SOPHOS

A Day in the Life of Sophos MDR Analyst

An Interview with Anthony Bradshaw, Sophos MDR Manager

Sophos Managed Detection and Response (MDR) is a fully managed 24/7 service delivered by security experts who detect and respond to cyberattacks targeting computers, servers, networks, cloud workloads, email accounts, and more.

Get a behind-the-scenes look at a typical day for Sophos MDR Analyst and Team Lead, Anthony Bradshaw. He'll dive into the importance of MDR, share the daily activities of a security analyst, and highlight a recent example of threat detection and remediation for an MDR customer.

A Sophos Whitepaper. February 2023

Before we look at a day in the life of an analyst, can you take a step back and first talk about Managed Detection and Response? MDR has become such a hot topic lately. As Sophos recently surpassed over 15,000 MDR customers and was named a MDR leader by Gartner, it feels like you're in a perfect position to explain what MDR is and why it matters.

Q. Before we begin, how would you define MDR?

As you pointed out, MDR is the industry acronym for managed detection of response, but it's so much more than that here at Sophos. It's threat intelligence, threat hunting, threat research, detection engineering, incident response, and so on. It's a complete package for protecting critical systems with the ability to have highly technical analysts responding to adversaries at the drop of a hat.

> That proactive defense is necessary as cyber threats increase in volume, complexity, and impact. Gartner anticipates that in just a few years — by 2025, actually — 50% of companies will be using MDR for threat monitoring, detection, and response.

Q. Can you expand on this rapid increase and why taking action is so important?

I think many factors contribute to this, but at a high level, organizations realize it's challenging and expensive to staff up an entire cybersecurity unit on top of all the other things that come with managing technology assets.

I saw a stat the other day that said there was a 78% increase in the number of organizations hit by ransomware last year. MDR allows organizations to offload that responsibility by allowing experts like our team of analysts, researchers, and threat hunters to deal with the cyber part.

When it comes to taking action, it's critical to get it right — and quickly. Threat actors can move very fast, and before you know it, your entire network is down, compromised, or you've had sensitive data stolen. Having protection like MDR allows you to worry about such things a little less because you have a massive team of cybersecurity professionals monitoring and responding to any potential threats all day, every day.

Q. Could you expand on a few of the key benefits of having a third-party Managed Detection and Response partner?

Sure. Working with an MDR provider like Sophos has all sorts of benefits, but the key thing is you no longer have to rely on internal resources to be up-to-date on all things cybersecurity. As you mentioned, the cybersecurity landscape is changing really fast. There are so many types of threats, and they're all happening one after another over and over. That's difficult enough to manage for an entire team of security analysts, let alone for an individual or small IT team handling everything by themselves.

Another benefit is that working with a team like ours reduces the complexity of managing a cybersecurity infrastructure, not to mention the costs for all the internal tools needed to provide security across an organization. Retaining and training existing staff on everything cybersecurity is an ongoing battle for companies. So, MDR allows you to replace all of that with a team of round-the-clock cyber experts to supplement the internal team — or some choose to outsource MDR completely.

> Staffing is definitely a challenge for companies these days, especially in the enterprise security sector. As one of the key benefits of MDR, let's dig into that subject for a minute...

Q. What are the responsibilities of an MDR analyst, and what skills and qualities do you typically look for when staffing up?

Our MDR analysts typically have three primary responsibilities: investigating incidents, responding to incidents, and providing customer service. Investigating and responding are obvious ones, but customer service is one I'd like to touch on. Our analysts interact with our customers all the time. Whether it's a quick phone call to confirm suspicious activity or a full-blown Zoom session to handle an incident, it's uber important that our analysts understand the value of providing excellent customer service.

For skills and qualities, we obviously love the tech side. If you have some baseline certifications or education in Security+ or Network+, that's an excellent start because it shows you're interested in the field and are a bit analytical. But soft skills are a must: communicating and articulating what needs to be said at a critical time is beyond valuable. We also look for experience from all backgrounds. We have former teachers, military veterans, and more that make up our really diverse teams. At the end of the day, we look for people who are genuinely passionate about cybersecurity. We can always train you on the hard and soft skills needed to be successful.

> Makes sense. Candidates need to be comfortable working with all types of data, have an analytical mindset, and have the drive to find and stop attackers — sort of like an investigative personality. This is probably a good place to note that even with human-led MDR, an essential and critical layer of cyber defense is still high-quality protection technologies.

Q. What tools and technologies does an MDR analyst rely on to get the job done?

Sophos analysts rely on a variety of proprietary and open-source tools to conduct investigations and handle threat hunting. We have a proprietary platform where our analysts spend most of their time, but they also use Sophos Central for a good bulk of their investigative analysis, as well as your standard open-source tools for investigating IPs, domains, files, and the like.

Q. Can you elaborate a bit more about what Sophos Central is?

Sophos Central is an all-in-one, cloud-based platform for our customers. Whether they use Sophos antivirus for their endpoints and servers, our firewall solution for email, or both, Sophos Central is basically a one-size-fits-all interface for all Sophos products. It allows customers to manage their environment and, simultaneously, allows the MDR team to go in and respond to any threats or conduct investigations in that environment.

Q. So, does that mean only existing Sophos customers can turn to your MDR team for support?

Here's the awesome part about Sophos MDR. We can ingest telemetry data from third-party software security products into the Sophos Data Lake; that's the hub that houses critical customer information from endpoints, servers, and so on. That data is automatically consolidated, correlated, and prioritized with insights from the Sophos Adaptive Cybersecurity Ecosystem and the Sophos X-Ops threat intelligence unit to accelerate threat detection, investigation and response so we can deliver better cybersecurity results.

The MDR team monitors that enhanced data and responds when we get alerts about anything unusual, like an odd email identity, firewall penetration, or detecting a Microsoft event with MS Graph API.

In fact, we're the only cybersecurity vendor providing this service. It's a pretty powerful tool, and the word is spreading. We're starting to see new customers reach out to us for the 24/7 protection they need.

> Now that we understand the MDR role, the skills required, and the tools used to provide that 24/7/365 protection, let's dig into why we're here.

Q. Please give us a play-by-play of a typical day for someone on your team.

A typical day for someone on my team looks like this: The first 30 minutes are spent getting up to speed on what happened in the previous shift and logging into their battle stations, so they're ready for the day. This gives them time to ensure they've got all the appropriate tools and applications at their fingertips. After that, they begin to work on investigations, detection tuning, threat hunting, incident investigation, and the like.

We also give our analysts frequent days dedicated to analyst development and growth. These days allow them to take a break from the normal day-to-day and work on projects, research, and even professional development like the next certification they want to obtain. Sophos offers a wide range of certification programs — and not just for our team, but for customers and partners as well.

Q. So the team is ready for battle. Can you share an example of how you and your team recently saved the day for an organization?

Let me tell you about a recent one in which our analysts responded to a relatively new 3rd party firewall vendor. The threat actor gained access to our customer's firewall interface and was able to make changes to their policy and create new admin accounts. These were used to pivot to their infrastructure, where they started to enumerate the domain and move laterally with Impacket.

Luckily for the customer, they had MDR deployed to their environment, and we could detect the lateral movement and domain enumeration. We immediately contacted the customer, where they confirmed the activity was unexpected, and began our incident response procedures. Working together, we contained the threat, allowing the customer to deploy a firewall patch very quickly. We also reviewed their firewall logs to confirm initial access and determine IOCs for the customer to block at their network edge.

> You must be very proud of the round-the-clock cyber support your team delivers to customers. From what we've heard today, it's easy to understand why Sophos is getting huge accolades in the industry.

Q. In closing, can you share your thoughts on why customers trust Sophos as their MDR partner?

Our customers trust us as their MDR partner because we have a proven track record of success in cybersecurity and have provided cybersecurity products and services to over half a million customers worldwide. I'm biased because I work here, obviously, so I like to point out that through Gartner Peer Insights and G2 Ratings, our customers gave us the highest-rated and most-reviewed feedback for any MDR service provider. Right now, over 15,000 organizations rely on us for 24/7 threat detection, investigation, and response, making Sophos the world's most trusted MDR service.

Let's not forget our expert analysts — they're on the frontlines every day, responding to threats, hunting for persistent bad guys, and neutralizing malicious activity before it's too late. And with third-party integrations, we can detect and remediate threats across all types of environments — including complex, multi-vendor scenarios — before those threats become more damaging, like ransomware or a wide-scale data breach.

Thank you so much for your time today, Anthony, and for shedding some light on MDR for the world out there. Your passion about cybersecurity really shows. I think your customers are lucky you and your team at Sophos have their back 24/7 365 days a year.

Sure! Thanks for having me!

To learn more about Sophos MDR and how we can support your business, speak with a Sophos adviser today or visit www.sophos.com/mdr

2023-02-23 (WP-NP)

SOPHOS