoring/ processing of target related activity

in Vehere   X InVehere   f Vehere

BOOK A FREE TRIAL

vehere