Detect and mitigate cyber attacks with Vectra and Carbon Black

CHALLENGE

Today's cyber attackers are adept at evading prevention security defenses along the network perimeter, and security teams are often overloaded with inconclusive alerts and slow investigations.

Once attackers get inside the network, they often go undetected for many months – giving them plenty of time to steal key assets and cause irreparable damage and embarrassment.

SOLUTION

Vectra and Cb Response integrate two authorative views of a cyber attack – the network and the endpoint. Vectra analyzes all network traffic to automatically detect attack behaviors and prioritizes each one based on the risk they pose to your organization.

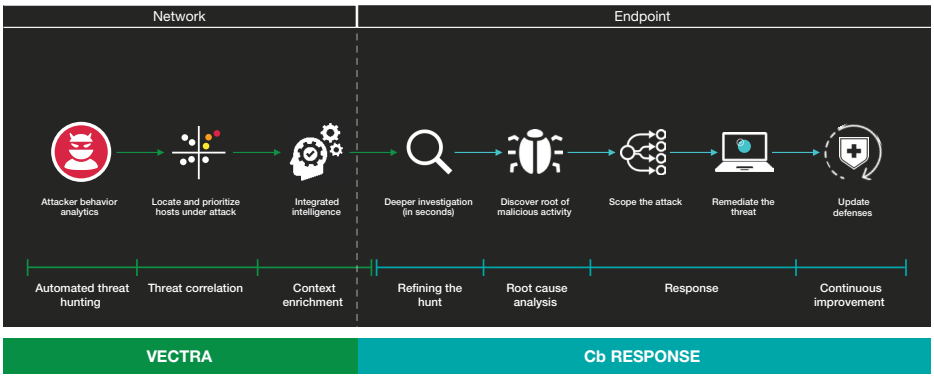
In addition to putting network-based threat context at your fingertips, Vectra conveniently allows security teams to pivot into the endpoint context of Cb Response to perform additional investigation and isolate the compromised host from the network.

BENEFITS

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

The integration of Vectra® Networks automated threat management with Cb Response from Carbon Black enables security teams to unify network and endpoint context to quickly detect, verify, and isolate cyber attacks in the enterprise.

Together, Vectra and Cb Response solve the most persistent security problems facing enterprise organizations today: Finding and stopping active cyber attacks while getting the most out of limited time and manpower of IT security teams.



Automated, real-time threat hunting and remediation across the enterprise

The need for a new approach to security

Modern cyber attackers can easily evade prevention security defenses at the network perimeter. Unable to rely solely on prevention defenses, security teams must manually investigate threats and sift through the noise in search of a weak signal.

In practice, this often means that cyber attacks are first detected and reported by an external third party, turning their discovery into a post-breach forensic drill rather than a proactive attack mitigation exercise.

A new model of threat detection

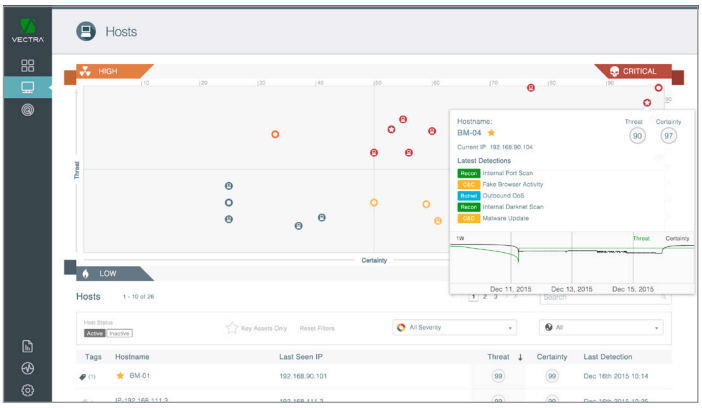
Vectra automates the hunt for hidden cyber threats by continuously analyzing all network traffic to detect attacker behaviors inside the network.

In addition to automatically correlating detected threats with host devices that are under attack, Vectra provides unique context about what attackers are doing, and prioritizes threats that pose the biggest risk. This enables security teams to quickly focus their time and resources on preventing or mitigating loss.

Using artificial intelligence, Vectra combines data science, machine learning and behavioral analytics to reveal the attack behaviors without signatures or reputation lists. Vectra even detects threats in encrypted traffic without using decryption.

Vectra applies this intelligence to all phases of an attack ranging from command-and-control (C&C) traffic, internal reconnaissance, lateral movement, and data exfiltration. All detections are correlated and scored in order to pinpoint the specific physical hosts at the center of an active attack.

This enables security teams to detect unknown, customized and known cyber attacks as well as threats that do not rely on malware, such as those carried out by malicious insiders and compromised users.



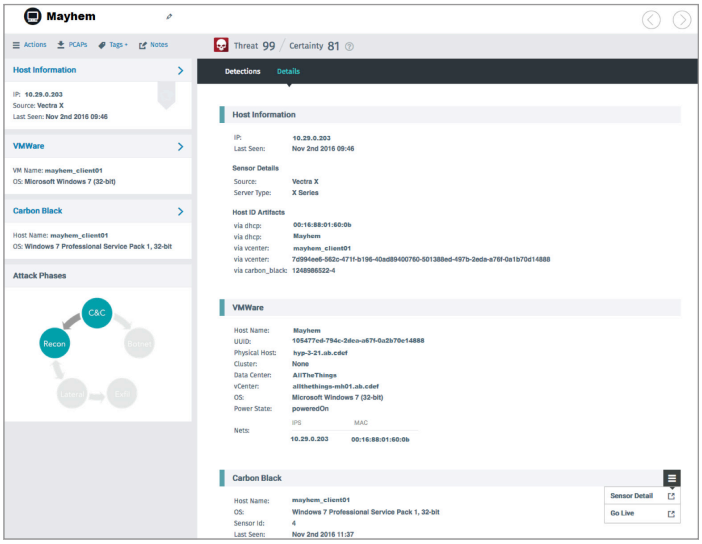
Vectra shows threat detection details of a specific host and the progression of threat and certainty scores over time

Easily integrate network and endpoint context

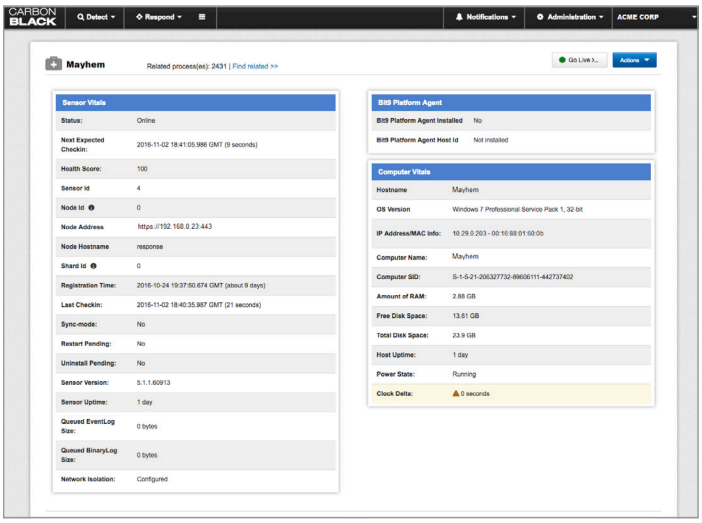
When a threat is detected, Vectra and Cb Response provide security teams with instant access to additional information for verification and investigation. Host identifiers and other host data from Cb Response are shown automatically in the Vectra UI.

Next, a single click allows security teams to easily pivot between the Vectra UI and the Cb Response UI for the same host or to securely connect directly to the host using the Cb Response Live Response capability.

In both cases, Cb Response 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 cyber threat while also learning more about how the threat behaves on the host itself.



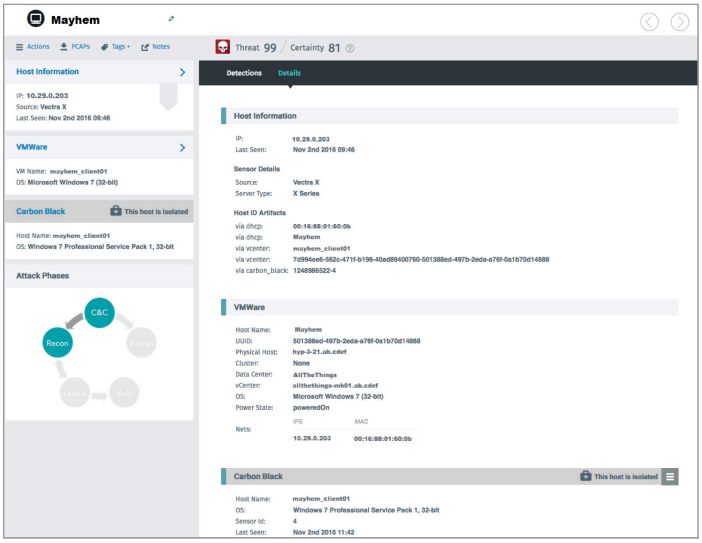
Host identifiers and other host data from Cb Response are shown in the Vectra UI



Cb Response 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, Vectra and Cb Response let security teams take swift, decisive action. Armed with network and endpoint context, security teams can quickly isolate compromised hosts from the network to halt cyber attacks and avoid data loss.



The Vectra UI shows that Carbon Black isolated a compromised host that was initially detected and assigned threat and certainty scores by Vectra

About Vectra Networks

Vectra Networks automates the hunt for hidden cyber attacks inside campus networks, data centers and the cloud by continuously monitoring internal traffic to detect active threats as they are happening. Vectra automatically correlates threats with host devices that are under attack, provides unique context about what attackers are doing, and prioritizes threats that pose the biggest risk. This enables security teams to quickly focus their time and resources on preventing or mitigating loss. The editorial team at Dark Reading recently presented Vectra with the Best of Black Hat 2016 award for Most Innovative Emerging Company.

About Carbon Black

Carbon Black has designed the most complete next-gen endpoint-security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

Email info@vectranetworks.com **Phone** +1 408-326-2020
www.vectranetworks.com