ASPIRE
Powering Business Transformation™

The Digital Aspirations Business Podcast – S1E4

Taking A Managed Detection & Response (MDR) Security Approach

Doug Stevens, Vice President for Managed Services, Aspire Technology Partners
John Rossiter, Principal Consulting Engineer & Chief Information Security Officer, Aspire Technology Partners

Doug Stevens: Hello and welcome to Episode 4 of The Digital Aspirations Podcast series. My name is Doug Stevens, and I'll be your host. This edition of Digital Aspirations comes to you in late May, as we approach the unofficial start of summer. And as in years past, I know many of us were looking forward to family gatherings, going to the beach, high school proms, graduations. And this year has a very different feel with the social distancing and some of restrictions that have been put in place that have disrupted our daily lives and, hopefully, for not that much longer.

But before we dive into the podcast, we just want to say we feel for all those impacted by COVID-19. We hope you and your families are all safe and well. And we want to give our sincere thanks to our health care heroes and first responders and thank them for their dedication and putting the well-being of others before their own. So, as a community, let's continue to flatten the curve. Let's do the right things. Let's work together to get back to more normal times and, hopefully, very soon.

In the meantime, as technology professionals, business has to continue. Many of the digital initiatives that we're used to pursuing have shifted, and a lot of those have shifted towards specifically addressing some of the challenges that the COVID-19 virus has presented to all of our respective organizations. We find ourselves talking about business continuity, working from home, and things like distance learning in the K-12 and higher education markets, virtual waiting rooms to support video conferencing in the telehealth space, and leveraging various technologies to enable contact tracing for public health.

So, as we leverage these technologies to achieve what are really important outcomes and enable these new capabilities for our organizations, I think it's more important than ever that we don't lose sight on the importance of securing these infrastructures against ransomware, cyber-attacks, and some of the other threats.

And that leads us into our topic today, which is Managed Detection and Response. And MDR is really the next generation or evolution of Managed Security Services. And joining me today is John Rossiter. John is the Principal Consulting Engineer and Aspire's Chief Information Security Officer. Welcome, John.

John Rossiter: Thanks, Doug.

DS: Excellent. So, in the current environment we're in, I'm curious how you're getting along with the work-from-home strategy here.

JR: Thanks for asking, Doug. I think work-from-home is probably not a big deal for most of us in technology, as you know. I guess the biggest issue for me and everybody else is probably being cooped up with your family 24/7. So, I think that's the biggest issue with work-from-home when everyone is at home. But thankfully, technology, and most of our professionals here at Aspire, have a lot of acquaintance with work-from-home. So, business as usual on that front

DS: Yeah, for sure. Actually, it's funny because I'm actually in the office today, but in the last several podcasts, I've been at home. So, leading up to this, it's usually the period where we're threatening our family, "Hey, be quiet. We got to record a podcast." So, hopefully, you're in good shape on your end.

JR: Absolutely. Same to you.

DS: All right. Now, so for our audience, John is the Chief Architect of our Security Operations Center. And he's really sort of the wizard behind the curtain for Aspire's manage security practice. John, any other interesting tidbits that our listeners should know about you before we jump in here?

JR: Well, I guess, I've been with Aspire, this is my 13th year. So, been with Aspire in a lot of different forms as the company has progressed, and gotten larger, and more successful in the market. I've had a lot of experience with lots of different technologies. Security has always been the core of everything that I've always done. I've been pretty much been doing it since year 2000-2001. So, in my illustrious career, I got to work with a lot of different technologies and securing most of those. So, it's been a lot of fun.

DS: Good. Well, as I was introducing you, I just realized that I used the "wizard behind the curtain" vag ue reference that I'm sure none of the millennials in our listeners have any idea what I'm talking about. They probably just don't know what we're talking about. That's the Wizard of Oz and John's the crazy wizard behind the curtain.

JR: Just watching that the other day with my girls. I made sure that they knew what that reference was alluding to. So, absolutely.

DS: Good for you.

JR: It's a good movie by the way. Still a good movie.

DS: It's a classic. Absolutely.

JR: Absolutely

The Difference Between Managed Detection & Response and Traditional Managed Security Services

DS: Well, thank you. Thank you for being with us today and sharing your experience and your perspective. So, with that, let's get started.

So, our listeners here, many of them, they've heard me quote Gartner before, and I'll just start with this statement. And I think that it's very true. The Managed Security Services market has been around for a long time, and it's a very mature market. And what's happened over the last several years is that the threat landscape has become much more complex and ever evolving. And what we're hearing from analysts like Gartner and, certainly from our clients and the companies that we speak to, is that the businesses now, they're much more focused on security outcomes. And it's no longer about Managed Firewalls and Managed IDS. It's more about: what can an MSSP do to help identify and respond to security threats more quickly?

Gartner published a research note recently. In it, they said that, especially in the mid-sized enterprises, IT has been over-invested in security protections, or security controls, products, and their recommendation is to allocate more of that budget to detection, and response, and those elements, which are traditionally more part of MDR capabilities. So, John, help us level set. What is Managed Detection and Response? And why is MDR different from traditional managed security services?

JR: That's a great question and a question we get quite often. So, when you look at your traditional Managed Security offerings, you've got a diverse set of tools, and not a lot of those tools work together. So, the MDR approach is more of a focused set of tools. And beyond a focused set of tools is a very seasoned Security Operations Center that is able to leverage those tools and understand them. Not only are we able to take advantage of the information that those tools are giving us, but we're able to react to them and actually mitigate issues. So, that's really where an MDR sets itself apart from a traditional managed security.

Traditional managed security is more along the lines of, "Hey, we see this is happening in the environment. We think it's bad. We're not quite sure." But because of the focus that we have on the MDR side, we're able to dig in and really understand. We work with our customers. We develop customized playbooks. We really get to know their environment, and their people, and their process. So, we're able to put all that together under one umbrella.

DS: So, we're still ingesting the data from the security controls across the enterprise. There's still that 24-by-7 monitoring element to this, but it sounds like we're leveraging automation and some of that machine learning to correlate and make decisions. And then, we're injecting the threat intelligence that would allow a SOC analyst and someone on your team to be able to focus on what's important, right?

JR: Correct, correct. So, we're utilizing those tools. We have experience, many years of experience of deploying these tools, so we know what to look for. And we build that into our SIM. We build that into our rules. And then, we get our SOC analysts, who are trained on all these different platforms, to get involved when we do detect an anomaly. So, utilizing big data, machine learning. We're able to really filter out a lot of the noise that a traditional managed security service would not be able to.

DS: Okay. So, that allows those folks in the SOC to be able to spend more time on investigations and doing threat mitigation?

JR: Correct. Real investigations, yes, absolutely. So, nine times out of ten, when we see these solutions deployed in customer environments, they don't have the people that understand and can deal with the alerts, especially on a 24 by 7 perspective. So, this is where we set ourselves apart there and what is a huge part of this service.

DS: Absolutely.

UNDERLYING MDR SECURITY ARCHITECTURE AND HOW IT ADDRESSES EXPANDED ATTACK SURFACES

JR: All right. So, just moving on here to another thought. And this is around one of the main security challenges that we see in organizations, and that's the expanded attack surface. So, there's cloud expansion happening. There's workloads and data that live in the cloud, that live on prem. There are hybrid environments now. We have, obviously, a ton of remote workers. So, what does the underlying MDR security architecture look like? And how would that help address this new expanded attack surface?

JR: That's a great question. So, with the MDR where we're not only just focused on your next-gen firewall, which is your perimeter, your traditional boundary of the network, but as we know, especially from work from home, we have this expanded attack surface where those endpoints are going home. Those endpoints are going down the street or across the country potentially. So, how do we monitor those? And that's really where the endpoint platforms come together. Whether or not you're utilizing the Cisco Security AMP for Endpoints along with the Umbrella Roaming Client, this is where we're able to capture the information and continue to ingest, and protect, and gain that visibility on to helping your users stay safe.

Beyond that, when we look at the cloud infrastructure, we utilize our networking tools that are able to baseline and understand, statistically speaking, what's actually occurring in those cloud architectures. Are there things occurring that happen outside what we consider to be normal, or is this an anomalous event? So, this is all baked into the MDR service, and this is, again, where we set ourselves apart.

DS: Nice. All right. So, it sounds like you're addressing potential threats at the cloud network and even at the endpoint layer.

JR: That's right. I mean, a comprehensive security play here would, be to make sure, that we're taking into account all these different attack vectors. So, just simply monitoring your firewall, even if it's next-gen, is not going to cut it, especially when those devices leave the network or go beyond the network perimeter to get your normal everyday business-critical applications.

DS: And then, there's the integration between the various tools that have some clear advantages from a security operation standpoint, right?

JR: For sure. That's one of the reasons why we have aligned ourselves with Cisco. They have the most complete portfolio and best integration among products. So, it just makes for certain efficiencies on the back end and really speeds our SOC analysis. And in addition, it gives that information to our customers in a very timely manner.

DS: And then, all of this, I'm assuming, that your team is going to manage this in a turnkey fashion for your clients—all of the underlying technologies.

JR: That is correct. So, we do offer, along with the MDR, the care and feeding of these devices with a more traditional approach where we're looking at policy and making recommendations, helping, troubleshooting, things passing through the network, those types of things. So, yeah, absolutely. We do offer the full complement when it comes to managing the infrastructure.

DS: Okay. Updates, and code updates, and those sorts of things as well.

JR: Absolutely, yeah. Everything that's necessary to make sure that we have functionality and we have a secure environment; we're patched to the latest threats.

DS: All right. Well, then, I'm going to talk about one of your favorite words, and this is a word that you use often here internally within Aspire, and that is context.

JR: Usually, yeah.

DS: Yeah, you have a context. I think it's tattooed on your back. But from a Security Operations Center point of view, the contextual awareness and some of that context-rich intelligence that's a key component of MDR. Why is that so important?

JR: That's a great question. Yeah, I do overuse that term a bit. I am guilty as charged, for sure. I've had a number of conversations with customers over the years, and there will be a few of them that don't understand potentially what the threats look like and why they need these various tools have asked me, "Hey, look, which tool should I get? I mean, I don't need all this other stuff. Which one's the best tool?" And I'll be like, "Well, it is many of these tools as you can get, I would recommend it." And the reason is because one specific solution is only going to give you really one piece of information. When it comes to security and when it comes to potentially identifying compromises, you're really dealing with the preponderance of the evidence. You don't have a full picture.

Think about it this way. So, if I have a DNS log that's telling me one thing, I don't have a lot to go on except for that one particular log. So, I can take a look at before and after, but if I can start to put together, "This is what DNS was telling me at the time that we had this alert happen, along with potentially an IPS event, and now, here's endpoint protection." That gives me another angle to look at and verify. And then, of course, my network traffic analysis, we can go back seven days, two, 30 days, even past that to really get an understanding of what the typical behaviors are on that endpoint. It's really important to start to analyze what's actually happening on that particular endpoint.

So, making sure we have those tools, that context, is really important from a SOC analyst's perspective. You can't have too much of it. You really can't. The more, the better. And the more complete picture that we are able to paint about what's actually occurring on that endpoint, which is so vitally important.

DS: So, that's really the validation piece and being able to understand what was happening within the environment before, and during, and around the time that you've identified something that triggers an alert.

JR: A hundred percent.

THE SOC ANALYST TO-DO LIST AFTER AN ALERT IS TRIGGERED

DS: Got it. Okay. That's actually a very good segue into my next question. And that is if you could help us sort of a picture, something happens within an environment, alert is triggered, what does the SOC analyst's to-do list look like when that alert is triggered?

JR: Great question. And that is one of the pieces that gets tailored through our onboarding process. So, when we take on a customer, we need to start to understand what their environment looks like. And that onboarding process is usually anywhere between two and four weeks. And so, we develop a really good sense of where we need to go, what types of alerts are very important for the customer. For instance, obviously, ransomware is one of those things where it's universal. It's obviously very important all the time. And then, on top of that or beyond that, what do we do if we get a browser hijacker, for instance, which is potentially unwanted? Not necessary. It's more of pest but can potentially lead to other issues down the line with potential compromises.

So, we get a feel for what the customer needs and what their wants are. But essentially, the alerts are received in most generic fashion. So, we get the alerts. The SOC analysts will go ahead and verify that alert. And then, they'll do an initial contact with the customer. They'll take a look at the surrounding information in our SIM, look at the timeline, all the different devices that have been part of that alarm. Again, that initial notification to the customer, "Hey, we received this. We're looking into it right now. And then, we'll start potentially a more full investigation," where we go more deeply into analytics. So, if there's an IP address involved or URL, we'll utilize several different tools to give us a better understanding of what we're dealing. We'll check blacklist, we'll check Talos, which is being utilized by the products themselves if we're utilizing the Cisco infrastructure. Beyond that, there are several others that we'll use as well.

And then, we're just trying to gain that contextual awareness that I mentioned earlier. So, we're pulling all the information together, whether or not we're utilizing our SIM on occasion. Also, if the customer has the requisite solutions, we're going to use utilize Cisco Threat Response, also known as CTR. That gives us a great visualization of what's actually happening. And then, of course, we'll contain, if we can, depending upon what's actually available in the customer environment. I would say, probably in the past year or so, Cisco has offered with their AMP for Endpoint product isolation on the endpoints. So, this has become very popular with a lot of our customers. We're able to isolate that device if we feel it is important enough.

And again, that is part of the onboarding. So, what type of device this is? Workstation? Server? How critical is it? And that will determine whether or not we can push the button on our own or we need to escalate to the customer. And then, after that, what we're doing is a more thorough write-up of what we found, and the incident itself, and that's where we go up the chain that the customer has prescribed for us in terms of letting them know what had occurred, and how we could potentially — lessons learned as well. A lot of times, it's user training; it's potentially updating of software and that sort of thing. It varies, Doug; and certainly, again, it's part of that customization that takes place with each one of the customers.

DS: I think that paints a very clear picture of that security outcome that organizations are looking for. So, your emerging technology to focus on what is most likely an issue. It's triggering an alert. And then, there's eyes on it. And someone's doing the analysis, they're leveraging threat intelligence to investigate further. They're making recommendations, providing guidance, and really helping the client to take some actionable remediation to limit the damage that could potentially happen.

JR: Absolutely. We're giving the customer real information. As you said, actionable. And that is the key word here. What do I need to do with this? So, we're guiding them through that process. Do we need to remove that device from the network? Do we need to work with IR as a next set of steps involved in this? Potentially. Or is it something as simple as what we have potentially unwanted, we need to just go ahead and remove that from a browser. So, it all depends on the threat. But we're there to guide the customer through whatever it is, and we're very flexible in that regard.

DS: Right. No, it sounds like it. Is that our biggest differentiator from your perspective?

JR: Absolutely—that we're willing to work with the customer and make sure that we understand their needs and their wants, what they're looking to get from the service. And that flexibility, I think, is really one of the reasons why we've been successful in this market. I hear from our customers, we do our quarterly business briefings with our customers, and I constantly get that feedback about the team. And it's usually very positive. And I think this is also a differentiator. If there are issues, we're always looking to work with the customer to change whatever it is on the back end that the customer needs to have an outcome that is successful.

So, we're always working. One of the biggest things that we do in our QBRs is, " Mr. Customer. I want to hear from you. I want to hear what your feedback is." And a good majority of the time, it is great feedback. But like anything else, there's always ways, always things that we can improve upon. And so, we're always open to that. We're flexible. And I think the architecture that we've developed engenders that.

DS: Yeah. It's about being an extension of the client security operations, right.

JR: That's it.

DS: And part of that is getting more-.

JR: That's the normal thing to do. That's the goal.

YOUR TRUSTED ADVOCATE: CUSTOMER SUCCESS TEAMS AND MDR

DS: It sounds like it's high touch. A lot of back and forth and working closely with the client. You didn't mention our Customer Success team and dedicated Customer Success Managers out there.

JR: That's a big one. They're part and parcel of the success that we do have with our customers. So, we have a dedicated Customer Success team. That is their job. They're always advocating for the customer, ensuring that nothing gets lost in translation. They're always there. They assist the account manager and the engineers. That's their primary touch point with Aspire. They can certainly come to any member of the team, but the Customer Success, they meet weekly. I work with them. And if there's any issues that are in the customer environment, everything kind of lights up through the CX team. So, they're, again, really critical for the success as a business.

DS: Yeah. I couldn't agree more. I think we're as far down the line in terms of the maturity of our customer experience and our Customer Success Team, as any partner out there. And that's a tremendous group and a tremendous benefit to our customers.

JR: No doubt.

DS: This has been a lot of fun, and certainly MDR is very near and dear to my heart, But, unfortunately, but that's all the time we have.

DS: That's all the time we have today. But any closing thoughts before we wrap up?

JR: I think we pushed through and talked about everything we needed to, but I definitely appreciate everybody's time today. And I echo Doug's sentiments, please go ahead, and do your part to stay safe and stay well. All right. And hopefully, we hear from you soon.

DS: Indeed. Well, thank you, John, for sharing your perspectives with our listeners. I really appreciate you being with us today. And to those listening to the podcast, if you'd like the discussion today and would like to hear more, please go to our website, aspiretransforms.com. And you can listen to the library of podcasts up there. And as always, thank you for listening, and we'll see you next time on Digital Aspirations. I'm your host Doug Stevens. Bye for now.

Outro: Digital Aspirations is brought to you by Aspire Technology Partners, a premier technology solutions and services provider designing, implementing, delivering, and managing digital infrastructure and IoT solutions to enable transformational business outcomes, creating more agile and efficient IT environments that deliver differentiated customer experiences for your organization. To learn more about Aspire Technology Partners, visit aspiretransforms.com or email us at podcast@aspiretransforms.com

Aspire Technology Partners is a Cisco Gold Certified Partner engrained in solution pillars that set us apart as a true Cisco solutions provider. We are committed to the continuous improvement of expertise and skillsets around Cisco initiatives that enable us to help and guide customers in the adoption and management of technology architectures designed to transform their organization. We hold Cisco Master Specializations in Collaboration, Security, Cloud & Managed Services, and Networking and is one of only 25 partners in the US to receive the Cisco Advanced Customer Experience Specialization.