IT Central Station
Unbiased reviews from the tech community

Case Study

Vectra AI

Headofinfosec82347

Head of Information Security at a retailer with 1,001-5,000 employees

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

What is our primary use case?

Vectra AI sits across our entire estate, we have an outsource provider for a lot of our backend systems. It sits in theirs and it sits in our own estates. It's deployed across our other numerous offices across the country. It sits across our entire state.

How has it helped my organization?

We don't have very much in the way of IDS or IPS on our estate, so we're relying on Vectra AI to do that sort of work for us. We're allowing that to look at our traffic and to flag up to us on our system. It helps my analysts investigate other things. We might get other alerts in the estate, Vectra AI is one of the first tools that they'll jump onto, to do further investigation of alerts that are raised up to them. It's a really good tool, not just for what it throws up, but for us to dig into our network as well.

What is most valuable?

What is pretty good is the unknown unknowns. It's the anomalies to the norm and the intelligence behind it that helps us to dig through a mountain of data and find the stuff that's important to us.

It allows us to understand what our normal traffic is, then pulls out the anomalies for us. For instance, a recent use case of it would be that it suddenly picked up that a file transfer was happening out of our estate that we weren't aware of. It hadn't been there before. There was a file transfer that suddenly appeared, that was actually in our estate that hadn't been there

before. We would never have been able to see that normally, it's just that Vectra AI saw it. It was okay, it was going to a third-party and it allowed us to investigate it and find it but we would never have seen that without a notification. It understands what should be happening and then usually says "This isn't normal," and it allows us to flag it up and dig deeper into that.It is very good at reducing alerts by rolling up numerous sellers to create a single incident or campaign for investigation. Although it doesn't reduce, it actually increases our alerts because we wouldn't have seen the stuff in the first place, but when it does create an alert, it pulls all investigative information together. We're not getting hundreds of alerts, we're getting alerts that contain all of the relevant components.

Vectra AI captures network metadata at scale and enriches it with security information. Although, we don't make the most of that, but we've never had a problem with its captures and it captures the correct data for what we want it to do. I think we could be using it better.

The information affects investigations by our security team by allowing them to be more effective and quicker in their investigations.

Vectra AI provides visibility into behaviors across the full life cycle of an attack in our network, beyond just the internet gateway. Although, we found it's flagging up early, so it's not developing to that further stage of that because it's flagging up at an early stage.

Its ability to reduce false positives takes quite a bit of tuning. We've had to put a lot of effort into tuning out false positives, so that's something that we've had to invest our time into. Obviously it's getting better and better as time goes on, but we still have to spend time tuning it.

We've seen our tuning has lessened those processes, but we're still getting more than we would want. That's probably some of our fault. It could be some issues with the way it's set up in certain areas. But, once we tune them out, they're staying tuned out.

It hasn't reduced the security analyst workload in our organization but that was never the purpose of it for us. It's an additional tool in our armory, so it hasn't reduced our workload, but it's made us more efficient.

It makes the team more efficient in speed of response. I would say it makes them more efficient in the breadth of their coverage of what they can respond to. It makes us have a more proactive response to incidents.

It has reduced the time it takes to respond to attacks. That comes back to the proactive point. It makes us able to lower down in the kill chain. We can react now, rather than reacting to incidents that happened, we can see an instant, in some cases, as it's being implemented, or as it's being launched.

It's not all attacks, but I would say that it's a shift less on the material chain. It's things that we might not even have spotted if it hadn't been for Vectra AI, so it's difficult to know how we would quantify that as an amount.

What needs improvement?

The false positives and the tuning side of it are some things that could use improvement but that could be from our side.

I don't want to criticize the product for performance with our role out of it. It does what it says it's going to do very well. We've got issues with the way we've deployed it in some places, but the support we've had in that is very good as well, so I'm very happy with the support we get.

For how long have I used the solution?

My company has been using Vectra AI for three years. I've been here for eight or nine months now, but the company has just been using it for three years.

What do I think about the stability of the solution?

We've had absolutely no issues with stability at all.

What do I think about the scalability of the solution?

Scalability is obviously based around the size of the clients that we have. We have had some issues around scalability but that's only because when it was implemented before my time but I know it is scalable. Obviously, we have to put some thought into that, some planning into that from our side, but it is limited on the size of the boxes. To summarize, yes, it is scalable, but it needs planning.

We have four users who use it in my company who are cybersecurity analysts.

Vectra AI is on everything apart from the clouds. Now we're on a journey towards more and more cloud. At least 70% of our company is covered by it.

We do have plans to increase usage. We want to move to the cloud.

How are customer service and technical support?

The support is excellent. We've had really good technical support from Vectra AI all the time. We have very regular catch-ups with them. They always pick the right people to do the calls, and we even have deep-dive sessions with our analysts with them and provide us with training. They've been excellent.

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

We didn't have anything in place before Vectra AI.

I have used another solution in the past. I used Darktrace where I was before. It compares very

favorably with Darktrace. I wouldn't say it was any better or worse.

The UI is quite different, but apart from that, there are obviously slight differences in the analytics behind it, but I'd be struggling to say that one of them was better than the other. They both seem to do what I do well. Vectra AI is a little bit more honest about their capabilities than Darktrace is.

I don't think Vectra AI enables us to answer investigative questions that other solutions are unable to address. I know that there are other solutions that could do it as well. They're as good as everything else out there, but I wouldn't go and say they're massively better. The thing that sells it for me is that the support has been very good. That's one of the bits that keeps me with them.

What was our ROI?

ROI depends on how you quantify that in security. It's really difficult to quantify what you find to a monetary value. We do see a return on investment because it's a good tool that we're using well and it's helping us to keep the company secure. It's really difficult to quantify a monetary value on that or say that you've got return on your investment. I wouldn't want to be without it. You can't put a price on security.

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

They compare very favorably against the competition in terms of price. Nothing in this area is cheap. There is a lot of value in the products that you're buying, but they have come in at the right price for us in comparison to others. I would say that they're competitive in their pricing.

What other advice do I have?

My advice would be to make sure it is planned and deployed properly. That's a problem with my organization, not a problem with Vectra AI. Otherwise, if you don't build it to the specifications that you were told to, you're going to spend your whole life trying to fix a problem that shouldn't be there. My advice would be the plan and implement as per the plan.

I would rate Vectra AI a nine out of ten.

Which deployment model are you using for this solution?

On-premises

Read 12 reviews of Vectra AI

See All Reviews