SANS Analyst Program

WhatWorks

WhatWorks in Reducing Time Detect at Scale Using Network Detection and Response Tools

ExtraHop

Introduction

The financial impact of ransomware attacks has increased the need for security operations to reduce time to detect and mitigate threats and restore connectivity. In addition, financial pressures as the world comes out of the pandemic are putting a premium on processes and tools that can quickly show positive return on investment without high staffing requirements. An effective and efficient way of achieving both objectives is for Network Operations and Security Operations to use common tools that support insight into both performance issues and security-relevant changes and anomalies.

During this SANS WhatWorks webcast, SANS Director of Emerging Security Trends John Pescatore interviews Lee Chieffalo, Technical Director at Viasat, about his experience with the business justification and deployment of Extrahop's Reveal(X) to increase visibility into network traffic. Viasat is a large ISP and services company that needs to protect its own networks and its customer systems from advanced attacks. The increased visibility and the higher fidelity of detection provided by Extrahop's Reveal(X) allows Viasat to detect and disrupt most attacks in progress.

About the User

Lee Chieffalo is the Technical Director of Cybersecurity Operations at ViaSat. Prior to joining Viasat, he completed three combat tours with the US Marine Corps and actively served for nearly two decades. After spending the majority of his military career as a network architect and engineer, he served his final three years as the lead networking and cybersecurity instructor for Marine Forces Pacific Command. Today, Lee still enjoys traveling the world and has visited 52 countries to date. In addition to working at Viasat, he also teaches for California State University in their cybersecurity program.

About the Interviewer

John Pescatore joined SANS as director of emerging security trends 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.

Question

Tell us a little bit about your background and the role you play at Viasat.

Answer

I spent 15 years in the Marine Corps, came out and joined Viasat in cyber security. Early on, we were asked to start building a cyber security capability for Viasat commercial services network on the ISP side of the house. Over the last seven-and-a-half years now, we've built that up and merged with the government side to build a pretty high-level SOC.

Now I'm the Technical Director of it, and my role is to go out and understand the existing and new technology and find the best ways to augment and implement that technology to increase our staff's effectiveness, efficiency, and accuracy.

We handle the cyber security operations for the customer service-facing network. We're responsible for protecting all of our customers that leverage our satellites for transport, which includes federal/state/local government, big and small business, as well as residential.

Question

What was the business problem that needed a solution that caused you to start looking at products like ExtraHop?

Answer

As a SOC protecting a wide range of customers, we've always been tasked with finding and removing bad traffic from the network, identifying suspicious traffic to make a call on, whether it's good or bad.

In order to do that, you need to be able to see what's crossing your network, and ExtraHop allowed us to get complete visibility of the ground truth of pretty much every frame that's written to the wire on the network. That key capability is the enabler of our other security capabilities.

Question

How did you convince management to approve the funding? Was this just part of the sort of yearly cycle of improving things, or was it a specific project to improve gaps in visibility?

Answer

It was both. We have some pretty critical customers on the network and we need to be able to understand the traffic that's being sent to them or produced by them in order to make a determination on malicious traffic or not. It was an easy justification from that side of the house.

But for the ISP side of the house, there had been more of a "We're a gateway to the internet, what do we care what people are doing?" approach. It came down to more of a bandwidth reclamation, bandwidth optimization type business justification for the visibility. Our cost per bit is a lot higher than a terrestrial ISP, because we're running on a billion dollar satellite, instead of just running fiber underground, so identifying malicious traffic and removing it before it consumes those resources is high business value first and cybersecurity gains come with that.

Question

How did you look at different solutions? How did you compare them? What process did you go through?

Answer

There's log data, there's NetFlow data, there's a lot of different ways that we could have gotten to that visibility. But every device on the network, regardless of if it's one of our clients, or part of our infrastructure, has to get to and communicate over our network. I'd say that it is in the high 99 percentile range that malware gets on the network somehow or another, either it sends traffic outbound, or you can see the attempt to compromise the machine coming inbound.

It just made sense to start with "Let's capture it in transit and be able to drop something." Also, from our customer network, as an ISP we don't own the administrative control over either end of the conversation, so the only place where we can prosecute on anything is on the network while it's in transit. That's why we needed to have something for passive network inspection.

Question

How did you go about comparing the alternative products?

Answer

We did a bake-off between ExtraHop and a few other vendors and ExtraHop outperformed everybody. They had the scaling capabilities that we needed, and the AI analytics capability that we wanted that was far above all the other people that we tested.

We deployed a set of their sensors for all vendors and we tried to place them in the same areas so they were looking at the same traffic, and we could compare apples to apples. We put it in one of our core nodes, a couple of hundred gigs per second of traffic, and some of the vendors that we tried couldn't even scale to the amount of traffic that we needed to push through it. ExtraHop was able to ingest and analyze that traffic with a very small resource footprint compared to some of the other competitors, which definitely set them ahead right away.

ExtraHop allowed us to get complete visibility of the ground truth of pretty much every frame that's written to the wire on the network. That key capability is the enabler of our other security capabilities.

Question

What does the physical and network architecture look like to get the visibility you need?

Answer

The taps already exist inside our core framework. They have to be there for Community Assistance to Law Enforcement Act (CALEA) requirements that the government demands. Since we have to have the ability for lawful purposes to be able to tap that traffic anyway, we just hung it off that tap and filtered a bunch of VLANs that encompassed that geographic region of the country. For the evaluation, we were looking at the depth and breadth of the traffic that we able to see, and to answer a few key questions about the performance of the overall product: How did the out-of-the-box detection work? How accurate were the rules, and how easy it was to augment those detections and implement our own behavior analytic models into the system in order to detect more advanced threats?

Pretty much, where our internet touchpoints are, where our primary internet circuits are, where we feed all that traffic in and out of the internet is where we hung up right off that. We used sensors on our primary internet touchpoints. One of our internet super highways just passively off-ramped the traffic and analyzed that, found a bunch of cool but dangerous traffic that we got rid of in the time we had the proof-of-concept active. ExtraHop exceeded expectations in all the test.

Question

It sounds like you're talking about really high volume rates of traffic. Are you looking at live data? Is this traffic being stored somehow?

Answer

ExtraHop has the ability to store 90-plus days' worth of traffic as necessary for future analysis and packet capture or other needs. We didn't really want to store our customers' data for that long and doing packet-by-packet payload analysis on a long-term scale was outside of the scope of what we needed to do. It was more for our management control plan in that area that we did that, but they have a NAS type extension that attaches to their sensor that just stores up to 90 days' worth of traffic as needed. Really easy to implement, really easy to configure, easy to maintain. It's racked in our core node, took maybe six to eight U of rack space.

Question

You mentioned using the preexisting filters or signatures: how'd you see the false positive, false negative performance work out?

We did a bake-off between ExtraHop and a few other vendors and ExtraHop outperformed everybody. They had the scaling capabilities that we needed, and the AI analytics capability that we wanted that was far above all the other people that we tested.

Answer

The ExtraHop system has two analytic looks, one for network optimizations, from a functionality, availability, optimization standpoint, as well as a security standpoint. From the network optimization side you get very more accurate numbers on number of sessions, latency, hop counts, network statistics that would allow our network guys and our traffic shapers to make a determination like, "How well is Netflix, or YouTube performing, or how well is audio traffic performing?" They could see the gaps or at certain times of day, how that traffic performed on the network. Very accurate information provided. We haven't seen anyone else come close with the tools to allow our traffic guys to make a determination on how to better adjust things on the network.

From a security standpoint, out of the box, ExtraHop picked up all the security relevant traffic issuers very quickly. Once it learns the network and understands the directionality of what's yours and what's not yours, they have really good detections on detecting rogue DNS servers, rogue DHCP servers, whether or not people are using expired or out of date crypto protocols, or operating

system identification, browser identification, and using really outdated browsers. I was really surprised to see people still using Android 2 on the network. Some customers that were going on the internet using really ancient systems, a lot of IoT devices that we discovered using really, really outdated Linux kernels that are highly exploitable and haven't been supported in decades.

Right out of the box, it enumerates all that stuff, certainly all of the low-hanging fruit type malicious activity. The port scanning, brute forcing, DDoS attacks, stuff that's really noisy, relatively easy to pick up via signatures, were detected and identified right away. Compared to our prior use of sampled NetFlow prior to that, we got significantly greater visibility on the network of what kind of bad traffic, unsolicited traffic that our customers were not asking for and we were able to remove it.

SANS and others have put out reports that a new IP address is typically attacked within 2 minutes of when it goes live on the internet. I got to see that play out live because we'd have new customers pop online, and within a minute, maybe a minute and a half, we'd see all the automated scanners and brute forcers just hammer that IP. I mean, 8 to 10 thousand attempts per second from all over the world is a huge volume of unsolicited traffic and it impacts everybody.

Question

So, both the Network Operations Center and the Security Operations Center teams are using ExtraHop?

Answer

Yes, with ExtraHop the NOC can do a lot of application troubleshooting directly. This works especially well with our DNS servers and DHCP servers, because you can see how they perform frame by frame from where the client requests something and their response. You can get latency and what they're responding to, how big those panels are, so you can make a much more accurate decision on what you need to do to make it better and start tweaking stuff.

When changes are made, any network differeces from those changes would be seen immediately and any problems corrected quickly.

Question

How's it typically used on the security side?

Answer

We have a little bit of a different SOC in the sense that we don't just have analysts sitting in seats looking at alerts. We get five billion live events per day, and we don't have enough analysts in the world to triage that directly. We like to feed everything into a risk calculus and an ExtraHop plays a big part of that. We have a set of triggers built into ExtraHop to pick up on various behavior anomalies or various adversary TTPs (Tactics Techniques and Procedures) that we identify from network attacks that we have studied. We generate a risk calculus based on that behavior, or that attack pattern or traffic pattern, and then send that into our Security Information and Event Management (SIEM) server to be combined with other data sources to get an aggregate level of risk. If that aggregate level of risk is higher than that client's risk acceptance, then we do something about it, so it depends on what the traffic is.

Sometimes there's traffic signatures that might be suspicious or malicious in nature, but either the attack pattern or the attack

site is irrelevant to the customer or the customer type, because maybe it's a scan to exploit something that the customer doesn't have on their network. They're seeing the malicious traffic, but it's irrelevant to their current situation, so it ends up scoring as a low amount of risk, so no action is taken. But once the aggregate risk scores above that aggregate risk score that the customer is willing to accept, then we either remove or mitigate the traffic the best way possible.

ExtraHop was incredibly easy to pick up on. Anyone with network experience had at most two one-hour sessions with ExtraHop over the phone to be able to do everything and between my team and them, it was real easy to pick up on, the ramp up time was really easy.

Question

Do you develop your own custom ones and push them into ExtraHop as well?

Answer

Yes. We have a group of data scientists that work with us. We also have a group of human and signals intelligence people that work with us that are embedded in the SOC, as well as some network and security engineers who understand how normal traffic should work or what normal should look like. They tear apart different threat factors, different TTPs that we get out of threat intelligence sources, government, and professional threat intelligence sources, or that we find on our own that we know that this is something that is abnormal on the network based on your behavioral patterns.

For the most part, as an internet customer, for pretty much every single internet customer, after about a month of looking at your traffic, I could tell you the websites you're most likely going to connect to. We're creatures of habit, so after a couple of weeks' worth of analytic data, I know 90% of what you're going to do. If you start going to abnormal locations, either you have somebody visiting your home or your business that's normally not there, or you've got some sort of malware that's doing something it shouldn't be able to do.

Attackers change their infrastructure on the fly, so by the time you get a threat intelligence source saying, "I was attacked from this infrastructure", it's already stale most likely, especially if it's an advanced threat. They're going to have a dedicated infrastructure to attack you guys, but they don't change their behaviors, their behaviors stay the same, just coming from different locations. With ExtraHop we can key off on that behavior, we can find and remove it before it gets out of hand, and that's where we build the models, and ExtraHop just triggers in order to find and remove that traffic.

Question

Once you made the decision to go with ExtraHop, how long did it take you to go operational with the product for SOC use?

Answer

The better part of a year, I think. To make any type of changes on our production network for our ISP side of the house takes a lot of proving that it isn't going to impact the operation, or the SLAs customers have signed up to for internet connectivity. With Government customers it was quicker than that – they were willing to move fast to get higher levels of security.

For government and critical infrastructure clients, and the commercial business clients, it was a lot easier to get in place to analyze their stuff, because they actually have a security level of risk they're willing to take, and it's not very high.

Question

Can you think of any of recent attacks where you've used ExtraHop to security advantage?

Answer

We haven't been affected by ransomware all that much, but we see it on the network. We've seen WannaCry, Petya, NotPetya and other ransomware strains target our customers where they either downloaded, clicked on the phishing link somewhere, or they had something to beacon out and we're able to see that beacon, we're able to see that payload get downloaded.

We are often able to stop known attacks in transit. We've found plenty of that, where we stopped the ransomware payload download, or stopped Dridex, Cidex downloads, which is financial bot, like a banking credentials trojan.

Question

Are there any metrics the SOC keeps that you'd be able to point to improvements in, based on your use of ExtraHop? Time to detect, time to mitigate, things closed per shift by analysts or anything like that?

Answer

Our ability to detect traffic with ExtraHop is much closer to real time. The way that we were doing it traditionally prior to the implementation of an NDR solution was pulling data that took a couple hours to process and transform and analyze, and we were always lagging behind. NetFlow is closer to real-time, but it's sampled because the rate of speeds on our edge devices is so high, you can't do one-to-one traffic. Getting useful indicators typically took a couple of hours; we were lagging behind.

That delay meant that often by the time we were able to say, "Something bad happened" the attack's kind of gone. Usually, they switch infrastructure at that point, and any mitigation we put in place was stale and kind of a waste of time at that point. We were able to take that time to detect and identify, and bring it down to seconds to minutes instead of multiple hours.

The average attack life was around 60, 65 minutes, so we were able to get there within two, two to three minutes, then we can at least stop a majority of the attack while it's still going, and hopefully save something. We were also able to have a lot of blocks, filters put on the edge for known malicious traffic, because we could see the attacks happening, we have millions of end points on our machines, on our network, we could see the DDoS botnets, we could see the scanning botnets and whatnot. They're attacking us continuously; we can identify where they are and we can just drop them at the edge, so they just don't attack anymore.

Question

To use ExtraHop effectively, did you have to get training from ExtraHop or get additional skills training for people to use the product?

Answer

ExtraHop was incredibly easy to pick up on. Anyone with network experience had at most two one-hour sessions with ExtraHop over

I remember one hour with ExtraHop was based on the triggers and how to implement and write the triggers in JavaScript. That made it really, really easy to hit the ground running with low ramp up time for effective deployment. Some of the other products we had looked at required months for somebody to become comfortable using, because a lot of proprietary stuff is built in.

We use a proprietary search language; it does a bunch of really cool stuff, but putting an analyst on it or a person on it that's never used it before, it takes six months for them to be useful. ExtraHop was the complete opposite of that, really easy to use UI, really robust documentation, real simple using pretty much industry standard languages to search for things, super simple product to use.

Question

Based on those two years using ExtraHop, are there any lessons learned you could pass on to the audience or something you might do differently when you got started based on what you know after two years of use?

Answer

We did switch to the virtual version of the product; that made things a lot easier to deploy and scale. That was one of the hardest things that we had to do when we were doing the POC for it, was scaling enough sensors to meet the bandwidth needs. ExtraHop was able to cluster to do it, but that took a decent amount of rack space, and infrastructure type work to get it. I would say the virtual solution's a lot easier to use, and go with that as needed. But other than that, it's the ground truth, this is literally everything that's going on, and that's written to the wire, so once deployed and properly tuned, it's the ground truth of the network.

I remember one hour with ExtraHop was based on the triggers and how to implement and write the triggers in JavaScript. That made it really, really easy to hit the ground running with low ramp up time for effective deployment. Some of the other products we had looked at required months for somebody to become comfortable using, because a lot of proprietary stuff is built in.

The more work you put into tuning the product and tuning it accurately, it's exponentially better on the backend of it. It's a continuous thing. You have to always spend a little bit of time going back into it, and this is going to be the case for any sensor, and updating it, making sure it understands your network as it's changing, so you can always have the most accurate picture you can. It's a great product, and it provides you the ground truth of what's going on on your network.

About ExtraHop

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25 and SC Media Security Innovator.

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.