vehere

DATASHEET

Vehere Network Forensics

Enhance Actionable Intelligence and Expedite Incident Response

An organization needs to be able to swiftly investigate and determine the scope and impact of the incident so they can effectively contain the threat and secure their network.

Vehere Network Forensics allows you to identify and resolve security incidents faster by capturing and indexing full packets at extremely rapid speeds.

Vehere Network Forensics supports investigation activities by making available full extent, origin and, scope of an attack and, enabling creation of in-house threat intelligence. The rich insights, with detailed context about each attack, enable security teams to perform more conclusive incident investigations and faster AI- assisted threat hunting.

Being able to reconstruct and visualize the events triggering a malware download or callback enables your security team to respond effectively and swiftly to prevent recurrence. They can increase visibility into attacker activity by decoding protocols commonly used to move attacks laterally across a network. This combination of high-performance packet capture and in-depth analytics aids in swiftly identifying and monitoring all aspects of an attack.

KEY HIGHLIGHTS

- Continuous lossless gigabit packet capture.
- High-speed scalable packet capture infrastructure enabling data acquisition to petabyte scale.
- Event-based Capture accelerates the investigative process by using Event-based Capture to identify suspicious sessions that should be the focus for deeper investigations.

KEY BENEFITS

Extensive data-enrichment resulting in comprehensive context availability to help speed up incident analysis

Optimized data-retention with intelligent storage utilization for better evidence management

100% Packet Capture. Classification and Categorization at Line-rates

Insight into undetected protocols and applications to facilitate improved evaluation of security risks

Detects thousands of protocols and applications irrespective of L4 port/protocol pair to maximize content analysis

- Session and contextual metadata for granular enrichment about various facets of communicating endpoints, application, protocol, content and user.
- Automated integrations to deliver better investigative value by advanced content inspection using sandboxes or, static analysis techniques.
- Comprehensive reconstruction capabilities to ensure seamless visibility into content without the need for reliance on third-party tools.
- Wide array of interactive visualizations to improve data analysis process and enable faster problem hunting.
- Comprehensive analysis & representation of IPv4 and IPv6 traffic to allow for seamless insights into network activity over any protocol.
- Advanced storage management that discards redundant or unwanted traffic to optimize storage utilization.
- Time-travel for better retrospective analysis to determine root-cause and assess impact to business assets.

ABOUT VEHERE

Vehere is a leading cyber network intelligence company that utilizes continuous network monitoring to improve security posture and reduce blast radius. Our innovative Network Detection & Response solution transforms raw packets into information to draw meaningful insights, explore relationships, determine root-cause and accelerate detection and incident response for networks of any industry, any size and every organization.

Book a Demo of NF

Learn more at **www.vehere.com**

Vehere InVehere Vehere

DIFFERENTIATORS

Granular search and query engine supporting advanced options – wildcards, regular expressions, keywords and mathematical aggregations

Time-step to represent network activity into controlled sequence of events for easy analysis

Visualize threat sources and risky communications using advanced graphs for better representation of social network of users

Detects advanced targeted attacks and zero-day malware by integrating with network-based or, standalone sandboxes for dynamic analysis of file samples