LogRhythm NextGen SIEM Review From A Customer

IT Central Station
Unbiased reviews from the tech community

LogRhythm NextGen SIEM

Review by a Real User

Verified by IT Central Station

SOC Analyst at a financial services firm with 1,001-5,000 employees

Briane Harris

WHAT IS OUR PRIMARY USE CASE?

We use it for centralized log management and for alerting. It's been working pretty well. We're on the beta program so what we're on right now has not been working quite as well lately. We're helping them find the bugs, but before this we didn't have any really major issues with it.

HOW HAS IT HELPED MY ORGANIZATION?

It makes everything quicker when it's all centralized. Anything we need to find, it brings to our attention. Even other products we have that feed into it, instead of having to watch all of them we only have to watch one. For example, we have CrowdStrike, so instead of having to pay attention that solution - because its dashboard doesn't really pop when an alarm comes up - we can see issues with the red on the LogRhythm alarm. That is very nice. We have seen a measurable decrease in the mean time to detect and respond to threats.

WHAT IS MOST VALUABLE?

Being able to find everything in one place is really nice when you're doing your searches.

WHAT NEEDS IMPROVEMENT?

One thing we have mentioned to them before is that we'd like to be able to do searches, or drill-downs, directly from an alarm. When you click it and the Inspector tab slides out, that might be a good place to be able to click the host to search for the last 24 hours. I know the search is right there but it would be even nicer to just click that and then have an option to search something there.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

Going into the beta, stability was very good, but in the beta its not been as great for us lately. There was a known bug where, after about five minutes it would duplicate alarms, up to about 10,000. After 10,000 alarms in five minutes, everything is shutting down. Also, some of the maintenance jobs get deleted when upgrading, so our database was filling up without deleting the old backups. Those are the two major issues so far.

LogRhythm NextGen SIEM

Read 40 reviews of LogRhythm NextGen SIEM

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

I just took it over recently but we got it built to last. It's been the same since we put it up.

HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?

I open tickets frequently, especially in the beta program. To get the first response is usually a little slow, but once they're talking to you it's very good.

WHAT OTHER ADVICE DO I HAVE?

Figure out what you need it for before just getting everything you can into it. That's probably the main thing. We recently brought in an external firewall and it has everything enabled. So make sure it can do what you want and don't try to do more than what you need. We have made a few playbooks, but we haven't done too much with them yet. For deployment and maintenance of the solution, it's just me doing the administration.
We're at 60 or 70 log sources right now. With some of the newer ones, we've had to open up tickets for them, like the newer Cisco Wireless. We've had issues with Windows Firewall and AdBlocker. We've had to get those fixed. We process about 600 messages per second. In terms of the maturity of our security program, we got this solution right after we started up, so it has been growing with us. We're now at a point where we're happy with it and getting good value out of it.

Learn more: Read 40 reviews of LogRhythm NextGen SIEM