vehere

DATASHEET

Vehere Network Detection & Response

Unrivalled Scale, Speed, and Visibility

Traditional security solutions are struggling to keep up with an evolving threat landscape that includes, among other things, supply chain risks, insider attacks, and living off the land methods.

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

It starts by automatically discovering and classifying every device communicating across the network, and using machine-learning driven behavioral analysis to detect anomalous and malicious activity.

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.
- Provides device, application, network and user – context for better insights.
- Bidirectional integrations with SIEM, Network & Endpoint Security Solutions, SOAR and Sandboxes.
- Advanced AI algorithms build and analyze model of host/ network traffic to determine malicious activity.
- Automated response actions to contain the threat in real-time or, orchestrate execution of playbooks by integrating with third-party solutions.

KEY BENEFITS

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

Automated Port agnostic protocol detection of thousands of protocols, which leads to accurate application detection and response

Wirespeed visibility layer 3-7, 100% Capture and Real-time Analysis using advance AI/ML. Reduce blind spots

Auto-Discover and classify every device that communicates on the network, including BYOD, IOT, and headless devices

Layer 7 Payload analysis and artefact extraction

- Scale horizontally by adding more nodes to the cluster without the need for expensive forklift upgrades.
- Detection and Powerful Analytics which automatically address the known, instantly detect the unknown and see the pattern of the unknown unknowns on your network, all while virtually eliminating false positives.
- 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.
- Advanced Forensics and Threat Hunting acts as long term repository and are powerful tools that provide analysts to investigate events in detail quickly and effectively, using evidence found in the original packets and files recorded from the network.

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 NDR

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, and IPDR .

Zero blind spot: Monitor Full Packet Capture at datacentre and Flow at branch level

Consumption of millions of IOCs and IOAs

Unscripted Threat Hunting for Emerging Threats

1-Click Evidence for Incident Response

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.