Speaker 1 (00:16):

Welcome back to the Hurricane Labs podcast. I'm Heather. And today we'll be talking all about the MITRE attack framework. So this framework, if you aren't familiar, is basically a map of security coverage, which helps to target specific attack methods as well as ID risk areas where coverage might need strengthening. In this two part series, we'll be hearing from a handful of our staff members who have been setting up our Mitre ATT&CK Framework, and today's show will provide more insight to what this framework is and its value to security teams to help with that. I have Hurricane Labs, owner and chief technical officer, Bill Matthews, along with SOC tier two team lead, Josh Silvestro, here with me. Bill Josh. Welcome.

Speaker 2 (01:03):

Hi, Josh. Hi!

Speaker 1 (01:05):

Thanks for joining me. So before we dive into the more technical side of MITRE we've been working on implementing this framework for a while now, how are you feeling now that it's in place and what are you looking forward to most about using it?

Speaker 2 (01:20):

Honestly, I'm thrilled. The truth is we work with a lot of different organizations. So there's a lot of, you know, from my perspective, a lot of pivoting between different types of information and trying to also pivot between a lot of different goals between different organizations. I really feel in the first couple of months, we've already been using it as well as going forward. It's going to continue to be a huge driving force between the relationship we have with our clients and getting things done and making sure they're appropriately protected. And the other thing to Josh's point, because we work with a lot of different organizations, this kind of a framework, um, with some minor adjustments helps us to have a common language with those clients. So we're speaking the same words when we talk about things, right? So when we say discovery, right, it means the same thing in the, in the context of this framework. So it really gives us a common language and I think that's very important.

Speaker 1 (02:09):

Yeah, for sure. Definitely. Why don't you go ahead and explain for us a little bit more about what the framework is.

Speaker 2 (02:17):

So basically what it lets you do is break down what logs, what information you have based on the attack or threat vector, or whatever fancy word you want to use. And so they break it down into 12 different sections and a point I want to make strongly here for our clients and for everyone else is you are never going to complete this matrix. It's you're never going to be a hundred percent. You simply don't have all of the things that they've, that they've covered because they've tried to cover across a lot of industries, right? So if you're a manufacturer, you're not necessarily going to have cash register logs. If you're a retailer, you're not necessarily going to have industrial control logs or something like that. So you have to make sure you pick and choose the things that really, really affect you. Right? So, um, for example, we don't use windows at all here, so we're not going to have windows management instrumentation. So one of the things we get is, well, why don't we have that? Well, because you don't do that. Um, so if you

don't do it, you're not going to have it. That's very important because it really does cover a broad area in these 12 sort of sections. So I don't know what Josh wanted to say about that, but that's, that's my opinion on it.

Speaker 3 (03:38):

Yeah. And to your point, about a hundred percent coverage, even if by some chance you're able to complete a hundred percent coverage. Something to keep in mind is this is just looking at known and common attacks. So if you're able to a hundred percent complete this map, doesn't truly mean you're, you're a hundred percent covered. That's technically never achievable, but it gives you a really good coverage and a good starting point. And from a high level, what's great about the MITRE attack framework is it allows you to, you know, look at the process through the attack chain from like initial compromise to fully compromised and, you know, data being stolen and exfiltrated from your environment and being able to break it down into areas of ways to detect that along the way and make sure you're fully, you know, trying to get a good coverage of your entire picture, opposed to, you know, becoming organizationally focused on one column, which kind of leaves you blind to potentially the rest of the attack and your network.

Speaker 2 (04:29):

So like one of the big focuses are, yeah, I see a lot of people talking about now is lateral movement and, um, all of that. So if you pay only attention to that, but you're not paying attention to let's say credentialed access, um, you can get into a lot of trouble there because credentialed access sometimes is more important to stopping lateral movement than detecting lateral movement. So that's one thing. The other thing that the MITRE framework really isn't is it does not measure the efficacy of the coverage you have. So you might have a happy blue thing in your, in your Splunk dashboard, but you have to make sure we're testing all of the, um, effectivenesses of the actual coverage. Right. So, okay, great. You have logs from your firewall, but what are we doing with them? How are they being used? How do they break down across these 12 sections? Um, that sort of stuff we need to make sure we're still not losing sight of how effective the alerts are around these sections.

Speaker 3 (05:29):

Yeah. And I guess while we're talking about things that aren't being covered by this or things you really need to keep in mind, um, again, just checking the box doesn't necessarily mean you're fully covered, you know, if you check off the brute force box, but your search is only really looking at brute force against windows environments. Uh, you're not really covered them, even though the box is checked, you're turning a blind eye potentially to, um, Unix hosts or, you know, AWS environments, cloud environment, stuff like that.

Speaker 2 (05:55):

Right. Your web applications, even right. Just on top of checking.

Speaker 3 (05:58):

The box, you also need to make sure that that check box is truly covering what's pertinent within your environment.

Speaker 2 (06:03):

But the cool thing about it is, again, it does give you a nice high level overview and gives you at least for us. Anyway, it was an easy entry to give us a way to build a more sophisticated roadmaps for clients so that we can say, these are the things you want, here's where they fit in into the attack matrix, but here's all the things we already have. So I think that's, you know, it's very useful to help give you a focus and again, to help you sorta X out the things you don't want. Right?

Speaker 3 (06:34):

Yeah, definitely. I mean, in prior to using this, uh, framework, you know, to help develop searches for our clients, um, we do have an initial implementation list we use, which is pretty wide coverage from, you know, again, brute force accounts to some network, uh, activity, you know, vulnerability, scanning, stuff like that. Um, but a lot of our clients in organizations we work with are really benefiting in the sense that, uh, you know, just through natural progression in someone's career, they become really focused. Um, so maybe you hire on someone who is very windows, heavy, loves windows is focused on, you know, an attack they had seen in their prior job. Maybe it was, you know, um, password spraying or something like that. So they become very focused in the type of things they're looking at. And once we started rolling this dashboard out, we found no some clients who have a lot of good searches in the scheme of the actual attack framework and chain, you know, only maybe have 20% coverage and then you start to drill down and you're like, well, they've got 10 different brute force searches, but you know, the rest of the column or other things are completely ignored.

Speaker 3 (07:35):

So this has been a really good way to look at an organization, say, Hey, here's where your focus was prior to the miter attack framework. Um, you know, in parts of the chain, here's where you have detection, but here's everywhere you're currently blind, uh, in whether, again, it's a skill gap. Um, it's just not a career focus or it's just something that your organization hadn't thought about prior. It's a good way to look at the areas that, you know, should I be looking at that? Cause we do have that type of data that is in our business plan and, you know, kind of gathering that stuff to make sure again, we're not turning a blind eye to, to other critical areas.

Speaker 2 (08:06):

Yeah. I agree. And I, I mean, the layout of it is now it's the layout of it. Right? So, um, it does just give you an easy way to see all of those things and to sort of map through them. So to answer Heather's original question, it's pretty cool. And it works really well when you actually use it. Some of these things are very, very deep, so no, you can't feel bad about yourself if you don't get all of them, you're never, that's just not achievable.

Speaker 3 (08:33):

Definitely. And even to a clear cut point is if you're a very local type of business, right? Everything's in house, you don't have any cloud services. I mean, especially with the revamp of the recent attack framework, I mean, there's dozens of different, very cloud specific techniques that you just can't cover. Because that's not how your organization's currently structured. So like what strategies are we, or should people.

Speaker 1 (08:56):

Use to use this as efficiently as possible?

Speaker 3 (09:00):

So I think, um, specifically what we've been doing with clients and what we've been seeing with clients is, you know, looking at what you already have in place is extremely crucial because if you just kind of go in blind and you're not really sure of what you already have, you might be duplicating efforts in wasting time. Um, so what we've done here at Hurricane, we've helped their clients, you know, populate the MITRE attack framework dashboard within Splunk. It shows all of their existing correlation searches in what areas they're actually covered. Again, there should be some additional work you should do, you know, annual health checks, make sure the searches are running correctly, make sure they're catching any logs you've added on. Um, but assuming those things are good and being done, then really what I've been suggesting is working backwards and saying, okay, so here's the areas of your framework.

Speaker 3 (09:42):

You have coverage. Um, but let's say there's several, you know, columns such as execution, persistence, or discovery that you have no coverage. You should start some focus there. Uh, cause again, this is part of the attack chain. So if you have three or four columns where you have no visibility, but you could, um, because again, you know, your business operates that way. You have those logs. If you don't start to populate those columns with detection, you're essentially turning a blind eye. So let's say someone gets to access, um, you know, doing a drive by compromise is one of the minor tech, uh, framework techniques. Uh, but then you have nothing in execution and persistence, essentially that attacker not only got access to your network, but there's two more steps that they can do to gain a foothold that you have no idea that's really happening because you have nothing in place to detect it. So really a lot of clients have been looking at columns where they have no coverage and saying, how do we populate those things? Or if they have a wide spread of coverage saying, where do we have the least coverage and let's increase what we're doing there.

Speaker 1 (10:40):

Now you've mentioned looking at a dashboard a few times, is that our app that you're referring to,

Speaker 3 (10:46):

Correct, there is a Mitre ATT&CK framework app, which bill himself helped with. And essentially it is the MITRE ATT&CK framework is everyone knows it. So if you go to your favorite search engine type in MITRE ATT&CK framework, one of the first links will always be a nice big display dashboard that shows all kinds of techniques and, and you can drill through and stuff like that. Uh, the app within Splunk looks extremely similar. Um, so that way, if you're a, either technical or nontechnical personnel, you can go to the MITRE framework site, dig through, get all the technical information you want. Um, but you can also look and Splunk and tie those things together. So for example, if you're in the Splunk dashboard, uh, you go to, you know, the execution column, you do schedule task job. You know, it may or may not show that you have a search there, but let's say you don't, what do you do with it?

Speaker 3 (11:37):

Um, or how do you get that data? What do you need if you go to the MITRE ATT&CK framework site, click on the exact same block and the exact same column, uh, it'll dive into what kind of data you need, you know, is it windows, Linux, what kind of a host should you be looking at? Um, as well as gives you some real world examples of attacks that have been seen. So that way you can kind of get a really good idea as well as if you wanted to duplicate for testing. Here's some ideas how to do it. So really the point of that app is to tie very closely to the MITRE ATT&CK framework and give you a way to see in Splunk

what you're doing to get the coverage, but also tie back to the main source. So you can get as much technical information as you need.

Speaker 1 (12:15):

So now that this is fully deployed, what has been the reactions of our customers that have worked with us to complete the process on their end?

Speaker 3 (12:24):

Um, what a lot of our clients been saying is, you know, the truth is there's a lot of management, there's, um, exact level of people that want to know what's going on with the organization, but don't necessarily have all of the time available to become the technical resource or fully, um, engage in the product to completely understand what's going on. And we've had a lot of good feedback from execs I've worked with and in other upper management who have said, Hey, as someone that just oversees, this department has a general understanding of, um, you know, everything in the security world. This has been a great way for me to look at it and say, Hey, a lot of these things are filled in and I'm being told, they're working as expected. That means we're doing good things, right. Um, also gauging progress, let's say, um, you know, someone new comes in or there's an organizational goals shift a bit.

Speaker 3 (13:08):

If we start today, you know, in six months, in a year, in two years, what is this dashboard going to look like? And when we do quarterly meetings and stuff like that, management can look and say, Hey, my team has clearly been effective because we populated this thing from 10% up to 25% in the last six months, or, you know, a year down the road, we're 40% full. It's been a great way for, um, management people overseeing the, the different groups to know how progress is being made or more importantly, you know, being able to look and say, Hey, these things aren't filled in, let's start building direction and plans around, uh, improving our security posture within the organization.

Speaker 1 (13:46):

All right. Well, Bill, Josh, thank you for participating today.

Speaker 3 (13:50):

Yeah. Thank you for putting us together. Yep. Thank you.

Speaker 1 (13:53):

If you're looking to learn more about our MITRE ATT&CK framework setup, you can check out Meredith Kasper's and Brian Karrigan's blogs on their work with it. Check out our links for more and be sure to stay tuned for part two of the series to hear from the team that implemented the MITRE framework. Thanks for listening. We hope you enjoyed the show. That's all for now.