Eye on Security Podcast

Automated Defense Brings New Features to Mandiant Advantage

Transcript

Luke McNamara:

Welcome back to another episode of the Eye on Security podcast. I am your host, Luke McNamara. And joining me today we have Mike Armistead, SVP for Mandiant Advantage products. Mike, how are you today?

Mike Armistead:

Good Luke, how are you?

Luke McNamara:

I'm doing well on this somewhat rainy Wednesday that we're recording this. But I'm interested in this conversation. I think we'll have a good discussion here today. Talking about some of the new features that are being launched with Mandiant Advantage. For those who maybe missed it before, we did an episode last year, last fall with John Hyatt and Jeff Gilfoyle, talking about the initial launch and some of the features that were coming with the intel portion of this, but I'm excited to hear about some of the other features that are now coming online. Mike, before we jump into this, tell us a little bit about yourself and your role here at the company.

Mike Armistead:

Sure. Today, I'm SVP of the Mandiant Advantage products. And I came to Mandiant Solutions as part of the Respond acquisition where I was a co-founder and the CEO.

Luke McNamara:

Excellent. And your current role here, you're obviously doing a lot with this new platform that we've been building out and launching, but walk us through a little bit of what that looks like.

Mike Armistead:

No, it's been really the sole focus since we got here. With Respond, we're bringing a component to the Mandiant Advantage platform that is going to enable automation of tier one triage of alerts. And we'll couple that with our Security Validation products. But it gave us the opportunity, honestly, to just expand what we had been talking about with Mandiant Advantage.

You mentioned in the fall, you had a podcast that discussed phase one, which was how could we bring all of this great intelligence in through a platform that everyone can have access to very easily, as opposed to it being a report that you got. And from paper form, modernizing that into a SaaS delivery form.

Well, what I've been doing as part of our acquisition is then bringing the other components and truly making this a platform. So Mandiant Advantage now, it's better to think of it as a set of products that are going to

give great outcomes from the intelligence and expertise that has always been part of Mandiant, but packaged in a way that is easily accessible, easy to deploy, can scale in a way that we can't do that just from our consulting and our other products that are maybe considered more manual.

Luke McNamara:

So one of the things that I know from the intel side, which again, I'm more familiar with a lot of the intel portion of what we've been unveiling and building out since the launch of Mandiant Advantage, is that it's giving us a way to reveal more of the insight we have about malware, about threat actors.

You've seen us do a lot more now to reveal some of the information around UNC groups. We're talking about that a lot more. So again, thinking about this from the intel side, more people are able to access that data that exists, but then there's a piece of this that dovetails into what's really in your wheelhouse, which is the automation piece of this.

So I have information about, let's say UNC2452, since we're talking about them a lot these days. I have information about maybe a new particular technique they're using. And I now, if I'm an analyst sitting in a security operation center, I have to think through my current controls that are in place, does it protect me from this, this new tactic they're using? Or I've got to figure out some way to action it somehow. How does the respond and the automation piece of this start to kick in and do that sort of work from the transfer of the intel, of what Mandiant knows, to what an organization is then able to respond and implement?

Mike Armistead:

So, Mandiant Advantage platform is really meant to bring that expertise and the intelligence in, and weave it through all of the products that are part of it. And really, the core things that help an organization really focus their efforts, their resources, their time. So they're not spending it on places that are either benign, or false positives, but they are spending on the places that matter.

So you mentioned the way that works is the threat intelligence might be telling you that you have this actor group that's maybe has a campaign in a particular industry, maybe your industry, and it's using certain tactics and techniques, as you had mentioned. Well, here's how it weaves through. It can provide, first, that information to a Security Validation product. And what that product can do is then use the information, really test your infrastructure, all the controls you have in place, to see what actually blocks those tactics and techniques, and what doesn't.

So what it starts to give you is a picture of where do I have gaps? And so with that knowledge of those actor groups and the methods they use, how good, how competent is my architecture to deal with that? And so, once you know that, then you know where to focus. You can spend your time on the gaps, not on the places where it's already shored up. And you can do that continuously. So that's a great way of weaving it in there.

With Automated Defense, which again is the new name for the former Respond product. It provides that in an operational sense. So when your security operations center and those analysts are seeing all these alerts flying by, you'd want them to know which things are alerting according to those tactics and techniques that those actors are using, and escalate those things more readily, especially if it's someone who's doing the latest kind of attacks.

And you might not have SIEM rules. You may not have playbooks or anything to deal with that. What we can do with the product is ingest all that threat intelligence and have it as one of the facts that our AI models use to say, "This is malicious and actionable. You should pay attention to it right now." And bubble those up. And

so when you think of Mandiant Advantage as a platform now, it's really based on a concept that also has a new name that also I'll tell it to you.

So think of it as, we have this breech intel grid that's at the heart of this platform. And what that means is, we're taking all the information that we know, actually from our consulting side that's doing the incident response, or doing red teaming, or engaging with customers, doing forensics on post-breach type stuff, as well as our managed service organizations that are triaging and investigating incidents all the time, and bringing that into this breach intel grid, which then feeds all the products to have this level of expertise and knowledge that you just, you can't really get anywhere else in any products in the industry.

So, super excited about weaving that through and then allowing organizations to take these steps so they can focus and prioritize based on the things that matter to them. Making it relevant to them is the real key part to all of this.

Luke McNamara:

And again, as we were discussing prior to this, some of the ways to maybe talk about it, one of the things that struck me, thinking again as an intel analyst, and from that side of the house, some of the difficulties I've seen over the years where you have intelligence, that we've produced, and the difficulties of applying that to a particular customer problem.

So you have this intel about this campaign that's going on, about an actor, about a new piece of malware that's being offered for sale on the underground, and you present that to a customer. And of course, one of the first questions the customer's going to ask is, are we protected against this? Is this something that we have to worry about? Have we seen this already? Is this potentially already in our network?

Luke McNamara:

And so that sort of connective tissue between the intel and being able to determine if you're at risk and to eventually action it, be able to address if there's a problem with security controls, is something I think that has always been a challenge that I've seen, again, from the intel side.

Mike Armistead:

Yeah. No, I mean, I think of it in two ways. One is, how prepared am I to deal with that? And that's really where the Security Validation product, as part of the platform, helps bring it in. And then also, hey, it may take you time to fill those gaps and to know how prepared you are. So operationally, am I recognizing those up to the minute kinds of things too. And that's the other side of the problem is, threat intel is useful in both preparing, but also in recognizing at the time. And so, the Mandiant Advantage platform provides both those sides of it.

Luke McNamara:

So I'm curious also from the perspective of someone who is a SOC analyst, how they might be utilizing this. So you talked about being able to better prioritize things like alerts and have intel feed into that. So working from the other side of the problem you have something that you're looking at and you can then go through this platform, go to the Mandiant Advantage platform, go and access potentially intel about this particular alert that I'm getting. Walk us through a little bit of what that would look like.

Mike Armistead:

I mean, let me take it from the actual product perspective and how it might feel to an analyst and various others in that process. If you do take it from a security analyst who's sitting in the SOC, who's typically staring at a console, if it's a big one, and watching these alerts fly by and somehow having to make a determination which ones are important, which ones aren't, what's related, what isn't, all those kinds of things. It's a very challenging type of problem.

What Automated Defense does is, it does a lot of that basic work, but at machine speed, and at machine scale, and machine consistency it ends up, because it doesn't just operate at single points in time. That there's this evaluation by the analysts, someone at 2:00 PM, but someone at 2:00 AM. They come from different backgrounds, have different biases, do all that.

And so, Automated Defense allows an organization to correlate all this information, like 50 to 70 kinds of facts that are happening at one time, and then group the ones that are related and then prioritize it based on where they are in the kill chain, what critical assets might be involved. All those questions that that analyst typically had to ask themselves, the system now asks those questions and only bubbles up the ones that are meeting a threshold.

So then they're going to see on the screen, Automated Defense, very clearly, what were the facts that Automated Defense used to say, "This is something that looks malicious and actionable." And one of those very much is going to be around the threat intelligence. And it may even be something that's a feature of our Threat Intelligence product, the M Score, which is providing the ability to... if that M Score is high, that means it's pretty relevant to you.

And so that analyst would then go, "Okay, wow. This is a high M Score. First of all, do I really know what that means? Let me click on that." Automatically, he goes on over to the Threat Intelligence M Score page. Allows them to get depth into what that's telling you about generally. Obviously, within the Threat Intelligence product, they can work around that to see more about those actors, more about even, let's say the organization is MITRE-based in the attack framework. What tactics and techniques are most used by those actor groups that are targeting them?

And so, understand why the Automated Defense product escalated this, and then take it... And usually the way it works is, that analyst is probably, at that time, because they're doing triage, they're going to probably give it to an incident responder. And they're probably going to also give it to, if they have a big enough team, to some of what you used to do, Luke, the threat intelligence expert and specialist in that too, and say, "How much do I need to be worried about this?"

And it's going to escalate on up. And typically, the incident responder may go back and look at the other factors that Automated Defense did. I kind of mentioned some of these, where we picked up these alerts, were they in a place where there's critical assets or at least critical zones? Or did the vulnerability scans that were fed into this, are they telling us there's parts that are vulnerable? That type of thing.

And ask those further deeper questions less about the alert and more about how suspicious is this, or is this destination worrisome? Those kinds of questions. And the threat intelligence specialist is going to, of course, be able to use the products to dive deeper into, "Hey, we saw this tactics and technique, am I seeing, like this UNC group, that maybe we hadn't seen this in the organization before and I'm starting to see indicators that it might be there."

Of course, one of those probably, the responder or the threat intelligence specialist is, well they're going to want to answer the question, is this a problem for me? Do I have to worry about this? And so that's when they'd kick off, using the Security Validation product, a test of, with all that information available to it, to see how well the infrastructure does with it, and to be able to come back and answer that question very definitively. "Hey, we found them. We're seeing them right now, and we're either blocking it, or we have some gaps. We got to mitigate this risk right now."

And that's really, in the end, that loop, that whole thing I just described, that can be very quick now. Instead of it taking days or weeks to get to all of this information, you can now get this in minutes, that loop can happen very, very fast.

Luke McNamara:

And I think that's the powerful and promising aspect about this technology, is that you're eliminating a lot of the friction that otherwise existed where maybe pieces of this were very manual, where you had to take content from a PDF of an intel report, and then go pull out the indicators, go pull up the hashes. Maybe go create your own rules for that and have to go search for that. But now you're eliminating some of the friction points that existed.

Mike Armistead:

Well, not only that, then take it a little further. Then you're trying to feed a SIEM or something else that maybe the operational side is trying to use in real time. And you have to write rules. You have to test that. You have to make sure that it's not so narrow that you're missing things, or too broad that you're... Because it happens a lot of times, you put a rule in and now you get another 1,000 alerts a day because it sees something that is close, but it's very hard to do.

The Automated Defense product delivers those kinds of recognition over those. We always like to talk about it as the questions that the most expert Mandiant analyst would have asked about seeing that alert. We've embedded that into mathematical models that help us go really fast through and take into account a lot of different facts to do that.

So, yeah, it's not only about taking the intel and having to do all those manual steps. There's lots of manual steps in the operational side too that have to happen that these days, that just increases the dwell time of any actor that might be in there. And we wanted to get that out fast.

Luke McNamara:

One of the things that it seems like this is helping enable, well, it's helping to enable a lot of different parts of the organization. And it seems like you've thought about this in terms of how this is being baked in into the larger Mandiant Advantage roadmap around how do you enable organizational teams? The fact that there's not single individuals using pieces of this, but they all have to work together in tandem. How has that shaped your view of the features that organizations want to see, and maybe also influence the roadmap of this as we continue to build new features and new ways for organizations to access Mandiant expertise.

Mike Armistead:

You bring up a great point because it's actually a bit of historical perspective there, because when we all started in security, it was networking guys looking at packets and really the heroes of the early days of just

doing the initial work. And what's happened is, the volume of information has just exploded as the businesses have become more and more digital. And that fact has forced us to add more people and specialize.

And unfortunately it's created silos in a lot of ways. Now, we've added a lot of automation in that. Those controls that are producing the alerts, they're also specialized and, frankly, siloed. So we've had other technologies that's tried to bring that together, but the volume has just gone up tremendously over the last 10 years. And it's just because the business is expanding. The attack surface has expanded. The techniques and the sophistication of the attackers has expanded. And so you have to have things that recognize that.

And so these are all things that, when you think about the roadmap and other technologies that we're trying to apply, it is really about how do you deal with the modern problem. Today, siloed types of alerts you get from a lot of places, you may have, what's the stat, something like 50 to 70 vendors that are in a normal security operation? It's tremendous about that. How do you weave together that? And so it used to be that people could do that in their head. They could weave those things together.

And today it's just, that's untenable, it's a problem. So you need automation to help you. I often like to use examples, and there's so many of them, but if you even think about a modern car. I have kids and they have no idea how to drive a stick shift, a manual transmission car. And you know what? That automation that's in that car, it shifts better than manual and it saves gas, helps wear and tear on the car. It does all that. There's assistance that are even in basic kind of things today.

We, of course, are applying that, orders of magnitude, ways of using more expert system-type techniques, machine learning techniques. All these things that allow us to bring together, like you had said, those different components, and do it at a speed and a scale that a modern security operations needs to have it at. And that's really the goal, right?

And the touch base we have with all of our products is, how can we get what Mandiant knows from all its expertise and its intelligence that it has gathered from its research, and its consultants and all that, how do we bottle that and bring that to every security team of all sizes? They get to know what they need to know right away. And it's actionable because it gets action through these other pieces of software. And I think that's a really key point to this whole thing.

Luke McNamara:

So, maybe I missed this earlier, but where does the action piece come together? So let's say we, in our scenario, there's been a piece of intel that we've ingested through a vendor. We're an organization and we're using the Automated Defense component of this. And we're able to detect that there was actually evidence, indicators of attacker behavior within our environment. Is that something that gets handed off to the incident responder to go deal with? Or where does that actioning piece fall into this?

Mike Armistead:

The other thing to learn from how all the interactions I've had with customers over the years is that, boy, they're all different. And they have different processes, they have different touch points. They may have automation that helps in this, they may not. So the way to think of Mandiant Advantage as a platform is, it is not a rip and replace kind of platform.

It is one that with your existing tooling and your existing processes, we fit really nicely just on top of that. So let me give you a couple of examples to make this more real. Like you said, if Automated Defense escalates

something and it indeed gets that pass to say, "Yeah, we got to take action on this." It can do this a number of ways. If you have a SOAR technology, for example, you could actually automatically feed that and if it could kick off a playbook that would do the actioning automatically, that's great.

A lot of people don't have that. They do have a incident responder. And in fact, they like to have someone in the middle of all that to make sure they're not turning something off that would block access to all their customers, or something like that. And so, it would be giving, but giving them with all the information they need to do it very quickly than that.

Automated Defense actually can, through products like the endpoint detection and response products, EDR, who have those capabilities, we could actually feed back down to it to say, "No, you've got to take some action here." And the EDR product could take some action. We basically have a two-way conversation with a lot of the controls. Not every control, because they're not as modern, a lot of them, and they can accept as well as that.

But EDR is one of these that can. It can take direction basically, and do something for you. And so, it really depends on the processes and the technologies that are in there. But the other part that I'd say about Mandiant Advantage platform is, we recognize that and we are a good citizen within people's, I like to call it, the plumbing that they have. And so we can pass a lot of this information through APIs. And so those APIs have a lot of the rich, even from Automated Defense to the Threat Intelligence, as you know, through that kind of thing. And we can get it to the places where their people are or their actioning happens.

Luke McNamara:

So we have these new features that are now rolling out in the Mandiant Advantage platform. By the time this one goes air, this Automated Defense stuff that we've been talking about here, people will be able to go and access that through the platform. I'm curious, your thoughts as we wrap up here. One, what are some of the other things people should expect to see for us on the timeline? I won't hold you to a specific timeframe, but some of the other features that are over the next year or so are going to be rolling out.

And then two, where do you see this space in particular within the industry going in the next couple of years?Again, as it's very much responsive to what organizations and customers are looking for, people do want to have that technologies that work together and play well with others. But I'm curious where you see this all headed.

Mike Armistead:

What you were just describing there, there is a new pretty hyped-and-hot category and it's called extended detection and response or XDR. And I think the XDR rose from a couple of places. It rose from the fact that EDR isn't the end all, and be all. You can't tell everything just from what's going on at your endpoint. You can tell a lot of things. It's great technology, but there's much more to it.

And so when you talk about our future? It's in this XDR category. And the XDR, if I can summarize what that category is about, it's how do I get the outcomes the... I'm looking at prioritized things that I need to take action on, and I didn't have to do a lot of those integration work myself. I didn't have to put all my intelligence into it.

And that's why I started with Mandiant Advantage as the embodiment of a lot of the expertise and intelligence from Mandiant, it's bringing that into it. So our XDR is very unique, actually. And so this is where

our future's going, I guess I'd say. A lot of the XDR vendors talk about it, but they talk about those controls. They've woven together maybe something on the end point, something in the network, here, there, other things. And typically, that's for just their products.

What the Mandiant Advantage platform does is, hey, you can choose whether it's the FireEye controls that you have today, or it may be other vendors that you have either as a SIEM, or other kinds of controls. We can sit on top of those and you don't have to do all that work to connect the dots that tell the story of when an incident is happening within that, because we do that. We bring the intelligence and the expertise. We bring the validation to what your IT network is. And we bring the triage or that analysis that you have to make about what's important or not, automatically.

So, we are going to do more in that area. I think there's one part that I'd say that is in the future, of course, and we offer this as a managed service today is, what if you don't have an alert fire, how do you tell if something might be in there? And that's the world of threat hunting. And we have a managed service that helps you do threat hunting. But we'll provide technology that'll also help in that. And I think this leads me to this other point that I want to make sure the audience knows about the Mandiant Advantage platform, it's also very flexible in its delivery.

So if you have an organization that once it has a hundred percent technology, and those components I'm talking about are not services, they're tech, it's the products, you can consume it that way. And they're SaaS-based, very modern, deploy very easily and work in a multi-vendor situation. But a lot of companies just need the help. They need the augmentation, they need the expertise and they'd like, frankly, a person behind some of that stuff. And so we can also provide this as either expertise as you go, or as a fully managed service.

And so, again, I think it's to the style of the different customers. They're going to get this more modern XDR, something that provides very fast detection and response, but without a lot of the baggage of having to put all that intelligence, and context, and everything in themselves. They're going to be able to get it out of the box. And so, in some ways we're trying to deliver this Mandiant expertise in a box. And that's how people should think about the overall platform too. And so we'll just add more and more of expertise to it.

Luke McNamara:

Well, it's exciting to hear some of the ways that we are continuing to be a force multiplier there, and the many different ways and different use cases that organizations and customers have... Being able to meet them where they are with what they're looking for with that expertise. So, fantastic.

Mike, thanks for coming on and helping break down and explain everything Automated Defense. I'll eventually get that terminology correct. But for folks that want to go check out more about this, as I mentioned, we're recording this ahead of time, but I believe we'll have some blog posts and some other information people will be able to find on the FireEye website.

Mike Armistead:

Yeah, absolutely. I mean, we're launching a lot of this capability just in the next couple of weeks. And there should be a lot of information. And in fact, redoing the website very much to talk about the broader platform and what it does along with the Threat Intelligence that it has been since the fall. So, very exciting time for us.

ˆLuke McNamara:

Fantastic. Mike, great to talk to you. Take care.

Mike Armistead:

Right. Thanks Luke. Bye.