#155 - SOC Skills Part 1 (with Hasan Eksi)

[00:00:00]

[00:00:11] **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. I'm your host, G Mark Hardy, and today we're going to talk about how we train folks to become really good incident responders within a security operations center. to do that, we're going to bring on Hasan Eksi from CyberNow Labs to discuss a number of skills, there's 20 of them in all for incident responders and things that they should know. Now I agree we might not get to all 20, but we're going to do the best we can in the time we have available. And so, Hasan, welcome to the show.

I'm going to take a quick pause and give us a commercial word from our sponsor. Adlumin provides enterprise grade security to mid market organizations. Its [00:01:00] 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, 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. Visit A D L U M I N dot com. Well, Hasan, welcome to the show. Can you tell our listeners a little bit about your background and maybe what got you started in training incident responders?

[00:01:51] **Hasan Eksi:** Thank you. Thank you, G Mark. It's an honor to be on your show. First of all I like to call myself a cyber security workforce developer. Real estate [00:02:00] people develop buildings and I develop cyber security training platforms then and help people transition into cyber security. I've been in security for the past 13 years.

I wore many different hats at multinational organizations, last two being Capital One and MasterCard prior to kicking off CyberNow Labs back in 2018, together with my co founder, Omer, and jumping into the startup world. Fast forward to today aside from everything that I do at CNL I'm involved with a number of

cybersecurity companies as an investor and as a board member as well about CNL and how things started.

If you go back to 18, I, Omer and I formed a Nova Northern Virginia cybersecurity meetup group that meets at Nova Labs here in Virginia. Some of you may have. maybe familiar with it it quickly grew to more than a thousand local members, and we saw how hungry [00:03:00] people were to learn pretty much anything about cyber in general, and we wanted to turn that experience into something unique and something that helped people realize their potential in cyber security, because most of the folks that attended those sessions were entry level people who are looking to transition into cyber security, but didn't really know how to do it.

That's when we said, challenge accepted, and kicked off CyberNow Labs. The only enterprise grade, SOC based, secured operations center based I'll try to not use acronyms as much as possible secured operations we've got more than enough of them based hands on cyber security training program.

And hands on experience is something that the industry is still, I think struggling to address to the state. Back when I graduated from University of Maryland with a comp sci degree, I thought, you know, I'll get a job very fast. And I had my first [00:04:00] set of interviews and shocked to learn that I I actually, despite the fact that I took a few cybersecurity classes, I knew very little about cybersecurity.

And I learned what hiring managers mean by hands on experience in those interviews. And we'll get to the definition of hands on later, and I think it's important. But our first cohort had only seven trainees. And fast forward to today, we've helped thousands of trainees with finding their first cybersecurity job.

CNL is the biggest cybersecurity vocational school in both the United States and Europe. It's not third party vetted, by the way based on our own data open for challenges.

[00:04:46] **G Mark Hardy:** Now I'll take your word for it. That sounds good to me.

[00:04:48] **Hasan Eksi:** The gap is big enough. The talent gap is way big, and we can have multiple CNLs in the space, really, and we will still not be able to address the gap.

And we did a [00:05:00] merger about a year and a half ago with Mike Myers Total Seminars Group and LP First Capital, and formed National Cyber Group with the leadership of Philip Niedermeyer. He's a Senior Advisor to the Cyberspace Solarium Commission. And NCG now publishes books like Secure to Plus, Net Plus, A Plus, to name a few.

And we have over a million students on Udemy, and we were moving ahead full force to close the cybersecurity gap, skill gap, and experience gap, as Debbie put it from CloudRangeCyber a few podcasts ago on your show.

[00:05:35] **G Mark Hardy:** Well, that's really cool. I mean, it's really good to see the unique focus that you're doing. And one of the things that really sticks out to us is kind of how different your program is from traditional learning opportunities. Now, here's what I mean by that for a lot of high school kids that want to get into cyber, there's a few things to do.

They can read books and study or get a cyber certification like security plus or a certified ethical hacker, and this makes them book smart and they learn [00:06:00] certain terms. And they can go to college and learn how to program or even find classes in cyber security. But there's still a concept based approach to learning.

See, a lot of college programs. Don't necessarily provide students with the tools that are used in the industry. So you might have a class on intrusion detection systems and get a high level overview of concepts. Maybe even write a few snort rules, but you probably aren't going to be playing around with some of the tools of Palo Alto's or CrowdStrike software in the course of what you're going to actually find in the workplace. Finally, you also see things like hack the box type of systems where you learn how to pen test using something like a Kali on a vulnerable system. However, this is more on the offensive side, and it really misses the majority of what we try to do in the cybersecurity world, at least as professionals on the blue teams, if you will, is finding the bad actors and doing the defensive role.

Now, Hasan, you're doing something really very different. You've created an opportunity where folks get firsthand experience. Using the very same tools that are encountered [00:07:00] in the workplace. Can you talk a little bit about the program that you've stood up and how it works?

[00:07:04] **Hasan Eksi:** I would love that. Thank you. First of all we call our trainees Cybersecurity Analysts from day one. Whether they start from the

definition of what an IP is. Or jump right into the incident response, doesn't matter. I believe one of the biggest challenges is to give people that confidence.

Because cyber, the word cyber security is intimidating enough. And make them feel that they're working like a security analyst. And make sure they understand the work they're about to dive into is the same type of work that their peers at Cisco, Arctic Wolf or other MSSPs are doing on a day to day basis.

We want them to think like an analyst. Every day, not just for one day, or for a week, or for a month. Every day, until they get the offer letter, until they have the offer letter in their hands. From that [00:08:00] point on, it becomes their problem, so that's where we stop. But moving on to our approach. We start with IT fundamentals where we spend two weeks to make sure everyone knows the ABCs of IT.

Everyone knows what an IP address is. After that we move into security+ where we spend eight weeks, not just. Five days, but eight full weeks on networking and SecPlus topics and really get them CompTIA SecPlus certified at the end. The primary goal here is to get them comfortable enough in speaking foundational cyber topics because this is what they need during the interview and certification is the secondary goal.

This is a topic by itself. I think we can do a podcast separately on certifications. But at this point. At the end of the eight week period, they know the language of cyber security and they can communicate with the cyber professional and have a decent conversation. It's like, I like to give this example to trainees it's like having a [00:09:00] driver's license, knowing all the theoretical stuff and reading, being able to read signs, etc.

But having no real experience behind the wheel. And there are a lot of people out there today. At this stage, the next stage is hands on where we spend 12 full weeks inside an enterprise grade security operations center with best of the breed products on a real network, working on real incidents and writing tickets, just like an incident responder at a MSSP again, just to name a few, they work with Splunk, QRadar, CrowdStrike, Sentinel 1, Proofpoint, and a bunch of other best of the breed products from various domains of cybersecurity.

And it's not a click here, click there type of training. It's more about SQL injection detected in one of the applications. What do you do? Brute force detected. What do you do? User clicked on a phishing email. How do you analyze that email? [00:10:00] And how do you purge it from all inboxes? How do you write instant response tickets?

And how do you communicate with other IT teams? These are, if you look at it, these are all the things that a, an instant responder does on a given day, right? At MSSPs. And my business partner, Omer he used to run SOCs and he says when there's a critical incident, the SOC floor gets less crowded and sometimes people disappear as well.

This happens because it's tough to be in a position where incidents may be coming at you from different directions at the same time, and you need to stay resilient and you need to stick to the plan. And it's not all technical either. Analysts that attend SOC shifts, secure the operation center shifts at this stage, and they learn how to run a shift, a real SOC shift.

The last part of the program is, all about interview prep and job search support. This is where we polish their [00:11:00] resumes and make sure they have all the right things on the resume. We ask them to attend associate shifts and mentor meetings every week until they get an offer letter. And these mentors are people who graduated from the program, found a job, and they're coming back to, to share their experience with others.

And we know... It's not an if, it's more of a when question. And if we keep doing the right things, the offer letter will present itself. That's the most difficult and challenging part. We just need to stick with the plan. And we also tell them we will support you until you get an offer letter. That's how much we believe the plan works.

We don't care whether it takes a month or a year. In fact we take it even further and say, we'll defer. 50 percent of your payments until you get a job as long as you're actively searching for a job. And the overall goal of the program is to help them become what we call a [00:12:00] T shaped person who has deep knowledge skills in incident response and security operations and a broad base of general cyber security skills.

[00:12:11] **G Mark Hardy:** Wow. I mean, that's sounds awesome. I mean, we're a big fan of what you're doing. It's really kind of challenging the paradigm of a traditional skill development for our industry, which is, get out your checkbook. And better have an extra set of checks because this is going to cost a lot of money. And and now you've been doing it a few years and in doing so, you've accumulated a number of accomplishments.

What are the ones that you're probably most proud of?

[00:12:38] **Hasan Eksi:** Sure. I think the biggest accomplishment is that because of our efforts and all the 120 hour work weeks that we put in for the past

[00:12:47] **G Mark Hardy:** part time, right?

[00:12:48] **Hasan Eksi:** we're together with the team. There are more people today waking up as a cybersecured analyst and influencing their circles and inspiring [00:13:00] them as well and helping their companies and their nation.

wherever they live, to be a safer place. The second thing is our cohorts are about 50%. It ranges from 45 percent to 55 percent depending on the cohort. Women, and most of them come with no work experience at all. Forget about IT experience. I'm talking about work experience, and they now work at places like NASA as a secured engineer, White House, GDIT, Tesla, Bank of America, Doge Telecom, BMW, to name a few, and these are real people with real stories and they have an impact on national security. They have an impact in their communities and success is contagious. So the community aspect is very important. Lastly, I must say I'm also proud of all the smart people I get to work with every day. It truly is a team effort and I was lucky enough to have great minds and committed souls [00:14:00] around me.

And we were locked in on the same mission 100%. And this is something I tell the trainees as well. Surround yourself with motivated smart people and stay away from negativity, Netflix, Twitter, and YouTube. The rest will come.

[00:14:15] **G Mark Hardy:** Well, this is going to be on YouTube, so we ought to have at least a carve out for something like that. Okay. So, I think in our discussions, there's 20 different skills that organizations need from incident responders. And, I know for our audience, you're thinking, 20 seems, A whole lot. But trust us, now, we're going to go through a number of those, and I recognize that to be able to do this justice, we probably need two or even three episodes here.

So, if we do not get all the way through, then we will put this information for you in the show notes. But listen along and tell me if this makes sense. The first thing you want is an understanding, as you had mentioned, about cybersecurity fundamentals. A strong understanding of basic cybersecurity concepts and principles like Operating systems [00:15:00] databases, networking.

It's really important. It's basically impossible to write any filters if you don't understand the basics of what's an IP address or what is a port or how to subnet

mask. And Hasan, how important is this to learn? And do you have any best practices that you use to take somebody who has zero experience in this area to learn these types of skills?

[00:15:21] **Hasan Eksi:** Sure. This is the key part. G Mark. And have you seen one of those marketing funnels?

[00:15:26] **G Mark Hardy:** Oh yeah. You know, you get the free stuff here and you go down and then all of a sudden that's the high

value stuff there. Yeah.

[00:15:30] **Hasan Eksi:** Yep. Starts with awareness at the top and considering, interested, and finally purchased. At the top of the funnel, you have the most number of leads, people, and as you go down, it gets smaller and smaller.

And finally, you end up with maybe 5%, if you're lucky, of the leads that end up purchasing. I think our challenges in cybersecurity is very similar and cybersecurity fundamentals is where everything sort of starts. This is the awareness stage and we want to maximize it as much as possible. We [00:16:00] need more people at this stage so we can end up with more people at the bottom of the funnel.

And As our group CEO, Gabe, he likes to call it. We need more people that wake up in the morning and say, I want to work in cyber security. And he's the guy who led a company called Zology. They're the nation's biggest dental and medical assisting school. And he's a marketing genius. And I was explaining to him.

How we spent like 0 in the early days on marketing and have cohorts of 150 people just to be a word of mouth. And he was pretty impressed because training companies spend well over 2, 000 on marketing to acquire one student today. It's great but it's not enough. It's not enough to address the gap at the national level.

And this is the reason why we now offer... Free two week IT fundamentals training and also free security plus training to qualified individuals as well on top of everything. And I repeat, we need more people at the top of the funnel, and I think we're already [00:17:00] falling behind the competition and most of the nations.

And as you know, China has a national cybersecurity center that graduates thousands of people every year that spends. 40 km2 space with schools, incubators, etc. And I think we can do better than that.

[00:17:17] **G Mark Hardy:** I think so too. And I think you're doing a lot of great actions on that area. So cybersecurity fundamentals, number one, number two is incident detection. That is the ability to identify potential security incidents through various means, including monitoring alerts, analyzing logs, and this is really fundamental to stopping attacks.

If you can't detect them, then preventing them is pretty much unlikely to happen. Hasan, can you talk about what we need to teach folks to identify incidents effectively in a SOC?

[00:17:44] **Hasan Eksi:** I think two things are important, knowing which way to look and attention to detail. The more time you spend working on different types of incidents, the more you're able to point out anomalies. [00:18:00] Because the more you understand baselines, what's normal and what's not normal. And this helps a lot. The first one may take hours, the first incident may take hours, or maybe days.

But the next one will take much less if you know exactly where to look. Just to give an example, we have quite a few ex law enforcement folks in the program and they're great at incident detection. With them, it's very natural. I think it has a lot to do with with their daily work constantly looking for anomalies or threats.

[00:18:34] **G Mark Hardy:** Yeah, and so Cybersecurity Fundamentals, Incident Detection, the third one is Threat Intelligence. Essentially when folks have good understanding of the current threats, the attack vectors, and the attacker's techniques. Remember, cyber is an evolving game of attacks and defenses. We build walls, they build ladders, we build moats, they build catapults, and so it continues. So what should new members in this community be learning about with respect to [00:19:00] threat intelligence?

[00:19:01] **Hasan Eksi:** So cyber threat intelligence AKA CTI is a broad topic and sky is really the limit here. But I think one needs to be. patient, be able to read, digest, and organize information, because there's a ton of it out there, and it's easy to get lost and really understand the criminal's way of thinking.

and their motivation to be a successful cyber threat intelligence analyst. There are tons of open source tools that can be used to play around, although we use

our own in house CTI solution. Understanding where IOCs come from, how do they work, custom rules, et cetera is key and really staying on top of emerging threats and being able to take action immediately.

And there's a whole. thing around industry specific threat intel too. If you're working in financial industry that's [00:20:00] different than others industry, you need to be plugged in to those feeds and really need to stay on top of your game and make sure you know what's going on in your specific industry.

[00:20:11] **G Mark Hardy:** Makes sense. Now, the fourth thing I want to talk about is that there are different cybersecurity tools, and it's important to know which one is best for the job. Essentially, you wouldn't use a rake to dig a hole, you'd use a shovel. So, gaining proficiency in various security tools that would be found in a SOC, such as a SIEM, your Security Information Event Management Tool, Intrusion Detection and Prevention Systems, Antivirus. Email, Security Gateways, Endpoint Detection Response, EDRs. That's really key. Hasan, do you find that folks often specialize in one of these tools more than the others, or is it really helpful to get people trained in multiple tools so that they can spot an incident from multiple directions?

[00:20:51] **Hasan Eksi:** There's multiple ways to do it here. We touched on some of those tools earlier. Cyber is a domain where you have limitless [00:21:00] opportunities to learn and become what's called that T shaped person. Every tool is different and some folks may like Splunk over QRadar. Or CrowdStrike over SentinelOne. And in case we come across that a lot in our training as well someone like CrowdStrike for no reason, they like the UI, for example.

But they like, or CrowdStrike over SentinelOne more. And what I tell them is that the name of the tool does not matter if you like QRadar for whatever reason, or Splunk for whatever reason, or CrowdStrike for whatever reason. Go for it. Dive deeper. Spend more time with that tool and do not stop until you feel comfortable using it.

And this is going to take practice. This is not going to happen overnight. It takes weeks. Sometimes it takes months. You need to be patient with it. And it'll be much easier if you do it this way, it'll be much easier for you to learn [00:22:00] Splunk, or for you to learn the other tools as well afterwards, because you know how it works.

You have the mindset, you know exactly where to look. And tools at their core do the same thing with slightly different approaches, right? It's a different UI.

It's like Microsoft Word in Windows versus Microsoft Word in Mac. They do the same thing, but they've got different approaches.

And if I were to pick a tool or domain out of all, I think it would probably be an EDR or XDR tool or domain. Because they are the key component of any SOC team nowadays . One of the Malware Researcher friends of mine put it years ago, probably 15 years ago now. This war started at the end point and it'll continue there.

And EDR tools are extremely powerful. CrowdStrike is a good example of this. But let's not forget the saying a tool is only as good as its user. It [00:23:00] takes practice, and more practice to become a CrowdStrike master. There is no magic happening there. And let's also not forget.

that it's more about the mindset and thinking than the tools at the end of the day. You need to know the purpose and strength of each tool to be able to effectively use it. I've been at many organizations where they spent millions of dollars in tooling and never touched it at all because they don't have the right person on their team.

And...

Learning different tools or domains. I like to give an example of those 1D, 2D, three dimensional, 4D, or I think they've got now 8D movies. It's the same thing. Each tool and domain gives you a different level of perspective and visibility. If you know one tool, it's like working in 1D. If you know two tools or domains, again, [00:24:00] that's 2D.

If you know three or more... Now you're looking at things from a three dimensional perspective, and it gives you a different level of perspective and visibility, which is what you need to get the work done.

[00:24:12] **G Mark Hardy:** That's very good insight. So, so let's continue. So we've done cybersecurity fundamentals, incident detection, threat intelligence, cybersecurity tools, and the fifth thing is going to be network analysis. Now, a lot of attacks come from network traffic. So we need to have our folks look and have the capability to analyze that network traffic for signs of suspicious or malicious activity.

And this might be looking at a tool like Wireshark or NetFlow Traffic to see how a DDoS is occurring, or spotting a port scan. Hasan, why might this be helpful to learn, and how have you seen this type of knowledge help incident responders?

[00:24:48] **Hasan Eksi:** The short answer, they get to see why things are happening the way they are. The long answer is in my experience, and this may be subjective, but some of the best technical cyber [00:25:00] people that I have worked with come from networking or system backgrounds. And the reason is they know how things work in and out, and their hands are dirty.

And all they're doing is looking at the same problem with a different hat. And this gives them a competitive edge that others may not have. And the reason why this might be useful is that it helps them understand why things work the way they work. It's like, again, going back to that 3D um, example, you're able to see 3D when others can only see two, two dimensional and there is, it's, it's at a different level and it, and it helps a lot.

It helps tremendously. And and there's that additional dimension that gives you a different perspective and because you're able to understand more, you know, what DNS is, you know, what the normal things that you should be seeing when you look at a DNS traffic versus others. And that. That helps you a lot.

[00:25:55] **G Mark Hardy:** And I'll agree with you. I used to teach that a lot when I was teaching at SANS. I want to make sure [00:26:00] people understood the networking and we would capture a protocol or a conversation and say, okay, why is this? Why did you see a port 53? What is that? Okay, it's DNS. Why is that occur? And so on. So having that fundamental understanding is, I believe, foundational. And I've told people, if you really want to learn security, it's great if you understand networking. our sixth item on our list is endpoint analysis and essentially having the skills to analyze endpoints, which would be computers, servers, et cetera for signs of compromise. Now, remember when someone calls the help desk and says, I think there's something wrong with my laptop, the help desk analyst, if they're trained well, might send this ticket over to the SOC if they think something malicious is happening.

Now, what should the SOC look for when they get this type of call?

[00:26:44] **Hasan Eksi:** Yeah, then this happens a lot and it's a typical IR instant response 101, which is preparation, identification, containment, eradication recovery, and lessons learned. And you can apply this methodology. [00:27:00] Any given time it's it should be applied to any incident that they

come across and and the way you would handle it is basically gather the information, verify it and verification is important and never jump to the conclusion meaning just because they thought they had malware doesn't mean there's actually a malware and vice versa and never trust the end user.

People will say, I didn't click on that link. Whereas you're seeing from your screen, you clicked on it at least a dozen times. What are you talking about? I can see it right here. I mean, clicked, and I can give you the times and they'll still say, No, man, I didn't click. Never. I never do that.

So, so never trust the end user. You're, and for that, you need to have accurate data points, obviously, and you need to trust in your tools. But not trusting the end user helps. A long way assessing the situation, looking for indicators of compromise, looking for anomalies, looking for suspicious [00:28:00] activities, behaviors or suspicious processes, for example is usually the next step and then after that, what comes next is the isolation and In most cases, re imaging, I would say, because you don't want to take any chances.

You may have cleaned everything, but how do you know 100%? Can you say I've cleaned everything 100 percent and this is all like clean, all good? Probably not. And in that case, it's better to re image and start things from scratch than take a slight chance.

[00:28:33] **G Mark Hardy:** I agree. And we avoid that shortcut by just saying, okay, let's just restore windows, you know, start over. And if you've got good images, if you've got some, a tool like Intune or some other way to do the manage endpoint, then you can just push out all the profile and it'll be set up correctly. So very good point on endpoint analysis.

And you're right. That's where a lot of the things happen and start and they stay there too, sometimes, we hope. Our [00:29:00] seventh then is going to be log analysis. So if an attacker is trying to steal domain administrator credentials, they might try to perform Active Directory attacks or do pass the hash.

And so the ability to parse and analyze logs from multiple sources, such as Windows event logs, is going to be key to uncovering security incidents. And what are some good ways to train people on log analysis?

[00:29:22] **Hasan Eksi:** Sure. And by the way, I forgot to add one thing and it's usually forgotten anyways, in the real cases too, the lessons learned piece.

[00:29:30] **G Mark Hardy:** Yeah, P I C E R L.

[00:29:33] **Hasan Eksi:** Yep. Yep. Lessons learned. Never forget that that, you know, what's, what was the root cause and what are the lessons learned? So this does not happen again.

SOC teams, instant responders are so busy every day with day work. It is very easy to skip that process. That step because there's hundreds of different, you know, tickets waiting for them to analyze and they just don't have the time

[00:29:57] **G Mark Hardy:** and I've heard the expression, a [00:30:00] lesson that's not learned is a lesson lost. And like George Santayana, we're going to repeat history because we didn't learn from it.

Okay, good. So let's talk about log analysis. What are your thoughts on that? Good way to train people that way.

[00:30:12] **Hasan Eksi:** sure. So, familiarize yourself with log analysis tools, I would say such as Splunk Elk Stack, the the ElastiSearch, Logstash, and Kibana or there are open source alternatives like Logging Made Easy, and in fact, this is very recent CISA just came out with it. It's a free log management solution.

Anyone can use it, download it. And one thing I see that works the best is shadowing, if they're working for for a company, obviously shadowing SMEs, subject matter experts in your organization and really trying to learn the way they approach incidents, how do they do what they do and what they look for and this will save a ton of time and make things much, much easier for you.

And [00:31:00] remember, you don't need to know it all. And there's no one who knows it all in, in cyber security. And it's always like, it's a learning challenge, right? There's always something new and you need to, that you need to keep up with. What you need to know enough to know where to look. Like if it's, if we're talking about Windows event logs, and if you know the basic ones from that point on, you can sort of deduce and try to. figure out things and, oh, if it's not this, then maybe it's that. So let me Google it. Let me put it on ChatGPT and see what that says, for example. But if you know where to look, it helps tremendously. And again, no one knows it all. So it's okay. It's okay to ask. Another thing is parsing.

You may have the best tool, but parsing is always an issue when it comes to logging. And don't expect everything to work nicely. Thank you. It never does. It never did for me at least and for the people I know in the industry. So, and it's IT in general, so be patient and be ready to put [00:32:00] on your engineer hat to tweak things if needed.

And remember your seam, your tool, whatever tool you're using is only as good as your engineers. whoever is engineering it, deploying it and configuring it. Because at the end of the day, The tool itself, it needs data feeds, and it needs the right configuration to be able to produce the right results for the analyst, for the incident responders, so they can do the job of, you know, of incident response.

Otherwise, you're going to be wearing multiple hats and working on multiple projects at the same time, which is, I would say, usually the case nowadays as well.

[00:32:41] **G Mark Hardy:** Yeah, Got it so interesting. And, you know, absolutely your tools only as good as your operators. And now if we have a good understanding what to look for in endpoints and logs, we get to number eight, which is the malware analysis. That is understanding and analyzing the actual malware to determine its functionality. Potential impact. So if a tool like [00:33:00] CrowdStrike or DefenderSpot's malware, we didn't know what it's doing. And otherwise, we might only remove part of the bad actor's access and actually tip them off that we know something's going on in the network. What should incident responders know about removing malware?

[00:33:14] **Hasan Eksi:** Sure. So, in incident response, everything begins with... with with the playbook, right? There's the instant response steps, but the playbook is where you get to learn how to react and what steps to follow when you're doing the actual work of instant response. And and it's very helpful, especially For tier ones, tier twos, and in some cases tier theories as well, because every company is different.

A bank is different than a gaming company and they'll treat things differently. And you really need that playbook to be able to navigate and that playbook should be ready for you. And it should be written by the SMEs before you, so that you can take it and just. Run with it.

It doesn't mean [00:34:00] everything will be there in the playbook. 100%. It never does. And it really shouldn't be either because you need to keep up, you need to be and everything changes very fast in industry today anyways. But first off, I would say if you're a tier one, right, you should probably be escalating it.

If you're talking about a case where you need malware analysis can you work on it? Yes, but it, Chances are very high that you need to escalate that to a tier 2 or 3, most probably, and have them take a look at it, especially if this is the first

time you're seeing it. If it happened before and you've got some experience running with it, great.

But if not escalate. Don't hesitate.

[00:34:45] **G Mark Hardy:** Yeah, and you're right, if you're tier one and you're wrapping yourself around the axle trying to do malware analysis, oh, look how smart I am, I'm figuring this out, etc. Meanwhile, all these other tickets are coming in and things might be getting out of hand. while [00:35:00] someone's head down. So absolutely take a look at those different tiers, understand where the division of labor is.

Now, some SOCs will organize with some very strict, Oh, you're tier one, you're tier two, maybe even tier three, if you're big enough. And others may say, well, no, we're going to move people around so you don't get bored at it. But the important thing is remember your role and stay in it.

[00:35:18] **Hasan Eksi:** Yeah. And stick with the plan,

[00:35:20] **G Mark Hardy:** Yeah, stick with the plan. So our ninth item is forensics and people need a basic digital forensic skills to collect and preserve evidence during an investigation. And especially if you're going to go send anything to law enforcement, one of the important things that I think is that anytime you start working on something that you consider an investigation, start taking notes from the absolute beginning. It might be a misconfiguration, it might be some user error, or it could be something big and scary, but if you're a half hour into it and then you realize, whoa, this is a problem and if you haven't taken any notes, then it's going to be really tough to reconstruct exactly what you did. So, what are some good examples of things to [00:36:00] teach people about forensics processes and interacting with law enforcement?

[00:36:04] **Hasan Eksi:** right.

[00:36:04] **G Mark Hardy:** Two questions,

[00:36:05] **Hasan Eksi:** comes to forensics, I think unless you are a forensics expert in which case you know what you're doing anyways, but I'm talking about IR folks and maybe tier one and two in, in SOC setting, et cetera. The most important thing to know is chain of chain of custody.

It helps a lot down the line. When forensics experts, and in most cases, you hand it over to a forensics expert and they conduct it anyways. They, that's

where they get in and that's where you sort of stop and start watching, and how they do things. But chain of custody, And when that's broken, then you can't talk about forensics at all because then, you know, there's nothing, there's no evidence involved and that's one thing that I should think, I I think that instant responders should be knowledgeable about, and forensics is also sometimes used to conduct root cause analysis, right?

And that's important because, you need to be able to conduct[00:37:00] a thorough root cause analysis that will help you identify what was that thing that was open that caused someone to exploit a vulnerability and compromise the systems. And sometimes you can't really get to it with Your resources, and that's where forensics come in and play a role too.

I would say even when it comes to lessons learned too, there's a lot that go into lessons learned aspect step as well from forensics,

[00:37:32] **G Mark Hardy:** Wow. So, yeah, I, I concur with you. And again, the chain of custody is important, just like physical evidence. That's one of the first things that a defense attorney may try to invalidate in court is to say, well, how do we know? that this person didn't tamper, or law enforcement, didn't tamper with it while it was in custody for eight months.

And one of your best defenses for that is to just have a hash. And you took all the hashes when you collected it, and you say, okay well let's compare them. And the [00:38:00] one thing I haven't seen done, that I always thought should be done, I've been telling people this for years. Maybe we should go on Shark Tank with this. Is hash your evidence, even if you're law enforcement, and stick it on the Bitcoin blockchain. Put, you know, move a hundred Satoshis from your left pocket to your right pocket. But the point is that you've locked that in and then it would reduce any argument about altering that to absurdity. Yeah, somebody could have made billions of dollars by hacking the blockchain, but they instead chose to change this particular evidence. Yeah, no. Well, I am already going to commit to a second episode with you. Cause I want to get through all 20 of these things. And I think 10 apiece is going to work out well. So let's do number 10. And then we'll wrap up for today and we'll pick up again. And the 10th skill is Vulnerability Assessment. And it's common for people in incident response to learn new ways that bad actors are trying to hack computers.

So they'll follow the next question that comes up, which is, well, are we vulnerable to this type of vuln? And it might mean looking at Qualys or Nessus scans and say we need to immediately take this system down [00:39:00]

because it's internet facing and it's vulnerable. So having that ability to quickly assess systems for vulnerabilities and then identifying the potential attack factors is going to be a key skill.

Hasan, how have you seen this play out in the workplace?

[00:39:13] **Hasan Eksi:** It's one of the I think toughest domains because everyone plays a part in it. to be successful. And that's where things get a little messy. And that's why I always, I've always admired vulnerability teams. Their jobs are extremely important and very challenging because they need to work with not only IT.

They need to work with business people, they need to work with system owners, and they need to convince them to do the right thing not just once, but every single time and stick with the plan. And that, that brings in the conversation of, you know, change management and testing. And you really need to love spreadsheets.

If you're in vulnerability management, I think, because that's what I saw, you [00:40:00] know, a lot of the vulnerability management folks play around with and that spreadsheet never ends. There's always something new that comes out and there's no timing of it either. Like a few things may pop up this week and then a few for a few weeks, everything goes silent.

And having good relationships with the business, with the system owners with the cyber security side of the house is really key in convincing people to do the right thing again, not once, but every single time. When there's a vulnerability out in the open, because it's really easy to ignore.

There's a lot of competing priorities from the business and other things, and things get skipped and overlooked. I had one of these cases when I was at Capital One as you may remember, the Capital One breach the one that started out with the server side request forgery on one of our AWS instances.

And it's an interesting experience[00:41:00] because when a breach happens, you don't, you know, that's when usually the SOC people, the security operations or incident responders, come into picture, right? Before that, it's all about the vulnerability management. So the more we address earlier in the game, right, the less we'll have to deal with after.

The breach happens, or the less number of breaches we should we should expect. So, again I, I honestly admire all those folks that work in vulnerability

teams. It's a hell of an effort to get everyone aligned on one thing. And not just once again, but do it consistently and persistently over time.

[00:41:38] **G Mark Hardy:** Got it. Okay, so I'm going to recap the 10 that we've covered, and I am then going to ask you if you could let people know how to contact you, if they want to talk to you before we get to the next 10. But today we covered Cybersecurity Fundamentals. It's the first item for what a SOC team member should know. Incident Detection, Threat Intelligence, Cybersecurity Tools, [00:42:00] Network Analysis. Endpoint Analysis, Log Analysis, Mailware Analysis, Forensics, and Vulnerability Assessment. And so the next thing, I'll give a little sneak peek for people, we'll cover Incident Triage. Incident response frameworks, communication, collaboration, documentation, memory analysis, incident containment and eradication, scripting and automation, cloud security, and crisis management. If you're into or getting into this line of work or you have people that you want to train or you want to refer for training, this is sort of the punch list to go through for that. So until the next episode of Hasan, if someone wanted to get in touch with you, what's the best way they can do so?

[00:42:41] **Hasan Eksi:** They can, the best way to reach me is Hasan at NationalCyber. com. H A S A N at NationalCyber. com or via LinkedIn.

[00:42:50] **G Mark Hardy:** Excellent. Well, thanks again for coming on the show. And thank you for our listeners for coming to increase your CISO Tradecraft. And we hope you've enjoyed learning the first 10 of the 20 important [00:43:00] skills that incident responders need. And as always, if you find this episode helpful, do us a favor, share it with your friends at work.

If you're watching us on YouTube, give us a subscribe so that we're able to go ahead. And Make sure that we can get rid of ads and reach more people and things such as that. So, Please listen to our sponsors. We provide one up top if you find them valuable. It's great. They make the show free to you and we think you're going to enjoy their products.

So that's it for today's show. Have a wonderful day. And until next time, this is your host G Mark Hardy. Stay safe out there.