vehere

FEATURE GUIDE

AI Counter-Terrorism
Link Analysis

Link analysis in cybersecurity is a powerful technique for identifying, evaluating, and understanding the relationships between entities like users, devices, and activities. It is like connecting the dots in a complex puzzle, but instead of dots, one is able to piece together a digital landscape to uncover patterns and potential threats and aid in threat detection and investigation.

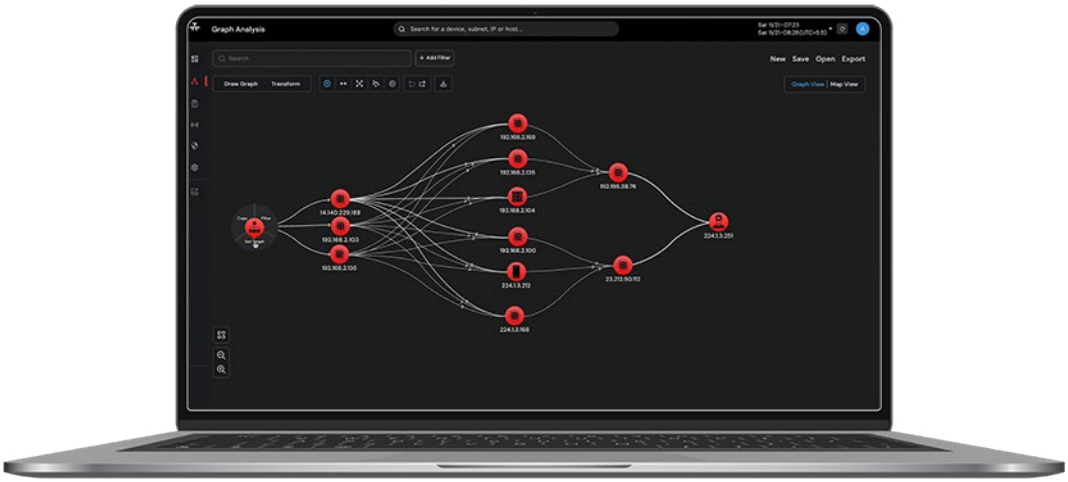
This feature helps the user to get a vivid understanding of the inter-relationship between the origin and the target in captured records. The connection between the origin and the target is displayed through an interactive pictorial view that also helps the user uncover important information about the same for a specific time range.

Key Capabilities

- Uses various network data processing algorithms of advanced analytics to analyze networks.
- Enhances user comprehension of the inter-relationships between the origin and target entities within captured records and identifies which nodes are more important or influential in the network.
- Involves an interactive pictorial view that displays connections between the origin and target, aiding users in uncovering vital information within a specified time range.
- Comprises multiple nodes, with each node representing either a source or a destination entity. Sources are linked to corresponding destinations via flexible, elastic strings featuring arrows directed towards the destination nodes.
- View all the session information transferred between any two nodes.
- Plot customized analytic graphs based on the source and destination IPDRs.
- Identify the nodes that hold greater importance or influence within the network structure.
- Download the node representation as an image file, with the downloaded file being in JPEG format.
- Get visual representations of the connections between the source and destination nodes on a geographical map through Map View.
- Reach up to six layers to find connections.

Advantages:

- Link analysis can reveal previously unknown relationships between individuals, groups, and organizations involved in criminal activities. By mapping these connections, analysts can gain a deeper understanding of the structure and dynamics of criminal networks.
- It can be applied to large datasets and allows agencies to establish linkage on different cases that may seem unrelated at first.
- Link analysis can help identify key criminals, allowing law enforcement agencies to target them for appropriate action.



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, and 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.