# From DIY to AI: Removing SOC latency by shifting from build-your-own SEIM rules to pre-built AI models

Why create and maintain your own detection rules when AI can do it for you?

**97%** **of security analysts worry they'll miss a relevant security event[1]. As new evasive threats are being conducted daily — making threat detection and response a top priority for cybersecurity teams securing hybrid cloud environments. In fact, nearly two-thirds of analysts say the size of their attack surface has increased in the past three years.[2]**

According to the Gartner Hype Cycle for Security Operations, 2022[3], SIEM adoption is considered "mature mainstream" with up to 50% market penetration, indicating that up to half of organizations follow a DIY (Do It Yourself) detection rules model. This methodology may be cost-effective when first starting out, but over time the costs can grow exponentially — far exceeding the original budget. What may be easy to fund through internal resources today, may not be the case tomorrow because, in certain instances, DIY can end up costing many times the initial costs because of the need to remove and replace current solutions from scratch. Organizations are in dire need of a robust and trusted threat detection, investigation and response (TDIR) — DIY models often don't fit the bill. The time and resources spent on DIY methods would be better spent integrating with the technology needed to strengthen your TDIR solution.

Enterprises today are faced with the decision of taking the simpler, and some might say, easier DIY approach as the foundation for building and maintaining detection methodologies in-house by placing chosen data into a SIEM or data lake. While this approach is often seen as more cost-effective and easier, this method wastes top talent time and resources by focusing on building and tunning models, creates even more noise, and does not properly address the challenge of unknown threats. Consequently, this leaves enterprises in a rather vulnerable position.

## Key challenges to consider

- DIY detection models across the hybrid and multi-cloud attack surface require deep expertise in many domains and data sets.
- Alert noise in the SOC becomes overwhelming for analysts, especially with the limited Machine Learning (ML) tools — and even modern SIEM platforms.
- Relying primarily on SIEMs that attempt to stitch together records and data generates more signals for SOCs to string together with limited context.
- Maintenance is challenging and as a result of analyst burnout and turnover — knowledge leaves the organization with the person who initially developed it.
- Tool effectiveness is unknown. Detection models (especially after tuning) are one-offs and the coverage against real threats is unknown.
- SIEM licensing costs are high, especially for network data sources — making any perceived cost savings evaporate before the real challenges are addressed.

### Why a purpose-built modern threat detection, investigation & response (TDIR) solution:

- Brings immediate value to SecOps vs. focusing on maintenance of alerts and tools.
- Allows top talent to focus on actively defending the business and developing the team rather than chasing new alerts.
- Reduces alert noise in the SOC by applying an AI-driven approach to detect, triage and prioritize threats.
- Delivers proven outcomes by leveraging models based on feedback from hundreds or even thousands of organizations.

Source 1 & 2 — Global Report: *2023 State of Threat Detection, The Defender's Dilemma*
Source 3 — Gartner Report; *Hype Cycle for Security Operations, 2022*

## Key criteria to consider

Today, enterprises need a formidable cybersecurity solution that they can trust to do what is needed to keep bad actors at bay. To achieve this, Vectra AI research and experts say that organizations need:

**Consolidated and unified attack telemetry coverage:**

- A TDIR solution that covers all high-value attack surfaces including endpoint, network, identity, public cloud control and plane, critical SaaS applications such as M365, and minimizes the need for additional integrations or workflows. By choosing a vendor such as Vectra AI for full visibility throughout hybrid cloud environments, teams alleviate the challenges from tool sprawl and the use of resources dedicated to building and maintaining multiple solutions.

**Threat signal clarity with entity-centric threat detection, investigation and response (TDIR):**

- A TDIR solution that provides AI-driven signal clarity for the highest-fidelity signal empowers security teams to move at the speed of hybrid cloud attackers. Without these pivotal insights, it is almost impossible to know where attackers have compromised, and where analysts should spend efforts to address the most critical and urgent threats. The Vectra AI Platform harnesses Vectra AI-driven Attack Signal Intelligence to provide the best-in-class AI-driven security in real-time, empowering organizations to be more resilient to exploits so they can achieve their business objectives.

**Intelligent control with AI-enabled operations:**

- Cybersecurity solutions should enable an easier workflow for SOC teams. Organizations need security teams to shift from focusing on any build-related activity to threat models that are specific to their organization. Additionally, threat models need to detect the most urgent and critical threats for teams to act and respond accordingly. The Vectra AI Platform is the only solution that empowers SecOps to be able to act and take the best course of action through AI-enabled investigation, hunting and response.

## Keys to success:

- Less time on building and maintaining detection models — asses detection engineering time and resources spent on creating and maintaining detection models.
- Simple integration with existing systems such as SIEM, EDR and IDR — identify and consider what use cases are ideal for SIEM vs. purpose-built TDIR.
- Native hybrid cloud coverage — TDIR solution that can detect both known and unknown threats with unified and conoslidated attack telementry across the entire hybrid cloud infrastructure.

The Vectra AI Platform is the only security solution that thinks like an attacker to identify real threats in real time. Vectra AI provides AI-driven Attack Signal Intelligence that thinks like an attacker to zero in on the tactics, techniques, and procedures (TTPs) attackers use to hide right out of the box. Unlike DIY solutions, there is no building and maintenance required. Thus, eliminating the endless cycles of building and maintaining threat detection models.

With the Vectra AI Threat Detection Investigation and Response (TDIR) Solution, SecOps teams can focus on threat hunting activities with the confidence that they have the most trusted signal clarity to analyze, detect and respond to threats in their network and public cloud.

**Learn more about the Vectra AI Platform**

## About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

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