The Cybersecurity Readiness Podcast Series

Episode Title	Enhancing Incident Response Effectiveness
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Markus Lassfolk, Vice President of Incident Response, Truesec Morten von Seelen, Vice President, Truesec Group
Summary Pitch	According to a 2023 IBM report, companies take 197 days to identify a breach and 69 days to contain one on average. The delay between infection, detection, and containment can cost businesses millions of dollars. Only 45% of the companies polled had an incident response plan in place. In this episode, **Markus Lassfolk, VP of Incident Response, Truesec**, and **Morten von Seelen, Vice President of the Truesec Group**, who have extensive hands-on experience in dealing with major cyber attack incidents, shed light on this very important subject matter.
Time Stamps	00:02 -- Introduction 02:47 -- Markus Lassfolk professional highlights 04:28 -- Morten von Seelen professional highlights 06:17 -- What does incident response mean? Why is it important? 09:10 -- Extent of organizational preparedness

	15:32 -- How should organizations prepare to help incident responders do their job better? 20:49 -- What are the different roles associated with major incident response engagements? How do you build a team to handle these engagements and how you retain the talent? 25:18 -- What are some of the most common mistakes that you see customers making? 30:27 -- How effective are tabletop exercises? 36:00 -- How important are security drills? 37:21 -- How should organizations go about looking to identify real expertise in incident response? 39:25 -- What kind of help can small companies get who don't have the budget? What would be your advice to them? 42:58 -- When I was reviewing some industry reports, one survey finds that while only 45% of the companies polled had an incident response plan in place, 79% of the companies have insurance. So they're almost implying that many companies could be of the view that let's not worry about the incident response plan. If we have good insurance, we are covered. Can you dispel that myth? 46:35 -- What's exciting, what's interesting, what are some challenges, what kind of mindset and skills one needs to have to pursue a career in incidence response? 51:23 -- Final thoughts

Memorable Markus Lassfolk Quotes/Statements	"If organizations gets hit by ransomware, they are usually down for three weeks, 21 days, on average." "From a preparedness standpoint, it helps if the customer has secure and safe backups that we can use." "In most of the cases, customers are either totally unprepared, or they're not prepared in the right way." "During an engagement, having the log files will help us get answers of what's been going on in the breached environment. When we don't have the log files, it's so much harder, then we have to start looking at other things which takes more time, which sometimes does not provide the answers, and then we have to start guessing." "The best thing that the leadership team can do is to give the incident responders and the IT department the support and room to do their job and and not expect to have status meetings every 30 minutes or every two hour because that does not give us time to work and actually produce stuff." "We advise our customers to make sure that they identify the key personnel on their site and try to reduce the single point of failures in personnel as we call it, because in every incidents, when we come in and start working, we start to see a pattern; there is one person who has the answers to everything and who everyone points to. And that person is the single point of failure." "They (customers) start restarting or shutting down servers and clients, which removes both evidence and valuable information from the memory of the computers. In a lot of cases, we have been able to extract the decryption keys from the RAM from a server, to be able to decrypt

	the server without paying ransom. But if you have rebooted that server, that information has gone, we're not able to do that." "Even if you have working backups, it's still going to take days to do a restore and start to get your systems operational. It's not something you can just snap your fingers and be up and running again." "For any company, small or large, preparedness is about not getting hit. It's all about patching, minimizing exposure to the internet, implementing multi factor authentication on all external facing services. It's it's all those hygiene things that we've been talking about for the last 5-10 years, there is no magic bullet."
Memorable Morten von Seelen Quotes/Statements	"I know Markus had experience with some of my Danish clients where the client told him, please restore our company. And that's some of the best cases we have had. We have all the IT administrators for a short period of time taking over everything in the company, restoring it, securing it, kicking out the bad guys and restoring the company's operations. And those are some of the fastest assignments we have. So, I'm not saying that you shouldn't prepare for breach incidents, just do it at the right level, and to the right extent. Don't overdo it, spend your time on something else." "Most of the time, the bad thing shows up last. So it will be at the end of the forensics, when they will say, " Oh, we found this evidence of data exfiltration. In my experience, it never shows up as the blinking lamp in the beginning, you need to identify the IP addresses, you need to identify the servers, it's never easy to identify the data exfiltration. But if you start the communication too early, and if you're too brave in your communication, especially if you're a registered company, and you have to withdraw your previous statement, just because you were too eager and say "we don't see any compromise of data." And then later on, we

	find those five gigabytes of data exfiltrated that that's just bad. So being too brave in the communication too early and not taking advice from people who made the mistakes before, that's a mistake we see quite often." Just remember to do the restore from the cold backup, not the image backup that you have lying right next to the server because that's gonna be compromised day one. But the real cold backup you have in storage or somewhere, that's the place you want to restore from." "If you are able to obtain cyber insurance, you are much more secure than others." "If organizations have mature security (processes), we see the cyber insurance premiums going down for them."