VECTRA

CROWDSTRIKE

Detect and mitigate cyberattacks with Vectra and CrowdStrike

CHALLENGE

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. These analysts need real-time visibility anywhere an attacker could hide.

SOLUTION

Cognito and Falcon Insight integrate two authoritative views of a cyberattack – the network and the endpoint. Cognito analyzes all network traffic to automatically detect attack behaviors and prioritizes each one based on the risk they pose.

In addition to putting network-based threat context at your fingertips, Cognito conveniently allows security teams to pivot into the endpoint context of Falcon Insight to perform additional investigation and isolate the compromised host from the network.

BENEFITS

The integration of Cognito and Falcon Insight saves time, effort, and allows security teams to take action before cyberattacks lead to data loss. Together, Cognito and Falcon Insight create an efficient security operations workflow that reduces response and investigation time, enabling security teams to quickly mitigate high-risk threats.

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

Together, Cognito and Falcon Insight solve the most persistent security problems facing enterprise organizations today: Finding and stopping active cyberattacks while getting the most out of limited time and manpower of IT security teams.

Reducing the time to detect and respond to attacks

The success or failure of security teams often boils down to the speed of incident response. Sophisticated attackers thrive by staying under the radar. Detecting them often requires hours to days of manual threat hunting by highly trained security analysts, who often need to pivot between consoles of different tools in the enterprise security stack.

On average, it takes 99 days between the time a network is compromised and the time the attack is detected. In addition, 67% of data breaches are discovered by a law enforcement agency or other third party.

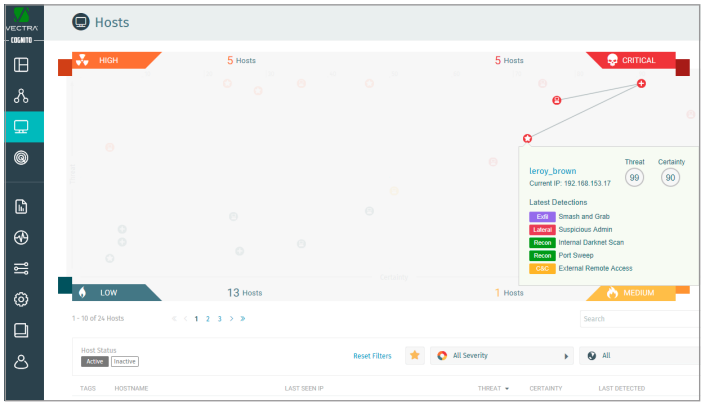
Vectra technology and product

The Cognito automated threat detection and response platform from Vectra provides the fastest, most efficient way to detect and stop attackers in your network.

Cognito automates the manual, time-consuming tasks associated with a Tier-1 analyst's role by providing real-time attack visibility. It prioritizes the highest-risk threats and puts contextual attack details at your fingertips to empower immediate action.

Uniquely combining data science, modern machine learning techniques and behavioral analysis based on artificial intelligence, Cognito performs nonstop, automated threat hunting to quickly and efficiently find hidden and unknown attackers before they do damage.

Cognito also delivers enterprise-wide visibility by directly analyzing all network traffic to gain high-fidelity visibility into the actions of all host devices – from the cloud and data center workloads to user and IoT devices – leaving attackers with nowhere to hide.



Cognito shows threat detection details of a specific host and the progression of threat and certainty scores over time

CrowdStrike technology and product

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. Falcon Insight solves this by delivering complete endpoint visibility across your organization.

Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to detect and prevent advanced threats as they happen.

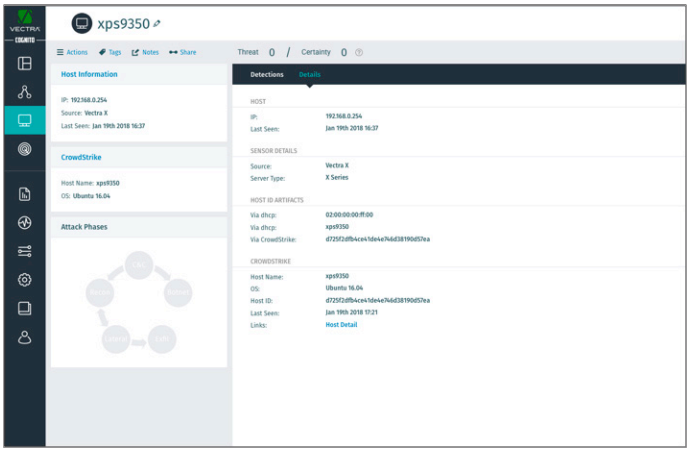
All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

Easily integrate network and endpoint context

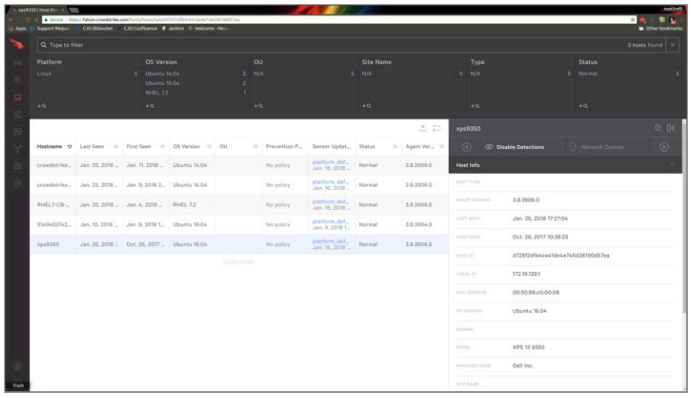
When a threat is detected, Cognito and Falcon Insight provide security teams with instant access to additional information for verification and investigation. Host identifiers and other host data from Falcon Insight are shown automatically in the Cognito UI to enrich Vectra's detection information from the network perspective.

Next, a single click allows security teams to easily pivot between the Cognito UI and the Falcon Insight UI for the same host or to securely connect directly to the host using the Falcon Insight response capability.

In both cases, Falcon Insight easily reveals traits and behaviors of a threat that are only visible inside the host. This enables security teams to quickly and conclusively verify a cyberthreat while also learning more about how the threat behaves on the host itself.



Host identifiers and other host data from Falcon Insight are shown in the Cognito UI



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

Take action

In addition to reducing the time to investigate threats, Cognito and Falcon Insight enable security teams to take swift, decisive action. Armed with network and endpoint context, security teams can quickly isolate compromised hosts from the network to halt cyberattacks and avoid data loss.

About Vectra

Vectra® is an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 168X. Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint, NAC, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

About CrowdStrike

CrowdStrike® is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The CrowdStrike Falcon platform deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack (IOA) -based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, Falcon instantly correlates over 70 billion security events from across the globe to immediately prevent and detect threats.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai