vehere

Vehere Network Detection and Response (NDR)

ADEON

About Company

Vehere is a new-age Cybersecurity software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere solutions have been battle-tested by counter-terrorism analysts in Defense & Intelligence communities.

Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial Institutions, and Smart cities to protect their critical infrastructure against real-time cyberattacks.

Top 8	Top 10	Top 3
Financial Institutions	Global Telecom companies	Smart Cities

Vehere Customer's

Government and Public Sector

- Brihanmumbai Municipal Corporation
- Indian Railways
- रक्षा मंत्रालय Ministry of Defence
- पावरग्रिड POWERGRID
- Middle East Intelligence

Telecom and Network Providers

- TATA COMMUNICATIONS
- Jio
- AT&T
- verizon
- orange™
- Vi™

Cloud, Data & IT Services

- NTT
- sify
- lightstorm
- Global Cloud Xchange — A Reliance Company
- BEYOND ONE™

Banking and Financial Institutions

- SBI
- Punjab & Sind Bank — (A Govt. of India Undertaking) — Where service is a way of life
- IDFC FIRST Bank
- Kerala Bank — Kerala State Co-operative Bank
- IDBI BANK

VEHERE

State of Modern Enterprise Cybersecurity

Threat landscape is evolving

Phishing, Credentials, Vulnerabilities

Leading initial access vectors

Living-off-the-land

techniques look normal on endpoints

241 days

Average Dwell Time

SOC efficiency has become a risk

70% of SOC teams flooded with alerts

53% of security alerts are false positives

Perpetual flood of notifications can desensitize even the most trained analysts leading them to miss threats

EDR has blind spots

Threat actors bypass, blind or disable EDR

Attackers disable (turn the sensor off), reconfigure (change settings to prevent sensor from detecting), bypass (choose techniques that don't get flagged)

Not all systems/devices support agents

Countless devices cameras, smart displays, printers, HVAC controllers, forgotten workstations, etc. operate quietly outside of scope of traditional endpoint protection

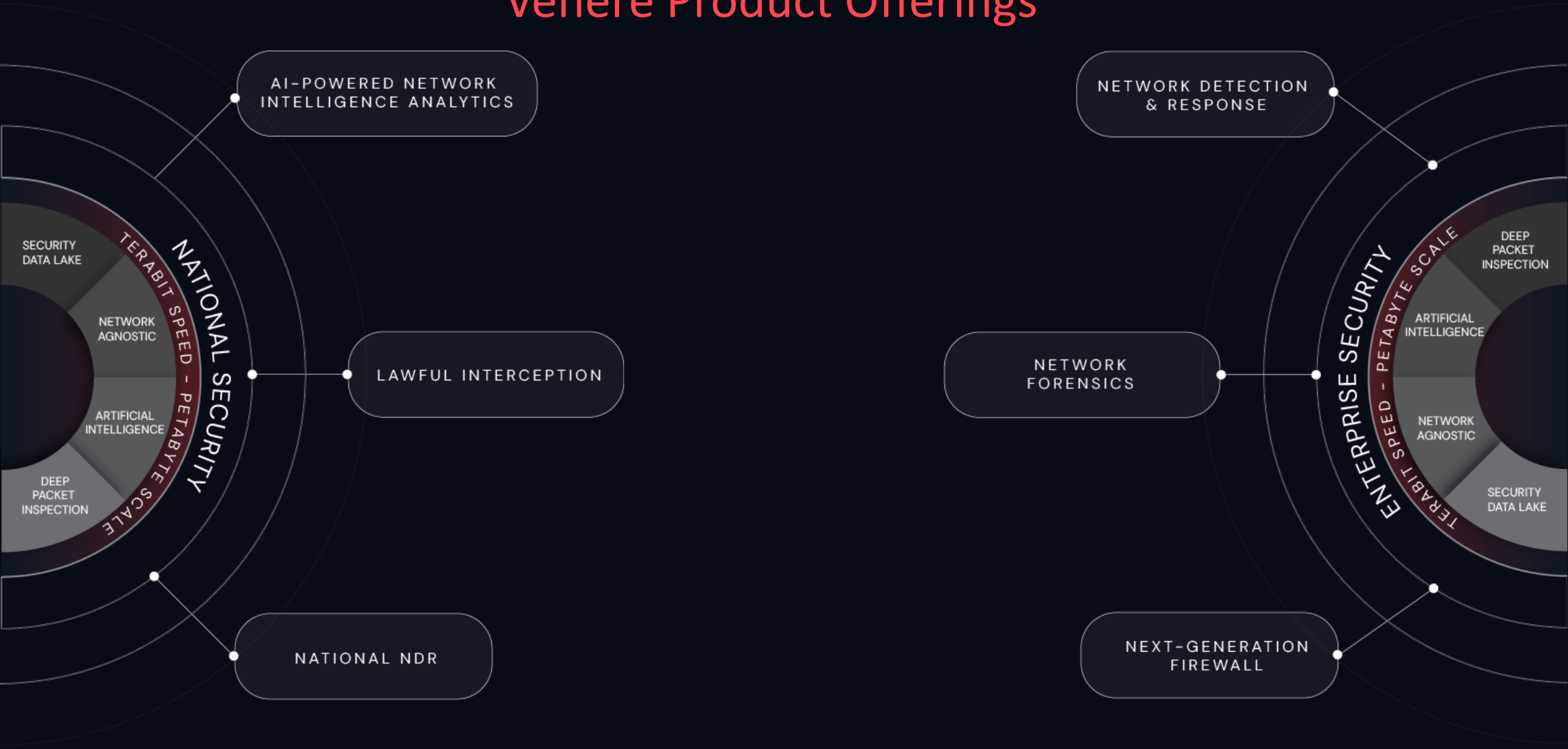
Hackers are logging in, not breaking in

SOC Teams are overwhelmed

Traditional Detection and Response is failing

VEHERE

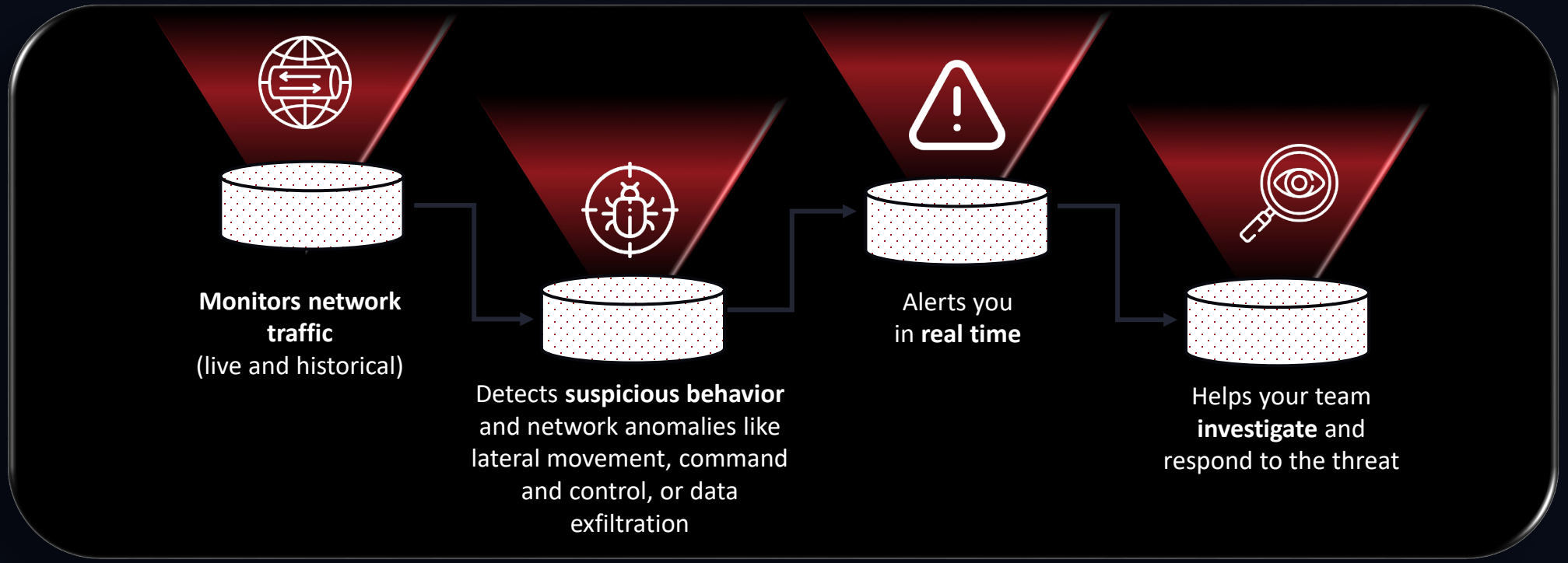
Vehere Product Offerings



What’s an NDR

Gartner

> Network Detection and Response (NDR) solutions use non-signature-based techniques, such as machine learning or other analytical methods, to detect suspicious traffic on enterprise networks. They continuously monitor network communications, log traffic, and use behavior analytics to detect threats and support incident response



VEHERE

The Vehere NDR Approach

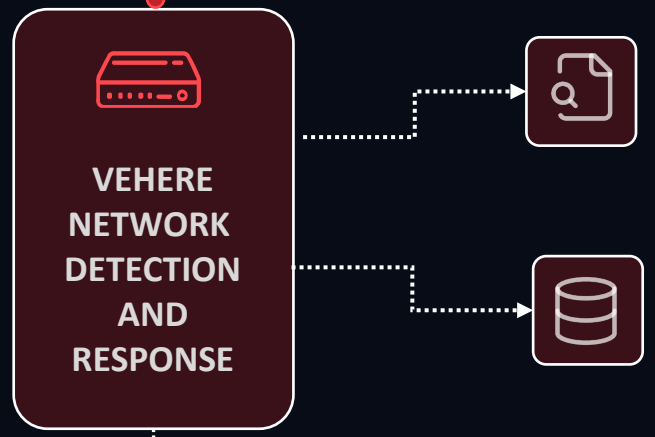
TRADITIONAL:

4 NETWORK SECURITY TECHNOLOGIES

NETWORK DETECTION AND RESPONSE	• Flow
DYNAMIC FILE ANALYSIS	• Detect Malware in 12-18 hours
NETWORK FORENSICS	• Non-indexed
INTRUSION DETECTION SYSTEM	• N-S

THE SECOND LINE OF DEFENSE

"ONE" GEN-NEXT TECHNOLOGY INSTEAD OF 4



NETWORK DETECTION AND RESPONSE	• Flow • Full, Continuous PCAP • Metadata
DYNAMIC FILE ANALYSIS	• Built-in Malware Sandbox
NETWORK FORENSICS	• Full Network Forensics • Complete Session Reconstruction
INTRUSION DETECTION SYSTEM	• E-W and N-S

Vehere NDR Value Proposition

VISIBILITY

- 100% Visibility with Lossless Packet Capture
- Analytics based on DPI with L2 - L7 metadata
- E-W & N-S traffic
- Behavior based protocol detection
- Historical metadata & content

BREACH DETECTION

- Behavioral Analytics
- Lateral Movement
- Discovery, Reconnaissance, Credential Access, Collection, Exfiltration, Impact, C&C, Initial Access, Execution
- IDS Rules for E-W & N-S traffics
- Risk Scoring
- MITRE ATT&CK mapping

PROACTIVE THREAT HUNTING

- AI/Machine Learning
- ML DNS Analytics
- Retrospective Detection
- UltraHunt 2mn IOCs at line rate -Integrate massive Threat Intelligence
- Geolocation
- 6-degree Graph Analysis
- Encrypted Communication Analysis

DYNAMIC FILE ANALYSIS

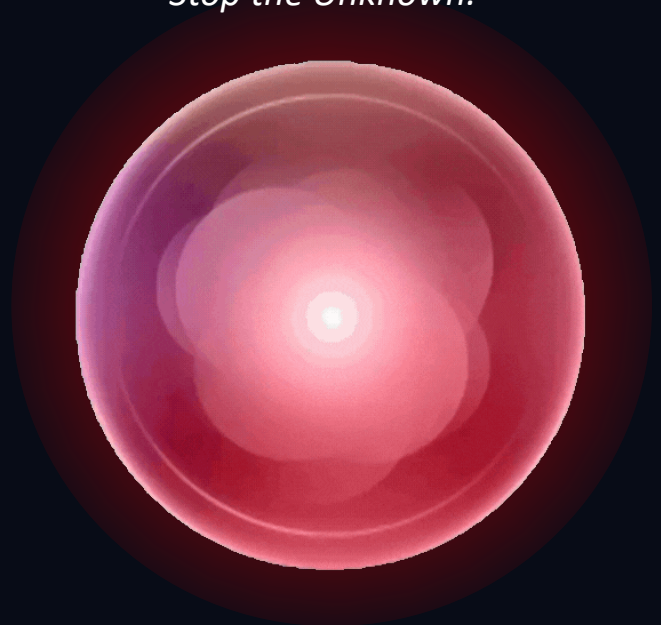
- Dynamic File Analysis: Our Malware Scanner detects Zero-Day malware
- Malware analysis mapped to MITRE TACTICS

FULL NETWORK FORENSICS

- Lossless network traffic capture ensures no evidence is lost
- Frictionless investigation to real-time alerts in minutes by live and historical network traffic analysis
- Automated Forensics and security data lake ensure compliance and actionable insights
- Patent-pending Indexed-Raw technique for fast retrieval of packets

Vehere Vision AI

See the Unseen.
Stop the Unknown.



An intelligence fabric that underpins all Vehere solutions – NDR, AI Counter-Terrorism and SIGINT for Cyber Defense

Fully On-Prem	Trained on your data	Always Learning

Because humans simply cannot keep up with the growing volume of threats

886B+
Daily Security Events
Cisco Talos 2024 Year in Review

241 days
Mean time to detect breach
IBM Cost of a Data Breach 2025

40%
Alerts are not investigated
Prophet Security: 2025 State of AI in Security Operations

Multiple Models, One Mission:
Eliminate Blind Spots

Predictive AI → Detects what's emerging

Generative AI → Explains what's happening

Agentic AI → Acts on what's learned

Any anomalous authentications today?

Detected a new geolocation login at off-hours on a first-seen device (risk score 53).

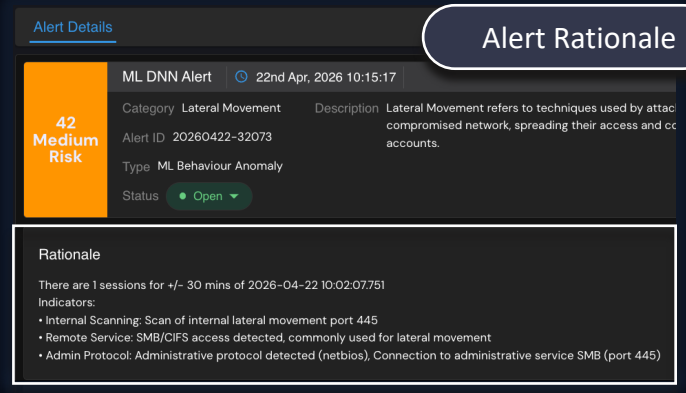
Why was this host flagged?

Unusual outbound connections and high data transfer - possible early signs of exfiltration.

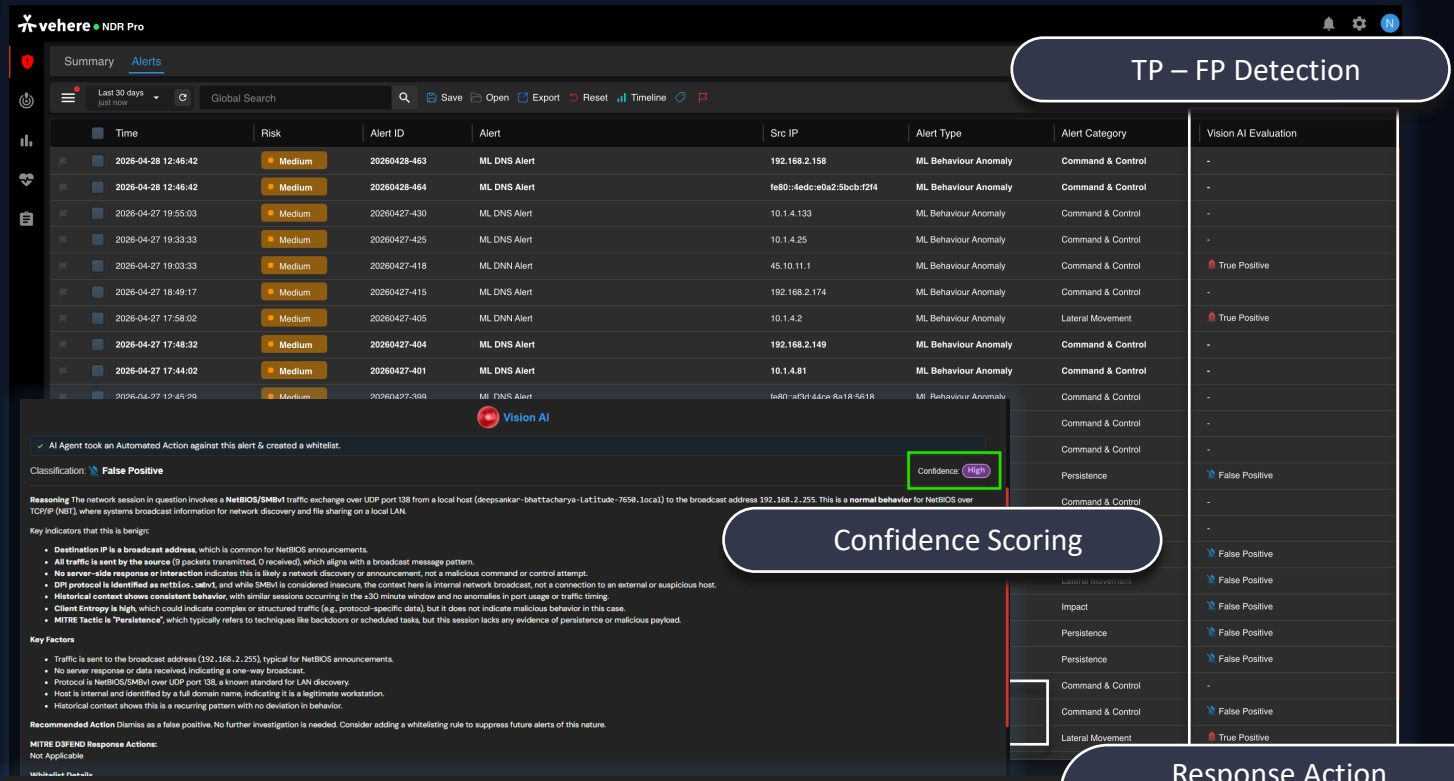
VEHERE

Multi-Agentic AI – Interpret, Analyze, Respond

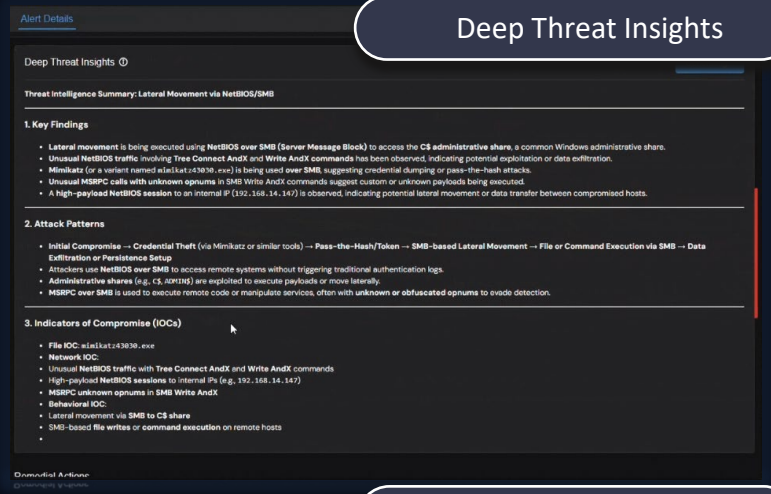
Alert Rationale



TP – FP Detection

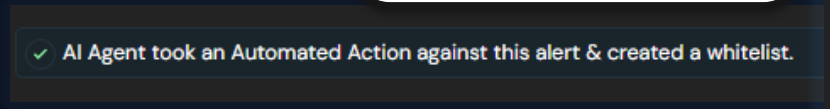


Deep Threat Insights



Confidence Scoring

Automated Whitelisting



Response Action Recommendations

MITRE D3FEND Response Actions:

- **Network Traffic Analysis (D3-NTA):** This technique helps in identifying anomalous network behavior, such as unidirectional traffic and unusual protocols. In this case, the traffic pattern (e.g., no response from the internal host, high volume from the source) is consistent with C2 activity. NTA can be used to detect and block such traffic in real time.
- **Network Isolation (D3-ISO):** This technique can be used to isolate the affected host (`DESKTOP-TS16JIM.local`) from the rest of the network to prevent further data exfiltration or lateral movement. Since the host is communicating with an external source in an unusual manner, isolating it is a key defensive action.
- **Network Communication Analysis (D3-NCA):** This technique involves deep inspection of network communication patterns and can be used to detect command and control behavior. The absence of inbound communication and the use of an uncommon protocol (`tcpmux`) are strong indicators of C2 activity, and D3-NCA can be used to flag and respond to such behavior.
- **Network Traffic Filtering (D3-NTF):** Applying rules to block or limit traffic to and from the source IP `45.10.11.1` can prevent further communication. Since the traffic is suspicious and not part of a known legitimate service, filtering it at the perimeter is an effective mitigation step.

VEHERE

Comprehensive Encrypted Traffic Visibility

Encrypted Traffic Analysis (ETA)

No decryption needed

- JA3/JA3S fingerprinting
- TLS handshake and metadata analysis
- Packet Size and flow characteristics
- Timing and Beaconing
- ML Behavioural Anomalies

TLS Decryption

Deep payload inspection

- Full HTTP Headers and URLS
- File extraction and analysis
- Malware signature inspection
- Data exfiltration detection
- Policy-based decryption controls

VEHERE

Platform Orchestration

INTEGRATION

- SIEM, XDR & SOAR Platforms
- AD/LDAP
- TIP Platform
- SNMP
- SysLog
- Threat Intelligence

paloalto NETWORKS splunk> opentext™ NETWITNESS

INFRASTRUCTURE

- Indexed Security Data Lake
- Ease of scalability – Add sensors or analytics cluster to support growth
- Infrastructure, Operating Environment and Application agnostic

DEPLOYMENT

- Non-intrusive; 24x7 vigil
- Analyze east-west and north-south traffic
- Flexible Deployment - both Flow and Raw Network Traffic Packet (PCAP)
- Analyze Internet, Intranet, Data-Centre, Private-Cloud, Public-Cloud, Infrastructure, Applications
- Offline PCAP Analysis
- Smart Storage
- Role-Based Access Control
- PII Masking

VEHERE ARCHITECTURE

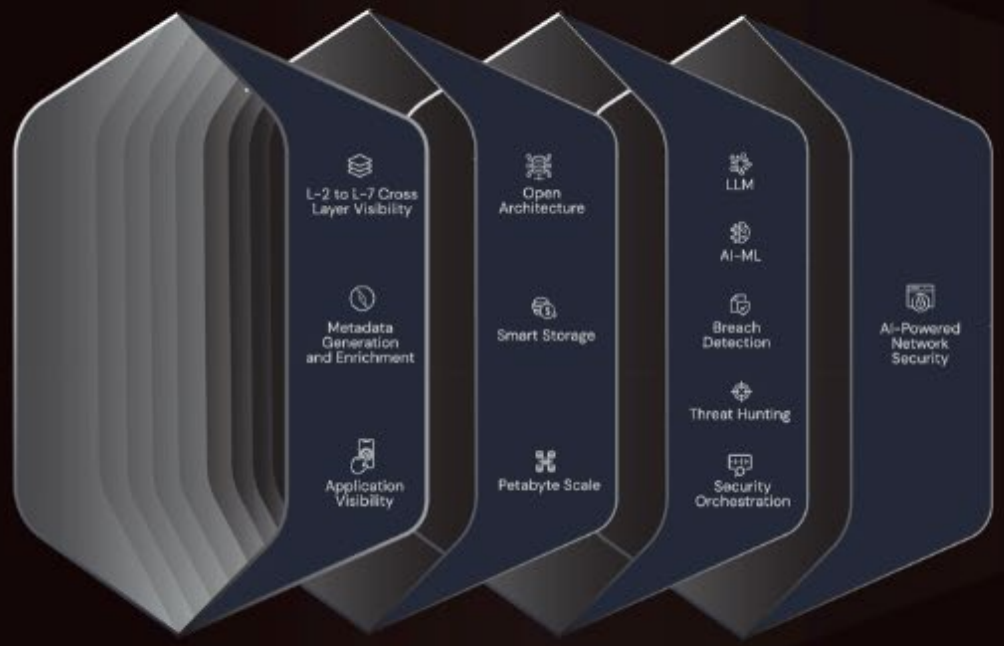
HUNT BEFORE BREACH™

Terabit Speed - Petabyte Scale

LOSSLESS CAPTURE

- Full Packet Capture
- PCAP
- Netflow
- IPFIX
- Jflow
- Sflow
- IOT
- OT

ULTRAHUNT THREATS



100% VISIBILITY

Network Detection and Response	Flow and Raw Network Traffic
Network Forensics	Indexed-Raw and Full Network Forensics
Next-gen Sandbox	Advance File Analysis for Malware detection
Intrusion Detection System	For N-S and E-W traffics

100% INTELLIGENCE

2Mn IOCs-ULTRAHUNT

3X PROACTIVE THREAT IDENTIFICATION

Why Vehere

100% VISIBILITY

100% Intelligence powered by Lossless Packet Capture

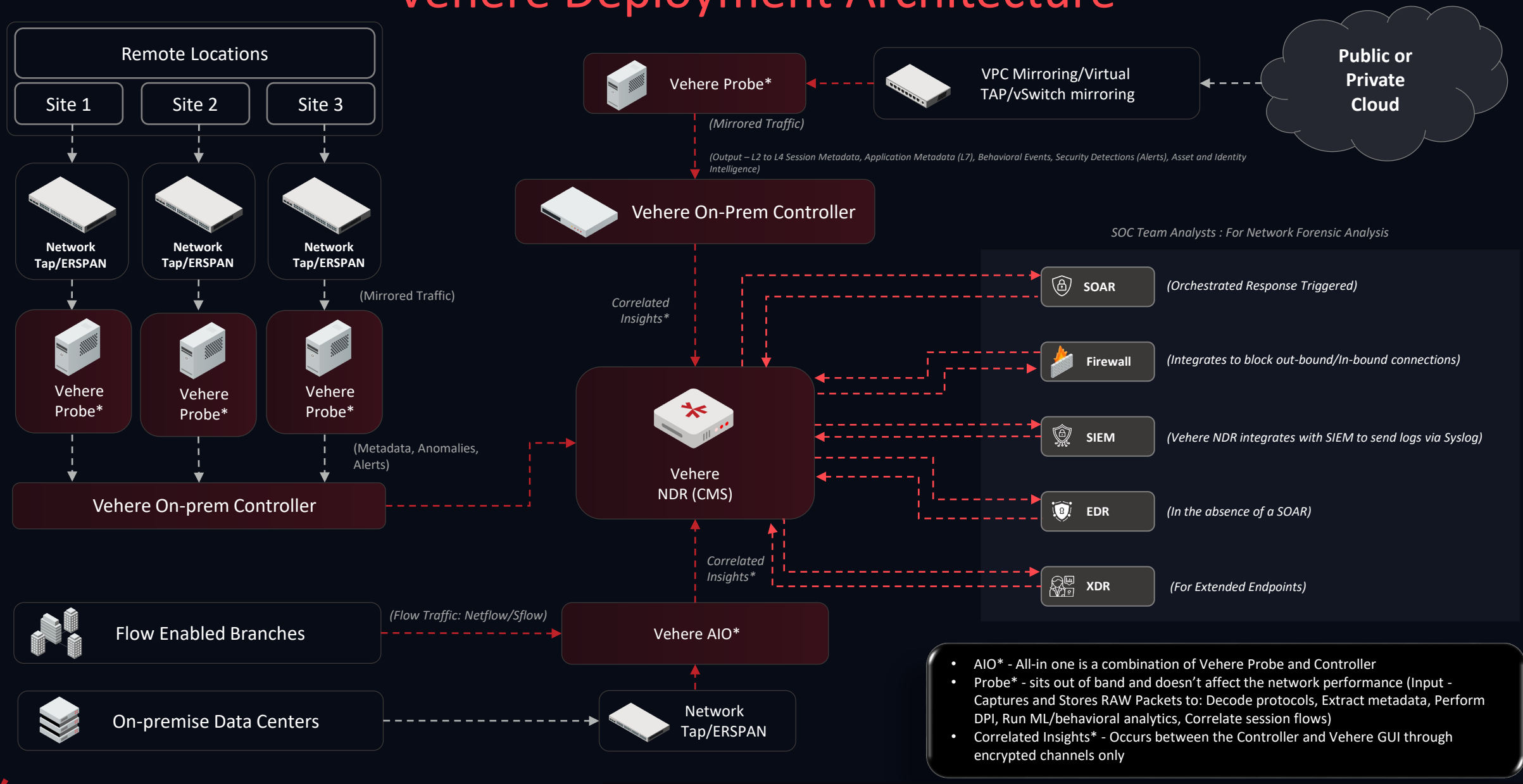
REAL-TIME DETECTION

Hunt Threats at lightning speed on terabit speed traffic

EARLY WARNING

Identify patterns and anomalies within petabyte-scale, distributed data

Vehere Deployment Architecture



- AIO* - All-in one is a combination of Vehere Probe and Controller
- Probe* - sits out of band and doesn't affect the network performance (Input - Captures and Stores RAW Packets to: Decode protocols, Extract metadata, Perform DPI, Run ML/behavioral analytics, Correlate session flows)
- Correlated Insights* - Occurs between the Controller and Vehere GUI through encrypted channels only

VEHERE

Vehere NDR – Detection Capabilities

Comprehensive defense against advanced cyber threats

Unknown Threats

Behaviour-based

AI/ML-powered detection

Advanced algorithmic threat identification

Entity Behavior Analysis (EBA)

Detects anomalies in user and entity actions

Native, Dynamic File Analysis

Sandbox execution for zero-day malware

Yara rules on unpacked files

Deep inspection of payload contents

Custom query editor

Flexible threat hunting capabilities

Known Threats

Signature-based

2mn+ known IOCs

Extensive global threat intelligence database

35,000+ Native IDS Signatures

High-performance intrusion detection

Static file analysis

Rapid signature matching for files

YARA on packed files

Identification of obfuscated malware

Custom rules

Organization-specific security policies

Vehere NDR in Action

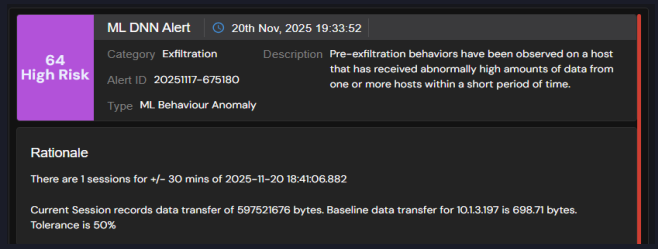
Initial Compromise (Foothold established)

An endpoint was successfully compromised and began communicating with an external command server

Internal host 10.1.3.197 initiated encrypted HTTPS communication. SSL fingerprint (JA3) matched known malicious threat Intelligence. Vehere TI Engine flagged blacklisted fingerprint.

Internal Data Staging (Preparation Phase)

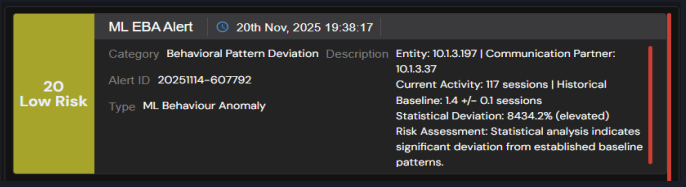
Attacker prepared sensitive data internally before extraction



597 MB internal data consolidation detected. Vehere DNN Pre-Exfiltration Model flagged abnormal data hoarding. Behaviour deviated sharply from historical baseline.

Internal Reconnaissance (Expansion Phase)

Threat actor expanded access and identified additional internal targets.



8,434% spike in HTTPS sessions. ML EBA detected massive behavioural deviation. Activity consistent with internal scanning and mapping

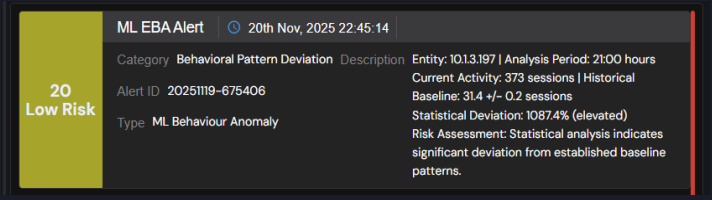
Lateral Movement and Credential Theft

Attacker escalated privileges and gained broader access within the network

SMB pivot from 10.1.3.197 → 10.1.3.42.Administrative share abuse (C$). Mimikatz deployed for credential harvesting. File reconstruction confirmed tool usage

Data Exfiltration (Preparation Phase)

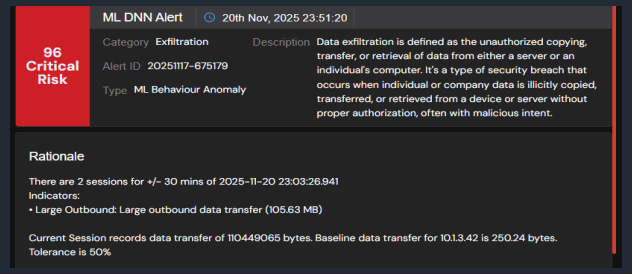
Attacker connected with c2 channels for exfiltration of data



Vehere ML EBA detects significant deviation (373 sessions, 1087% increase) in sessions from standard baseline (31.4 sessions)

Data Exfiltration (Impact Phase)

Sensitive data was successfully exfiltrated after internal compromise at off-hours



105.63 MB transmitted externally via HTTPS. Vehere ML Exfiltration Engine triggered high-confidence alert. ML Entity Behaviour Analysis detected unusual off hours activity.

VEHERE

Dashboards

Security Posture at-a-glance

- Centralized Network Visibility
- Behavioral Analysis and Anomaly Detection
- Contextualized Threat Insights and Alerting
- Deep Protocol and Application Awareness
- Rapid drill-down into sessions, payloads and network interactions
- Network Usage Trends (traffic patterns, application usage etc.)

Detection

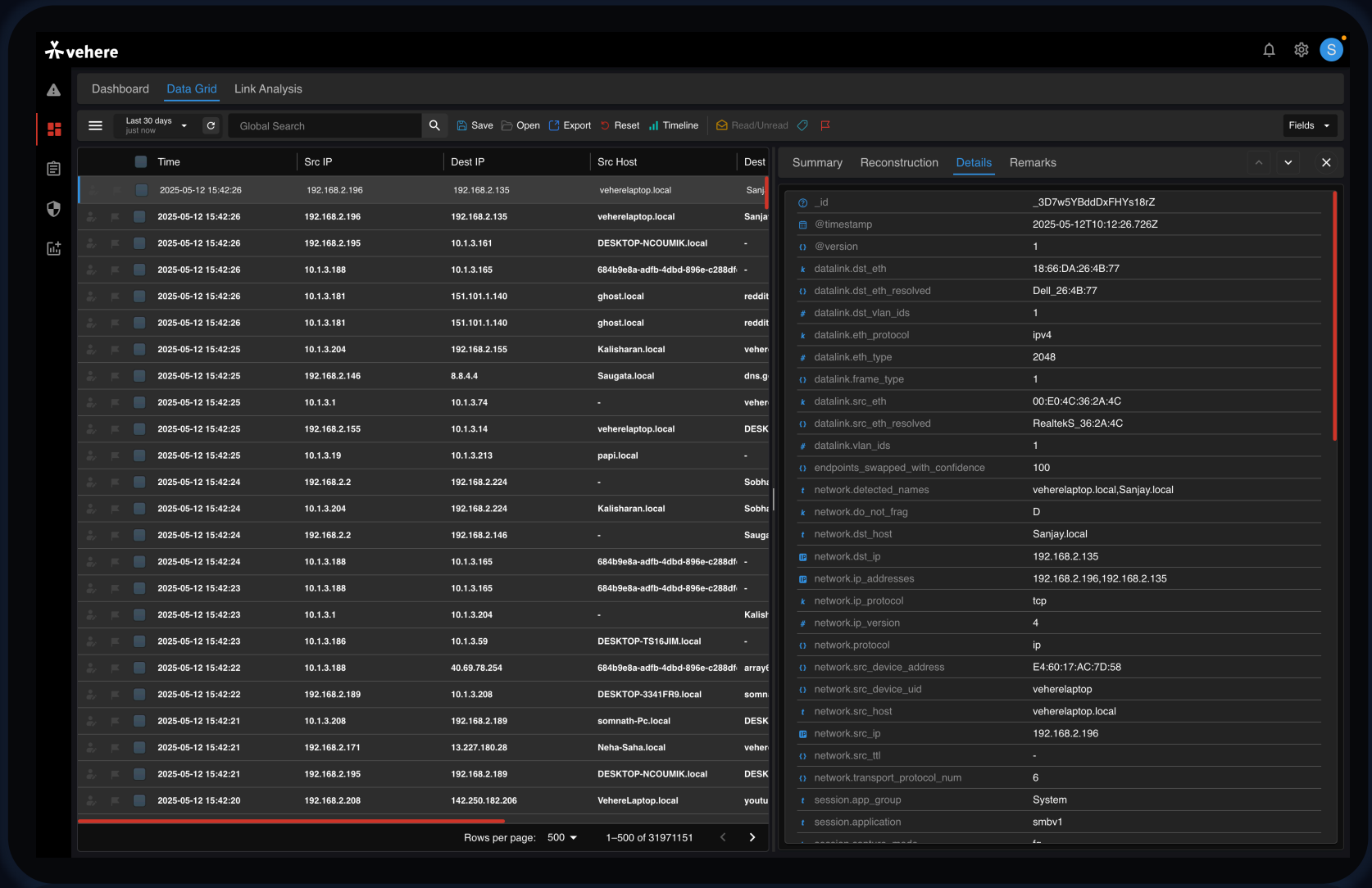
Risk Prioritization:

- MITRE ATT&CK Mapping
- Alert Severity Categorization
- Analytics on 400+ L2-L7 metadata fields
- AI-powered TP and FP detection
- Identifies relationships across users, devices, sessions etc. to reveal attack paths
- Consolidates repetitive alert triggers within a defined time window into a single enriched alert

Visibility

Deep Session Analytics:

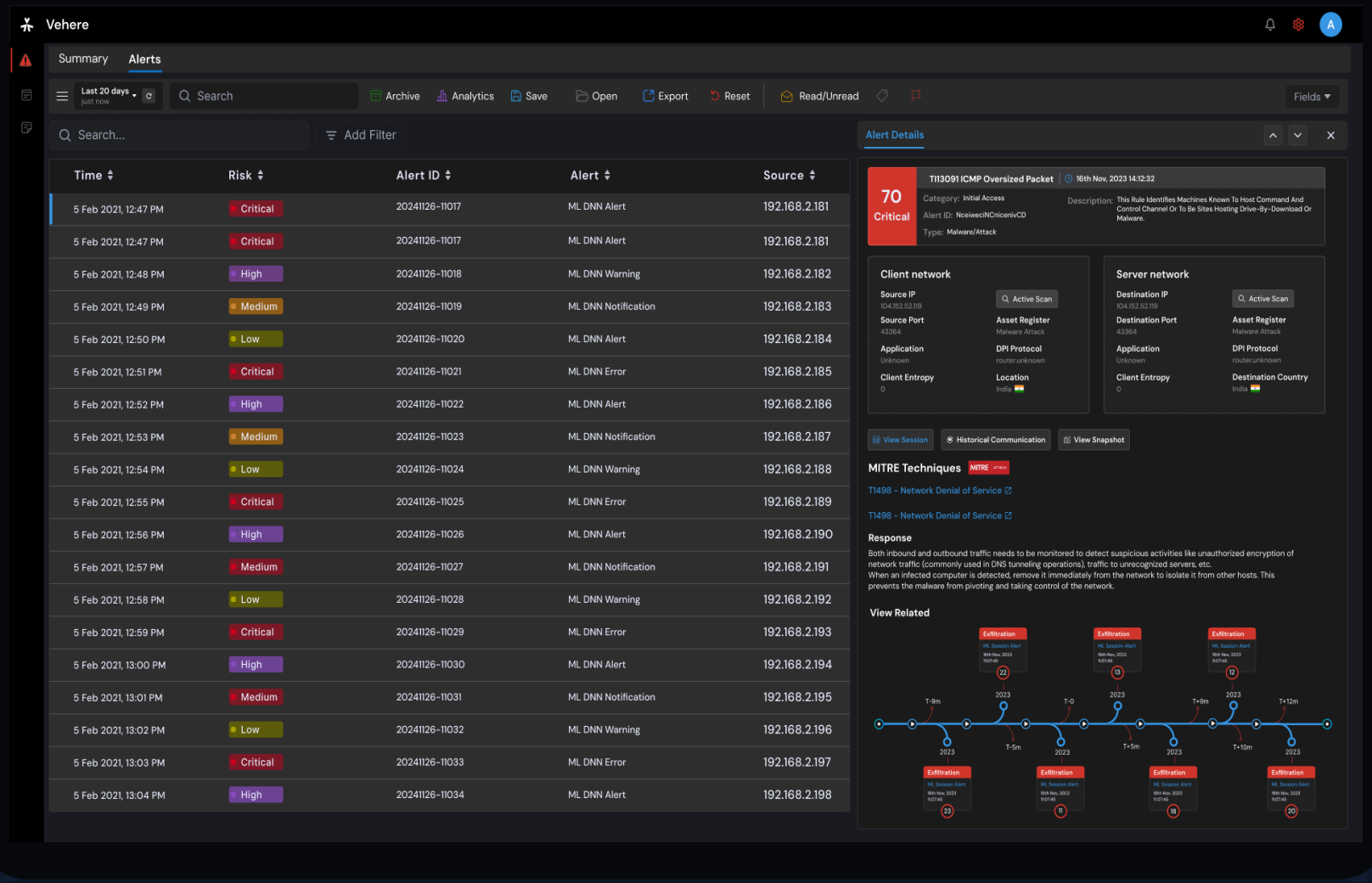
- Session-Level Insight
- Protocol and Encryption Context
- End-to-End Flow Context
- Timeline Correlation
- Entropy and Fingerprint Indicators
- Metadata-Rich Analysis



Investigation

Threat Investigation and deep dive:

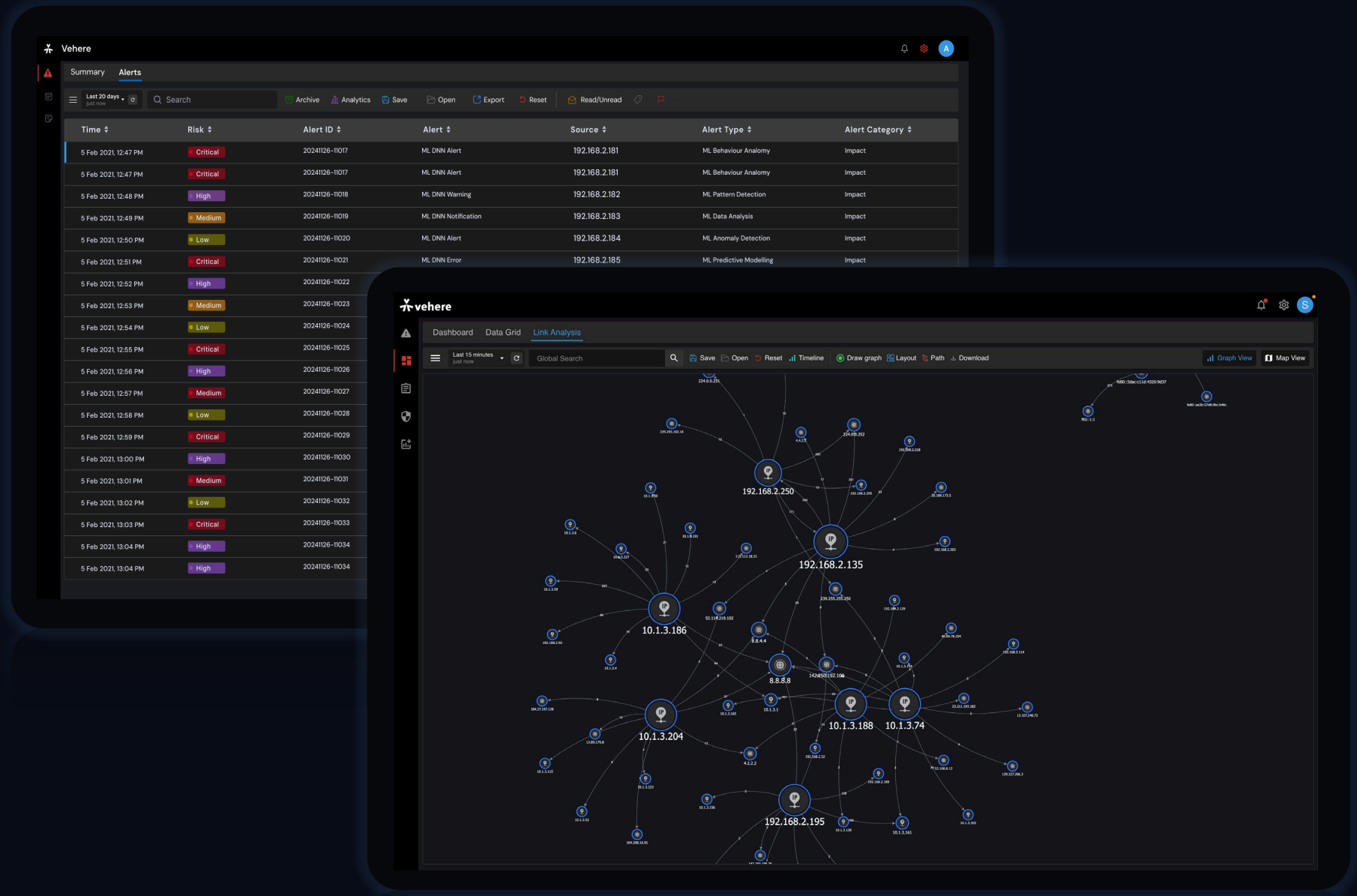
- 1-Click Evidence for Incident Response
- Investigation Acceleration
- Time-Based Filtering
- External Threat Context
- Session Correlation
- Communication Timeline and Historical Linkage
- Visual Threat Chain Representation
- Rule-engine-based alerts, IDS Rule-based alerts, ML-based alerts, and On-Demand Scan-based alerts



Hunting

Threat Hunting:

- Entity Relationship Mapping
- HTTP Request Visibility
- Source-Destination Mapping
- Hostname Contextualization
- Protocol Awareness
- Application Identification
- Temporal Event Analysis
- Query-Based Filtering
- Behavioral Baseline Reference

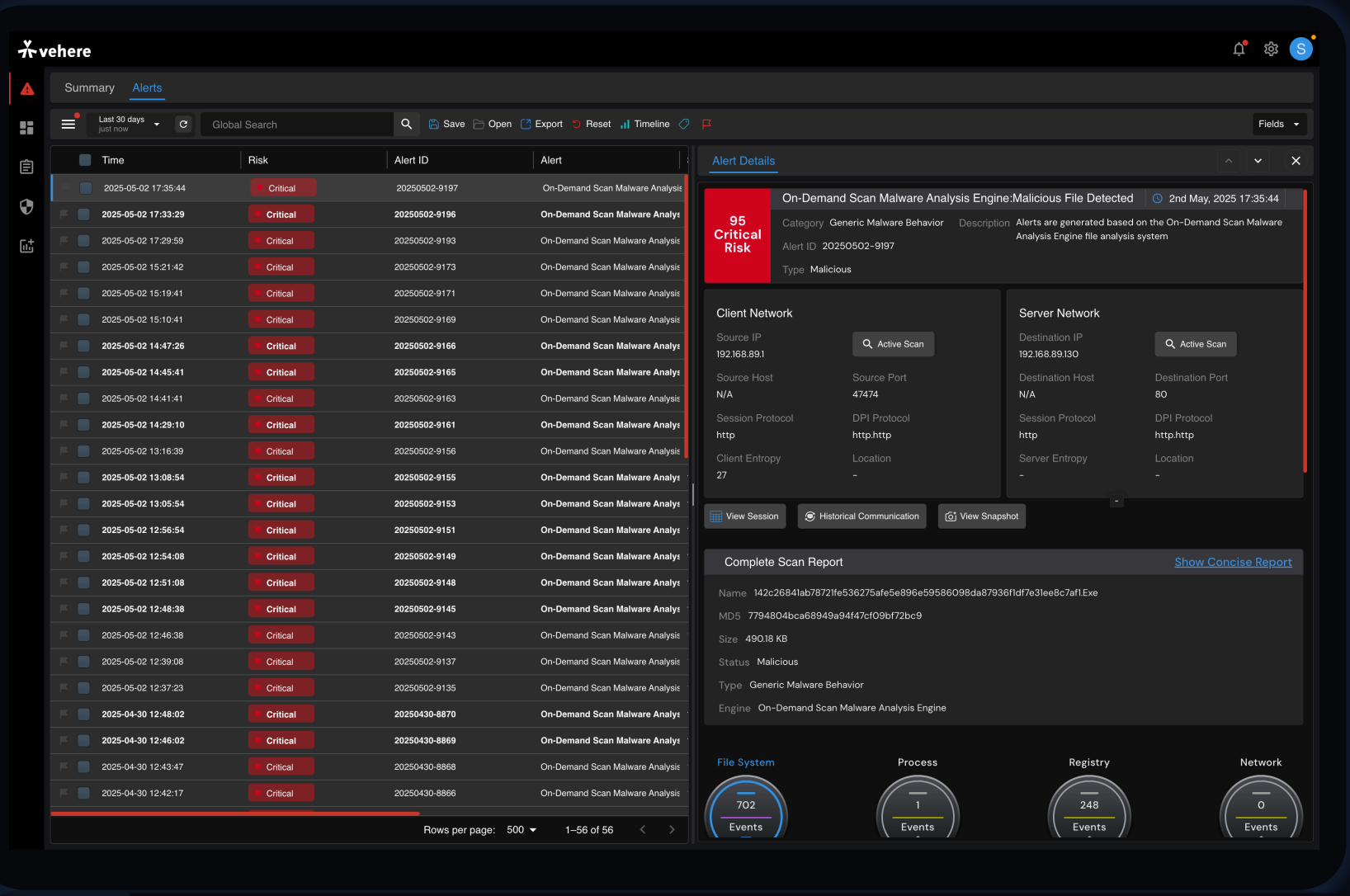


VEHERE

Containment

Threat Containment:

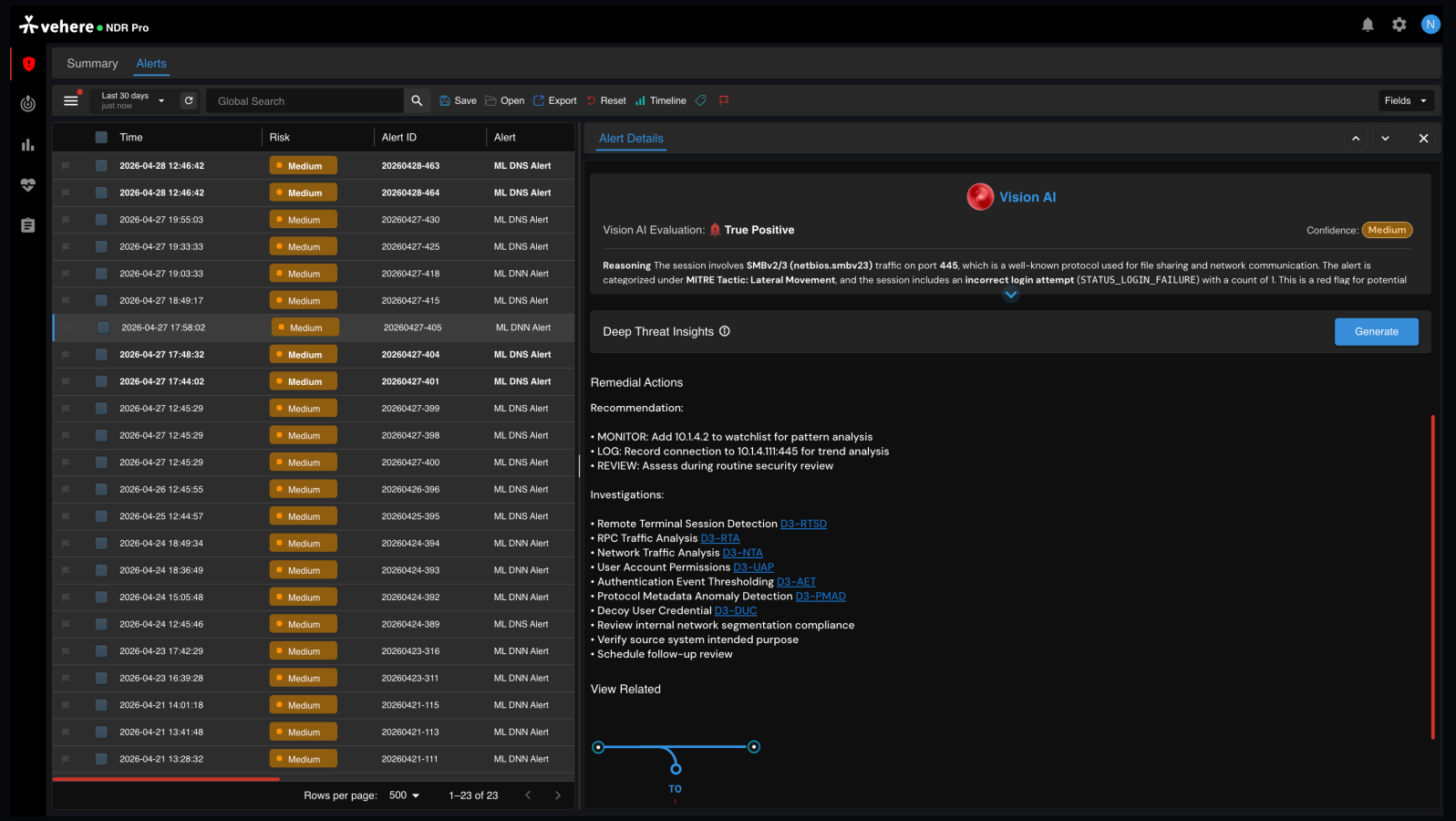
- Integrated **dynamic file analysis** for isolation, inspection and detonation of suspicious payloads
- Automated response actions to contain threats in real-time



Response

AI-Powered Response

- AI-powered TP and FP detection
- Confidence-based Alert Verdicts
- Auto whitelisting of high-confidence FP
- MITRE D3FEND framework mapped response recommendations
- Seamless SIEM, SOAR integrations via API



VEHERE

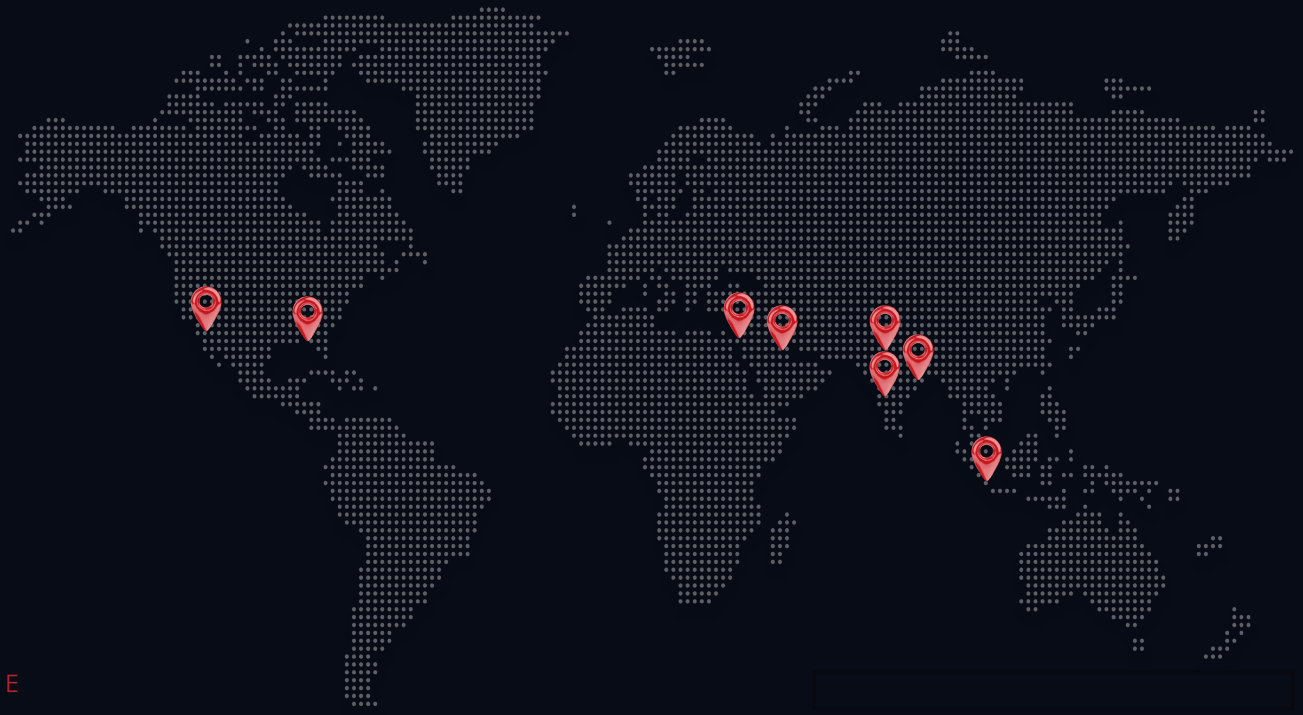
Vehere Presence & Vision

Vision

To be the world’s most admired cyber defense innovator, empowering nations to safeguard sovereignty and enterprises to stay resilient

Global Presence

- California
- Dallas
- Singapore
- Dubai
- Riyadh
- New Delhi
- Mumbai
- Bengaluru
- Kolkata



8+
Patents

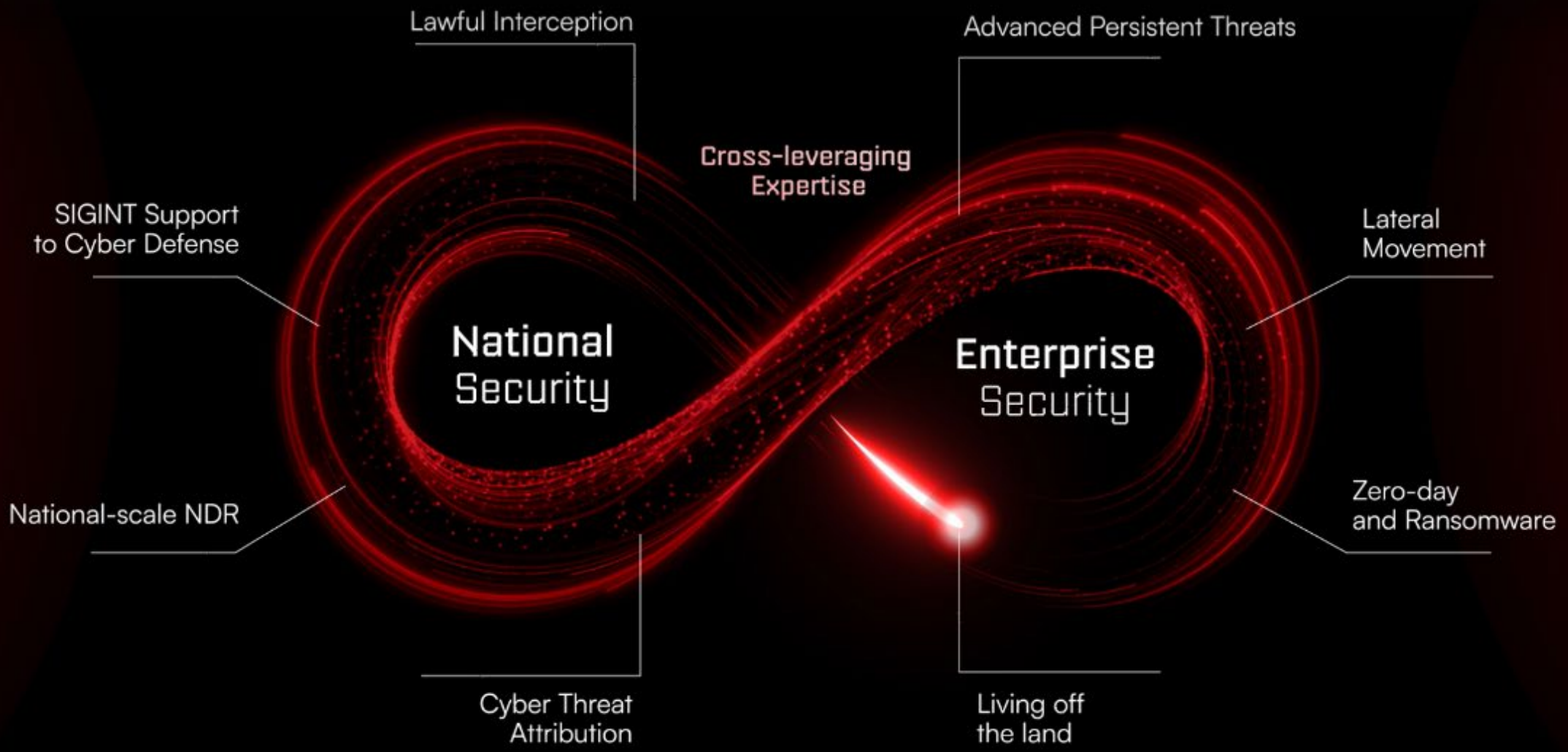
~200
Headcount

100%
Retention Rate

38%
Projected CAGR

VEHERE

Cybersecurity Deep Tech That Protects Nations, now ready for the Enterprise



Buying Options

Buying Option 1

VEHERE NDR

Powered by Vision AI

Detect, Alert, Analyze, Hunt

WHEN IT FITS

- ✓ Primary need is real-time threat detection and AI-powered threat hunting
- ✓ Known and unknown threat detection with precision
- ✓ L2–L7 visibility across 5,000+ protocols with metadata extraction
- ✓ Continuous visibility into network, devices and users

Customer gets:

- AI-powered Network threat detection and Alerting
- 35000+ rules for Rule-based Detection of known threats and IDS, ML-based Detection for novel threats
- Behavioral Analytics and Anomaly Detection

+

Buying Option 2

FULL PACKET CAPTURE

Powered by Vision AI

Capture, Store, Investigate

WHEN IT FITS

- ✓ Customer needs packet visibility and retention without a full detection stack
- ✓ SOC already has detection tools (SIEM, EDR) but lacks forensic evidence and session reconstruction
- ✓ Compliance mandates for PCAP and long-term metadata retention
- ✓ Deep network visibility for incident response and root cause analysis

Customer gets:

- 10G Full Packet Capture and Long-Term Storage
- Session Reconstruction, Patent-pending Micro-second Search and Custom Reports
- Application Visibility, Traffic Analytics and Link Analysis

=

Buying Option 3

4-IN-1

VEHERE NDR PRO

Powered by Vision AI

NDR + Full Packet Capture

WHEN IT FITS

- ✓ Customer requires real-time AI-powered threat detection and continuous full packet capture
- ✓ Full-packet forensic evidence for rapid investigations
- ✓ Unified platform for threat detection, hunting, forensics and guided response
- ✓ Integrated IDS and lightweight dynamic file analysis without additional tools

Customer gets:

- Complete NDR and Full Packet Capture
- Native IDS and On-demand Dynamic File Analysis
- Vision AI full capability with multi-agent threat intelligence

Feature Comparison in each offering

CAPABILITY	NDR	FPC	NDR PRO
Packet Capture at 10G	INCLUDED	INCLUDED	All-Inclusive
HA Probes	INCLUDED	INCLUDED	✓
Rule based Threat Detection	INCLUDED	NOT INCLUDED	✓
ML-based Threat Detection	INCLUDED	NOT INCLUDED	✓
Raw Packet Storage	NOT INCLUDED	INCLUDED	✓
Threat Hunting	NOT INCLUDED	INCLUDED	✓
Forensics	NOT INCLUDED	INCLUDED	✓
IDS-based Rules	INCLUDED	NOT INCLUDED	✓
Alerting Dashboard	INCLUDED	NOT INCLUDED	✓
Application Visibility	NOT INCLUDED	INCLUDED	✓
Device Profiling	INCLUDED	INCLUDED	✓
Analytics Dashboard	NOT INCLUDED	INCLUDED	✓
Data Grid	INCLUDED	INCLUDED	✓
Link Analysis	NOT INCLUDED	INCLUDED	✓
Session Reconstruction	NOT INCLUDED	INCLUDED	✓
Advanced Search	NOT INCLUDED	INCLUDED	✓
Reports	NOT INCLUDED	INCLUDED	✓

ANY QUESTIONS? CONTACT US!

sales@adeon.international