VECTRA | CROWDSTRIKE

Vectra AI and CrowdStrike Falcon Next-Gen SIEM

Key Challenges

Visibility is the crux of catching cyberattacks before they become full-blown, business-critical incidents, especially getting visibility on all attack surfaces now that many organizations are a mixture of on-prem and cloud environments. Legacy log management systems and previous detection and response technologies are inundated with noise and complexity, obscuring the visibility and stunting the speed needed for analysts to monitor their security system's health and catch threats before they escalate. The costs of data ingestion and retention for these legacy log management systems are astronomical when SOC teams need to store and analyze a lot of data in today's data-centric world.

Solution Overview

Vectra AI's integration with CrowdStrike's next-generation SIEM, Falcon Next-Gen SIEM, eradicates the challenges SOC teams encounter with legacy log management systems today. With CrowdStrike's next-gen SIEM, analysts can see and analyze petabytes of data coming in from cloud vendors, EDRs, identity, SaaS applications, and network metadata. Vectra AI provides best-in-class AI-driven network telemetry for Falcon Next-Gen SIEM users so that organizations can be protected on all fronts. Gone are the days were queries take minutes, maybe even hours, precious moments in catching an attack before it becomes business-critical. With Vectra AI and CrowdStrike's Falcon Next-Gen SIEM, SOC team can modernize their security program and be leaps ahead of an attacker.

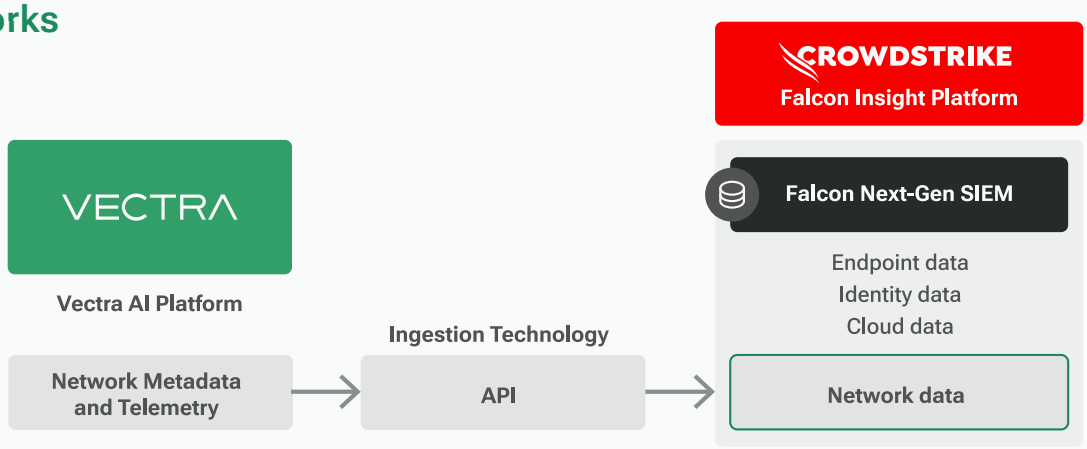
Solution Components:

- Vectra AI Platform with Attack Signal Intelligence
- Vectra NDR
- CrowdStrike Falcon Next-Gen SIEM

Key Benefits:

- Single view of priorities, across hosts, accounts and data sources for network detections on the Vectra AI Platform
- Seamlessly transition between the Vectra AI Platform and CrowdStrike Falcon Next-Gen SIEM for deeper investigations
- Light-speed, real-time log management spanning across network, endpoint, cloud, SaaS, and identity

How it Works



1. Vectra AI's Network Detection and Response feeds network metadata and telemetry into CrowdStrike's Falcon Next-Gen SIEM.
2. From there, users can single-click pivot from a detection into CrowdStrike's next-gen SIEM to do a deeper investigation of their organization's security health.
3. Data visualizations and lightning-speed log queries on the Falcon Next-Gen SIEM platform expedites investigations, allowing users to take rapid action prior to a full-blown attack.

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

About CrowdStrike

CrowdStrike, a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. For more information, visit www.crowdstrike.com.

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