SANS

Analyst Program

WhatWorks

WhatWorks in Maintaining Deep Security and Enabling Detection and Response Across Data Center and Cloud Apps

ExtraHop

Introduction

Business use of multiple cloud services has continued to grow. And security operations have been pushed to extend security visibility, detection and response capabilities to the cloud, while retaining an integrated view across cloud and on-premises systems and networks. One effective and efficient way of achieving this visibility is for network operations and security operations to use common network visibility tools that support the views and 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 D.J. Fernandez, IT Security Engineer at Grand Canyon Education, to gain Fernandez's insight into the business justification for advanced network detection and response (NDR) capabilities and the key evaluation factors that resulted in the election and deployment of ExtraHop's Reveal(x) platform to increase visibility into network traffic to secure Grand Canyon's business and customer systems.

Join Pescatore and Fernandez to hear details on Fernandez's selection, deployment and experience using ExtraHop. The webcast includes a discussion of lessons learned and best practices and gives you the opportunity to ask questions to get deeper insight.

About the User

David-John Fernandez is an IT security engineer for Grand Canyon Education. In his free time he enjoys reading cybersecurity news, investigating security incidents and jumping into his own security projects. David-John also believes in the concept of continual growth for security professionals through shared knowledge and a feedback-oriented approach to IT security--via hands-on and theoretical experiences and discussions.

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 Grand Canyon.

Answer

My name is David-John Fernandez. I've been working with Grand Canyon Education as a junior information security engineer and information security analyst for around a year and a half so far. I'm nearing the end of my bachelor's degree studies in IT and cybersecurity.

Grand Canyon Education is an education services company that was split off from Grand Canyon University (GCU). We are expanding our services to other college institutions across the U.S., but primarily we service GCU as a customer and we work with other departments such as our networking team, our database team and our telecom team to provide further value with performance monitoring and anomaly-based security and performance detections with ExtraHop.

Question

Walk us through the business need that drove you to look at visibility, detection and response tools.

Answer

We had limited IDS capability, and there was a security incident that occurred between the December and January time frame for our company. Our CISO and CTO were looking for network detection and response (NDR) tools that could be used both to more quickly detect potential security incidents, but also provide our networking and other teams with better visibility into performance-related issues, in addition to gaining improved visibility into north-to-south and east-to-west traffic and accurately identifying risk factors.

We looked at several NDR products, including Extrahop's Reveal(x). We looked at all the details that were available on the website—features, costs, etc. I prepared a presentation for our executives, presented the material and then we did a proof of concept with ExtraHop.

Question

What were the criteria you used to narrow the list down from other products to only proceed with ExtraHop?

Answer

We looked at all the features based on a comparison with the other NDR solutions, and we assessed that ExtraHop would provide the most value to multiple departments in addition to IT security. It included a long list of items that it would monitor in regard to performance monitoring, help us gain further visibility into rogue assets that may be in our network that we're not really aware of.

Two big factors that also helped to convince us moving forward with ExtraHop were the SSL decryption capabilities that were offered, so we could inspect traffic that was usually encrypted and the support for historical metrics and packet look back.

That has been very valuable to many departments within our company because whenever there's an issue that occurs, whether it's an outage or a security incident, we have the packets and the metrics [and] we can dig into them further to try to identify the root cause with high fidelity.

Question

What during the proof of concept convinced you to go forward to deployment?

Answer

I worked with a solutions engineer and a sales engineer, to get the system started, and learned how to install the servers into our data centers. So I got hands-on experience with that. I then got in touch with the respective department leads and went through the value of the solution and then showcased how the data can be monitored—the dashboards that give visibility into critical performance and security events, etc. I showed them detections that occurred based off of the machine learning in ExtraHop.

Using ExtraHop also improved our existing processes to find and highlight deviations from the baseline of normal network activity—that was a real selling point.

Question

How did you collect network traffic to feed to Reveal(x)?

Answer

We configured a tap with our current Gigamon appliances. It was a span port configuration to the ExtraHop Discover (EDA 6200) servers at two data centers. The wire data is processed and reconstructed through the EDA 6200s for further analysis and processing. The rest of the wire data flows with the EXA and ETA appliances to process and store packet flows and L7-related transaction metadata.

Question

What is the typical analysis flow?

Answer

We have the data being sent over ExtraHop Reveal(x)'s open data stream connection method to our Splunk SIEM. The data is put in JSON format initially and then forwarded to Splunk where it is finally processed and indexed.

The first step is to establish a baseline, where we capture traffic under normal, stable conditions for two to four weeks. After that is complete, Reveal(x) provides built-in categories of detections that can relate to abnormal web application traffic, lateral movement, reconnaissance attempts, general exploitation activity and more. If there's a spike from the baseline with a particular metric, Reveal(x) will escalate that by creating a detection which indicates that this activity could be a potential incident, and it adds other investigation steps and supporting information to supplement the data. It basically creates a detection for review to determine if the event is truly anomalous, or if it could be a part of backup traffic or other legitimate activities that consume large amounts of network traffic or resemble general anomalous network activity. This data can then be assessed further through further review with system administrators or across our security operations tools using the Splunk SIEM and our other security controls.

I worked with one of our IT security engineers, and we assessed the detections using a risk-based analytics approach. Detections relating to categories of concern were higher priority than detections that did not relate to traffic patterns or a category of concern. We used this newly engineered capability to rate events as high, medium or low risk. Then we used custom searches to generate security-notable events for our SOC and incident response analysts to review.

We get the initial hit from prioritized notables in Splunk and then we review the detections in more detail in ExtraHop as well as other supplemental tools and especially take a look at the history of the detection and the devices in question. We also look at the following data points: Has it been seen on the server over a series of time? Is this something [where] we need to create a new detection rule because it's a known false positive, because it's our vulnerability scanner scanning the asset and triggering tons of detections? Or is it something that we should look into assessing further based off of other potential IoCs or IoAs and then taking the relevant remediation actions from there?

Additionally, the dashboards have been the most powerful feature of ExtraHop, in my opinion.

We found them straightforward to customize. Of course, the dashboards will vary for each organization that uses ExtraHop because you might be primarily a cloud shop or a database company or you might work in the education sector like us. There is an extensive list of metrics that you can populate those dashboards with to create custom visualizations to really show how system traffic changes over time and if there are any other details that require further threat hunting. We have a threat hunting dashboard that we can use whenever we get an indication of a potential incident.

Question

How long did it take you to go from making the decision to go with the product to becoming operational?

Answer

We were in POC from December 2019 to around the middle or end of January. From there it took us about a month or two to process the procurement order and then get started up. We did an immediate rollout from POC to production. Everything we were running in POC just went right into the production capability.

Question

Is Reveal(x) being used for both security use cases and performance use cases?

Answer

It is being used across our team, the database team, the networking team and, recently, the most with our telecom team as well, given recent issues driving greatly increased remote access and assuring sufficient network performance requirements. The work-from-home requirements caused us to make the "digital transformation" nearly overnight.

We currently have a VPN dashboard that has all the respective metrics that we need to assess traffic load and to determine if we need to expand the bandwidth or adjust traffic prioritization in relation to traffic use and what services/protocols were observed. We recently had issues with Cisco Jabber Unified Communications software and some of our calls dropping unexpectedly. We created Reveal(x) dashboards to help provide a visual illustration to support root cause investigation. We were seeing retransmission timeouts (RTOs) being unexpectedly high at a certain period of time, and we could drill down and see packet drops or TCP resets, etc. alongside those metrics.

The visibility from the dashboards, records, metrics and packets within ExtraHop helped us visualize what issue was occurring and if the data related with some type of attack or not.

Question

Where are you using the SSL decryption capability?

Answer

Currently, we are mostly using the SSL decryption capabilities to inspect server application traffic. Those are high-value applications, so we really want to monitor them closely and very quickly determine if there are any anomalies or attack patterns in the HTTP stream. It is powerful and works great.

Since ExtraHop's monitoring the traffic across all protocols, we've actually found some hidden "gems" in our infrastructure. For example, one system was using a Telnet connection, which meant we were sending some credentials in the clear. We were able to pinpoint that system, identify the credentials that were being used in the clear and then validate that those credentials were not being used with our other systems through manual analysis and further follow-up.

We have also been using ExtraHop's response and threat hunting capabilities to help improve our infrastructure from a security hygiene perspective and then mapping those risks accordingly by level of likelihood and severity if exploited. ExtraHop provided a custom security hygiene report to us that helped us prioritize the remediation of those discovered risks.

Question

You've been operational for nine months now. Based on what you know now and the experience you have now, are there some lessons learned or something you would do differently at the beginning based on what you know now?

Answer

One of the first things I would have done from the beginning is to more deeply look into the assets that were most important to the organization. This could have been efficiently completed earlier by proactively creating all the respective device groups appropriately and mapping that to the appropriate standard and advanced analysis priorities so that our levels of analysis would be prioritized based on the criticality of the assets. For example, would we want to give our VPN clients advanced analysis and then use that quota instead of our servers? Initially, we prioritized using our Reveal(x) license quotas on VPN clients for advanced analysis. Then we realized the server side of the business applications was more critical, and we adjusted the allocation.

We then populated the Reveal(x) analysis priorities and device groups primarily by using SolarWinds Orion and other sources to assign the business criticality of the asset. We then mapped those custom device groups to the appropriate analysis priority and allocated the servers to advanced analysis. We ended up using our servers in Reveal(x) advanced analysis to look at the layer 7 transactional flows. Our client devices would receive aggregate network metric data through standard analysis. So that's one transformation we made to optimize the system further that I think would have been better had we done it from the beginning.

Reveal(x) gives us powerful capabilities to quickly identify and investigate suspicious network anomalies.

The methods you use to analyze your baseline of network activity also drives the quality of any form of an anomaly-based detection. There is the initial baselining, and then as you start to investigate alerts, you find other events or flows that are not malicious and you may want to update the baseline accordingly based off some form of historical document. ExtraHop supports doing that with their detection history, but we started using a wiki system to keep track of the details of adjustments relating to normal baseline network activity. Having that history of normal network activity when compared to the baseline, as well as newly created security and performance detections, would have been very useful to have earlier as well when we started to do our investigations in Reveal(x).

Question

To use the Reveal(x) capabilities, what level of skills did you need? What sort of training or education is required to really make use of the product?

Answer

I would say to be organized and just a willingness to learn.

ExtraHop provides great training materials through their training store, with a basic user certification provided to ExtraHop customers free of charge.

Beyond that, the engineer should have basic knowledge of network and internet protocols, as well as basic cybersecurity concepts. But the Reveal(x) user interface is easy to learn and use once you use it more over time.

Question

I think you mentioned you worked with one of the solution engineers to get started. Did you use ExtraHop technical support services for call-in questions—and if you did, how do you rate their service?

Answer

Yes, we used the support team and the solutions engineers. I would rate their service with a high rating—since I'm in a university, I'll stick with theme of the university grading system and give them an A!

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.