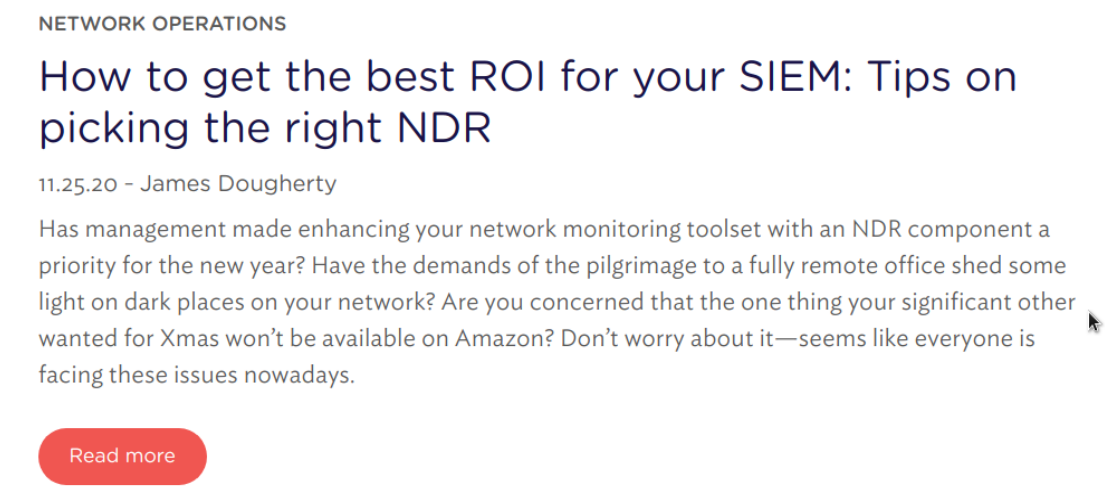
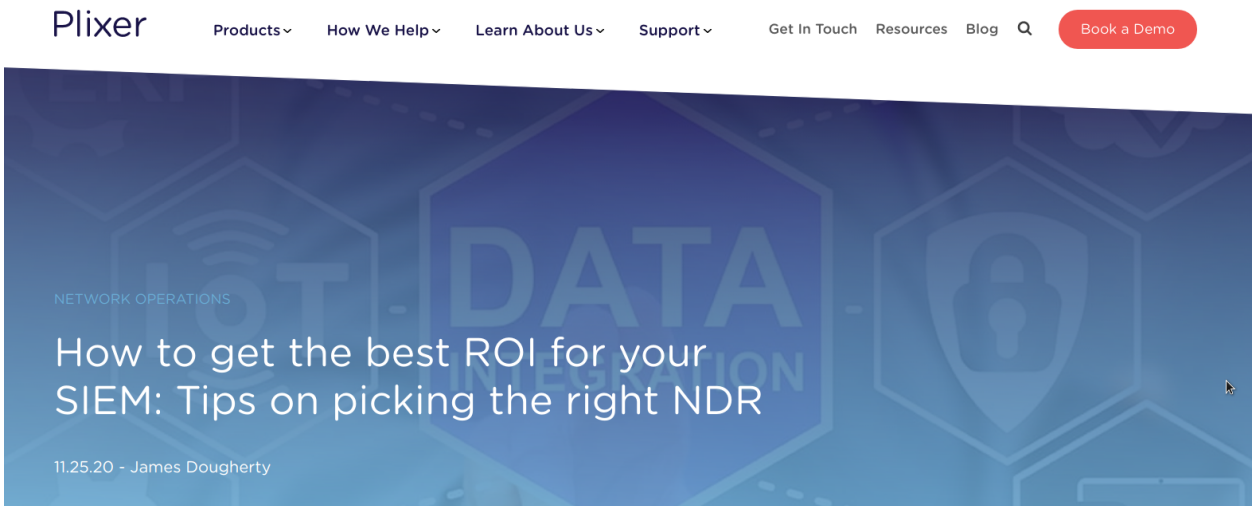
Originally Posted On:

How to get the best ROI for your SIEM: Tips on picking the right NDR
https://www.plixer.com/blog/picking-the-right-ndr/





Has management made enhancing your network monitoring toolset with an NDR component a priority for the new year? Have the demands of the pilgrimage to a fully remote office shed some light on dark places on your network? Are you concerned that the one thing your significant other wanted for Xmas won't be available on Amazon? Don't worry about it—seems like everyone is facing these issues nowadays.

Over the past few months, I've been working with clients on these exact issues and I've decided that I would pass along what I've learned. Well, except for the Amazon part. I really don't know

what my significant other wants. I just opened the Amazon account to her and said, “Go for it.” I might have to sleep on the couch for a week, but I know she’ll get what she wants!

Seriously, I want to talk about some of the pitfalls that evaluators have run into while looking at NDRs for their SIEM-enhancement projects. Along with that, I would like to give some helpful hints on what to look and ask for from a vendor.

> “A tangled web of non-integrated systems and alerts from siloed systems. Enterprises are now being forced to utilize a ‘Frankenstein’ of stitched together tools to create a platform that *might* cover their security bases. “ - Ana Mezic, Security Boulevard

In most cases, the people I’ve worked with were looking to accomplish three things.

1. Reduced workload

Management might call this “improving efficiency,” but us trench soldiers call it common sense, right? For years we have all been scripting our way to fewer steps, but with the complexities of today’s networks, finding the time and resources to do this is difficult. I mean, with the amount of data that’s out there, you really do have to start working smarter. When looking at any tool, ask the vendor what their vision for the future is. How are they, as a company, working towards reducing the steps needed to find the cause of a situation while still providing deeper context? Are they leveraging some of the newer technology like machine learning to help the end-user?

Trust me, you don’t want to be the one left holding the ball when SHTF and people start asking questions. Make sure you have confidence in the application and the company that supports it from the beginning.

2. Solid foundation

The devil’s in the detail! Your NDR tool will be the foundation of your toolset. You need to ask yourself what you need to see and what you expect to see. It’s funny, I always ask this question at the beginning of projects that I work on but many times I get a blank stare and they say “conversation data.”

Although this is a vague answer, it does point out a big problem. Simply put, teams often don’t know what they want until they need it. This makes things tough because the idea of knowing everything about everything puts a lot of weight on an admin’s shoulders. You really want to take on the best players, or in this case application, for your team. You want people who know their stuff going to bat for you. That’s why the phrase “best-of-breed” evolved from a gut-wrenching marketing term to a mantra chanted by many of today’s toolset gurus.

So when someone like me asks you what you need to see, I would respond with a few questions of my own. I would ask the company about other companies they have worked with that had similar goals. What challenges have they come up against? How did they solve it?

On the technical side, there are a few questions I would also ask. How is conversation data gathered? Are they probe-based or do they leverage other information like metadata provided by their current network devices? How does their deployment model affect your resources and is it scalable? How do they store your data and are you limited to what data you can retrieve?

3. Optimizing existing tools

It's all about the Benjamins, right? In my almost 30 years of experience, I find it rare for a company to scratch everything and start new. Please don't flame me with hundreds of examples of how the company you used to work for got rid of all of the monitoring tools and went for vendor XYZ. Trust me, it's rare for medium- to large-scale companies to do this.

This means that any new tool needs to be able to integrate with your other applications in some form or fashion. When looking at a tool, ask the vendor if their database is open. Do they have the documentation and resources to help you with your integration project? Do they provide integration options at the GUI and API/script level?

Specifically on the NDR side, an application's API is the glue that fits everything together. When considering a network detection and response tool for your SIEM, the API's functionality—and more importantly it's flexibility—is something that tends to be overlooked. APIs are developed to play a specific role: unlocking data from systems, composing data into processes, or delivering an experience. My advice is to make sure you can connect data to your other applications through reusable and purposeful APIs. Not only will it make your life easier, but management will think you are a rock star!

Adding context to an incident and not having to click through multiple applications to find its cause not only saves time and money but also improves the ROI on all of your tools. Are you looking for conversation-rich visibility along with the flexibility to integrate that data into your

current environment? Why not evaluate Scrutinizer?

James Dougherty

I have worn many hats in my professional life. Support engineer, developer, network admin and manager are all points on my resume, but the one common thread with all of these jobs is that I enjoy working with people; that is what I do here at Plixer. I make sure that everyone understands our product and can get the most out of it. It's just simple 'no bull' support!

Let me know if you have any questions, I would be happy to help.

- Jimmy D

Plixer

68 Main St Ste 4
Kennebunk, ME 04043

Phone: 1 (207) 324-8805