Eye on Security

The Inception of Mandiant Advantage

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security podcast. I am your host Luke McNamara. Joining me today to talk about FireEye's newest product launch, Mandiant Advantage, I have John Heit, Senior Manager of Intel Product Management, and Jeff Guilfoyle, Principle Product Manager. Gentlemen, welcome today.

John Heit:

Thank you, happy to be here.

Jeff Guilfoyle:

Thanks for having us on.

Luke McNamara:

So before we can even get into the meat of the discussion here and I want to as much as possible focus on the story of how we got to Mandiant Advantage and what thought and sort of the design behind the specific platform, what exactly is Mandiant Advantage? John, let's start with you.

John Heit:

So the idea behind Mandiant Advantage, what this is going to be, is we wanted to create a SaaS platform as your gateway to all things Mandiant. Now earlier in the year we did some rebranding and reorganization across FireEye where we took the hardware and the tech product part of the company and kept that under the FireEye roof and then we took the parts of the company that were really centered around a deep expertise, tech agnostic expertise, and put them under the Mandiant Solutions brand so that's your intelligence, your managed defense, your consulting, and validation or the artist formerly known as Verodin. And what we wanted to do is we wanted to create a place where all of our users and our customers can have a single platform where they can come and engage across all those different areas of expertise and intel is going to be the first step in that direction and so Advantage is going to be the way we actually serve that out to our customers.

Luke McNamara:
So with any sort of design for platform like that obviously it would be important to make sure that the end users actually want to use the features we're going to incorporate in a platform like that. So I know part of that process was going through and talking to customers and potential customers what would you want to see in a product like this for your particular use case, for what you're trying to accomplish, how you want to consume threat intel. So Jeff maybe walk us through some of the things that we've been hearing from customers over the years and how that played into the design here.

Jeff Guilfoyle:

Yeah, thanks Luke. So we have historically been in a very unique position in the marketplace and in the industry in that we deliver incredibly high quality and valuable finished intel and we really had kind of 2 sets of requests from our customers. One is on the finished intel side of the house, the more mature customers they wanted faster access to our intel; they wanted more information about upcoming actors, malware families, trends. So that was 1 of the big design goals of this new offering was to just help facilitate the flow of that information and intelligence from our incident responders, from our analysts and researchers, and get that information into our customers' hands.

The other really big use case and 1 that I think is probably the biggest shift for us as an organization has been really getting into more of the indicator space, an area where we've always had a really solid offering but with our new capabilities, with the new platform that we've built, we are now taking the information that we're learning from breach intelligence, we're taking in a bunch of open source intel feeds, and bringing in just almost a ridiculous amount of telemetry from across the FireEye appliance ecosystem and putting that into our customers' hands in a way that will help from the most mature organization down to the company that just has their first SOC person, their first sim installation, and help them focus on the alerts in their environment that are the most relevant, the most important, the most impactful, and help them walk through what those next steps are, what do we need to do, what do we need to focus on, where do we need to go.

And so it's really an interesting challenge from the product perspective in that we are simultaneously adding in a great new set of capabilities for the least mature customer and the most mature customer at the same time. It's a pretty big set of goals that we were going after and that we've achieved with this.

John Heit:

And 1 of the things that really came out of these conversations that we had across our customer base and interacting with consultants and a whole range of organizations is that more often than not the conversation from a customer starts with some variation of the question, "What do you know about X?" So our customers come to intelligence, come to Mandiant, come to FireEye and say, "What can you tell me about this actor, this malware family, this indicator, or even what's going on in the world right now, what's going on in the news?" And being able to start with that question and then quickly figure out how do we find the right answer that matters to you and be able to make you smarter and better protected, better positioned than you were a few moments ago, and that kind of a concept, you can see

that in the way we've architected across the Advantage platform, the information that's in there, the data, the intelligence, the visualizations, all kind of getting from the what do you know about this and how do I get from something that is sort of generic or either coming from something very strategic, "What can you tell me about Russian activity?" to the very, very specific here are indicators, here are tactics, techniques, and procedures that apply to that type of problem where it matters to you. Or it could go the other direction, "I have this indicator, I have this alert, it's scary; what do I need to do about this? What do you guys know about this?" and being able to pivot all the way back up the chain to this is actually tied to this type of organization, this state-sponsored act or that's increasing the act because of X, Y, and Z.

Luke McNamara:

And I think that's what's really interesting about this is that it's adding additional value, not just for Advanced users, for users that have been consuming finished intel via a report form or indicators via API et cetera for a while, but also that it's now an expansion of the consumption of intel for less mature customers and particularly I think the SOC use case is very exciting to see that. As much as the landscape has changed and is dynamic it's those sort of needs that customers have and the sort of customers that are looking for threat intel seems to have really evolved as well. Maybe talk a little bit more about some of the particular features that as you're thinking about these 2 different types of customers, and even that's a little bit unfair because within those there's a lot more variation than just really advanced customers, very sort of the beginning of their intel maturity journey customers; there's a lot of variation within even that. But what are some of the particular features that when you were thinking through what do we really need to be revealing here, what do we need to be addressing whether it's visualizations or whether it's more data faster, how did that play into this development process?

Jeff Guilfoyle:

Yeah, great question. A lot of what we have looked at through the development of this new platform is what are all of the different elements that we can expose and this is very much going to be an ongoing journey for us. This isn't something that we're ever going to call complete. So what we're starting with is kind of if we think about the richest set of intel we have, right, so if we're talking about things like threat actors where we have done an incident response investigation, if we're thinking about malware families that we have been tracking for a long time, and we understand so much about how they work, how that actor works, how that malware family works, and so we have this very rich graph of all of the different inter-related elements associated with that particular thing. And so we've come up with some interesting ways of exposing that data to our customers directly so whether you're in a browser plug-in and you start from an IP address or a file has or a URL and you're able to pivot from there into the user interface and see this full view of all of this information we have, so that's kind of 1 of the ways we've tried to take all of this information we have and make it a little bit more real and a little bit more tangible.

And then at the other end of the spectrum we're doing that same thing from an individual indicator perspective. What can we tell? How can we leverage the full FireEye technology sack, the full appliance ecosystem, all of the network appliances, all of the endpoint agent around the world and take that information and turn that from a data point into something that is actionable intelligence? And as I said this is something that we're going to continue to look

at, explore, and advance our capabilities in, but what it's really about is giving a visual representation and building into our APIs the ability to surface that data and at the underlying level in the database itself having all of those disparate pieces of information that are connected together so that regardless of what tools you're using, what platform you're using, what endpoint product or network protection or sim you're in, we can get that information to you and help you understand the context of what it is you're seeing.

We definitely are in the early stages of where we want this to go, this is going to be something that we're going to continue to work on in the weeks, months, and years ahead, but it's been really a pretty exciting process up to this point getting to where we are and then being able to look and see at what the next steps are and where we're going to be able to continue to take this going forward.

Luke McNamara:

And I think it's great to hear you mention and highlight their context. That's still such a key part of what this is focused on doing for customers, scoping down the sort of threats and activity they really have to care about. That hasn't changed even though the platform itself is evolving and some of these use cases are evolving. That still is part of the problem that a lot of customers have in trying to focus on where do I put my resources, what threats do I care about, how should I view this particular piece of malware in the larger environment of what may be hitting my network.

I think maybe when we're talking about use cases and we're talking about revealing more data it's also interesting to see that we're also highlighting more about our process as well. And John I know 1 of the use cases that you've used and highlighted with the launch around this is the story behind FIN11 and how we got there. Maybe talk about that a little bit and how the platform like this really highlights as we're going through finding clusters of activity, understanding more about what they're doing before we even get to the graduation of an APT or a FIN group, what we're kind of showcasing in that and using that particular group as an example.

John Heit*:*

Yeah, absolutely. That's a great story. So with FIN11, the story there, this summer we published our – the official graduation so the proper profile of announcing this new actor that we have labeled and we have a bunch of intelligence on and sophisticated analysis around. But you know the story didn't start this summer. It goes all the way back to 2016. In 2016 we saw through some of that FireEye telemetry a number of initial incidents that were using the FlawedAmmyy backdoor and FlawedAmmyy is just a modification of the Ammyy Admin remote access tool. And so they thought, "Okay, this is interesting. We'll start to track this," and we're doing all of this work on a graph database, which is really sort of the heart and soul of where we do a lot of our most sophisticated analytic trade craft.

And we move from 2016 into 2017 and we keep watching this cluster of activity and this use of the FlawedAmmyy backdoor emerge and we say, "All right, now there is now a distinct set of activity on our graph using this particular tool in a particular way. This cluster, we are now going to call this UNC902, Uncategorized Activity 902, and this was 1 of the ways in the early

part of our analytic process we're going to take something that goes from just being particular blobs across a graph to it's starting to define a cluster of activity that's something that we need to watch.

We're moving out of 2017 and getting into 2018 we start to see more and more activity tied to this cluster. We see some campaigns that our managed defense colleagues are picking up across hospitality and retail and finance, seeing some fishing campaigns, we actually respond to a number of incidents actually going to victim environments, seeing the weaponized Office files, the Zip files, the downloaders, and actually doing some of our own organic intelligence collection and engagement, and getting a better understanding of more and more what this cluster of activity really involves and it keeps getting more and more robust. We keep adding new incidents, going through late 2018 we start to see there's some Blue Steel POS malware, we start to see new uses of particular backdoors, and we're seeing it across these different types of intelligence streams.

And we get in towards 2019 we finally say, "We have this robust section of our graph that is all tied together." And we say, "This is now what we call a temp group." At that point we called it Temp Warlock and in our pre-Advantage world that would be the first time that we told the world about this actor and this type of activity. We may have published an indicator or some small bits of this activity but it's really at the Temp Warlock stage that we sort of announced to the world, "Hey, here's a new actor that we're tracking," and we start to give some glimpses into the insight that we have through the graph and start to be able to define the actor and really focus on that attribution and say, "Here is a defined set of activity. We think there's a common actor behind it," and then eventually this summer we get to that full actor graduation and we launch that proper profile of FIN11 and that analytic process is very sophisticated, it takes an incredible amount of work across multiple analytic teams, but they're all working off this same graph. They're all living in this space studying, looking for commonalities across incidents, across intelligence streams, and building out that view and before Advantage that would be the point that you really got to see it as 1 of our users or 1 of our customers, Temp Warlock and then finally FIN11.

With Advantage we're able to take customers all the way back to that 2016 stage, actually be able to see those clusters as they start to emerge, as we start to track them, so we can actually expose those UNC groups. FIN11 started as UNC902. We have over 2,000 of these UNC groups that we track across our graph. Now not all of them become FIN actors or APTs of course but that kind of visibility is 1 of the most radical changes that come out of this so that when we get to FIN12, FIN46, go all the way down the line APT65, when that comes out we'll have been able to start on that early part of the graph with our customers and walk that whole analytic process shoulder-to-shoulder with them and that's really exciting. That's pretty crazy for us.

Luke McNamara*:*

Yeah, I like that focus of walking alongside customers shoulder-to-shoulder very much – a lot more of a partnership model and a lot more actionability on their end to have as our thought process changes and evolves over time. You know often the assessments that we're making in our intel products they're not binary to where it may seem to so you know the old way of publishing around an APT group, but if we finally graduate and reveal this APT or FIN group

our thought process is changing and evolving over time as we're collecting the data from those different sources and to be able to kind of highlight that through that process to customers I think is exciting.

So I've had a chance to look at some of the content and what we're revealing in the Mandiant Advantage platform. Disappointed there's no pew-pew map but in terms of the visualizations there a lot of really cool features. Jeff what are some of the things that you're most understood and excited to see how customers use things that we have baking with this platform?

Jeff Guilfoyle:

You know it's a great question and 1 of the things that – I'll kind of share a little bit of a personal secret is I'm a bit of an API geek and I like to just play with things from time-to-time, prototype different applications against different platforms. And 1 of the things that to me is the most exciting is everything that our customers see in this new user interface is driven by a new set of APIs. And it really has been an exciting time to be on this side of the house because I can go through and look at applications that I've worked on before, integrations I've written, and make sure that we are addressing those use cases as much as possible within those APIs. So just kind of from a generic perspective I am just absolutely thrilled with the work our engineering team has done to bring this product to the forefront and for our customers going forward it's really just an incredible set of tools that they can build on. So all of our integration partners, all of the different sims and tips and sorter tools that we integrate with are going to be able to make use of all of those new APIs. They're not something that we're not exposing to our customers; this is a part of what they get access to is the data and then those APIs that provide access to that data.

The other thing I think that just is something that again is very new for us is what we're calling the M score. This is our machine learning pipeline that we're running all of our indicators through and this will give a very easy to understand value to determine if an indicator is likely malicious, what have we seen about it, what do we know about it, all of those things, the global prevalence, have we seen this on FireEye appliances, have we learned about it from OSN sources, have we seen it in IR? All of those factors come into that machine learning engine and provide a single numeric score and so that is really going to be how we make things easy for our customers to use. So the integration, the process of training and building that model and then scoring those indicators, building it into the user interface, building it into the browser plug-in, building it into the APIs I think is really going to change how our customers are able to operationalize the intel that we're providing.

If you look at the volume of indicators that come off of the FireEye appliance telemetry around the world it's not a small number and being able to distill that down into okay, these are the things in your environment that are the most impactful and most important and most urgent for you to address right now is something that I'm just so happy and proud to have been a part of this and so excited to see what our customers do with it.

Luke McNamara:

Yeah, I'm really interested to see and hear some of the stories on how this gets incorporated into analytic workflows in particular. Certainly a lot of different use cases but I'm really

interested to see how analysts on the user end start using this and incorporating this. In terms of – you know as we know and we've talked about here none of this is static, certainly not the threat environment, and probably not what our customers and organizations we're helping to keep secure are expecting from vendors. In terms of how technology will change obviously there's a lot we can't imagine what the use case is going to be 5, 10, 15 years down the road and it certainly seems like we've got a very robust platform that as use cases evolve, as customer maturity evolves we have different ways of incorporating and building into what we have here today. I guess maybe broadly what are some of the things you could expect or see us incorporating down the line as this platform gets improved and built upon?

John Heit:

Yeah, 1 thing that's for sure it's going to be highly dynamic and that's 1 of the things that's really exciting about this platform is that we're going to be able to experiment and to present different types of data in different ways in a way that we haven't been able to do certainly in the intelligence business in the past. Part of exposing far more of our data and far more of expertise in process means that there's going to be a lot more room to innovate and to find places where the things that we do are particularly valuable or where there's places we need to evolve in how we do our process, how we expose our information, what kind of analysis we do, so there's a lot of that that's just really exciting.

I think the next really big part of this journey across the Mandiant solutions business is validation. That's going to be the next major pivot that we pursue here so being able to have taken this platform and hopefully provide people a real decision advantage in their intelligence workflows, reaching some particular point where they now have the insight they need to be able to make a decision, and be able to pivot directly from that saying, "Am I protected? Can I validate my protection, my controls against this actor, this type of threat right now?" That could be a real game-changing space for us and that's going to be the next really big thing that we go after.

Luke McNamara:

Good closing plug there for Mandiant Security Validation; I like it. Jeff, John, thanks for joining us today. I know I learned a lot more about the Mandiant Advantage Platform than when I went into this. For folks that are looking to find out more information about it or maybe get some more details around Mandiant Advantage where should they go to check out Mandiant Advantage for the information?

John Heit:

For new folks we encourage you to go to the platform. You can sign up for a free account and check it out. Advantage.Mandiant.com is where you'll find it and we look forward to seeing more people on there.

Luke McNamara:

Awesome. Thank you both for joining today.

John Heit:

Thanks Luke.

Luke McNamara:

Take care.

Jeff Guilfoyle:

See you next time.