Vectra Attack Signal Intelligence™ Integration with Amazon Security Lake

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*."

This is the unknown. We argue unknown threats are the biggest risk to organizations today. The challenge for security teams defending against the unknown comes down to three things:

How to cover more attack surface without adding more complexity?

How to detect more evasive attackers without creating more alert noise?

How to ensure SOC analysts keep pace without burning them out?

The unknown threat is how attackers get the upper hand:

- Bypassing prevention
- Gaining access to cloud environments
- Progressing laterally
- Hiding behind alert noise
- Stealing data

Erasing unknown cloud threats

With Vectra Security AI-driven Attack Signal Intelligence™, customers gain advanced investigations for AWS environments with less complexity and increased visibility. Vectra Attack Signal Intelligence takes a risk-based approach to cyberattacks while reducing manual tasks, alert noise and analyst burnout, empowering 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 threats matter

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

In minutes, integrating Attack Signal Intelligence with open-source OCSF communications into Amazon Security Lake provides customers with a consolidated and simplified approach to threat detection, investigation and response.

Native integration to detect real threats

Vectra Attack Signal Intelligence natively integrates with Amazon Security Lake, providing a consolidated solution to detect, investigate and respond to real threats in AWS. Amazon Security Lake customers gain:

- Access to Vectra's Attack Signal Intelligence.
- Simplified, native integration from Vectra to Amazon Security Lake.
- Consolidated data store allowing security teams standardized access to real threat data.
- Real-time signal delivery to Amazon Security Lake.

Get unified visibility across your entire AWS estate

Vectra ensures all AWS traffic and various data logs are continually monitored and examined for active account misuse and advanced tactics and techniques that typically go unseen.
for the right detection.

Uncover incidents and know when you have been compromised

Gain access to terabytes of data from your AWS environment and streamline efforts to categorize, analyze and respond to incidents with the full context behind any AWS-based threat.

Advanced investigations for AWS attacks

Eliminate the guesswork for your SOC analysts with Vectra AI-driven detections, AI-driven triage and AI-driven prioritization for faster and more precise investigation and remediation in one single security AI-driven solution.

Stay ahead of attacks with simplified security operations

Get ahead and stay ahead of attacks

- **Attack coverage** – erase unknown threats across AWS.
- **Signal clarity** – automatically detect, triage and prioritize unknown threats.
- **Intelligent control** – arm human intelligence to hunt, investigate and respond to unknown threats.

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.

Your organization is more resilient to attacks

- Up and running with actionable detections in minutes.
- Future-proof your cyber defense as your attack surface expands.
- Know exactly what threats matter across AWS.

By integrating Vectra Attack Signal Intelligence into Amazon Security Lake, security teams gain real time access to real threat data with the ability to respond at speed, ensuring that a compromise does not turn into a breach. After deploying Vectra in 15 minutes, customers will be able to send high-fidelity alerts to Amazon Security Lake as a custom source using a dedicated CloudFormation template. Once installed, alerts will appear immediately in Amazon Security Lake in OCSF (Open Cybersecurity Schema Framework) format. By utilizing Vectra and AWS, customers get access to Attack Signal Intelligence in a consolidated security lake.

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