IT Central Station
Unbiased reviews from the tech community

Case Study
CRITICALSTART

Preston Broesche

Director of Information Technology at Kirby Corporation

Review by a Real User
Verified by IT Central Station

What is our primary use case?

I have a very small team and anytime I can maximize efficiencies within the work I'm trying to do with Kirby, it's a good thing. That's what I was trying to do by using CRITICALSTART.

How has it helped my organization?

The most valuable part of the service is the time saved. CRITICALSTART helps with so many of these alerts that my team and I don't get alert fatigue. It saves us time to concentrate on the more important things. It probably saves us a day or two, 10 to 15 hours, a week.

I also talk to CRITICALSTART analysts and the value in that is immense. I just talked to my Board of Directors about that this morning. The value from it is what I'm spending on the service versus what I would have to spend to build a team like that internally. It's at least one-fifth of the cost. There's value in that for me. And their availability is generally pretty quick. I've never really had to wait very long for anything. The availability of the analysts where they will say, "Hey, I know we sent an alert on this, but you should really take a closer look at it," via a phone call or a message, is just phenomenal.

In a given quarter, I get 589,000 security events and 584,000 of those get reduced by the service before they even get to me. The alerts that actually come through to me end up being about 1,400 in that quarter, which is a 99.7 percent efficiency rate.

What is most valuable?

The Trusted Behavior Registry helps resolve alerts in the sense that CRITICALSTART is doing a lot of that initial triage for me. Out of a given 500,000 events and alerts, for example, that come through, they're taking out 495,000 of them. That only leaves me with a subset of that to actually have to triage, and that's where it benefits us. They take care of Tier-1 and Tier-2 triage.

And the new mobile app is awesome. It is one of the best I've ever seen. It's much better than its predecessor. It's more intuitive, a whole lot easier to navigate and get where you need to go. It's less repetitive and just generally easier to use. It allows me to not have to be sitting at my computer all the time. I can be on my phone or tablet or wherever I'm at. It makes it a lot easier to answer tickets and do that kind of thing.

Also, the intuitiveness of the updated user interface for the service is spot-on. It is much easier to navigate, and know where to navigate, in the newer interface. I've never had an issue with responsiveness. It's very quick and doesn't sit there and chug on anything. It's fast, it's efficient. It has enabled our SecOps team to take action faster because if you have multiple ways of connecting to it and actually getting your alerts answered and taking care of things fast, it is extremely helpful.

All the information that you need to make a determination is usually in the alert itself that comes through the Zero-Trust Analytics Platform (ZTAP). I don't find myself going back to the app itself very often. That still happens, but not as often. The ability to flow the information forward, from the alert standpoint, helps me because it saves me from running back to get the information. It's improved my efficiency.

Finally, there haven't been any data sources that the service wasn't able to integrate with.

What needs improvement?

The only thing I can think of that I would like to see, and I'm sure they could work this into a service pretty easily, is not only alerts on issues that are affecting my company, but some threat intelligence of a general nature on what's out there in the environment. That might be a nice add-in.

For how long have I used the solution?

I have been using CRITICALSTART for about seven years now.

How are customer service and technical support?

If I have issues, all I have to do is either send a message or a ticket over and ZTAP will pick up the phone and call somebody. It's pretty easy.

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

We were all internal prior to using CRITICALSTART for this. We didn't use a third-party external service to look at any of this data. We were actually doing it ourselves.

How was the initial setup?

From the time we entered into an agreement to use this service until we could start using it, it was pretty quick. They jumped right on it from a project management standpoint. On a scale of one to 10, the project management aspect was a 10. Their performance was spot-on. I was actually using it, even though we were still tuning, within a week or so.

In terms of initial setup, you have to start pointing all your sources to the app to have them adjusted. Once you start doing that, you can start getting some data out of it. Within that week I started seeing events start coming through.

The initial setup is always straightforward. The complexity comes in the tuning, because then you have to say, "Is this normal? Is this not normal? Does this only happen once a year?" That's where the complexity comes in. The fine-tuning took a couple of months. But that was more on my side then it was on CRITICALSTART's side.

I was the only one involved in the setup from our company, and I'm the only user. Our entire domain reports into it from a SIEM perspective, and every node that we have is reporting in from an endpoint protection standpoint. That's 5,000 to 6,000 user nodes and probably another 1,000 servers. It's a 100 percent adoption rate. They don't get a choice.

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

Overall, for what I'm paying for it, and the benefit I'm getting out of it, it is right where it needs to be, if not a little bit in my favor. For what it costs me to actually have this service, I could afford one internal person to do that job, but now I have a team of 10 or more who are doing that job, and they don't sleep because they work shifts.

Licensing is always one of those things that you can have some degree of negotiation on. There are hard costs associated with the service because they're paying salaries. I always look for opportunities to improve from a pricing standpoint, but I've not been displeased, so far, with it.

Which other solutions did I evaluate?

I knew of a few other options. Alert Logic is one of them, and there was another one called Fulcrum that has a service now around it, but it's

nowhere near the maturity of what CRITICALSTART has.

I also had an existing relationship with CRITICALSTART. We did have an issue and they stepped in and helped us with that issue and really went to bat for us. That helped build that relationship from a trust standpoint.

There wasn't any kind of bake-off. It's a close-knit community, so I didn't really have to go to that level. I knew I didn't want certain other ones.

The main difference between the other options and this one is the quality of the personnel within the SOC. It's their knowledge and depth and the way they handle customers. Their guiding principles fit really well to get you the best service that you can possibly get.

What other advice do I have?

I would suggest using a phased approach, instead of dumping everything in from the beginning and then trying to sort it out, triage-wise. If you add types of sources or tools to it one at a time, instead of "everybody into the pool" right away, that really helps you. That way it allows you to get your handle on the smaller piece of the pie first and then work your way forward.

As for what to start with, it depends on what you're pushing to them. I didn't start necessarily right away with the MDR, but I did have my endpoint protection being looked at by them, at least. Then I added in my SIEM, which added to the overall complexity level. Unfortunately, I didn't have one completely finished before I added the next and that slowed me down a little bit. That was too much for one person to try to handle all by himself.

The biggest lesson is that even if you have a small team and limited resources, you can actually be effective as a company, from a security program standpoint, by using their service.

My expectations have been more than met in terms of service delivered on time, on budget, and on spec from CRITICALSTART.

Read 10 reviews of CRITICALSTART

See All Reviews