Emulating the Adversary to understand the True Risk and Exposure

Mon, Nov 21, 2022 12:18PM • 46:30

SUMMARY KEYWORDS

vulnerabilities, credentials, environment, host, pantera, test, remediation, exploit, product, tenable, plantera, validate, run, organization, password, security, cybersecurity, attack, external, achievement

00:13
Good afternoon, webinar community and LinkedIn Live community. And thank you all for attending our once a month webinar. Glad to have you here. And we are having a guest speaker today, which is has a really exciting topic to share with you around penetration testing and the product Pantera. And we hope that you learned something and sparks your interest and even maybe wanting to have a demo after this. If you can go to next slide, Justin. Oh, good. Go through the introductions. I'll introduce myself. I'm Charles Maddox. I'm with the AI for group. I'm the founder and principal. And you know, at the AI for group, we're a company that focuses on digital transformation, a lot of experience with software development, electronics, and DevStack ops and Agile transformations. And I got a lot of experience in that as well as I for group as a whole Deonte you want to introduce yourself, sir? Our cybersecurity director.

01:12
You're on mute sir. I just want to introduce myself, cybersecurity director. And we're really excited about this product and terror. We think a lot of companies need automated pentesting considering everything that's going on in the landscape of things and been there for a few years and just happy new year to build this back as up and very excited about what we're doing what our products and services companies. Thank you.

01:41
Justin, will, you could take it away from here.

01:45
Great. And thank you folks for having me and folks on the Zoom, it's really nice to to meet you virtually. And hopefully, you know, in the next 3540 minutes, you get some value out of this. So Justin bryza, I run channel enablement here for the Americas, then at Pantera, just coming up on an eight and a half months. Prior to that I spent plenty of time in the hardware and infrastructure cybersecurity space. What I want to talk about a little bit today is our product and platform pen Tara, I'm going to go through, you know, probably five or six slides just to sort of paint the picture on who we are what we do. And then we'll jump right into the actual product itself. And we'll walk through a very high level demo. You know, I believe if you know questions, there's there's probably a chat or q&a feature within zoom. So don't be

shy, throw them in there. If you know, I probably won't catch them during the presale, but I'm happy to obviously spend time towards the end to to answer them or if we require a follow up. I'm sure I could work with Charles and Tim to get you the appropriate information. So who is Pantera? Right? And really, we are an automated security validation platform. Right? So you may hear that term, or you may not because quite honestly, it's sort of a new realm in the cybersecurity industry. We are offensive security or red teamers product. And what are we set out to do? Right we are our goal at Pantera is to become the authority when it comes to cyber risk validation. Right? And there's there's an underpinning methodology on how we do that. But if I was to sum it up in one sentence, it would be we want to give organizations a real life understanding of their risk and exposure by actively acting and emulating a hacker, right? So we are the attacker in your environment. Right? And that leads to too many different aspects. Or use cases, I guess you could say, on where pen Tara provides value in our customers environment. So obviously, understanding of exposure and risk is one thing, but because we are emulating real life TTPs we are essentially acting as someone with malicious intent would, right? It allows our customers to really improve their overall security readiness, right? We can validate products controls policies in place already, we can obviously understand where there are holes and gaps that need to be addressed and remediated. But it's really a holistic picture on you know, where from a cybersecurity readiness do I stand? What do I need to do to get better? And then how do I validate that I made the correct changes to decrease my risk and increase my resiliency? Who has been Tara? We're just seven years, seven years young founded in 2015. We are you know, just north of 250 employees, fairly well funded. We got a big chunk of Serie C earlier this year. Vertical agnostic, right so as I build out this little side, we have over 600 customers in every vertical size of customer persona of customer out there. There's not honestly there's not one organization that wouldn't be able to, to garner some value from from the Pentair platform, we are truly global and over 45 companies, and this continues to increase at our at a rapid pace. Right? So what is the problem we solve? And it really boils down and took the three key pillars. Right? I mentioned this the first one, how are you? How, how do we help an organization be confident of their exposure and risk when it comes to cybersecurity? Right? We as security practitioners invest a lot of time, resources, money into products and solutions to uh, you know, really ensure that when the day does come when something malicious happens in my environment, whether that's something that happens from an internal standpoint, right, someone gets a hook into my network, it's a disgruntled employee, there's some credential that was left or obtained, right? Or from an external standpoint, right, my web apps, my external assets, etc. When the day does come that one of those gets breached. And we all hope it doesn't. Right. But the reality situation is it probably will. Are we confident we've done enough to prevent catastrophe? Right? Are we confident that the products, the policies, the procedures, all the fun stuff that we built out on on a defensive standpoint, are going to act and function as desire? And really the only way to ensure that is to test it? Right? So Panthera is acting as that, you know, essentially emulating an attacker in your environment prior to the real thing happening, to give the organization a true understanding of where do we stand when the day does come? And that leads to, you know, answering the question of are our defenses working? Right? I mentioned, we're all making these investments and all these different products within our security stack. They are intended to perform a certain function, whether that's an EDR, a sim, web application, firewall, soar, whatever it may be, they all have their place. Right? But when are they? Are they set up to work together? When that when you know, when the day does come? And how do we understand, right, again, emulating the attacker that they're configured correctly, we haven't left any holes, things along those lines. And then lastly, right, I'll argue this is probably the most important

aspect of tentera is there's there's many great vulnerability management and assessment platforms out there. And I'm not going to sit here and say that Panthera wants to replace any of those they have their place in an environment. And that's not what we have Cantera are trying to do, right? We are trying to work in conjunction with our friends in the vulnerability management space, really, to make things more efficient, is really what it comes down to. And what do I mean by that? Right? So we are all anyone who spent time in the vulnerability management space working with the different solutions, right? I'm sure would agree with me, when when I say there's a lot of noise. And what I mean by that is, if I'm an organization, it's not unrealistic for me to have hundreds or even 1000s of vulnerabilities in my environment, right. And that's exactly what a vulnerability management assessment platform is there to do. Point out all my vulnerabilities, that allows me to help my patch management procedures that allows me to help my upgrading all that types of things, right. But what Ben terror set out to do is really try and be that silver bullet, right? You're sort of red team in a box to say, Okay, I have all these vulnerabilities in my environment. Now I want to go through and actually see which ones are actively exploitable, right? Just because I have a vulnerability on my list from my vulnerability assessment management solution, does not mean that I don't already have a security control in place to prevent it from being exploited. If I do have something like that in place, right, I would argue that falls lower on the list of remediation, right? It's yeah, there's a vulnerability present, but no one nothing can happen. It nothing malicious can happen. But what about those vulnerabilities in your environment? Right, that aren't protected from being exploited, right? That's where Pantera steps in. To take it to the next level. Right? We will provide an understanding because remember, we're actively exploiting in an environment we are running real live attacks. So we're giving you a true real life view into where from my organization's from a vulnerability standpoint, do I need to focus my remediation efforts to get the you know, the best the best bang for my buck essentially, right? So three use cases are three problems I guess we're trying to address one is under Standing just exposure and risk in general, right to allowing you to validate the controls in your security stack that you've already invested in, right to make sure they're not misconfigured. Or there's holes that we that weren't intended to be there. And then three, really allowing you to put your vulnerability management assessment platform on steroids, right? To give you a true insight into well, what do I really need to care about tomorrow, and what can wait till next week.

10:33

So let's talk a little bit about the platform, I have one slide, I'm going to talk to it and then we'll get into the demo. So the platform itself is built of two different aspects, we have what we call Pantera. Core, that is a piece of software that sits on prem, in your ad environment, right? behind the firewall, sort of, I guess you could say, like an assumed breach scenario. We do not use agents on endpoints, right? There's no concept of an agent in Pantera. Why? At our core, and I'm gonna sound like a broken record, right? We're emulating the attacker. If I'm an attacker, and I get into an organization, I don't have the luxury of putting an agent on an endpoint right endpoint prior to doing that, right? I have to take what the environment gives me Pentair is that exact same thinking or methodology, right? We are going to be putting in environment, there are some different controls you can put when you set up the tests and their different, you know, tests and things like that, obviously, but we were non deterministic. Right? We will do, you could run the same test twice, it will probably do two different things. But we're only given what the environment gives us. All right. On the flip side of that, we have what we call Panthera surface. That is a SaaS based product, really aimed at an organization's external assets, websites, domains, subdomains, services, networks, things along those lines. It's mapped to the OWASP, top 10.

Again, aimed at giving organizations and understanding of where do I stand from an external exposure? If someone was snooping around with malicious intent to I have vulnerabilities, we are going to actively try to exploit those just as we would on the internal one. To truly say, Yeah, you know, if we have these vulnerability vulnerabilities, are they exploitable? Or are they not? I will show you both of these in the coming moments here. So we will move we'll start with core screen here. So hi, Tara core. Remember, this is an internal you could call it a pen test internal validation. Software sits within an environment, obviously, there's multiple different ways it's, you know, can be deployed based on topology, we have predefined tests. And what I mean by that is, because we run in custom in organizations, production environments, we don't go in lab environments. We don't want to go in duplicate environments, we want to be in the production environment, right? Why emulating an attacker, we need to be where they're going to be to give you a true real life understanding. Because we are doing that we have to have a really altra high focus on being safe. And what do I mean by that we are actively exploiting, right, so we have to ensure that we're not going to cause unintended harm in your environment. There's a lot of q&a and research that goes behind every exploit we add into this product, we have a team of roughly 35 to 40 research engineers, most of them out of the Israeli Defense Forces, our founder was the former head of that, right? That are going into ensuring that when we design exploits to go into our product, we're not going to cause unintended consequences. As a side effect of that being safe by design, right? We're not allowed to, we can't have the luxury of allowing allowing operators to add their own malware or define their own attack paths, right? Because that would take away some of that assurance we have on whether or not we're going to cause harm. Quite honestly, we don't have any concept of an attack path, right or defining an attack path because it doesn't mimic mimic the real life scenario. So we I'm just gonna go through this really quickly, we have a blackbox blackbox test. This is where almost everyone who's new, new to Pantera starts super simple, we don't authenticate all we want is Pentair to have an IP in the environment will provide the scopes of the task whether that's a subnet two subnets three subnets whatever. We do have some configure ality configured configured, we're going to look for configure reality they're configured configurability that's what I was looking for. Things such as a stealthiness level, right? So do I want Pentair to be super noisy when it's going through the discovery and enumeration right use case there is is, hey, I want to trigger my IPs. I want to trigger my sim. If you have a sock, maybe I want to see if my sock is sleeping or paying attention, right? Are they alerting the right people is my IR plan in place, we can also have been terribly, super stealthy. I don't want to trigger IPs, right? I'm not going to do ping sweeps I'm not going to do our ARP sweeps and things along those lines. Use Cases vary, right? It all depends on on the end goal of what we're trying to do in the test. We are actively exploiting in the environment, right? So we are going to give you as an operator of Pantera, the control of do I want to approve the exploits during the test? Or do I want to let Pentair just run and as their chewed up, exploit them dynamically? Why do we have this in place? Most of the users of the operators who use Pentair in their environment are using it to validate their controls, right? Yes, it does. It's obviously very good at understanding what vulnerabilities are there and are we able to exploit them. But part of the natural process of what pen tester does under the hood, right, which mimics a pen tester, an automated pen tester, right? Is naturally validating controls along the way. Perfect example, if I do a file based credential credential extraction, I want to attempt this on a handful of hosts, I'm probably going to be in parallel checking my EDR solution to say, Hey, is it picking up on the DLL file that Pentair is trying to push to the host. So by having the require approvals for exploits, I can be really strategic about what exploits are happening at what timestamp. And then in parallel, I can make sure that I'm checking my

controls to ensure that they're doing what they're are not doing what they're supposed to be doing. Lastly, part of the benefit of having something like Pantera is not to be stuck in these point in time assessments, right? Yes, manual human pentesting is great. You could argue whether this is something that would replace it or not, I would say it's not right. I think again, it can work in conjunction with that. But if having the ability to do and run this test on a cadence, regular cadence, weekly, monthly, quarterly, whatever, environments change all the time, right? So I want to be able to retest on a cadence, and then I can start to build a baseline of hey, is my resilience going up or down? am I introducing new owner vulnerabilities or not? So we have the ability to schedule this, obviously. We also have a what if or a gray box, if you're familiar with pentesting terms that is essentially very similar to a black box. But we're giving Panera Bread Chrome, right, we're going to provide a credentials. It's a what if scenario, a great use case I hear from a lot of our customers is, you know, they're running those phishing education campaigns where they send out a fake phishing email to the organization. If someone clicks on it, and that someone had privileged credentials, or high, high, high privileges and their credentials, they will then take those ronto What if in Panterra, add the credentials, just to say, here's what our blast radius could have been if this was a real life scenario, right? Again, painting the picture before it actually happens. are going to testing this is where things start to get really cool. And this is kind of you know, as as folks become more familiar with the Pentair platform, they start obviously, to become more strategic with it. Targeting testing is really where we go with that right ransomware emulation. So I can essentially allow pen Tara to actively launch a ransomware attack at a set of hosts in my environment, I can slap between the different campaigns, right, I can select different variables, do I want to try and decrypt files on the host? Do I want to try and exfiltrate data? All with the goal right of launching a completely benign and safe ransomware attack with all the real life TTPs? Right. So it's going to seem as though it's a real life attack against my infrastructure, to give me an understanding of where do I stand if if it was to really happen, right, what's working, what's not working.

19:10

And then the last one I'll just touch on before I get into a GUI of a former test is Active Directory password strength assessment. So we can have Plantera synced with my ad environment, ingest all of the credentials and details, run it through our software and producing a nice, really easy to read one and a half, two page report with pie charts and bar graphs and all that fun stuff. Right? Really outlining where is my Active Directory password strength, you know, as a baseline, are there things that are outside the 90 day limit? Are there passwords that are less than the minimum eight or nine characters whatever will be able to be pen terrorist actively able to attempt to pass crap passwords, right, so were we able to crack any How long did it take? What methods did we use? Right? Are there weak passwords or the reused ones, just as of two months ago, we added a leak credential feed to Panthera right from both an internal and an external. On the internal side core, which is what you're looking at, we're using this for password strength assessment at password strength assessments. So now we can ingest credentials, we've obtained from whether it's the dark web, public social media sites, whatever breaches whatever it may be, and use this, again to compare against your ad environment and say, hey, you know, you have 12 credentials that are found in the dark web for the right person that wants to buy them, that are still active in your Active Directory environment, you may want to change those, right? Obviously, you definitely want to change those. And then we have some other stuff around critical vulnerability, scanning, targeted testing, etc. So let's jump into a blackbox testing and start to explore around I'll give you an explanation of what you see here. So when we run a blackbox test, right,

obviously, we define the time and the scope, how many hosts we want to do and how long we're going to do it. Typically, folks are doing these for anywhere from six to 12, you know, no more than 24 hours, they're not letting run Plantera run continuously, right? Again, they're using it as that red team in a box, a power tool. So first thing it's going to do is look for the devices and get an understanding of what they are go through discovery, enumeration are they Windows workstation, servers, Linux, whatever it may be. And then it's going to, you know, point them out here on the bottom half of the screen. Right? I mentioned the approvals process. This is a view of what that means. So in this, in this specific test, Plantera had queued up 72 possible exploits. And if I do a filter, I can show you all the different ones we found vulnerabilities to in this environment. Right. So this dropdown changes every time you run Panthera, it's only presented what it is found in this test run in the scan. Right. So I can be strategic. I mentioned the file based credential extraction, maybe I only want to do that, right. In this case, there's just one, I would click the button, I would click approve, and I would go and let it do its thing I could then in parallel, go chuck my CrowdStrike sign or whatever it may be and say, Hey, is it picking up on the DLL is a blocking it whatever it may be? Right? Obviously, as an underpinning to everything we do, we have to look for vulnerabilities right, we need to understand what we can take advantage of before we can take advantage of it. So we are going to list the vulnerabilities we found in the environment, we will rate them on a criticality score. Nothing you see here from these numbers, these 10 910, nine, eight nines and all that are based on CBSs scores or any external metric for that matter. Everything is based on what Panthera was able to do in this specific environment in this specific scan, right, again, real life and needs to be real life to the organization. We can't take external metrics and say this is a time, you know, because CBSs says that you need to fix it tomorrow, right? It may not matter who cares, it doesn't matter. If we are successful and exploiting a vulnerability, or obtaining some sort of information, like a directory file, accessing shared files, capturing credentials over the wire, whatever it may be, we label it as what we call an achievement, right? So an achievement and Cantera is we are successfully able to either obtain some sort of information or exploit a known vulnerability. Right. And this is where things get super cool. So we will list all the achievements here you can see in this specific task, there was 520 of them, some of them have multiple achievements. 129 on some, as I scroll down into the fives, you can see we're capturing credentials, Pentair is sitting on the wire, as it's going out to understand what the environment is what point vulnerabilities may be there. It's also trying to sniff traffic, right? Trying to understand other legacy Windows or even current Windows protocols that I could take advantage of as a software and fake a host into giving me something they don't want to get, right. We're gonna look for directory listings, you know, things such as SEF files, numerating, web services, etc, etc. Where it gets really cool. For every one of these achievements, we build out what we call an attack map. And I'm gonna let this build Excuse me. So an attack map in Plantera is another way to think of this as an exploit Kill Chain. Right? Here's the time we were verified domain admin account cleartax password, what does that mean? Here's the result user password domain. This can be on a few skated if you wanted it to.

24:45

Right, but that's great. Okay, we pointed out the time, right, but how I want to know how I got there. I want to know every single step Panthera took as a software completely dynamically to get that credential, right so I can work my way down through through this attack map, then if I go all the way to the top, you can see the trophy is an achievement, right? The Broken shields of vulnerability. So my first achievement or my first success, successful action or exploit of a vulnerability was this five, five. And

what did we do? We captured credentials over the SMB protocol. Here's the details. Here's a little insight on what this would mean for someone with an attackers mindset. But more importantly, I can then go through and understand exactly what happened. So what vulnerabilities did we take advantage of to get these credentials? We forced the heart host to authenticate to us, right? Perfect. What vulnerabilities now we moved, we're moving laterally, think about a human, you know, a pen tester or someone a hacker, what are they going to do? They obtained credentials, they're going to look around the environment, can I use these anywhere else? In this case, we performed a relay attack, we don't even need to crack the password. If we can relay the hash, who cares, right, we'll just relay it. In this case, there were some SMB settings that weren't configured appropriately, we were able to relay just so happens on that next host, we were able to get into the memory and obtain additional NTLM hashes. And we can point that out right here exactly what we obtained. Cool. Pantera is going to try and build on that. Can we go further. So Panthera is going to look around and see are these credentials valid? In this case, that administrative credential is valid on eight other hosts in the environment? Right? Sweet. Can we move on further than that? Just so happens, it has remote code execution capabilities on one of those eight. Perfect, we're making progress. Now we found a different host, we found different credentials that also allow us to execute code on this host. So what are we going to do? We're gonna attempt to push down a remote control channel and push down code. In this case, it's a PowerShell script. Why are we doing that? Because we want this host to phone home to printer software. So we're going to talk the next stage and then attack. There's a use case here. There's a validation use case. So as pentamer is going through performing its offensive actions, right? Do we have something in place as an organization that should be picking up on this didn't alert on PowerShell execution on this host? Maybe it did. Maybe it didn't? Maybe it shouldn't? Maybe it should, right? It's a validation story. We opened the command and controls session, we pushed out malware, aka dll file. Do we have controls in place that should prevent this from happening? My AV didn't block the payload, maybe it did block the payload, right? In this case, it didn't, we got to a different host. We got to the into the memory of this host, there were NTLM hashes stored in clear text. And we were able to find the domain admin, right. So I just walked through what is it 12 to 14 steps that Pantera did in a matter of, you know, maybe an hour if this was someone with a human day, day and a half, right? That's part of the power of vintera efficiency, right? Obviously, we all know the power of automated solutions and software, why not use it? Couple cool. Other things cool about the attack map, and I apologize for zooming in and out. Everything we do in Panthera Corp is mapped to the mitre attack framework, right? So every time we perform an action, we are going to map it to the mitre attack framework. What was the adversary level? What was the technique? Some technique parameters? Is it used by anything else in the wild? Right? The goal here is to give an organization of understanding of where they map from a defensive standpoint to the TTPs on the mitre attack framework. Right? We also, if I click on a vulnerability, it will provide insight on the vulnerability and then a remediation recommendation, right? What would I need to do to help remediate this Pentair is never going to go in and actually remediate things. What what our goal is to make it easier on you and your team to make the remediation. So we'll give a very high level here. And then we also build out a remediation wiki. It sits within the pencarrow software. So nothing's ever falling out of your environment and going to a cloud or anything like that. But what the Pantanal remediation wiki is is essentially a place where without having to go to Google or go to the textbook, or whatever it may be, we're going to give you a deeper dive into what's the vulnerability? How is it taken advantage of what are some of the ways you may want to remediate in your environment, whether it's using Active Directory group policy or local on the machines if there's only a few small sort of them? And then lastly,

and probably the most important argument, in my opinion, the most important, how do you then use Plantera to validate that you've addressed the vulnerability, right? So we exposed it, we prove that it's legit by exploiting it. We're showing you how to remediate it and then we're going to show you how to go back and validate that you've actually fixed the vulnerability. It's no longer there, right? And as you can see, we do this for a hand All I have quite a few different vulnerabilities. As I scroll scroll through here. Naturally, we're going to provide a list of the vulnerabilities in the environment, we also do something that we do very differently is we provide a remediation priority that's not based on severity, right? Our list of remediation vulnerability has nothing to do with the criticality. It's what it allows us to do in the overall scope of things, right? This four seven was the start of that obtaining domain creds, if we wouldn't have captured those creds over the wire way at the top of the attack map. None of that would have ever happened. Right? So this is going to be your number one remediation priority, right? This is where things differ very much from the vulnerability management assessment. We're not we don't care about the severity, because we're actively exploiting, we know what matters and what doesn't, right. So yes, the criticality is great from a content standpoint. But from a remediation standpoint, it's really who cares, right? What did it allow us to do, and this left gave us the keys to the kingdom. We do a mitre attack map for the entire scope of the environment, color coded so you can get an understanding of where you stand. This is something that you can export after every test new a report, establish a baseline things along those lines, I'll show you a quick report, trying to stay conscious of time here. So this is a former report, we have two options, we have a detailed and a executive level. So this is a detailed, but the executive level is basically the first few pages of this. The one thing that I think is really cool about this is we because we're running in the environment, the same test time over time, at least that's the goal, right? You're going to scope out a test once you're gonna establish a cadence and when you're gonna run it over time we can start to build a resilient score, right? am I introducing risk? Or am I remediating risks, and that's what this resilience score essentially does over time. And then it gives you a score, right? You know, executives love this stuff, right? Because they can baseline what they're doing, they can validate their investments in security products, you know, validate all that types of stuff. If I scroll down, we'll do a scorecard a little bit, we will then provide host findings. So if you want to hand this over to inventory, team, asset, asset team, whatever it may be, if we're able to access any shared files, credentials and passwords, so what were you able to, you know, were we able to compromise accounts? Were any of them privilege? How are we able to do that if we're able to craft passwords? Was it something that was done prior to an exploit? Or was it something that was done after we got onto a host and scrape that on the memory or Alsace or whatever it may be. And then it will obviously go through and list all the different vulnerabilities and achievements, the same thing I just showed you, in the GUI. Right. So that's a super quick view of Pentair core. You know, as Charles said, at the end, I'll give you a link, if you want to spend more time in this, we're happy to do it, I went through a lot of stuff. What I do want to do now is just pivot over to our external product and show you surface. It again, it's almost the identical the same concept of what we're trying to do in core, obviously, how we do it's a little different. And some of the things we do are a little different, but understand the external exposure, right? Understand what's a vulnerability externally, and then give you a way to go in and validate it via actively exploiting it, right? So we're not just gonna give you a list that says, hey, you have these 10 vulnerabilities, we're gonna tell you, we were able to exploit them or these we weren't. Right, again, prioritizing remediation. So what do we see here? Obviously, we'll list our assets. attractions, I'll come back to that in a second. Because that's super cool. Vulnerabilities and achievements means the same thing as core vulnerability is the actual vulnerability and achievement as we validated that it actually

exists, right? We may have dropped payload, we may have grabbed credentials, we may have uploaded something, whatever it may be. Our techniques, and our methodology is mapped around the OWASP, top 10. But we also did map it to the mitre as far as what we're doing, right? And we'll give you some action types. asset, location, asset inventory, attack surface over time. So as my external surface changing dramatically, DevOps teams love to spin stuff up and not take it down or forget about it. Is it something that's publicly facing is something that shouldn't be publicly facing, right sort of that shadow it sort of paradigm.

34:39
And then I can click in and look at different things. So obviously, I can look at my different assets, domains, subdomains, IP ranges, services, websites, etc. I mentioned attractions attract attraction and Cantera is, it's either a potential vulnerability meaning we can't confirm the vulnerability exists. But more importantly, why I really like attractions, it's things that aren't really considered vulnerabilities. But if not properly configured, right couldn't be a vulnerability. Things such as an open FTP port, open MySQL port, a website login page interactive form. There are numerous valid business reasons why an organization would have these facing on their external assets. Right. But are they configured and secured properly? Do I not allow anonymous to login to my FTP server? You probably shouldn't on the external, but there is going to try that. Right? Or if I have a login page, right? Can I do some sort of Blitzer SQL injection attack or harvest leak credentials and log into it? Right? I have an interactive webform. Can I do a remote or a local file inclusion? Can I abuse the underlying code to take advantage of that form? You know, there's, there's things you can do when you're developing this. To prevent that, we're going to check that right, you may be all perfectly fine and good to go. Right? We just validated it for you. Right? And you can see there's a whole bunch of other different stuff here that we talked to, obviously, we list all the vulnerabilities as well. You know, and these are ones that after we go through and validate and get an achievement, well, here, we do assign a CBSs score. We can you know, log for Shell, it's found five times, here's the different places that was found. You know, what does it mean? Right? And then I can start to hone in on that. So I could say, I want to go to I don't know, maybe this website here, I want to look and it's going to tell me okay, here's the details of this specific site. Are there different attractions in this case, there was a file upload and an interactive form. Great. Are there other vulnerabilities? Nope, just the log for Shell, it's gonna give us an insight into that remediation as well. Provisioning is very similar to the approval process in core, right, so I have these attractions, I have these vulnerabilities, I want to actively validate if they're a vulnerability or not. Right, so I'm going to attempt to do a remote file inclusion, I'm going to attempt to do a sequel injection on my login form, I'm going to attempt to validate log for Shell, right include this the next time I run a test, I click test now come back, if it's an achievement is successful, if there is no achievement, it wasn't successful. So all those things we just provision, the only one we validated was logged for Shell, right? And then I can go on and click into the attack map. And it will provide me more detail on exactly what we did. Right? Here's the different parameters. Here's the host, here's the URL here was the web request, etc. We have an attack, map and coat and surface just like we have in core. As I scroll down, there's you could see there's point vulnerabilities, there's gathering credentials, and AWS from a host extracting some of these latest vulnerabilities with some of our security vendor friends, all the way to discovering directories logging, I mentioned that that FTP, right attraction. We found a poor, we tried to log in anonymously, and we were able to do it right, probably not a good thing. All the way down to founding date finding databases, enumerating web services, accessing files on web servers, right? So

we will do all this from an external standpoint, the thing to remember here is the way the Putera external platform works. We're not authenticated, we don't have any keys or doors in whatever we're doing anyone with the right intentions, or the wrong intentions, I guess you could say, well do the exact same thing or have the exact same capabilities, right? So it's a true real life view into, okay, how exposed Am I externally? And then you can see, here's all the different I mentioned, the provisioning, right? So I can go through and I can click these and then I just say test now and this would be validating my my vulnerabilities. Well, that is core and that is Pantera. Service. Charles, I'm right around 240. And I don't like to spend the whole hour I want to leave time for questions. So I'm going to stop there and put up my last slide. Just in case anyone has further information or details and then I'll try if we did have any questions, I will try and address them now.

39:32
Thanks for that. Justin. Any questions from our either LinkedIn live or live webinar? Checking the chats here, while we're waiting for those come in? Justin, I had a quick question for you. You know I for we're we have a lot of experience with helping ops teams develop better processes for remediation and their workflow. One thing that came to mind as I was seeing Some of the information that you're presenting when you have some of these identified vulnerabilities, what what tools? Are you familiar with that? And Tara, are you seen in any use cases like connecting with like the JIRAs? Or the ServiceNow? To actually complete the workflow and actually fix it? Yeah, yeah.

40:21
So ServiceNow is probably our most popular. I don't have it in this lab version, but we actually have a button in the attack map where if we find a vulnerability, you can click Send to ServiceNow. And it will open up a ticket. The other thing we are coming up with an integration for a company called torque, I don't know if you've heard of them, their security automation, sort of remote automated remediation ticketing kind of platform. And then we also have an integration with Palo Alto is XOR product, right? Where we can essentially send them and then it will create a remediation. automated security playbook. Well, you know, integrations are something that we're actively working on, you know, this year and early next year, right? It's kind of been on, quite honestly, up until 2002. was on the backburner, but ServiceNow was the big one. And now it's where does it make sense for us to go next? Right. Makes sense? Yeah.

41:17
Yeah. Good question, too, just thinking about it? Will it be able to integrate with products such as tenable, from the vulnerability side of it? Would it be able to get Pentair to work side by side with tenable? And that says,

41:33
yeah, so it's a good question. Honestly, I get it almost every time I do a demo. From an integration side, I don't know of any anything on the plans to physically integrator or digest data out of any of those, those vulnerability products, right. The reason why is if you kind of think to our sort of whole Northstar of acting like an attacker, we don't want to provide Pentair information at a time, right? We want it to be, you know, dumb, for lack of better words, right? So if we're providing it vulnerabilities, I guess our product team see it as cheating, right, where it's kind of already knows what it needs to do. But that

being said, we always work alongside of almost every customer who buys pen, Tara has one of those products, whether it's tenable, whatever it may be, right? And they're not ripping them out, right? They're using us as more of that silver bullet strategic right to say, okay, tenable gives me the 1000 foot view of my vulnerabilities. I want to use Pentair to give me the 10 foot view of what one's actually matter. Right, then I still need tenable to define my patching schedules and things like that right, on a broader basis. But maybe I use Pentair to define the ones that I gotta have the team stay the weekend to fix right versus wait till next Tuesday.

42:53
Right? Okay. Fair enough.

42:59
All right. Let's see any questions coming in quite yet? Well, the ante did you want to kind of give an overview of just how the i Four group, you know, what our cybersecurity services and offerings and, you know, opportunity to involve up and Tara and like the tangibles, we can, you know, potentially help our clients?

43:23
Yeah, definitely. So yeah, just to give a quick overview, we're a cybersecurity consultant, company boutique. And we get involved with vulnerability management, and then bring those new product Carpenteria from the pen testing aspect. And then we also get into DLP as well. And then so we have partnerships with various companies tenable. This company Tara, and Forcepoint, and, and a few other products as well. And we'd like to make a bet to sit down and we can meet up with him and talk to you about how we can help come in with solution like Matera to help look at your your, your your networking enterprise in a more more realistic standpoint, whereas tenable only gives you this big overview, this kind of gets into the weeds of it. So, you know, we're really excited about that. We work with enterprise level environments and mid level environments as well. And then we also bring Isao cybersecurity as part of our one of our services that deal with helping us an agile within your cost structure. So good example, from the vulnerability standpoint, you have your infrastructure to the InfoSec team. A lot of times companies are not, some companies are not really having these groups talk to each other like they should. And this is where agile becomes a grid of good methodology, bringing into your company to fill in those gaps. Get those for instance, stand on meet and so you can start getting down to the root of things which are vulnerability and not having patches not being patched, which that's one of the most critical things going on right now. Things are not being patched for On a point where should be and so product like Pantera would definitely help that scenario, and product like tenable as well, too. And so we just want to say that we'd like to talk to you about anything. Anybody see this video, you can definitely reach out to me or Charles, um, and look at our website, the i Four group.com. And we definitely would like to schedule time to talk. Thank you.

45:24
Thanks. Yeah. And as the last slide here shows, there's some contact information for all of us and even scheduling a demo with Pantera. You know, that'd be something that you might want to get involved in as well. And Well, Justin, any last words? I think we're probably at our close here.

45:43
But just thank you for your time. It was it was fun talking and I look forward to engaging further.

45:50
All right, sounds good. But thanks, everyone. We'll see you guys at the next webinar. Stay tuned. And this video will also be shared to those that were on the invite list and also to our LinkedIn community at large. So thanks again. Everyone. Enjoy the rest of your day. Have a good day. Thank you. Bye bye