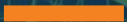


WhatWorks

A short, solid orange horizontal line is positioned above the main title.

WhatWorks in Reducing Time to Detect with Limited Staff Using Network Detection and Response Tools

Introduction

The visible financial impact of ransomware attacks has increased the need for security operations to reduce time to detect, mitigate, and restore. Visibility into network traffic is a critical security control for keeping up with the changing threats. At the same time, business demands for more mobile and cloud-based applications are making monitoring and threat detection more complex. Financial pressures in today's environment are also putting a premium on processes and tools that can quickly show positive return on investment without high staffing requirements.

In this SANS WhatWorks, John Pescatore interviewed Alfonso Powers, Director and Chief Information Security Officer at Assante Health to gain his insight on what he went through in the business justification details and deployment of ExtraHop Reveal(x) to increase visibility into network traffic. Assante Health is a Southern Oregon-based health care provider, with 200,000 customers and 6,500 employees across six hospitals. The increased visibility and the higher fidelity of detection allows Assante's small security team to detect and disrupt most attacks in progress.

About the End User

Alfonso Powers is the Director and Chief Information Security Officer at Asante. Prior to joining Asante, he served as the Director of Information Technology (IT) for a regional managed service provider and also as an IT leader in software development. He has a passion for information security technology and a continued interest in offensive security techniques. Over the past five years he has built Asante's information security program through strategic partner relationships and working closely with senior leaders. When not working with technology, he enjoys spending time with family, golfing, and traveling.

About the Interviewer

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008, and is an NSA-certified cryptologic engineer.

About SANS WhatWorks

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.

Question

Tell us a little bit about your background, your position at Asante, and what Asante Health does.

Answer

I'm the Director and Chief Information Security Officer at Asante Health. I've been with the organization for over six years now and report directly to the CIO. My background has been information security over the last 10 years or so. Prior to that, I did a lot of professional services and some software development; but my career really started from the ground up, working on a service desk.

Asante Health is Southern Oregon's premier healthcare provider, covering nine counties and about 200,000 lives. We also service a little bit of Northern California. Asante has three main hospitals and over 50 clinics in the service area. We have about 6,500 full-time employees. Contractors and part-time employees bring the total to somewhere between 7,000 and 8,000.

Also, medical devices are very active on our production networks. They're hard to secure because the vendor configuration and installation standards are usually not very good from a security perspective. That's unfortunate but understandable. From the medical care delivery side, the devices need to work, so the vendor sets up the network and makes sure everything works. It is up to us to close the security gaps.

Question

What was the business problem that drove you to look at solutions like ExtraHop Reveal(x)?

Answer

When I got to Asante, the security control framework that existed was immature for the most part. We really didn't have many solutions in place. The major threat we were looking at needing to mitigate was ransomware. Network detection and response (NDR) like Reveal(x) was one of our final pieces to put into that security orchestration automation response (SOAR) architecture. I felt we needed that kind of visibility into network threats that might be active inside the network. We had a pretty solid set of perimeter security controls in place, but security inside the network is a little more difficult.

We started investigating NDR in 2020. Then in 2021, one of our Community Connect partners that uses Asante's EMR electronic medical record system got hit by ransomware and was down for over 30 days. This created a little bit of angst and anxiety in upper management at Asante. That gave closing our visibility gap some more urgency—and in 2021 we made the investment.

Question

Did you have an existing budget for this effort? How did you get the funding to do this?

Answer

The budget and the funding did not exist prior that partner's ransomware event. So, we had to scope it out and go to management for the funding. Fortunately, our board of directors has many local business owners who were familiar with the risk of ransomware. The board was actually asking us what we were doing to mitigate ransomware risk. We were able to point to what we had already started looking at.

So, we made this proposal to the executives at Asante, who ultimately took it to the board. It got approval that way.

Question

Okay. So now you needed to build out network detection and response to close that visibility gap and had the budget. What was your process for selecting a solution?

Answer

First, I got our security team together and defined our requirements. We had already deployed a SOAR product. A top requirement was that the NDR product had to work with that—and integrate with our SIEM product, too. We also had requirements around our network's speeds and feeds and the like.

We ended up evaluating two products, one of which was ExtraHop. It was a close decision, but ExtraHop had a couple of features that pushed it over the top. One key feature was SSL decryption, which is really important for us—to know that we could see everything in the network.

The user interface for Reveal(x) is also more of a single pane of glass. The other tool we evaluated, we had to open up different consoles to actually get all the data. Another important capability was the continuous packet capture, which lets us log network data all the time, whereas in the competitor's tool you had to turn that capability on and off as you needed. Those were the decisions that ultimately swayed us. So, over a 6-month evaluation those were the main features that gave the edge to ExtraHop. It was a good proof of value.

Question

What was involved in setting up and getting going with Reveal(x)?

Answer

The way our network is architected, all network traffic flows back through our main data center from all of our facilities. We use a span port connected to a network switch, which feeds the ExtraHop appliance with all the data—and that's how it's analyzed. We went with a span port to get started but will be moving to a network tap very soon.

During the proof of value we did with ExtraHop, we ran it for a full 30 days, which enabled the machine learning to build a good baseline of normal network activity. But, the more we saw, the more it alerted us to other things—essentially security issues that we kind of stumbled on.

Question

How do you use Reveal(x) in production?

Answer

The data that's collected through and analyzed by the tool results in alerts being created that are fed to our security information and event management (SIEM) product. The SIEM processes and prioritizes all alerts and then sends alerts to our automation platform. The SOAR platform will then take it and alert the actual analysts and the rest of the team who need to follow up on potential issues.

For complex issues, the analyst will then use the Reveal(x) tool to investigate more deeply. We don't have a large team, so we try to automate as much as possible. The team can take action based directly on the alerts.

ExtraHop gives you a lot of data. Usually it can make a good determination of whether it is a false positive or a legitimate incident based on the behavior of what it sees.

Question

How does Reveal(x) prioritize alerts?

Answer

ExtraHop uses critical, high, medium, and low severity levels for its detections. Critical is almost always some form of active exploitation for which we want rapid response times. The priority levels have seemed pretty accurate.

Question

Can you give us a recent example of how this works?

Answer

A lot of ransomware attacks exploit vulnerabilities in the **Windows Server Message Block** protocol. ExtraHop Reveal(x) will alert when it detects an unusual volume of connections over a network protocol. In this case, Reveal(x) alerted on **SMB** events that were outside our normal network behavior. So when that alert came in, the analyst was able to determine that an actual employee was doing part of their job by digging deeper into the traffic with Reveal(x). The employee was doing a bunch of scanning and copying out to a network share. Based on that type of alert, Reveal(x) will allow us to isolate the threat during the analyst investigation, using an EDR technology from the endpoint protection platform we use on PCs. If, as in this case, it was legitimate traffic, the analyst can perform the EDR isolation remotely. If the analyst determines it was a legitimate incident, he or she can also use the tool to remove the threat.

With Reveal(x), when something like this happens, you can tell it that the behavior is normal, and Reveal(x) learns from it.

You can declare events as false positives to eliminate future events, but we don't like to do that. In this case, it was legitimate employee activity—but it really was outside normal actions. We still want the product to detect, alert, and have an analyst look at it.

Question

What's the skill level an analyst needs to use the tool?

Answer

There is a lot going on in Reveal(x), for sure. Training is recommended. Any senior analyst would quickly be comfortable using it. But I wouldn't say it is geared toward an entry-level security person. Overall, we have four or five Reveal(x) users who each had about 5–7 days of training.

We've also used Reveal(x) to troubleshoot several performance issues, both in the on the network side and virtualization side of things. At those times we had other teams also looking at the data. But, day in, day out, it's usually just information security using Reveal(x). It does provide a lot of data that is useful and important for those other groups.

Question

You mentioned indicators of compromise. Is there a feed of IoCs that comes from ExtraHop Reveal(x)? Do you use external threat intelligence feeds? Do you use all of the above?

Answer

ExtraHop provides its own threat intelligence, which we use. We are not currently using any other intelligence feeds.

Question

You've been using ExtraHop Reveal(x) for over a year now. How have you found the performance to be from a false positive/false negative perspective?

Answer

I think it has worked out pretty well. We've really done some hard work, tuning the tool to really give us good data. We are finding good value with it.

Question

You mentioned one of your key requirements was looking at SSL traffic. How has that worked out?

Answer

That has worked out very well. We had a jump start on it because we knew that our edge firewall was passing a lot of SSL traffic. We were able to size everything properly with ExtraHop Reveal(x) to make sure we had full visibility into the encrypted traffic. For privacy reasons, there are some categories of traffic we do not decrypt.

Question

Are you storing the stream data and the packet data? How does that work?

Answer

Yes, we are storing it. It is done with ExtraHop Reveal(x). During the sizing process, Reveal(x) will help you size how much hard disk space you'll need for your use cases.

Question

What are your plans for expanded use of Reveal(x) in the future?

Answer

We want to expand it to network performance and metrics. That's something we definitely will be looking at as we get more into adopting things, such as zero trust and micro segmentation. We also have a small Microsoft Azure footprint. We are looking at folding that cloud data into our tool set.

Question

You went from evaluation to operational use. What sort of lessons did you learn that you could pass on?

Answer

I would say: Definitely make sure you have the resources dedicated to deploy the technology successfully. This is a powerful tool that, as I mentioned before, you really need focused tuning and training to get the value.

It's easy to turn it on, set it up, and start getting all this data.

That's great. But to really start seeing meaningful improvements in your security status will take some time and some patience.

Another thing is: Make sure your stakeholders and others that support information security know what may happen when you set up a tool like this. Especially at the start, you should expect false positives. If you're not careful, you're going to, potentially, impact business operations in places. But, tuning of the tool will really help reduce the possibility of that quickly. Make sure that's well-understood from all the other stakeholders and other operational owners in the organization. It will pay off in the long run. You get just way better buy-in that way.

Question

Do you keep any metrics to demonstrate the value to management and stakeholders?

Answer

The best one is, by far, no incidents so far! We do report on how many detections, how many minutes it took for an analyst to resolve and go through the workload, and other numbers like that. You can compare that to how the manual process would look and how long analysis and detection would take. There is no comparison. Comparing manually going through all the data versus what you get from the tool puts a big light on why Reveal(x) was a good investment.

Question

Have you used tech support from ExtraHop? How do you rate the support?

Answer

The support is included in the agreement. When our teams have interacted with them, I would say their support is pretty good.

We get good response time from them. Their engineers are smart and have always been willing to help us.

Question

How was the integration with your SIEM product and your automation product? Was that straightforward, or is that one of the things that took some help?

Answer

The SIEM integration was pretty straightforward there. The automation product has been more difficult; but, ExtraHop has been willing to do whatever it can to make the integration to the other product work. They're taking a lot of feedback and findings and are adapting that automation integration to actually improve it.

Question

Anything I didn't bring up that you'd like to bring up about your experience using Reveal(x) over the past year?

Answer

I'd say we very quickly saw that the tool actually helped us identify other vulnerabilities on our network. A Reveal(x) alert would be reporting weird behavior that turned out to be an exploitable vulnerability in software running on our network. One member of our team investigated a weird web request that Reveal(x) reported going on in an application. Based on further investigation and research—and doing some testing—***we were able to find a serious SQL injection vulnerability in a product we were using. That points out that the tool is valuable for both threat hunting and vulnerability assessment.***