Vectra AI Introduces Vectra Match for Signature-based Detections to Aid SecOps Team Investigations

Consolidate your security footprint with network detections and signature-based IOCs in one single sensor

Vectra Match delivers enhanced capabilities for detection and response by ingesting intrusion detection signature context for more efficient and effective threat hunting and investigation. Vectra Match leverages the industry standard for open-source IDS (Intrusion Detection System) – Suricata. Vectra Match integrates directly into the Vectra NDR sensor which helps your organization reduce your overall security solution footprint. In doing so, your SecOps teams can now incorporate signatures to enable identification and matching of the desired network CVEs and other potential exploits. Your security team will gain signal clarity on known and unknown threats across your network through the combination of Vectra Match signature context and the power of Vectra NDR with AI-driven Attack Signal Intelligence™.

Key Benefits

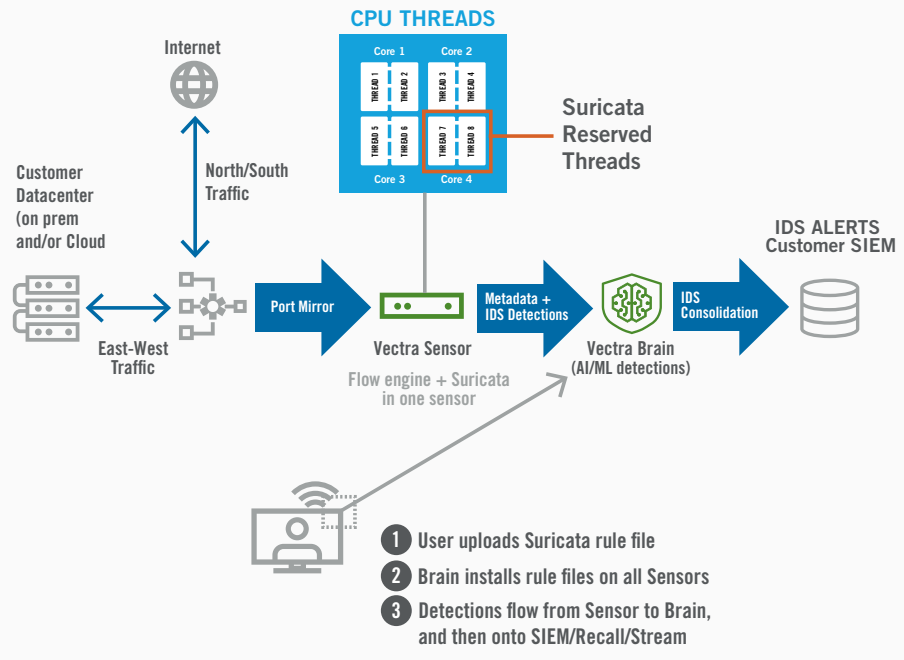
- Meet regulatory compliance requirements
- Single sensor for NDR and Suricata
- Streamline SOC analysts' workflow efficiency during threat hunting activities

The perfect match for your Vectra NDR deployment

Only Vectra Match with Vectra NDR provides your SecOps team with both signature-based technology and AI-driven detection to provide the measures necessary for detecting known indicators for attack identification — including vulnerability exploits. Vectra Match also meets the industry mandates for certain CVSS scores in the market today, meaning that your organization can meet the current regulatory standards while also reducing tool sprawl, which consequently, helps improve your SecOps team workflow. Vectra Match with Vectra NDR provides the most precise signal clarity to detect modern and evasive attacks on your network.

- **Vectra AI NDR Sensor –** Vectra provides customers with the opportunity to have numerous NDR deployments via sensors that cover everything from corporate data centers to cloud workloads. This enables organizations to leverage existing Vectra NDR investments and get visibility where they cannot install vendor appliances — providing uniform network context across hybrid cloud environments.
- **Optimized Workflow –** Optimize your current SecOps security solution workflow with Vectra Match, Vectra Stream, and Vectra Recall for an in-depth metadata analysis with signature-context that is coupled with Vectra NDR to better detect and prevent advanced cyberattacks from executing.
- **Rich Context from all Data Sources –** Vectra AI provides your SecOps team with the full attack storyline, highlighting both known and unknown attacks. Implement AI-driven detection with the engine of Suricata in one cybersecurity solution.

Vectra Match Architecture

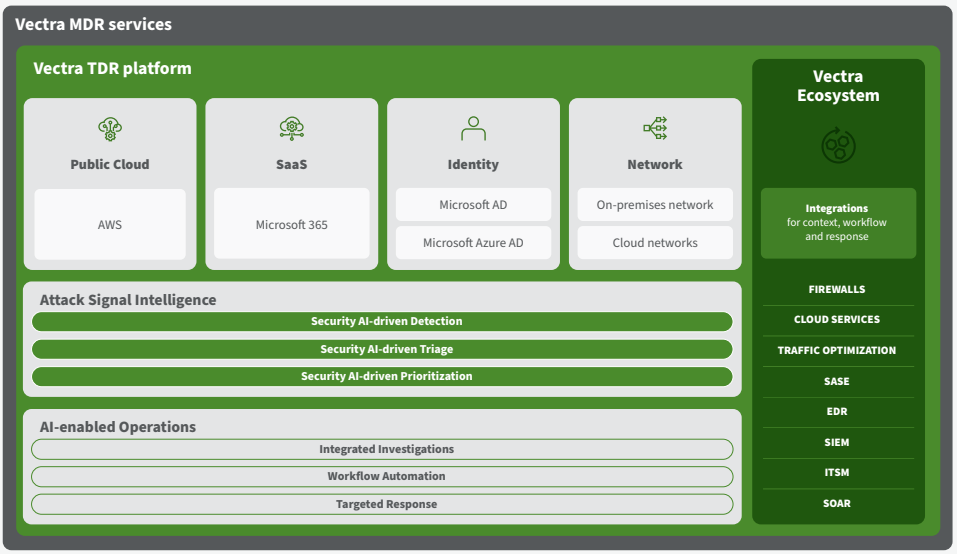


Technical Requirements

Surface Both Known and Unknown Attacks

Traditional IDS and IPS solutions primarily rely on Suricata's known signatures which historically don't have ML/AI. This is not enough to address both known and unknown attacks. Organizations need to have access to the current threat intelligence of both known and unknown attacks to have a true detection and response cybersecurity solution. Today, SecOps teams are overwhelmed with thousands of threat alerts daily. Discerning these alerts is critical to responding to incidents in real-time. To do so, SecOps teams need a solution that provides exploit detection and identifies attacker behaviors in real-time.

Today's security teams are challenged with more attack surface exposure and more evasive attacker methods. Therefore, organizations must level up their current threat detection and response solutions by identifying both known and unknown threats in real-time across the entire network infrastructure. Vectra NDR with Vectra Match are the only threat detection and response solutions that harness Vectra's AI-driven Attack Signal Intelligence™ — empowering SecOps with a risk-based approach to detecting modern cyberattacks while reducing alert noise and addressing security tool sprawl. Vectra Match goes beyond legacy IDS solutions by providing SOC analysts with the rich context of every incident for better threat hunting and more proficient investigations.



Explore the Vectra AI-driven Threat Detection and Response Platform and MDR services powered by Attack Signal Intelligence.

About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

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