CSO FROM IDG

August 23, 2018 www.csoonline.com

REVIEW

Review: Using AI to outsmart threats with Vectra Cognito

Part traffic monitoring tool, part IDS, part SIEM, the Vectra Cognito platform defies classification.

By John Breeden II

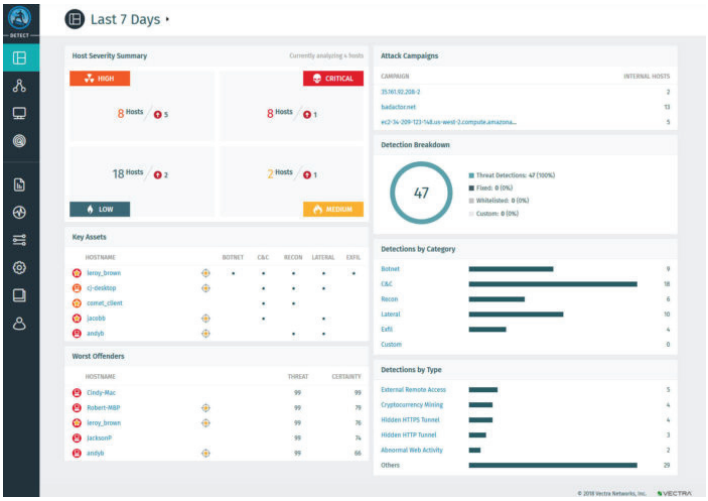
Don't expect the pace of change to slow down in the cybersecurity industry. Even the so-called traditional protection methods will need to incorporate new technologies and methodologies. Many new cybersecurity programs will span multiple categories, or even resist neat categorizations at all.

The Vectra Cognito platform is a perfect early example of this trend. It incorporates artificial intelligence (AI), deep machine learning and traffic monitoring into a tool that is able to detect threats that other programs miss, even if they are already entrenched inside a protected network. Cognito would probably be classified as a traffic monitoring tool, though that is a poor fit.

With its ability to dynamically detect threats and track them as they expand or are remediated within a network, Cognito acts more like a competent intrusion detection system (IDS). An even better description might be that it provides a look at how IDS systems in the future may operate when faced with advanced intrusions. There is even a threat hunting component, which further complicates any easy categorization.

Regardless of what you call it, the Cognito suite from Vectra is installed as two main components. The first is comprised of network sensors that collect both vertical and horizontal traffic. They can be tiny hardware sensors or virtualized ones. Sensors report to the brains of the suite, which is a 1U appliance where all the artificial intelligence about what is going on in the network is applied.

Currently, the brains of Cognito is only available as hardware. Each appliance can handle data from up to 500 sensors, so many organizations will likely only need one. Reports are compiled by the appliance and sent to the dashboard interface, making it act like a more traditional Security Information and Event Management (SIEM) console in that respect. Cognito can also send its data to many other SIEM or security appliances if desired.



John Breeden II/IDG

Looking like a traditional Security Information and Event Management console, the Cognito Detect dashboard is actually a window into dynamic threat tracking.

Pricing is based on the number of protected devices that are tracked by the suite. It's worth noting that with device-level pricing, it means the sensors are essentially free, so organizations should feel free to install as many as they want to capture every aspect of network traffic.

Testing Cognito

The platform itself is broken down into two components called Detect and Recall. They can operate independently of one another, but are designed to work together, with Detect finding threats and Recall assisting in deeper investigations and threat hunting. As such, it's much more likely that an organization will have Detect and not Recall if they are only installing one component. Much of our testing was on the Detect side, though we did conduct a few hunts using Recall.

Detect is designed to operate behind the front lines, looking for especially advanced or malicious programs and users that have already bypassed perimeter defenses. For the most part, users are only going to be detecting the kind of advanced persistent threats that cause the most problems in enterprise networks since they can remain undetected for months. Detect can find, quite easily, all the low-level threats too, but those should be blocked before landing on internal assets if there is any level of defense already in place.

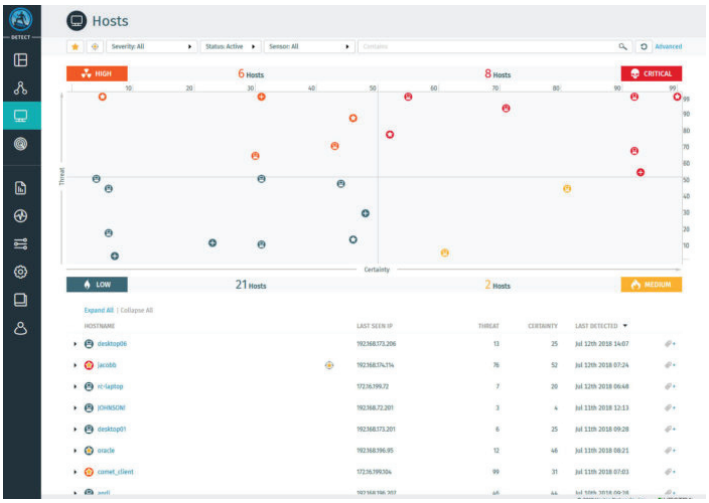
Cognito Detect looks at security a little bit differently than most programs. For one, it tracks devices, not IP addresses, collecting the MAC address of computers and other identity factors like host names. That way, even if a device moves to a different office or starts operating from a remote location, Detect will know what it is, what it does, and have access to its complete history.

To find threats, Detect looks for behaviors that all infiltrators must follow. Even if they have already compromised a machine within a network, they can't do much without performing lateral movement, which can only be accomplished using a handful of techniques, though hackers are getting quite adept at moving "low and slow" to avoid detection. Detect works because it meshes many detection algorithms and engines, and ties them all together with an AI that seemed unfoolable in our tests.

In terms of detection, it can find hidden DNS tunnels, suspicious relay requests, stealth HTTP postings, matches against threat feeds, port scans and sweeps, suspicious LDAP queries, RDP recon, shell knocker activity, SQL injections, data smuggling, outbound DOS and spam, cryptocurrency mining activity and many others. The secret is using the AI to not only coordinate all those events at machine speed, but also to pull in related events and behaviors and decide if that is an indication of a larger problem or even a full-scale threat campaign. It can do almost everything from the first day of installation, but a few of the bad behaviors that it can uncover, such as an administrator acting suspiciously, require a short learning period (ideally a week long) to establish a baseline.

Discovered threats are grouped into a quadrant system where dots represent compromised hosts from critical down to low priority. All threats displayed in the grid are dynamic, meaning Detect's AI keeps a watch over them, moving them automatically into new quadrants if the threat level increases, such as if new behavior is detected like data exfiltration, or if more hosts start displaying similar symptoms.

In a testbed environment, Detect was able to find horizontal movement, even if an attacker covered their tracks and disabled services after making a probe. It could



John Breeden II/IDG

The Cognito Detect program breaks down threats into four quadrants based on their severity and the program's certainty that an event is malicious. Threats are tracked and can dynamically move throughout the four quadrants, or disappear if remediated.

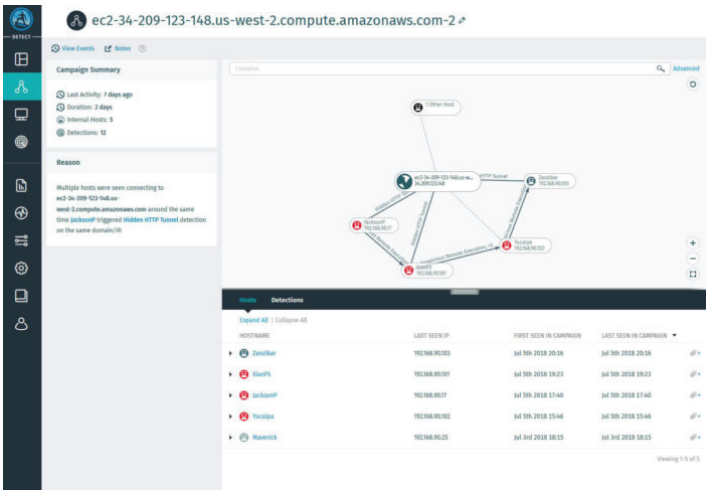
also differentiate between a normal human visiting websites and a malicious program that was trying to beacon out to a command and control server, but doing it at random intervals to try and appear like normal traffic. It could not trick the Detect AI.

And Vectra does a good job of letting human users know what the AI is doing and why. Every detection comes with a detailed explanation about how it was discovered, why it should be a concern and how to remediate the problem. This could allow junior analysts to punch above their weight when dealing with tricky threats.

John Breeden II/IDG

The Cognito suite can be used by security staffers at various levels of experience. Every detected event comes with a lengthy explanation about what it is, what dangers it poses, and how to remediate the problem.

Beyond just detection, Detect was able to group related activity that was occurring in the network. For example, the dashboard let us know that another host on the network tried to do lateral movement using the same technique, even disabling the services it was using to perform the operation once complete. Still another host was beaconing out to the same suspected command server, even though the domain was algorithmically obfuscated and dynamically created on the other end.

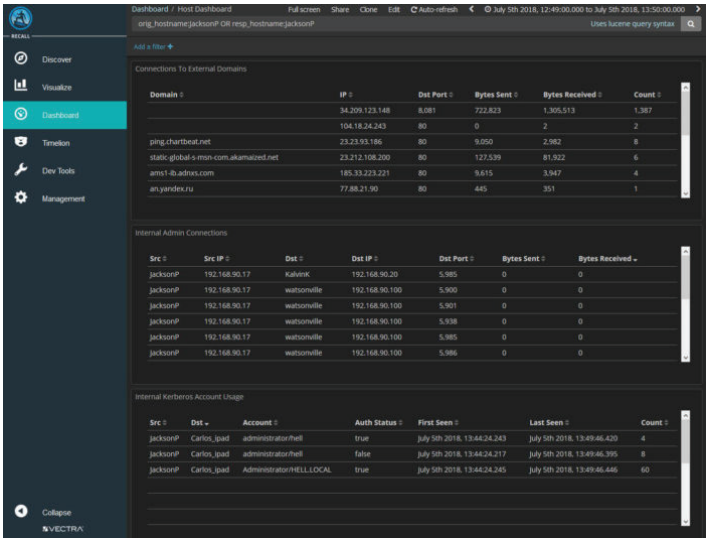


John Breeden II/IDG

Cognito Detect uses machine learning to find similar patterns of discovered threats occurring on different machines, which can unmask large threat campaigns hiding as single incidents.

When grouped together in a single graphic, Detect showed clear evidence of either an ongoing threat campaign, or a single threat actor using similar techniques to compromise multiple hosts over time. Armed with this type of information, stressed IT teams can decide if they are dealing with something an intern can fix, or a major situation that requires multiple analysts.

While Detect goes a long way in exposing threats, the Recall program can add historical context and assist with true threat hunting. Recall collects historical traffic data and can store as much of it as an organization wants, or has space to support.



John Breeden II/IDG

While Detect can set threat investigators on the right path, the Cognito Recall program can group historical data about potential threats in one place, or answer questions to support a threat hunt. It works automatically with Detect, but can also incorporate other programs if needed.

Every incident in Detect has a link to launch Recall. Clicking on it opens up a new dashboard where Recall gathers every related, or possibly related, activity that previously occurred within the network. This means that almost nothing needs to be correlated by hand, which often bogs down the beginning of a threat hunt. Instead, those who suspect that an incident may just be the tip of the iceberg can click on it in Detect and receive nearly instantaneous justification, or refuting, by Recall using historical data.

Vectra Cognito Detect and Recall help to realize the promise of combined operations in cybersecurity between thinking machines and technically savvy humans, with both doing what they do best. It was more than a match for any threat we tossed at it, including those that bypassed traditional defenses and would have been more or less free to roam the network had Cognito not unmasked them through their hidden, but bad, behavior.

VECTRA
Security that thinks®

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