SDS PODCAST
EPISODE 273:
PREDICT, PREVENT, DETECT:
CYBER SECURITY

Show Notes: http://www.superdatascience.com/273
Kirill: This is Episode Number 273 with Cybersecurity Strategist, Matthew Rosenquist.

Kirill: Welcome to the SuperDataScience podcast. My name is Kirill Eremenko, Data Science Coach and Lifestyle Entrepreneur, and each week, we bring you inspiring people and ideas to help you build your successful career in data science. Thanks for being here today, and now, let's make the complex simple.

Kirill: This episode is brought to you by SuperDataScience, our online membership platform for learning data science at any level. We've got over two and a half thousand video tutorials, over 200 hours of content, and 30+ courses with new courses being added on average once per month. You can get access to all this today just by becoming a SuperDataScience member. There is no strings attached. You just need to go to SuperDataScience.com and sign up there. Cancel at any time.

Kirill: In addition with your membership, you get access to any new courses that we release, plus all the bonuses associated with them. Of course, there are many additional features that are in place or are being put in place as we speak, such as the Slack Channel for members, where you can already today connect with other data scientists all over the world or in your location, and discuss different topics such as artificial intelligence, machine learning, data science, visualization, and more or just hang out in the pizza room and have random chats with fellow data scientists.

Show Notes: http://www.superdatascience.com/273
Kirill: Also another feature of the SuperDataScience platform is the office hours where every week we invite valuable guests in the space of data science and interrogate them about their techniques, about their methodologies in the space of data science, and you actually get a presentation from the guest, and you get an opportunity to ask Q&A at the end. In some of our office hours, we just present some of the most valuable techniques that our hosts think are going to be valuable to you.

Kirill: So, all of that and more you get as part of your membership at SuperDataScience. So, don’t hold off, sign up today at www.SuperDataScience.com. Secure your membership and take your data science skills to the next level.

Kirill: Welcome back the SuperDataScience Podcast, ladies and gentlemen, super excited to have you back here on the show because today’s guest is one of the top leading world experts in the space of cybersecurity. Matthew Rosenquist is the former cybersecurity strategist at Intel. Matthew spent 12 years at Intel Corporation working in the space of cybersecurity. He is on the board of multiple companies as their cybersecurity adviser.

Kirill: He’s made numerous appearances at conferences and on podcasts where he talks about cybersecurity, and he constantly shares valuable information about cybersecurity on LinkedIn, where he has over 180,000 followers.
Kirill: So, even if you don't listen to this podcast today, make sure to go to LinkedIn and follow Matthew because he shares some very valuable information in the space of cybersecurity.

Kirill: What are we going to talk about today? Well, this podcast was extremely insightful. At some points, I found myself listening in awe to what Matthew was saying because he showed some very cool examples of cybersecurity, whether it's in the corporate space or individual space, how data science is connected to all of that, and what kind of world we live in now, what it's all about.

Kirill: So, here's a couple of spoilers from what's coming up. So, in cybersecurity, you need to find a balance. You cannot protect everything, but at the same time, you need to protect the most crucial thing. So, here, today, you will learn what that balance means, what it's all about between protecting enough and also balancing the cost it takes to protect. Matthew shared his view on the threat agent archetypes from cyber criminals to nation-states, to data miners, and more. You'll hear Matthew's story of how his career developed.

Kirill: We talked about the dark web. I was always curious what the dark web is about. Well, in this podcast, you'll get a small overview of what the dark web actually is. We talked about hacks, some recent hacks such as the Equifax hacks, some healthcare hacks, the Marriott hacks from last year. We talked about the role of data science in cybersecurity, and the first steps you can take to get into the space of cybersecurity or incorporate cybersecurity in your

Show Notes: [http://www.superdatascience.com/273](http://www.superdatascience.com/273)
career because those data scientists that manage, data scientists, machine learning experts, artificial intelligence experts, those who manage to incorporate cybersecurity in some form or another in their careers are going to be super valuable and going to do a lot of good for this world. So, it's definitely something that you might want to consider for your career.

Kirill: My favorite quote from today's podcast was actually, "Technology is the playing field." It's a link to or a preview of what Matthew will say on this podcast about how he thinks about strategy of cybersecurity. I think you'll find it extremely valuable, and you'll be very surprised extremely. I was extremely surprised by the book that Matthew recommends on today's podcast. So, make sure to listen to the end and check it out.

Kirill: That's just some previews. There's plenty more happening in this podcast. Great fun. Can't wait for you to check it out. So, without further ado I bring to you Cybersecurity Strategist, Matthew Rosenquist.

Kirill: Welcome back to the SuperDataScience Podcast, ladies and gentlemen, super excited to have you back on the show here today because we've got the former cybersecurity strategist from Intel, Matthew Rosenquist joining us. Matthew, welcome. How are you doing today?

Matthew: Doing great. Thanks. Thanks for having me.

Kirill: Thank you for joining us this lovely morning in Northern California. What an amazing chat we just had before the podcast. It's really exciting to meet with
a cybersecurity strategist. I don't think I've dived into this world deep enough before. So, very excited to kick things off. How did you get into this space of cybersecurity?

Matthew: Well, I've been doing security for about 30 years now. I originally started by doing investigations, internal and external for companies, primarily for theft, fraud, embezzlement, counterfeiting, things of that sort. So, when I moved to Intel, there was a huge need. Intel's a massive data company, and tremendous intellectual property and computing assets around the world.

Matthew: So, back in the day, what, 23 years ago, somewhere in that area, we didn't have a security operations center for crisis management or anything. So, I developed some proposals, some proposals to land and create, build and run Intel's first 24x7 security operations center. I proved that, yes, this is something we need to do, and they gave me the green light. I built it, ran it, managed it, and from there and on, just took progressive challenges within the company.

Matthew: I managed our 24x7 cybersecurity response, basically our SERT team. I built that from the ground up and was the corporate incident commander. So, I was in-charge of everything, managed the cybersecurity for all of our mergers, acquisitions, divestitures, site closures around the world. I was on the product side, protecting some of our products, and all of our IT systems. I'm all over the place.

Matthew: It's a fascinating challenge. I love working with the industry, and I love synthesizing those technology
world and the behavioral aspects not only of the attackers, but also of the victims and the process that connect all of those things. So, I am hugely passionate about cybersecurity.

Kirill: That is amazing. Having a title commander inside a business, I've never heard of that before. That probably just sticks to your passion. That's crazy as you said.

Matthew: Oh, it's wonderful, right? The different roles and challenges, I couldn't ask for a better career. I really couldn't.

Kirill: Speaking of, as we just discussed, you just recently resigned from Intel, and what was that decision associated with?

Matthew: Oh! I've been working again for 30 years, and although I love this, I wanted to spend more time with my family. I wanted to go off and work even more in the industry working with various advisory boards. I'm on several right now, and do more external speaking. My regular full-time job was impacting that a little bit, but it was something that I've been working towards.

Matthew: Think of it as semi-retirement, so that I could be full-time doing industry cybersecurity work. Intel has been great. Part of my last role was actually building and managing the cybersecurity for our artificial intelligence product group. So, I got to come in, build that from the ground up, run it, in addition to helping out all the other divisions and reaching out to the industry. So, it's a tremendous time commitment there that now I can shift off and do things like talk with you today.
Kirill: Fantastic. I'm very grateful as I'm sure most of our listeners are as well. It's a big step as well in somebody's career to take that step away from full-time work in order to commit more of your time to giving back to the community and contributing to impact a broader variety of people and companies, and industries, and countries. So, I think it's a very exciting time that you're entering in your life right now.

Matthew: Oh, it is, it is. Some of the highlights of my career is really reaching out and advising academia, advising businesses, and advising governments around the world. I've been doing that for the better part of my career. I just get to expand on that now.

Kirill: Fantastic.

Matthew: At the end of the day, this is such a big challenge that we have. If we don't communicate and collaborate security professionals across all the domains and all the industries, we lose because the bad guys are working together. We have to work and collaborate together to move forward.

Kirill: I totally agree. Maybe to kick us off a little bit into this world of cybersecurity, so for those of our listeners who are not fully immersed or even for myself, I worked in cybersecurity a bit when I was in Deloitte Forensics, but nowhere near to the line of experience, enrollment that you had in this industry. For our benefit, could you give us a brief overview? What is cybersecurity? How is it different to information technology and the problems that are faced in that
space, and what's the state in the world of cybersecurity?

Matthew: Oh, those are some big questions. Okay. Let me take a shot at this. When we look at cybersecurity, cybersecurity is an evolution, right? An evolution from data security, information security, managing uptime, but if you really just think about it, cybersecurity is the combination of digital security and everything around that, the confidentiality, availability and integrity of systems, data, people, things of that sort, plus privacy, and also, safety now because we are empowering and relying upon technology in such a manner that we're putting our lives at risk, whether it's critical infrastructure, whether it's the trains, planes and automobiles that are going to be driving us or flying us.

Matthew: When we look at all of that, the security, the privacy and the safety, that's really what encompasses cybersecurity today and moving forward. Now, cybersecurity has risen basically at the same pace as the digital transformation. As we embrace digital technology and it becomes part of what we value, it also becomes a target, right? No matter what thing out there is valuable to us, there's always an attacker shortly thereafter. Right now, digital transformation is turning everything, everything from our finances, our healthcare, our government, our politics, our communications, all of that, digital, and it's valuable to us.

Matthew: So, when we look at the threat agents, the attackers, well, they want to leverage that for their own games,
and there are many different types of threat agents out there, whether it be government or cyber criminals or data harvesters, thieves. They all want a piece of that. So, there’s a certain amount of equality as we rise in technology in regards to the threats. Threats always accompany that.

Matthew: Where are we today? Well, we've got some challenges today, right? If we look at cyber crime, for example, it's estimated by 2021, cyber crime overall damages will total over $6 trillion.

Kirill: Whoa! Is that in just one year?

Matthew: Yeah, yeah, just in one year. Now, that’s up from about three trillion a couple of years ago. 2015, it was estimated about three trillion.

Kirill: Whoa!

Matthew: That includes not only the losses, but the recovery and everything else. World Economic Forum last year or actually, was it earlier this year, they estimated that by 2021, it could be one to two trillion. I'm sorry, 1% to 2% of GDP, of global GDP could be impacted by cyber crime.

Kirill: So, cyber crime. Wow! That's huge.

Matthew: That's massive.

Kirill: A lot of countries are not as large as that.

Matthew: Yeah. Exactly. In fact, they come up with their ratings every year, the top 10 things you need to worry about whether it be natural disasters or wars or whatnot. Cybersecurity-related issues hit three of the top 10,
took three spots of the top 10. The top one being number two, the number two spot.

Matthew: So, I mean, there's a lot of risk out there, and we're just scratching the surface, but again, it's relative to our insatiable desire to embrace digital technology, which is fantastic, right? We embrace that because of all the great benefits. It connects and enriches our lives. So, we want that, but we also have to be able to manage that risk, right? It's not eliminating it. It's finding that optimal level of risk, and that's really what cybersecurity in the future of cybersecurity is about is finding that optimal level and maintaining that right parity, so that we have that right level of risk and cost and impact or productivity issues, right? Finding that right balance.

Kirill: That's fantastic. I'd like to dig deeper into that because I watched one of your videos online, and you spoke about this, and really strike a core of me that balancing between preventing everything and cost. Could you explain a bit more? Why wouldn't you just go and aim, as an organization or as somebody who's representing the values and needs of consumers, why don't you go and aim to prevent everything, like put in safeguard mechanisms to prevent absolutely any kind of attack from any brand on the cyberspace?

Matthew: Oh, it's a great question. When I talk with executives and many times even boards, that question comes up, right? They want to know, "What do I need to do to get rid of all risks, to not be hacked or attacked?" The reality is it's almost impossible, right? Technology is constantly evolving. If you consider right now the
estimate, every year, there's over 100 billion lines of code written every single year.

Kirill: Wow!

Matthew: We also have estimates out of Carnegie Melon and a few other places on how many bugs are written in code, and it's somewhere between 10 and 25 per thousand lines, but even at that rate, you're talking about millions of vulnerabilities, just in software. We're not talking about hardware or wetware, right? We call people in the industry wetware, which really is the biggest area. So, technically, it would be impossible to eliminate all risks.

Matthew: More importantly, that would be wildly expensive to try and track down every single vulnerability, every single opportunity, and you're talking about intelligent, intelligent attackers. Cybersecurity is fundamentally different than information technology challenges.

Matthew: I'll give you an example. In IT and I worked in IT many years, most of the challenges there we consider as single-faceted threats. If, for example, you have a server and the power supply goes out on it, you know what you need to do. You need to go down to your data center and rip that old power supply out, put the new power supply in, start a backup, and you're up and running.

Matthew: In fact, it's scriptable. You can script that action, and based on data, you can determine how often you need to do that, right? You can do meantime before failure, and other statistics to have a predictive model to go in and do it ahead of time as part of preventative
maintenance. It is scriptable, it is easy. Once you're done, you're done.

Matthew: When you look at cybersecurity, you're talking about an intelligent threat, one that has its own motivations. It's a person. They have their own motivations, objectives, resources, plans. They're creative. This is a multi-faceted threat. They may attack your system and get in and start moving laterally. You may detect them and block them in one area. They're going to adapt to you. They're going to see what you did and try and get over, around, through. They're going to find the next path of least resistance. When you block them there, they're going to do it again, right? It is not a single-faceted threat, something breaks, I fix it and we're back to normal. It is an engagement like a soccer, right? One team against another. It anticipates the enemy, and it will maneuver around your defenses.

Matthew: So, our world is not static, and we have to take into account those behavioral aspects, which account for almost half of cybersecurity, right? You've got behavioral, technical, and a sliver of process between. We have to encompass all of that.

Kirill: I guess what makes it even more complex is often, these attackers don't follow a predictable incentive structure in the sense that they're not after, sometimes they're after making money or ransom, but a lot of the time, they just want to come in and destroy thing, which if we try to predict that, it's like, "Why?"

Matthew: Yeah, yeah. I'm actually part of a team, a threat agent group. It's a think tank. We've over the years mapped a
number of different what we call threat agent archetypes, right? If you think one of them being the cyber criminal, the organized cyber criminal, their motivation is personal financial gain. They have a certain number of resources. They're willing to break or bend the laws to a certain extent, right? We profile that one archetype, but then you've also got nation-states. You've got data miners. You've got all sorts, disgruntled employees. You've got all these different archetypes. Each one is different and different capabilities.

Matthew: No solution works perfectly across all of them or even for any one. So, for every organization out there, you have to, at first, understand who's primarily going to be coming after you, what are their methods, and now, how do you predict, prevent, detect, and respond to that, and then learn. It's a massive challenge.

Kirill: No. Totally agree. Before we dive in to solutions and the roles in cybersecurity, I'd like to ask you, if you don't mind, to share that example again that you shared at the start, before we started the podcast. Why I found it so valuable is because that example of how digital technology can differ and have a massive impact when it's on an aggregated level versus an individualized level or versus an application level, that example really puts into perspective how cybersecurity is relevant not only for organizations and enterprises, but also for the individual users and for absolutely any one of us, and how it can impact our lives. So, if you don't mind, please, could you share that example again?
Matthew: Yes. Absolutely. So, I'll give you a little background here. Data, really, is the lifeblood around cybersecurity. Right now, it's estimated that less than 10% of data that's being gathered about you, me or anything is actually being used for decisions. So, there's this 90% of the data that's being captured and stored. It's not being deleted. It's being stored.

Matthew: When we look forward, and we're seeing the tip of the iceberg now, artificial intelligence is really going to be one of those tools that will be able to look into that other 90% and start to tease out information, especially machine learning, deep learning. There's some great tools and technology and research in this area that's proving that it can go and do that.

Matthew: It's one of the actual big concerns that we have in cybersecurity when we look at the security and the privacy, and even the safety of digital systems moving forward. The example that I give is there's a difference between simple analysis, taking a database or a couple of databases and coming to a conclusion that could be beneficial versus aggregation of a whole bunch of those that might create a situation that is uncomfortable, and maybe a little more invasive than what we would want, and that could pose risks across that domain of cybersecurity.

Matthew: So, if we look at a single case, maybe a good case, traffic cameras or tracking people that are breaking or causing risks in traffic, if you combine databases from traffic cameras, maybe vehicle registration databases from the government and some facial recognition, and I'll pick on you, right? Traffic cameras may have
identified that you went through a red light last night. Maybe about midnight. They want to issue you a ticket or give you some training. Based on let's say the fuzzy pictures, the deep learning system could piece things together and get a partial license plate and tie that in, and maybe even tie in your vehicle body style and maybe a unique scratch on your bumper. Because of all of that, the algorithm comes up and says there's a 92% likelihood that you ran a red light last night, and we're going to send you a ticket or make you take some vehicle safety training. That would be a good thing, right?

Matthew: If we then take the case looking down the road, where that same type of analysis is done on multiple databases and then it's aggregated together, a different story might appear. So, if we looked at those same street cameras and maybe grocery store records and video, and medical history, social media posts, credit card transactions, home security devices, vehicle tracking, all those kinds of records, you might have a different story.

Matthew: Maybe that story would unfold to something like this. Maybe just before midnight, your home security system detected that you pulled out of our garage and closed the door behind you. Okay. A grocery store and your purchasing records indicate that you went to a nearby store, and you purchased chocolate, flowers, maybe some alcohol. The algorithm determined there's a 94% chance based on what you bought that you anticipated a romantic encounter. All right.
Matthew: Then if we look at the onboard vehicle records and maybe camera records, it also indicated that you were speeding on this rainy night, and that you ran that red light. Again, in the first example, it could also determine that, but it adds to the story, right? So, 92% likelihood that you were there, and maybe even a greater chance now.

Matthew: Onboard vehicle data and your phone data, your location data shows that you traveled precisely 4.3 miles, and you traveled to an apartment complex. Based on everything, and the speed, it indicated that there's a 94% chance that you were in a rush specifically to meet someone. That's interesting.

Matthew: Your social media accounts and public records indicate that your ex-girlfriend from a couple of years ago also lives in that complex. The algorithm may come back and say, "Ah! 83% chance you were intending to meet her." If we dig deeper, we see that she had just clocked out of work not too long beforehand. She took the public train home and she arrived within nine minutes of you showing up. Well, that increases the chance of that meetup to 96% non-coincidence. All right. The picture is getting a little clearer here.

Matthew: If we do an analysis over the tone, the timing, the wording of your last social, your text, your call data, it indicates that there's an 87% chance both you and her planned for a, let's say, carnal encounter based upon your health monitor, which was tracking your heart rate, your body temperature, your respiration and your
O2 levels. That activity probably did take place and it took about 14 minutes to complete.

Matthew: If we then turn the tables a little bit, and we go back in this algorithm, looks at her recent web search activity, let's say from earlier in the week, maybe she searched for an uncomfortable word, maybe a word like chlamydia in her browser, and then she subsequently visited a medical site, where she spent 27 minutes looking at diagnosis and treatment, and then shortly thereafter, scheduled a medical test with her primary care physician, which showed up on her digital calendar. That would indicate a 98% or let's say an 89% chance that she might have an STD.

Matthew: If we go back and look at your past shopping records, let's say over the past seven months, and it indicates that you haven't purchased any prophylactics, shame on you, that there's now, based on all the other information, a 66% chance you have now contracted a communicable disease.

Matthew: Now, that's interesting data. That's potentially powerful and valuable data, right? Drug companies might be interested in that data because they may want to sell you a solution. Your doctor would definitely want to know that, so he could provide a better level of care and interdict this before maybe even symptoms show up. Your insurance company would probably want to know that based on risks and what they want to charge you. Your employer and other employees may want to know that that condition is there and take appropriate measures.

Show Notes: [http://www.superdatascience.com/273](http://www.superdatascience.com/273)
Matthew: Your wife, if you have one, your wife probably would also want to know, and you may not want her to know, which gives certain leverage, especially to criminals that may want to extort that particular information. Interesting enough, you know who would also be interested? The tourist department of the country that you had planned to visit in a couple of weeks. You already bought the tickets. They may be interested. They may turn around and deny you access now to travel to their country because you have this condition.

Matthew: Now, this is all just grabbing information, doing the analysis, and aggregating it across. There is a huge difference between that simple analysis and that multi-faceted aggregation of analysis. The aggregation across these databases creates an entirely new narrative, and that could be hugely invasive, right? That undermines a lot of what we would consider private, but basically, it creates new data, new information from what is already out there. Now, that's a force multiplier of the data that already exists, and that could be tied to you forever in your life, in your digital life. So, all of that absolutely can impact safety, privacy, and security. That's what cybersecurity is. That's what I'm interested and so passionate about.

Kirill: That is just incredible, Matthew. I can't imagine that this is really the world that we live in. Sometimes you wake up and you don't think about these things, but it is the reality of things, and it's progressing really fast. So, what is the role of the cybersecurity strategist or the cybersecurity expert in all of this? How can you
prevent these things or how can you safeguard people from all of this transpiring just in the way you described it?

Matthew: Well, a cybersecurity strategist tends to look at the big picture, right? We tend to look forward. The past is interesting. The current has some value, but really, the value proposition of any good strategist is to look forward in time, so that you can see the risks, but you can also see the opportunities. So, that's part of my role is to be able to communicate, and highlight, and work with professionals in the industry, in academia, businesses, and even with governments, to help them understand what are the risk that they face in the future, and what are the opportunities to, again, find those optimal level of security or privacy, safety, things of that sort moving forward.

Matthew: Right now, in the example that we just gave, there's a lot of discussion in the industry about AI ethics because that plays a role. The data we just talked about, in individual databases, has tremendous positive value, but now, when you start aggregating it out, you do have those impacts for security, privacy, safety. You may not have the transparency. There may be bias involved. It may undermine equity and equality for people moving forward.

Matthew: So, the discussions right now are around AI ethics, what should be gathered, what should be stored, what should be aggregated, what should be anonymized, things of that sort. We're at a point that if we start working on that now, we can avoid a lot of those problems moving forward. That's really what
cybersecurity is about. Let's look at those threat agents. Let's see how they're changing and shifting. Where are they going to go? Are they going to invest more in ransomware or is that shifting and they're going to crypto mining next year? Those kinds of discussions, so that people can be more proactive, and even if they can't prevent problems, at least they can put in detective mechanisms that allow them to respond.

Matthew: The reality is you can’t protect against everything. It would just be too wildly expensive. There are scenarios that may have a very low chance of occurrence, but a very, very high impact if they do, right? We call them black swan events. In many cases, you don't want to try and protect against those. It's just far too expensive.

Kirill: Interesting.

Matthew: So, instead, you put in controls to quickly detect and respond to them, and that then becomes the optimal way.

Kirill: Maybe perhaps even minimize the impact.

Matthew: Yes. Impact is a result of two things, right? It's a result of the attack occurring on what damage, but it's also how fast you can respond to minimize the ongoing impacts because you have to look at the big picture. You really do.

Kirill: Got you. So, I guess in your example with aggregating all these datasets, the caveat there is that these datasets are not just publicly available to anybody,
and somebody would have to hack into each one of these storage facilities or organizations, whether it be the traffic cameras, the browser search history, your personal credit card purchases and things like that in order to put this whole story together. The more protection layers each one of these organizations has and the more diverse they are, I guess, that makes it more difficult for the hackers to put it all together.

Matthew: It does, but keep in mind, some of the data is for sale. You can buy it legitimately. You can do web searches. If you put my name in Google, you can see a whole bunch of information about me. I can do the same to you, right? It's open available. Other information, there are companies that specialize in building profiles about you, right? Maybe they pull in public records about if you've been arrested, things of that sort. You also have to understand there are huge numbers of data breeches out there. So, a single attacker doesn't have to breech all of these. It just has to be any attacker, anytime in the past, and that data tends to filter down to the dark web.

Matthew: So, you don't have to go hack it yourself. You can just go buy it or harvest it from an attack somebody else has previously done. Right now, the dark web, the very, very smart threat agents there, the cyber criminals there, they're already starting to aggregate the data, so that you can buy a profile. It's no longer the victim's email address, name and phone number, and maybe their national ID or Social Security number. It's now a whole profile about them that you
can start to buy. That's just going to get deeper and richer in the examples that we have.

Kirill: I always find it very interesting when I'm talking to somebody and we get into a conversation or I hear online dark web. Can you tell us a bit more? I'm sure you're probably one of probably the person I know who's most experienced in this space. Is it like a separate chain of websites? What is the dark web? What does it feel like? What does it look like?

Matthew: So, think of the regular internet that you and I see, the worldwide web. We interact with it in browsers, and we can Google search it, and it's very indexed. There is a whole another layer beneath that, if you will. It's less organized. It is not indexed on purpose. It is set up to where the participants can interact in a very private, anonymous way. There are legitimate things to do out there. You can purchase. There's stores and whatnot that you can do things with, but there's also a certain element where it attracts criminals and people that want to put illegal wares or products up for sale or services up for sale.

Matthew: You have to know how to get in there. It is not friendly for the average user to go into that domain, but it is vast because they can upload tremendous amounts of information without repercussion. So, there is a lot of information. Every data breach that you've seen more than likely, that information or a subset of it is residing in that dark web.

Kirill: Wow!
Matthew: So, you can purchase it, you can interact with it. It's a resource out there. It's just not a very visible resource to everyday people, but it's there. Chances are, it has some or a tremendous amount of your personal information that's out there.

Kirill: That's crazy. That's crazy. So, all of these hacks that we hear about like in ... What is it? In the 2017, there was an attack where three credit agents, three credit bureaus or agencies were ... Sorry. Equifax, one of the top three credit bureaus was hacked and there were 143 million information of US consumers were stolen. So, things like that would be available just lying around in the dark web. That's really insane that anybody can have a piece of that.

Matthew: Yeah. Last year alone, in 2018, there were over 6,000 significant data breeches.

Kirill: Wow!

Matthew: That included over five billion records. That's one year, one year.

Kirill: Five billion? That's insane.

Matthew: Five billion. Those are the ones that were reported. Now, if you can imagine if you're in a jurisdiction that doesn't require you to report, you're probably not going to. So, those are just the ones we know of. That number increases every year. The depth of data increases. So, the richness of the profile then increases, right?

Matthew: The Equifax had some financial information about people, but they combined it with the healthcare data

Show Notes: [http://www.superdatascience.com/273](http://www.superdatascience.com/273)
breeches, the massive ones from 2015. So, now, they've got your finances, and your credit ratings, and all of that combined with your healthcare records, your doctors, and what drugs, and treatments you've had, and so forth. So, again, it just starts to aggregate and build a better, stronger, more detailed profile about you.

Kirill: That's insane. Then there's a hotel last year. I think it was Marriott.

Matthew: Yes. That was another massive data breech.

Kirill: 500 million guests' data. That's insane.

Matthew: Their passport information, yes.

Kirill: What is going on? Is it just that companies don't have the right cybersecurity measures in place or are these hackers just becoming much smarter than what we are capable of protecting now?

Matthew: So, there's a number of different factors here. First of, the number of hackers are going up, the number of technologies that we're embracing. Therefore, the amount of vulnerabilities is also going up. Many of these companies actually have good security, but there's always a way in. Depending on that threat agent and how dedicated they are, they will find a way in at some point.

Matthew: Now, you can put security controls to be able to detect that quickly, to be able to limit it or compartmentalize them in some cases, but you even look at some of the data breeches, the NSA, the CIA, some of the top
security organizations in the planet have had data breeches.

Kirill: Yeah, the irony.

Matthew: So, it's very difficult to protect against everyone all the time. So, it's not saying that these companies are completely off the rails and they're not doing anything. Many of these companies do have good security, but you have to stay at the forefront. You have to be thinking about the next attack, not what happened yesterday. I would say most companies right now are looking in the historical record to see what they need to protect against, and they're not looking forward because that's what you really need to do.

Matthew: So, it's challenging. It is not easy, and it's expensive. It's difficult. There's not very many resources. You don't have enough cybersecurity professionals even if you did have the budget to go out and hire. They just don't exist. Estimates right now and the next couple of years is there will be up to three million unfulfilled cybersecurity positions.

Kirill: Wow! That's crazy.

Matthew: We just don't have the people or the talent.

Kirill: That is crazy.

Matthew: So, it's tough. It is very tough.

Kirill: I guess that explains why you have a whole calendar for where you're speaking and a whole list. That's why you're in so much demand.

Show Notes: http://www.superdatascience.com/273
Matthew: Yes. There is a demand. There's lots of demand. For those people who are interested, especially in the data science industry, data is the lifeblood of cybersecurity, and we're seeing this great intersection between the data sciences and analysis and cybersecurity. So, there are wonderful opportunities coming up, especially if people have a passion of doing forensics or figuring out what type of threats or risks or trying to tease out an attack out of a flood of data, right? Find the single needle that you're looking for out of a stack of needles. That's really what data analysis is, and we're seeing great leaps forward both on the defensive side, in detecting things, but also on the attacker's side. We're seeing the threats actually use data science and artificial intelligence, and everything else.

Kirill: Are you suggesting our data scientists go to the dark web?

Matthew: No, no, no, no. We don't want them to go to the dark side. I need them on the good side. I need them all to be white hats. We just don't have people, but also understand that the very tools that are being used for good, they're also being used for harm and maliciousness. So, there becomes a battle there as well. Very soon, we're going to start having intelligent agents and bots and AI algorithms trying to detect the bad algorithms. So, it's a constant evolution in this. It's very, very exciting.

Kirill: I totally agree with you. Let's expand a bit more on that. So, I love your quote, "Data is the lifeblood of cybersecurity." Tell us a bit about what kind of roles exist for data scientists. For instance, people listening
to this podcast who never considered a career path in cybersecurity and after hearing how passionate you are about it, they want to explore it further, how would you describe what roles exist there in cybersecurity?

Matthew: There's so many different opportunities. So, for example, looking at information, let's say you have a large company and you have assets, you're constantly being bombarded by attacks. You're being bombarded in your network. People are trying to get through your firewalls, people sending phishing attacks through emails or texts or even phone calls or video chats, right? There are all sorts of different attacks that can come through. It's all bits and bytes.

Matthew: Being able to develop systems that can identify what is good data versus bad data, what is somebody trying to make an attack and compromise versus somebody just trying to get work done. There's lots of work in the industry trying to determine certain baselines of, "Okay. This type of activity by our employees is good. It's safe. It's normal. Whereas this type of activity may be abnormal, and we need to go look at it." Again, we're pretty chaotic. That type of technology has not been perfected. We're nowhere even close because we all do something different.

Matthew: Do you search exactly the same webpages everyday? Do you log on exactly the same time, use the same tools, type the same words into your word browser? No. We are constantly changing, and adapting, and integrating new technologies and ideas. Again, data scientists around that, hugely valuable. That goes for
not only within an organization, but it also goes for security companies.

Matthew: You've got, especially around artificial intelligence, you've got systems that are looking to detect deep fakes, fake videos or audio or fake texting, chat bots, all sorts of things, right? Again, it's a matter of pulling in data, trying to understand, "Is this real or is it synthetic?" There's an entire industry about trust because right now, you're trusting it's me on the phone, right? It really may not be in a few years. It could be my agent, my AI agent doing this, so that I could be talking to five or six different people simultaneously while I'm having a margarita out on my patio, right?

Matthew: So, you've got areas like that. You've got that massive, massive amount of data in these data lakes, oceans, really, that people and companies want to be able to tease out value, but there's potential security and ethical and security risks that we have to worry about.

Matthew: If we look at, for example, let's look at the automotive industry, right? I mean, the automotive industry by next year, they estimate about 90% of the cars will be online, not autonomous, but at least be connected. We're going to see autonomous cars come in after that.

Kirill: That's new cars probably.

Matthew: Yeah. The data itself, when you look at autonomous cars, autonomous cars will create about 4,000 gigabytes of data, each car everyday.

Kirill: Wow!
Matthew: 4,000 gigabytes. That data has value. It also has potential risks. So, again, looking at all that and in data science, how do you figure out what is good, what is potentially bad. If you're talking about that, you're talking cybersecurity. So, in every aspect of cybersecurity, there will be a role, a job, a need for somebody who has the capability to do an analysis on vast amounts of unstructured data to figure out if there's something wrong or if we need to go fix something or dress something or if there's a risk that nobody yet knows about that we need to interdict now before something bad happens in every aspect of technology.

Kirill: Totally. Totally. I got your point. I want just to comment on the whole deep fake situation. I recently heard an audio on YouTube where they got Joe Rogan, the famous podcaster. Have you seen this one, Matthew?

Matthew: Yes.

Kirill: They faked his voice as if he's talking about a hockey team made out of chimps. It's just super funny. It really sounds like him or the other one where they put Elon Musk's face on a baby. That was a funny one as well. Yeah. So, there's definitely some interesting ... I agree with you that anywhere that there's data being used especially in digital space, there is a room for cybersecurity. I guess the next question from here would be, what's the first step? For somebody who's not in the cybersecurity space already, and they understand the value of cybersecurity, understand that wherever there's data, wherever there's digital,
there is or there should be cybersecurity to some extent, what is the first step for their career and for them getting more involved in this space or learning more about it or getting the right skills or understanding the tools and slowly venturing and exploring the space of cybersecurity?

Matthew: Well, the first thing is to understand that the core skills for data analysis, they're hugely important. So, you have to continue to progress down that path, and always learn more, expand your skills, the new technologies, the new engines, the new algorithms, all those kinds of things. You still want to have that. Keep that passion alive because it's really about applying that to a particular field.

Matthew: Now, when it comes to cybersecurity, again, there are just so many different areas. The next step, really, is to find your passion if there's something particular you're really interested in. Let's say your home systems got hacked and you want to figure out how to stop that or detect when there's network attacks. Great. Start doing some research about that. Look at the companies that are working in that space and you're going to find opportunities. Connect with people in that role.

Matthew: Let's say you're interested more in digital forensics, and figuring out, "Okay. What happened for fraud or for theft or something like that?" Again, identify those roles, connect with those people, connect with those organizations, follow those thought leaders in that space because there's a whole culture that's emerging out of there that you can participate in and leverage.

Show Notes: [http://www.superdatascience.com/273](http://www.superdatascience.com/273)
Matthew: Another example would be the crime sprees that are going on or the attacks or IoT. Right now, industrial internet of things are just regular internet of things. That industry is blossoming. Some estimates put the total number of IoT and IIoT devices to be over 100 billion just by next year. Again, that's creating a tremendous amount of data and a tremendous opportunity for attackers.

Matthew: So, again, find your passion in the cybersecurity space, whatever it is, whatever sounds interesting to you. All you're going to have to do is dig a little bit and you're going to find how the understanding and analysis of data will help push forward that industry. Connect with those thought leaders, follow them, and interact because, again, in our industry, the security professionals out there realized that there just aren't enough people that are coming up to take over for cybersecurity.

Matthew: So, the thought leaders in our industry probably more than most, we work with people that have questions, that are interested. Connect with me via LinkedIn. I get connections and questions all the time, but I'm happy to answer them because we want to help that next generation who are going to inherit these cybersecurity problems. I want to help groom that next generation of cybersecurity professionals out there. So, you will find when you connect and follow people in areas that you're interested in in cybersec, they will work with you. So, don't be hesitant, don't be shy.

Kirill: Love that advice. Fantastic. I totally admire your passion to, as you said, help the next generation that
are going to be faced with this problem. Is there any portal or what are the best materials that you share that people can or specifically some of your maybe lectures or maybe your presentations, any articles or anything else that is best to get started with to understand better your advice in this space?

Matthew: The best thing is probably to follow me on LinkedIn. You can look at my profile. I try and post almost all the presentations that I do out there. I’m prolific in talking about different industry events and why they’re relevant not only today, but especially for tomorrow. I’ve got a good following. I think it’s about 190,000 professional followers in LinkedIn. About 10% are actually C-level or higher, so the C-suite as well as boards and owners of companies. The next, I want to say 40 something percent, tends to be management, but I’ve got a huge range of people.

Matthew: Go out there, take a look at the videos, at the blogs, and more importantly, chime in, right? If there’s a comment out there that you find interesting or you have a question, jump in to the conversation. Comment, post your questions, and whether I respond or somebody else in the industry responds, you’re building those connections and you’re getting insights, not just my insights, but insights of the entire community that I’m a part of, and that’s tremendously valuable.

Kirill: That’s another way to further grow your network. You post comments, somebody will post a comment, and then you guys have a similar interest, and then you connect with them.

Show Notes: http://www.superdatascience.com/273
Matthew: Yes. Absolutely. It's not just the public comments. I get a lot of comments through LinkedIn's instant messaging or email. So, you don't even see them online. So, I collaborate with industry professionals all over the world about all sorts of different topics. We have to. We have to work together. The challenges we face are so almost insurmountable that we have to communicate, we have to collaborate. The bad guys do it, right? We have to as security professionals do it. Otherwise, we won't move forward fast enough. We won't maintain parity in the pace and innovation of the attackers. So, we have to, and we know this. All the top security professionals out there know it and we all work together.

Matthew: So, join that community, right? I'm on LinkedIn, medium, blogger, Twitter. I post most of the stuff to LinkedIn, but you can also Google search me, but don't just limit it to me. Find the professionals in the cybersecurity industry that you're most interested in. The topics that they discuss and areas that they work in, follow them. You may not like what I talk about. Great. Follow somebody else, and work and communicate with them.

Kirill: Yeah. Totally agree. I also find that for some reason, LinkedIn in a space like data science for you in the space of cybersecurity works really well. I think people love connecting on a professional level and like seeing things that you post, the things that you share and you're expanding an effort. So, I highly encourage everybody as well to see that LinkedIn as a great place
to connect with people like Matthew and others in the cybersecurity space as well.

Kirill: I guess, well, another thing I want to talk to you is, any good books that you can recommend on cybersecurity? For somebody who's really interested in learning more about this topic, what is a book that they can pick up and get a feel for it?

Matthew: Well, I'll tell you my favorite book. This is going to be a little odd, right? Keep in mind, a strategist, right? You're talking to a strategist. I'm looking forward. The book that I found most relevant, and you're going to laugh, because it has nothing to do with digital technology, is actually The Art of War by Sun Tzu.

Kirill: Wow! That is awesome.

Matthew: It is. Here's why. Let me justify that explanation, right?

Kirill: You really take your job seriously.

Matthew: I do.

Kirill: Commander Matthew.

Matthew: Right. Sun Tzu was a master strategist, right? Two and a half millennia ago, he created this series of advice, military advice, but this book, it's a classic tome, and it's still relevant today. In fact, it's taught in every major business class, in military warfare, even sports, in any adversarial type of endeavor because it looks at many different factors. It doesn't just look at the technology of the day. It looked at the people behind the technology. It looked at the attackers and the
defenders. It looked at their mental states. It looked at taking advantage of the environment.

Matthew: Back in the day, 2,600 years ago, they didn’t have digital technology, but all those same ideas and concepts, amazingly enough, they are relevant today. They are relevant when we look at the attackers and look at their motivations. How do we undermine their confidence? How do we evaluate what capabilities that they have? What is their path of least resistance? Where are they going to maneuver to? How can we find an optimal way of defense or potentially even offense? So, Sun Tzu did a great job, and there’s many different interpretations and follow-ons to his work, but The Art of War, very much applies to the art of digital war.

Kirill: I think I understand now what comes together in the sense that we’re ... Because cybersecurity is one of those spaces where you can just learn certain principles and just follow them or certain frameworks, methodologies, get good at them and you’ll complete the job to a very good level of satisfaction and get good results. It’s so undetermined as you repeatedly mentioned on this podcast. We don’t know where we’re going to the next year, let alone decade. We don’t know what’s going to be happening next year in terms of how this intelligent opponent is going to react, what they’re going to do, what things they’re going to be looking at.

Kirill: So, for somebody to be successful, like super successful as a cybersecurity expert, it’s not enough for them to just be told what to do and do what they have to, as in your example, have to be a strategist.

Show Notes: http://www.superdatascience.com/273
They have to be a commander, decide what the organization is going to look at, what threats they're going to cover, what threats they're not going to cover, how they're going to flank the opponents, and so on. So, it all adds up that you have paired a book on this topic is Sun Tzu's Art of War. It's just brilliant when you look at it that way. So, big kudos for sharing that. I think that's a great idea for people to read.

Matthew: You can never underestimate the impact of the behaviors when it comes to cybersecurity. In the origins, every attack starts with a person. It's a person. They may be writing malware. They may be doing something. At the other end of the spectrum of that story, there's always a victim, and that victim is human as well. So, the playing field is technology, and a lot of people only focus on that. It's a crucial piece, but you also have to integrate the human factor. If you don't, you're going to fail.

Kirill: Love it. love it. Matthew, I guess final question. Are we going to win this war?

Matthew: It's not about winning or losing, right? It's about finding that optimal balance. We don't want to impede technology because technology is awesome, right? Again, it connects and enables the world. It enriches our lives. So, we don't want to stifle that, but at the same time, we don't want to be overly victimized.

Matthew: So, it's about finding and maintaining that optimal balance of risk, and that's really what we need to go to. We're not there yet. We're not even keeping pace with the attackers yet, but we're improving. We are much
better off than we were a year ago or five years ago, and we're trending better.

Matthew: So, the gap is not close. The attackers definitely have the advantage. We're going to see a lot more victimization in the next few years. It's going to not be pleasant, but security and cybersecurity is evolving. I think if we all work together and we have brilliant minds, especially like data scientists, that gives us an important step forward. So, are we going to win? I don't think it's ever a win-loss game. We need to find that right level and maintain it. That's really the goal.

Kirill: Fantastic. Well, on that note, Matthew, thank you so much for coming and joining me on this podcast. I'm sure thousands of people are going to see value in this, and hopefully, going to incorporate some level of cybersecurity practice in their data science careers. Once again, thank you so much.

Matthew: Thank you. It's truly been a pleasure. It's a great conversation.

Kirill: Thank you so much, ladies and gentlemen, for being on the podcast today, for sharing this time with Matthew and me. I hope you enjoyed today's episode. So much knowledge. Matthew shared so many valuable tips, insights, and experiences, examples from his career. I am extremely grateful for him coming on the show.

Kirill: What a surprise that it should be a cybersecurity strategy or as a successful cybersecurity strategist, he actually thinks of cybersecurity the same way that Sun Tzu thought about war. That was mind-blowing.

Show Notes: http://www.superdatascience.com/273
for me, personally. I think it totally makes sense. It's very exciting to hear that the space of cybersecurity is such an interesting field to be in. I highly encourage you, the listener, to see how you can incorporate even a little bit of cybersecurity, even if you're not going to go head in, full on into cybersecurity, which you might after this podcast, but even if you want to incorporate a little bit in your career as a data scientist, as a machine learning expert, as an AI expert or AI architect, it's going to be very valuable for your career because with how ubiquitous data is, cybersecurity is going to become more and more important and not only will you become more valuable to employers and companies, but also, you will actually be able to do more good for the world and make sure that the creations that you come up with are protected and are safe for people to use.

Kirill: So, that was Matthew Rosenquist. You can find the show notes for this episode at www.SuperDataScience.com/273. That's SuperDataScience.com/273. There you'll find all the links, all the materials that we've mentioned in this episode. Also, you'll find Matthew's LinkedIn there, the URL to his LinkedIn. Make sure to follow Matthew on LinkedIn. He's got 180,000+ followers. He must be doing something right and sharing really valuable content. You don't want to miss out on that. So, follow Matthew.

Kirill: If you enjoyed this podcast, share the love. Spread the word about cybersecurity. Send this link, SuperDataScience.com/273, to somebody you know

Show Notes: http://www.superdatascience.com/273
who's interested in cybersecurity, who's in this space or simply who is passionate about data or data science because cybersecurity comes hand-in-hand with data.

Kirill: On that note, I will leave you with that, and thank you so much for being here today. I look forward to seeing you back here next time. Until then, happy analyzing.