



Vehere Network Detection and Response (NDR)

ADEN



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

Financial
Institutions

Top 10

Global Telecom
companies

Top 3

Smart Cities

Vehere Customer's

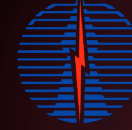


Government
and Public
Sector



रक्षा मंत्रालय
MINISTRY OF
DEFENCE

सत्यमेव जयते



पावरग्रिड
POWERGRID



MIDDLE EAST
INTELLIGENCE



Telecom and
Network
Providers



TATA COMMUNICATIONS



AT&T

verizon

orange™



Cloud, Data &
IT Services



sify



lightstorm



GLOBAL
CLOUD
XCHANGE
A RELIANCE COMPANY



Banking and
Financial
Institutions



ਪੰਜ ਅਤੇ ਸਿੰਧ ਬੈਂਕ
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

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

Hackers are logging in,
not breaking in

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*

SOC Teams are
overwhelmed

EDR has blind spots

**Threat actors bypass,
blind or disable EDR**

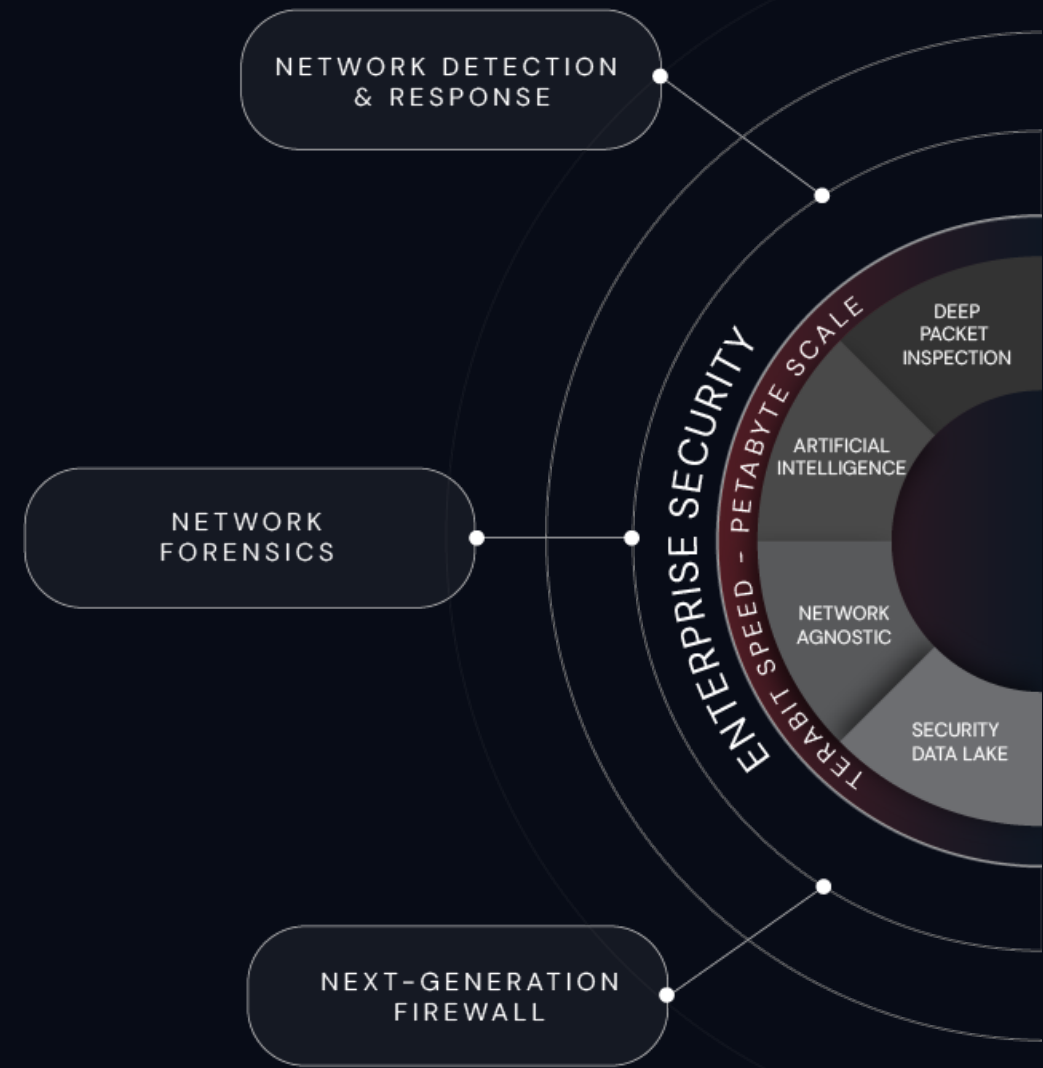
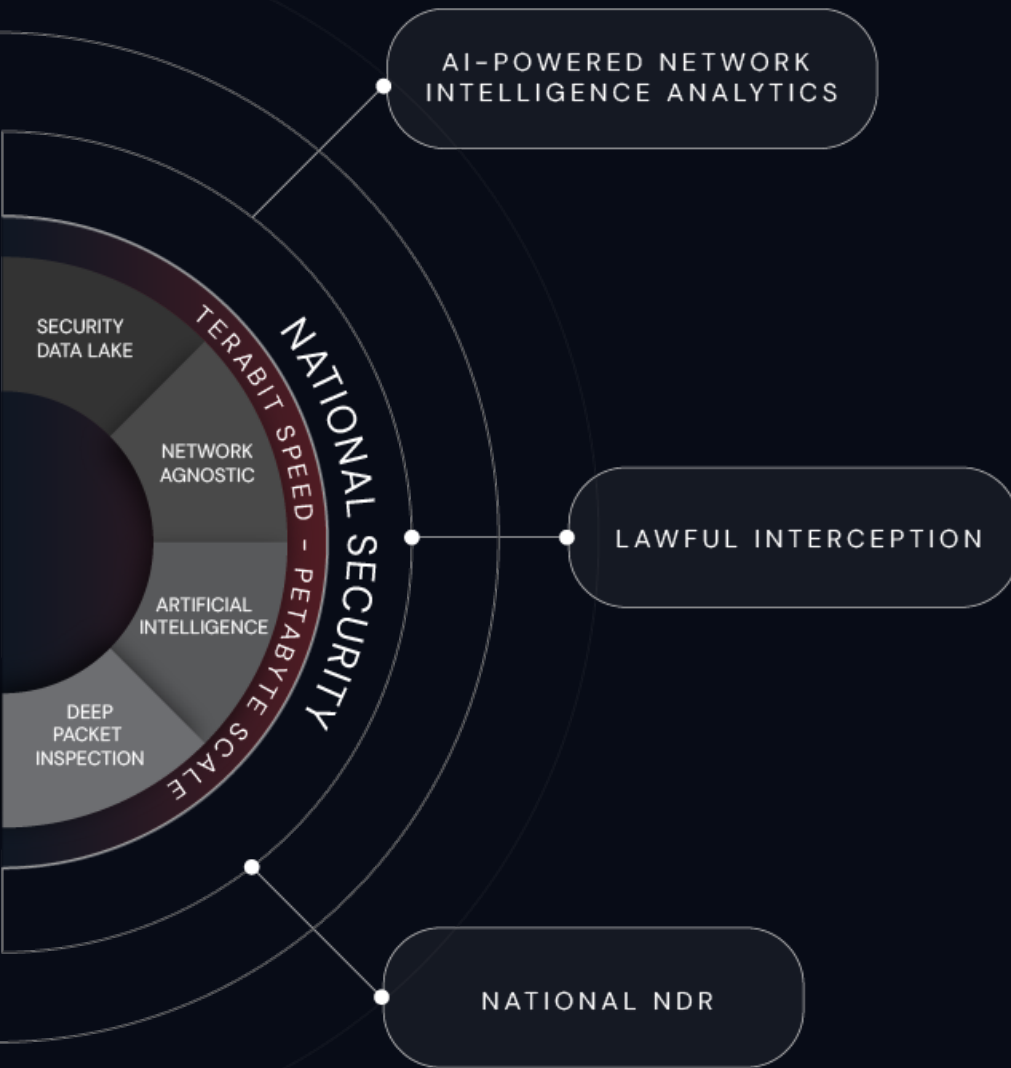
*Attackers disable (turn the sensor off),
reconfigure (change settings to prevent
sensor from detecting), bypass (choose
techniques that don't get flagged)*

**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*

Traditional Detection
and Response is failing

Vehere Product Offerings



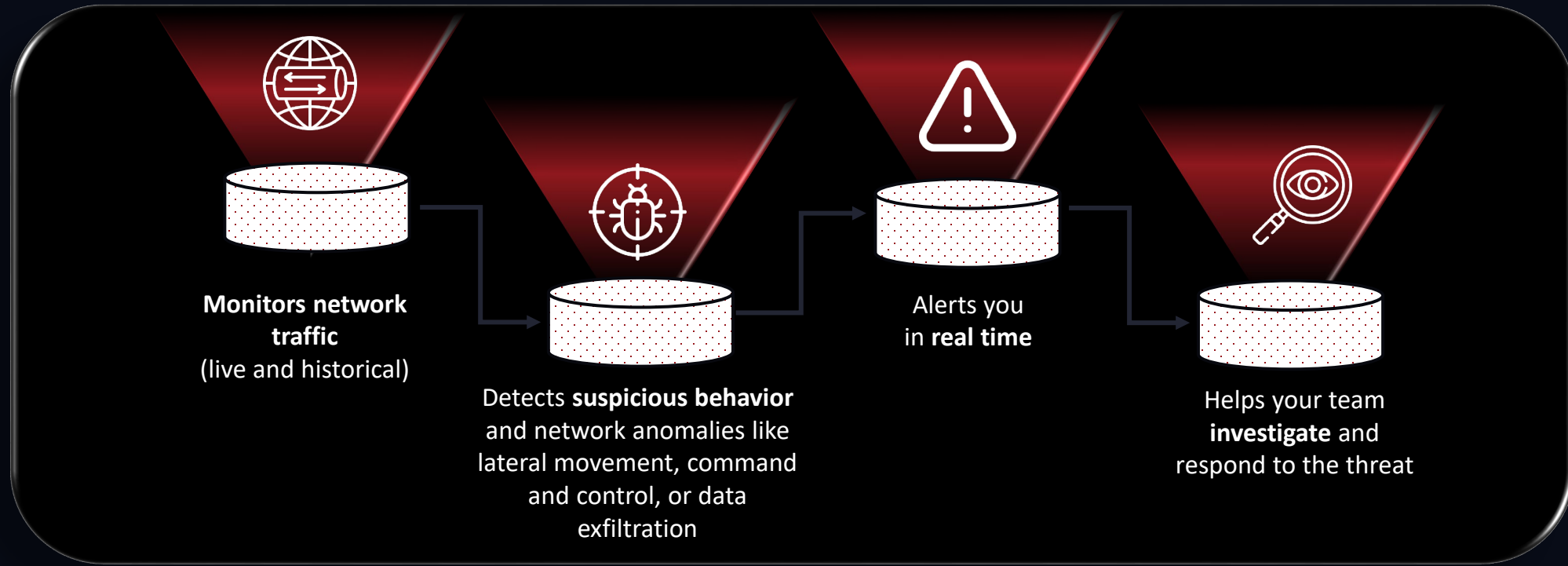
What's an NDR

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 ”

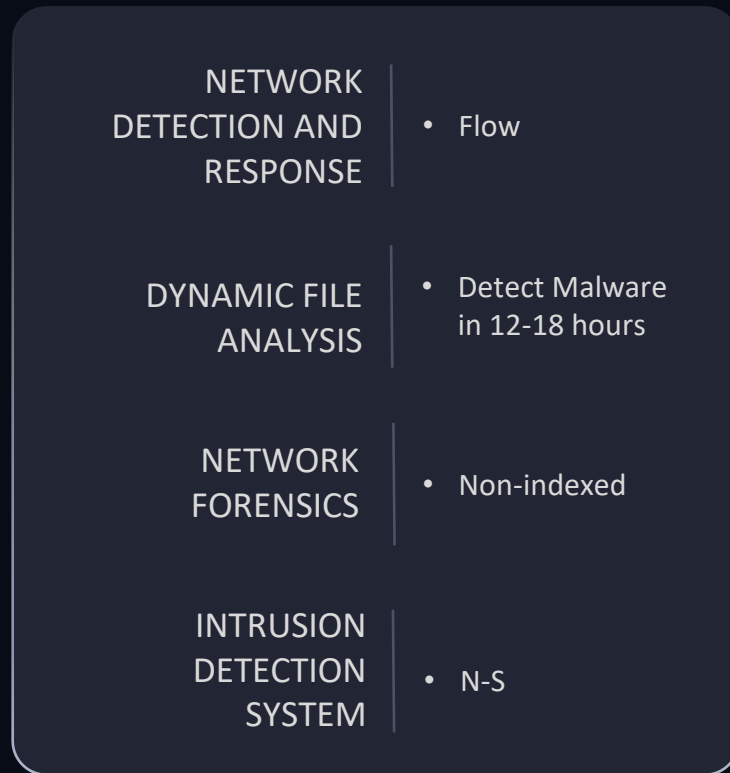
”



The Vehere NDR Approach

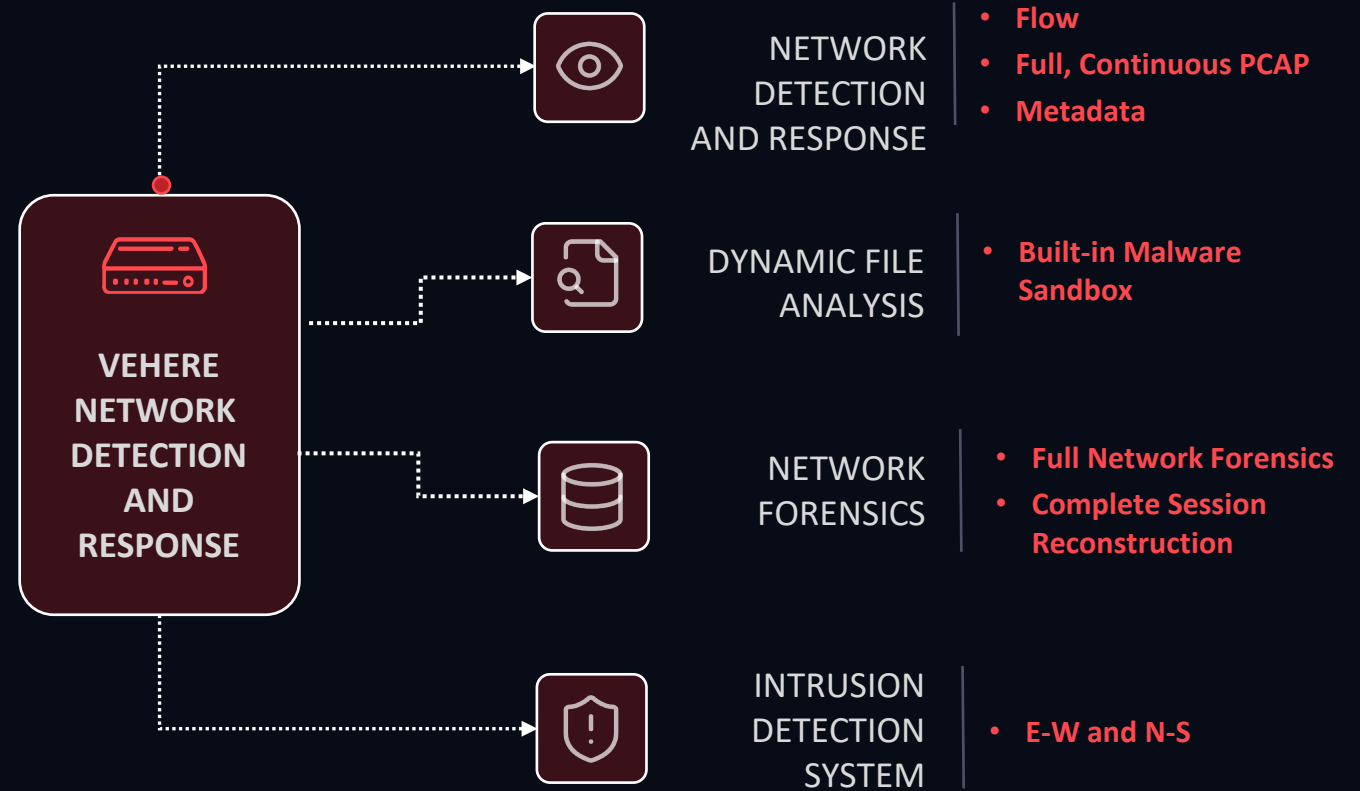
TRADITIONAL:

4 NETWORK SECURITY TECHNOLOGIES



THE SECOND LINE OF DEFENSE

"ONE" GEN-NEXT TECHNOLOGY INSTEAD OF 4



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.

Multi-Agentic AI – Interpret, Analyze, Respond

Alert Details

42
Medium
Risk

ML DNN Alert

22nd Apr, 2026 10:15:17

Category

Lateral Movement

Description

Lateral Movement refers to techniques used by attac compromised network, spreading their access and cc accounts.

Alert ID

20260422-32073

Type

ML Behaviour Anomaly

Status

Open

Rationale

There are 1 sessions for +/- 30 mins of 2026-04-22 10:02:07:751

Indicators:

Internal Scanning: Scan of internal lateral movement port 445

Remote Service: SMB/CIFS access detected, commonly used for lateral movement

Admin Protocol: Administrative protocol detected (netbios), Connection to administrative service SMB (port 445)

Deep Threat Insights

Threat Intelligence Summary: Lateral Movement via NetBIOS/SMB

1. Key Findings

Lateral movement is being executed using NetBIOS over SMB (Server Message Block) to access the CS administrative share, a common Windows administrative share.

Unusual NetBIOS traffic involving Tree Connect AndX and Write AndX commands has been observed, indicating potential exploitation or data exfiltration.

Mimikatz (or a variant named mimikatz43036.exe) is being used over SMB, suggesting credential dumping or pass-the-hash attacks.

Unusual MIMIKATZ calls with unknown opnum in SMB Write AndX commands suggest custom or unknown payloads being executed.

A high-payload NetBIOS session to an internal IP (192.168.14.147) is observed, indicating potential lateral movement or data transfer between compromised hosts.

2. Attack Patterns

Initial Compromise -> Credential Theft (via Mimikatz or similar tools) -> Pass-the-Hash/Token -> SMB-based Lateral Movement -> File or Command Execution via SMB -> Data Exfiltration or Persistence Setup

Attackers use NetBIOS over SMB to access remote systems without triggering traditional authentication logs.

Administrative shares (e.g., C\$, ADMIN\$) are exploited to execute payloads or move laterally.

MIMIKATZ over SMB is used to execute remote code or manipulate services, often with unknown or obfuscated opnums to evade detection.

3. Indicators of Compromise (IOCs)

File IOC: mimikatz43036.exe

Network IOC:

Unusual NetBIOS traffic with Tree Connect AndX and Write AndX commands

High-payload NetBIOS sessions to internal IPs (e.g., 192.168.14.147)

MIMIKATZ unknown opnums in SMB Write AndX

Behavioral IOC:

Lateral movement via SMB to CS share

SMB-based file writes or command execution on remote hosts

Automated Whitelisting

AI Agent took an Automated Action against this alert & created a whitelist.

Summary

Alerts

Global Search

Save

Open

Export

Reset

Timeline

Time	Risk	Alert ID	Alert	Src IP	Alert Type	Alert Category	Vision AI Evaluation
2026-04-28 12:46:42	Medium	20260428-463	ML DNS Alert	192.168.2.158	ML Behaviour Anomaly	Command & Control	-
2026-04-28 12:46:42	Medium	20260428-464	ML DNS Alert	fe80::4edc:e0a2:5bcb:f2f4	ML Behaviour Anomaly	Command & Control	-
2026-04-27 19:55:03	Medium	20260427-430	ML DNS Alert	10.1.4.133	ML Behaviour Anomaly	Command & Control	-
2026-04-27 19:33:33	Medium	20260427-425	ML DNS Alert	10.1.4.25	ML Behaviour Anomaly	Command & Control	-
2026-04-27 19:03:33	Medium	20260427-418	ML DNN Alert	45.10.11.1	ML Behaviour Anomaly	Command & Control	True Positive
2026-04-27 18:49:17	Medium	20260427-415	ML DNS Alert	192.168.2.174	ML Behaviour Anomaly	Command & Control	-
2026-04-27 17:58:02	Medium	20260427-405	ML DNN Alert	10.1.4.2	ML Behaviour Anomaly	Lateral Movement	True Positive
2026-04-27 17:48:32	Medium	20260427-404	ML DNS Alert	192.168.2.149	ML Behaviour Anomaly	Command & Control	-
2026-04-27 17:44:02	Medium	20260427-401	ML DNS Alert	10.1.4.81	ML Behaviour Anomaly	Command & Control	-
2026-04-27 19:45:24	Medium	20260427-394	ML DNS Alert	fe80::a5f51d44c9c8a18185618	ML Behaviour Anomaly	Command & Control	-

AI Agent took an Automated Action against this alert & created a whitelist.

Classification: False Positive

Confidence: High

Reasoning: The network session in question involves a NetBIOS/SMBv1 traffic exchange over UDP port 138 from a local host (deepsankar-shattacharya-Latitude-7658.local) to the broadcast address 192.168.2.255. This is a normal behavior for NetBIOS over TCP/IP (NB1), where systems broadcast information for network discovery and file sharing on a local LAN.

Key Indicators that this is benign:

Destination IP is a broadcast address, which is common for NetBIOS announcements.

All traffic is sent by the source (0 packets transmitted, 0 received), which aligns with a broadcast message pattern.

No server-side response or interaction indicates this is likely a network discovery or announcement, not a malicious command or control attempt.

DPI protocol is identified as netbios, and while NetBIOS is considered insecure, the context here is internal network broadcast, not a connection to an external or suspicious host.

Historical context shows consistent behavior, with similar sessions occurring in the +30 minute window and no anomalies in port usage or traffic timing.

Client Entropy is high, which could indicate complex or structured traffic (e.g., protocol-specific data), but it does not indicate malicious behavior in this case.

MITRE Tactic is "Persistence", which typically refers to techniques like backdoors or scheduled tasks, but this session lacks any evidence of persistence or malicious payload.

Key Factors:

Traffic is sent to the broadcast address (192.168.2.255), typical for NetBIOS announcements.

No server response or data received, indicating a one-way broadcast.

Protocol is NetBIOS/SMBv1 over UDP port 138, a known standard for LAN discovery.

Host is internal and identified by a full domain name, indicating it is a legitimate workstation.

Historical context shows this is a recurring pattern with no deviation in behavior.

Recommended Action Dismiss as a false positive. No further investigation is needed. Consider adding a whitelisting rule to suppress future alerts of this nature.

MITRE D3FEND Response Actions:

Not Applicable

Confidence Scoring

Impact

Persistence

Persistence

Command & Control

Command & Control

Lateral Movement

Response Action Recommendations

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

Platform Orchestration

INTEGRATION

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



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

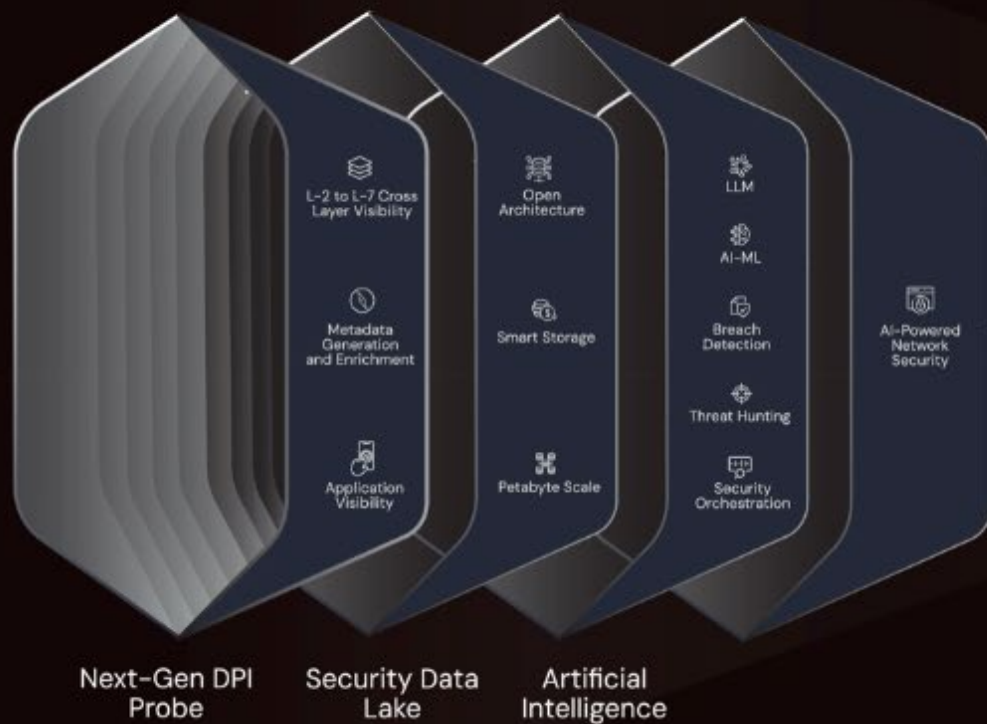
HUNT BEFORE BREACH™

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

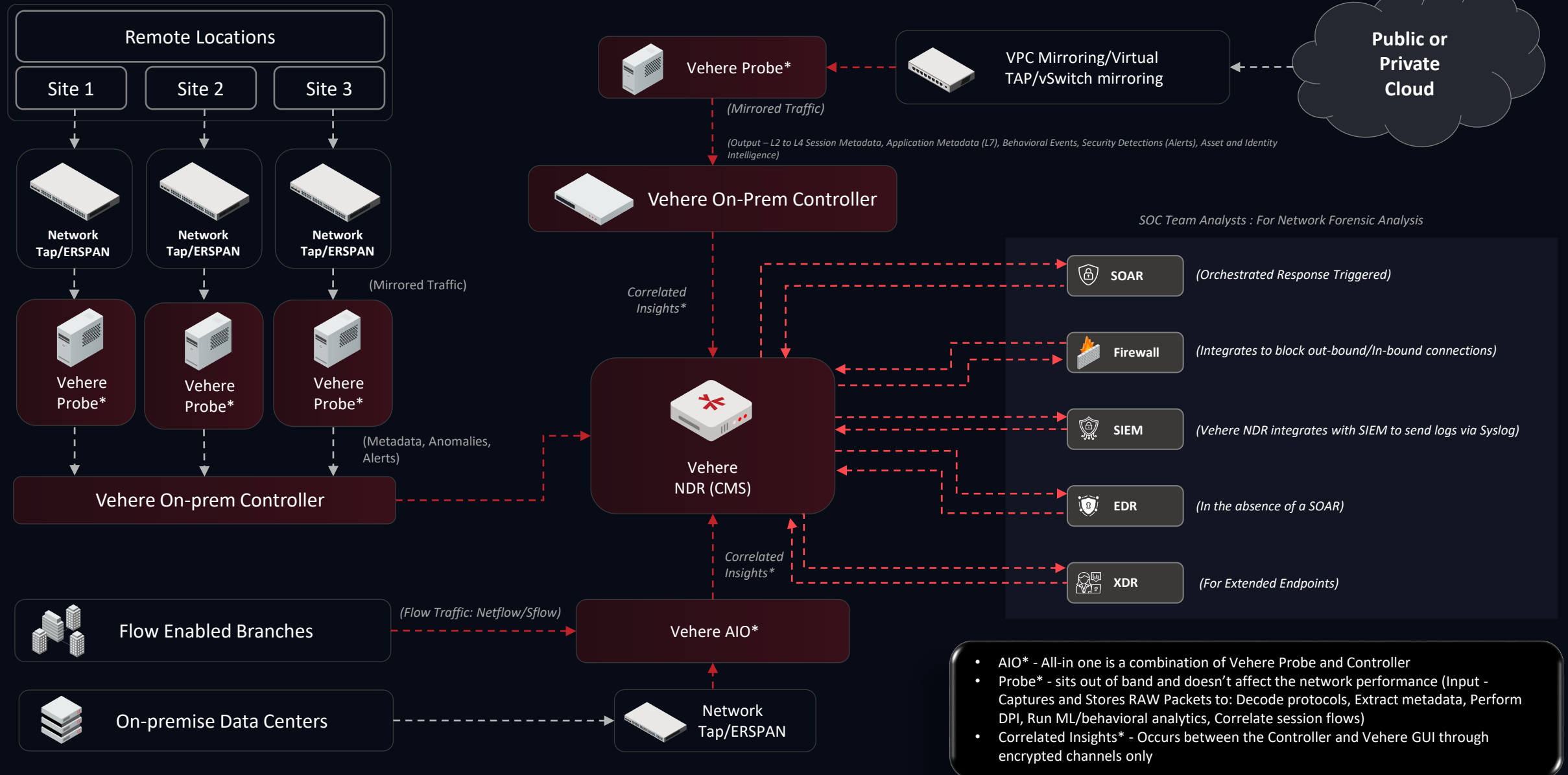
Hunt Threats at lightning
speed on terabit speed
traffic



EARLY WARNING

Identify patterns and
anomalies within petabyte-
scale, distributed data

Vehere Deployment Architecture



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

9
Low Risk

Ti10007 Blacklisted SSL-fingerprint

20th Nov, 2025 11:43:45 | 2

Category: Reconnaissance

Description: This rule is used for detection of ja3 fingerprint taken over SSL fields of SSL certificate seen in malicious traffic. JA3 with JA3S is a method to fingerprint the TLS negotiation between client and server. This combined fingerprinting can assist in producing higher fidelity identification of the encrypted communication between a specific client and its server.

Alert ID: 20251120-293761

Type: Malware/Attack

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

64
High Risk

ML DNN Alert

20th Nov, 2025 19:33:52

Category: Exfiltration

Description: Pre-exfiltration behaviors have been observed on a host that has received abnormally high amounts of data from one or more hosts within a short period of time.

Alert ID: 20251117-675180

Type: ML Behaviour Anomaly

Rationale

There are 1 sessions for +/- 30 mins of 2025-11-20 18:41:06.882

Current Session records data transfer of 597521676 bytes. Baseline data transfer for 10.1.3.197 is 698.71 bytes. Tolerance is 50%

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.

20
Low Risk

ML EBA Alert

20th Nov, 2025 19:38:17

Category: Behavioral Pattern Deviation

Description: Entity: 10.1.3.197 | Communication Partner: 10.1.3.7
Current Activity: 117 sessions | Historical Baseline: 14 +/- 0.1 sessions
Statistical Deviation: 8434.2% (elevated)
Risk Assessment: Statistical analysis indicates significant deviation from established baseline patterns.

Alert ID: 20251114-607792

Type: ML Behaviour Anomaly

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

Data Exfiltration (Impact Phase)

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

96
Critical Risk

ML DNN Alert

20th Nov, 2025 23:51:20

Category: Exfiltration

Description: Data exfiltration is defined as the unauthorized copying, transfer, or retrieval of data from either a server or an individual's computer. It's a type of security breach that occurs when individual or company data is illicitly copied, transferred, or retrieved from a device or server without proper authorization, often with malicious intent.

Alert ID: 20251117-675179

Type: ML Behaviour Anomaly

Rationale

There are 2 sessions for +/- 30 mins of 2025-11-20 23:03:26.941

Indicators:
• Large Outbound: Large outbound data transfer (105.63 MB)

Current Session records data transfer of 110449065 bytes. Baseline data transfer for 10.1.3.42 is 250.24 bytes. Tolerance is 50%

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

Data Exfiltration (Preparation Phase)

Attacker connected with c2 channels for exfiltration of data

20
Low Risk

ML EBA Alert

20th Nov, 2025 22:45:14

Category: Behavioral Pattern Deviation

Description: Entity: 10.1.3.197 | Analysis Period: 21:00 hours
Current Activity: 373 sessions | Historical Baseline: 31.4 +/- 0.2 sessions
Statistical Deviation: 1087.4% (elevated)
Risk Assessment: Statistical analysis indicates significant deviation from established baseline patterns.

Alert ID: 20251119-675406

Type: ML Behaviour Anomaly

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

Lateral Movement and Credential Theft

Attacker escalated privileges and gained broader access within the network

42
Medium Risk

ML DNN Alert

20th Nov, 2025 20:29:36

Category: Lateral Movement

Description: Lateral Movement refers to techniques used by attackers to move laterally within a compromised network, spreading their access and control to other systems or accounts.

Alert ID: 20251118-675320

Type: ML Behaviour Anomaly

Rationale

There are 6 sessions for +/- 30 mins of 2025-11-20 20:02:06.691

Indicators:
• Internal Scanning: Scan of internal lateral movement port 139
• Admin Protocol: Connection to administrative service NetBios (port 139)

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

Dashboards

Security Posture at-a-glance

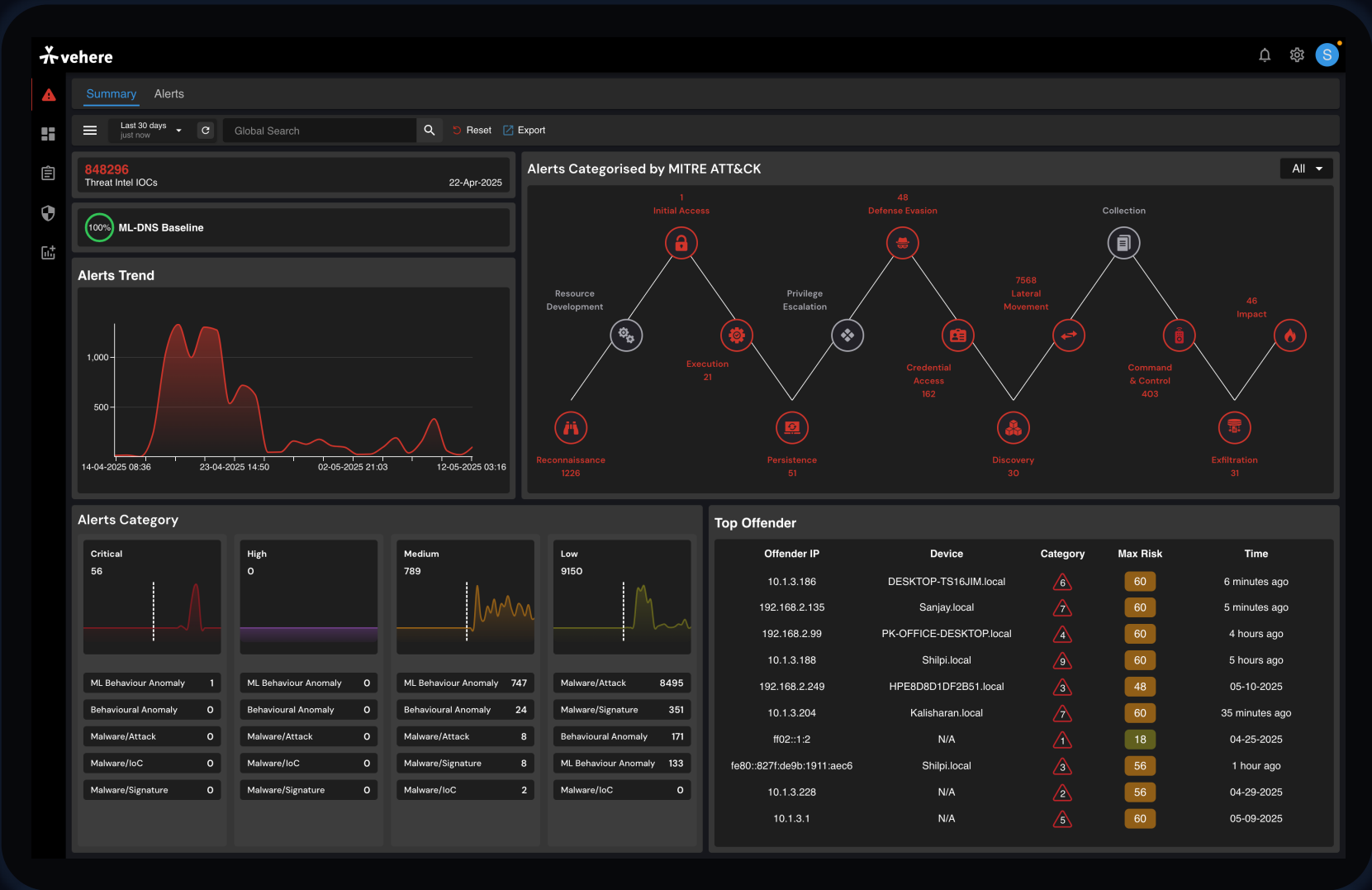
- Centralized Network Visibility
- Behavioral Analysis and Anomaly Detection
- Contextualized Threat Insights and Alerting
- Deep Protocol and Application Awareness
- Rapid drill-down into sessions, payloads and network interactions
- Network Usage Trends (traffic patterns, application usage etc.)



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

The screenshot displays the VeHERE network analysis tool interface. The main window is titled 'Data Grid' and shows a list of network sessions. The columns include Time, Src IP, Dest IP, Src Host, and Dest. The sessions are sorted by time, showing a range of activity from 2025-05-12 15:42:20 to 15:42:26. The sessions involve various hosts, including 'veherelaptop.local', 'DESKTOP-NCUUMIK.local', 'ghost.local', 'Kalisharan.local', 'Saugata.local', 'veherelaptop.local', 'DESK', 'papi.local', 'Sobha', 'Kalisharan.local', 'Saugata.local', '684b9e8a-adfb-4dbd-896e-c288df', 'DESKTOP-TS16JIM.local', 'DESKTOP-3341FR9.local', 'sommath-Pc.local', 'Neha-Saha.local', 'DESKTOP-NCUUMIK.local', and 'Veherelaptop.local'. The destinations include 'Sanjay', 'Sanja', 'reddit', 'veher', 'dns.g', 'DESK', 'Sobha', 'Saugata', 'Kalish', 'arrayt', 'somm', 'DESK', 'veher', 'DESK', and 'youtu'.

On the right side, a 'Details' panel is open, showing a summary of the selected session. The summary includes fields such as _id, @timestamp, @version, datalink.dst_eth, datalink.dst_eth_resolved, datalink.dst_vlan_ids, datalink.eth_protocol, datalink.eth_type, datalink.frame_type, datalink.src_eth, datalink.src_eth_resolved, datalink.src_vlan_ids, endpoints_swapped_with_confidence, network.detected_names, network.do_not_frag, network.dst_host, network.dst_ip, network.ip_addresses, network.ip_protocol, network.ip_version, network.protocol, network.src_device_address, network.src_device_uid, network.src_host, network.src_ip, network.src_ttl, network.transport_protocol_num, session.app_group, and session.application. The values for these fields are displayed in a structured format.

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

The screenshot displays the Vehera Threat Investigation interface. The main panel shows a list of alerts with columns for Time, Risk, Alert ID, Alert, and Source. The alerts are sorted by time, showing a sequence of events from 5 Feb 2021, 12:47 PM to 5 Feb 2021, 13:04 PM. The risk levels vary, with several 'Critical' alerts. The right panel provides a detailed view of a specific alert, 'TII3091 ICMP Oversized Packet', which is categorized as 'Initial Access' and 'Malware/Attack'. It includes client and server network details, such as IP addresses, ports, and applications. The interface also features a 'MITRE Techniques' section, showing 'T1498 - Network Denial of Service', and a 'Response' section with a detailed description of the threat. A 'View Related' section at the bottom shows a timeline of related events, including 'Exfiltration' and 'Session Alert'.

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	192.168.2.190
5 Feb 2021, 12:57 PM	Medium	20241126-11027	ML DNN Notification	192.168.2.191
5 Feb 2021, 12:58 PM	Low	20241126-11028	ML DNN Warning	192.168.2.192
5 Feb 2021, 12:59 PM	Critical	20241126-11029	ML DNN Error	192.168.2.193
5 Feb 2021, 13:00 PM	High	20241126-11030	ML DNN Alert	192.168.2.194
5 Feb 2021, 13:01 PM	Medium	20241126-11031	ML DNN Notification	192.168.2.195
5 Feb 2021, 13:02 PM	Low	20241126-11032	ML DNN Warning	192.168.2.196
5 Feb 2021, 13:03 PM	Critical	20241126-11033	ML DNN Error	192.168.2.197
5 Feb 2021, 13:04 PM	High	20241126-11034	ML DNN Alert	192.168.2.198

Hunting

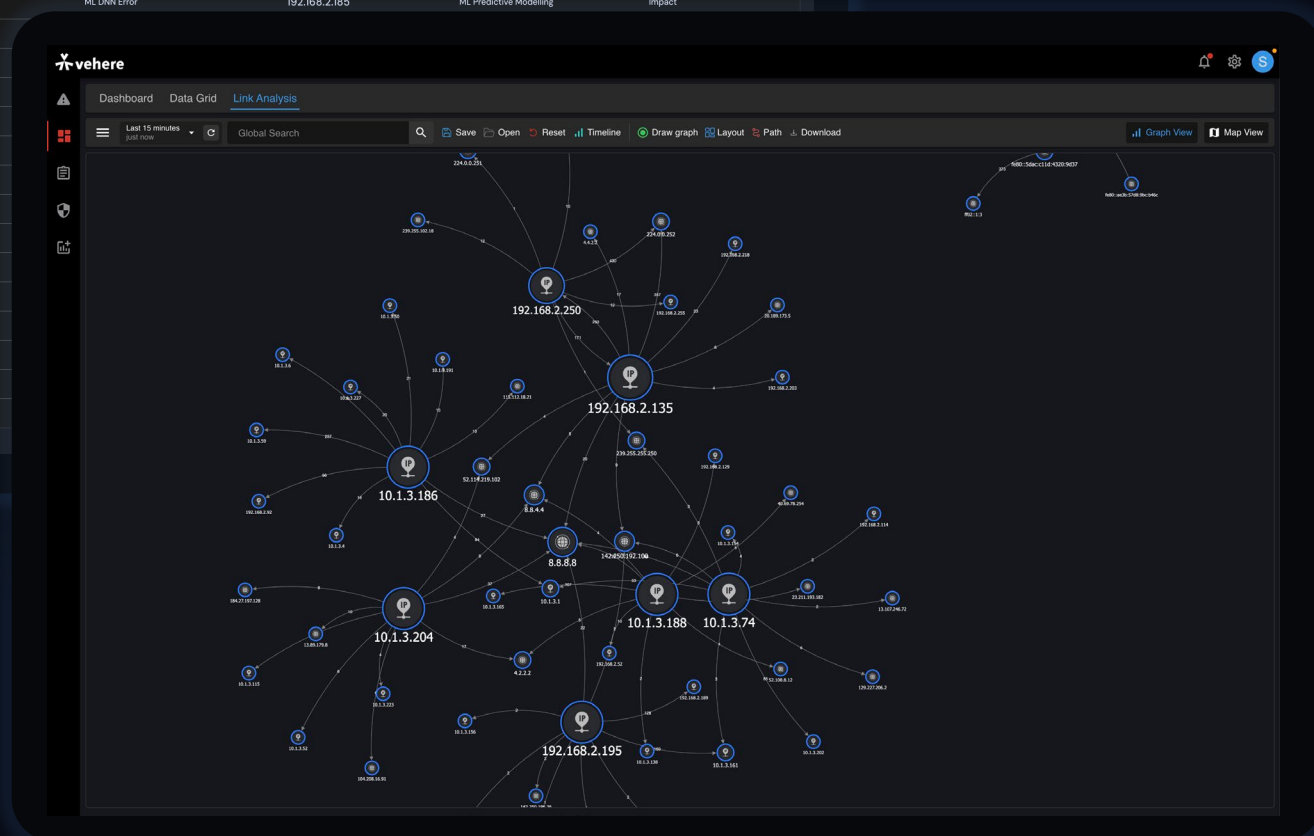
Threat Hunting:

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

Summary Alerts

Last 20 days just now Search Archive Analytics Save Open Export Reset Read/Unread

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



Containment

Threat Containment:

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

Summary

Alerts

Last 30 days

just now

Global Search

Save

Open

Export

Reset

Timeline

Fields

Time	Risk	Alert ID	Alert
2025-05-02 17:35:44	Critical	20250502-9197	On-Demand Scan Malware Analysis
2025-05-02 17:33:29	Critical	20250502-9196	On-Demand Scan Malware Analysis
2025-05-02 17:29:59	Critical	20250502-9193	On-Demand Scan Malware Analysis
2025-05-02 15:21:42	Critical	20250502-9173	On-Demand Scan Malware Analysis
2025-05-02 15:19:41	Critical	20250502-9171	On-Demand Scan Malware Analysis
2025-05-02 15:10:41	Critical	20250502-9169	On-Demand Scan Malware Analysis
2025-05-02 14:47:26	Critical	20250502-9166	On-Demand Scan Malware Analysis
2025-05-02 14:45:41	Critical	20250502-9165	On-Demand Scan Malware Analysis
2025-05-02 14:41:41	Critical	20250502-9163	On-Demand Scan Malware Analysis
2025-05-02 14:29:10	Critical	20250502-9161	On-Demand Scan Malware Analysis
2025-05-02 13:16:39	Critical	20250502-9156	On-Demand Scan Malware Analysis
2025-05-02 13:08:54	Critical	20250502-9155	On-Demand Scan Malware Analysis
2025-05-02 13:05:54	Critical	20250502-9153	On-Demand Scan Malware Analysis
2025-05-02 12:56:54	Critical	20250502-9151	On-Demand Scan Malware Analysis
2025-05-02 12:54:08	Critical	20250502-9149	On-Demand Scan Malware Analysis
2025-05-02 12:51:08	Critical	20250502-9148	On-Demand Scan Malware Analysis
2025-05-02 12:48:38	Critical	20250502-9145	On-Demand Scan Malware Analysis
2025-05-02 12:46:38	Critical	20250502-9143	On-Demand Scan Malware Analysis
2025-05-02 12:39:08	Critical	20250502-9137	On-Demand Scan Malware Analysis
2025-05-02 12:37:23	Critical	20250502-9135	On-Demand Scan Malware Analysis
2025-04-30 12:48:02	Critical	20250430-8870	On-Demand Scan Malware Analysis
2025-04-30 12:46:02	Critical	20250430-8869	On-Demand Scan Malware Analysis
2025-04-30 12:43:47	Critical	20250430-8868	On-Demand Scan Malware Analysis
2025-04-30 12:42:17	Critical	20250430-8866	On-Demand Scan Malware Analysis

Rows per page: 500 1-56 of 56

Alert Details

On-Demand Scan Malware Analysis Engine:Malicious File Detected 2nd May, 2025 17:35:44

95 Critical Risk

Category Generic Malware Behavior Description Alerts are generated based on the On-Demand Scan Malware Analysis Engine file analysis system

Alert ID 20250502-9197

Type Malicious

Client Network

Source IP 192.168.89.1 Active Scan

Source Host N/A Source Port 47474

Session Protocol http DPI Protocol http:http

Client Entropy 27 Location -

Server Network

Destination IP 192.168.89.130 Active Scan

Destination Host N/A Destination Port 80

Session Protocol http DPI Protocol http:http

Server Entropy - Location -

View Session

Historical Communication

View Snapshot

Complete Scan Report

Show Concise Report

Name 142c26841ab78721fe536275afe5e896e59586098da87936f1df7e31ee8c7af1.Exe

MD5 7794804bca68949a94f47cf09bf72bc9

Size 490.18 KB

Status Malicious

Type Generic Malware Behavior

Engine On-Demand Scan Malware Analysis Engine

File System

702 Events

Process

1 Events

Registry

248 Events

Network

0 Events

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

The screenshot displays the Vehera NDR Pro interface. On the left, a table lists alerts with columns for Time, Risk, Alert ID, and Alert. The table shows 23 rows of alerts, all with a 'Medium' risk level. The right panel shows the 'Alert Details' for a selected alert (ID 20260427-405). It includes a 'Vision AI' evaluation section with a 'True Positive' verdict and a 'Confidence: Medium' label. Below this, the 'Reasoning' section explains the alert is categorized under MITRE Tactic: Lateral Movement and includes an incorrect login attempt. The 'Deep Threat Insights' section has a 'Generate' button. The 'Remedial Actions' section lists recommendations: MONITOR (Add 10.1.4.2 to watchlist), LOG (Record connection to 10.1.4.11), and REVIEW (Assess during routine security review). The 'Investigations' section lists various detection rules like D3-RTSD, D3-RTA, D3-NTA, D3-UAP, D3-AET, D3-PMAD, D3-DUC, and D3-PMAD. The 'View Related' section shows a timeline view.

Time	Risk	Alert ID	Alert
2026-04-28 12:46:42	Medium	20260428-463	ML DNS Alert
2026-04-28 12:46:42	Medium	20260428-464	ML DNS Alert
2026-04-27 19:55:03	Medium	20260427-430	ML DNS Alert
2026-04-27 19:33:33	Medium	20260427-425	ML DNS Alert
2026-04-27 19:03:33	Medium	20260427-418	ML DNN Alert
2026-04-27 18:49:17	Medium	20260427-415	ML DNS Alert
2026-04-27 17:58:02	Medium	20260427-405	ML DNN Alert
2026-04-27 17:48:32	Medium	20260427-404	ML DNS Alert
2026-04-27 17:44:02	Medium	20260427-401	ML DNS Alert
2026-04-27 12:45:29	Medium	20260427-399	ML DNS Alert
2026-04-27 12:45:29	Medium	20260427-398	ML DNS Alert
2026-04-27 12:45:29	Medium	20260427-400	ML DNS Alert
2026-04-26 12:45:55	Medium	20260426-396	ML DNS Alert
2026-04-25 12:44:57	Medium	20260425-395	ML DNS Alert
2026-04-24 18:49:34	Medium	20260424-394	ML DNN Alert
2026-04-24 18:36:49	Medium	20260424-393	ML DNN Alert
2026-04-24 15:05:48	Medium	20260424-392	ML DNN Alert
2026-04-24 12:45:46	Medium	20260424-389	ML DNS Alert
2026-04-23 17:42:29	Medium	20260423-316	ML DNN Alert
2026-04-23 16:39:28	Medium	20260423-311	ML DNN Alert
2026-04-21 14:01:18	Medium	20260421-115	ML DNN Alert
2026-04-21 13:41:48	Medium	20260421-113	ML DNN Alert
2026-04-21 13:28:32	Medium	20260421-111	ML DNN Alert

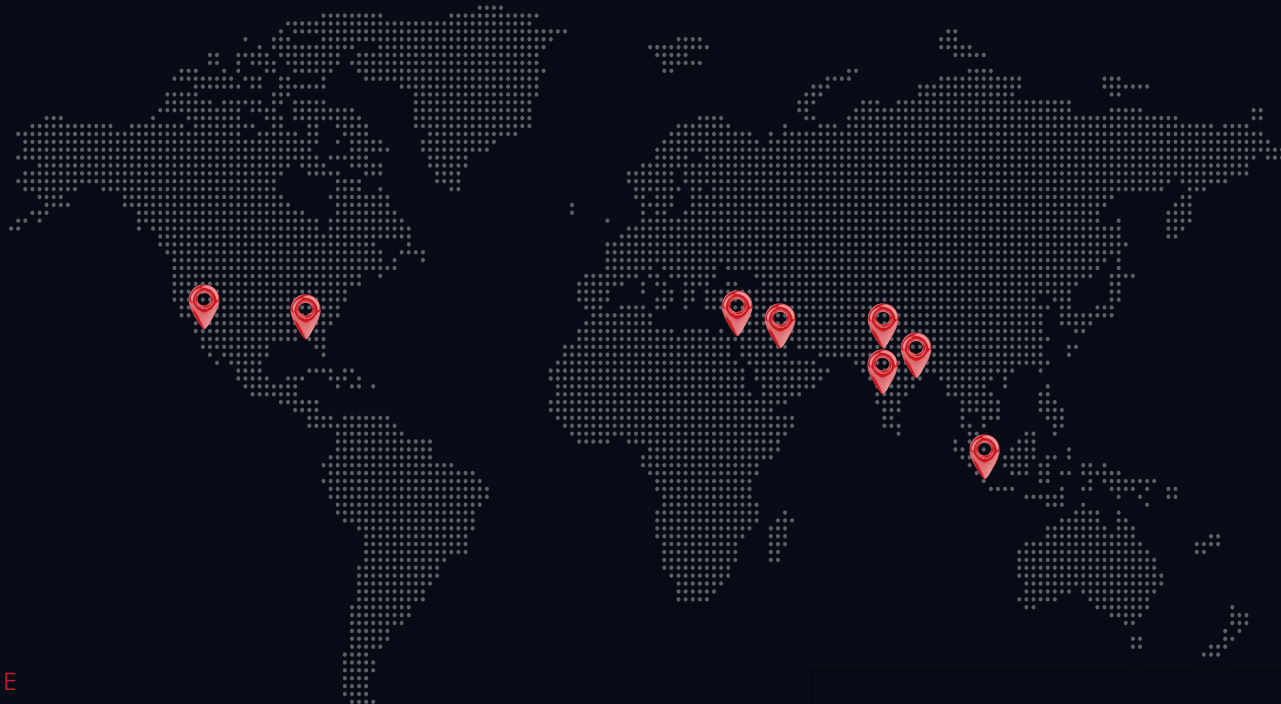
Vehere Presence & Vision

Vision

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

Global Presence

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



8+

Patents

~200

Headcount

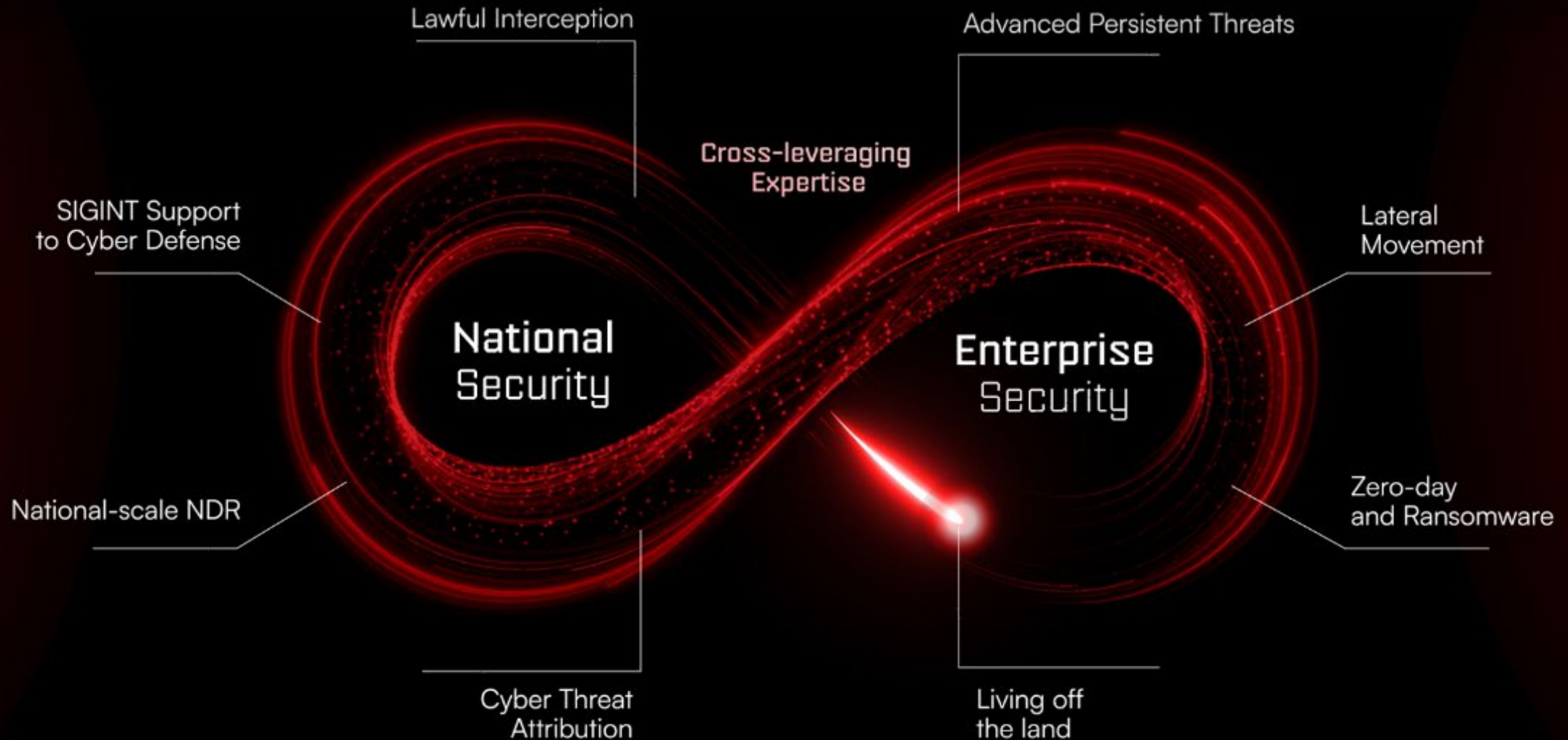
100%

Retention
Rate

38%

Projected
CAGR

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



Buying Options

Buying Option 1

VEHERE NDR

Detect, Alert, Analyze, Hunt

Powered by Vision AI

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

Capture, Store, Investigate

Powered by Vision AI

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

NDR + Full Packet Capture

Powered by Vision AI

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

ADEON