vehere

DATASHEET

Network Forensics

Discern root cause and bolster threat hunting

Vehere PacketWorker NF is a Network Forensics solution that allows you to detect a broad array of security incidents, improve quality of response and precisely quantify impact of each incident by using high speed full packet capture technology.

PacketWorker NF supports investigation activities by making available full extent, origin and, scope of an attack and, enabling creation of in-house threat intelligence. Analysts can review specific network packets and sessions before, during and after an attack.

KEY HIGHLIGHTS

- High-speed scalable packet capture infrastructure enabling data acquisition to petabyte scale.
- Automated integrations to deliver better investigative value by advanced content inspection using sandboxes or, static analysis techniques.
- Wide array of interactive visualizations to improve data analysis process and enable faster problem hunting.
- Session and contextual metadata for granular enrichment about various facets of communicating endpoints, application, protocol, content and, user.
- Comprehensive reconstruction capabilities to ensure seamless visibility into content without the need for reliance on third-party tools.
- Comprehensive analysis & representation of IPv4 and IPv6 traffic to allow for seamless insights into network activity over any protocol.

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

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

- 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.

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

ABOUT VEHERE

Vehere builds intelligent and active solutions for real time Cyber Situational Awareness which forms the core component of Enterprise Cyber Defense and Homeland Security. Harnessing the power of advanced Big data Analytics, Artificial Intelligence (AI) and Machine Learning (ML), Vehere's Cyber Situational Awareness solutions have acquired a high level of efficiency, to effectively reduce the risk of a breach and to proactively defend against threats.

Book a Demo of PacketWorker NF

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

Vehere InVehere Vehere