#214 - Deceive to Detect with (Yuriy Gatupov)

[00:00:00] **G Mark Hardy:** Hey, have you ever been deceived by somebody? How did that make you feel? what if you can do that to the bad guys? We're going to show you how you can go ahead and build deception into your enterprise to help protect you using some amazing technology and a very special guest. Stay tuned.

[00:00:25] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft. The podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy and I'll be your host today, while we continue to explore cutting edge security strategies with industry leaders. Today we're going to dive into a topic that's revolutionizing how we think about threat detection, cyber deception technology.

Now in our world of increasing cyber threats, we face a fundamental challenge. Defenders need to be right 100 percent of the time, while attackers only need to be lucky once. But what if we could change [00:01:00] that equation? What if we could shift the balance of power back to the defenders? Today, we're going to explore how deception technology is transforming from a niche solution into a mainstream security strategy.

We'll discuss how organizations can use it to detect threats earlier, understand attacker behaviors better, and significantly reduce dwell time. All while decreasing operational costs and false positives. But momently, we're going to hear from our sponsor. Do zero day exploits and supply chain attacks keep you up at night?

Worry no more. Harden your security with ThreatLocker. Worldwide companies trust ThreatLocker to secure their data and keep their business operations moving. ThreatLocker takes a deny by default approach to cybersecurity and provides a full audit of every action, allowed or blocked, for risk management and compliance.

Onboarding an operation is fully supported by the U. S. based Cyber Hero Support Team. Get a free 30 day trial and see how [00:02:00] ThreatLocker can

help prevent ransomware and ensure compliance. Visit ThreatLocker. com. Now, we covered cyber deception with Kevin Fiscus back on episode number 43 in August of 2011.

And we brought Kevin back on episode number 127, How to Stop Bad Guys from Staying on Your Network, in May of 2023. Today, I've got a new guest who's going to show us even more about what we can do to use deception technology as a critical component of modern security architecture. Yuri Gatapov, welcome to the show.

[00:02:34] **Yuriy Gatupov:** Thank you, Mark. And, yeah, I hope it's going to be interesting conversation, for your audience. you are free to ask any questions you wish. I will share my knowledge, my experience, and, thank you.

[00:02:50] **G Mark Hardy:** So if we've got our expert here, so let me do a little bit of background on deception because traditional security has always been a game of catch up. We'll build walls, [00:03:00] attackers will find ways over them. We deploy intrusion detection and they'll try to blend in with normal traffic. We implement endpoint protection and end up using fileless malware.

This reactive cycle. has led to an increasingly complex and expensive security stack that still leaves organizations vulnerable. Now, active defense represents a fundamental shift in this paradigm. Instead of just watching and waiting, you can now take control of your attack surface. You can create environments where you can dictate the terms of engagement with potential threats.

And this proactive approach is particularly crucial given today's regulatory landscape. With new breach notification laws that propose even higher penalties, significant fines, possibly even jail time, The stakes for missing an attack have never been higher. But what makes deception technology different from our traditional security tools?

Think about how we typically detect threats. We look for known bad signatures. We monitor for unusual behavior. We track anomalies in our data. And all of these methods generate massive [00:04:00] amounts of data and alerts, many of which turn out to be false positives. Security teams spend countless hours chasing down alerts, That often lead nowhere.

Deception technology is going to flip this model on its head. Instead of trying to spot the needle in the haystack, it creates an entirely separate controlled environment that legitimate users have no reason to access. When someone

interacts with a deception asset, you know with near certainty that they're malicious.

It's like having a security camera trained on a fake vault in your bank. Anyone trying to open it, it's clearly up to no good. But modern deception goes far beyond simple honeypots. Today's solutions will create elaborate illusions, complete mirror images of your real infrastructure that appear vulnerable, at least to attackers.

And these environments include everything from fake employee credentials to simulated industrial control systems. They're designed to be indistinguishable from your real assets, but with one crucial difference. They're completely instrumented for detection and analysis. Now, this approach is offers several unique [00:05:00] advantages.

First, it drastically reduces false positives. Since legitimate users should never interact with deception assets, any activity is highly suspicious. Secondly, it provides unprecedented visibility into attacker behavior. When a threat engages with a deception asset, security teams can observe their tactics, tools, objectives in detail.

They don't know that they're being watched, and this intelligence is invaluable for strengthening your overall security posture. But perhaps most importantly, deception technology helps address one of the most challenging aspects of security, detecting unknown threats. Traditional security tools rely heavily on known signatures or behavior patterns, but deception works regardless of the attack method.

Whether it's a zero day exploit, a sophisticated APT, or an insider threat, if they interact with the deception environment, they're detected. Now, this technology is particularly effective at catching attacks during the critical reconnaissance phase. When attackers first breach a [00:06:00] network, they need to understand the environment.

Mapping out systems, looking for valuable targets, seeking paths to those targets. Deception technology turns this necessary step against them using their own curiosity and methodical approach as a detection mechanism. This capability to detect threats early in the kill change is transformative.

Industry data shows that some attackers can often spend months inside networks before being detected. During this dwell time, they're free to explore, expand their access, and exfiltrate data. Deception technology can dramatically reduce

this window of opportunity, catching attackers before they can do significant damage.

And the economics are compelling as well. Unlike traditional security tools that require constant updates, signature management, and fine tuning, deception platforms are relatively low maintenance. They don't generate the massive data volumes that need storage and analysis, and they don't require large teams of specialists to manage them effectively.

Now, as we move into a conversation with our guests, keep in mind how [00:07:00] this technology fits into the broader evolution of cybersecurity. We're moving from a model of building higher walls to one of strategic control, where we can actually shape how attackers perceive. and interact with our environments.

Quick word though, CISO Tradecraft is partnering with CruiseCon for a cybersecurity conference that's held during a luxury cruise. Now, usually events like this are reserved for Fortune 100 CISOs, but we've worked a deal for CISO Tradecraft listeners, so you can join us on the Royal Caribbean Voyager of the Seas from February 8th to the 13th, 2025.

Admiral Mike Rogers, former director of the NSA, is the keynote, as well as a number of great speakers. If you want to beat the cold while doing some valuable networking, Head over to cruisecon. com and use the code CISOTRADECRAFT10 for a 10 percent discount to the exclusive event. And so now finally, Yuri, welcome to the show.

Yuri is a co founder of Labyrinth Security Solutions, a company that's pushing the boundaries of what's possible with deception [00:08:00] technology. And Yuri brings years of experience in this field and has helped numerous organizations. implement successful deception strategies. So let me start with a question.

First of all, what motivated you to focus on deception technology?

[00:08:17] **Yuriy Gatupov:** actually the story started five years ago in 2019. I was doing the, cybersecurity at that time also, but from the commercial perspective, yeah. Involved on many projects of, implementing, different cybersecurity solutions. And, that time I met two guys, two engineers to Let's say now, nowadays, you call them not Pentesters, but Red Teamers, but that doesn't change the situation.

Yeah. and they were working on the MVP and, their idea was very simple. So we want to, create the solution that the product, the technology, which we, as the [00:09:00] Pentester, as the Red Teamers will not be able to bypass. So what's going to be the efficient tool to catch me every time? Yeah, because for every antivirus rules, I have wrapper, I have the new technology, new techniques and etc.

So anytime they were doing their job, they found the way to screw up the security stack of the customer. So when the idea was set up. The idea behind it was very simple, what's going to be efficient and not complicate your life, not guessing yes, not probably, maybe, yeah, and efficient enough to catch them.

So when they present the idea to me, I just, my experience was, sometimes you have the project where the implementation is like year long. And it's quite normal, yeah, but you start paying money the first year of subscription, you are still in implementation [00:10:00] phase. And nowadays the situation is the same for many products, yeah?

So your value is you don't even understand when you start to receive. So for me, the idea was brilliant and I started working on it.

[00:10:18] **G Mark Hardy:** interesting. Now, you'd mentioned, for example, antivirus, and in the past, what a sophisticated attacker would do is they would purchase or borrow, so to speak, copies of detection tools, and they would tune and tweak and modify their payload until it would get past all the commercial versions that were likely in use, at which point they would then introduce that into the environment and companies that were relying upon these either signature based or behavioral based tools, the attackers had already tested all of their tools against those defenses. But now what we're talking about is something completely different, which is instead of matching up to a known set [00:11:00] of bad tools, content or behavior, you're going to change the perception of the attacker.

And the idea is that instead of just simply trying to watch them do bad things to your system, you're going to present to them something that looks quite interesting that they're going to say, Hey, let's potentially attack that first or look at it. At points, you've got them. as I was going through your literature on labyrinth security, you have something called points.

what, how do the points work? And if you were explaining to somebody.

[00:11:32] **Yuriy Gatupov:** To simplify, basically this is the imitation of the vulnerable system and as you mentioned we don't want to just mirroring the existing infrastructure of the customer. Our goal is to present the vulnerable services to the, attacker. So point is that you can call it decoy, honeypot, a lot of different things, but the essence is that this is the vulnerable service presented in the network.[00:12:00]

in our case, it's always usually active one. Yeah, it's not like a passive stuff. We also like to generate some traffic, some noise, to be, seen alive. And, The main idea is to attract and keep, yeah. So detect and keep busy with the service. So besides that, the point is, Honeypot, it's also high interaction. Means that, you are not able to recognize that you are playing with it, with, imitation. Yeah. So from the first match, you will never get the white screen. Yeah. If you send the comment, you will get the proper response. And, we can keep, that guys busy for many, hours. It's like improving with our customers, in some cases.

Yeah, I will, describe them later. but the main idea is the point is the, [00:13:00] attractive imitation. We're supposed to attract and detect and collect the information. About the activity of the bad guys in the corporate network.

[00:13:10] **G Mark Hardy:** Now, when a bad guy first lands in an enterprise or an environment, they're going to potentially look around. Now, doing port scans is noisy. And it often gives you away. And so I thought I heard you say that you will actually have your Devices, your decoy devices generating their own traffic that potentially could be sniffed.

which then looks a lot more like a real device if it's actually communicating with others. Because if I'm passively watching traffic, I'm going to look to where the nodes are. Where is everybody talking to? Those are probably the things of interest. And is that the basic approach behind how you initially create some of that interest in a target, rather than simply say, here's an Excel spreadsheet sitting in the root network directory of the, HR department.

[00:14:00] So

[00:14:01] **Yuriy Gatupov:** you are right because there are like many scenarios and sometimes adversary can be very, quiet. try, to be not noticed and, not instead of coming, yeah, start listening. Yeah, so we have the special type of points, to detect such a, let's say, man in the middle type of the attack, yeah, when it's like a listener deployed in the network.

And, also we cover the endpoint as well, that endpoint is the source of all the, troubles, yeah, in the network. So usually everything is started from the initial access to the endpoint. so we also provide the breadcrumbs. we call them like, we call the agent, cedar agent, which we deploy on the end point.

And we provide the breadcrumbs, also start to attract, the adversary from the very beginning. [00:15:00] That breadcrumbs, it's some artifacts which you expect to find on the machine when you start, learning the, what you have in hand already. So it could be like some. Passports, in plain text, some keys from, the station and whatsoever.

And if the adversary decided, okay, I, know how to escalate my privileges. I know how to, get, to SSH server or whatsoever and try to use these artifacts. We will immediately direct them to the points. Where we can make a detection and keep them busy with our points. That's an additional layer of protection, which we also provide to our users.

[00:15:48] **G Mark Hardy:** breadcrumbs then are not too overt. They're not like a big sign saying, go here, look here, free food or something. But the normal expected artifacts that if I [00:16:00] were an intruder, I would say, Hey, that looks about right. Or I would, that falls within the realm of what. An attacker would expect to see. So you're not raising any suspicion and there's some wisdom in that.

So could you walk us through a typical attack scenario as you'd started? And then at what point does your detection actually take place? And then what should happen once a detection is made? Do you kick them out right away? Do you sit back and watch? Do you call law enforcement? what's the best way to go about using these types of technologies?

[00:16:37] **Yuriy Gatupov:** So basically there are like plenty of these scenarios. Yeah. And, The best case scenario for us, if, we catch them on the endpoints, yeah, from the very beginning of the journey, yeah, as we mentioned that we put this artifacts and it's not like something, very outstanding from the rest, of the stuff on the, on, on, the machine.[00:17:00]

And by the way, it's, customizable. You can customize, change the language, change the, I don't know, like the order of domain names and whatsoever. So you can do it. We provide the ability for the customers to blend it, to your real infrastructure, our solution as much as possible to be not visible. So this is the best case scenario.

So if the guy is It's trying to use one of these artifacts, which we placed like 50, 100 of them, not on the, visible places. Yeah. But if they know where to look, we know where they are going to look to, for this stuff. So we provide this stuff. That's the best case scenario. sometimes it's not the case and, so for example, if the adversary have, has the access to, credentials, like with stolen or sold credentials, [00:18:00] and they start, learn the infrastructure.

So here I have also like several scenarios. Sometimes they are going directly to Active Directory, sometimes they try to find DNS, sometimes they know that, okay, let, me check what you have on the web, yeah, based on the web, web console or whatsoever, depends on your skills, yeah, and depends on what you have in your hands to, to compromise the infrastructure, to elevate your privileges, yeah, let's say in the system, we are covering pretty much all of the cases.

So you can be quiet and deploy the listener, our, decoys, our points will generate this, net bias, request, like all the traffic we have points would generate traffic outside of the network as well. So you can set up. Okay. So please. go to cnn. com and, yeah, pretend to check the news.

Yeah, so it's like normal [00:19:00] behavior during the day. Now you decided, okay, my work is too boring. Let's go to check, what is going on. Yeah. you can set up where this decoy will, establish their connections. So when the guy, they observe the network, they say, okay, that's the, real stuff, the lifestyle.

And when he sketched the next. would say big task for us and, what we see is, additional value, which can be, by the way, provided, in my opinion, as of my knowledge, can be provided only by deception by properly done deception. This is this part we call it engagement. So after detection, we also engage or involve, you can call it any way.

But the main idea is after detection, we'll also mislead the adversary and keep them busy. playing with our imitations. And keeping them away from the real assets. And this is very [00:20:00] important, especially for the infrastructure, where you don't have 24x7, security operation team. Or even if you have it, yeah, but the team can be busy.

And people, they sometimes they sick. they need some rest during the night. They need to go to vacation, weekends, whatsoever. And it's only in a spy movie, like someone start, reacting, okay. I have the alarm in my, console. Everybody starts reaction. Probably.

[00:20:29] **G Mark Hardy:** it's always in 72

point font

[00:20:31] **Yuriy Gatupov:** yeah, yes, exactly.

[00:20:33] **G Mark Hardy:** big alert or something.

[00:20:35] **Yuriy Gatupov:** In normal life, yeah, everybody will say it doesn't look like this. And look at this statistic. What's the shortage of qualified, employees in cyber security? Millions. I don't believe there is any infrastructure, probably except for, I don't know, some Pentagon or CIA, they have enough people and resources.

I'm not sure, but I cannot judge. But I [00:21:00] never seen an enterprise that everybody is happy and have 100 percent stuff. Always, if I ask this question, people say, nobody, raise hand. Yeah, I have, even extra people. It doesn't work this way. So to win this time is crucial because this is the time you are on the safe side and this is the time, between the actual incident start and your reaction start.

And this time could be very, crucial.

[00:21:26] **G Mark Hardy:** So here's a question. If I am positioning deception assets and breadcrumbs, if you will, an attacker lands on a platform. They haven't done anything yet, so they're still not detected. What is to make, prevent them from maybe guessing, say, Hey, I'm going to pick this. It's real. And they never touch your breadcrumb. How do you make sure that yours is either more compelling or gets caught up?

Because it would seem to me that it's a matter of, okay, pick a hand. This has deception. This does not. But if I pick the one that does not have deception, I still haven't [00:22:00] detected them. And until they bump into one of these. So how do I try to get my attackers sooner? To trigger one of my alerts.

[00:22:11] **Yuriy Gatupov:** Yeah, it's a good question, because in my opinion, 100 percent prevention and 100 percent detection is not possible. Okay. And I cannot tell you, yeah, so we will be 100 percent sure that among the other artifacts on your machine. in the nursery we'll choose, our breadcrumbs because of what?

We just provide, what they're looking for. And sometimes, yeah, you are right, there is a choice. Because, there's some, real SSH key could be also on your machine, yeah? Or some, login and password in the plain text. We cannot, ensure that, among all that's, choices, they will, choose, exactly the, [00:23:00] breadcrumbs to be catched.

But this is the only first LA layer of protection because even if they choose something, real, yeah. So they start the journey in the infrastructure they have a lot of decoys, across. And, you told them the very beginning that this is the, shift of the paradigm. Yeah. Now, because nowadays, if you are CISO, you are on the defense side, one mistake and you're done.

You can do your job, for years perfectly, but one mistake and this is it. the adversary, they have, endless, amount of their attempts to try, and try. There is no, you, there is no countermeasure. You cannot stop them. you cannot prevent people from Russia or China or North Korea, trying to do it again, and again.

Not possible. Okay. and they [00:24:00] have also, when they're inside, they have plenty of choices and plenty of attempts, like to do something before they will be catched. But we want to change it. One mistake and you've done. One touch to the decoy, you've done. So all your strategy, like you can be very quiet, very conscious, like whatever you're doing.

But. One, one mistake. So now the game will be the same for the adversaries. I don't have endless, attempts. try to find a way to, penetrate your network. Yeah. And, to find a way how to escalate my, privileges and, move across. No. 1, 1, 1 mistake. This is it.

[00:24:43] **G Mark Hardy:** Got it. Now, I, first of all, I appreciate your honesty. Most of it, most vendors will come and say, Oh, we're perfect. We catch everything. and you're being realistic. Of course it does take time. thank you for that. But also how long, let's say an organization were to say. [00:25:00] Okay, I'm convinced. I want to go ahead and do this.

How quickly will an organization start to see value after deploying these types of deception solutions?

[00:25:12] **Yuriy Gatupov:** That's good question. the, answer will be a little long. sometimes we are lucky it. The la last example in Uzbekistan, that's, big enterprise in Uzbekistan. We started the POC and then two weeks, they asked about another. call And, you're wondering, okay, so probably there's some Q&

A session, some technical questions, but they asked about the price and they are ready to buy it.

What happened? Because, oh, we catch, malicious inside. So how they prove? Yeah, but yes, Mark, but you, it, happens with our solution three times for like for five years. So that's [00:26:00] immediate value. Yeah, so because, that's the question of luck, nothing else. The second scenario is very good for us and some customers for us for four or five years because they have the, security assessment exactly the same time when they test it.

The solution and that's what we advise to all our customers, potential customers. Yeah, guys, if you have a chance, so it's the best case scenario. For example, once in six months, you go through the security assessment and you have red teaming exercises. So before, before that, put the solution, deploy it, tune it, leave it.

And what's going to happen because one of the best example, of, such, exercise is, our customer software development company for quite big for 13, [00:27:00] 000, employees and, 30 offices around the globe. So they're our customer for this, they started year number five, yeah, subscription this year.

And for them it's not questionable, should they have deception or not. Because from the very beginning, they have the assessment from FireEye. I think you know FireEye, very, well known and quite skilled guys. Yeah, and the guys from FireEye, they have eight or nine hours

to be not noticed at all, just because, it was the night. Yeah. And there was no night shift in the security operations team. So during nine hours, they generated 1, 300 alerts in our system, hard workers. But the guys were like very hard, hard, workers. They didn't find any real assets, any. So they played eight or nine hours during the night only with [00:28:00] decoys. And security team came back to the office in the morning. In 30 minutes, they stopped the malicious activity. They sent the message to the IT, so please isolate this server because it's like it's infected. So please stop. Yeah. And it was like, finally a guy say, Hey, how is it possible? How did you do this thing? You can just, okay, that was fast, but investigation, yeah? Because it's not students, I would say. It's highly paid professionals. And for that custom, it's also not questionable, because the rest of the solutions will not provide First of all, I told you engagement is very important. We provide them with the engagement.

They didn't get to any real asset. So they spent all the time playing with the decoys. Yeah, so because our decoys, they have high interruption wins. If it's a

web, it's a web, okay? It's not the hard archive, not just a static page. You can go from page to page, you can log in, you can try to execute some, I don't know, like a SQL [00:29:00] injection or whatsoever, and the page will react in the way in which the page is supposed to react.

No way to recognize, okay, that's not real, not possible, okay? the good scenario, and to finish my answer, yes, sometimes customers say nothing happens because our solution is silent. From one hand, it's good. We do not produce tons of unnecessary data. From the other hand, they say, okay, but for one year, There is nothing.

Probably I compromised and you didn't catch it. Or, I'm so cool, yeah, nobody tried to hack me. that's the tradeoff, that's the cons to be silent. This is why we introduced the new feature, Attack Vector Validation. That's the addition to our platform. It's not directly related to, Honeypots, to the Deception, but that's the logical, add on to our platform.[00:30:00]

And basically what we validate, security controls, we validate security policies and efficiency of the security team. Very simple tool. You can build the scenarios from actions and execute them running by schedule or manually. That's it. you can use different, sorts of party, payload for that and et cetera, et cetera.

So this is the part of interaction we also want to bring just because of that reason, yeah. which you write in your question, how to prove, yeah, because it's good if you have this security assessment, but it's not everybody like, going through the, proper, reteaming, assessment.

[00:30:44] **G Mark Hardy:** Yeah, and I like the example you gave about an organization that did not have a night shift for the security team, so you left the deception running overnight. And you caught the potential attackers there that were just tied up with the honeypots, tied up with the high [00:31:00] interaction assets and never really moved on to the valuable stuff because this looked so exciting and so enticing.

I have back here on my bookshelf, let me just reach for

it, a old classic, the cuckoo's egg, and this is Clifford Stoll from the 1980s who had done something very similar at a much lower level of technology. I've had this book for, quite a while. I actually got this when I was in London and I was over there working at the office of Naval Technology, went to a cybersecurity presentation.

This would have been, I think, 1990. And they had said, you're the only security guy here. Why don't you go? And then the next day this book showed up and I called them and I said, I'm not allowed to accept. a gift or anything. I'm here actually as a capacity at the, my government job. And they said, Oh, no, everybody gets this.

This is not just for you. And I asked, and they said, if everybody gets it, then it's [00:32:00] okay. And it's a great read. But the idea of deception really came up with Cliff's book here, where he had ended up spotting it then later at the end of the book, you find out it's somebody from East Germany operating on behalf of the Soviet Union, an whole different world back then.

But similar. entities trying to get in. And he had set up deception and monitoring and then all these interesting things where because of the slow download speed you had a chance to get there. But now what we're looking at is when we have gigabit speeds, an exfiltration of the crown jewels could be done In fractions of a second, instead of taking a few hours of slow modem downtime, having something like this, the deception that will not only tie up an attacker, but alert the defenders seems absolutely critical.

If an attacker could get in, find the crown jewels and exfiltrate them, that could happen before you even have a chance to send an alert. But by having the [00:33:00] deception in place, It's a much higher probability the attackers will stumble into it. Create an alert, you're aware of them, you can watch their tactics and techniques.

While they're rummaging around here, you can protect your real assets a little bit more to make sure they're out of reach. And you're much better, in your defense. Now, I'm thinking along the typical lines of IT systems, and that's what Cliff's book was about many years ago. But what about OT, operational technology, and SCADA?

Will this still work in that type of environment? Because I think industries are understanding that their OT and SCADA systems are becoming more and more of a potential target.

[00:33:45] **Yuriy Gatupov:** Yes, you're right on the price for, OT, the price of cybersecurity could be different. Yeah. Even, way higher than classical IT network. yeah, deception is the [00:34:00] perfect match. One of the few solutions on the market, which, once again, we are silent. We do not generate noise. Don't not, generate the traffic.

We do not collect the traffic. once again, our agent is, additional, yeah, so it doesn't mean that the solution will not work with the agent. We, advise people to have it, the attitude to the agents, yeah, in, IT and IoT environment as well. So one guy recently told me, listen, I have 11 agents. Running on laptops in my organizations and there is no single chance to put any additional agent.

Okay, so Basically, our solution is agentless. Okay, so we have this additional layer if you wish and we do [00:35:00] recommend to have but if the situation is that you have 11 agents running on the laptop or It's a SCADA OT environment where the agent is not possible to put your still, I don't know, Windows XP, or it's a so critical system that's not allowed at all.

You can put the solution, which will be silent to not interact with, interrupt your operations. You can be sure that you would not collect traffic, would not like, interact with the real assets. And, moreover, we have the special type of points for SCADA. So we imitate like PLC. Siemens S7 protocol and, plenty of, different stuff, Modbus and, et cetera, et cetera.

[00:35:46] **G Mark Hardy:** So it's interesting because I think some organizations will say our OT, our SCADA systems, they're isolated, they're safe. Nobody can get into them. And yet we hear over and over again, somebody [00:36:00] has left a gateway open or a connection that they forgot about that was there that somebody had used it as a junk box to get in.

And so it was seen that if somebody says my defense for my systems is it is air gapped. Then here is a way to say, prove it. Let's prove it. We're going to show you that if you are in fact air gapped, we can set these up. Because of that, nobody will interact with these. And after a certain period of time that there's absolutely zero detections, okay, fine, we believe you.

But things change, and if it's a mission critical system, we cannot go with a simple snapshot like we do with a pen test. Okay, on the 7th of June at 4 in the morning, I was secure. Okay, but that doesn't help me today or even a few hours later. In this continuous ability to detect, silently if you will, the presence of an [00:37:00] adversary seems to be An extremely valuable capability of this detection and this deception.

So in that type of environment, if we were to go ahead and some CISO said, Hey, I like this, I want more. First of all, from our conversations, you're not, Yet marketing in the United States. So if you're here in the U S you have to say, sorry, maybe you can get it over in Europe, at that market. So we're not pitching anything.

So we're holding to our, roles here, but when I met you and we met in London a couple months ago. I was so fascinated by your solution. I wanted to help people understand. So if a CISO were to continue to explore deception technologies, whether it's yours or somebody else's, how do they calculate a return on investment?

If I say, I'm going to put this much into my deception, how do I know that I'm actually making, with limited resources, a prudent decision? And I can see, That [00:38:00] once I catch an intruder with it, that would be the proof. It would most likely to say it was worth buying it, but you don't have that proof in advance.

How do we convince somebody that this is in fact, a good transaction?

[00:38:16] **Yuriy Gatupov:** so basically, now we are trying to position our solution as an intrusion detection system. the simple way is. It's to compare the value of our solution, the price of our solution, yeah, and the price of any NDR, yeah, Network Detection and Response, or Network Traffic Analyzers, or whatsoever. But don't forget to put we just made the basic maths, recently for one project and the solution of, Network Detection and Response was like 300k, yeah, the price.

That's what they need. three additional people to operate it because it doesn't bring any [00:39:00] value by itself. So the calculation is that 300K for the solution and 150K each, three guys, this 450, yeah. our solution is very simple. Up and running in two hours usually. My last experience with the German customer was 53 minutes.

So we started in 53 minutes, it was like already deployed and we're working. Afterward, you can start tuning, but initial, initial setup is very easy. So time to value is it's very quick. Yeah. You will start, getting the value immediately just because it's not like a long process of implementation, installation and implementation.

The main thing, cost is close to zero. Because you don't need to update any databases, you don't need to store, collect and store data and etc. etc. So the concept [00:40:00] is deploy and forget, okay? Once in six months you have the new release with new features, you can learn the release notes, say hey, it's interesting, let's update it and forget for the next six months.

Okay, the solution is the working, and by the way, I forgot to mention about the SCADA the solution is working in air gapped environment because there is no

cloud. We are not sending any data to any cloud and we're not collecting any data from any cloud. So the solution could be used in the air gapped environment.

So basically, you can calculate how much money you just save with the additional personnel. That's the easiest calculation you can then say, Hey, I don't need to have these three guys, because now it's so obvious, so simple, no special knowledge, like no script language to learn, no syntaxes to learn, nothing like that. I can appoint [00:41:00] any IT guy who is any K administrator and he will understand what is going on and how to run the solution, because the simplicity, yeah, that's, the key point.

[00:41:11] **G Mark Hardy:** Got it. So we're getting toward the end of the show. So let me try to summarize what we've been discussing in the last several minutes. We first started by talking about a fundamental challenge in cybersecurity, which is. The asymmetric nature of attack and defense. And the attacker could only have to find one opening, but the defender has to block them all.

And what we've learned is that deception technology isn't just another tool in the security stack. It's a strategic shift in the paradigm that helps to level the playing field. By controlling the environment the attackers can see, we can move from a purely reactive stance to one where we could influence and monitor attacker's behavior on an active basis.

Now, these implications are profound. Think about the current security operations center. How much time do your people spend chasing false [00:42:00] positives? And how confident are you in your mean time to detection? We've heard today's about high fidelity alerts and early detection capabilities that could fundamentally transform the efficiency of your SOC.

When your team receives an alert from a deception platform, they can act with confidence because you know that a legitimate user would have no reason to interact with these assets and you've got somebody, a bad guy if you will, on the hook. So some takeaways from this discussion. Start small, but think strategically.

You can begin with critical network segments, expand based upon your risk profile, you can go into air gapped environments such as OT and SCADA systems because there's no requirement to communicate back to a cloud. You want to ensure your deception assets align with your actual infrastructure to be convincing, but also it's going to stay manageable. Also, this technology isn't

just about detection, it's intelligence gathering, because every interaction with this environment and the deception will provide new insights into the [00:43:00] attacker's methodologies or tools or objectives. You'll start to understand what they're going after and how to better harden your systems.

And if we successfully deploy Deception, we're going to have to balance automation along with what you had said, the customization, although you can automatically deploy Deception assets. The ones that closely match your unique environment are going to be the ones that are going to be the most persuasive to an attacker.

So I think that the deception technology market is going to grow as the attackers become more sophisticated, as the regulatory environments put more and more cash in. Pressure, potential fines, even jail time on leaders. And as you had mentioned, like a ciso, it'd become like a fighter pilot. The old joke, what do you call a fighter pilot with a record of 80 and one dead.

He just lost his lost dog fight. And so a CISO that has 80 blocked intrusions in one major compromise, unemployed. So we integrate this with other security tools and things such as that. Now, if you'd like some more information, you wanna get a hold of Yuriy. [00:44:00] I have your email at info@labyrinth.Tech. Now let me spell labyrinth because not every person gets it right.

L A B Y R I N T H dot T E C H. I have to admit, although I was a spelling bee champion, When I was a little kid, my first attempt at re spelling labyrinth, I got it wrong. And so that's why I put it out there for everybody. Basically, you can't defend against what you can't see. Deception technology is going to take that invisible attack or make them visible to you so you can understand that better.

Yuri, any last words? Are we ready to wrap up here?

[00:44:36] **Yuriy Gatupov:** I wish you the, Merry Christmas. Yeah, because we are close to, to, the main celebration of the year. yeah. Hope you will have time, for some rest to spend with family, friends. And, yeah, I wish you that, More, like less cyberattacks in [00:45:00] the new year, like more good news and more good technologies, on the market.

And, yeah, so all the best and, hope to see you again, next year to meet you again, somewhere in Europe, in London or any other place, you will visit, will be my pleasure to, meet you

[00:45:20] **G Mark Hardy:** Excellent. Yuriy Gatupov, thank you very much for being part of our show today. This is your host, G. Mark Hardy. If you like CISO Tradecraft, make sure you're following us on LinkedIn because we have more than just podcasts. We also have a Substack newsletter. Look for us on YouTube or your favorite podcast channel.

And if you can give us a thumbs up or five star, that'll help other people find our show as well. We thank you for your time. We thank you for your interest. And until next time, stay safe out there.