PeerSpot

Case Study

CRITICALSTART

Justin Hadley

Sr. Manager, Security Engineering at a financial services firm with 501-1,000 employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We were looking for a third-party managed detection response provider for our integrations with Cylance and Carbon Black. We had to deploy the Cylance and Carbon Black agents after we received them from CRITICALSTART.

Types of challenges that we were looking to address:

24/7 monitoring Reducing alerts. Getting Level 0 and 1 taken care of, along with that first triage of alerts. Those are taken care of before our team has to look at it.

How has it helped my organization?

The way that the user interface presents data enables our team to be able to make decisions significantly quicker, rather than have to dig into the details or go back to the original tools.

The transparency of data in the platform is perfect. The way they built it out, you are seeing everything as they are seeing it. There is not a black box; it's not the magic sauce happening behind the curtain. You have the ability to see everything that they do right there in the console.

The service has significantly increased our analysts' efficiency to the point that they can focus on other areas of the business. We went from triaging an email inbox and a few other tools to being able to manage the queue appropriately at regular intervals. We also have begun looking for other tasks or items to further advance some of the analysts' careers.

Services have been fully delivered on time, on budget, and on spec. Whether it be

for implementations, go-lives, or enhancements for anything that we want to add to the platform, they have always been consistent, ready, and willing to help out, build out, and troubleshoot should there be any issues.

What is most valuable?

Their Zero Trust Analytics Platform (ZTAP) engine, which is kind of their correlation engine, is by far and away one of the best in the business. We can filter and utilize different lists to build out different alerts, such as, what to alert on and when not to alert. This engine helps reduce our number of alerts and false positives.

The service's Trusted Behavior Registry helps the provider solve every alert. The way that they have it built out is very intelligent. The way every alert comes in, it gets triaged one direction or another. If it is already a false positive, then it is still getting addressed and reviewed on a regular cadence. Also, true positive alerts get escalated to the appropriate personnel.

Its mobile app is great. The ability just to be able to quick reference and see what's coming in when you're on the move or go. You don't always need to have your computer or laptop handy, because you can operate it just from the mobile app. It can communicate with analysts, which is great.

The mobile app is great at affecting the efficiency of our security operations. Those guys are using it throughout the day, whether that be at the office, home, or off hours. Typically, they triage from the mobile app. Then, if an escalation needs to be done on a computer, they will pull out a computer.

We were on the original UI for a few years, so the updated UI has been a refreshing change. It has significantly more ability to filter and translate data, then load that data. It is rather intuitive to click through for some of our junior analysts or interns, especially as we are starting to onboard and teach them different aspects of the security operations team.

What needs improvement?

The biggest room for improvement is not necessarily in their service or offering, but in the products that they support. I would like them to further their knowledge and ability to integrate with those tools. They have base integrations with everything, and we haven't come across anything. They should just continue to build on that API interface between their applications and other third-party consoles.

For how long have I used the solution?

We started using it in 2017.

What do I think about the scalability of the solution?

We have about 15 to 20 users. That is a mix of

the security team, sysadmin server administrators, and the network operations group.

How are customer service and technical support?

Our team members talk regularly with CRITICALSTART's analysts. They go back and forth with them regularly on individual incidents or investigations as well as support calls or conversations around monthly trends.

The number one value their service, as a whole, provides is the people. They hire the right guys and train them. We can then leverage their knowledge of looking at the greater picture. They are able to see all of their different clients, then translate what they are seeing there to our individual instance.

Whether it be alerts that they have already given us, or if we want to do some different threat hunting, have different ideas that we're trying to dig into, or we need assistance with an investigation, they are always a phone call away. They have analysts ready and willing to dive into a specific issue, even if it's not related to something their service has provided or alerted us to.

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

We didn't have a third-party provider previously.

The primary reason that we went for a service like CRITICALSTART was just the need to lift the burden off of a small team. When we started with CRITICALSTART, there were four of us. Now, we are a team of 15 or 16, so our team has grown. However, being able to have that first layer with a first set of eyes on alerts, incidents, and investigations as they came in, it was a big point for us, rather than getting stuck in our backlog and trying to keep up.

How was the initial setup?

We entered into an agreement to use CRITICALSTART's service, then it took us two months before we went live.

There was nothing significant that we had to do in addition to the initial setup. When we do firewall changes, we just do it through our agents and communicate back to CRITICALSTART appropriately. This took four to six weeks of our setup time.

What about the implementation team?

Four people from our organization were involved in the setup:

Our security operations manager Our internal IT manager Our network operations team Myself, as I manage the security engineering team.

What was our ROI?

Monthly, we are looking at 10 to 12 million alerts that the Trusted Behavior Registry sees. Of that, about 250 to 300 get escalated to our team.

CRITICALSTART takes care of the Tier 1 and Tier 2 triage for us. We only escalate up when there is a true positive that needs to be investigated. On a weekly basis, this saves us close to 50 to 60 hours.

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

The pricing has always been competitive. They have always been good to us. They will make it a fight. They don't try to hide anything; it's always been fully transparent and well-worth what we pay for it.

There are SLAs within our contract regarding the different alert tiers. This was a big factor in our decision to go with this service. They are willing to stand behind their product and team, then put that in a contract. It is evident that they are doing the right thing for their clients. They have not missed any SLAs so far.

Which other solutions did I evaluate?

We also looked at CrowdStrike. Their service just wasn't quite as mature. They only integrated with their only product.

We looked at Arctic Wolf, who is not local. Critical Start is just down the street from us. Being able to build that relationship locally was a big selling point as well.

What other advice do I have?

Trust the CRITICALSTART team. For the products that they resell and support, they know them very well. As you go down that path, you have a good heap of knowledge to rely on. Do not try to build it out or figure it out yourself.

We have since transitioned Cylance and Carbon Black over to CrowdStrike. We still use them for that service and also use them for our SIEM, because they host and manage Splunk for us. That all integrates into ZTAP. Using that and any new products that we bring in-house, we work with CRITICALSTART to see if they have already gotten an integration connector built. Typically, we'll use theirs. If there's already something built, or they have the appetite to build it, we'll use that service as we onboard it internally as well as into CRITICALSTART.

The biggest lesson is transitioning from alert overload to being at a point where we do have eyes on alerts, where every alert is truly possible. It's something that a lot of people sell and not a lot of people do very well. Being able to come into this relationship, then where we're at today, it kind of opened my eyes to: There is the opportunity and the possibility to do this. Stuff is not going to get dropped or missed by

our operations group.

I would give them a nine (out of 10). They are right there at the edge, probably a leader in the market. That's kind of why we chose them. Of course, there is always room to improve, but they're doing a lot of things right. We appreciate their team.

Read 10 reviews of CRITICALSTART

See All Reviews