#203 - Be SOCcessful with the SOC-CMM

[00:00:00]

Introduction to CISO Tradecraft and SOCs

[00:00:12] **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 I'm on the road again today, as you can tell if you're watching on YouTube. If you're not watching on YouTube, come on, get on the channel, and you'll get a chance to go ahead and do more than just listen.

Anyway, thank you for being a listener on CISO Tradecraft, and today we're going to be talking about SOCs, and specifically how do you become SOCcessful? And we're going to talk about the power of the SOC CMM. Now, if you think about it, in today's rapidly evolving cybersecurity landscape, having a SOC is no longer a luxury above a certain point.

You're going to have a necessity. Now, granted, if you're an SMB, you're going to go ahead and outsource that, but [00:01:00] usually around 2000 users or so, plus or minus. I think if you take a look at Carson Zimmerman's numbers, it actually came to 1400 seats or more. It made sense economically to run a SOC.

Now, that number may change over time, but think about this. And here's the real question. If you're going to have a SOC, how effective is it?

Understanding SOC CMM: A Game-Changing Tool

[00:01:20] **G Mark Hardy:** And are you confident that it's providing the maximum possible value to your organization Well, today I want to talk to you about a SOC CMM, Capability Maturity Model. That's going to be a revolutionary tool that's changing the game in measuring and improving your SOC capability maturity.

Now, It's free to download, free to use, which is great. It's like the NIST Cybersecurity Framework. but notice that this is not a sponsored episode. We're

not getting paid to plug it or anything like that, but we do believe it's a powerful tool. It could significantly boost your SOC effectiveness for your team and for you as a CISO or training to become a CISO. So let's get into it. What is a SOC CMM? [00:02:00] The concept of a security operation center capability maturity model is going to be short for a comprehensive self assessment tool. And that's going to be designed to help organizations measure, evaluate, and grow your SOC's effectiveness.

Now, it was authored by Rob van Os, Dutch, because if you go to their Excel spreadsheet, you find out that it's got Dutch in it, through extensive research, including literature studies and surveys across 16 different participating organizations.

Evaluating SOC Maturity and Capability

[00:02:29] **G Mark Hardy:** Now, the SOC CMM provides a structured, evidence based approach toward evaluating your SOC across five key domains, business, people, process, technology, and services. Okay. But what is going to set SOC CMM apart is the dual focus on both maturity and capability. Now they're measured on different scales, but we'll get to that. For the business people and process domains, SOC CMM is going to evaluate maturity. How well these aspects are managed and optimized, and for [00:03:00] technology and services, it'll assess both maturity and capability, your actual ability of your SOC to deliver results in those areas.

The SOC CMM follows maturity definitions established within Carnegie Mellon's Capability Maturity Model Integration, or CMMI, module. Essentially, each CMMI maturity level characterizes performance for the SOC into one of six different levels. And organizations will begin by filling out an Excel spreadsheet.

That gives them a way to measure if the domain maturity is Non-existent, Initial, Managed, Defined, Quantitatively Managed, or Optimized. Now, what does that really mean? at the lowest level of zero, it's non existent. It means that this aspect is extremely ad hoc or it's incomplete. There's no assurance of delivery.

When you get to an initial capability, okay, then the maturity is saying, yeah, it's delivered in an ad hoc fashion. When you can get to it, you get to it. A managed level says that it's managed using [00:04:00] some ad hoc feedback on the quality and timeliness of deliverables. you're actually going ahead and incorporating some feedback.

If you get to the next level of 3, Define, we're now talking about it being documented and delivered consistently. that sort of sounds like where we like to be, right? But you can go beyond that. And go to level four with a quantitatively managed, which means it's systematically being measured for quality, quantity, and timeliness of deliverables.

And ultimately you get to the optimizing, where it's continually being optimized and improved upon. Now, granted that as you go through a study such as this, and you're evaluating yourself, you're not going to go ahead and be maxed out across the board. That's not the idea. It isn't to come out with a perfect report card.

It's really to come up with a diagnostic tool to help take you look at where you are, And then have a series of discussions to determine where do you need to be. You might find out that, for example, being at level 3 defined is perfectly acceptable for one of these particular categories, but others you might want a little bit more.

Now note that the technology and [00:05:00] services domains can be further evaluated by the capability levels, which are going to be indications of completeness. And four capability levels are determined. They are called Incomplete, Performed, Managed, and Defined. Now, there's no prerequisites for advancing to a higher level, so the capability growth is continuous as well.

It's zero or incomplete. That capability, it's just not there. You don't even have the capability in your SOC to deliver this aspect. At a level of one, there's sufficient capability to deliver at a basic level. Two is you can deliver it consistently, which is really good. And it sounds like, yeah, we're there.

But again, there's one beyond that. Number three, defined. The capability for this aspect is optimized and well documented and delivers true added value. So it really looks like to max these things out, not only do we have to go ahead and perform them, But then we have to define them and then optimize them.

[00:06:00] And that seems to be the theme here, which is again, very much keeping with the CMMI.

Benefits and Implementation of SOC CMM

[00:06:04] **G Mark Hardy:** So why should CISO spend time using something like the SOC CMM? In an era when cyber threats are becoming increasingly sophisticated and frequent, your SOC needs to be at the top of the game. And

here's why SOC CMM can be helpful for any organization serious about cybersecurity.

Number one, it can help you identify your strengths and weaknesses. The SOC CMM allows you to pinpoint areas where your SOC excels, and also where it might need improvement. And this granular level of insight is going to be invaluable.

Next, it could help you measure growth. You can track your SOX progress over time. This not only helps in setting and achieving goals, measuring your progress, of course, but in demonstrating the ROI to stakeholders and leadership. So if you're asking for additional investment and you can come back and report on a periodic basis, start.

Again, some sort of a standardized scale that you're making progress. These funds are being used effectively. [00:07:00] You're going to be able to get potentially more support going forward to make this happen. It's a standardized assessment. As I said before, the model is based on the widely recognized CMMI capability maturity model integration framework from Carnegie Mellon University.

And this ensures a robust industry standard approach to evaluation. It's also a holistic type of evaluation, because you're assessing both maturity, which is how well the processes are managed, and capability, your ability to deliver on results, the SOC CMM is going to provide a comprehensive view of your SOC performance.

And it can also help you for risk based improvement planning. Because the SOC CMM will help prioritize improvements based on risk, make sure your efforts are focused where they'll have the most significant impact. All right, cool. How does it work? SOC CMM will offer you two types of assessments that can allow you to cater to different needs and timeframes.

If you're in a hurry, Let's do a quick scan. It's a high level overview.

Understanding SOC Assessments

[00:07:56] **G Mark Hardy:** It's perfect for regular progress checks or when time is limited. It'll [00:08:00] cover all the domains, but with less depth than a full assessment, which is the other type, and the full assessment is comprehensive evaluation covering all aspects of your SOC in detail.

It involves thorough documentation, reviews, in depth interviews, and technology assessments. Now, these assessments are going to typically have a process that are going to involve workshops with a diverse group of SOC team members, including your engineers, your analysts, and your managers. And this diversity of input assures a well rounded evaluation and will often lead to valuable discussions and new insights.

And ideally, the assessments are facilitated by an external assessor or an internal auditor to ensure there's some objectivity. And they'll challenge any assumptions that might be in there because you know what they say about assume. The facilitator will guide the team through each domain using a 5 point scale for maturity and a 3 point scale for capability questions.

Deep Dive into SOC CMM Domains

[00:08:55] **G Mark Hardy:** So if we dive down into that SOC CMM model in detail a little bit more, [00:09:00] the current version is 2. 3 and it consists of five domains with 26 different aspects or elements in them. Here's a brief overview of what these five higher level domains cover. Number one is a business domain. It's going to focus on how well the SOC aligns with and supports business objectives.

It covers important maturity aspects of things such as business drivers, customers, Charter, Governance, Privacy and Policy Related Questions, Business. Number two, the people domain. It's going to evaluate the human aspect of the SOC, including recruitment, training, and retention strategies. And this will look at maturity of employees, roles and hierarchy, people management, knowledge management, training and education.

The third domain is process. We'll look at the maturity of the SOC process from incident response procedures to continuous improvement practices. And this domain is going to cover the maturity of the SOC management, Operations and Facilities, [00:10:00] Reporting and Communication, Use Case Management, and Detection Engineering and Validation.

The Technology domain is going to examine both the maturity and the capability of the SOX technological infrastructure, including tools for threat detection, analysis, and response. Now, examples of technologies you can assess for maturity would include things like a SIEM, for your security information event management, UEBA, the user and entity behavior analytics, NDR for network detection response, EDR for endpoint detection response, SOAR

security orchestration automation response, pretty much any of these major tools that you're using.

You're going to take a look at that to see are they implemented? Are you running them in a mature metal? Mature manner, which we said, of course, from that perspective, it means that you're, doing the job, it's documented, and you're optimizing, ideally, what you're doing. You then look at these technologies in terms of technical capabilities, data ingestion and [00:11:00] processing, technical and process integrations, rule based detections, anomaly detections, even visualization and output.

For example, organizations would select if the SOC dashboards are either not in place, partially implemented, but incomplete. Averagely implemented, but not fully documented, mostly implemented, documented, and approved, or fully implemented, documented, approved, and actively improved. And number five, the fifth domain, Services, evaluates both the maturity and capability of the services provided by the SOC, such as security monitoring, security analysis, threat hunting, log management, security incident management, threat intelligence and vulnerability management.

Now, what would the output look like for this type of a model? Typically, what they show here is a radar chart showing the capability maturity scores for the 26 different elements being scored across the five domains. Now note that maturity scales are from 0 to 5. Whereas [00:12:00] capability is from 0 to 3, and capability is only measured on technology and service domains.

Nonetheless, it gives you a graph with 37 different data points. It's bound to get busy. And if you superimpose that on top of the targets you have for each, You now have 74 data points to interpret. Definitely not something you would use to brief senior management. So why bother with something that's busy?

of course you want to change the output and use this because this is a great tool that is going to allow you to track your progress as we said before, gain an initial assessment, start to document what you're doing, and ultimately provide some sort of an external reference that says, Hey, we're doing the right things.

Benefits and Flexibility of SOC CMM

[00:12:42] **G Mark Hardy:** Here's what could set apart the SOC CMM. from other assessment tools. It's specifically a SOC tailored maturity model. It measures the SOC, which means it has a lot more details on how to improve

your SOC than what you might find in just a generic ISO 27001 in this maturity assessment or some other [00:13:00] standard.

It also allows you to visualize your progress. You can get clear graphical representations of your SOC's current state and improvement targets. Again, radar charts, you can show these things growing or whatever, and that will be done with Excel. So these radar charts, bar graphs, however you want to do it, it makes it easy to communicate results to both technical and non technical stakeholders, if you don't overdo it in terms of the complexity.

And it's perfect for copy paste into PowerPoint, if you will, once you've made that easier. Your NIST Cybersecurity Framework Alignment. The SOC CMM will align within this cybersecurity framework, both versions 1.1 and 2.0. And this alignment will help organizations understand how their SOC capabilities map to this widely adopted framework, as well as utilize this data for other compliance requirements.

It's free and accessible because unlike many other enterprise assessment tools or anything for the ISO standards category, SOX CMM is available for free download, and you get it right from the SOX eMM website. No email registration, no [00:14:00] paywall. It's very easily accessible to any organization of any size.

It allows for continuous improvement. It's not just a one time assessment tool. It's designed to support continuous improvement, allowing you to regularly reassess and refine your SOX capabilities. This is a really important story to tell. And, it's flexible. The advanced version of the SOX CMM will support weighting of different elements, allowing you to customize the assessment based upon what's most important to management in your organization.

Now we probably wouldn't recommend this option unless you found a lot of the questions either were not required for your company or industry, or you're well along in terms of maturity process and you want to go ahead and tweak at the very edges.

Real-World Application and Conclusion

[00:14:40] **G Mark Hardy:** So let's consider a hypothetical scenario to illustrate how the SOC CMM can drive real improvements.

#highlight

[00:14:46] **G Mark Hardy:** Imagine a mid sized financial services company that's been running a SOC for years. The company decides to use SOC CMM for a full assessment. The results show high maturity in the technology domain, but maybe low scores in the people in process [00:15:00] domains. If you dig a little bit deeper, the company will find out that although they've invested heavily in cutting edge security tools, they lack a structured training program for analysts and have poorly documented incident response procedures.

Now, armed with this insight, they created an improvement plan focusing on developing a comprehensive training curriculum and formalizing their processes. Six months later, a quick scan assessment, rather than the full one, shows significant improvement in these areas, resulting in faster incident response times and more effective threat detection.

This tangible progress helps a SOC manager secure additional budget for the next fiscal year, demonstrating a clear ROI to the board. So take some action with this. Why does it matter? See, in the world of cybersecurity, if you stand still, it means you're falling behind. Your SOC needs to continuously evolve and improve to stay ahead of the emerging threats. The SOC CMM provides a roadmap for this journey of continuous improvement. So don't let your SOC operate in the dark. Take a look at the SOC [00:16:00] CMM today and start your journey toward a more capable, mature, and value driven security operations center. You can find it at their website, which is SOC-CMM.com, or just click the link in our show notes. And with SOC CMM, you'll always be moving forward, enhancing your organization's cyber resilience Step by step. Remember, a mature and capable SOC isn't just about better security. It's about doing business better. It's about minimizing risk, ensuring compliance, and enabling your organization to thrive in the digital age with confidence.

with that, thanks again for listening to today's episode, and we hope you've enjoyed it. Now, here's a little sneak peek. Next week, we're going to do a special Halloween episode on Zombie IT and Shadow IT, so be sure to subscribe to our show if you haven't done so yet. And go ahead and hit that subscribe button.

Also, if you found this episode helpful, do us a favor and pay it forward. Share it with your SOC department. And remember, if they get better, that's good for you. It's good for all of [00:17:00] your customers, and we want to help you keep your enterprise secure. So thanks again for listening to CISO Tradecraft. This is your host, G Mark Hardy.

And until next time, stay safe out there.