VECTRA AI

EBOOK

TRUSTED SIGNAL IS EVERYTHING

Attack Signal Intelligence for the Agentic SOC

AI agents are only as good as the signal they reason from.

Vectra AI Pro Platform - Three paths to the Agentic SOC

CONTENTS

What's inside

From the shift changing the SOC to the three paths you can take with Vectra AI.

02 The shift: attacks at AI speed

03 Why signal is the core problem

04 How trusted signal is built

05 Network and identity data

06 Enrichment and signal intelligence

07 One platform, three paths

08 Path 1 · Build your own agentic SOC

09 Path 2 · Add agentic workflows

11 Path 3 · Operationalize with experts

12 How to get started

THE SHIFT

Attacks move at AI speed now.

They don't hack in. They log in. Now they do it at machine speed. It helps to see the shift clearly before choosing your next move.

Timelines compress from days to minutes

Post-Mythos, attacks can be planned, adapted, and executed at AI speed across identity, cloud, SaaS, and network at once.

Reducing mean time to respond is the game

That pressure is driving the SOC from human-centric workflows to agentic workflows, where AI agents help investigate and take response action.

The shift is real, and it is fast

Exploits outpace patches, AI agent identities expand the attack surface, unmanaged devices create blind spots, agentic AI attacks move faster than defenders, and multi-domain attacks are now the norm.

THE NEW TEMPO

Days → Minutes

Attack timelines are collapsing as adversaries plan, adapt, and execute at AI speed.

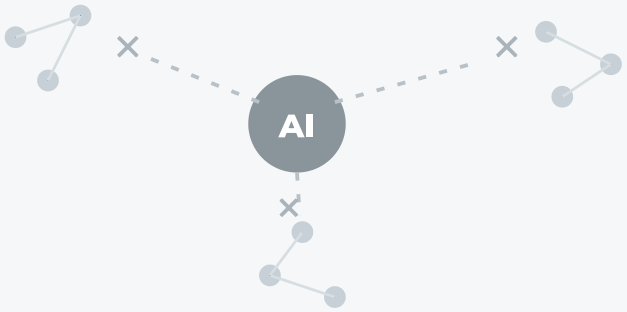
As leaders make that shift, one question becomes urgent: what is the AI reasoning from?

THE CORE PROBLEM

AI Agents are only as good as the signal it reasons from

AI agents can summarize, search, correlate, recommend, and act. But in security operations, those capabilities only create value when they are grounded in trusted signal.

WITHOUT TRUSTED SIGNAL



Data stays siloed and disconnected. The agent sees fragments it cannot link into one story, so it reasons without the full context.

Too much data, too little clarity, and too much work

WITH TRUSTED SIGNAL

Data is completed, correlated, contextualized, and enriched, so signal intelligence turns activity into one clear security meaning.

Agents and humans move faster and make better decisions

Without trusted attack signal intelligence, agentic AI just automates and amplifies noise. Speed without trusted signal makes bad decisions faster.

How trusted signal is built

Raw activity becomes trusted signal intelligence in four layers, each one adding to the last.

Network data
What happened

Which systems communicated, protocols used, how data moved, and where lateral movement and command-and-control appeared.

Identity data
Who or what

The user, service account, machine identity, workload, or AI agent behind the activity, the privileges used, and whether behavior fit the entity's role.

Enrichment
Context to reason

Entity attribution, behavioral baselines, privilege and attack-stage context, risk, historical sequence, and the evidence behind the signal.

Signal intelligence
Why it matters

Correlated, contextualized activity becomes security meaning: a compromised host, lateral movement, trust abuse, attacker progression.

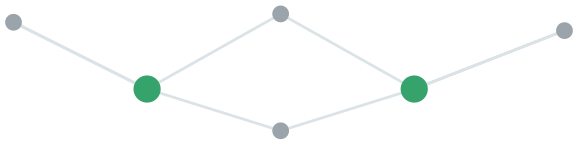
Vectra AI correlates signal across network, identity, cloud, and SaaS, and pulls in context from ecosystem EDR and SASE partners.

Network and identity: the two data sources agents can't reason without

Network answers what happened

Attacks increasingly unfold between endpoints, not on them. **1 in 3 devices has no EDR agent,** and network data sees what endpoint tools cannot.

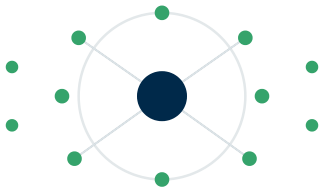
- Which systems communicated
- How entities interacted
- Where C2 appeared
- Which unmanaged systems participated
- Which protocols were used
- Where lateral movement appeared
- How data moved
- How patterns changed over time



Identity answers who or what

Identity is the primary control plane of the modern enterprise, and **80% of attacks now involve identity compromise or abuse.** Non-human identities can outnumber humans by as much as 109:1.

- Which user, service account, machine identity, workload, or cloud identity was involved
- What privileges or access were used
- How authentication and access patterns changed
- Which trust relationships were used
- Whether the activity aligned with the entity's normal role
- How identity behavior connected to network behavior



Network tells you what moved. Identity tells you who moved it. You need both to see the attack.

FROM ACTIVITY TO MEANING

Enrichment and signal intelligence: turning activity into meaning

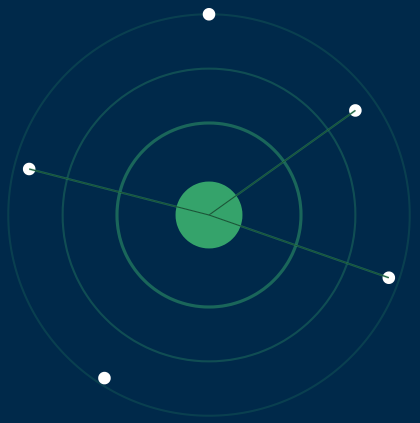
Enrichment adds context to reason

- Entity attribution to the right host, account, identity, device, workload, or system
- Behavioral baselines: normal, unusual, rare, or suspicious for that entity?
- Privilege, attack-stage, risk, and evidence context mapped to attacker progression

Attack Signal Intelligence says why it matters

- A host or account behaves like it may be compromised, or moves laterally
- A service account shows misuse; a pattern suggests command-and-control
- A cloud or SaaS action indicates trust abuse; an unmanaged system joins an attack path

> "For us, Vectra AI brings together correlated network, identity, and cloud signals with the context to understand what happened before, what happened afterwards, and the full attack story. That helps us compress investigation and response, act with greater confidence, and stay ahead of attackers."
>
> **AJ Wiggan** · Security Operations Manager, Gamma



Attack Signal Intelligence arms both humans and AI agents to see the full attack story faster and respond with confidence.

CHOOSE YOUR PATH

One platform. Three paths to the agentic SOC.

Same AI. Same Attack Signal Intelligence. Pick the path that fits your team.

BUILD

Build your own agentic SOC

For security architects, detection engineers, and AI SOC partners building their own AI-driven SOC architecture.

ADD

Add agentic workflows

For teams strengthening the SOC they already run. Vectra AI Pro adds agentic workflows out of the box, powered by the same trusted signal.

OPERATIONALIZE

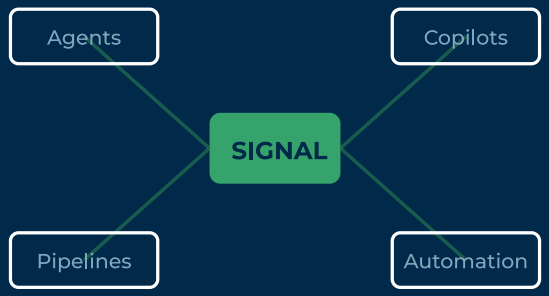
Operationalize with experts

For teams that want help putting AI and Attack Signal Intelligence to work day to day.

PATH 1 · BUILD

Build your own agentic SOC

For: Security architects, detection engineers, and AI SOC partners building their own AI-driven SOC architecture.



What Vectra AI provides

Behavioral detections
High-fidelity, domain-specific detections across network, identity, cloud, and SaaS.

Network metadata
Protocol-level evidence behind every signal, from DNS to lateral movement.

Identity context
Who or what was involved, and how access, roles, and trust were used.

Entity attribution
Connects signal to the right host, account, identity, workload, or system.

API-accessible signal
Programmatic access to detections, entities, and enriched metadata.

MCP-ready access
Open-source resources to connect AI agents to Vectra AI signal, live for a year.

WHAT YOU GET

Control and extensibility. You own the architecture, and Vectra AI grounds it in signal your agents can trust.

PATH 2 · ADD

Add agentic workflows

For: Teams adding agentic capabilities to the SOC they already run.

You don't rebuild the SOC. You get the **same domain-specific behavioral detections, network metadata, identity context, and entity attribution** as the Build path, plus agentic workflows out of the box that detect, correlate, triage, and prioritize, then build a natural-language case that explains itself.

What the agentic workflow adds

AI triage, correlation, and prioritization

Connects related activity across network, identity, cloud, and SaaS, then ranks hosts and accounts by attack progression, severity, velocity, breadth, rarity, and entity importance.

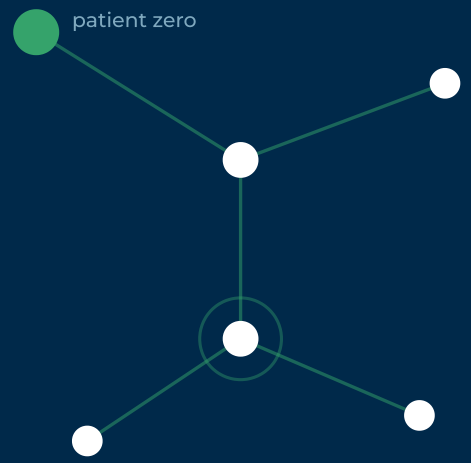
Attack graphs

See the shape of an attack across entities and domains instead of reviewing isolated alerts. Identify patient zero and blast radius.

The natural-language case

Answers why the threat was prioritized, what evidence proves it, how activity connects across entities and domains, and what actions to take with confidence.

ONE ATTACK, ONE GRAPH



From isolated alerts to a connected story across entities and domains.

PATH 2 · ADD

Agentic investigation

Autonomously correlates detections, queries underlying metadata, reconstructs the attack chain, and delivers an evidence-backed incident summary with prioritized response recommendations, working alongside analysts.

AI-assisted investigations

Pivot from signal to supporting evidence, explore metadata with AI-assisted search, and run curated hunts across hybrid environments.

AI-assisted hunting

Test hunt hypotheses, uncover suspicious behavior that never started as an alert, and turn successful hunts into repeatable workflows.

AI-enabled response

Lock down compromised identities, isolate hosts through EDR, and block attacker communications through firewall integrations, manually or automatically, with human-in-the-loop always in control.

What your peers say

Less noise, faster response, more efficient SOC

Globe Telecom

Incident response from 16 hours to 3.5 hours, attacks contained more than 75% faster, alert noise cut 99% and escalations 96%, protecting services for 80M+ customers.

Luxgen Motor

92.6% reduction in alert noise and 95.3% reduction in escalations, with a team of fewer than five.

"Investigating Vectra AI alerts takes 100 to 1,000 times less effort than dealing with raw firewall logs. The platform gives us context we used to spend hours trying to build ourselves."

Sébastien Wojcicki · Head of Operations & Security Excellence, Advens

PATH 3 · OPERATIONALIZE

Operationalize with experts

For: Teams that know where they want to go with AI but need help making it work day to day.

What Vectra AI experts help you do

Integrate
Align signal to your escalation paths, investigations, response, and daily tools.

Monitor
See what is happening across the enterprise and where risk is emerging.

Hunt
Turn threat hunting into a repeatable SOC practice with reusable workflows.

Optimize
Find tuning opportunities and gaps for cleaner signal and clearer priorities.

Respond
Validate signal and guide next steps, with humans in control of key actions.

Prove
Translate the work into evidence of measurable, ongoing progress.

THE OUTCOME

Move from AI experimentation to daily SOC execution, with proof that exposure is down, response is faster, and controls are effective.

HOW TO GET STARTED

Start with three questions

01 What security questions do your AI agents need to answer?

02 What signal, metadata, and context do those agents need, and where should it flow?

03 How much help does your team need: **build**, **add**, or **operationalize**?

The agentic SOC runs on trusted signal intelligence. Get the signal right, and AI makes your team faster, sharper, and more resilient. Get it wrong, and it just scales the noise.

Trusted signal is everything.

See how Vectra AI powers the agentic SOC →

Talk to Vectra AI about your path →

About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents, and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI-powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world.

VECTRA AI

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