

Vectra AI-driven Prioritization

How Attack Signal Intelligence arms SOC teams to focus on what is urgent

Vectra AI-driven Attack Signal Intelligence™ exposes the complete narrative of an attack, providing your analysts with a level of signal clarity that helps your SOC team focus on the critical and most urgent threats. Built-in capabilities of AI-driven Prioritization automate alert prioritization efforts with each detection, arming SOC teams with an efficient means to discern where to focus resources and what matters most to the business.

As events continue to unfold, AI-driven Prioritization ensures SOC teams can quickly discern what is urgent in the ever-growing pool of threats they face. It analyzes, scores and ranks for you, so you know where to commit valuable resources and avoid delaying efforts where they're needed most. Furthermore, SOC analysts can reduce the mean time to identify (MTTI), contain (MTTC) and respond (MTTR) to active attacks across their hybrid and multi-cloud environments, minimizing impact to business.

Key Benefits

- **Automated** – no rules to create, tune or maintain
- **Intuitive** – eliminates guesswork for SOC Analysts
- **Unified** – correlates attacker TTPs across all domains and data sources
- **Simple** – sorts and ranks attacks by severity and impact

How it works

AI-Driven Prioritization factors in Attack Velocity – Accurately deduce and analyze the acceleration of an attack progression as an essential component of labeling an urgent priority in the overall risk scoring process where time is of the essence.

Influence your own scoring methods – Your SecOps team can define the key assets and group entities that are the most critical to your business and ensure these assets are the most important consideration as part of the definition for incident priorities.

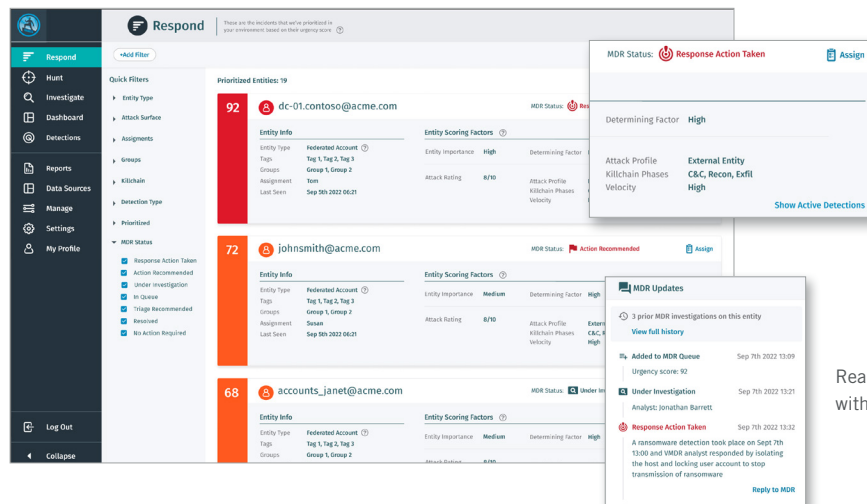
Thorough understanding of roles – With robust behavior-based models, gain a full understanding of each end-user in your organization's roles and permissions to quickly spot when something has taken a "left turn".

Turn the tables on attackers – Vectra AI-Driven Detections detect up to 90% of attackers' tactics and techniques listed in MITRE ATT&CK to enable your SecOps team to think like an attacker.

Valid & vetted incident scoring – Vectra AI pinpoints all data sources across all domains to define what behavior contributes to a critical and progressive urgent incident.

Rich context from all data sources – Vectra AI provides your SecOps team with the full attack storyline, highlighting the utmost gravity of the incident for the most precise incident response.

Easily know which threats pose the biggest risk and cut down response time.

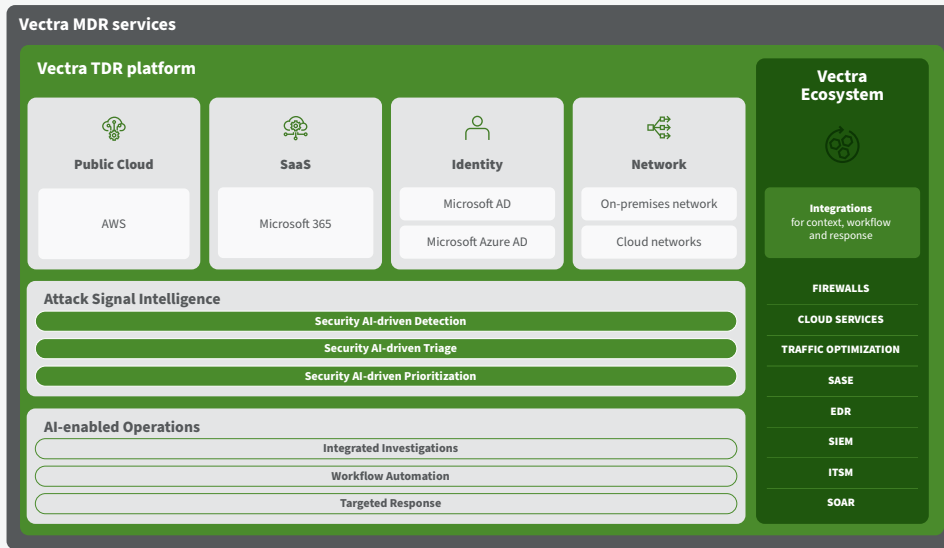


Clear response action visibility for prioritized threats.

Real time collaboration with Vectra analysts.

Summary

In the enterprise world a threat is a culmination of several related individual elements. These elements span across the attack surface and different domains such as hosts, accounts, networks, and cloud. Therefore, organizations must level up their current incident prioritization by identifying and defining incidents that are both critical and urgent across all these domains. Only Vectra AI-driven Attack Signal Intelligence™ provides the means necessary for SOC teams to have a hard and fast order of incident priorities needed to investigate and respond to the most urgent attacks, thus reducing risk for the organization.



Explore the Vectra AI-driven Threat Detection and Response Platform and MDR services powered by Attack Signal Intelligence.



About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. 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 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 services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.