# Vectra Security AI-driven Attack Signal Intelligence™

**For decades, cyber security has relied on what is known. Threat detection and response methodologies have relied heavily on signatures, anomalies and rules to see and stop cyber attackers from infiltrating organizations and stealing data. This approach is broken.**

As enterprises shift to hybrid and multi-cloud environments, embracing digital identities, digital supply chains, and ecosystems — security, risk and compliance leaders are faced with more.

- More attack surface to cover.
- More evasive and sophisticated attackers.
- More tools and more data sets to analyze.
- More signatures, anomalies, rules to maintain.
- More alert noise, triage, false positives.
- More analyst fatigue, burnout, turnover.

Despite more tools, data, signatures, policies, rules, alerts and people — the core problem remains the same:

**“We don’t know where we are compromised – *right now*.”**

### The unknown threat is how attackers get the upper hand

- Bypassing prevention
- Circumventing signatures and anomaly detection rules
- Infiltrating, progressing laterally
- Stealing data

## Vectra Security AI-driven Attack Signal Intelligence erases the unknown threat

Vectra Security AI-driven Attack Signal Intelligence takes a risk-based approach to cyberattacks while reducing manual tasks, alert noise and analyst burnout. Attack Signal Intelligence empowers security analysts to:

### Think like an attacker

AI-driven Detections go beyond signatures and anomalies to understand attacker behavior and expose the complete narrative of an attack.

### Focus on the malicious

AI-driven Triage reduces alert noise by distinguishing malicious from benign threat activity to expose malicious true positives while logging the benign.

### Know what is critical

AI-driven Prioritization reduces noise, automates alert triage and is 85% more effective at prioritizing the threats that matter most to the business.

## Prioritize real threats, not weird events

Rooted in security research and data science on attacker behavior, Attack Signal Intelligence goes beyond simple anomaly detection to detect real attacks and progression throughout the cyber kill chain.

### AI-driven Detection

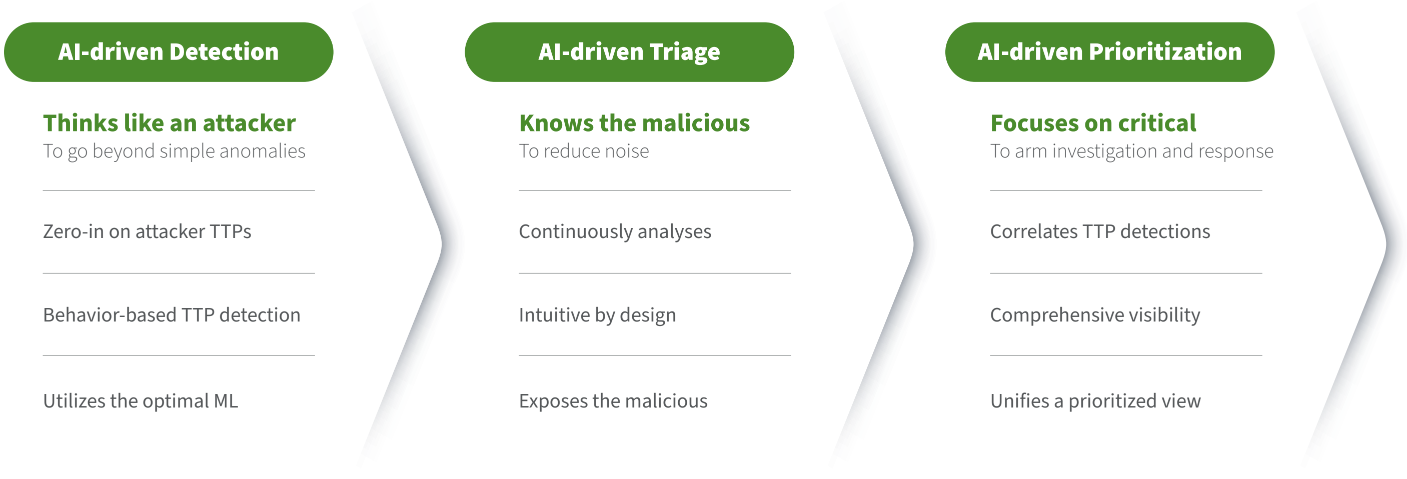
- Zero in on attacker TTPs used to progress attacks.
- Behavior-based models accurately detect attacker TTPs.
- Utilize the optimal ML approach for the right detection.

### AI-driven Triage

- Continuous analysis of all active detections for commonalities.
- Intuitive by design to distinguish malicious vs. benign activity.
- Automated to expose the malicious and log the benign.

### AI-driven Prioritization

- Correlated detections of attacker TTPs across domains.
- Comprehensive visibility of the complete attack narrative.
- Unified view of prioritized threats by severity and impact.



**AI-driven Detection**

**Thinks like an attacker**
To go beyond simple anomalies

Zero-in on attacker TTPs

Behavior-based TTP detection

Utilizes the optimal ML

**AI-driven Triage**

**Knows the malicious**
To reduce noise

Continuously analyses

Intuitive by design

Exposes the malicious

**AI-driven Prioritization**

**Focuses on critical**
To arm investigation and response

Correlates TTP detections

Comprehensive visibility

Unifies a prioritized view

## Turn the tables on attackers with AI-enabled operations

Arm security leaders, architects and analysts to get ahead and stay ahead of modern cyberattacks.

**Integrated Investigations** puts answers at analysts' fingertips.

- Focus on critical threats ranked by severity and impact.
- Hunt for threats dwelling across the attack surface.
- Investigate with context and forensics in a single user interface.

**Automated Workflows** reduces complexity and cost by automating manual tasks.

- Consolidate analyst work streams in a single interface.
- Simplify SIEM data feeds, dashboards, reporting.
- Customize integrations to existing ticketing and reporting workflows.

**Targeted Response** puts humans in control of response with analyst-driven enforcement.

- Flexible response actions triggered automatically or manually like locking an account, isolating an endpoint or triggering a SOAR or ITSM playbook.
- Leverage out-of-the-box integrations with top EDR and SOAR providers.
- Managed response leveraging Vectra MDR services.

Unlike other approaches that center on simple anomaly detection and require human tuning and maintenance, Vectra Security AI-driven Attack Signal Intelligence automates threat detection, triage and prioritization without human intervention. By harnessing this technology, security teams are empowered to erase the unknown, turn the tables on attackers and make the world a safer and fairer place.

## About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. 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 enable 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 cyberattacks.

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