IT Central Station
Unbiased reviews from the tech community

Case Study

Vectra AI

reviewer1362528

Manager, IT Security at a energy/utilities company with 201-500 employees

Review by a Real User
Verified by IT Central Station

What is our primary use case?

The Detect platform that we have is on-prem. We have what's called "the brain", then we have sensors placed in different key/strategic areas in the organization. It is helping us do a lot of the monitoring. We also have some SaaS offerings from the Recall platform, which look at some of the metadata, etc. If we were doing things like incident response, it gives us a bit more granular type of information to query. However, the Cognito Detect platform is all on-prem.

We are using the latest version.

How has it helped my organization?

We had a gap where we didn't necessarily have a managed service, which we do today, but at the time we needed something that would help us detect malicious behavior and anomalies within the organization. We found that Vectra solved this. We were able to find issues within minutes or hours of them occurring, then we were able to action them rather quickly.

Some of the metrics that we try to show from an incident response perspective are the effectiveness of our controls, like mean time to detection and mean time to remediate. E.g., mean time to detection shows how quickly the organization detects it from when it first occurred, then determines the remediation aspect as well. We take those numbers and correlate them back to how effective our tools are in our organization. Vectra's really helped in the sense that our mean time to detect is within zero the majority of the time, meaning that from the time we detect it to the time it occurred is within zero days. This promotes how effective

our controls are.

When we get an alert, we're not wasting hours or so trying to determine if, "I need to find more logs. I need to correlate the data." We're getting actionable data that we are able to action on right away. I have found value in that.

We can find things quickly that users shouldn't have been doing in the organization. Simple things, e.g., all of a sudden we have a user whose exfiltrating a lot of gigs of data. Why are they doing that? We found value there. My very small team does not have to waste cycles on investigating issues when we get a good sense of exactly what is occurring fairly quickly.

We have the solution's Privileged Account Analytics. We have seen detection on certain cases, and it's been good. It actually is a good feature. We already have an organizational approach to privileged accounts, so we have seen a few detections on it but haven't necessarily seen abuse of privilege because of the way our organization handles privilege management. We are an organization where users don't run with privilege. Instead, everybody runs with their basic user account access. Only those that need it have privileges, like our IT administrators and a few others, and those people are very few and far between.

If we are investigating something, we may be investigating user behavior. Using the metadata, we can find exactly, "What are all the sites he's going to? Is he exfiltrating any information? Internally, is he trying to pivot from asset to asset or within network elements?' Using that rich set of information, we can find pretty much anything we need now.

The solution provide visibility into behaviors across the full lifecycle of an attack in our network, beyond just the internet gateway. It augments what we are doing within the organization now. Being able to discover/find everything that is occurring within the kill chain helps us dive down to find the root of the problem. It's been beneficial to us because that's a gap we've always had in the past. While we may have gotten an alert in a certain area, trying to find exactly where it originated from or how it originated was difficult. Now, by utilizing the information that Vectra produces, we can find exactly what the root cause is, which helps with discovering exactly how it originated in the first place.

With a lot of the detections or things that are happening, I would not say they're necessarily malicious. Where I find it very valuable is that it gives us an opportunity to understand exactly how users are sometimes operating as well as how systems are operating. In a lot of cases, we have had to go back and reconfigure things because, "Oh, this was not done." We realized that maybe systems were not setup correctly. I really liked this aspect of the solution because we don't like false positives. We don't want Vectra to produce things that are just noise, which is something that it doesn't do.

Vectra produces actionable data using automation. That has helped us. It's less manpower now to look at incidents, which has

definitely increased efficiency. Right now, in a lot of cases, our mean time to detection is within zero days. This tells me by the time something happened, and we were able to detect it, it was within the same day.

What is most valuable?

It gives you a risk score of everything that you just found. The quadrant approach is useful because if there are things in the lower-left quadrant, then we don't necessarily need to look at them immediately. However, if there's something with a high impact and high risk score, then we will want to start looking at that right away. We found this very valuable as part of our investigative analysis approach.

The solution's ability to reduce alerts by rolling up numerous alerts to create a single campaign for investigation is very good. Once it starts adding multiple detections, those are correlated to a campaign. Then, all of a sudden, this will increase the risk score. I've found that approach helps us with understanding exactly what we need to prioritize. I find it very useful.

The amount of metadata that the Recall solution produces is enormous. What we can find from that metadata is exceptional. Once you get to know how to use the tool, it's much simpler and more intuitive to use when finding information than using a traditional SIEM, where you have to build SQL type commands in order to retrieve data. So, I do find it very valuable.

What needs improvement?

I would like to see a bit more strategic metrics instead of technical data. Information that I could show to my executive management team or board would be valuable.

I would like to see some improvements on the integration aspects of it. They are getting better in this. However, most organizations have a plethora of cybersecurity solutions that they run, and I think that there is a bit more that could be done on the integration side.

For how long have I used the solution?

About four years.

What do I think about the stability of the solution?

The stability is good. I don't think we've ever had an issue with it at all. I don't think I've ever seen it misbehave, crash, or anything like that.

It is continuously updated. Whenever they release a new patch or updates, they push it to the brain (the centralized management).

What do I think about the scalability of the solution?

We have never seen an issue from a scaling perspective. It is not an issue for us.

We have a team of less than four people. We don't really have a Tier 1 or Tier 2. We just have people working in cyber.

There are areas where we would like to increase our capabilities. We have 100 percent visibility for anything leaving the organization. There are some areas within the organization where we would like to monitor some of the internal workings. One of the places where we are looking to expand is into our OT segment. We do have a path for where we would like to see this go.

How are customer service and technical support?

They are very competent and good. They are always able to solve problems.

Which solution did I use previously and why did I switch?

A few years ago when we were looking at this, we had a gap in the organization. We didn't have like a managed service offering. We had an on-prem SIEM, but we didn't have a large team so we didn't have resources fully dedicated to looking to see threats and correlating them with other event logs to see exactly what was occurring. The reason that we didn't have a managed server previously was cost. Therefore, we looked for alternative ways to solve the gap, lower the resource count, and be able to automate and integrate within our enterprise solutions.

How was the initial setup?

It was pretty straightforward. You can plug the appliances in, whether it is into a switch, router, or some other demarc point from a SPAN port, then you let it learn. That is it. There's nothing really you have to do.

Our deployment took days at most. Once you configure it, you just let the system learn. Usually, within a week, it starts to detect things. For it to be effective, it needs to know what the known baseline is.

You plug it in, let it learn, and it's up and running.

What was our ROI?

We saw ROI within the first six month due to the reduced impact on our staff and we have been deploying it for years.

Vectra has absolutely reduced security analyst workload in our organization. This was the real thing that we were trying to find: How can we do this? With a small team, it is very hard. We have a small team with a large stock of solutions. Therefore, we were looking for the best way to reduce the amount of manual effort that's required for an individual. We've found Vectra has significantly reduced the workload by probably 200 percent for our staff.

Which other solutions did I evaluate?

We looked at NextGen traffic analysis type of solutions, like Darktrace. Then, we looked at Vectra. I found Vectra was a bit more intuitive. I think both products had some really good offerings. What really helped us make a decision was we were trying to find things that help us produce actionable items. I liked Vectra because the one thing it was trying to do is it was show you exactly what is happening in the kill chain. The whole premise behind it was, "These are things that are actually occurring in your network, and they're following a specific pattern." I really liked it because in my view it was very actionable and automated.

I don't want to have to spend cycles on things on unnecessary things. One thing I found with Darktrace was it produces a lot of good things, but it's too much in certain cases. Whereas, I like the way Vectra tells you exactly the things that are happening right now in your network, then groups it based on exactly what the type is, providing you a risk score.

Also, it did seem like it was like a resource built into a box with AI capabilities. I found that the amount of effort we have to spend on analysis from it is a low cost to us. Vectra just fit in well with my team mandate.

I found Darktrace was a bit more noisier than Vectra. Sometimes, when you deal with products like this, the noise is time and effort that you may not necessarily have.

Once we started to do the PoCs, we ran Vectra in certain use cases with the sense of, "Okay, let us know exactly what's kind of going on within the network." What we found in a lot of cases is, and these weren't just cybersecurity incidents that were occurring, and Vectra gave us a good sense of how a lot of our solutions were operating. We ended up finding out, "This is exactly what this solution may be doing. Maybe there is a misconfiguration here or there."

What other advice do I have?

There was no complexity with Vectra; it is very simplistic. However, for the tool to be effective, you want to make sure that you place your sensors in appropriate places. Other than that, you let the tool run and do its thing. There's really no overhead.

I would probably rate it as a nine or 10 (out of 10). We have been extremely happy with the solution. It's been one of the best solutions we have in our enterprise. I would put it at the top of the list.

Which deployment model are you using for this solution?

On-premises

Read 12 reviews of Vectra AI

See All Reviews