Lowenstein Sandler's Cybersecurity Awareness Series

Session 13 – Inside the Cyber Criminal Mind with eSentire

By Ken Fishkin

OCTOBER 2024

Ken Fishkin: I'm Ken Fishkin, Senior Manager for Information Security for Lowenstein Sandler, and as part of Cybersecurity Awareness Month, I wanted to have a special interview with John Moretti, Principal Architect of one of our key security partners, eSentire.

Now eSentire's sole purpose is to monitor our network and computers 24 /7 looking for unusual behaviors. So, John, can you go a little bit more detail about what your company does for us?

John Moretti: Absolutely, Ken. Yes. So, we're monitoring and watching your environment 24 hours a day, seven days a week. So, things like network traffic, endpoint traffic, log data. A lot of the devices your environment produces logs. So, we use that data to understand what we're seeing and then when we see something out of the normal, we take action on your behalf.

Ken Fishkin: Excellent. And what are some of the types of unusual behavior that you've been seeing specifically toward law firms?

John Moretti: A lot of law firms were seeing a rise of phishing attacks, right? Those emails that look legitimate, but they are malicious, and they have some links that redirect you to bad websites and things that allow threat actors to get into your environment. So, looking for those key indicators or something malicious in an email is critical.

Ken Fishkin: All right. I mean, we have a lot of tools in place here and we're trying our best to stop those kinds of threats, as well. So, would you say eSentire's more like having belts and suspenders on? Making sure that if any of our tools fall through, you'll be there to hopefully catch anything?

John Moretti: A hundred percent. I mean, if you think about a tool, right, a tool is just a tool. You have to be able to utilize that tool on your behalf to make sure it works all the time. So, having another set of eyes to see the needle in the haystack makes all the difference in the world and being able to utilize those tools on your behalf is critical. So, making sure that when we see that abnormal behavior that we take action on your behalf to stop the threat in your environment. I mean, it doesn't matter how many tools you have in your environment, someone will definitely click on something

someday. It's getting harder and harder to see what's bad and what's not. So as soon as someone clicks on something and it is bad, you want someone to attack it right away to make sure that your business doesn't have that disruption.

Ken Fishkin: And what would happen? Let's say somebody had some malicious software installed on their computer. What part does eSentire play at that point?

John Moretti: Well, that's a great question. So, what we would do is hopefully we'd be able to prevent it from even being downloaded or installed, right? But now there's a lot of threat actors that use new technology today; AI is big. So sometimes if that malicious content gets installed, our other component that we offer with our endpoint agent, we'll see it, attack it, isolate it, and remove it off the system, so that way it doesn't spread in the environment as quickly as possible. So, it's like our team is sitting in your office working 24 hours a day, seven days a week for you to make sure we don't see anything that's out of the normal and take action.

Ken Fishkin: That's wonderful. So, we've had had a few issues where we had to have a machine be put in isolation and it's a wonderful feeling where it doesn't impact the whole company. It just impacts one individual and that person, if it does turn out to be some kind of a virus, we're able to just give that person a new machine and blow away the old one. It's very self-contained. I've seen it in action before and it's a wonderful solution, so I really want to commend all the people that work with eSentire for the hard work that they've done because they really are a big insurance policy for us to make sure that we don't get hit with ransomware or phishing attacks or some kind of extortion. So, it's great to have you in our back corner.

John Moretti: Thank you. It's great to hear.

Ken Fishkin: Thank you.