Heather (00:13):

Welcome to the Hurricane Labs Podcast. I'm Heather. And today we have a few of our team members here to talk about what considerations and steps go into establishing a SOC team and what you'll want to consider when deciding if that team will be internal, or if you'll work with an MSSP to manage your security needs. Hi, everyone. Thanks for joining me today. Why don't you go ahead and introduce yourselves.

Brian (00:39):

Hi, my name is Brian Kerrigan. I was part of the HL SOC team for many years, and I've moved over to our Search Development team, but I'll be providing some insight from my SOC days.

Dusty (00:51):

Dustin Miller, part of our SOC Tier 1 team. So I handle a bunch of the alerts that come through our SOC everyday.

Austin (01:03):

I'm Austin. I've been with Hurricane for the last year and a half as a SOC T1 Analyst.

Steve (01:10):

I'm Steve. I oversee our Security Operations team. I've been with Hurricane for as long as I can remember.

Brian (01:17):

Since before time.

Heather (01:19):

Alright, well, thanks for joining me today you guys. Why don't you go ahead and first help us figure out why exactly we need a SOC team at all.

Brian (01:30):

Steve, why do we need a SOC team?

Steve (01:34):

I mean, I think why you need a SOC team, if you look at most of the major security breaches that we've seen over the last, you know, however many years you want to look at one of the things that keeps coming up as a recurring theme is that there, there was, there was something going on and nobody was looking to see that. And I think that's, that's kind of the role a SOC performs is, is constant monitoring of what's going on in your environment from a security perspective. And that's the kind of thing that helps you stay, you know, or try to get one foot up on the on the enemy here. So, you know, really, I think a SOC is something that a company really of any size needs to look at, but especially as you start building more of an online presence and start opening up what your attack surface might look like. There's a difference between a small local bookshop that has one little website running on some hosting platform and a giant e-commerce kind of retailer. So I think SOC is important regardless of that. On the smaller end, maybe your SOC is just one person who's on call all the time. And on the higher end, it's 24x7 team with lots of different options in the middle,

Dusty (02:51):

Also, there's MSPs who kind of serve as a SOC-as-a-Service where either they can be initial investigation or triage however you want to have them perform that capabilities, but that can take some of the pressure off of your yourself as a company to look into the initial investigations, as well as a lot of the time these MSSPs have a lot more experience looking at the different activity going on in your environment.

Brian (03:25):

Which is probably a good point. Obviously we offer our SOC services as a service, but obviously some other companies might have their own internal SOC teams. So obviously there's many different ways you can go about setting one up. Do you have your own? Do you have provided for you? Is it a hybrid of both? So a couple of different ways you can look at that problem and how to solve it. Maybe we can talk about the benefits of doing each one of those.

Steve (03:55):

Yeah. And I think it's important to kind of distinguish what we're talking about here, because you know, for a lot of companies, the security is one team is one department, and that includes the people who are running the running the security tools and also responding to alerts and also making policy decisions and also doing deep investigations, if something really bad happens. But, you know, that the SOC is one specific function inside of a security program. And for some companies on the, on the bigger end with a bigger security team you're going to have people who are dedicated to functions like SOC, which is kind of a tier one alert, triage, basic eyes on glass kind of function versus an incident response team who's gonna do deeper dives into confirmed, I don't want to say incident or breach, because I know that those are scary words, but confirmed events or issue that needs deeper investigation. Then you're also going to have, you know, threat hunters and threat Intel experts and it may be that in your business your security team handles all of those roles. We are specifically talking about the SOC role today.

Austin (05:07):

I guess, like what kind of expectations should you have when you're looking to choose starting your own SOC versus going with say an MSSP for a SOC?

Brian (05:20):

I think Steve kind of touched on that at least initially you know, the different breakdowns that you can have as part of the security program that you can have. So yeah, like you said expectation-wise, if you have an internal SOC or an external SOC do you want them handling multiple tasks out of that pool? Do you want to do triage and deep investigation and threaten intel? So delineating exactly what that team will do and if they'll work with others whether internal or outsource or handle it all themselves is definitely a good first step in kind of drawing up a plan on what you want.

Steve (06:05):

Another important thing you have to do up front is you have to decide you know, what kind of coverage you need your SOC to have. So maybe you need that to be 24x7. Maybe you don't. Maybe security events can wait until the morning in your line of business. I think that's probably less common, but I'm sure there are scenarios where that applies. And really what what kind of budget are you working with because that's going to affect how many people you can hire–can you, can you staff 24x7 or do you need an on-call rotation? And on-call rotations for a SPC can be difficult because you know, you're trying to strike a balance between, you know, monitoring enough to avoid the kinds of scenarios that you want to avoid, but not alerting on so much, especially with on-call team where you're overwhelming them. And so what we often see happen is you know, companies will only notify the on-call person of critical priority events, but the initial detection that a SOC receives could be a lower medium that upon investigation is actually that critical event. So there's, there's definitely visibility concerns as you start to explore what kind of coverage your team needs and that's a good instance where you might want to explore partnering with somebody who can provide that 24x7 coverage if you don't have the staff to do that.

Brian (07:28):

Well, in addition to staff too, budget would also help you determine, you know, what kind of tools you're going to have available obviously to get visibility into different parts of your company you might need to be purchasing software or platforms or hardware to kind of host those or spin the different tools up such as like antivirus or different monitoring tools. So I'm sure that plays a big part and budget as well. I mean, you might be able to speak more to that Steve than I can.

Steve (07:55):

Yeah, that's absolutely true. And it's you know, part of the cost of a security program in general, outside of just the people. But yeah, that's, I mean, that's, again, if we're talking about how you make those make, those are what you need to consider upfront before you make the determination of how you want to build your SOC. One of those is what are the, what are the platforms that you expect the SOC to use? And then is that something, you know, you can procure internally, is it something that you rely on a partner to provide? And, and you know, what, again, what kind of, what kind of coverage do you want, are you paying for the latest, greatest endpoint monitoring and also the latest next-gen firewall, and also are you doing SSL decryption? And these are all things that provide additional coverage, but have a budget hit. And so there are things that you need to consider as you decide what data your SOC is going to be monitoring.

Brian (08:51):

Yeah, that's probably a good segue is as far as budgeting, what kind of tools are you going to get, or what kind of data should you be monitoring from a security perspective? I mean, obviously we, I know we have certain focuses on what we build with when we're working with customers, but maybe we can talk a little bit about the different types of data you should have visibility to, you know, regardless of whether you're handling it yourself or outsourcing it.

Austin (09:14):

I believe that's where our Big 8 PDF that we have kind of comes into play–things like proxy logs, firewall logs, network logs, end point, you know, the more and more that you have visibility to, keep in mind as well that if you're going to be rolling your own SOC, that's more things that you're going to have to keep up with and maintain adding to the additional complexity of keeping your SOC program running.

Steve (09:39):

And I think just as important as you know, the data is really having a comprehensive picture of everything that you own. Yeah, one of the scariest things is, you know, you collect all the data and you think you've got total coverage, and then you find out that, Oh, the business has this, this other division that, you know, kind of runs itself. And we don't really think about it very much except that their credit card processing system just got compromised. And where are the alerts for that? And it, it turns out that it's, it's something that you hadn't considered in your, your data inventory. And so that's important too. It's not just which types of data, but where are all of the places that provide that data and making sure that you don't have any corners of the company that are unmonitored and exposed.

Dusty (10:23):

I mean, I think the recent SolarWinds Orion compromise shows the importance of knowing your assets. I have heard via Twitter and other sources, how companies who either didn't know if they were using Orion or where it was being running. So when you hear of a big compromise, like the Orion Sunburst one, if you don't know what you're running on your systems, you have no real starting place to look into whether or not you might be impacted.

Brian (10:57):

Yeah, that's a good point. Like I know definitely from my time in the SOC like, especially as a big part of working with Splunk, like we do the like assets and identities knowing what all your systems are, you know, what their addresses are, what your, what your different networks are, as far as like who your users are, you know, what departments, if they have different, you know, obviously their manager or their contact information, having all that information, at least for our purposes, like helps us as an external service, get a better understanding of perhaps an environment. And even if you weren't, didn't have an external SOC, if you don't have one team handling everything, being able to have that kind of information available to the people responding to your events or issues or whatever you're calling them is a big key and I think ensuring a good flow information when something happens, if they have to second guess if someone has to second guess themselves every time they see an event you know, what is this machine, or, you know, whose machine is this, or where can it be found in the company? I think that definitely throws a wrench in the works. If you constantly have to ask those questions, every time something happens. So definitely building out a good picture, both for yourself and if you're working with an external provider on, you know, what hosts do you have? Where are they? Who are your users? How are they connected? The more of that you can build out the better.

Steve (12:24):

Yeah. I think every organization has some amount of tribal knowledge. That's you know, just floating around in the minds of everybody who works there and who's been there for a little while. And that's definitely one of the challenges is whether you're building an internal SOC or partnering with an external SOC, unless you're going to only repurpose existing employees as SOC analysts, you're going to have to hire new people who aren't going to have all that knowledge and establishing the place where you're going to keep track of those things and making sure that it's a standard process to keep it up to date is a really important step. And it's certainly not, I certainly wouldn't call it a requirement of implementing a SIEM, but you you are setting yourself up for success better if you have all of these things. Not even, not even fully implemented, but just, just have them in your mind and have some awareness about them as you start implementing your SIEM so that you, you know, what you know, and you know what you don't know.

Brian (13:24):

Tongue twister there. And even a good flow from that too, is once you know, what you have then figuring out exactly what are the biggest things that you want to protect or monitor, or, you know, just in general, keep an eye on. What are, what are your family jewels per se? What are the most important things? You know, I think you've, you've said it before Steve, you know, if this, if this were to break tomorrow, you know, are you as the company now out money or is the company sunk? You know, what are the most important things to be monitoring? And having those obviously mapping out your, your assets first helps with that. But then obviously I think as a next step is then determining what your, what your priorities are in relation to the security while you're building on top of that.

Austin (14:08):

Even on top of that you know, sometimes you're required to monitor certain things. If you're in a PCI environment or a healthcare environment, there's certain things that you have to monitor. So you kind of have to roll that into, you know, what you're planning to keep an eye on.

Steve (14:24):

I think Austin, and that's a good point that, and that we kind of didn't talk about and that's, you know, what is, what is the goal of your SOC? Because, you know, in some cases, the goal of your SOC may be to, you know, have better visibility into things and respond to security alerts and make sure, you know, lower your time to detect and time to remediate and those kinds of big metrics. But sometimes, sometimes the goal is that you have a requirement from an audit and that's, that's a valid use case for having a SOC, having a SIEM. And it's, it's something you should be honest with yourself about if that's the only reason that you're doing it, then that, that just kind of guides your decision making along the way. And all of the, all of the choices you make are about what's, what's in scope for this audit and what are the audit rules and what is the audit, or what is the compliance standard we're looking at require us to do, and you just follow that path. But if goal is more general holistic security, then that's where you know, you're not making decisions based on the compliance. And hopefully the decisions you make that are the good security choices you want to make, hopefully those line up with your compliance. And if not, you need to kind of plug the gaps somewhere along the way. But identifying that the goal of, of the SOC program is just as important as any of these other conversations we've talked about.

Brian (15:45):

Yeah, that's true. And an audit can definitely provide like a roadmap for your initial use cases, get the ball rolling per se. You know, obviously Austin mentioned PCI, so maybe you have, you know, maybe you're doing sales and you need to protect credit card information, or you know, you're in healthcare and you have to present patient information. That can be your initial compass. The point you throw is, okay, do I need, I need to protect or any day, keep an eye on authentication. For example, one of our, one of our Big 8 that we mentioned, who's logging into what, you know, is it allowed, is it is expected. It can definitely kind of point you down the road of where you should start keeping an eye on things or what to keep an eye on per se.

Dusty (16:37):

Also try to figure out a way to get metrics for what you've been doing. Because one of the biggest things you hear about IT security is that it's a sunk cost where you only see the cost if you're breached. But if you are able to create metrics that show the value that you provide, that can either help maintain the budget you're getting, or even increase it so that you can do more with your monitoring and such.

Steve (17:13):

Yeah. The the paradox of being in charge of a SOC is, you know, your boss comes to you and says, Hey, we're not handling any breaches. We haven't, we haven't had any major incidents. What exactly are we paying all these people for? But then also when you are handling a bunch of breaches, the boss comes to you and says, Hey, why why are we having so many of these things? What are we paying everybody for? So, yeah, having going into this with a set of criteria that you think define what success of your program looks like, I mentioned time to detect time to remediate. Those are, those are metrics that matter whether you have a SOC or not, and some improvement on them, maybe what you can use to justify the budget requests. Whether at some point, somebody has got to answer to a boss who signs a check and the more, the more things you can point to that were not good before and are good now, the more you can continue to justify that, that cost to the business.

Brian (18:09):

But if you're just starting out though, and you don't have like a platform to already gauge those metrics, I mean, like, what would be your, how would you maybe initially justify starting a SOC or building a SOC, whether external or internal one or an external relationship?

Steve (18:25):

I think that's where you start to get into something along the lines of risk management. And that is definitely outside of the scope of trying to have this conversation. But I think, I think in general, what you, if you're, if you're trying to start a SOC, you probably have a reason for it. And maybe that's just that, you know, you know that you need a SOC and you don't have one now and maybe it's in response to you, you got breached and the company wants to spend money on security to make sure it doesn't happen again. Or maybe it's a compliance or audit requirement, but you know, that that idea is coming from somewhere and think about it from what problem are you trying to solve? And, and the metrics will come from there. If, if the problem you're trying to solve is compliance-related, then you know, the metrics to success are, do we check all of the boxes for, for the compliance standard? If the, if the motivation is the business got breached and we want to you know, we want to improve security, then see if you can find a way to measure how many incidents did you have last year, and how long did it take you to detect them and to fix them compared to now you can measure that in your SOC program and see those numbers go down over time. So tying that back to the motivation, I think will help you figure out what were the metrics that you need to measure come from. And what, you know, you made it identify metrics up front, and as you start to measure them, they don't make sense, but you discover new ones that make more sense. And, you know, like I said, measuring with just volume of alerts is kind of a paradox because neither end of that spectrum is good, but measuring with time to time, to contain time to remediate the, the metrics that are in the, you know, most of the incident response frameworks that exist. Those are very common ones to try to decrease over time. And you may not have a baseline to start with from before you had a SOC, because you haven't measured those things before, but measuring them as you roll out the SOC to show improvement that's I think how you would try to do that.

Brian (20:26):

Yeah. I think that's where I was kind of coming from. Obviously, if this is a new endeavor for you, what do you tend to, what would you focus on versus if you already have a team and trying to develop metrics around how that team is doing?

Steve (20:37):

Yeah. Unfortunately, if it's not something that you've tracked in the past, then you know, you could try to go back in and recreate some of those metrics, but it may just be better to start fresh and move forward with measuring that, you know, just decide today, we're going to start measuring that. And even if, even if you haven't started building your SOC program yet you can still, you know, I've seen people do it in Excel spreadsheets, or word docs or SharePoint or Google docs, or, you know, any of those options, just start recording what you do and how long it took. And you know, as you, as you get to build the program, you can formalize that a little more, but there's no reason you can't start collecting that information now, as you, as you start preparing to build out a SOC team,

Brian (21:22):

Well, let's say we were going to build our own internal SOC team. You know, assuming we didn't have one or knowledge already, where would we start? What do you guys think? What do we need to figure out first?

Dusty (21:32):

Probably what are most important, I guess what our crown jewels are in the company, like, what is the one thing we do that needs protected the most? If, for example, if we're a healthcare, probably the PII we have, whether it's customer or employee data that does not need to be leaked out. So finding how to protect that data first and foremost.

Steve (21:56):

Yeah. I think, I think that's a good point. See, but where that becomes especially difficult and why this is not an overnight kind of project, you know, let's use PII as the example and whether that's health information or credit card numbers or employee information or customer information, it's, it's PII is PII. And you, you start to think through this and okay. So that's the thing I need to care about most. Okay. Where does that data live? And then you identify the application where that data exists and you identify the database server where the back end data lives, but that's not, that's not everything. You know, that data flows into the application and it probably flows out of the application. And the next thing beyond just identifying that data is identifying the flow of the data and what systems are accessing that data, what systems input the data, what systems output the data. How does it flow across the network? Is that encrypted or is that something we need to monitor? What about what, you know, what firewall does it flow through? Is the web app, is the application a web application that has a proxy in front of it? I think it's, it's more difficult, I think, than just identifying what the data is. And you have to start mapping out all of the, all of the things that actually touch that data.

Brian (23:16):

I was just gonna say it's more of an initial question, I think, and then that leads to all the additional ones that you're getting into, I think.

Steve (23:24):

Yeah, absolutely. And I think that process, once, once you start going through that process, you have to start considering the criticality of things, you know, one of the, one of the biggest initial steps of going through an audit is how do I minimize the scope of this audit as much as possible? And, you know, as you start to see all of the places that these, that the data flows, even if it doesn't exist permanently there you have to start ranking things. And how important is monitoring you know, the application and the database are probably the most important things to monitor, but what about the, how important to you is it to monitor the desktop where employees enter that data or retrieve that data? It's, it's easy. It's easy to get into the trap of, well, all of it's critical. I have to care about all of it because that's, that's impractical, especially as you start out, but even as you grow you can't care about everything to the same level and you have to start ranking it. And that kind of goes into your, your asset management plan and, and which things are the most critical. And those are the things you have to focus on first.

Austin (24:35):

Yeah. And as we were talking about earlier, definitely having a list of assets will help immensely there.

Brian (24:42):

Well, and obviously if we're, if we're hypothetically making our own, our own SOC here for sake of conversation, you know, do we have, do you have one team? Like we mentioned before doing all of that, you know, looking at the servers, looking at the network, looking at the, you know, trying to look at the information itself, or are you breaking it down? Is your, is your SOC choice going to be working out of a SIEM product? You know, in our case, you know, such Splunk or others to look at that information, are they working with other teams, you know, where, what is, what is the limit on your SOC going to be, which then kind of I think works into, like you were mentioning earlier, Steve you know, coverage. You know, are you, you're always monitoring the servers 24x7, do you all want to know that any incident something happens? You know, can it wait? You know, how much of it, how big does your team need to be? I'm just trying to think, think of a, think of how we would be spinning up this hypothetical SOC of ours.

Dusty (25:41):

And also something to consider with that is contracting with a customer, like a client like us, where if you can't provide the 24x7 coverage, that's one thing we do provide is 24x7. So you don't have to worry about having that monitored all the time because you contract it out.

Brian (26:03):

Right. And again, if you are contracting out or you, you know, what level are you, you've kind of you using the external service for? Is it something like, again, and then there's triage? Is it something where that service will work all the events and, you know, give you the reasons like handle remediation as well, and just give you the results? Are there reports is it a hybrid between the two? Like figuring out that delineation as well? You know, does it make more sense to include people that have tribal knowledge, like Steve said in that process or to just take escalations from like, say an initial triage and figuring out that sweet spot for your environment, I think is another important step. You know, what other, what other tools do you need to work with? Do you have, do you have antivirus tools of your own, do you know, do you contract out that for, as a service? You know, do you have network monitoring view you go outside for that, you know, do you have expertise within your company along those lines, or do you need to basically borrow, you know, buy it from the outside figuring out what the tools with the software and hardware that you need and where best to get that goes hand in hand with what kind of staffing you're going to need internal or external as well.

Steve (27:23):

I think there's an interesting chicken or the egg problem here where you have to decide, do you want to bring in people and let people choose their tools, or do you want to choose the tools and bring in people to, to work with those? And I think both of those are good approaches. And it kinda just depends on how quickly you're going to hire people. And, you know, are you hiring, do you have the budget to hire people with a lot of experience? Are you, you know, is it something that you have to do on the, on the entry-level side? And so you need to provide, you need to make those decisions for them. Are you hiring Level 3 analysts, or are you hiring Level 1 analysts really? And level three analysts. I think you can hire them and have them select the tools themselves and level one analyst. You're gonna need to do that for them. And, and then you you know, it's really just evaluating the data and the tools you have and what do you need on top of that? Can you repurpose the tool you already have to fill a new need rather than you know, spending budget on, on a new tool? And I think that's, especially if you're a smaller, if you're a smaller company just starting out on this path, I think reusing the tools you have in some way, so that you're not you know, you don't want to have a day one SOC budget that's the same as somebody who's been doing this for 10 years, because that's going to be a huge sticker shock to the business. And so what ways can you reuse what you have to accomplish your goals, prove value, and then get the budget you need to start getting, you know, best in class tools to fill those, those holes.

Brian (28:55):

I think I think another key point to that, I don't know if we touched on yet or not, regardless of whether you're doing it all in, you know, in-house, hybrid, or externally, is a documentation, lots and lots of documentation. You know, if you've run into a problem before you know, document what was done, so you don't have to reinvent the wheel the next time it happened. If you've, you know, if you've used the tool or seen a tool, you know, documenting that to see, you know, for future reference, whether it's a new hire that you're, you're showing the ropes, or you know, just an additional asset that your existing team can use, just avoiding brain drain. If, you know, you have higher that, that leaves, and you have to replace them, you know, documenting both your network and your process and you know repeated issues that come up all the time, you know, anything you can do to avoid having to repeat a process over and over I think is another big, important part of any SOC really. So documentation, documentation, documentation, documentation.

Austin (30:07):

Yeah, that documentation is really gonna play off for like, say you get an alert for repeat failed log ins for a user, or some vulnerability scanner. Okay. So this alert fired, what kind of steps do I have to follow, or what steps were followed in past alerts to kind of guide me through this alert? So documentation definitely is going to play a big role in that.

Brian (30:27):

Right, whether, you know, whether you call it like a knowledge base or, you know, if it's through a ticketing system or whatever works best for your environment.

Steve (30:38):

Yeah. And I think it's, whatever works best is a good way to say that. Because it's, it's whatever, whatever you're going to use, right. Don't implement something brand new that nobody's ever used. And you're going to have a bunch of organizational resistance to using, because you want this to be accessible to as many people in the organization as possible because you need it to be as up-to-date as possible. So maybe you have some system already that you use and you just piggyback on that. Maybe you find ways to import existing data into something new, but it should definitely be something everybody can, can readily access readily update. And we'll actually use.

Brian (31:14):

Yeah, because out of date information, isn't helping anybody. So,

Austin (31:18):

And then, yeah, this information changes daily, new things are added, new stuff is added to the environment your notes need to be added. So it definitely needs to be something that's easily accessible.

Brian (31:32):

I would definitely agree.

Steve (31:34):

Yeah. And, and the, the last thing I would say about documentation is not only is it something that you need to make sure everybody can readily access, but you have to make sure that everybody is always checking it because what, what can happen a lot of the time is an analyst can get in the rut of, I have handled this the same alert 10 times this week. I don't need to read the documentation, but the 11th time is when the documentation was updated to say you know, that this is a critical incident and needs to be escalated immediately. And if that's not, if the analyst isn't reading that documentation every time to see if something changed you're putting yourself at risk of again, operating on out of date information.

Dusty (32:17):

That also plays into communicating communication with that documentation. So whether it's emails or some other type of communication to whoever is impacted that Hey, such and such changed, and this is a new process just finding some way to control the spread of information easily so that it's not stuck in one person.

Brian (32:45):

Is there anything else that we can think of, you might need to, let's say build your own SOC? Obviously we've got figure out your stuff, figure out your tools, figure out if you're doing it all by yourself or if you're getting some services externally document everything figure out your, you know, figure out your, your environment and document that. So it ties back again because it's so important, you know, into your assets and identities again, you know, what do you have, who do you have? And then obviously figuring out what your direction for detection and protection is, whether that's coming from an audit or from past experience. Uh so you know, what you should be looking at, or what your important things to be looking at are which then can lead to what kind of data do you need and you know, what can you see now? What are you missing? What you need visibility to. I know that's a, that's a mouthful, a laundry list to go through, but anything else that you think we might need to add things to think about for building your own SOC?

Austin (33:54):

I mean, it's heavily customizable. So obviously one solution is isn't going to fit every single company. So, like Brian just said, you're going to have to go through and play with different things. Like, you know, is this documentation the way that we're handling it? Is it working? Yes. No. If it is great, if it's not then get rid of it, find a different solution for that. Is our desktop EDR system let's say for example, you know, this antivirus is this, is this working properly for, is it giving us the logs that we want? If it is again, great, if not, then swap it out. It's going to be a lot of playing with it, if you're trying to roll your own SOC.

Brian (34:39):

Trial and error as it were.

Heather (34:42):

Alright. Well, thank you for helping fill us in on SOC team nuances. I appreciate you joining me today.

Brian (34:55):

Thanks for having us.

Heather (34:56):

For sure. And that's all for today. If you're interested in partnering with an MSSP, you'll definitely want to check out our next podcast. This same team will be coming back to talk about the best practices for building and maintaining an effective relationship with an MSSP. So stay tuned and we'll catch you next time. Bye