VECTRA

Key Findings from the Gartner Market Guide for Network Detection and Response

Market Guide for Network Detection and Response

29 March 2024 - ID G00784755 - 21 min read

By Jeremy D'Hoinne, Thomas Lintemuth, Nahim Fazal, Charanpal Bhogal

The network detection and response market continues to grow and expand to hybrid network scenarios with IaaS deployments. Security and risk management leaders should reposition NDR as a key provider of AI analytics in the context of more automated security operations assistants.

Overview

Key Findings

- Network detection and response (NDR) is commonly used as a complementary detection technology as part of a broader arsenal of security operations center (SOC) tools
- The emergence of "AI-augmented" analytics workflows, in the a useful source of insights for aggregated and summarized
- A handful of NDR vendors capture most of the attention in the more specialized detection use cases, these well-known shortlists.
- organizations narrowly automated responses past

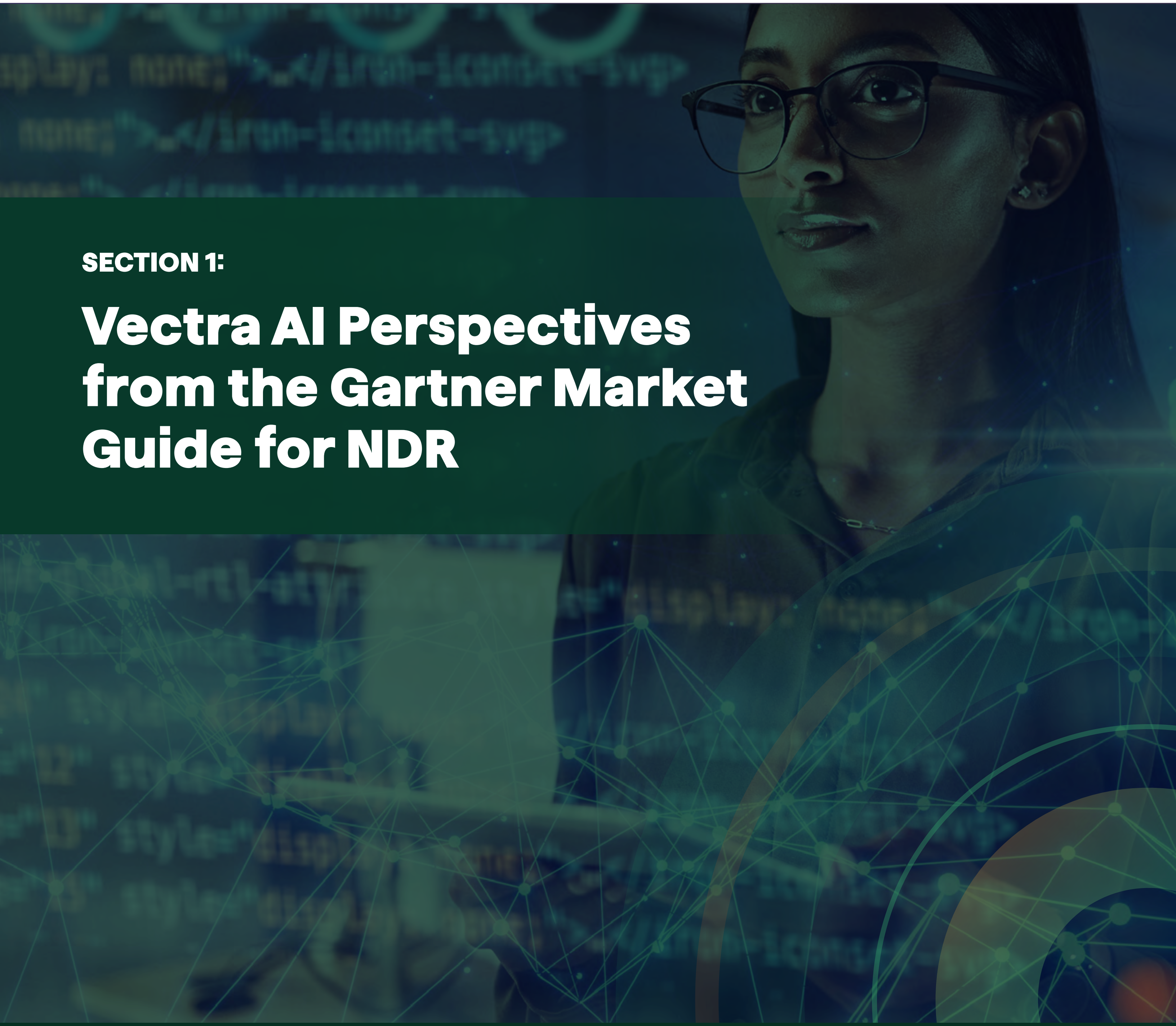
"The network detection and response market continues to grow and expand to hybrid network scenarios with IaaS deployments. Security and risk management leaders should reprioritize NDR as a key provider of AI analytics in the context of more automated security operation assistants."

Gartner Market Guide for Network Detection and Response,
Published 29 March 2024 - ID G00784755

We couldn't agree more.

Gartner is a trusted resource and advisor to who we are and what we do at Vectra AI. We see eye to eye with Gartner on many things, but not always everything. In this report, we share where we align to Gartner and where our perspectives differ when it comes to Network Detection and Response (NDR).

Table of contents



SECTION 1:

Vectra AI Perspectives from the Gartner Market Guide for NDR

- A NDR and XDR lines are blurring
- B NDR for Cloud is the future
- C NDR signal and response are critical
- D Aggregation of Incidents is a requirement
- E Decryption of network traffic is an optional capability
- F Where is identity in the NDR guide?

A NDR and XDR lines are blurring

Gartner: "Hybrid network NDR is the privileged evolution for stand-alone NDR providers (as) they expand their portfolio to cover new types of networks, often starting with operational technology (OT) and infrastructure as a service (IaaS)... NDR can contribute to XDR by bringing network event analytics into the mix. By continuing to add other sources of telemetry, such as endpoint and identity and access management (IAM) integrations, NDR could overlap more with the XDR market."†

XDR that starts with NDR. The Vectra AI Platform delivers comprehensive visibility across your data center, hybrid cloud, and IoT/OT networks, as well as network and cloud identities (human and machine), and IaaS, PaaS, and SaaS environments. Unlike XDR solutions that start with endpoint detection and response (EDR) and integrate NDR, the Vectra AI Platform starts with NDR and integrates EDR to deliver an extended detection and response (XDR) platform.

Vectra AI contends the benefit of an NDR-centric approach to XDR is that the network is the source of truth, the first line of defense when it comes to modern hybrid attacks, so start there.

B NDR for cloud is the future

Gartner: "As NDR providers "embed in their NDR products new detection techniques to support these (hybrid) use cases, the primary detection telemetry will still come from the analysis of network traffic patterns, but could expand beyond that by adding other types of detection, such as security posture anomalies for cloud infrastructure."

"For IaaS, NDR sensors are deployed closer to the server workloads, as most organizations now have server farms hosted on one or many of the IaaS platforms. Because the deployment constraints are different, NDR providers are more likely to leverage cloud-native flow analysis APIs and accept their limitations when compared to on-premises networks...For SaaS, NDR providers leverage SaaS APIs to monitor user connectivity to SaaS services, with Microsoft 365 being the most popular example."†

The Vectra AI Platform has already extended its native NDR capabilities to cover hybrid cloud networks. Vectra NDR for Cloud powered by Gigamon provides cloud network threat detection and response for AWS, Microsoft Azure and GCP IaaS environments.

Vectra AI does not accept the limitations of cloud-native flow analysis which is why we partnered with Gigamon to incorporate their telemetry into the Vectra AI Platform. By combining native Vectra NDR detections with Gigamon telemetry, the Vectra AI Platform provides visibility to threats for both on-premises data center networks and cloud IaaS networks in a single NDR solution.

C NDR signal and response is critical

Gartner: NDR (must) provide detection based on behavioral techniques (non-signature-based detection), including machine learning (ML) and advanced analytics that detect network anomalies. NDR must also have automated responses, such as host containment (through integration) or traffic blocking, directly or through integration with other cybersecurity tools, and after initial tuning, a low false positive rate to become a trustable source of insight and support automated response use cases.†

The Vectra AI Platform is built on behavioral-based detection. With 150+ pre-built AI/ML models for attacker behavior analytics and 35 patents in behavioral-based threat detection, Vectra AI's Attack Signal Intelligence advanced analytics automatically correlates detected threat events to deliver entity-centric prioritization of attacks. With AI-driven Attack Signal Intelligence, SOC teams go from 1000s of alerts per day to single digit alerts per day, thus providing the signal clarity SOC analysts need to focus their time and talent on what matters most.

With accurate attack signal clarity, SOC analysts can investigate instantly and take rapid confident response action to disrupt and disarm attacks, whether it be isolating an endpoint, locking down and account, or blocking traffic. The Vectra AI Platform's Automated Response framework provides a suite of automated response actions for your existing firewall, EDR, and SOAR.

D Aggregation of Incidents is a Requirement

Gartner: "The emergence of 'AI-augmented' analytics overlays, in the form of SOC assistants, will benefit the NDR market as a useful source of insights for aggregated and summarized views. NDR products must provide alert aggregation of logical security incidents based on multiple factors, not just alert ID and repeated alerts through integration with other SOC tools for richer context."†

Vectra AI has been doing "AI-augmented" analytics for over a decade to assist SOC teams. The primary focus being accurate attack signal at speed and scale. We agree "SOC-assistance" in the form of LLMs will benefit SOC teams investigate faster, but we contend the problem to solve first with AI is alert noise, or lack of clear signal.

Vectra AI Attack Signal Intelligence - native the Vectra AI Platform's network, identity and cloud threat detection and response automates the correlation of threat events detected and aggregates them into a single entity-centric prioritized alert. To do so, we use "AI-augmented" analytics to answer three fundamental questions SOC analysts must answer: Is this attack real (attack rating), should I care (entity importance), and how critical is it to the organization (urgency score)?"

E Decryption of network traffic is an optional capability

Gartner: "Optional NDR capabilities include Transport Layer Security (TLS) traffic decryption."†

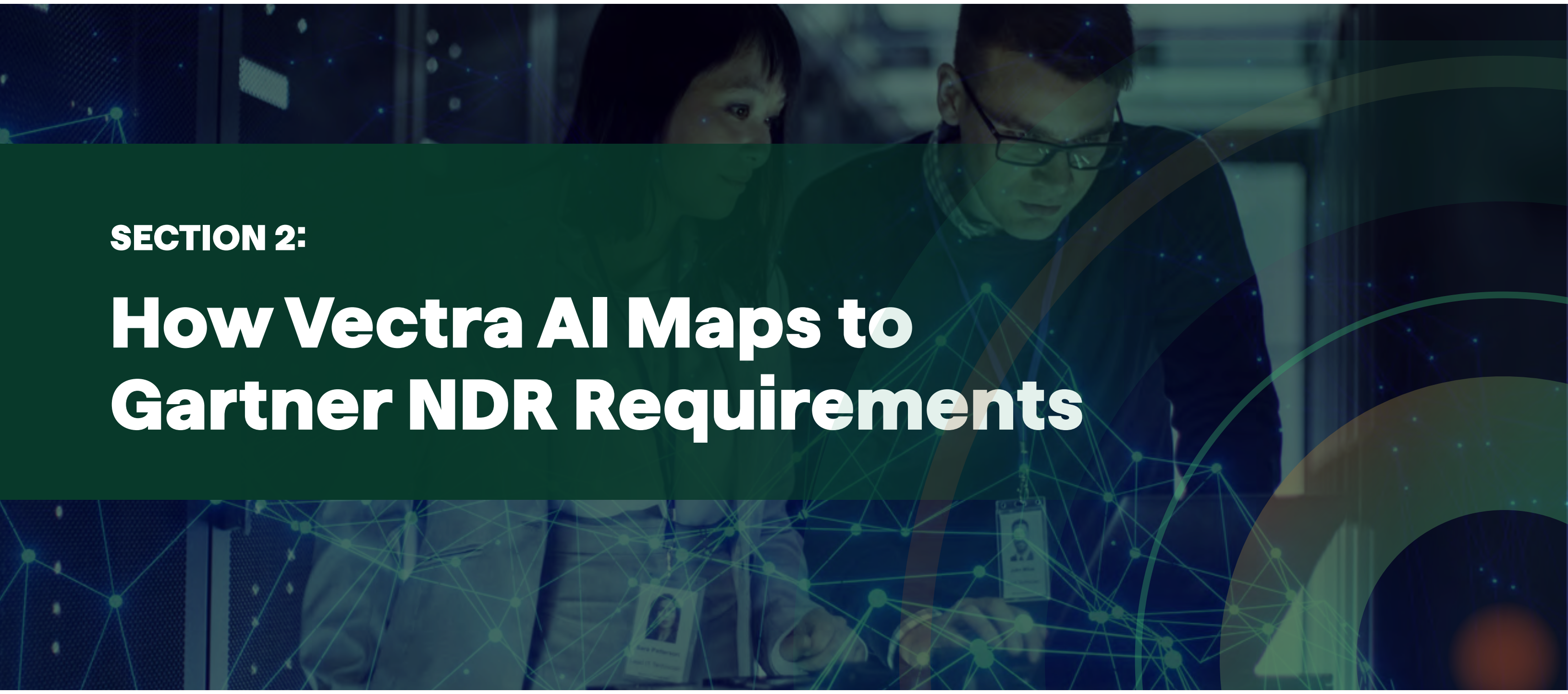
We applaud Gartner for recognizing decryption of network traffic as "optional." Vectra AI has been making the argument that you do not need to decrypt to detect for years. Unlike competitive NDR solutions, Vectra AI Attack Signal Intelligence sees through encryption removing the operational burden of decryption, not to mention eliminating sensitive data exposure risk decryption poses to organizations.

F Where is identity in the NDR guide?

Gartner excludes identity detection and response as a must-have for NDR.

We believe this is a missed opportunity for Gartner. Vectra AI's perspective is that all modern enterprises are hybrid, thus all modern attacks are hybrid attacks, and all hybrid attacks are identity-based attacks. Vectra AI contends that modern hybrid attackers need two things to be successful: a network and an identity – making identity threat detection and response (ITDR) an NDR necessity. By combining NDR and ITDR, SOC teams are better equipped to defend against modern hybrid attacks.

Identity is the modern hybrid attackers' linchpin. Case in point – Scattered Spider. Scattered Spider does four things extremely well. They compromise an identity (human or machine identities), elevate privileges, move laterally across domains, and locate and access valuable assets. By integrating native network signal (NDR) with native identity signal (ITDR), SOC teams can keep pace with hybrid attackers like Scattered Spider – seeing them and stopping them early in their progression.



SECTION 2:

How Vectra AI Maps to Gartner NDR Requirements

Gartner's NDR must haves – Vectra AI Platform delivers on all 3

1 **Deliver form factors compatible with on-premises and cloud networks to analyze raw network packet traffic or traffic flows, and monitor both north-south and east-west traffic.**[†]

Vectra NDR – part of the Vectra AI Platform – delivers the network visibility customers need based on the environment customers have.

Vectra NDR covers data center, cloud (AWS, Azure, GCP IaaS), and IoT/OT networks with complete visibility for north-south and east-west traffic.

Vectra NDR can be deployed on-premises, or in the cloud (SaaS) with actionable threat signal in a matter of hours.

Vectra NDR leverages both physical and virtual sensors, and with the addition of Gigamon GigaVue, SOC teams gain real-time observability and intelligence into all attacker movements in one, easy-to-deploy solution.

2 **Model normal network traffic and highlight unusual traffic activity with detection based on behavioral techniques such as machine learning (ML) and advanced analytics.**†

The Vectra AI approach to threat detection blends human expertise with a broad set of data science and advanced machine learning techniques. This model delivers a continuous cycle of attack intelligence based on security research, global and local learning models, deep learning, and neural networks. Using behavioral detection algorithms to analyze metadata from captured packets, our cybersecurity AI detects hidden and unknown attacks in real time, whether traffic is encrypted or not. Our AI only analyzes metadata captured from packets, rather than performing deep-packet inspection, to protect user privacy without prying into sensitive payloads.

Global learning begins with the Vectra AI Threat Labs, a full-time group of cybersecurity experts and threat researchers who continually analyze malware, attack tools, techniques, and procedures to identify new and shifting trends in the threat landscape. Their work informs the data science models used by our Attack Signal Intelligence, including supervised machine learning. It is used to analyze very large volumes of attack traffic and distill it down to the key characteristics that make malicious traffic unique.

Local learning identifies what's normal and abnormal in an enterprise's network to reveal attack patterns. The key techniques used are unsupervised machine learning and anomaly detection. Vectra AI uses unsupervised machine learning models to learn about a specific customer environment, with no direct oversight by a data scientist. Instead of concentrating on finding and reporting anomalies, Vectra AI looks for indicators of important phases of an attack or attack techniques, including signs that an attacker is exploring the network, evaluating hosts for attack, and using stolen credentials.

Our AI-driven Prioritization engine combines thousands of events and network traits into a single detection. Using techniques such as event correlation and host scoring, our AI correlates all detection events to specific hosts that show signs of threat behaviors. We then automatically score every detection and host in terms of the threat severity and certainty using our own threat certainty index.

Finally, we track each event over time and through every phrase of the cyberattack lifecycle putting special focus on entities that are strategic value to an attacker.

3 **Aggregate individual alerts into structured incidents for fast threat investigation, and provide automatic or manual response capabilities after detecting malicious network traffic.†**

At Vectra AI, we boil this down to 3 things SOC teams need:

Coverage + Clarity + Control

Coverage comes from our 150+ pre-built AI/ML models and 35 patents on attacker behavior analytics. Our domain specific detections cover more than 90% of ATT&CK techniques and have the most vendor references in MITRE D3FEND enabling us to detect events that are security relevant.

Clarity comes from our AI-driven Attack Signal Intelligence that analyzes individual detections to establish an attack profile and give it an attack rating. Attack ratings are combined with entity importance based on ML that learns the customer environment. (Entity importance is customizable by the customer). The combination of attack rating and entity importance creates an urgency score. Urgency scores are entity-centric (for both hosts and accounts) and based on aggregated and correlated threat events, so instead of thousands of individual daily alerts streams, SOC analysts get prioritized alerts in the single digits per day.

Control is arming SOC teams to rapidly and confidently investigate and respond to prioritized entities (hosts and accounts) under attack. With deep investigative context and native, integrated, automated and managed (MXDR) response, SOC teams are equipped to take control of hybrid attacks early in their progression.

Gartner's Standard NDR Capabilities – Vectra AI Platform delivers on all 5

1 Monitoring and analyzing traffic in IaaS environments.†

Vectra NDR for Cloud – part of the Vectra AI Platform – provides full coverage, clarity, and control on attackers with Gigamon Deep Observability Pipeline. The Vectra AI Platform provides continuous monitoring of on-premises and cloud (IaaS) network traffic to pinpoint in-progress attacks that evade perimeter defenses.

Gigamon accesses traffic across physical and virtual networks, filters this traffic, and sends the intelligence to Vectra AI for real-time threat analysis. Key benefits of the Gigamon and Vectra AI integration:

Vectra NDR detects in-progress attacks that evade prevention security defenses and spread inside networks – *automatically and in real-time*.

Visibility into physical, virtual traffic across the network, Vectra NDR combines data science, machine learning, and behavioral analysis to detect all phases of an attack.

Gigamon taps traffic across physical, private cloud, public cloud, and container environments and delivers the intelligence to Vectra NDR on the physical network – ensuring all traffic is monitored and analyzed to avoid blind spots. Gigamon ensures that only relevant traffic and sessions are sent to Vectra AI, prioritizing security efforts on traffic that poses the most risk.

Together, Vectra and Gigamon offer a turnkey solution to secure traffic in virtualized environments. Customers do not need an intermediary to feed cloud traffic into Vectra AI – significantly simplifying the process of implementation.

The Gigamon Deep Observability Pipeline communicates with taps sitting across an infrastructure to access East-West traffic. Once East-West traffic is accessed by taps, it is then sent to either GigaVUE® HC series appliances in physical datacenters or mirrored to GigaVUE® Visibility Nodes in virtual environments for aggregation, deep packet inspection, and filtering of traffic. The HC series and Visibility Nodes then present a filtered intelligence stream that contains only important traffic to the Vectra AI Platform. Once the Vectra AI Platform receives the network traffic from Gigamon, it is automatically correlated with detected threats and prioritized on the user interface.

2 **More traditional detection techniques, like intrusion detection and prevention system (IDPS) signatures, rule-based heuristics, and threshold-based alerts.†**

Vectra Match is a capability of Vectra NDR that ingests intrusion detection signature context. This means, SOC teams gain complete clarity on known and unknown threats by combining signature context with the power of behavior-based Attack Signal Intelligence. By combining the two, SOC teams can uncover sophisticated threats across the network, including those that may bypass a legacy Intrusion Detection System (IDS) or Intrusion Prevention System (IPS).

Vectra Match runs on Suricata which enables your SecOps team to process multiple events at the same time without having to interrupt other requests. In order to have better signal clarity, your team needs a network detection and response solution with Suricata that will:

Reduce noise: With Vectra Match and Vectra NDR, you will dramatically cut down on the number of false positives by accurately detecting and analyzing all inbound and outbound traffic, ultimately detecting malicious traffic attempting to enter the network.

Validate threat signals: In order to find the needle in the haystack, you need to be able to have the full haystack. Vectra Match with Vectra NDR unifies visibility and context for known and unknown threats into your existing SIEM.

Enhance threat detection and response: Identify network-based indicators of compromise (IOCs) such as domains and IPs, as well as malicious attacker behavior to align your SecOps team and narrow down the most critical and urgent threats on your network environment.

3 **Alert aggregation of logical security incidents based on multiple factors, not just alert ID and repeated alerts through integration with other SOC tools for richer context.**†

This is where the **Vectra AI Platform's signal clarity** comes into play. Like mentioned above, Attack Signal Intelligence takes an entity-centric approach to alerting reducing thousands of individual daily alerts into single digits per day.

For each prioritized entity, SOC analysts get;

- snapshot of why an entity is being prioritized,
- can jump into the prioritized entity and start investigating,
- see a list of individual detections that make up the attack's progression,
- quickly filter prioritized entities by key characteristics.

Investigations include rich context derived from 3rd party integrations with AWS, Crowdstrike, Cybereason, Fireeye, Gigamon, KVM, Keysight, Microsoft 365, Microsoft Azure, Microsoft Defender for Endpoint, Microsoft Hyper-V, Netscope, Nutanix, SentinelOne, VMware, and Zscaler to name a few.

In addition, Vectra AI signal can be sent to SIEM and SOAR SOC tools like Google Chronicle, CORTEX XSOAR, Crowdstrike Falcon LogScale, Elastic, Fortinet, IBM Qradar, Microsoft Azure Sentinel, and Splunk to accommodate existing SOC workflows.

4 **Automated responses, such as host containment (through integration) or traffic blocking, directly or through integration with other cybersecurity tools.**†

The Vectra AI Platform includes automated and manual response actions that are native, integrated and managed via Vectra MXDR.

Native response actions include: AWS account lockdown, Azure account lockdown and SB lockdown.

Integrated response actions are available via wide range technologies via the Vectra Automated Response Framework to rapidly targets hosts and accounts that are observed behaving in ways above a user-defined security priority threshold. Vectra AI sends immediate notification of such behavior via email and/or syslog, while issuing entity isolation actions to the configured third-party tools like EDR, Firewall, and SOAR solutions.

Managed response is also an option where SOC teams can outsource investigation and response actions to expert Vectra MXDR analysts.

5 **A low false positive rate, after initial tuning, to become a trustable source of insight and support automated response use cases.†**

Vectra AI's perspective is that "low false positive rate" does not reflect the true pain point when it comes to alert noise. You can have a low false positive rate, but stlll a high number of benign true positive alerts. In order to maximize the value of SOC time and talent, what SOC analysts need is accurate and actionable attack signal. We need to stop talking about false positives and start talking about real attack signal, hence Vectra AI Attack Signal Intelligence.

Secondly, "after initial tuning" presumes work is needed up front by security architects and detection engineers to arrive at low false positives. And, let's face it, there is no such thing as initial tuning. Tuning is never-ending for detection engineers to reduce false positive rates. When we hear the word "tuning" we hear "detection latency" and the last thing SOC teams need is more latency. Latency only gives attackers more time to progress and achieve their goals. Vectra AI's mission is to deliver the most accurate and actionable attack signal at speed and scale without the need for tuning. Only then will we become a "trustable source of insight" for security architects, detection engineers, and SOC analysts, and we believe we have the best attack signal on the planet.

SECTION 3:

Vectra AI Takeaways from the Gartner Market Guide for NDR

The Gartner Market Guide for Network Detection and Response underscores the evolution and emergence of NDR in the era of Cloud, AI, and Automation. It validates the same challenges we hear from customers when it comes to the growing cloud attack surface, alert noise, and the need for accurate attack signal, rapid investigation and confident response. It acknowledges that the lines are blurring between NDR and XDR.

In the Vectra AI spirit of accurate and actionable signal, here is what we see the Gartner Market Guide for Network Detection and Response signaling, and key considerations for Security Leaders, Architects, Engineers and Analysts:

There is no DR (detection and response) without AI – it is the only way SOC teams will keep pace with attackers. Security buyers beware of AI labels, demand vendors prove AI legitimacy.

There is no XDR without NDR – it is the first line of defense, the source of truth. Security buyers should look at NDR as the logical first step on the path to XDR.

There is no NDR without Identity (ITDR) – identity is the attacker's linchpin and key to their success and Gartner missed it in their report. Security buyers must require identity coverage when shortlisting NDR vendors.

VECTRA

The Vectra AI Platform

The Vectra AI Platform delivers real-time extended detection and response (XDR) for hybrid attacks spanning networks, identities, and clouds of all types. Powered by our patented AI-driven Attack Signal Intelligence, the Vectra AI Platform modernizes the SOC by reducing exposure, removing latency, and maximizing the value of existing talent.

How we do it is simple.

Coverage: With domain specific detections for over 90% of MITRE ATT&CK, and the most references for MITRE D3FEND countermeasures, SOC teams get integrated hybrid attack coverage in one place.

Clarity: With 150+ pre-built AI/ML models for attacker behavior analytics and 35 patents in Attack Signal Intelligence, SOC teams get the signal clarity to focus their time and talent on what matters most.

Control: With deep investigative context and native, integrated, automated and managed response, SOC teams are equipped to rapidly and confidently take control of hybrid attacks early in their progression.

Learn more about the Vectra AI Platform with Attack Signal Intelligence and what it is, does and means for your SOC.

About Vectra AI

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

[†] Gartner Market Guide for Network Detection and Response, Published 29 March 2024 – ID G00784755

For more information please contact us:
Email: info@vectra.ai | vectra.ai