Heather (00:12):

Welcome to the Hurricane Labs podcast, I'm Heather and we are going to be continuing our chat about MITRE in the first installment of this two-part Miter series. We heard from Hurricane Labs chief technical officer, Bill Mathews, along with SOC tier two team lead, Josh Sylvestro who provided an overview of what the MITRE framework is and its value to security teams. Today, we'll be hearing from the team members who actually set up the framework and they're going to give us a few more details about what setting up this framework was like some of the challenges they face and what they're excited about now. So we have with us Meredith Kasper, Brian Karrigan, and Kurt Wolfe from our SOC team to chat with us. So before we dive into the nitty gritty of MITRE ATT&CK framework, what was it like setting up this framework for Hurricane Labs?

Brian (01:08):

It was definitely a bigger project, I think, than we had initially realized, but it was good in the sense that it got us a better understanding of the framework itself and how it relates to security searches and datasets, and also allowed us kind of a deeper understanding of each of our customer environments as we went through them and tried to map them to the framework itself.

Kurt (01:33):

One of the private biggest challenges of the whole thing was just the not only is the framework big, it's also the number of clients we had to go and maps searches for. That probably took us a matter of about two or three weeks to, to finish just that step up.

Heather (01:48):

Now, the framework is sort of a collection of various attacks that have been implemented, is that correct?

Meredith (01:59):

It is a collection of different attack vectors used in known adversarial techniques when somebody is either performing a pen test, conducting malicious activity on your network or running some purple team exercises. And these items in the framework are mapped to overall overhead techniques that range from the initial access to how somebody would actual trait their data and then under those are specific assets frequently used throughout this activity.

Kurt (02:34):

Yeah. I was going to say in like put it in a little bit more simple terms without all the kind of IT lingo with some of it at the end of the day from a kind of a non IT perspective that the MITRE framework is just a collection of like exploits and attacks that are actually used in enterprise environments and out in the wild that are actually effective, right?

Brian (02:58):

Like real world activity versus just a use case that someone thought up.

Heather (03:05):

So what did you have to go through in order to pull that information together?

Kurt (03:10):

First step was honestly kind of figuring out how we were going to add it to Splunk itself. Um, we had to play around with, uh, the enterprise security app a little bit to actually understand how the mapping of the searches actually worked and how we could correlate that kind of back to an app and show it on a map. Kind of. Brian did a pretty, pretty big deep dive into the ESF itself. And we figured out we could use analytics stories.

Brian (03:36):

Yeah, there's a, uh, there's an app you can get from a Splunk called, uh, enterprise security content update, which added a feature called analytics stories like Kurt mentioned, which is basically a description of a use case and a listing of the searches that are in Splunk that either support or detect that use case. And for us the important part being the mapping where you can map, uh, several different frameworks, uh, to the data, depending on what technique is being looked for in search. So for us, obviously that was MITRE. And then each story then lets you add all those sub searches into it. Uh, each one you can add the mapping of the different techniques or tactics used from MITRE. Uh, so that gave us a, basically a forum we could fill out for each search, uh, to break it down simply. And then we just had to go through and do that for, for every search that we had in production for every customer that we had in production.

Kurt (04:36):

Yup. And the theory, the initial process of going through and making the list of all the searches, I think mentioned a bit earlier, took us around three weeks. Here's the hardest part we kind of ran into, like for example, with, um, map aware, um, like malware source types and everything like your IDS or intrusion detection systems when trying to map some of the searches, the signatures themselves, or the IDS itself detect so many different types of attacks. Uh, we had to keep some of that a bit more broad than going into extreme specifics, which is possible with MITRE framework. So I think that was kind of the first challenge is finding out just how broad or how specific we were going to map some of the searches.

Brian (05:17):

Yeah. The benefit of this, the benefit of a single customer doing this is that they only have to do it for their environment, uh, the, the issue or not issue. But the, the challenge of being a service provider is that you have many, many environments to go through and do the same process over and over.

Kurt (05:37):

Oh, it's different data.

Brian (05:40):

Correct.

Heather (05:41):

But that provides more, you know, informed, I guess, more information for all of our customers though, right? Like, cause then you're having a larger pool of data, right?

Brian (05:50):

Yeah. Yeah. I mean, it's, it's win, win for everybody. Uh, so it's, it's a valuable sacrifice of time and effort. It's just, you know, it's easy to reap the rewards at the end, but it's hard to see that benefit when you're, when you're in the trenches in the middle of it. And I think one of the, I think one of the values that we brought to our handling of it too, was the fact that we were trying to make the mappings match specifically what our customer searches were looking for, as opposed to saying, "Hey, this, like for example, this search looks for ransomware. Um, so let's add every tactic that, that ransomware ever used for MITRE." We would actually go and break down the search and look at, okay, exactly what activity would we find with this search? So if it was broad, we would only add broad categories. Um, if for example, ransomware would use like a DNS vector, but the search at that particular customer, either wasn't looking at DNS logs or couldn't look at DNS logs, you know, we wouldn't add that mapping, you know, just out of hand, we kept it. We tried to keep it focused to exactly what you search was, would be able to see to hopefully add kind of better value for the customer when they started reviewing the data.

Kurt (07:07):

Exactly.

Brian (07:08):

It's another, another place where that, that value actually would come from then as another app that we were installing at each customer, uh, called the MITRE ATT&CK app for Splunk, which basically provides, uh, an overview dashboard where you can see the, the MITRE attack matrix and then kind of highlight where your searches have coverage against those techniques. So just at a quick glance, you could see, okay, I had, you know, I have coverage against, you know, phishing attacks. I have coverage against remote code execution, but I don't have coverage against data exfiltration, you know, based on what, you know, what parts of the grid were highlighted. And that's where our mappings really tied in from the analytics story to this dashboard.

Heather (07:56):

So will this framework be something that is used primarily by people like us that do like manage services or is this something that our customers would be looking at as well to see what their own companies stance is?

Meredith (08:08):

Both. We are able to use it to further assist our customers in whatever they feel they're lacking in just by looking at the Mitre ATT&CK app. But initially we can also use that ourselves to say, Hey, we see this out in the wild. We would like to help you fix that coverage gap. And if you have the data, we can fill the gap

Kurt (08:37):

From like an internal perspective as well. If, if the customer kind of know the direction they want to go with some of their searches here, let's say they had a internal pen test take place. And they recognize that these specific, you know, MITRE ATT&CK frameworks or that specific parts of that MITRE attack framework for used against their environment from there, they could also kind of reach out to us and say, "Hey, we realized that we were ex like exploited in this manner. Can we try to focus on searches in this area?" So it kind of allows us to work with the customers a bit more and also like help them figure out what they need to focus on to help make their environment safer.

Brian (09:16):

From both a search perspective and kind of a, a maturity, uh, perspective. So we're not only, Hey, do I have searches that are looking for this, but am I even, do I even have the data that looks at this at all? You know, it's great to know that there's an attack, uh, out there that looks at, uh, you know, remote desktop or DNS or fishing. But if you don't have the logs in Splunk that shows you those events, it doesn't matter if we have, if you have a search for it or not, because he can't see it.

Kurt (09:48):

It's flunked. The delete owns the comment. You are, what you eat.

Brian (09:52):

Wow. I had the idea always click save. When you're done with your work,

Meredith (10:01):

I feel attacked. And I don't stand for this.

Brian (10:04):

Meredith story to tell you about how saving works.

Heather (10:08):

Oh, please do tell.

Meredith (10:11):

Wonderful implementation of MITRE. I mean, interesting discovery. So you can say each individual search, once you add your minor in attack mappings, and then you have to save the story overall. Well, if you don't click the save story overall button doesn't really do much. And then you have to redo about a third of the words you just did. And then you do that about 40 more times throughout the course of this entire project.

Kurt (10:37):

Basically Meredith we had to go to save. It would be working together as a group on the, on the searches and we'd be covering different analytic story parts. So there'd be times where Meredith said she was done with XYZ groups and Kerrigan and myself would sit there and refresh the pages and be like, yeah. Okay. Forgot to click save again. But it eventually became a joke cause it happens so many times.

Meredith (10:55):

Listen. It's hard to remember.

Heather (10:59):

Well, now you're done though, right? Like you've gotten to this point where you're just doing the basic upkeep,

Kurt (11:06):

We've finished all of the customers we were able to, at this point, we're still pending on a few, but that's more so due to either apps being on an older version that don't have analytics stories available or, um, some more specific issues at certain customers where permissions kind of play a problem. So as far as like the initial setup, we're pretty much done at most places and there is ongoing work. So whenever our SOC architect team basically we'll implement new searches, we have to make sure we're mapping all those to MITRE each time a new search has made otherwise the, the map isn't really useful to either our team or the customer, because the MITRE mappings are now out of date. When they go to check in IES, right.

Brian (11:48):

The coverage won't match the actual searches that they have.

Heather (11:51):

Right. Yeah. That makes sense. Well, that's all I have for you today. Thanks very much for partaking. I appreciate it. Alright, bye guys.

Brian (12:01):

Bye.

Heather (12:02):

Friendly reminder. If you're looking to learn more about our MITRE ATT&Cframework, you can check out Meredith Kasper's and Brian Karrigan's blogs on their work with it. Our latest books also include a perspective piece on Neuralink as well as a look at a day in the life of a SOC architect here at Hurricane Labs. So be sure to check them out. And if you like what you hear, check out our careers page because we're hiring. See the links for more information. Thanks for listening. We hope you enjoyed the show and we'll catch you next time!