Heather (00:13):

Welcome to the Hurricane Labs Podcast. I'm Heather and we're back with part two of Designing a SOC Team. So last time we talked a little bit about why we need a SOC team and what sort of considerations should be at play when setting up your SOC team, what sort of assets and identity management what you need to protect what sort of data you need to be collecting. Now I have our team back here today to talk a little bit about how to establish an effective relationship with an MSSP. So, thanks. Welcome back. Thanks for joining me again.

Brian (00:49):

Thanks again for having us. Again, my name is Brian Karrigan. I'm a search developer and former SOC analyst and architect.

Dusty (00:59):

I'm Dusty Miller. I'm a Tier One Analyst. I help with handling daily alerts in the SOC.

Austin (01:05):

I'm Austin. I'm also a T1 Analyst with Hurricane.

Steve (01:08):

And I'm Steve. I oversee our security operations team.

Brian (01:11):

Alright. So last time we talked about kind of building up your own internal SOC. And today I think we're going to discuss what aspects you're looking for in a relationship with an external provider and MSSP, as it were. Maybe we'd start out talking about what you would imagine would be a successful relationship. What are you expecting to get out of a contract with an MSSP such as us? Steve, we'll serve this one up to you first.

Steve (01:40):

Yeah, so I think that's a really good question and you know, it's something that we constantly iterate with our customers. But to start with, I think it's important to know what your performance objectives are for the team. And you can be very operational at first, as you start to build this out. And that may just be how many alerts are you handling? How long are you taking to return those back to us? Do you have an SLA, a service level agreement that says you're going to get them back to us in a certain amount of time and, you know, are you measuring them against that? And then, you know, as you start to mature and you have a working operational arrangement, then you can start to evaluate as the service provider helping you grow the value of your program, are they bringing new content to the table? Are they providing feedback on what you could be doing differently? Is the detail in the alerts that they're sending you, is that sufficient for what you need? Is there something that you could do differently there, and then alsojust straight simply talking about the integration between you and your service provider. Is this something where you kind of just ship data off to them and when you need to when something happens, they send that back to you, or is it something more like, you know, you're operating out of the same platform, looking at the same stuff have access to the same data. What does that integration look like and how well is that performing? And much like we talked about just in general, as you build a SOC is you, you need to know what you're measuring and what you're improving over time, so that you can

communicate to the decision-makers where the, where the money is going and why they may need to spend more of it in the future.

Austin (03:25):

Communication definitely is going to be a big one. You know, communicating what you want that team to do when an alert, fires, how you want them to handle things, and that goes back to documentation, just as we said, in the first episode, just documentation of everything is going to be a very, very key to maintaining a successful relationship with your MSSP.

Brian (03:47):

Right. I was going to say communication right before you jumped in. And definitely in all aspects, not just around, I would say alerts themselves, but also, you know, like we were talking about for success criteria, you know, goals, what are the goals? Do you want new use cases? What, what are those use cases? I think good communication between both teamson what do we have, what do we need, what is important? What is not a good flow of back and forth will definitely be important, because obviously when you're working externally, the external team doesn't know your environment, as well as you do. They might not know immediately, you know, what the important bits are, what to look for, you know, who to contact you know, what's, what's expected what is not. So a good back and forth both about, you know, not just what's actually happening, but what you're looking for, what should you be looking for? You know, what do you have versus what do you need, just communication at all levels? I think, you know, seeing the people working the alerts between the management of those people just between the businesses themselves. Good communication.

Austin (05:07):

Yeah. I mean, without that essentially you're not getting your full value of a MSSP. You're kind of just buying SOC services to check a box, or like having a SOC and having that communication definitely is going to aid the relationship that you have.

Brian (05:25):

Right. And I know when we talked about building your own SOC, we talked about kind of staffing and coverage levels you know, are you 24x7? Is it only working hours? So, you know, if you're working with an external provider, you know, are they, are they filling the gaps? Are they, are they only providing, like, let's say nights and weekends holidays you know, are they, are they working side by side with your team? You know, what's the scope of their coverage? Figuring, you know, it goes back just like you're figuring out staffing internally, figuring out what kind of cadence you're getting coverage from your provider, I think is another big part and communicating those expectations.

Steve (06:18):

Yeah. I think ongoing communication is a big thing because you know, those expectations may change over time as well. You know, initially you may need more help from your provider, but as you get to, you know, staff up your SOC, maybe, maybe you only end up needing them overnight weekends or things like that. So making sure you have constant communication with the service provider to, you know, just to reset your expectations, to make sure priorities are aligned. Those are really important communication lines to keep open with the service providers so that you know what they're expecting, they know what you're expecting.

Brian (06:57):

I think along both those lines as far as like expectations and communication, you know, how is that communication occurring? Is it just via email? Do you have escalation via phone calls? Is there a ticketing system that you use? Is there a ticketing system your provider uses? Do they work together? How, how are you sharing the information from an alert or a question about the environment? So definitely ironing out those details for what works with your environment.

Dusty (07:31):

I also feel like being open to some form of automation is important. A lot of times you see customers who might need stuff escalated specifically for compliance, but it's not necessarily something that needs to be investigated. And that would be a good opportunity to be able to just have some automation in place to cover the compliance, but not add extra work for the people working the alerts.

Brian (08:06):

You need to know what happened, but you don't need to know why it happened per se.

Dusty (08:09):

Yes.

Steve (08:10):

Yeah. I think that's really common. It's something that we've encountered in our own compliance program as well is that there are things that have to be, you know, they have to be ticketed, they have to be documented, but they don't necessarily have to be investigated. And you know, a common thing is if you're auditing change control or actually that's probably the best example is if you're auditing change control, there's not really an investigation for the analyst to do. You need a ticket that says we detected this change and you need the people who make those changes to either say, "Yeah, we did that, and it was approved" or, "Hey, we didn't do that. We need to dig into it." And maybe in that case, you need to start a security investigation about, about, or how this change happened outside of change control. But you can almost look at it like the security detection you have in place needs some additional input that only can come from a human answering a question. And so it's an extra step before a security investigation needs to happen. So yeah, I mean, I think it's important as you work with your service provider to understand what their level of customization is. And so is that, you know, you can provide one escalation runbook and that's it, and they will follow that for everything, or can you get granular? Going back to the ticketing system thing is that, you know, are you expected to work from their ticketing system? Are they expected to work from yours? Are you integrating too? Just understanding, you know, what level of customization customization they can provide and what level of customization you need. And maybe initially again we talk about this whole thing is an evolving process. Maybe initially you don't need a lot of customization, but over time, you know, you have specific requirements that you build into your program that you need your service provider to be able to adapt to.

Brian (10:03):

And not only integration between ticketing systems, but, you know, depending on the nature of the relationship, for example, is the external SOC just looking at events? Like, do they have access to a SIEM? How do they access your SIM? Are they hosting it or are you hosting it? Is there any expectation of remediation? If so, how, how does the external team access your environment? Do they connect via

VPN? Do they have their own credentials? Do you give them credentials? You know, if, as soon as it goes beyond just a communication aspect, there's a lot more like nitty-gritty details on how the relationship between the two environments is going to occur. I know authentication alone can sometimes be a headache between two organizations.

Dusty (11:00):

Also, having well established boundaries of where the MSSP is going to take stuff. So knowing if the MSSP does incident response or we'll handle malware outbreak, like what the end point of their coverage is, if they're just doing the initial investigation, or if you can also contract with them to handle any incidents that may happen.

Brian (11:34):

I think that all comes back to, again, communication, again, as far as pushing out, you know, documenting what the process is, documenting what the goals are communicating, you know, figuring out that success criteria we started with you know, what the goal of that relationship is. And just like Steve said the, you know, certain parts of the process will evolve over time. You know that expectation might evolve over time too, you know, more than just triage, maybe more or less, perhaps, like I said, if you're building out your own team and in relation to an external relationship, you know, you might slowly scale back on what you expect the MSSP to do for you, but always communicating what that goal is documenting, documenting, what that process is. Because a lot of times that could change as well when you're dealing with an external group. You know, maybe you're sending events or communication to one person, and that person leaves so communicating that process of documenting how that's going to change. It all kind of, it all sounds like the same points over and over, but they all just, they're all inter networked and on how that relationship is going to work.

Steve (12:58):

Yeah. I think all of that kind of comes back to how you view the partnership with the provider. And, you know, you may consider them almost like, I don't even know the word I want. So I think that comes back to how you want to view the relationship that you have with this external partner. And you may view them as just kind of a disposable, interchangeable, expendable service provider whoyou know, if you don't like the work they do, there's a half a dozen more that you've already talked to you and are ready to go, or you may view them as you know, some kind of a value add providerwhere they're selling you a product, but then providing something on top of that. All the way up to you may consider them a complete security partner. And I think how you view that is going to dictate how, you view that integration. I think you're probably less likely to do fairly deep, detailed, complex integrations with somebody who you think is easy to replace if you don't like the work and somebody who you really, really view as a strong security partner. I think you're more willing to open up the integration points there. So I think that's a big factor in general is how you view that partnership

Brian (14:19):

That could almost lead to another good point is, especially if that partnership was along the lines of a disposable one, like you mentioned, is what happens when you end such a relationship? Like obviously both organizations have their own information access, et cetera. So how do you cleanly break something off like that and avoid problems such as brain drain and, you know, loss of institutional knowledge? Or IP,? What's the best you being managing relationships might have a good, a good insight to that.

Steve (14:53):

Yeah, I think IP is an interesting one that is, you know, a little more contractual than even I could necessarily talk to you completely. But I think it's important to understand where all of the ownership of all of the content that comes from your relationship belongs. Do you own that? Does your provider own that? Is there some kind of shared ownership and understanding that even if I can't guide you one way or the other understanding that I think is important to knowing what things will look like at the end of a relationship. I think brain drain is a concern, if you're not communicating well with your provider or your provider's not communicating well with you. But if you have that robust communication back and forth, then hopefully there is no big knowledge transfer at the end of a service engagement. You've been working from the same set of documentation this whole time. And you take your copy and the provider takes whatever's theirs or destroys it, or whatever your contract says. And that's, you know, there's no knowledge transfer to be done because you are, you've been doing that incrementally throughout the whole service. If that's not the case, then, you know, yeah, you're gonna need to plan for some kind of a brain dump knowledge transfer at the end, so that you can get all the information the provider has about your environment. But you also need to consider things like who owned the platform. Is it something that the provider gave to you as part of the service? And now you're losing that and you have to consider, you know, do you have compliance requirements for how long you keep data for, and will that be impacted? So lots of things to consider there, and I wouldn't wait until the end of our relationship to consider them. I think that's a conversation you shouldn't be afraid to have with your partner along the way is, is what happens if this doesn't work out? What happens if you know, we have, we have to cut budget. What happens if you transition to a different service model? Like there's lots of scenarios that aren't just, you know, your provider sucks and you don't want to use them anymore to consider when you consider, what is the end of this relationship look like? That could even be that you decide, you know, your plan for growing your maturity says that after three years or five years, you should have your own internal 24x7 SOC. And, and if I thinkif you have a good partner in your, your external SOC provider, then that's a conversation you can have with them and say, look, this is our goal. This is, we all, we want to be upfront and honest with you that this is our goal, and that way they can help you achieve that goal. They don't have to be there to, you know, just, just if all you need from them is to support you along the way until you have all these yourself, that's fine. But but finding a provider or finding a partner who can help you achieve that goal of having an internal SOC is an option as well. And I think having open and honest communications with security partners is critical to the success of any kind of engagement like that.

Brian (18:07):

And again, it always comes back to communication. But also, you know, like you were saying, like having that kind of information or conversation being a part of your even initial like success criteria for the relationship, like you said, if it's a goal that it's only going to be temporary. So, you know, building that into the process from the get go is like, how will it, you know, how you guys kind of decouple at the end, or even not even if you expect it to be open-ended, like you said, planning for, you know, a worst case of, you know, needs changed and the environment, or the relationship is no longer practical for whatever reason, you know, costs or platform or otherwise, like I said, planning for that from the get-go or at least having the channel of communication open to discuss it, I think would go a long way versus, you know, a sudden drop-off and a scramble to replace lost knowledge or lost capability or staff you know, on a time crunch.

Steve (19:08):

Yeah, I think that's really the thing is that all of the communication you have with your provider is to avoid some kind of scramble at some point. You want to communicate your success criteria to them so that they know what they're, what's what you're expecting of them. And there's no scramble at renewal time so that they can try to meet these expectations they didn't know about. And you're communicating about how you need to integrate and how you need things escalated and what information you need from them. So that you're not scrambling when a real security event comes through and you don't have all the information you need. And you know, you're continuously updating documentation and having those conversations so that if the relationship doesn't for one reason or another, you're not scrambling for a knowledge transfer. So you can, you can certainly approach the relationship where you're just going to scramble in those events if necessary, but a really truly successful when I think is going to have much more constant communication.

Heather (20:09):

Alright. Well, I think that about covers it. Thank you very much for joining me again. We appreciate it.

Austin (20:17):

Thanks for having us on,

Heather (20:19):

And that's all for today, folks. Thanks for joining us. And until next time stay safe.