IT Central Station
Unbiased reviews from the tech community

Case Study

Vectra AI

reviewer1358853

Information Technology Security Engineer II at a mining and metals company with 10,001+ employees

- Review by a Real User
- Verified by IT Central Station

What is our primary use case?

We use it as an intrusion detection system to monitor traffic that's going on within our network.

How has it helped my organization?

There was an event that happened before I started here, a ransomware event, and Vectra AI was able to quickly detect and alert on the activity. That greatly reduced the time it took for the company to respond to the incident.

Cognito provides visibility into behaviors across the full life cycle of an attack in the network, beyond just the internet gateway. By detecting everything before the internet gateway, it's able to get a fuller picture of what was going on before the target left the network. It greatly increases our ability to investigate events that occur.

The Vectra product also triages threats and correlates them with compromised host devices. As a result, it helps to reduce the time to respond to incidents.

In addition, it does a really good job of bringing the higher-level alerts to our attention while not bombarding us with alerts on lower-level activities that, I find, we don't usually need to investigate. When I first started using it I was investigating everything and I quickly learned the low-level threats, as shown by their scores, were low for a reason and they really didn't need to be looked at too closely.

I would estimate it has reduced our security analyst workload by around 30 to 40 percent. It has increased our security efficiency and has

also reduced the time it takes us to respond to attacks by about 50 percent.

What is most valuable?

One of the most valuable features is all the correlation that it does using AI and machine learning. An example would be alerting on a host and then alerting on other things, like abnormal behavior, that it has noticed coming from the same host. It's valuable because we're a very lean team. It helps reduce workload on our team daily by performing tasks that we don't have to do manually.

It does a really good job of reducing alerts by rolling up numerous alerts to create a single incident or campaign for investigation.

It also does a really good job detecting things. Some things it detects are not really threats, but it is stuff that it should be detecting, even though the behavior, sometimes, isn't malicious.

What needs improvement?

It does a little bit of packet capture on alert so you can look at the packet capture activity going on, but it doesn't collect a whole lot of data. Sometimes it's only one or two frames, sometimes it does collect more. That's why they have the addition of their Recall platform, because that really does help expand the capability.

I would also like to see more documentation or user guides about using the product.

For how long have I used the solution?

I've been using Vectra AI for a little over one year, but it was in place at our location before I started working here.

What do I think about the stability of the solution?

We haven't had any issues other than one power supply failure, but there was a backup power supply and they sent the replacement quickly. Other than that, I haven't seen any issues with stability of the product.

What do I think about the scalability of the solution?

I haven't had any experience in scaling it out beyond what was set up before I started here.

We have about 1,600 employees on site, but I'm not sure how many devices that equates to. Each person has one or more devices. We're scaled out about as far as we can go.

I'm the only person using it directly in our company, as an IT security engineer II.

How are customer service and technical support?

They have very good tech support.

What was our ROI?

Our company definitely saw return on investment when it had the ransomware attack. They were able to stop it quickly. That was definitely a huge savings. Otherise, the company was going to have to shut down production.

What's my experience with pricing, setup cost, and licensing?

I don't really have anything to compare it to, but I would assume the pricing is fair.

I believe they are licensing current devices or hosts. When I was last talking to a rep, we were having to go through a true-up process, but that hasn't started yet.

Which other solutions did I evaluate?

I have thought of evaluating other things, just for evaluation’s sake, but I haven't done so yet.

What other advice do I have?

It's helped me learn how to investigate alerts in a more efficient way.

It also captures network metadata at scale and enriches it with security information. Part of that I was able to witness using a proof of concept for the Cognito Recall platform, which collects all the metadata and then forwards it to an Amazon instance in the cloud. From there you can do a lot of correlation and you can do deep-dives into the data. That was also a really good product, and I would like for us to purchase it, but right now it doesn't look like that's going to happen.

Vectra will alert on activity going to some of our cloud providers, for example Microsoft OneDrive or Teams, but our systems won't really inspect on any type of SSL traffic, and it doesn't provide that much use for external communication that's encrypted. It's something we do not have set up and that's why we're not able to get that full visibility.

Which deployment model are you using for this solution?

On-premises

Read 12 reviews of Vectra AI

See All Reviews