Bryson Bort, CEO of SCYTHE and Founder of GRIMM

Breaking the Cybersecurity Status Quo

Bryson Bort is the CEO of SCYTHE and founder of GRIMM. Here he discusses the information security status quo and why the industry fails to truly progress. He addresses the promise of AI and machine learning and shares how his latest venture plans to halt malware for good.

Ashwin Krishnan: [00:00:02] So, I have with me Bryson Bort, did I get your last name right?

Bryson Bort: [00:00:07] Yes.

Ashwin Krishnan: [00:00:08] OK, I'm bad at names, last names particularly. Let's start with your thought process in terms of, what are we going to be seeing, or what are people already at the expo seeing, at Black Hat but without really offering a solution to what vendors should be doing. I think just saying, "Hey, stop doing what you're doing," is kind of pontificating without any real solution. From your perspective, how do vendors start behaving differently? Clearly what's happening right now, which is just using buzzwords, just using jargon, and trying to throw FUD isn't working at all. What's your take?

Bryson Bort: [00:00:53] So, it's not that it's not working. We have an ecosystem of agents that are incentivized with certain behaviors and that's not vendor specific. I don't mean that as in this particular vendor, but as in the overall vendor ecosystem and the yin and yang relationship that it has with the CISOs and the practitioners. Let's be honest, what's a CISO? He's a con man. He is the greatest con man that we've seen in the history of mankind, but how could he or she be anything but? When you look at what their options are it's the herd mentality of, "I'm going to do all the things that are known, and I'm going to cross my fingers and hope that nothing bad happens during my tenure." Contrast that with the CIO. The CIO is in a day-to-day operational requirement, if something does not happen the CIO gets immediately yelled at. The only time the CISO is ever in the hot spot is when something really, really bad happens to the business.

[00:01:52] That brings us to the next problem, which is information security and IT are filled with nerds who talk nerd really, really well. Well, the business operations don't talk nerd, they talk business. The reason that the business exists is for whatever its purpose is: making the best cookies on the planet, building shoes, coming up with the latest mud cream from Zaire. Whatever that purpose is, that's why that business exists. Modern business succeeds and scales based on the quality of its IT system to do that. IT is very nestled in with business. Think large budget, purpose of this existence, this mission. IT is a fraction of that supporting and enabling it to scale and work globally. Then you have security, which is a fraction of IT. So, you start to see the relational piece and that ties to the budgets and ties with how important things have to happen at that piece. Security is there to assure that IT can successfully help business do what its mission is. That's the side of it from the customer and the practitioner perspective.

[00:03:01] Now let's take it to the vendors. The vendor hall is filled with brilliant folks who all believe in what they're doing, and if you actually get past the hype and say, "Really show me what you've got," what they have is a really good pinpoint solution to something. The overall knowledge area of the way information security works today is - I really like quantum physics and if you think about the understanding of how we look at the growth of the universe, the universe is expanding and it's this sort of sphere that bubbles out and it's not perfectly uniform - that is the allegory for our understanding of information security. We are every year continually surprised by learning at Black Hat, at

DEFCON, at these conferences, the latest research on the edges from offense, "Oh, look what we can do now." Then the defensive products all, two to four weeks later, adapt and it's like, "Well, remember that thing that happened last month? We can do that now because the universe of knowledge has expanded into it." Just like in one of the potential theories of our real universe in information security that space of knowledge is infinite which is why you look at the overall industry. All we're continuing to do is react to the attacker and come up with a point solution that's basically just patching our level of knowledge until we get surprised again. That's the Sisyphean nature of where we continue to have an ecosystem that generates a lot of money, a lot of ideas, but makes no progress other than maintaining an effective status quo.

Ashwin Krishnan: [00:04:38] You mentioned earlier the effective status quo can only be maintained if you have that ratio, that infinite to finite. Is the challenge also that you can't turn anything off? Everything that you have accumulated over the course of decades, even if you haven't seen that attack, is there the confidence to say, "Let's take that particular one off the firewall because we haven't seen this at all?" Are we at a point right now where the CISO has the moral courage to stand up and say, "We're changing how we going to look at things. We're going to start turning things off?" Or is it this spaghetti of piecing together various things because you don't get fired until a breach happens. Since you are not in the crosshairs until a breach happens you can potentially get by for 18 months, which is I guess the average tenure of a CISO.

Bryson Bort: [00:05:41] Well, the other dirty secret of the CISO is the only time they get any validation that any of their controls, any of their product, any of their personnel perform anywhere close to expectation is when something bad actually happens. And let's be clear, it's not when it happens it's the 200 days later when they discover that it happened.

[00:06:07] So, turning things off has two things. One, that doesn't solve the problem. I, as an attacker, there is a solution for me to get to things that are turned off. This is the edge of understanding the attacker perspective, and this has been my career for two decades: building offensive capabilities. There is always a way. I will always find a way. There is no scenario that you can come up with that I cannot come up with a solution for. It's a question of how much effort do I need to put in. It's going to be a cost function not an if function. That's a key understanding. The threat model in the past has been, "Well I don't have to be faster than the bear. I just need be faster than you running away from the bear. That’s because the attacker will go after you since you're a low hanging fruit." The shift that I'm predicting in the environment is that that model is going to fail.

[00:07:00] The example I draw is WannaCry last year. I don't believe WannaCry's purpose was to take down half of England's hospitals. I don't think that's what its purpose was. What I think we saw was the transfer of nation-state knowledge out into a public sector that exponentially increased the effectiveness attacks that are now available to whomever. What does that mean? Well, look at how interconnected everything is, the fact that everything only speaks in very few ways to each other. It's a rather homogenous environment, both from an IT and a security perspective, because we have consolidation around multiple vendors and certain things, and they all fundamentally work the same way. The original threat model of "I have to avoid you coming after me" is now going to be replaced by, what I call, Collateral Splashed Image. I think that's what happened in England with WannaCry. They were going after something over there, some other industry, some other target, because there was some connection and there was some shared resource. Vulnerabilities are not silver bullets. They're required to be very surgically precise to work, but if there's enough homogeneity in the environment it will work across places that the attacker never intended.

[00:08:18] Kind of the same way that Stuxnet got out, one little logic error and suddenly anything that matched that with Siemens was a vulnerable target. Clearly, whoever was behind Stuxnet was not trying to go after German manufacturing systems, that was clearly not the intent, but that didn't stop it from happening. And I think that's going to be the increased risk we have going forward.

Ashwin Krishnan: [00:08:38] So how does it work? And this is interesting for the vendors. Say, as a vendor, you've been at fault or you've been diagnosed to have a problem and it's been breached in a customer environment. Is the thought process, like the Siemens example, that if that same vulnerable product is available across 20 or 2,000 different customer bases, does a vendor need to start thinking about the overall scope? Do they need to understand that this is not just a one-and-done thing where they share a patch with the customer? Should they be trying to solve for a bigger goal? Lots of times, it's just Band Aid solutions to, "Hey, there's an escalation coming in over here, let's roll something out." Should executives be saying, "No, this is bigger than that?" That requires gumption. There's obviously going to be negative press. Your shareholders are going to be unhappy. Your stock price is going to tank. What's the incentive, why would a vendor stand up and do the right thing?

Bryson Bort: [00:09:47] Well, they are. I mean, you go back to the original premise, the vendor ecosystem is doing what it's incentivized to do and tying it to the yin and yang with the CISO. I'll throw this one back on you, Ashwin. Give me a better approach.

Ashwin Krishnan: [00:10:03] There isn't!

Bryson Bort: [00:10:03] There is, yes, there is. OK, I came up with a hypothesis this year and I'm working on it. Here's how it goes. We've already covered that when we try to go to the attacker we lose repeatedly. This is because we are stuck in the Groundhog Day's loop of, "I continue to discover edges and my learning moves into the infinite knowledge of which I will never reach a finite state and there will be no equilibrium." The best I got is, "I have to pour in effort to maintain a status quo." OK, that's the current industry writ large. Well, what if we looked at it a different way? What if, instead of thinking, "How do I go to what the attacker is doing?" I thought, "Where does the attacker come to me?" Most of the industry effort on that has been around the detection and prevention of exploitation which is an infinite space. So I never win. By the way, I have no metrics to quantify anything. There is zero proof that anything works better than anything else, which is why I argue there's no such thing as a cyber expert. We have a bunch of opinions, and I can make very strong cases for my opinions.

Ashwin Krishnan: [00:11:14] There's really good-looking cyber reports that justify anything.

Bryson Bort: [00:11:17] Oh yeah! I love it. Threat intelligence, it's great. What does it do? It gives me a femoral understanding. Where does the attacker always have to go? After they gain access, which is the purpose of exploitation, all they've done is open the door to your house. They haven't walked in yet. What do they do once they walk in? They drop code to accomplish their goals, they haven't done anything yet. They drop that implant, they drop that payload, it's a stage zero drop or to make sure it's safe, and then they start pulling in additional capabilities or it's an immediate ransomware that's going to spread. Well, that code only consists of two things, communications and capabilities. How does it talk? What does it do? All right Bryson, that sounds great, you're doing a good con-man routine here, make your point. Communications. It has to talk through the wires of the enterprise, which means it has to talk through the same protocols, communication protocols, that every business talks with. That's how businesses are interconnected and able to talk to each other. If I'm talking Greek and you're talking Romanian we're going to miss each other, that's why we negotiate things like my mail to your mail. Regardless of the language, we're going to use SMTP, and all of us on the web are going to use HTTP and HTTPS, and we're going to resolve the domains with DNS. You start looking at it, there's only a handful of communication protocols that are used throughout business. The attacker has to use those protocols to talk back home. That's a finite number.

[00:12:54] And then what does an attacker want to do? While there might be a handful of ways to skin the cat, if you look at the end behavior it's limited. They don't want to do everything. It's not like they're popping Excel and, you know, doing Hello World. Credential thefts, ransomware, passive active surveys, escalation pivot, lateral movement, there's a finite number of actions they want to do on computers.

[00:13:21] So, the research that I'm pulling together and my thesis here is, we're no longer in an infinite space. The number of permutations of capabilities and communications might be a large number, but guess what, it's a computed number. It's a finite number. I now know everywhere that an attacker can look and talk in an enterprise.

Ashwin Krishnan: [00:13:41] Further to that point, now as these things get institutionalized and you have platforms that are available you're going to get more of the same. So, if you have phishing as a service, you have infection ...

Bryson Bort: [00:13:52] Phishing is an access vector.

Ashwin Krishnan: [00:13:53] Yeah, okay ...

Bryson Bort: [00:13:54] Again, what does the phishing do? The phishing gets the credentials, gets the access, and then I do something, right? The phishing is a service; all that does is show you repeatedly two things. One, email is the greatest attack vector of all time because there is a marginal cost difference between sending one email and one billion emails. So, statistics are my friend as an attacker. Two, somebody will always on purpose or accident click on a link. That's all it proves. And training your users doesn't solve the problem, all it does is change the statistics of how many times it does get clicked out of a billion. It's still clicked. You're still back in the access vector again. It opens the door to what I do next. And what I do next has to be in that space, that is the entire potential space of what an attacker can be and do. So, instead of us going to try and understand again. There's always going to be one. But where do they end up? They always end up like that. They're always code or payload doing those things that way. They have to be, what else could they be? I mean, if they show up with their own custom-rolled protocol, I'm sorry the most junior analyst can spot something you want to cross the wires.

Ashwin Krishnan: [00:15:08] It has to be standard protocols.

Bryson Bort: [00:15:08] Yes. It has to be like anything else, so the secret squirrel stuff doesn't work. You have to blend in. You are the wolf among the sheep, put on the sheep's cloak. That's what the communication protocols do.

Ashwin Krishnan: [00:15:22] Interesting. So, the approach that you are suggesting is making this more finite because of communications and capability. But are the capabilities that you allude to, these five or six things that you talked about, are those enduring? Are you seeing those evolve as well? I mean, I could masquerade through 443, and my egress firewall rule may not fire up at all. I could use encryption that ...

Bryson Bort: [00:15:57] 443 is by definition encrypted. You don't have an SSL splitter at your perimeter, you're done.

Ashwin Krishnan: [00:16:02] How do you do that?

Bryson Bort: [00:16:04] Well, that's not fair because there's ways of dealing with encrypted traffic. Where you're looking at the metadata that's not encrypted and you can, in fact, pull out TTPs and understand what's happening with that traffic without looking inside. So, that is a possibility.

Ashwin Krishnan: [00:16:19] Yes, ok granted. So, given that you're a wolf in sheep's clothing, from a defense perspective - back to the vendor community - if I'm looking for anomalies, I'm looking for variations so I can spot the attacker and you're suggesting that they're going to use the same mechanisms, how do I assess things up?

Bryson Bort: [00:16:44] So, what if there was a possibility to ... Your problem is you have all these vendors and all these products and all these things, but you have no metrics to be able to assess or compare the difference, and you have no ability to tune the sensors and the tools to be able to do anything.

[00:17:05] So you're stuck on the blue team side which is being overwhelmed with false positives. What if I could arbitrarily spin up actual implants that replicate against that entire known spectrum continuously to solve that problem. Is that cool?

Ashwin Krishnan: [00:17:30] That's sounds cool, but is anybody doing it?

Bryson Bort: [00:17:33] I happen to have started a company called SCYTHE and that's our platform.

Ashwin Krishnan: [00:17:36] OK. Give me a little bit more insight into what you guys do and how you solve for that.

Bryson Bort: [00:17:44] I mean, what I've just said, we allow an end customer to replicate the entire potential attacker's space. And the way we do it is by providing you the ability to spin up out of that space the actual campaigns with the payloads themselves. The failure in that space would be to approach it with the technically-limited nerd perspective of, "I'm just going to do traffic and test technical controls." Well, what's the largest surface area of every organization? You said it earlier, it's people. So, if I'm not including people in this, then I'm missing a proportion of understanding my controls. If I'm not working with the real thing in seeing the behaviors of that thing, not just assessing it technically, then I'm missing the other critical point, going back to earlier where we were talking CIOs, CISOs, and the business perspective, which is what is the business impact? Tell me why that matters. Well, that matters because this person clicking this email led to these series through the MITRE ATT&CK framework of this computer to this computer, to these things, to our customer data. We now understand that the controls failed. Now, if we tune our EDR to be looking for these behaviors this way, we would stop that kind of campaign. And, by the way, we would stop that kind of campaign forever because we can prove that, and we can run that over time with multiple looks out of that space.

Ashwin Krishnan: [00:19:12] So what you're suggesting is, I hate to use the word revolutionary, but it's definitely something that has not been talked about in the past. From a CISO standpoint, you are against the CIO who is extremely tight with the business, increasingly so. You're coming with the approach which says, "OK, I'm actually going to understand what an attacker does and be able to simulate that in the environment." How does she explain that to her peers on the board? As to, "My job is changing, I can't deal with infinite. I'm going to deal with the finite, which means I'm going to have to do something which is mimicking what an attacker really does." What sort of mentality shift do CISOs have to go through to be able to embrace that?

Bryson Bort: [00:20:06] I presume your question is one of risk.

Ashwin Krishnan: [00:20:10] Right. What does it mean to the business, if I do what you suggest?

Bryson Bort: [00:20:13] The one area in attacks that I've never seen anyone be able to successfully simulate in a production environment, by the very nature of what it is, is DDoS because that is operational impact.

Ashwin Krishnan: [00:20:26] Correct.

Bryson Bort: [00:20:27] So the best you got is you can do things in a lab, right? That's the one area where I have never seen a solution, and I've had a few people pitch me some different ideas to it, but I haven't seen anything that really convinces me. Other than that, I mean creating simulated malware just means that, where you simulate it like ransomware. How would I simulate ransomware? Well, there's the way of actually doing what ransomware is, like one of the campaigns from last year which used DNS communications for its C2.

It used SMB communications, sometimes out of the perimeter, but to move laterally. And then of course it encrypted the hard drive, popped up and said, “Give me bitcoins.” Doing that would not make anybody happy.

Ashwin Krishnan: [00:21:14] The CIO's not going to come and say, "Hey, that's good!"

Bryson Bort: [00:21:15] Thank you for proving that by breaking everything. Get out and the lawsuit will be coming. How about instead, I have all those same comms, I have an encryption capability that if it lands on that box makes copies of files of interest. So, we do the copies, encrypt those files, and the user goes on, but clearly, you've marked that that would have been a ransomware campaign. You can see what was detected, what was the response to this unauthorized encryption happening in the environment, without actually infecting the environment another way.

[00:21:51] We're now seeing crypto-jacking. It turns out that the utilization of computational capacity in the world writ large between enterprise computing and IoT is woefully underutilized. Perfect when bitcoins now pushing, I think it's down to like seven or eight thousand dollars a bitcoin, but I'll take that. Instead of causing the 100% spike, we'll have something that pays attention, uses the resources that are available, and works in a more constrained manner. It never affects the user and is ultimately chewing cycles to demonstrate that with sending out fake data like it's going to wallets. You make sure that it's doing it, and it doesn't do it optimally the way a crypto-miner would actually want to do things, but it does something that simulates it there, so you can see it. You can see the effect and there's enough to notice the activity, but you don't affect the end user. Those are examples of how you do that.

Ashwin Krishnan: [00:22:50] Those are great examples because I think at that point you could easily convert that into a report where a non-technical board member could see if this had actually happened this would be the impact.

[00:23:01] Again, I hate to use the word revolutionary, but this is definitely so. The few companies that I've spoken to that are actually talking about stuff that is showing what the business impact is versus just throwing a bunch of reports out there that make you look good.

Bryson Bort: [00:23:18] I mean, let's put it in perspective. If we're right, we've just created the map to allow everything else to be measured. We are not solving the solution. We're just able to help all of those other vendors prove, tailor, quantify what's being done so the business can look at it from portfolio investment, rationalization, and measurement. I haven't solved the problem. All I've done is create a map.

Ashwin Krishnan: [00:23:48] But the map is measurable, it has bounds. It makes things quantifiable. As a CISO you can go, "Okay, this is the impact."

Bryson Bort: [00:23:55] Right, but I do want to put it into perspective, that's all we've done. I believe it's going to be disruptive, but let's keep it in perspective of what it does accomplish. It ties back to one of the other problems that we see over and over again in information security which is the talent-shortage rate. If you're a mid-size company, you're trying to go from zero to one security personnel. If you're a high-level company, you've got the pyramid shape of a ton of juniors who are dealing with a bunch of false-positive trash and sifting through the haystacks looking for needles without even knowing what those needles look like. Then you have a few very good people up above. And that is the promise of machine learning and artificial intelligence.

[00:24:43] As you know. one of the things that I've pushed out in the past is that AI is a lie. It is, and it isn't. Let's qualify the statement. First of all, artificial intelligence today does not effectively exist in an operational environment. You have a lot of machine learning algorithms and capabilities, and we've just grabbed on to the artificial intelligence hyperbole because it's a nice marketing skit. Artificial intelligence will happen in our lifetime. There will be some operational relevance to it and it's going to happen like that [snaps fingers]. It will be one of the things where incremental improvements in the billions make no difference. Then suddenly going from a fraction to one-tenth of an effective FTE, it's going to be immediately noticeable in the environment. The promise of machine learning and artificial intelligence that so captures the interest of the community is it solves the talent problem.

[00:25:38] I have more data than I can shake a stick at. Right now, I have a bunch of poor human beings sitting there churning through it in mind-numbing fashion because what else do I got? That machine learning and artificial intelligence promise does solve that problem. The caveat is where is it at, promise versus reality. The other risk is it has the same potential flaws of any human being ...

Ashwin Krishnan: [00:26:06] Yes, the biases.

Bryson Bort: [00:26:07] It has the biases of its makers. It has the algorithms trained by whatever the quality of that data is, its ability to be affected by whatever data somebody else pushes into that environment intentionally. The fact that it can only see what it can see; it can only analyze what data it gets. Well, what have attackers been doing since the history of computing? We have been intentionally providing you only the data we want you to see, which is why it takes so long to find us. Someday somebody will find a way to flip an evil bit on us and then we'll be lost. Until then, you know that's the way it is.

Ashwin Krishnan: [00:26:48] Cool, any last thoughts? What would success mean for you at Black Hat?

Bryson Bort: [00:26:52] What does success mean for me at Black Hat? That all of the vendors don't bring torches and tar and feather me out of the conference for saying there's no clothes.

Ashwin Krishnan: [00:27:04] This has been very, very fascinating. Bryson, thanks for your time.

Bryson Bort: [00:27:07] Ashwin, thank you very much.

Main discussion topics:
00:53 The difference between a CIO and a CISO. Aka, the CISO is just a con man.
03:01 The real reason information security is not progressing.
07:00 The interconnected nature of IT makes it easy for ransomware to attack multiple targets, whether they intend to or not.
10:03 Communication is key. Malware communication protocols are the solution to stopping attacks.
13:54 The attackers are wolves in sheep's clothing.
17:44 What if we could replicate the attacker's potential space?
24:43 Can AI solve the talent problem?