The Cybersecurity Readiness Podcast Series

Episode Title	How to Tackle Burnout in Cybersecurity
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	Thomas Kinsella, Co-Founder & Chief Operating Officer at Tines
Summary Pitch	Security Operating Center (SOC) staff members are often consumed with tedious manual tasks that lead to burnout and can cost organizations millions of dollars in losses due to human error. Thomas Kinsella, Co-Founder & Chief Operating Officer at Tines discusses at length the challenges faced by SOC team members and makes actionable recommendations on how to decrease burnouts, increase retention, and create a better work environment for the security analysts.
Time Stamps	01:26 -- So, before we get into the Voice of the SOC Analyst report details, Thomas, I'd like to give you this opportunity to provide some highlights of your professional journey. 03:54 -- What led to the study. What's the purpose of the study? 06:39 -- Would you like to add anything about the methodology for the study? 08:53 -- So would you say that it's mostly mid-market organizations that you all were able to tap into? 09:18 -- Let's go through each one of the findings. The first one says 71% of the analysts experience some level of burnout. This could be due

	to the fact that 69% are understaffed, and 60% have seen increased workloads over the past year. Was this surprising to y'all? 11:27 -- Referring to another finding which states that 64% say they are likely to switch jobs in the next year. So the turnover is going to be very high. What do you recommend organizations do to deal with this challenge? 14:05 -- Why hasn't this automation aspect been addressed yet? 19:39 -- When organizations make the decision of investing in an automation platform, what does it take to make the implementation a truly successful experience? 22:19 -- What do you think about job rotation and job enrichment? Is that done well enough to make make it a little more interesting for the staff? 24:52 -- So, talking about job rotation job enrichment. Yeah, I think this creates a great opportunity for an organization to get the security people outside their comfort zone, and expose them to other company operations. And also get people from the other business operations and bring them into the SOC center. Does that gel with you? 34:29 -- One of the first actionable takeaways from the SOC report is -- "improving time spent on reporting." What do you mean? Because I would think that you want to reduce the time that is spent, the manual hours that is spent in delivering different types of reports. Can you clarify? 36:49 -- Moving on to the second recommendation, which is: "making triage, enjoyable," how do you do that? And if you could clarify for the audience, what do you mean by triage? 41:36 -- So moving on to the third recommended takeaway or actionable item, which is -- "increasing retention by measuring and minimizing burnout." Can you expand on that?

	47:53 -- Let's talk about the fourth actionable takeaway -- it's time for no-code automation. What does that mean? 50:49 --Do you have any final words for the listeners?
Memorable Thomas Kinsella Quotes/Statements	"It seems to me they (SOC team members) enjoy the work, they feel respected, but that you're just spending their time shifting from screen to screen investigating alerts that are not high enough fidelity." "People (SOC team members) don't mind working hard if they feel like they're adding a ton of value and feeling like they're productive." "Purchasing a tool is often equivalent to purchasing weights, or purchasing an exercise bike, they actually just look good in the corner unless you're prepared to use them." "If you generate some challenges, and get people thinking creatively, and get people digging deeper, they remember the parts about security they really love." "Shame is the exact opposite of what we should be doing in security, we have to be encouraging people to report and knowing that people are gonna make mistakes. That's why we have defense in depth."