PeerSpot

Case Study

Devo

Dennis Pope

Security Delivery Senior Manager, Cyber Solutions Architect/Engineer at a tech services company with 10,001+ employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We're primarily using it to correlate WAN and endpoint activity for our clients. We work with vendors that have endpoint solutions or that control the networks for our clients. We are receiving their feeds, along with some of our other custom deployed equipment, to not only collect endpoint data, but to monitor network activity and correlate it to identify threats, vulnerabilities, attacks, and provide incident response.

How has it helped my organization?

We've integrated Devo with a SOAR solution. We have prioritized the severity of our alerting in Devo and that corresponds directly to automated playbooks that are kicked off in the SOAR. With that SIEM-SOAR solution, we have drastically reduced the number of incidents that our analysts have to work through, and we have improved our time to respond as well as the time to remediate, through that integration.

Devo absolutely saves us time. We brief our project manager and client weekly on the number of man-hours saved just by having this SIEM-SOAR integration. Considering the quantity of data feeds and events and endpoints that we have, we can actually present a funnel chart that shows how many "events" we start with and how many become actual incidents. We then have that calculated into the number of dollars saved. It's phenomenal when you look at it. When we show the people who are in charge of getting funding that we saved this number of man-hours, which correlates to this number of dollars, they're more willing to fight to get that funding for the next fiscal year.

What is most valuable?

The strength of Devo is not only in that it is pretty intuitive, but it gives you the flexibility and creativity to merge feeds. The prime examples would be using the synthesis or union tables that give you phenomenal capabilities. There is such a disparity in how, say, a network feed or an endpoint feed comes in. They're all over the range, not only in the information they present, but in how that information is categorized. The ability to use a synthesis or union table to combine all those feeds and make heads or tails of what's going on, and link it to go down a thread, is functionality that I hadn't seen before.

It also provides high-speed search capabilities and near real-time analytics. I haven't had any problem with it in those contexts. The high-speed search and near real-time analytics are important to us because when it comes to incident response, we have a certain amount of time to turn these events and incidents around. That's how we're graded. That responsiveness, where it's not waiting on any results, is critical to how we do our jobs and how we stay alive in this game.

And because of the ease of integrating Devo with the SOAR solution, we've created an API for a visualization capability, and that works pretty easily. I'm usually an incident response, content development, threat hunting guy. But I was able to do all this stuff on the back end myself. The way it's set up makes it easy for someone who is not a back-end engineer to go in and set up that kind of integration.

We look for historical patterns and analyze trends with that data. That historical data is critical when putting separate events together and trying to detect a pattern or when looking for a low-and-slow, advanced, persistent threat. Without that reach-back capability, you would just see these one-offs and you would never put that information together. What makes a SIEM work is not only seeing the real-time event feed but being able to reach back and put things together. That's at the core of any SIEM solution.

What needs improvement?

We have a list of things that we'd like to see. I have had all my analysts put in suggestions. I've tested a number of solutions through the years, and I've found that companies appreciate that analyst perspective and anything that makes future releases more user-friendly.

The biggest thing we've found, when trying to integrate Devo with the SOAR solution, is the priority or severity rankings. If they could make those a little bit more intuitive that would help. It seems that when we set the priority of an alert, it doesn't always translate, in the back end, the way you would expect. The severities include "very low," "low," "medium," "high," and "very high." Those correlate to numerical value ranges one to three, four to five, six to seven. It's a little confusing. It would help if they made that priority/severity labeling and numerical system match up a little better.

Also, it would help if some of the error

messaging could be a little bit more descriptive when you run a query and an error pops up. It would be good to have a log where you could find those, as well.

Another issue is that an admin who is trying to audit user activity usually cannot go beyond a day in the UI. I would like to have access to pages and pages of that data, going back as far as the storage we have, so I could look at every command or search or deletion or anything that a user has run. As an admin, that would really help. Going back just a day in the UI is not going to help, and that means I have to find a different way to do that. That's a big one.

For how long have I used the solution?

I started looking into it and training on it in August of 2020, so I have been using it for about 16 months.

What do I think about the stability of the solution?

I can count on one hand the number of times it has gone out. It's very stable. A few times we've needed to reboot the stack and that has usually resolved the issue. We're pleased with the solution when it comes to incident response.

What do I think about the scalability of the solution?

It's highly scalable.

How are customer service and support?

I have all the personal numbers of my Devo support guys. I can text them and they usually respond within the hour. It's excellent customer support. I've been in this game for 20 years and you can generally expect someone to get back to you within a business day or two. But if I'm in a pinch, these guys usually respond within an hour.

In terms of being an ally to our business and providing a customer-first approach. They are a highly trusted ally and partner. The success of our solution relies directly on their delivery. We include them in all of our success stories. We consider Devo on par with our company.

How would you rate customer service and support?

Positive

How was the initial setup?

Setting up the solution was pretty complex. Working with the number of external vendors that we had, the way that they would

send the information to us, and the fact that they were constantly changing the way that data was being sent, meant we were constantly having to go in and tweak the relay rules. To know what you're doing with the relays, and putting in those rules, takes some homework. Devo was very responsive and worked with us hand in hand, troubleshooting and putting in the parsers and the relay rules to help us get things integrated.

It took six to eight months of that type of work just to get it to work. For our project, the setup was very complex. We had two environments, a lab environment and a live environment and it took that long to get both running. That seems like a lot of time. But we were working with a number of different vendors, and this was the first time any of us had ever done this.

Which other solutions did I evaluate?

I'm a long-time ArcSight and Splunk user. I see Devo as the evolution of both of them. If the capabilities of those two got together and had a baby, it would probably be Devo.

Devo is a definite upgrade from both ArcSight and Splunk, in my experience. It combines some of the best of each and it takes it to another level when it comes to ease of use and how you can expand the capabilities.

Another benefit of Devo is that it enables us to ingest more data compared to other solutions. This project has such a widespread ingestion of so many endpoints and networks.

What other advice do I have?

The ease of use of Devo really depends on whether you've had experience with a SIEM before. If you have, you should be okay. If this is your first time walking into a SIEM, it may be a little bit overwhelming, which is natural for any SIEM.

But it's very easy to pick up and has great documentation. The tutorials that Devo has provided, the upfront user training, and their lab environment are all very helpful. I just sat through a monthly tutorial where they had one of their commercial users come in and speak for 35 minutes on their best-case uses. The support element, combined with the training that they provide upfront, creates a customer experience where you're not flying solo. You have a lot of people to lean on. We use Devo as a service, but I've found that there is so much documentation at my fingertips that I really don't need to reach out to them that often.

Where they have exceeded my expectations is the training element. They're constantly putting out training tidbits and interactive sessions. They don't have to do that but they're holding sessions where they bring in analysts who do straight run-throughs. That's stuff you don't get anywhere else, other than with someone in a SOC environment. Those sessions are invaluable for picking up tips on how to better use the solution.

In terms of Devo providing a multi-tenant cloud-native architecture, if you can switch domains, it does. At this point in the evolution of our architecture, that is not important because we only have one client at this point. But I do see the usefulness of it to separate your domains and your traffic while, at the same time, potentially filing some of that activity or using it for correlation. We're just not at that stage right now.

Which deployment model are you using for this solution?

Private Cloud