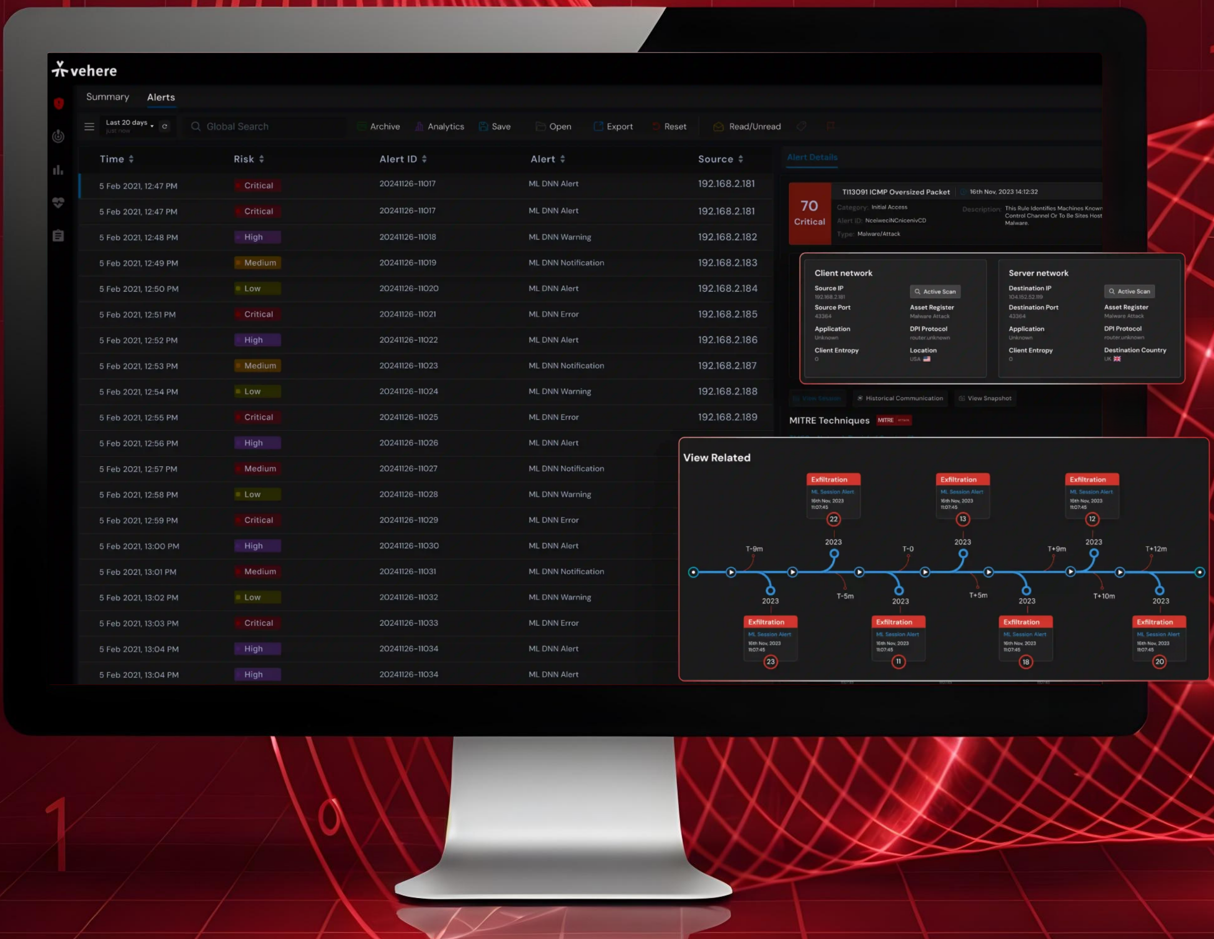
vehere

DATASHEET

Battle-Tested Network Forensics

Built for Combat. Engineered for Scale.
On-Premises by Design



Time	Risk	Alert ID	Alert	Source
5 Feb 2021, 12:47 PM	Critical	20241126-11017	ML DNN Alert	192.168.2.181
5 Feb 2021, 12:47 PM	Critical	20241126-11017	ML DNN Alert	192.168.2.181
5 Feb 2021, 12:48 PM	High	20241126-11018	ML DNN Warning	192.168.2.182
5 Feb 2021, 12:49 PM	Medium	20241126-11019	ML DNN Notification	192.168.2.183
5 Feb 2021, 12:50 PM	Low	20241126-11020	ML DNN Alert	192.168.2.184
5 Feb 2021, 12:51 PM	Critical	20241126-11021	ML DNN Error	192.168.2.185
5 Feb 2021, 12:52 PM	High	20241126-11022	ML DNN Alert	192.168.2.186
5 Feb 2021, 12:53 PM	Medium	20241126-11023	ML DNN Notification	192.168.2.187
5 Feb 2021, 12:54 PM	Low	20241126-11024	ML DNN Warning	192.168.2.188
5 Feb 2021, 12:55 PM	Critical	20241126-11025	ML DNN Error	192.168.2.189
5 Feb 2021, 12:56 PM	High	20241126-11026	ML DNN Alert	
5 Feb 2021, 12:57 PM	Medium	20241126-11027	ML DNN Notification	
5 Feb 2021, 12:58 PM	Low	20241126-11028	ML DNN Warning	
5 Feb 2021, 12:59 PM	Critical	20241126-11029	ML DNN Error	
5 Feb 2021, 13:00 PM	High	20241126-11030	ML DNN Alert	
5 Feb 2021, 13:01 PM	Medium	20241126-11031	ML DNN Notification	
5 Feb 2021, 13:02 PM	Low	20241126-11032	ML DNN Warning	
5 Feb 2021, 13:03 PM	Critical	20241126-11033	ML DNN Error	
5 Feb 2021, 13:04 PM	High	20241126-11034	ML DNN Alert	
5 Feb 2021, 13:04 PM	High	20241126-11034	ML DNN Alert	

70 Critical

TI13091 ICMP Oversized Packet 16th Nov, 2023 14:12:32

Category: Initial Access

Alert ID: NceiweciNCnicenivCD

Type: Malware/Attack

Description: This Rule Identifies Machines Known Control Channel Or To Be Sites Host Malware.

Client network

Source IP: 192.168.2.181
Source Port: 43364
Application: Unknown
Client Entropy: 0
Asset Register: Malware Attack
DPI Protocol: router.unknown
Location: USA

Server network

Destination IP: 104.152.52.119
Destination Port: 43364
Application: Unknown
Client Entropy: 0
Asset Register: Malware Attack
DPI Protocol: router.unknown
Destination Country: UK

Capture Every Packet. Reconstruct Every Attack. Zero Blind Spots at Petabyte Scale.

Modern SOCs operate in an environment where alerts are constant; encryption is pervasive, and attackers move laterally within minutes. Logs and alerts alone no longer provide enough context to answer the most critical incident-response questions: *What exactly happened? How far has it spread? Was data exfiltrated?*

Vehere Network Forensics delivers continuous packet-level visibility, session reconstruction, and deep historical lookback, transforming fragmented alerts into a coherent attack narrative. Built for terabyte-speed environments and petabyte-scale data volumes, the platform is battle-tested and combat-ready for mission-critical SOC operations. It enables security teams to capture, index, and analyze packet and flow telemetry across encrypted and unencrypted traffic, providing the high-fidelity evidence required to eliminate blind spots and reduce mean-time-to-detect (MTTR). Designed for combat against modern cyber threats, Vehere unifies detection and deep investigation within a single, scalable platform, enabling rapid containment and forensic-grade reporting.

Full fidelity packet capture (PCAP) for deep investigation.

Full session reconstruction to rebuild attacker timelines.

Metadata extraction from real network traffic.

Encrypted traffic intelligence without decrypting payloads.

Evidence preservation suitable for legal, audit, and IR workflows.

Network Forensics is foundational for modern SOCs because it enables post-incident clarity, supports threat hunting, and provides the ground truth needed to validate or refute alerts from SIEM, EDR, and NDR tools.

Vehere Network Forensics Highlights

- Continuous Line-Rate packet capture ensuring lossless traffic acquisition across high-throughput networks
- Patent Pending Indexed-RAW PCAP Storage enabling ultra-fast packet indexing, search, and retrieval
- Full Session Reconstruction and Traffic Replay with East-West / North-South flow correlation
- 180-Day Retrospective Threat Hunting across historical PCAP and flow telemetry
- L2-L7 Deep Packet Inspection (DPI) with protocol decoding across DNS, TLS, SMB, HTTP/2, SSH, and VoIP
- Encrypted Traffic Intelligence (ETI) using TLS fingerprints, JA3/JA3S, certificate telemetry, and behavioral analysis
- IOC-Driven Threat Hunting across IPs, domains, hashes, JA3 fingerprints, and network indicators
- On-Demand Dynamic File Analysis via extraction of objects and files directly from captured traffic

Vehere Network Forensics: Technical Specifications

Effective Network Forensics extends beyond packet capture; it requires a platform engineered for high-fidelity network visibility, rapid investigative workflows, and resilient performance across distributed environments. The specifications below outline the core capabilities powering Vehere Network Forensics, including sustained capture throughput, deep protocol decoding, real-time indexing, encrypted traffic intelligence, and efficient long-term retention.

Function	Attributes	Description	Capability
Packet Capture	Capture Throughput	Sustained lossless capture at 1/5/10/25G	All of them
	Max Capture Speed	Peak packet capture rate (e.g., up to 20 Gbps)	100G
	Capture Interfaces	SFP+, QSFP+, Copper/Fiber	Copper/Fiber
	Capture Modes	SPAN, ERSPAN, TAP, Cloud VPC mirroring	All of them
	Timestamp Accuracy	Hardware / nanosecond timestamping	Hardware
	Burst Handling	Protection against packet drops during spikes	Yes
Storage and Retention	Smart Storage	Selective or Filtered Storage	Yes
	RAW Packet Storage	Patented Indexed Raw Technique	Yes
	Onboard Storage Capacity	SSD/NVMe size and JBOD Storage	JBOD
	Expandable Storage	External storage options	Yes
	Retention Window	Days → weeks → months configurable	Configurable to months
	Compression Ratio	Efficiency of compressed storage	70% on Metadata storage
	Selective Capture Filters	Ability to exclude media, large transfers, encrypted payloads	All of them
	Legal Hold Support	Forensics-grade preservation of packets	Yes
Protocol and Decoder Support	Decoder/dissection Coverage	HTTP(S), DNS, FTP, SMB, VoIP, Email, etc.	All of them
	Custom Query Support	Ability to define custom queries	Yes

Metadata Extraction and Indexing	Metadata Types	L2-L7 metadata extracted	All of them
	TLS/SSL Metadata	JA3/JA3S, SNI, certificate fields	All of them
	Real-Time Indexing	Instant flow/session indexing	Session
	Search Latency	Typical sub-second search performance	None
	Export Formats	JSON, NetFlow v9, IPFIX, SiLK	JSON
Investigation and Search	Search Types	Session, flow	All of them
	IOC Compatibility	IP, domain, hash, JA3, cert fingerprint	All of them
	Filtering Capabilities	Time, protocol, direction, attributes	All of them
	Timeline Reconstruction	Visual attack sequence playback	No
	Drill-Down Navigation	Alerts → flows → packets	All of them
Encrypted Traffic Intelligence (ETI)	ETI Features	JA3/JA3S, SNI, TLS versions, cipher suites	All of them
	Certificate Analysis	Expired, untrusted CA, self-signed	All of them
	TLS Behavior Monitoring	Detection of anomalous encrypted flows	Yes
	ETI Without Decryption	Visibility into encrypted traffic	No
Deployment and Scalability	Deployment Types	Physical, VM, Cloud	All of them
	Multi-Site Support	Distributed probes	On-site Probes
	Centralized Management	Unified control plane	Yes
	Cluster Scalability	Scale-out indexing and storage	Yes
	Remote Site Capture	Lightweight capture nodes	Yes
Security and Compliance	RBAC	Role-based access permissions	Yes
	PII Masking	Built-in redaction	Yes
	Audit Logging	Full access and action logs	Yes
Integrations	SIEM Integration	Splunk, QRadar, Elastic, Seceon	Yes
	SOAR Integration	PaloAlto, Cortex	Yes
	Threat Intelligence	STIX/TAXII	Both
	Ticketing Integration	Cortex (Via SOAR)	Yes
	API Support	REST APIs for search and export	Yes

Licensing and Packaging	Licensing Model	Throughput, metadata, retention-based	Throughput -based
	Included Components	Probes, controllers	All of them
	Support Packages	Customised enterprise support	As per the agreed SLA

Full, Continuous Packet Capture Vs. Selective Packet Capture

Capability	Full Continuous PCAP	Event-Based PCAP
Complete Network Visibility	✓ Captures all packets continuously	✗ Only captures packets after an alert triggers
Pre-Attack Forensics	✓ Full visibility before, during, and after attacks	✗ No visibility before alert occurs
Unknown Threat Investigation	✓ Enables investigation of unknown or zero-day threats	✗ Limited to known signatures/ alerts
Attack Timeline Reconstruction	✓ Full attack chain reconstruction	✗ Partial timeline due to missing packets
Retroactive Threat Hunting	✓ Retroactive analysis of historical network traffic	✗ Cannot go back to investigate past traffic
Alert Validation	✓ Packet-level evidence for validation	✗ Difficult to validate false positives
Insider Threat Detection	✓ Detects slow, stealthy, insider attacks	✗ May miss low-noise or stealthy activity
Compliance & Legal Evidence	✓ Forensically sound packet records	✗ Incomplete packet evidence
Protocol-Level Deep Analysis	✓ Full protocol decoding and payload inspection	✗ Limited visibility
SOC Investigation Efficiency	✓ Single source of truth with packet evidence	✗ Requires multiple tools and assumptions

Why choose Vehere Network Forensics?

- Proven Line-Rate Continuous PCAP at Terabyte Speeds and Petabyte Scale
- Patent pending Indexed-RAW Packet Storage enabling ultra-fast packet indexing, search, and retrieval
- L2-L7 Deep Packet and Protocol Intelligence with advanced decoding across DNS, TLS, SMB, HTTP/2, SSH, and VoIP
- Encrypted Traffic Intelligence (ETI) using TLS fingerprints, certificate telemetry, and behavioral analytics without decryption
- Rapid Incident investigation via historical lookback, session reconstruction, IOC hunting and MITRE ATT&CK mapping
- SOC-Ready, Battle-Tested Architecture with scalable storage, real-time indexing, and seamless detection-to-forensics pivot

About Vehere

Vehere is a new-age software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere has been supporting criminal investigation analysts in Defense and Intelligence communities. Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial Institutions, and Smart cities to protect critical infrastructure against advanced cyber threats and nation-state attacks.

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.

Address:
1390 Market Street
Suite 200, San Francisco, CA 94102

Unit No. 5, 1st Floor, Andaz, Asset Area 1
Aerocity, New Delhi–110037

E: sales@vehere.com

W: www.vehere.com