VECTRA SECURITY THAT THINKS® | CROWDSTRIKE

SOLUTION BRIEF

Detect and Mitigate Cyberattacks with Vectra AI and CrowdStrike

The Vectra® Threat Detection and Response® platform integration with Falcon Insight™ endpoint detection and response from CrowdStrike® enables security teams to unify network and endpoint context to detect, verify and isolate cyberattacks in the enterprise quickly and automatically.

Together, Vectra and CrowdStrike solve the most persistent security problems facing enterprise organizations today: finding and stopping active cyberattacks and optimising the time and resources of IT security teams.

Challenged by Lack of Full Visibility

When it comes to hunting down and responding to network cyberattacks, even a highly qualified team of security analysts can be overburdened by manual, inefficient processes and lack of visibility. Analysts need real-time visibility and context across any surface an attacker could infiltrate. By harnessing Vectra's patented Security AI with CrowdStrike, security teams gain full visibility of threats across network and endpoints.

Erase the Unknown by Integrating Vectra and CrowdStrike

From within the CrowdStrike dashboard, customers can leverage Vectra to gain **coverage** with attack visibility and context across surfaces, **clarity** that reduces alert noise and prioritizes critical threats and **control** to see and stop threats across an existing stack.

KEY BENEFITS

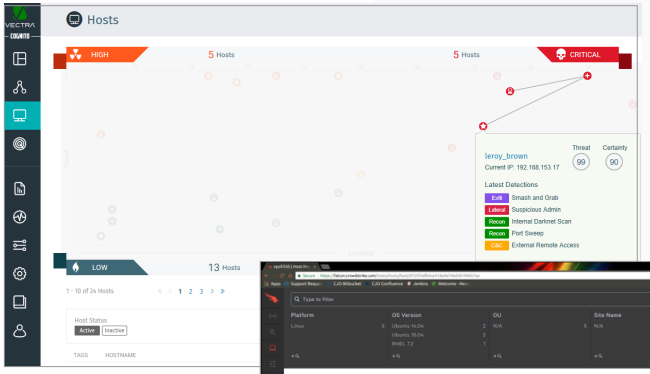
- Single view of priorities, across hosts, accounts, and data sources.
- Seamlessly transition between Vectra and CrowdStrike for deep investigations.
- Automated threat detection and response solution for both the network and endpoint.

- **Coverage:** Vectra's AI-driven detections are triaged to deliver a high-quality signal in the CrowdStrike dashboard, providing deep context about every attack across multiple attack surfaces—public cloud, SaaS, identity, network, and endpoints.
- **Clarity:** Security teams can easily prioritize critical threats due to an 80% reduced noise rate. The integration of Vectra's Security AI provides attack intelligence data to CrowdStrike, so teams can address real threats faster.
- **Control:** Analysts gain an optimized process to see all threat data across existing stacks and surfaces in the CrowdStrike dashboard and can connect to the Vectra platform for complete threat investigations.

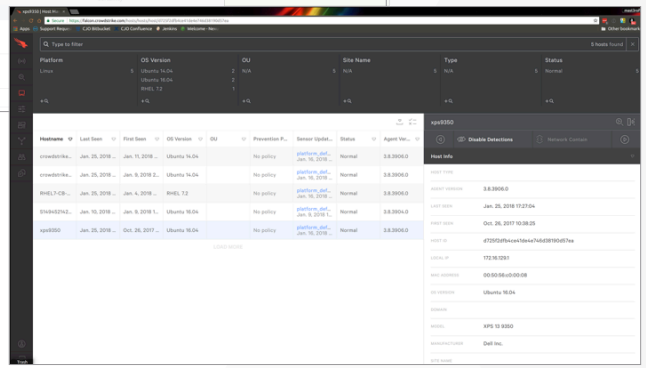
All too often security teams operate in the unknown. The unknown caused by ever-expanding attack surfaces, evasive and evolving attacker methods and overwhelming alert noise that attackers use to hide in plain sight. The unknown is what gives attackers the upper hand. By combining Vectra Security AI with CrowdStrike endpoint detection and response—security operations teams can erase the unknowns and turn the tables on attackers.

Capabilities

- Single unified view across endpoint and network activity with active detections across all data sources to allow incidents to be found before they can cause harm.
- The view is organized by severity and threat score, allowing administrators to easily see the most critical threats and those that require immediate attention.
- Ability to drill down into CrowdStrike from the entity list and see all attacker behaviors observed for a specific entity.
- Seamlessly access and analyze data from the network and endpoint to accelerate incident investigation and response time.
- Use the network and endpoint context to isolate compromised hosts from the network to halt cyberattacks and avoid data loss.



The Vectra platform shows threat detection details of a specific host and the progression of threat and certainty scores over time



Falcon Insight reveals traits and behaviors of a threat that are only visible inside the host

About the Vectra Platform

The Vectra Platform is AI-driven threat detection and response for hybrid and multi-cloud environments. Harnessing patented Security AI, the Vectra Platform pinpoints attacker methods, prioritizes threats, and automates response controls leveraging your existing security stack. With the Vectra Platform, you get unified attack visibility, context across public cloud, SaaS, identity, network, and endpoints, and controls to respond immediately in the most effective way.

About CrowdStrike Falcon Platform

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon Platform leverages real-time indicators of attack, threat intelligence on 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 – all through a single, lightweight agent. With CrowdStrike, customers benefit from superior protection, better performance, reduced complexity, and immediate time-to-value.

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