#156 - SMB CISO Challenges (with Kevin O'Connor)

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and today we're going to put ourselves in the shoes of a CISO for a small or medium sized business or maybe a mid sized bank or law firm or something like that and try to determine what security we need.

And of course, what we can afford now before you'd skip, because you may not be in that organization. Remember, you might find yourself in that role someday or mentoring somebody who is. So we're gonna give you a solid foundation of what you'll need to be successful in that type of role. So before we get going, let me share with you a word from our sponsor.

Adlumin provides enterprise grade security to mid market [00:01:00] organizations. Its security operations platform and managed detection and response services combine all your data into one view to illuminate security risks and accelerate security workflows. Security teams are often stretched thin and must respond to increasing threats like ransomware, and data theft.

AdLumin's patented technology simplifies these challenges by providing machine learning detection and automated response capabilities to halt threats quickly. The platform also includes threat hunting, automated incident response, vulnerability management, honeypots, darknet exposure monitoring, compliance reporting, and monitoring and more.

See how Adlumin can enhance your security program without increasing your workload. A D L U M I N dot com. Alright, well, back to the show and I'd like to introduce our guest speaker today, Kevin O'Connor, who coincidentally is the Director of Threat Research at Adlumin. Kevin, welcome to the show.

[00:01:52] **Kevin O'Connor:** Hi, it's great to be here today. Yeah, I'm Kevin O'Connor, the Director of Threat Research here at Adlumin. I spent, most of my time in the cybersecurity industry. I spent about a [00:02:00] decade at the National Security Agency working on, defense mission. Also got to do a lot of the like overt hacking for the U.

S. government to get the foreign intelligence and all that fun stuff. And then I got to join up with CrowdStrike for Hot Minute and then over to Adlumin where I've been working as the Director of Threat Research for a while.

[00:02:14] **G Mark Hardy:** That's pretty cool. Yeah, I was too old to do the NSA thing. I... Just as they were standing up cyber command was when the Navy said, yeah, you're too old and feeble to continue. You have to retire. It's like, but guys have been waiting my whole career for this. Like, yeah, yeah. Off you go. So glad to see that you had that opportunity.

And interesting that you work, not necessarily on the offense, but also the defense as well, right?

[00:02:35] **Kevin O'Connor:** Yeah, I mean, that was really fantastic. When I joined up with the NSA, I actually joined a program to sort of make like, Defensive Information Security Engineers. And of course, like, doing rotations throughout the agency, I sort of found my passion, which was the offensive, because, you know, who can say no to that kind of cool stuff?

[00:02:48] **G Mark Hardy:** Well, offense is cool. I mean, I'll be a full disclosure. My son does, uh, runs a pen testing team, red team. And, I brought him to his first DEFCON when he was just at 14 years old. And he said, like. I like [00:03:00] this. I want to do it. And I've kind of tended more, well, Blue Team. And that's where I told him, I said, it's a little bit tougher to defend against all these things.

It's just kind of fun to find holes and things like that. I remember Marcus Ranum, a friend of mine, he did a keynote at Black Hat 2 and practically got booed off the stage when he was saying, like, the real challenge is to go ahead and build the defenses. But fast forward quite a few years later and we find out that If all we had were offensive capabilities and no defense, we probably wouldn't have many businesses surviving today.

[00:03:31] **Kevin O'Connor:** No, I wouldn't think so. I really like the, you know, offense is nice, because it really does get people interested in the industry, right? Especially when you're talking about, like, the youngins and stuff like that. You know, the offense is always cool and sexy, so everybody kind of wants to hop on that.

But, I mean, the defense, like you had said, really just as important, if not more important.

[00:03:45] **G Mark Hardy:** And I agree. So, so let's think about a little bit about what we want to talk about today. So one of the things we found out is that a lot of vendors that I talk to out there have enterprise solutions. Well, of course, if you're in sales, that's what you want. Hey, I got 50, 000 seats in one phone call. [00:04:00] Well, that's great.

And it helps you make your numbers. But the reality is, is that there's an awful lot of small and mid sized businesses that require security services. I work as a CISO for a couple firms and a lot of them are, I remember trying to find one. They said, well, what's your smallest C count? I go, a thousand. I said, well, we're not even one, we're close to that.

So we could pay for a thousand and, but that's as small as we go. It's not worth it. So first of all, let's sort of start with what are the requirements at a SMB or small and medium sized business? And in particular for organizations that don't necessarily have a huge budget, and it's rare to find that combination SMB, huge security budget.

We tend to outsource or have managed stuff. So managed security services may be the way to go. So what would that concept be like and why would it be important to small and medium sized businesses?

[00:04:48] **Kevin O'Connor:** So I think that the requirements that small and medium sized businesses have, on the security front are, are ultimately really similar to the, the ones that, you know, the enterprise has, right? It's really just about the scale of it. You know, the small and medium businesses don't [00:05:00] necessarily have the, the, the same number of integrations and applications and, you know, different vulnerability and exposure on the, you know, the internet and things like that.

So I think things like, managed security services can really help out, small and medium businesses by sort of offering them the ability to, you know, enhance their sort of cyber protection by adding on things like, you know, 24 7 SOC capability, right? So when there's something that's going on after hours, you know, at a small business, they don't have the IT staff that can respond to that, right?

This way there's somebody that can kick it over and sort of handle that kind of thing after business hours, during business hours. A lot of the businesses we serve don't have a specialization in IT, right? So they don't necessarily know what's going on or how it works. Through direct interaction and through our partners and stuff like that, we can provide some of these services to, you know, sort of help protect the traditional business, right?

Like think about a dentist's office, right? I mean, they have. You know, critical medical data, billing information, things like that. But, but who's protecting them and who's looking out for them, right? It's not, they don't have the giant enterprise staff that a lot of these larger companies do. You know, making sure that data doesn't get compromised, making sure that the endpoints are safe and things like [00:06:00] that.

So I think things like managed security services can really, hopefully for a cost effective price really help out the small medium business.

[00:06:06] **G Mark Hardy:** Yeah, I would. When you look at things such as HIPAA or PCI DSS, some of the regulations, we're going to talk about that a little bit, but the idea that if you're a small business, like a dentist's office, for example, they don't say, Oh yeah, don't worry about HIPAA or, yeah, don't worry about PCI. Like, yeah, you do need to worry about that.

And although you're probably not going to have a full blown secure enterprise solution there, there still needs to be some common sense stuff that's in there. So when I think of managed security services, I think of. Somebody who, as you said, it's, it's sort of like the phone, a friend, think something just hit the fan.

What was it? Or I get a call from them. Yeah. Something is, is in your environment or whatever, but does that also work to help, let's say a new CISO or a new, you know, not even a CISO at that point. It might be just the head of it, or even kind of double headed as it security. Is there something that in that role that would help them get started?

Or do they just basically say, yeah, go [00:07:00] figure it out. And when you got your act together, give us a call as a managed security service company.

[00:07:03] **Kevin O'Connor:** Yeah, I mean, I think managed security services are great because they can really help expand the CISO's toolkit, right? And their abilities. We all know one individual can't know everything about the security stack and be the expert, right? The guy who, who is the CISO probably isn't resolving, alerts for...

Your EDR popping off for viruses and stuff. So I think that's where really managed security services can help by bringing some of that, subspecialty expertise to enhance the business

[00:07:26] **G Mark Hardy:** got it. Now, of course, the name of the game is an SMB, as I mentioned before, is limited resources. You don't have enough money to do everything you want. In fact, you might not have enough money to do everything you need to be doing. And so, in looking at these organizations, when you go to senior management, which could be a leading partner in a law firm, or board of directors, or even executive committee, and say, hey, I need a check.

I need to go ahead and outsource it. They might say, well, why don't you just do it yourself? And unlike, Bill Murray and Stripes who are retrained ourselves, or I think there's a different value [00:08:00] proposition here. How do we communicate that effectively to the management of these organizations

[00:08:04] **Kevin O'Connor:** When I'm talking with CISOs and stuff like that, the thing I always bring up is 24 7 operations, right? Imagine having to have a team to cover your network 24 7 to respond to any sort of, incidents, detections, or alerts, right? That's going to be at least... How many staff to be able to cover that, right?

You're talking about at least three people. Whereas, being able to outsource that kind of thing you get a lot more coverage and you get protect your business.

[00:08:25] **G Mark Hardy:** Yeah, I know that some organizations, when they start out with a baby SOC, they said, Oh, all right, we'll do Monday to Friday, nine to five, because after all, that's some of the bad guys have got a really good union and they're in our same time zone, and usually neither's the case, and yet.

Something's better than nothing. And so if an organization is trying to staff it during the day, okay, fine. Does managed services work 24 by seven or does it, is it kind of like a call attendant where you leave the office and you press the managed services button. When you come back in and get a cup of coffee, you take it off of call forward.

[00:08:57] **Kevin O'Connor:** Yeah, you know what? You can actually get it both ways, which I think is really [00:09:00] interesting. It really helps some of the businesses that are more medium sized that might have, like you said, a SOC running during business hours. And I think that's really great actually because they can sort of expand your capability and integrate with you, right?

So they can Take on what you're doing, you know, after hours. And I think what's really critical about that is that, you sort of get the, the fall over too, right? So with three people, some guy, you know, is sick or something like that. All of a sudden you have a shift that's uncovered, right?

With something like an external SOC, you don't have to worry about that. I will say that, um, it, it does make sense to sort of run your own SOC or something like that during business hours because that's when the majority of your users doing things right and a lot of the security problems are going to come up.

What are some of those after hours things when somebody's checking their email on their phone or, at home on their outlook, when problems really do come up. And I'll say working, managed security services and also incident response, it's always that sweet spot after 5 p.

m. I'll tell you, it's after 5 p. m. before 10 p. m. You know, after midnight and things like that, I'm not getting too many calls from businesses. But like, you know, that 7 p. m. discovery that then takes, work and analysis into 5 a. m. That's really that [00:10:00] sweet spot of annoying.

[00:10:01] **G Mark Hardy:** Yeah, and it's interesting. You mentioned having a SOC even during the day. There's probably a minimum threshold below it wouldn't makes sense. Carson Zimmerman had put a book together a few years ago on, SOC and access. He was a MITRE at the time, so it was a free download, like 300 pages and really good stuff.

And, he had suggested that a little checklist where you go through, do you have this? Do you have this? And then. Based on the end, you ended up with a score and it kind of gave you a minimum threshold for a SOC, but not all small businesses or medium sized businesses kind of have a feel for where that cut line is.

If you've got any sense for that, you know, I, again, I can tell you what Carson's number is out of his book if you reverse engineer the model, but I kind of, well, interested in your input first.

[00:10:44] **Kevin O'Connor:** Yeah, I mean, I think for having a 24 x 7 SOC, I don't think there really is a Bottom line, like a number of users or endpoints or something like that where it's not useful. I think it could definitely get more useful when you're dealing probably with like 20 plus devices, right? I think that's where you really start seeing, a [00:11:00] lot of sort of events and stuff like that and detections come through against individual devices.

I think that's sort of where you see the number where it starts to become really worth

[00:11:07] **G Mark Hardy:** Yeah. And for him, he puts that number closer to 2000, that is to say. Yeah, a lot. Now, or if, again, if it's kind of divisible by seven, it was like one, four, two, you know, you know, 1, 420 thereabouts, which is still a lot. And the idea is this, if you're going to staff up one seat, 24 by seven, we say, yeah, that's three people.

Yeah, not really. It's five people, because if you think about it, people have to have weekends off and then two weeks of vacation and holidays and things such as that. And I had worked in the military in 24 by seven seating. And we had. If there were five people, life was good. We averaged about 40 hours a week.

If you had four, you tended to pull a lot of overtime. And at three, you're at port and report, you know, seven days a week. 52 weeks a year. You're going to break. It's something's going to go there. So then we have five people. And then what does it cost to hire somebody? Well, I got salary. [00:12:00] Yeah. But then you got benefits and social security and Medicare and unemployment.

And then this, and this, by the time you're done, it's at least double that. So now you're talking 10 X. And so for somebody who says, yeah, we'll roll our own. Well, what does it cost to get a competent person who can manage this? Okay. Take that salary, put a zero at the end of it. And that's your reference point.

[00:12:18] **Kevin O'Connor:** I like that.

[00:12:19] **G Mark Hardy:** To go out to a managed security services. And there's not too many managed service companies that are going to say, Oh yeah, we're even more than that. Because you can hire those five people and then you get six or seven. So you got depth, someone calls in sick or they have an issue. You can keep them going.

And most. Places don't all catch fire at the same time. And so as a result, like a fire department, you're not going to be fighting every single customer fire at the same time. And so as a result, you can manage that. So that makes a managed security service business scale well. And I'd been part of one that we started up many years ago, and that's how the economics work.

[00:12:56] **Kevin O'Connor:** Yeah, I think that's a really good point, right? I think like the 20 devices when I was [00:13:00] coming from it, I'm thinking more like if you're looking for a managed security services, right? Because like you said, if you're setting up your own internal SOC, you're going to want a lot more endpoints to justify having that.

Because like you said, right? And I mentioned earlier, like one person is not enough, right? You need five people covering ships. We have a lot of folks that came from like the National Threat Operations Center over at the agency. And they have those rotating ships, overlap between the ships so that there could be handoff between analysts.

And just the cost, man. I mean, getting folks that can work even these tier one soft positions or especially tier two, tier three, you're looking at some really expensive salaries. So, you know, take your, your 140, multiply that by five. And then, you know, you're talking about a huge investment into

[00:13:39] **G Mark Hardy:** zero to handle the benefits and everything else. Oh yeah,

[00:13:41] **Kevin O'Connor:** And that's why, that's why I think things like managed trace. Yeah.

[00:13:44] **G Mark Hardy:** plus the connectivity.

[00:13:46] **Kevin O'Connor:** Yeah. And then all the engineering that has to go behind it too, right? Like, people's IT systems aren't necessarily set up to where a SOC can necessarily take advantage of all the data, right? You have to make sure that you're forwarding data to a centralized location.

You have some sort of. dashboard to review things like detections [00:14:00] and, alerts. And I think that's where the managed security services really shine and why I really push those for small, medium business, right? Because otherwise you can't afford it. It's just, it's not affordable.

[00:14:08] **G Mark Hardy:** And, most companies don't generate their own power, unless they're a power company, of course, you go ahead and that's a service. And so in a way, what we do is we look at it to say, what services do we need? to make our enterprise run well. And, interesting because I remember two years ago working at the law firm.

Now I'm going to date myself on this one. They were using such antiquated stuff. They were using WordPerfect 5. 1 and DOS when everybody else was in Windows. All right. Now that's obviously long gone, but the whole idea was they seemed, and the different law firms I talked to, to be late adopters of technology.

If you look at, Moore's. Curve there in terms of say, the gap that you find there crossing the chasm, the late adopters of the people that say, okay, fine, everything's now on a discount. Let's go buy it because everybody's out of the new model, but with the value of information that they possess and the importance [00:15:00] that it would have to clients, that doesn't make sense to me.

So if you're talking to a senior partner at a law firm or something like that, how do you convince them to up their game to meet the modern cybersecurity threats?

[00:15:10] **Kevin O'Connor:** So I actually just, went out to ILTACON, which is like a legal conference that was out in, I think it was Orlando specifically, focusing on that industry. And that was a really fun time and great to be at. And I'll say that, the law, the legal area, traditionally, right, you, they are a little bit behind the times of technology, I would say, right, because they're, they're using technology to supplement what they're doing, right?

It's, it's sort of an enabler, so they're not necessarily looking for the best and the greatest, they're looking for what can get the job done, you know, and a lot of times it's just word documents and research. I'll say an area in, the legal sector that I'm actually seeing them sort of advancing is in all this e discovery stuff, if you've seen it.

Tons of technologies, tons of different firms and stuff doing e discovery, which I think is huge and, traditionally, for a law firm, the discovery process is actually a really big vulnerability for them because you get, a lot of associates and things like that are just going out on the web, downloading files and things, and I've actually, I've recently done an incident [00:16:00] response for any, legal firm, and, in that case, they were actually hacked by ransomware, and they were able to get all of their, their, essentially their data stolen, right?

So long as the data was on, on the website Ransomware, then that's the last thing you want from your law firm, right? Whether they're handling mergers and acquisitions or they're handling, private personnel cases to have your, all your legal stuff up there on the, on a website, a darknet leak site, isn't great.

So, I think that's really how I push the legal firms to, to look at these kind of solutions the need for this in their business.

[00:16:29] **G Mark Hardy:** Yeah, that makes very good sense. Another thing in terms of, we're talking about SMB, in a different industry, banking. Okay, so large banks have huge cybersecurity budgets. You read about like JPMorgan Chase having half a billion dollars or something like for a security budget, but mid sized banks or a lot of credit unions don't have that luxury.

Now, Is the threat to these smaller entities less than the big banks? I mean, remember the robber Willie Sutton, they said, why do you rob banks? Well, that's where the money is. Or if not, what can these bankers do with their limited security budgets to be able to protect against what is a [00:17:00] significant threat?

[00:17:00] **Kevin O'Connor:** You know, I, I think they're this, either the same targets as large banks, like these, these community banks and the, the credit unions and stuff. Thank you. Or they're actually bigger targets. If I'm a hacker going out and attacking folks, right? Like going against the Bank of America, it's going to take a lot more resources to sort of penetrate and then like, even once you're in the network, it's going to take a lot more resources to understand it and then fully be able to, exploit that and leverage that for profit, some of the smaller banks, it's easier to go against.

And, if you're a ransomware group. If you could spread pretty quickly, throughout their internal systems, you could really cut off all of their endpoints at once, take the bank down for the day, and, they're going to be forced to pay you probably because they want to resume activity and they need to, whereas something like the Bank of America is going to be more insulated from that kind of thing, I think.

[00:17:41] **G Mark Hardy:** Yeah. So, so really then it sort of argues more in favor of. Security for these smaller banks or credit unions to be able to outsource that because they probably don't have the resources and even if they get access to them, my experience has been, if you have a relatively narrow environment and you're a [00:18:00] top notch security person, you're going to get bored.

You're going to want something bigger to play with. You get in a major bank, there's just an infinite number of things you could end up doing. And so again, that seems to be a solution there as well. And, I think part of the challenge for a lot of organizations is meeting compliance requirements.

Particularly in financial, because financial, that's where the money is, has probably some of the earliest set of requirements between the SEC and FINRA and probably a number of other organizations. The thing is that compliance does not equal security. Compliance is a minimum passing grade. It's like getting a C Okay, you didn't fail.

But he just got your nose over the threshold and you'll pass. And if it were high school, you'll go on in the next year. The problem with that, of course, from a security perspective is that compliance will get funded, but sometimes the people writing the checks are compliance minded and they go, okay, that's it.

You're compliant. Yeah, but we're not secure. Yeah, but you're compliant. So how do, how can CISOs leverage the sort of a [00:19:00] compliance mandate to fund true security and not just meet their reporting requirements? Any thoughts on that?

[00:19:06] **Kevin O'Connor:** I think it's important to spell out to business leaders that meeting minimum compliance requirements doesn't absolve you from, potential litigation or potential at fault for something that's the result of a breach, right? A lot of times compliance requirements are proactive and prescriptive, right?

whereas a lot of times the things you're getting in trouble to with a breach are, reactive when your data has been stolen and all that. And not all, things that sort of fall in the compliance sphere talk about what happens with data leakage and all that kind of information.

And I think the businesses we were talking about, ransomware is just it's just totally going crazy in the space, right? This is just untenable, I would say. Just the way they're able to target these businesses and then exploit them. So I think that's really what I would focus on, right?

[00:19:44] **G Mark Hardy:** Yeah, and, and I think what you point out, I mean, I've heard it said, this is. Every organization had a major credit card breach, and I'm not going to mention names because we've all heard of them before. Was PCI compliant at least a minute before the breach? I think somebody had argued. Yeah. Well once you're breached, you're technically not [00:20:00] compliant.

So we have a perfect record. It's a little bit like a hospital that says, hey, he's getting ready to die. All right, transfer him someplace else. Oh, okay. No, no one's ever died here. But the reality check is that when we look at that, we want to figure out ways that we can Emphasize that message that compliant organizations do get hacked.

And maybe compliance at a minimum is what, in some cases we force security onto people in the real world. You buy a car today, it's going to have seatbelts, it'll have airbags, it'll have probably I think anti lock brakes, and I know as of a couple years ago you have to have a backup camera. And there's a lot of other safety features that are all built into an automobile so that they all.

Sort of kick in automatically, but the thing is when we build out our IT infrastructure, it's not like you're buying something off an assembly line. You don't go to the dealer and say that IT infrastructure, please set it up in my office. I'll come back Monday and I'll expect everything to [00:21:00] run. We got to build our own.

And in building our own, we tend to have to work within constraints and budgets and things like that. So. If, and this is sort of a tough question because it's always going to be, it depends, but where do you say, Hey, this is something I absolutely have to have organically. And then here's something that I could potentially outsource to a managed security service provider or somebody else who's going to monitor my stuff such that I don't need that in my enterprise.

Is there a cut line in there or just a quick thought about what might be that

[00:21:33] **Kevin O'Connor:** you know, it's... It's not an easy cut line. And I'll say for like small, medium business, mid market segment, that you can outsource more than you would think. I think one thing that, folks don't realize that they can outsource. So you'll get a lot of companies, especially in the small market, where they'll go and they'll outsource their entire IT, right?

From security to, you know, IT implementation, running administration. But one thing that you can't, I found has never been successfully outsourced. is, like understanding your data and the data risk. So one thing that [00:22:00] happens is once we, a lot of times we're doing an incident response, to a company that's already been breached or something like that, and their data is on the dark web, the first thing we ask is, okay, what data is there, right?

Like what data was stolen? Or, hey, we know that these directories off this computer were stolen. What's the importance of the data that's in here? What's the significance to your business? What's the impact? And I think even just understanding exactly what data is out there and on what systems is something that really needs to be held internally because you're the only one who knows your business or you're the one who knows your business best.

[00:22:27] **G Mark Hardy:** Yeah, that makes very good sense. Now, if we're looking at that, because you can't outsource the accountability, you can't say, yeah, we got popped, but it was our vendor. It's, blame them. We hear that. We see that. But at the end of the day, your customers don't care. Your customers know they entrusted you and it didn't work.

So off we go to something else. So if we look at a security operations center, which is typically something that we would manage, but a security operations platform, I've heard that term before, and that, is that a SOC that's run by an MSSP? Is there something different? And if so, what are the benefits of one over the other, if any?[00:23:00]

[00:23:00] **Kevin O'Connor:** Yeah, so I would say when you're talking about the managed security services, a lot of times folks are thinking about things like SOC or proactive patch management things, even like pen testing services. When you talk about, a platform, you're really talking about like a piece of software or a portal where all your relevant security, your security relevant data can be integrated to, so you have that single pane of glass.

Just look through what's going on in your network, right? Types of software and platforms will do detection. And what's really valuable is they'll do things like cross integration detection as well. You're not just looking at, the EDR for your semantic or your CrowdStrike or something like that.

You're looking at something that's integrating the EDR logs along with your Office 365 logs, right? So that you can see the malware message delivered, the phishing email with the PDF. And then you can actually see the EDR logs of the execution of the malware, in CrowdStrike and things like that, and then tie it back to a network log or something.

But I think that's where you really see the benefit is sort of that single pane of glass and the integration, being able to pull all the security data from your cloud, your, authentication providers if you're using the Okta or something, your [00:24:00] EDR, your firewall, all that.

[00:24:02] **G Mark Hardy:** Yeah. And, and of course, it's more important to be able to. Act in that real time instead of coming in Monday morning and getting a report saying at 0 1 58 on Sunday morning, you went bankrupt because that's when the last of your sensitive data left the enterprise. And that's when the last of the servers got encrypted.

So it's got to be more than just reporting and, which kind of gets us into the concept of managed detection and response. If we identify, protect, detect, respond, recover, if we can protect everything, then nothing goes wrong, but that's not realistic. We have to end up detecting and responding. So detecting and responding is primarily an IT responsibility, but also it's a common offering by vendors.

Can you, can you help folks understand a little bit about what that would entail if you're outsourcing that part of that chain and why it's essential?

[00:24:54] **Kevin O'Connor:** I think one of the big pieces is response and also how quick you can respond to, right? So when you're dealing with managed [00:25:00] detection and response, a lot of times you might be dealing with a service where the different security platforms, whether it is that that MDR platform itself or some component like the EDR, are sending up these alerts and detection saying like Hey, we just found malware on this Windows system and remediation failed, right?

Some, a next step needs to be taken, by your organization to fix that. Or you'll know remediation was successful and you can move on with your life, right? And then just expand that out to every point of your sort of enterprise and your security stack. That's how those work.

And I think that's great because, it does bring the security issues to the forefront to allow you to address them. And then because all the data is integrated into these systems, you could You know, pivot between data sources and see exactly what's going on in your network.

[00:25:39] **G Mark Hardy:** Yeah, and that's a very good point because you really want to have everything collect into one place. And on a large enterprise, you'd have a data lake or something where you just dump all this stuff in there, which you go back and look for later to say, Hey, this long, low, slow type of attack. But when things are actually hot and some bad [00:26:00] actor is interacting with your people, your systems, or some software is doing that, ideally, malware or something like that, that's a big deal.

And you can't wait until Monday morning to respond to that, particularly if you have servers and some compromise takes place over a weekend. And so then again, that sort of argues back again to, unless you can staff up a 24 by seven. You have to have some sort of equivalent, even if it's a lower intensity, to keep an eye on these things, because they say, you don't want to just find out Monday morning.

Yeah, we want bankrupt. Now,

[00:26:30] **Kevin O'Connor:** Here at Unlimited where we work, SOC at night for them essentially, right? So they're working during the day and then we're working the night shift for them, and then there's handover. I think that's a great way to go, if your organization is large enough to support that sort of IT staffing requirements.

Yeah. So vulnerability management really falls under a

[00:26:44] **G Mark Hardy:** one of the challenges that I found, is the CISO's vulnerability management. It's, I think it's a challenge for a lot of security leaders and in a perfect world, you do continuous vulnerability management in being able to identify and address vulnerabilities effectively. How could that work and how could a [00:27:00] third party?

Do that, if at all, as compared to somebody just going ahead and running the trap lines, as I like to say, looking for anything that's out of date or has a patch issue, et cetera.

[00:27:10] **Kevin O'Connor:** and like vulnerability discovery on systems. And, patch management is super critical because we see the zero days come out every day, right? And most of the time that they, the vendors have a patch pretty quickly, right? I know there was like a Cisco iOS exploit that came out, I think it was last week or something.

And there actually was no patch for it, which is always scary. And where you should hopefully be able to rely on your patching vendor or your... Your managed, services vendor to implement these sort of, we'll call them, like, defenses, you know, despite not having a patch.

So, like, in that example, just not exposing your Cisco interface to the internet is probably good enough, right? Or disabling the admin interface. So I, I think that those things are, are really important. And I think being able to work hand in hand with the business. So like, I know we make sure that our SOC is, , I think it's either weekly or biweekly with the business owner for, whatever IT infrastructure is going on so that they could actually brief them on what are the issues that are being [00:28:00] observed?

What are the issues the SOC's having and investigating issues? Where more data might need to be collected, just to be more pointed and effective.

[00:28:06] **G Mark Hardy:** Makes sense. Now, in the event of a breach, whether it's a ransomware or just a security breach or somebody in there doing lateral movement, we then get into incident response. And then even the forensics function becomes crucial. How would these play out if someone were dealing with a third party vendor with a major security incident internally?

Would they, would the team send them daily updates, quarterly updates, or they get on a zoom call and they just say, Hey, we're going to work And we're going to handhold you the whole time.

[00:28:37] **Kevin O'Connor:** A lot of it really is the Zoom updates, right? Especially when you're initiating sort of an incident response or the forensics procedure. You want to make sure that you're there with the SOC, whether it's internal or external or the business, the business decision makers.

At least when you kick off these sort of things so that they can understand the scope of what's going on and exactly what needs to be done. I remember one incident response we did. We created a war room, right? With the SOC that originally was investigating the issue. The [00:29:00] business IT admins who were like, Oh, this is looking bad.

And then of course us as the incident responders. And, you know, just being able to have that one on one, or, the multi on multi, chat live, was really critical to being able to, like, kick the attackers out of the network, right? These attackers were emailing the admins, from internal email accounts, ransom letters, from accounts that had been compromised, right?

And then they're hitting them on Teams as well, internally, so you're like, oh no. We got to get these guys out ASAP, right? So being able to do things like that, effectively implement MFA so that folks can't use credentials that have been compromised and stuff to access. I think that's critical.

[00:29:32] **G Mark Hardy:** Yeah, and I think, you mentioned MFA, and that's something that I absolutely push very hard on any place I can, and every place I can get it. As a policy, if I come in as a CISO, that's one of my first things. At the very, the very top. All admins shall use MFA for all access. Now, rule 1a is all users shall use MFA for all access, but that's not always a possible and then be desirable depending upon the level of risk.

[00:29:57] **Kevin O'Connor:** Yeah. You have to expect passwords are going to be compromised, right? [00:30:00] Like we know from these days, whether it's, a breach on the vendor's side that exposes the password or it's something a user does where they're, putting their O365 login into a fake portal. the password breach has happened and without MFA, it's really...

There's no stopping an attacker just from pretending to be you. Right.

[00:30:14] **G Mark Hardy:** and, and that brings up a question of human error because I'm seeing more and more sophisticated attacks where it's an absolute lookalike for Microsoft. Unless you're purely paying attention and you're reading up there in the URL. and I think that, gee whiz, if Microsoft has that same login, I think it was like.

Used to be the same picture from Rio up in the mountain looking down. It's why don't you say if somebody is our customer and that image is rendered anywhere other than Microsoft and flag that as being your security porn, so to speak, you shouldn't be seeing that. But nonetheless, we can't make those sites go away and they're still effective or they wouldn't be using them.

So how do we better defend against human error, to be able to prevent those vectors from Allowing an attacker into our enterprise with some, well, valid credentials.

[00:30:59] **Kevin O'Connor:** [00:31:00] So just like you focus on the MFA, which yeah, I absolutely focus on as well. One of the first things I'll tell businesses also. is, implementing, user training and awareness, right? So something like I know before, the phishing training and awareness, right? Being able to recognize these messages as they come through, to see that they are spam, or, even just letting users know, hey, look up in the URL on your web browser, ?

See if it says Microsoft. com. And if it doesn't say Microsoft. com, you might not actually be on that website entering in your credentials. I think user prevention and training and early intervention and awareness is really where you're going to be able to cut these attacks off at the forefront.

I think that's important because They're not super advanced, right, and a little, just a little bit of training can really avoid most of the password compromise situations. I also really recommend, , password management utilities, right, like your 1Pass, Bitward, and all that. , I think those are great. I think that businesses should even be providing those to, people for personal use and stuff because, we see compromise between the personal accounts and the business accounts.

So I think being able to secure your employees on both fronts there is super helpful. I know here at AdLibbin, we offer it not only for business, but [00:32:00] also family accounts, which is super helpful. I just think doing things like that are really going to help prevent compromise.

[00:32:04] **G Mark Hardy:** Yeah. And I think the vendors are helping out too. I know Google Chrome is going from 118 to 119 or wherever we are. It's now pretty much turning HTTPS everywhere as a default. And so even if you type in Website. com typically is a port 80. It's going to say, nah, I'm a smart browser. I'm going to go on a 443 and it lets it deliberately comes back and it get like the reverse.

You go to 80 and you go ahead and you get three, redirected, go here to 443 and the browser figures that out here. We're saying it almost has to go the opposite way. And so the average person is going to be much less susceptible to the man in the middle attack, where if you go out HTTP, And the man in the middle says, okay, you want to go to your bank?

I'll go to the bank for you. HTTPS to the bank. Hey, give me the user ID. Give me the password. And oh, by the way, here's your MFA challenge over [00:33:00] goes to the attacker who's still in the middle. And unless the user notices that lack of a little lock icon in the upper left hand corner, they just have facilitated it.

And you may say, pay my electric bill, move some money from saving to checking log out, like, okay, yeah, you're logged out, but the attacker now have a session. Even though it was MFA protected, and the weakness in that whole scenario for a potential man in the middle was the lack of HTTPS, because the way the protocols are set up is that if you start with a query, you cannot come up with a response that would meet the cryptographic requirements, unless someone has wholesale compromised the target And then they're into having that certificate and that's a whole different discussion.

Let's not worry about that.

[00:33:42] **Kevin O'Connor:** What we've, what we've actually been seeing recently actually is , actors doing things like mimicking bank portal websites, right? The login pages, like the O365, but essentially for your bank. And what they'll do is they'll either forward these requests onto the bank and act as a TLS proxy essentially.

So they're able to break that TLS, that 443 layer and recover the [00:34:00] credentials. Or, They'll just harvest the different images and stuff like that and rebuild the website themselves essentially or a different version of it. But that way actually does allow them to recover clear text credentials even over an HTTPS site, which is the issue.

Because you're essentially putting it in, right? You're giving them your credentials. So they just take that then they forward it on to the real website and then, get all those from

[00:34:21] **G Mark Hardy:** Exactly. So yeah, we fix that with some of our tool sets. We fix that with our security awareness. And then at some point in time, we want to check it out. And so that's where you get into the fun stuff. We were talking about the early part of the show, the red deeming or the ethical hacking, which is, I think it's just another term for pen testing.

Is there a lot of difference in pen tests that are available to a small and medium sized business? Is it. Is it appropriate to do them once a year? Is it appropriate to do it more frequently? And then when does that factor in to the IT validation update lifecycle? Do you do it first and then go fix everything or do you fix everything first and then call for the pen tester?

[00:34:59] **Kevin O'Connor:** I [00:35:00] always say fix everything first and then call for the pen test. Especially when you're starting out, there's a lot, that could be done. And I think these early results from pen tests that will discover, everything's wrong with your network aren't going to be super helpful. So I think you can make the pen test more useful by making sure that the responses are more pointed after you've already implemented that base security.

I think pen tests are awesome. I think they, they definitely help out small and medium businesses as well. I don't think they need them to the extent that some of the larger businesses do. And I would say, yeah, once a year is great if your business can afford it. But really make sure that you're doing it, when you make significant changes to your architecture and infrastructure too, right?

Or you integrate specific new systems and, there's different inroads and outroads. I think that's where you can really see a lot of the pointed benefits of the red team pen testing type stuff.

[00:35:42] **G Mark Hardy:** Right. And as I mentioned at the show, my son runs a red team for a business and when they find out that some of their clients come to them and said, Hey, we've got a compliance requirement, do a pen test.

And we were like, aren't you doing updates next month? Yeah, but we need a pen test this month. So checking the compliance box, [00:36:00] again, I'll get funded, but as you had pointed out correctly, it ought to be more strategic to say, you got a rollout coming out.

Let's agree that we can postpone that test, roll it out. Do everything the best you can. If you will, the pen test is that Marine Gunnery Sergeant coming up and grabbing your rifle and Inspecting it to say you missed a spot. As compared to you're coming in from the field. Let me inspect that rifle Oh, it's all muddy and it's still got powder and it'll be a mess.

So it's a good point on that one A couple last topics I want to think about and we discussed it briefly was ransomware. I mean, ransomware attacks, if they're successful, they're both expensive as well as well embarrassing and potentially legal liability as we had found out from a, from Joe, the CISO who had some issues there.

We said, , we'll just classify them as a, as a pen test, which is a bad idea. Don't do that. But we see that they continue to increase in spite of. are presidents of traditional defenses. So they're winning for [00:37:00] some reason. What can businesses do differently to protect against this growing threat?

[00:37:05] **Kevin O'Connor:** Yeah, so Ransomware has really been the cat and mouse game in defense that I've been watching for very many years, right? When Ransomware first started out, they were going against, computers using things like symmetric keys, right? So security researchers and defenders were able to do things like recover the key off the box that had just been encrypted, in ransomware, and recover the data, so you don't need to pay them to get your data back.

To go against this because they want their money, the ransomware group started using things like asymmetric encryption, right, where the keys aren't necessarily stored on the box, so you can't recover the data even if, you're on the target and able to work on it. From there, the industry started, the defense industry started focusing on the secure backups game, where, if you keep your backups secure, make sure they're immutable, make sure that ransomware can't mess with your backups, then worst case, you can always just recover the system, right?

Well, because that became so effective, what the ransomware group started moving on to was that data extortion, right? Or what we call double extortion, where not only are they encrypting your data so you can't use it and the systems are harmed, They're taking [00:38:00] the data and then threatening to release it publicly, for bad press.

Or what we see tons of, and I've watched these guys, they go and they, other hacker groups will go and curl this data and stuff like that to get, credentials and so that they can go and hack you with it, right?

[00:38:12] **G Mark Hardy:** Or, or even including to say, you know what, we're going to give this to the regulatory agencies

because their fine is going to be this. And yeah, our fee is here. So you're actually making a good business deal by making us go away and not turning you in.

[00:38:28] **Kevin O'Connor:** Yeah, so they're really just changing the business prospects and proposition of how this all works. And it's really just been a cat and mouse game to get people to pay. And I'll say that, , now that, the data exposure has been so effective, we're actually seeing a lot of these new ransomware groups, things like yamea, , actually avoid data encryption altogether.

And they're not even bothering to encrypt your data, they're just stealing it. And the benefits to that is they can go low and slow for longer, steal more data without, overtly triggering something in the system and saying, oh, this is locked out and it's broken. I recently dealt with a ransomware case in the legal industry.

And they, with the data they stole, were [00:39:00] actually going through, like, emails and stuff and reaching out to, the law firm's partners, right? Whether it was clients or other folks that they're working with in their cases to say, hey, these guys got hacked, right? So they're, they are really trying to bring harm and damage to your business.

It's not like they're just putting it on the internet and letting it float there for somebody to see. They'll actually reach out to some of these people, or, allegedly will. And I think that's just, it's really tough, it's really tough to solve., I think we need to get better about... , things like, , I guess it really falls under like data attestation, but like the secure loading of data where data can't be loaded on systems that it's not approved for.

So even if you steal these binary documents and things like that, you can't load them without the security requirements that come with, a laptop that's considered within the enterprise, right? And this is where we get into the really complex using like security co processors and different machine attestation that you can do, for security and stuff.

But I think that's really the. It's a long game to beat ransomware and that sort of threat.

[00:39:55] **G Mark Hardy:** Yeah, and I think we'll find out as everybody goes to Windows 11, as Windows 10 is being [00:40:00] deprecated, you know, a little over a year, , and it's having a TPM as a requirement for Windows 11, A, it makes you buy new hardware if you like stretching out your old computer, but then it gives you a way to actually get that device absolute identity from a cryptographic perspective, instead of, okay, fine, yeah, I stole the hard drive even, but yeah, it's still not the right processor on the motherboard, and so it's a different device.

[00:40:22] **Kevin O'Connor:** Yeah, I think that's the way that the industry is really going to have to move to solve this problem once and for all, because it goes beyond ransomware too, right? I mean, like, when an APT group like, in China or Russia, the bear or the panda is hacking your computer, they're looking for the same thing too, right?

They want to exfil data that's not theirs and then read it. , and being able to prevent that reading, I think, is the really important part.

[00:40:42] **G Mark Hardy:** Well, got it. Well, Kevin, this has been awesome. I mean, we could probably talk for another 45 minutes, but we're, we're getting close to the end of the show. So as a recap, we were talking about how small businesses, medium sized businesses, possibly even dentist offices, law firms, , small, medium banks, credit unions really do have a requirement for [00:41:00] cybersecurity, but that's, can be met with a trusted vendor that's providing managed security service providers. And by being able to do that, they can get beyond compliance. They can actually get some real security. That's going to function not just on a once a year audit or a periodic basis, but can either work side by side with a security team or at a lesser level, maybe take over when the lights go out and in the evenings and weekends.

Guard the hen house, so to speak, while everybody's out. We've looked at the importance of managed detection and response, knowing when things happen, that we find them pretty quickly and to prevent that from even happening in the first place, a solid vulnerability management program where we know what needs to be patched and how often it's patched.

And is it up to date? And do we know that? And can we assure ourselves that we don't have this risk when something comes out with a CVE score of 9. 8 or 10. 0 and I go, , I'm not vulnerable to that. You sleep better, and then ultimately incident response and forensics when something does blow up on you.

And again, [00:42:00] human patching, so to speak, being able to do security awareness training and testing and drills and exercises goes a long way. So any last thoughts you have before we wrap up? Otherwise, I think you've covered it beautifully. And, as I understand it, that where you're at tends to do a little bit of all these things and they're under one house.

Is that right?

[00:42:20] **Kevin O'Connor:** Yeah, absolutely. I mean, AdLumin kind of offers all these services. We try to integrate it into, one big sort of managed security detection response portal. And whether you go with Adlumin or somebody else, like a traditional IT provider versus security I think that these things are super important, and no business can really afford to overlook security these days.

They're coming for you, they're coming for everyone, which is the scary part because they want your money. And you know, everybody has something sensitive in their business pretty much, right? Whether it's the patient medical records and billing data or even just your customer list. You know, I think everybody has something that's worth defending and everybody should, make the minimal marginal investments to at least try to protect that.

[00:42:57] **G Mark Hardy:** Got it. Well, thank you. This has been Kevin O'Connor, Director of [00:43:00] Threat Research at Adlumin. I'm your host, G Mark Hardy with CISO Tradecraft. If you're watching us on YouTube, please go ahead and click the subscribe button. It helps us get rid of unwanted ads and get the message to you a little bit more cleanly.

If you're on a podcast channel, a couple of thumbs up or stars, whatever it is that help us boost our rankings so other people can find it. So we hope you found this episode today helpful for you and useful, and I wish you the best during the week. And until next time. Stay safe out there.