

KPMG and Vectra: Delivering Effective Security Observability and Unmatched Signal Clarity

The shift to hybrid cloud environments has led to an expanded attack surface, making it easier for attackers to infiltrate, compromise credentials and steal sensitive data. Defining an actionable cyber strategy refined to your business needs is now more crucial than ever.

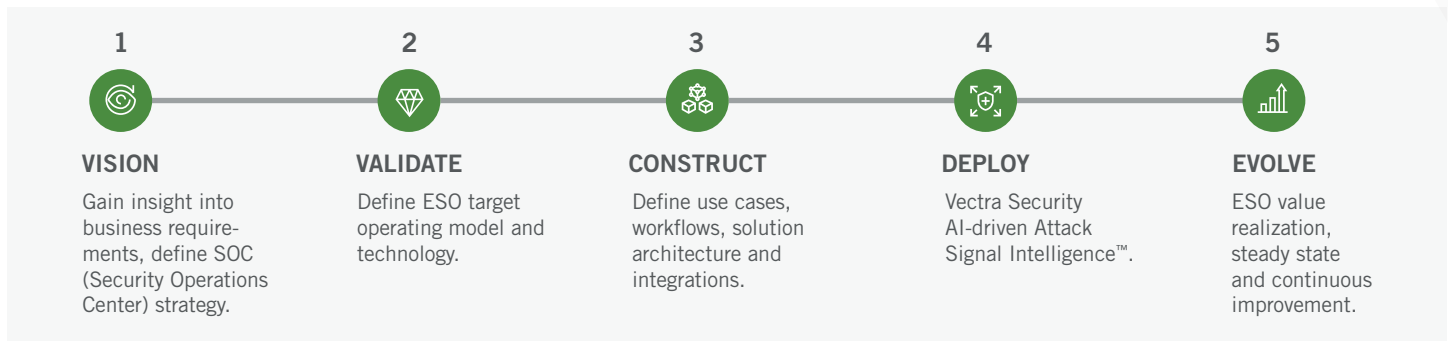
KPMG Effective Security Observability and Vectra Security AI-driven Attack Signal Intelligence™ together empower global organizations to align a cyber strategy while taking a risk-based approach to cyberattacks, reduce manual tasks, alert noise and analyst burnout so security teams can focus on the most urgent threats to their organization.

Key challenges addressed:

- Cybersecurity strategy
- Visibility gaps
- Inefficient security processes
- Attack signal clarity
- Security analyst burnout

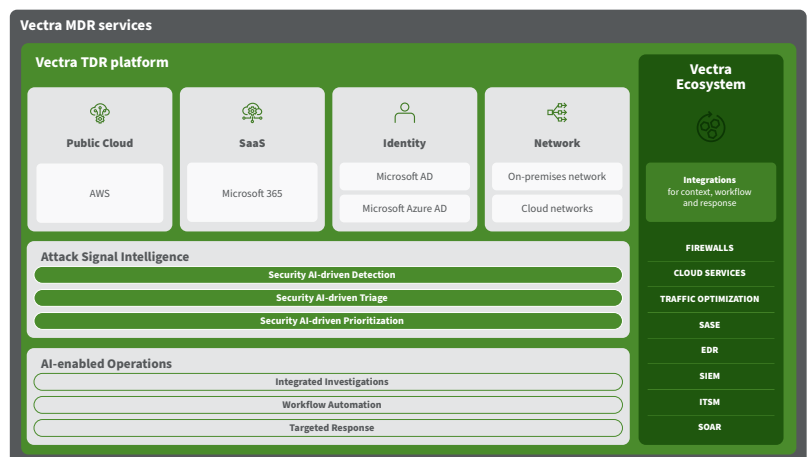
KPMG Effective Security Observability (ESO)

Delivering effective security observability (ESO) is a key to the success of any cyber strategy. Doing so requires five key steps:



The Vectra platform harnessing Security AI-driven Attack Signal Intelligence™

KPMG Effective Security Observability includes the deployment of the Vectra platform and Attack Signal Intelligence as a key element of the service engagement. The Vectra Platform empowers KPMG and its customers with the right **coverage**, **clarity**, and **control** across today's global hybrid and multicloud environments, exposing the complete attack narrative across the entire cyber kill chain.



Only Vectra provides:

- **Attack Coverage across 4 of your 5 attack surfaces:** cloud (IaaS and PaaS), SaaS, identity and networks — monitoring for attacker TTPs throughout the entire cyber kill chain and across hybrid and multicloud attack vectors.
- **Signal Clarity with Attack Signal Intelligence:** patented AI-driven technology automates threat detection, triage and prioritization, empowering security analysts to focus on the most urgent threats to the organization.
- **Intelligent Control with AI-enabled operations:** integrated investigations, automated workflows and targeted response actions optimize security investments in tools, processes and playbooks to boost SOC efficiency and effectiveness.

Effective cybersecurity strategy

KPMG's Effective Security Observability with Vectra Attack Signal Intelligence helps global organizations create a successful cyber strategy. Together, this solution prioritizes critical cyber threats and makes security teams more capable of detecting and preventing modern, multicloud attacks before a breach occurs.

Resiliency: Future-proof your expanding attack surface across 4 of 5 attack surfaces — cloud (IaaS and PaaS), SaaS, identity and networks.

Efficiency: Cut time, cost and complexity and gain 85% more SOC efficiency.

Efficacy: Arm human intelligence to be more effective boosting SOC analyst productivity 2x.

This unique partnership provides an end-to-end comprehensive security observability strategy. By understanding a customer's unique business environment and by utilizing the right combination of people, process, and technology, KPMG and Vectra simplify security complexity, provide attack signal clarity, and automate threat detection, triage and prioritization. With this combination, security analysts can quickly resolve urgent threats, freeing them from unproductive work, while gaining clarity into what really matters.

KPMG Cyber Security

The Vectra Platform with Attack Signal Intelligence™

Engage - Submit a request for proposal from KPMG

About Vectra

Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS (software as a service), 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 (Managed Detection & Response) services to stay ahead of modern cyberattacks. Visit www.vectra.ai.