Peer Review for Vectra Cognito Platform

Edit

"An Important Part Of Any Security Stack"

Submitted: February 26, 2021

5.0 Overall User Rating

Report Inappropriate Content

Product(s): Vectra Cognito Platform

Overall Comment: "The overall experience with Vectra Cognito Detect has been very positive from pre-sales to production use. The detection capabilities are outstanding. Every detection has value and help you understand what "normal" is in your environment. After deployment, we took an aggressive approach to identify "normal" and create good filters to the point that we don't only monitor the high and critical quadrants but also the low and medium."

4.0	Evaluation & Contracting	5.0	Integration & Deployment
5.0	Service & Support	4.0	Product Capabilities

Lessons Learned

What do you like most about the product or service?

I consider detection capabilities to be the most important part of the product and I Vectra's approach is rock solid. Get familiar with the Vectra Kill Chain, high level categories, and the individual detection types, and it will become obvious why Cognito Detect brings so much value. Each detection is accompanied with a great explanation of why the detection triggered, possible root causes, business impact, and steps to verify. I also like how Vectra associates each detection back to MITRE techniques.

What do you dislike most about the product or service?

Creating custom filters was awkward initially and I think had limitations. After time I got used to them so there are maybe still limitations but it doesn't seem to interfere. Also there are improvement opportunities with the dashboard and specifically the statistics. Same comment for reports. Admittedly I haven't spent a lot of time

Reviewer Profile

IT Security Architect

Industry:
Manufacturing

Role:
Security and Risk Management

Firm Size:
1B - 3B USD

Implementation Strategy:
Worked with just the vendor

Review Source

Invited by Vendor (direct, user community)

Learn More

management

Please explain the business problems or needs that prompted the purchase of this product or service.

To increase and/or add visibility where needed

If you could start over, what would your organization do differently?

Start sooner

Evaluation & Contracting

4.0

Why did you purchase this product or service?

Create internal/operational efficiencies
Improve compliance & risk management

What were the key factors that drove your decision?

Overall cost
Other...
Product functionality and performance

Integration capabilities

Which other vendors did you consider in your evaluation?

Darktrace

Integration & Deployment

5.0

Version number(s) currently in use in your organization

6.4.0-15-12

How extensively is this product being used in your organization?

Company-wide

When was this product or service deployed at your organization?

2020

How long did your deployment take?

0 - 3 months (<3)

What was your implementation strategy?

Worked with just the vendor

Service & Support

5.0

Product Capabilities

4.0

Scalability	**4.0**
Integration	**4.0**
Customization	**4.0**
Ease of use	**4.0**

Additional Context

Deployment architecture

Hybrid Cloud and On-premises

North America

How long have you used this product or service?

1 year to less than 2 years

How frequently do you use this product?

Daily

What is your role with this product or service? (Select all that apply)

I am the administrator
I helped select or purchase this product
I am on the team that set up, implemented or customized this product