uberknowledge

Joe Slowik, Principal Adversary Hunter at Dragos

Think Like a Practitioner When Trying to Execute as a Vendor

Joe recommends being strategic in your partnerships and being authentic in your message by selling a solution instead of a product.

02:29 A unique vendor message is the way to connect with customers, not spam.
03:23 The problem with anomaly detection as threat detection.
05:12 The challenges of and differences in protecting the ICS environment.
07:53 Gain trust by respecting the work that has already been done, even if it's outside your realm.
10:26 Think like a practitioner when you're trying to execute as a vendor.
11:02 Don't sell a product, sell your customer a solution to their problem.
11:59 Truly get to know your customer by embedding for a day or two and know your market by attending industry-specific events.
15:04 Sharing works well with complementary capabilities but less well with competing capabilities, so be strategic in your partnerships.
16:44 Attackers are using your own code against you.
18:05 The adversaries are becoming more automated.
20:08 Security conferences are a great opportunity to get inspired, collaborate, and continue pushing the community forward.

Ashwin Krishnan: [00:00:02] Ok, so with me I have Joe Slowik. Joe's LinkedIn profile describes him as a Threat and Adversary Hunter with Dragos. But let's start with what we were chatting about earlier. In your role as a procurement and assessment person in the U.S. Navy, what were some of the things that you were

seeing coming in from vendors? How did you deal with "noise" coming in? And shifting forward to your role at Dragos, what are you doing differently to ensure that you're not doing the same thing that you were subject to years ago?

Joe Slowik: [00:00:48] So, my background is I was a U.S. naval officer, so responsible for decision-making including procurement, and then I was running incident response at Los Alamos National Lab. So, I was very much a point person to decide on what sort of products we were using and definitely also a destination point for lots of unsolicited messages, e-mails, phone calls, and whatnot. And what always struck me was how similar all the messaging seemed from the various vendors. Whatever the newest idea would be or the latest and greatest trend in the information security space, all the players seemed to pick up on that and not really differentiate, at least not very obviously from how that looked. I can't even recall how many presentations on machine-learning algorithms and artificial-intelligence-focused threat detection I've sat through. And I feel kind of bad because I'm sure there were many people working very hard on these products, but I almost never could walk away with any idea for how product A differed from product B or C or D or E going down the line. Similarly, from a threat intelligence feed perspective, I was always a big believer that we need to know what's coming up next and, even with access to government resources, having access to the commercial space gave a different perspective on items. Really looking for products that could differentiate themselves in that environment well and then investigating those — seeing how many just boiled down to an indicator feed once you really dug into the product.

[00:02:15] So then, once I decided I'd had enough of government for one reason or another and moved into the vendor space myself at Dragos, now how are we doing things differently in order to counter or move away from what I thought was ineffective? A lot of that is based around having, what I think is, a fairly unique mission and really emphasizing that. It's also how we present ourselves, really stressing that we are an intelligence-focused, behavior-focused security company in all that we do and really pushing that message not through

unsolicited emails but really working hard through events such as Blackhat. But also at many smaller events, many industry focused-events within areas we support, so industrial-control focused events, not just security events but actual conferences for asset owners and operators to push the message of not just what Dragos does but how we're doing it and how it's different from how some of the other players in this space are operating. So, if you look at most of our competitors, not to turn this into really a business talk, but again the emphasis seems to really have shifted on to anomaly detection as the primary means of doing "threat detection". The problem that we find with this, and that I found personally in doing security operations in various roles previously, is the signal-to-noise ratio is terrible but you get SOC operate analysts, security personnel that have to chase their tails on an anomaly which has no enrichment and trying to figure out how does something that is anomalous then translate to malicious.

[00:03:47] So the standpoint that we've taken — again we're a company that's been built out of practitioners — it's been very much, what do we want to see, how would we do this, and how do we transfer the knowledge we have to individuals that might not be as experienced or just building on a program? So, we've really focused on technical knowledge transfer of how do adversary behaviors work? What fundamental activities does an adversary need to undertake in order to achieve an intrusion through multiple stages: initial access, entrenchment, pivoting all the way to final attack delivery? What detections do we build around those fundamental techniques that have to be leveraged in order to carry out success? That's sort of what we do, and we try very diligently to emphasize that message, and so far, I'd say it's worked rather well. Maybe it's harder than to just simply blast out the unsolicited message and hope for the best, you know, the sort of, "If we throw a bunch of things against the wall and see what sticks, maybe we'll get lucky." Instead it's very manual and very resource driven, but it's worked very well not just in building ourselves as a company but also in building a brand for ourselves as being very community, very content, and very much threat focused as an entity.

Ashwin Krishnan: [00:04:58] Let's talk about the threats you were talking about earlier about Industrial Control Systems (ICS). What's different and unique about ICS that most practitioners and vendors fail to comprehend?

Joe Slowik: [00:05:12] So, in looking at the environment and how ICS has developed over the last 10-plus years, one item that comes up repeatedly is the idea of an IT/OT operational technology convergence. It's been emphasized repeatedly, if you talk to actual operators in the field, it's nothing new to them even though it seems to be making waves on the vendor front. But what gets lost is there's an opening as a result of that convergence because you brought IT vulnerabilities, IT risk surface, IT threat surface into the operational environment. But that operational environment lacks a lot of the things that we take for granted in the IT environment in terms of logging, visibility, and ability to recover operations. I'd say what's gotten lost in the pivot by a lot of much bigger companies into this space is you can't just turn on a dime and patch a system if there's a vulnerability. You might not be able to do that for months or years until you hit a maintenance period or that equipment gets replaced entirely because it's a continuous process that's not going to be analyzed until it breaks down or it comes up on a refresh period.

[00:06:16] Similarly, from a response method you can't simply go. "Oh, we have an infection. Wipe the malware, clean the box, move on." Again, that's a completely unreasonable answer in many cases because where the infection sits may be a vital piece of the entire process network. The malware itself may not be doing anything that impacts that process. So it's best to just leave it alone, and add some network rules to make sure it doesn't spread. So adding that nuance and appreciation for — you know, whereas in IT environments you really can build almost a one size fits all, one active directory implementation looks very similar to another active directory implementation, but a cracking facility or a plastics-extruding facility or a manufacturing plant within the same organization looks very different from another plant in the same organization because they were built at different times and have subtle differences in technology. This means that you have to really have an appreciation for what

differences are built in and what your capabilities and limitations are for response and analysis.

Ashwin Krishnan: [00:07:17] When you talk about ICS, you talk about these industrial sensors. You mentioned plastics, so there are these non-tech organizations that are now becoming tech users. So what's the barrier to communication or understanding or comprehension where these organizations that are becoming tech users inherently don't have the high tech skills?

Joe Slowik: [00:07:46] I'd say that's a misnomer almost, actually, because they've been tech organizations for a while, they're just becoming tech organizations in a different flavor.

Ashwin Krishnan: [00:07:53] Right.

Joe Slowik: [00:07:53] I think that's one thing as an industry, coming someplace like Blackhat, you see lots of talks about how there's so many vulnerabilities that ICS all over the world is going to explode. That completely ignores all the hard work that engineers have been putting in for decades to make systems that are reliable and fault tolerant, but largely from a process perspective as opposed to a cyber perspective. So there's already a lot of talent and recognition there. The issue is gaining trust of that environment so that people will actually listen to you. You don't succeed at that by talking down to that audience and saying, "Look at all the bad things that you're doing, this operation is messed up." And then once gaining that trust say, "Hey, you know we're peers in this and trying to fight the same sort of battles; let us help you." Then moving on from that to appreciating how those environments work and not trying to shoehorn in solutions that are inactionable and inappropriate for those environments. Instead working to realize that we can't do these typical things. I can't just blacklist a process. I can't just walk in and, you know, really lock down network traffic in a way that might look very familiar in an IT environment. Instead I have to think, "What are my options based upon how your facility works?" And in providing recommendations to clients, understanding that they may have

limitations in what they can and cannot do within this space, provide a broad list of suggestions so that you can apply what's applicable instead of just setting the one-size-fits-all approach.

Ashwin Krishnan: [00:09:19] Yes. So, you mentioned something that absolutely most vendors do. You suggest truly not talking down, not singing off the same playbook and that means you have to truly understand the customer environment, but that takes time and resources which most vendors choose not to put in. So, what you're suggesting is actually an approach which will pay dividends, but it does take investment and time and, truly, I hate to use the phrase "put themselves in the customer's shoes," but that's really what you have to do. And as we talked about earlier, you've already seen that starting to pay off. So what advice can you offer to other vendors who are looking to rise above the noise? What are some of your learnings from going down the path of not talking down to customers, truly understanding what problem they're trying to solve, and being able to build an alliance with the prospect or the customer to solve for a unified goal?

Joe Slowik: [00:10:26] The biggest thing I would say, and what's helped me immensely just based upon my past career experience, is think like a practitioner when you're trying to execute as a vendor. And when I say that what I mean is, I'm not just building a product. I might have a great idea but I'm implementing it and framing it. Whether we're talking in marketing or technical messaging, how is someone actually going to use it? Think about those use cases and how it fits in to solve problems because we're not selling — looking at the vendor space, if you're looking at it as selling a product, you're probably wrong to begin with. You should look at it as trying to sell solutions. So identify what the problems are that you're trying to solve and work your communication in that respect. And in that respect, advertising a technology may not be the most appropriate way of communicating that. Instead messaging how this technology solves these concrete problems for your target audience is probably the best messaging stance to take.

Ashwin Krishnan: [00:11:20] So one thing you mentioned about Dragos, which is interesting, is you said this is essentially practitioners who are now coming together to solve a problem. Most vendors don't have that luxury. So, what advice do you have for vendors who haven't ever been on the practitioner side of the house; how should they go about understanding truly? If I'm a vendor and I come to you saying, "Hey Joe, tell me what your problem is." You're getting bombarded with 20,000 emails, right, so why would you spend time even educating me? So, what are the avenues that vendors should use to try and get into the customer's shoes without the customer actually giving them that much time?

Joe Slowik: [00:11:59] So from an initial relationship standpoint, it is hard. I would say it almost depends, especially if you don't have people or just people that you're bringing into the organization don't have that background. Looking for opportunities with customers that you already have is different, more like, "Hey we're partnering on this. We're providing you with a solution to your problems. Can we work together? Can our people embed or visit for a day or two with your organization to see how you're doing things so that we can get better?" Then that builds an appreciation for how things are used. It's more difficult when you're talking about a new enterprise completely that doesn't have customers yet. So how do you actually move along those lines? From that perspective, I'd say research and listening. Going, not to the big security conferences necessarily, but think about your target market and go to those events. If you're trying to sell something in the financial sector try to participate in FS-ISAC or events that are actually tuned to that environment. See one of the people on the ground who is using these sorts of products. What are the issues they're having, how are they communicating this, and tune your product to that.

In the industrial space one thing that Dragos does, while we do participate in the big security events like Blackhat, most of our time is spent on industry events because those are the people we're selling to, that's our audience. The greater threat intelligence community or the security instrumentation community doesn't like what we're saying? We don't care because that's not our audience. Our

audience are the people who are running oil refineries and power plants and making sure that how we communicate and how we're framing things is more appropriate. That's an approach that any company can take as long as they have the time and willingness to do so.

Ashwin Krishnan: [00:13:31] Yeah. That's a really interesting point because we kind of get fixated on going to these brand-name events, right, with like-minded souls who live and breathe the same thing. But you're right, there are lots of other industry-focused events where your customers actually show up. You may not have a speaking slot on a panel, but you can go and listen and hear what others have to say.

Joe Slowik: [00:13:51] Exactly. People might look down on a panel discussion of a bunch of engineers talking about oil refinery problems, but I would say that's an excellent opportunity to try to operate in that space and to see what their issues are. How does the facility operate? Even something as simple as having an understanding for how these environments work by watching a few "How It's Made" episodes or YouTube videos that give an understanding for how the process works. Whether you're talking about how a credit card company operates or how power is generated, being able to speak the customer's language and having an understanding for their process means you can start building out what their security needs are from there.

Ashwin Krishnan: [00:14:29] Do you have any suggestions for the vendors actually to create a community where they can start sharing more information? We seem to be in this siloed view of the world where I'm going to talk to a customer, glean some data, and go build my roadmap or strategy. At Dragos or in your previous jobs, have you had the ability to see whether groups of communities of vendors coming together and sharing information has yielded any results, or do you think that's a fool's errand?

Joe Slowik: [00:15:04] I think it works out really well when you're talking about complementary capabilities, but it's very hard when you're talking about

competing capabilities. That's an important distinction. Another thing that I'd say makes us stand out from others that are operating in the space we're in is we, aggressively might not be the right word, but we diligently pursue partnerships with organizations that don't do what we do but that allow us to fill in gaps and integrate with a lot of different solutions. So, we can come to a client and say, "Hey you have this problem, that's not something we solve, but we are integrated with and work together with guys and girls at this company. As a result, we can try and develop a solution that really fits your need as opposed to just being another blinky box sitting in the server rack.

Ashwin Krishnan: [00:15:51] So, the approach that you're taking is really looking at how the adversaries go about their business. Any thoughts or insights that you can share on how the adversary community is evolving over time? They're not sitting still.

Joe Slowik: [00:16:08] No.

Ashwin Krishnan: [00:16:09] So for instance, yesterday I was having a conversation where we were talking about phishing as a service where there are full-fledged platforms. We talked about AWS and S3 and EC2 and all that, well the exact same full stack exists for anybody who wants to launch a phishing attack. So from your perspective, how has that community evolved and what should — as practitioners as well as vendors — it's not a fixed target, so given your particular insight, given your vantage point, how has that community evolved and what should we be expecting going forward?

Joe Slowik: [00:16:44] So, the community has evolved by almost a sort of regression in tactics, but it's highly effective. I mean if it works it's effective. Going back a few years to the 2013-2015 timeframe, we were seeing development of custom malware for operating in ICS environments, things like Havex or items along those lines. But now what we're seeing increasingly, at least for initial stage intrusions, is that adversaries have pivoted to using as many native-system tools and command-line techniques as possible. One, because they don't have to

bring in tools to the environment which is a detection point, and two, because it's very effective, especially in industrial environments where the visibility is still poor, to hide as a result of that. So from a solution standpoint, what do we do to counter this migration and these threats? Visibility is key. You're really building in not just log monitoring but getting very aggressive in terms of process monitoring, power shell logging when you have systems that are Windows systems that are using power shells, really tracking executables as they move throughout the environment to stay ahead of that issue. Then when we see the snapback from this current trend, one thing that has emerged already is we've seen the re-rise of the worms, for example with last year's Wannacry and the other, the MS17-010 exploit kits.

[00:18:05] We haven't seen too many cases of state-sponsored actors using them yet. Maybe Olympic Destroyer being a counter to that, but that relied mostly on credential theft and reuse. But I would expect in the future to see adversaries start weaponizing those wormable techniques to go back to a more automated fashion, instead of what we're seeing right now with a lot of very much hands-on keyboard malicious scripts, malicious commands run fairly manually across the enterprise. Counter to that on the actual ICS attacks standpoint, we're seeing dramatic increases in automation and the technical codification of ICS manipulation in software. So looking at attacks previously, Stuxnet being an outlier, is that the Ukraine power events and other similar items largely relied on a human operator. In 2015, someone remotely logged onto an engineering workstation and basically flipped switches. Whereas in 2016, with that Ukraine event we saw the switch-flipping action codified in malware. The person executing it didn't need to know anything about how an actual control system works. They just needed to run the executable. And that passed on to the Trisis event in 2017. So, we're really seeing adversaries put the work in to have a development codify that specialist knowledge, so that any sort of hands-on keyboard person can run it without having to have that information. It really allows operations to scale more effectively.

Ashwin Krishnan: [00:19:35] Wow. Yes, and sometimes we get caught up in efficiencies and use of cloud, but all these tools are also available to the adversary.

So, what would success mean for you at Blackhat? I know you've been here or will be here the entire week. What would be a mind-blowing Blackhat for you. What's the one outcome that ...

Joe Slowik: [00:19:54] The biggest thing with Blackhat — and I regret that I have so many things going on, I will not be able to sit in as many briefings as I would like because there's always great content — but the nice thing with Blackhat, even as large as it's become, is that everyone's here.

Ashwin Krishnan: [00:20:07] Yes.

Joe Slowik: [00:20:08] From the standpoint of people I follow on social media or interact with in chatrooms or whatever, this is always an opportunity to do face-to-face meetings and collaborate. And my big hope every time I come to an event such as this is that I come up with an idea for a project, either on my own based on things that I learned or that I could work jointly on with some of our partners or even just friends, to solve another security problem. That as a result of this, we can continue pushing the security community forward and, you know, just make life harder and harder for the adversary with every passing year.

Ashwin Krishnan: [00:20:42] Cool. Very good. Good. Good chatting with you.

Joe Slowik: [00:20:45] Excellent. Thank you very much.