# Who we are, why we exist and what we do

## The best Attack Signal Intelligence™ on the planet.

AI-driven cybersecurity platform and services

For the past two decades, cyber security defense has relied on what is known. Threat detection and response methodologies across people, process and technology have relied heavily on signatures, anomalies, rules to see and stop cyber criminals from infiltrating the organization and exfiltrating data. The problem with this approach is that it 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 cloud vulnerabilities and exploits
- More evasive and sophisticated attackers
- More accounts compromised, more privileged access
- More rapid progression of attacks

If there is one thing about the security industry, the approach to more has always been more.

- More attack surface to cover, buy more tools, accumulate more data to analyze
- More evasive and sophisticated attackers, create more signatures, anomalies, rules
- More alerts to triage, prioritize, investigate, and respond to, hire more people.

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

**“We don’t know where we are exposed or compromised - right now.”**

The unknown threat is the result of an attacker’s ability to bypass prevention, circumvent signatures, blend in and infiltrate, and progress laterally inside an organization to wreak havoc. We argue the unknown threat is the biggest risk to organizations today and is creating security complexity, noise and burnout. Attackers have the upper hand and in order to turn the tables on attackers, we must erase the unknown threat, The challenge is how do we...

- Cover more attack surface without adding more complexity?
- Detect more evasive attackers without creating more rules and noise?
- Ensure defenders keep pace without burning them out?

For over a decade, Vectra has been researching, developing, pioneering, and patenting Security AI centered on erasing the unknown. We call it Attack Signal Intelligence and when harnessed, it empowers defenders to:

- Think like an attacker, their tactics, techniques, and procedures (TTPs).
- Know what is malicious and relevant to reduce noise and burnout
- Focus on the urgent to focus on what's critical and lower business risk

Unlike other approaches that center on simple anomaly detection and require human tuning and maintenance, Vectra's Attack Signal Intelligence exposes the complete narrative of an attack. We do this by continuously monitoring for attacker TTPs, executing pre-defined models in real-time to detect and correlate those TTPs and automatically surface the threats that matter most to the business.  As a result,

### Your organization is more resilient to attacks

- Up and running with actionable attack signal in days if not hours
- Future-proof your cyber defense as your attack surface expands
- Reinforcements at the ready with Vectra MDR services

### Your processes and workflows are more efficient

- Reduce SIEM costs and detection rule creation and maintenance
- Automate analysts' manual tasks and time to investigate and respond
- Optimize existing investments in EDR, SOAR and ITSM

### Your security analysts are more effective

- Reduce analyst burnout with accurate detection of malicious true positives
- Increase analyst throughput by accelerating investigation and response
- Builds analyst expertise and skills hunting and defending against advanced attacks