Best Practices to Address Tool Sprawl for Your NDR and IDS solutions

Vectra Match for NDR consolidates behavior-based and signature-based detection correlation

This best practices document highlights an effective path to utilizing exploit detection and AI-driven detection to contextualize attacker behaviors while avoiding security tool sprawl. Your team can levearge this document to help answer the question: "are we maximizing our ability to stop both known and unknown attacks in a single solution"?

Key Challenges

- **Detecting known and unknown threats** to surface attacks that bypass legacy IDS and IPS solutions.
- **Threat hunting and investigations** that accurately uncover network-based indicators of compromise (IOCs) and the most urgent threats.
- **Expanding vulnerabilities and exploits** require both signature and behavior-based detection.

Don't settle for the status quo with your current Intrusion Detection System (IDS)

Today, there are more choices for security solutions than one can count, and the growing number of threats and vulnerabilities are increasing right alongside them. Intrusion detection systems (IDS), intrusion prevention systems (IPS), and the convergence of the two, known as intrusion detection and prevention systems (IDPS) have been around for several years. These solutions are signature-based which are important in uncovering malicious activities in the network. However, these solutions do not leverage AI-driven detection capabilities — and therefore leave gaps in your threat detection and response solutions. Enterprises need a threat detection and response security solution that detects both known and unknown attacks in the network in order to arm themselves properly against malicious actors.

How to keep tool sprawl to a minimum

Optimize your threat detection and response with one sensor:

Vectra Match erases the need for managing and tuning each of your separate deployed IDS sensors. With Vectra NDR and Vectra Match your signature-based solutions and NDR security tools are both deployed on the same sensor. This greatly reduces your security footprint and address tool sprawl.

Silence the noise from IDS:

Coupling Vectra NDR AI-driven detection with Vectra Match exploit detection for CVEs significantly reduces the number of false positives. In doing so, SecOps can focus on responding to incidents that have been vetted — with all the contextual insights from behaviors in your network to paint the full picture of the most critical and urgent threats.

Detect both known and unknown threats:

IDS, IPS and IDPS solutions are often placed at the perimeter of your network. These solutions often focus on north/west movement but can miss east/west movement and focus on in-line protection. Vectra Match with Vectra NDR focuses on detecting both known and unknown behaviors with an expanded threat intelligence database and visibility into your entire network both on-premises and in the cloud.

Keys to success:

- Less tuning and managing of separate security sensors.
- Simple integration with your chosen SIEM, such as Vectra Stream or Vectra Recall.
- Complete visibility into your network infrastructure, not just the edge of your network.

One solution to prioritize threats across your SOC

With the evolving number of malicious actors threatening enterprises today, it is crucial that organizations can pinpoint the most critical and urgent threats, so they can take the necessary steps to mitigate attacks from executing or reaching their chosen targets. Taking resources away from managing and tuning activities with Vectra Match automates compensating controls and then redirects SecOps to vital threat hunting activities. With Vectra Match and Vectra NDR, organizations can address signature-based use cases along with behavioral detection in one single solution.

Contact our team today to learn more about Vectra Match

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