vehere

DATASHEET

Network Detection & Response

Gain full visibility and detect latent threats to improve cyber situational awareness

Vehere PacketWorker NR is a Network Detection and Response solution that analyses network and endpoint telemetry data to uncover hidden assets & applications, speed-up threat detection and, help improve incident response by providing relevant context for investigations.

Using purpose-built artificial-intelligence algorithms PacketWorker NR analyses host behavior in real-time and initiates defensive actions against detected threats.

KEY HIGHLIGHTS

- Analyze user-internet (north-south) and, trusted-trusted (east-west) communication.
- Provides visibility into public, private and, hybrid cloud environments.
- Alerts annotated with MITRE ATT&CK and MITRE SHIELD framework.
- Automated response actions to contain the threat in real-time or, orchestrate execution of playbooks by integrating with third-party solutions.
- Scale horizontally by adding more nodes to the cluster without the need for expensive forklift upgrades.
- Lightweight "hidden" agent for acquiring telemetry data from devices "on-the-move" to ensure consistent security posture across the organization.
- Signature-less technology sans the need of correlation with an external threat intelligence source.

KEY BENEFITS

Detect risks in encrypted communications without the need for man-in-the-middle, decryption tools for operational efficiency and reduced complexity

Location and device agnostic user and application profiling for improved visibility and threat detection

Kills offending connection to deliver a swift response enabling augmented security posture

Active and Passive technology to discover devices and applications across traditional, cloud and, IT/OT Networks to improve risk assessment

- Advanced AI algorithms build and analyze model of host/ network traffic to determine malicious activity.
- Provides – device, application, network and, user – context for better insights.
- Analyze traffic-profiles, security risks and, host behavior in real-time to get an accurate picture of the environment for better assessment of the security posture
- Time-travel for better retrospective analysis to determine root-cause and, assess impact to business assets.
- Bidirectional integrations with SIEM, Network & Endpoint Security Solutions, SOAR and, Sandboxes.

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 NR

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

Vehere InVehere Vehere

DIFFERENTIATORS

High-speed, real-time ingestion of structured and unstructured network data from multiple sources – capture from interface, flow-data/IPFIX, telemetry data from endpoint-agent and, IPDR

Analyze almost any type of encrypted communication using mathematical modelling and heuristics

Actionable intelligence leveraging scientific methods and processes powered by deep-learning algorithms in support of accurate decision making

Advanced geospatial and temporal analysis enabling better investigation outcome

Multi-dimensional data analysis to improve threat hunting