#148 - Threat Modeling (with Adam Shostack)

[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. I'm your host for today, and I'm joined by a friend of mine that I've known for a number of years, Adam Shostack, and we're going to talk about the world of threat modeling and why it's so significant for cyber security professionals and other security professionals, especially for those people who are on their track to become a chief information security officer. So a distinguished subject matter expert in the field of cyber security threat modeling, you've written two books on threat modeling and everything else like that. Plus some fascinating professional credentials to boot. So thank you very much for being a part of CISO Tradecraft.

[00:00:52] **Adam Showstack:** Great to be here.

[00:00:54] **G Mark Hardy:** tell us a little bit about yourself and your background.

Sure. So I've been in application security [00:01:00] for about 25 years now, a little over 25 years, and I had the opportunity to do this at Microsoft for about 10 of those joined in 2006, and they gave me this assignment, which was this threat modeling thing is broken. Go fix it. And at that point, I'd been threat modeling for seven, eight years.

I had written a paper with Bruce Schneier on the topic. And what Microsoft needed was scale. What Microsoft needed was not Adam and Bruce sat on the phone and talked about threats. It was how do we help 30, 000 software engineers develop better, more secure products? And so, they gave me the opportunity to figure that out.

The easiest way to share what I had learned was to write, threat modeling, designing for security. And then more recently, I've also written threats, what every engineer should learn from Star Wars, because as I [00:02:00] transitioned out of Microsoft, people started to call me and say, Hey Adam, could you help us learn to do this?

And I said, sure, and one day somebody said, so where do I go to learn about these threats that you're talking about? And I realized there wasn't a single, easy, fun place to go. And so I wrote Threats, What Every Engineer Should Learn From Star Wars. Came out in February this year. The reviews have been really awesome.

Well, congratulations, you know, a reading from the book of threats. Hey, so let's get into that a little bit, but before we do. Give me just a moment to share with our audience a word from our sponsor. Risk3Sixty is a cybersecurity technology and consulting firm. It works with high growth technology firms to help leaders build, manage, and certify security, privacy, and compliance programs.

They publish weekly thought leadership webinars and downloadable resources such as their PCI compliance program workbook, a business case for SOC 2, iSO 27001, The Path to Certification, and many more [00:03:00] titles all available for download at no charge at risk3sixty.com/resources. Let Risk3Sixty help you build your business case to achieve certification compliance.

That's Risk3Sixty.com/Resources.

And thank you for our folks here. But anyway, back to Adam. Thank you very much. So, wow. Threats, modeling, things like that. Well, let's, let's start with some basics if we can. Let's just start with a threat because sometimes people confuse threats and vulnerabilities.

And so, you know, if you already know that, don't tune out. Just, we're going to cover this anyway. We're going to, I like to build from the beginning. A threat. What's a threat?

[00:03:35] **Adam Showstack:** A threat is a promise of future violence. He threatened to beat me up.

[00:03:38] **G Mark Hardy:** That's it's actually not a bad one. Yeah. It's something that could go wrong. It's a threat actor is going to be obviously the instrument. of that future violence.

[00:03:47] **Adam Showstack:** Sometimes, sometimes there are threat actors. But we've got a volcano going off in Hawaii. That is certainly a threat to the people there.

[00:03:56] **G Mark Hardy:** or an earthquake in Morocco.

Yeah, And so, so threats [00:04:00] don't have to be from humans. They could be natural sources. They could be cyber threats. They could be malware. It could just be error. It could be a lot of things.

[00:04:07] **Adam Showstack:** Yep, and we use the term. You called in two of the other really important uses of the term there as threat actors, which we often abbreviate to threats, and as malware, which we also often call a threat. So I think that As professionals, we should be both fluid, able to go back and forth without getting really sticky about language, but we also should be clear, especially as we aim to communicate across the business.

When we work with people who are not grounded in security, bouncing from a piece of malware as a threat to a security problem as a threat, leads to confusion and leads to them not able to get to the thing we need them to do, which is [00:05:00] to fix some problem, to enable some controls, to manage detection better, to manage a response, all of those things, so that being clear as we speak can be helpful.

[00:05:13] **G Mark Hardy:** that's a very good point because a lot of times we, we look at risk, which my brief definition of risk is measurable uncertainty. If it's certain, it's not risk. And if it's not measurable, you can't really do anything with it. So, but risk being a product of threat times, vulnerability times asset impact.

And so breaking those terms out, sometimes we have to be concerned that you can't always change the threat. You can't make volcanoes go away. You can't go out there and make the hurricane go in a different direction, but you can change your potential vulnerability to that with countermeasures or avoiding the risk entirely and moving to someplace like Nevada where you're not going to have a hurricane or the like.

More to the point of what your research has been is more on the threat modeling. So rather than focus on the risk equation, let's come back to, to threat. So what is threat [00:06:00] modeling and why is it so important?

[00:06:02] **Adam Showstack:** So threat modeling is important because it's the measure twice cut once of cybersecurity. Anytime we build something, we're expending materials, we're expending, in the physical world, we expend materials, right? Measure twice, cut once, so that the piece of wood is not too short for the place you need it to go.

And in the cyber realm, we're expending human effort, people writing software. And so we threat model by asking four key questions. What are we working on? What can go wrong? What are we going to do about it? And did we do a good job? And there's specific technical ways to answer each of those questions.

You know, for example, we often use data flow diagrams to express what we're working on. But if we're working on a single page web app, maybe we'd use a state machine [00:07:00] to show how it works. We often use STRIDE, spoofing, tampering, repudiation, info disclosure, denial of service, and elevation of privilege.

[00:07:09] **G Mark Hardy:** That's 500 points on Hacker Jeopardy, by the way,

knowing all the answers

Is it really?

Well, not anymore. I don't do the show, but I had done it for about 20 years with

[00:07:17] **Adam Showstack:** Okay, okay, so, 500 points for ya. And that's one way to do it. Another way to anticipate what can go wrong, or to answer what can go wrong, is to use killchains. We can use killchains prospectively to talk about... What could go wrong in a system? And so threat modeling is this collection of techniques that helps us anticipate future problems so that we can either move to Nevada, build out of concrete, or otherwise think about what are we going to do to reduce the impact of these threats that are associated with [00:08:00] our systems.

[00:08:01] **G Mark Hardy:** So it seems then is that by doing effective threat modeling, we're able to enumerate the range of potential future destructive things or future bad things that might occur. And then we could go ahead and map them out accordingly. Something that hits us out of the blue that we didn't expect that we didn't see coming is a little bit difficult to threat model.

Those black swan events and things such as that, COVID. A once happens once a century like clockwork having a pandemic is a little bit tough to model and quite honestly is often not within the purview of a business to manage. Now, one might argue that a government should have that oversight, and if you think about.

I mean, we're mentioning hurricanes. Remember Hurricane Sandy when it hit New York City and the last hurricane they had that hit New York and New York

was what, 1950s or something like that. Well, the average business who said, Hey, yeah, we'll put our data center in the basement. Probably wasn't thinking on 50 year horizon, but the city government should have had 50 year horizons.

And so [00:09:00] what we look at is depending upon where we're at in the organization or what. What type of organization is the criticality of, um, if you will, boiling the ocean a little bit more until we get to the point where we've sort of enumerated all these threats. So once, how do we know when we're done?

How do we know that our threat modeling program has reached, if you will, a saturation point where it's beyond the cost effective point to keep going? And then what do we do next?

[00:09:25] **Adam Showstack:** Okay, so there's a whole bunch there.

[00:09:28] **G Mark Hardy:** I know. Sorry about that.

[00:09:29] **Adam Showstack:** So, there are some very mechanical answers, right? If you don't have a Dataflow diagram, you probably haven't done a good job. If you don't have a list of threats, you probably haven't done a good job. If you don't have a spoofing threat, the S in STRIDE, probably haven't done a good job.

And so we can use techniques like that to say, did we cover what we expect? Did we follow a [00:10:00] procedure? And you can write lots of different procedures to help you threat model, but did we do those things? And if we can't answer them, yes, we're probably not doing a good job. And I want to come back to the question of how do we get started in a second.

But I want to, I want to first talk about the Black Swan thing. It's easy for us as security professionals to focus on the Black Swans. It's also easy for people who are not security professionals who are building systems to forget to install the fire alarms. to forget to put the ground fault indicated sockets into the bathrooms.

And when I look across the flaws that attackers take advantage of over and over again, they're not black swans. They're not once in 50 year events. They are things where a small [00:11:00] amount of expertise Brought in through some basic threat modeling can have a dramatic effect on what it is you're building.

And the reason that I wrote The Threats What Every Engineer Should Learn From Star Wars book is I believe, well maybe we have some Jedi's? We also

have... The pilots, and the ground crews, and the rangers, and the cooks, and a rebellion involves all of those people coming together to achieve a goal. And I would like everyone in your organization to do a little threat modeling.

And I think this is where a CISO or an aspiring CISO can really have impact is by not aspiring to be the hero who's going to do it all. Like when I joined Microsoft, I said, I've got to [00:12:00] scale. This is the opportunity for you. And so, thinking about this, and realizing, and I was talking about policies and procedures, and it was sounding a little heavyweight, perhaps.

So I want to loop back to just asking the four questions of what are we working on, what can go wrong, what are we going to do about it, did we do a good job? If you simply start asking those questions, your threat modeling, and you're going to develop skill, And as you develop skill, as you get more experience, you'll start to be able to say, Wow, this one went well.

This one didn't. What happened there? Do a little bit of retrospection. Do a little bit of asking questions. Did we do a good job? How come? Really powerful. Doesn't have to be complicated.

[00:12:52] **G Mark Hardy:** Sounded that way. Now you had said that you'd come back to the question about getting started. So let me remind you of that, if I might.[00:13:00]

[00:13:00] **Adam Showstack:** Really, just ask the four questions.

[00:13:03] **G Mark Hardy:** That's it then. It sounds pretty straightforward. Yeah

[00:13:06] **Adam Showstack:** It's very straightforward. And so let me give you, let me give you the simple but hard part. Give people a chance to answer the questions. Listen to them as they speak, appreciate their answers. I have almost never met a person who had no idea what could go wrong. I meet lots of people who say, Dude, you wrote a book on this.

You tell me what can go wrong. But you know, I know, I know lots about threats. They know a lot about their system. They know a lot about their business. And... Everyone has a perspective on what can go wrong if you are willing to respectfully listen to what they have to say. And once you start to do that, more and more stuff comes out, and it turns out that [00:14:00] having the language of, what can go wrong here?

really enables collaboration across the business, which is so important to a CISO, right? There's so many stories, there's so many stories about conflict between security teams, business people, security teams, and operations people. If we get everyone into the habit of talking about what can go wrong, then we get to the question of what should we do about that. And we may have disagreements, but at least we have a list of things that might go wrong. We can input that into our risk management process. Some of them are really easy to fix. Some of them are really hard to fix. But once we have that habit, We can get more and more skill, we can get more and more technique into how we do this work.

And one of the, you know, one of the mistakes I see people making [00:15:00] is they want to have a debate about do we use Stride or do we use Killchains or do we use this or do we use that. Do something, you know, and, and look, if you're a young person listening to this podcast, I hope you are maxing out your 401k. And we could get into all sorts of debates about asset allocation and this and that, but there's this wonderful thing that banks have created called target date funds, right? You know, Mark, you and I are going to retire in a few years, so we might buy a 2030 target date fund.

And the bank will adjust that so that it's more bonds and less stocks than a 2050 target date fund. It lets you get started, and if you want to get clever about it, you can. But the crucial thing is get started. Put some money in your retirement account. Think about what can go wrong. I might run out of money in retirement.

What am I going to do about it? [00:16:00] I'm gonna, I'm gonna take advantage of these tax advantaged funds.

[00:16:03] **G Mark Hardy:** Yeah. So really it's more than just looking at the threats. It's looking at the whole ecosystem to be able to say, If I could take, for example, your book on threats, it kind of get me thinking in the right idea, go to the subject matter experts who are in my organization, who may be aware of it either consciously or subconsciously.

But if I can go through and say, well, what about this or this now? Oh yeah, that there. Now, what you're doing is you're really adding value. What you're able to do then is you're sort of coaching people through their own self awareness of what their threat environment was like. And because you all ultimately are trying to defend the same organization, you're sort of seeing as that person is pulling everything together, unifier, if you will, as compared to somebody who's pushing against unity.

And that to me seems like a really good career builder, as well as just helping you add value in your particular role or job.

[00:16:54] **Adam Showstack:** And, and the, yes, absolutely. And the other thing that is [00:17:00] so important is the when. You know, once, once you've built your house out of wood, it's very hard to go back and rebuild it out of concrete. You have to tear down all this. You have to, you've paid for the wood. It's no good anymore. It's junk because it's been cut and nailed and painted and what have you.

You have to tear all that down. You have to dispose of it. And then you have to build a new place to live. if we can have the conversation early, Instead of waiting for the pen test, instead of waiting for the people to run in and say, Mark, I need you to approve this risk. We get such a different result.

It's. It's magic and I know the people who are listening, some of you are being like, eh, don't work that way. I, I've been doing this for years and it always hurts. I'm gonna say, stop beating your head against the wall. Threat modeling gives you a way to get started [00:18:00] early, to have the conversation early, and when you do that, so much changes.

[00:18:07] **G Mark Hardy:** So now by having that early conversation, by involving multiple elements, by having some sort of a methodology, whether, as you said, it's the, the stride or dread for another 400 points, right? Damage, reproducibility, exploitability, affected users, discoverability. So there's probably a lot of other models, but from your perspective, it doesn't matter which model, it doesn't matter which mutual fund, just get into one, if you will, just.

Get something that's defensible. So people say, why are we doing it this way? Well, you know, it's a reading from the book of Microsoft or reading from the book of threats and then you can invoke something a little bit higher than yourself, but more importantly, it gets everybody on the same page. And so now you're using a similar terminology, same measurements.

All trying to come ahead and roll this thing all up together.

[00:18:52] **Adam Showstack:** Yes,

[00:18:53] **G Mark Hardy:** I like your analogy of the wood house, but sometimes we find out that when we take jobs, we come into a business, we come into an [00:19:00] opportunity, and everything's, it's made of wood. You know, how do you know she's a witch? It's made of wood.

Right. So, know, for little Monty Python fans there. And so, you can't tear the whole thing down and everybody stays out in the rain and shivers. You have to start building it up. And so, there's going to be a way to, to slowly move from a, You know, if you will, a threat vulnerable environment to a less threat vulnerable environment.

And that seems to seem that we have to prioritize things that we can do. Our modeling might have prioritized this threat as the worst threat, and therefore this asset might be the first thing we start to build out of concrete. And instead of, and then we'll abandon the wooden one. Does that, that makes sense?

[00:19:39] **Adam Showstack:** It does, and I think there are two, two ways to think about what we're gonna go chase. We can chase the most fluid thing. Or we can chase the most worrisome thing. And the reason I like to chase the most fluid thing is because we're [00:20:00] already planning to make changes there. And so it's easier to make changes.

That's sort of tautological, but the organizational energy of where replacing our CRM system is a great time to think about what do we do to secure our CRM system?

[00:20:18] **G Mark Hardy:** There's a lot of wisdom in that. So I say that again, go for fluidity because those are the things that are up for grabs anyway,

I love that.

[00:20:27] **Adam Showstack:** and the other way to do

it is you can do some very inexpensive threat modeling. Back of the envelope, how does this system work with five or six lines and five or six boxes? Right? So our CRM system talks to customers via web browsers and apps and something else.

And it sends its data to payments and to manufacturing and to shipping or our HR system talks to this and does this. Really, [00:21:00] really simple and very high level. What's the worst that could happen if this system goes badly? You don't have to do this in depth. You don't have to do the fancy diagrams.

Look, my book is full of fancy diagrams. I'm, I'm a big fan of learning different techniques. And I want to assure you that if your goal is to go broadly across an enterprise, The best way to do it is to do it quickly, so that you can say, Hey,

wow, when I compare these 50 systems, these 500 systems, whatever it is, these are the ones that give us the most worry.

And if you're going to do a two week, a one month project for each of 500 systems, well, if you're doing a month for each of 500 systems, that's 10 person years. Maybe you need to get it down to two hours per system.[00:22:00]

[00:22:00] **G Mark Hardy:** Mm hmm.

[00:22:00] **Adam Showstack:** And if you're going to do that, and let's talk about modeling, right? Models... There's a, there's a British statistician who said all models are wrong and some models are useful.

And what he meant is that a model involves throwing away detail. You know, behind me, you can barely see, you, you can only see the end of it. I've got the Luke Skywalker land speeder model over there. Here, let's move the camera so you can see it. You can also see my Lego space station. The model...

[00:22:30] **G Mark Hardy:** those are illegitimate business expenses. You're writing your book on

threat on

Star Wars. Okay, I get it.

[00:22:36] **Adam Showstack:** The model is inaccurate, but it's evocative, it shows us something, and that model landspeeder is pretty big. It took me a couple hours to build. I can build another one with fewer pieces, less fidelity, less accuracy, but it might also be useful because it's cheap and easy to build. So [00:23:00] threat modeling involves sometimes different levels of modeling, more and less accurate, faster or slower.

And I take a page from the agile world here, stop early. Do it quick, see what you learn from having done it, and see what you need to enhance.

[00:23:22] **G Mark Hardy:** Now let me play a little bit of devil's advocate here and give you a chance to show the redemption. So, I understand the value of threat modeling. I am going to go ahead and enumerate with my experts, all of the potential things that could be out there that are future, bad, et cetera. I come up with a comprehensive list.

I'm able to then, if you will rack and stack them against my asset list, but there's a person who might come in there and said, so what? Who cares? You can't change those threats. For the most part, most threats are immutable. They exist whether or not you want them to exist. [00:24:00] And so therefore, all that care and effort in doing the threat modeling Isn't that akin to when Steve Jobs used to say, when I take the cover off the iPhone, I want everything to look beautiful inside, even though nobody could see it.

Well, obviously there's some value in that because we know that the iPhone was a work of art, internal, external, and it worked really well. So how do you address the fact that you're not over engineering that part of the problem, but in fact, it's causing the foundation for effective response to that?

So, we could

[00:24:32] **Adam Showstack:** spend an hour on that. It's a great question and the first part of my answer is, if you haven't gone and looked at, excuse me, You have to go and look at the building as a whole. There's an old cartoon with a 20 foot high single slat in a fence and no other slats in the fence, and your attacker just goes around it. There's a, there's a photograph of [00:25:00] one of those lifting gates on a road with grass and snow, and you can see in the snow where everyone has driven around the gate. So at some point, you need to look around. And get an evaluation of what the whole is. And even if we're not going to do anything about some of those things, how do you know you're defending the business if you haven't evaluated the business by looking at the value flows of your business, right? If you're on a tear over SQL injection. Great. You're going to fix the SQL injections and those are probably really important. But if you miss the fact that you have no login screen, if you miss the fact that you have no defense against brute force and your admin password, like it is on my printer is literally on the page that you get when you go to the [00:26:00] printer, it don't matter that you fix the SQL injections because your password is literally in your HTML source code. anyway,

[00:26:08] **G Mark Hardy:** So do you find that examples when threat modeling helps to discover critical vulnerabilities? I don't know whether, you know, printing out the about me page on a printer qualifies as sort of the threat modeling, but one of the things we do care about obviously is critical vulnerabilities and then addressing those.

So let's talk a little bit about how, as I say, foundationally, this moves us toward that actionable remediation.

[00:26:32] **Adam Showstack:** sure. So, so I think about vulnerabilities, and I think about flaws. And a vulnerability is a thing that everyone agrees shouldn't be there. And a flaw might be a feature that's badly designed. It might be a missing feature, right? Let's say you have a login screen that has [00:27:00] no password strength tool. Is that a problem, right?

Maybe it should, but maybe you've got mandatory multi factor authentication, and so you don't really care if the password is good because you're using a strong second factor like an app. We need to look for those things, and yes, the threat is always there, but we get to the third question of what are we going to do about it.

And so, I think we need to look to both vulns, but we also need to look to, oh, we, we have no way to detect that somebody is trying to log in as Mark. Is that a vuln? It sure is a feature that if I bring it to the business people, they might want to say, yeah, we should fix that. I don't want to be critical here, but I'm gonna point out a behavior, which is that we only want to [00:28:00] look for the vulns that we can use to pop to get a great result on a pen test.

And I think that's a mistake. I think we need to think more broadly. We need to think about the threats. Then what are we going to do about it? Some of that might be preventative. Some of it might be detective. Some of it might be responsive. But, if we're not threat modeling, what are we doing to ensure that we're thinking about the system as a whole? One answer is we're going to use a controls catalog, right? And we're just going to take all the controls from the control catalog and put them in place. But if we're not sure what we're fixing, if we're not sure what threat we're addressing, we're going to be less effective.

I want to point out a behavior which is to focus in only on vulns, and I think it's so important to also look at the system as a whole, make sure it has the security [00:29:00] controls, the security properties that we would like it to have. Because if we focus in only on the vulns, we find ourselves missing some of these important features that we need to develop or deploy in order to make the system as a whole work the way we want it to.

[00:29:21] **G Mark Hardy:** Interesting. Now, have you seen the threat modeling work well with third party risk and looking at business partners? And if so, is there anything different about that or is it pretty much the same approach just with a different data set?

[00:29:34] **Adam Showstack:** You know, we continue to ask, what are we working on? Giving this third party a bunch of our data. What can go wrong?

They can lose control of it. They can use it in ways we don't want them to. And so, you know, as a, as a trainer, I often get these exceptionally long contracts from people. And my first response is, don't [00:30:00] give us your most crucial design docs.

Don't give us any customer data. I don't want your customer data. The way we, the way we threat model. The way of asking the four questions remains identical. The details of how we answer those questions adjusts. And this is one of those things that actually really helps illustrate why does Adam keep talking about the four questions. It's because when we get to Does anything change?

You're still doing the same things, you're just doing it a little differently. It's like moving from one programming language to another. Yep, a bunch of stuff has changed. We're writing our code in this language instead of that one. And a bunch of stuff has stayed the same. We're still thinking about what the code needs to do, thinking about edge cases, we're still using version control, we're still, hopefully, writing [00:31:00] unit tests.

[00:31:00] **G Mark Hardy:** Yeah, sounds good. Now, a couple last questions before you get to wrap up here. Are you seeing anything in terms of new or emerging trends or technologies that may impact threat modeling. And if so, is it for the better or for the worse?

[00:31:13] **Adam Showstack:** You know, like anything else, LLMs are coming to change our world. Um, and it turns out that LLMs are not particularly good at thinking about threats to new systems. The thing that I'm talking to some people about, haven't figured out if it's going to work, is let's use the LLM to draft documentation, to take notes out of a meeting, and get those notes into a good form faster.

I do think that in five years, We'll see LLMs that can threat model better. There was an interesting talk from some folks at Datadog at Black Hat this summer about using LLMs to help you figure out which [00:32:00] features the security team wants to talk to you about. Well, that's related to threat modeling, right?

Is something going to go wrong with this feature is a lightweight way of asking what can go wrong. So I think that, for me, is the most interesting shift in my world is LLMs.

[00:32:21] **G Mark Hardy:** And so I guess kind of almost like a penultimate question here is that as we look at populating our threat models and the like, and we've talked to experts and we've collected their information and things, how

much of that can be automated? And does it make sense to try to automate it or does it still really need the human touch in there to be effective?

[00:32:42] **Adam Showstack:** A lot of the difficulty in threat modeling is getting yourself out of your head, right? It's hard to write code that works. It's hard to write code that's performant. It's hard to think about what can go wrong with the code [00:33:00] as you're writing it. So, I think that... These tools are really going to help us do the work, but they're not going to replace the human expert. They're going to augment us, they're going to help us think about this new thing in a better way. And I think over a couple of years... We're going to see some big transformations happening.

You know, we already see people using machines to help them write code, which was scary when it first started happening in the 1950s, and people replaced assembler with compilers. Oh, but you thought I was talking about LLMs. Um, but seriously, we, we are getting further and further from the machine. And sometimes when we do that, we see the machines that write code that write code do it badly and then we figure that out and we help them write code better.[00:34:00]

I think we're going to continue to do that and security will become easier as a part of how we have the machine write the code as we start to standardize on questions like, Show me the vulnerabilities in this code that I just wrote. Show me the vulnerabilities in this configuration file for this product.

What do other people do with this product in this situation? Oh, you're using this configuration option. Many of our customers also use these three configuration options. That seems like a really interesting thing. And as we get there. The ability to up level and the ability to ask what are we working on and what can go wrong and to answer those questions in cogent ways is going to get more and more important.

[00:34:53] **G Mark Hardy:** Well, that sounds great. And we're kind of running close of out of time here. So I just want to call something out for our listeners. Adam's written two great [00:35:00] books on this topic of threat modeling, which you can find on Amazon. And we'll put some links to that in our show notes if it's okay. The first is Threat Modeling, Designing for Security and Threats.

And the second, which you said came out earlier this year, What Every Engineer Should Learn from Star Wars. Of course, threat, what every engineer should learn. Great. They're a wonderful way to condense their knowledge and

put them together. As you can see, I got a whole bunch of them over my shoulder.

Most of them are read. Some are still on my list of things to read, and I have not had the privilege to read your book, but it sounds like I need to put that on my list of things to do and so it's been a pleasure. Any last thoughts you'd like to share with us before we wrap up?

[00:35:33] **Adam Showstack:** I, I think my, my last thought is some people get a little bit intimidated by the size of my first book and think that threat modeling has to be hard. Just go to the four questions, get started by asking what are we working on and what can go wrong. It's transformative. Every day I meet people who tell [00:36:00] me how starting to ask those questions has enhanced their career, helped them deliver more value to their organizations, and so the journey is rewarding, but only if you get started.

[00:36:14] **G Mark Hardy:** So the trick is get started, just, just do it if you will, so to speak. Well, Adam, thank you so very much for being part of the CISO Tradecraft show. It's nice again to see you again, at least virtually, and hopefully catch up with you again in person at another one of our security, either conferences or speaking events that we tend to do so.

For our listeners, we hope that this podcast really helps to drive some thinking toward the importance of threat modeling and being able to ask those four key questions. What are we working on? What can go wrong? What are we going to do about it? And did we do a good enough job? But if you ask that repeatedly and you focus on that in a structured methodology with a way to show results, you're going to improve, you're going to reduce your, your risk because you're able to identify where the problems are coming from.

I like your idea about look for what's in flux, look what's about to [00:37:00] change. You have a better chance of changing that than something that is not going to be updated or funded for a while. So for our listeners, if you're following us on, LinkedIn. That's great. If not, please do so. We do have more than just a podcast for you.

In addition, we have additional notes that we put out there and we forward some high volume, basically say high, high signal to noise information. If you're watching to us on YouTube, click the little subscribe button. It does help us because if we get our numbers up, we can avoid getting those nasty commercials that sometimes pop up without us wanting them to pop up with.

And if you're following us on LinkedIn, share with your other friends as well. So thank you again for being part of the show. This is your host G Mark Hardy. And until next time, stay safe out there.