vehere

FEATURE GUIDE

AI Counter-Terrorism
Metadata Analysis

Metadata analysis is an effective technique in network traffic that involves examining the descriptive data rather than the actual content of the data itself. This metadata can reveal valuable insights into network behavior, identifying potential threats, and optimizing performance, all while preserving data privacy. It focuses on analyzing the "envelope" of the data rather than its content, which allows for a proactive approach to security organizations.

Key Elements of Network Metadata:

- Source and Destination IP addresses to identify the origin and recipient of network traffic.
- Timestamps that indicate when the network activity occurred.
- Protocol that specifies the communication protocols used (e.g., TCP, UDP, HTTP).
- Port numbers, which designate the specific services or applications involved in the communication.
- Packet size indicates the amount of data transmitted in each packet.
- Flow information, including details about the duration and volume of network flows.

Key Capabilities:

- By analyzing metadata like IP addresses, timestamps, and protocols, security agencies and law enforcement agencies can identify suspicious traffic patterns without decrypting data, enabling the detection of malware, DDoS attacks, and unauthorized access.
- Metadata analysis helps identify deviations from typical user behavior, potentially flagging compromised accounts or insider threats.
- Network administrators can detect potential data leaks or exfiltration attempts by analyzing traffic volume, frequency, and destinations.
- Metadata analysis helps in the identification of congested areas, bottlenecks, and bandwidth hogs by analyzing packet sizes, frequencies, and IP flow patterns.
- It can help prioritize investigations by quickly identifying critical information, such as the location of a suspect or the timing of a cyberattack.

- Metadata can provide evidence to support other forms of evidence, such as witness testimony or physical evidence.
- Metadata analysis often does not require access to the content of communications, minimizing privacy concerns.
- It can reveal the locations and movement patterns of suspects, aiding in tracking and surveillance, helping agencies to focus on specific individuals or groups of interest, and reducing the scope of surveillance.
- Metadata analysis enables LEAs to identify, map, and understand the structure of criminal networks.

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.

Vehere InVehere Vehere