The Cybersecurity Readiness Podcast Series

Episode Title	Elevating Your Offensive Security Program
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Mark Carney, CEO @ Evolve Security Yaron Levi, CISO @ Dolby Labs
Summary Pitch	Dr. Dave Chatterjee hosts a discussion on elevating your offensive program with Mark Carney, CEO @ Evolve Security, and Yaron Levi, Chief Information Security Officer (CISO) at Dolby Labs. They emphasize the importance of a proactive, continuous approach to cybersecurity, contrasting it with traditional reactive measures. Key points include the need for a threat-informed, programmatic mindset, continuous threat exposure management (CTEM), and the integration of business objectives. They stress the importance of intelligence, risk assessment, and the role of third-party providers as partners. The conversation highlights the necessity of senior leadership commitment and the challenges of defining and measuring risk in cybersecurity.
Action Items and Discussion Highlights	▪ Adopt a continuous threat exposure management (CTEM) approach to offensive security. ▪ Develop a programmatic mindset for offensive security, focusing on fundamentals like visibility, validation and prioritization of vulnerabilities to minimize risk and build resiliency. ▪ Approach offensive security with intentionality, thoughtfulness, and pragmatism, leveraging intelligence, prioritization, and a hybrid of in-house and outsourced resources.

	▪ Establish long-term partnerships with third-party providers, ensuring cultural alignment, business context understanding, and a shared responsibility model. ▪ Establish a continuous, threat-informed, and programmatic approach to offensive security, going beyond a one-time test and compliance-based exercise.
Time Stamps	00:00 – Introduction 01:50 – Guests' Professional Highlights 03:35 – Why are we discussing offensive security? 04:44 – Offensive vs Defensive Security 05:57 – Security Mindset 06:18 – Security Trigger 06:34 – Defensive Security followed by Offensive Security 09:25 – Importance of Top Management Buy-In 11:54 -- What has been your experience of top management's approach to security posture? 12:01 – Evolution of the security industry 14:31 – There is no standard way of doing security 15:18 – How do we define harm that is caused by cybersecurity? 16:40 – Challenges and Dilemmas of Cybersecurity Governance 18:38 -- Key elements of a mature offensive security program 23:03 – Destroy Your Own Business (DYOB) Approach 25:47 – Programmatic Approach 27:44 – Getting the Basics Right

	29:42 – Top Five Ways of Grading Your Offensive Security Program 33:09 – Selecting third-party service providers 37:34 – Final Thoughts
Memorable Mark Carney Quotes/Statements	"It's all about the goal of fortifying your infrastructure to the risk appetite of your organization." "I think the industry is in need of a new standard and a new approach that is threat informed, more continuous, and more programmatic." "Once you put the foundational elements of a defense program in place, which is sort of your first response and your first kind of programmatic efforts, then you got to go test it. And it's this sort of back and forth play that I think is very important. You can't protect what you don't practice and measure against different types of adversarial attacks. So, I think it is very important that it never ends. It's always kind of this continuous motion where disruptive technologies or a new threat, or CISA puts an alert out around a live exploit, and you need to go test your defense mechanisms against that. I think this continuous motion is very, very important for our industry." "So, I think moving to this programmatic approach, the softer side of programs and running programs, my basketball analogy is, everybody likes to, hit a half-court shot or a dunk; in the cybersecurity world, a lot of times, we just need to work on the fundamentals of cyber hygiene. And those are not sometimes the most exciting and the most fun things to do as a cybersecurity leader." "Enabling your team to provide the softer side -- the processes, procedures, programs, etc., are paramount."

	"Finally, what is the outcome that you're really trying to drive and achieve? And that outcome is resiliency. How do you measure that? 'Decreasing mean time to remediate' is one such measure."
Memorable Yaron Levi Quotes/Statements	"In many cases, a lot of organizations still don't really have a mature security program; many organizations don't even have a security team or a CISO." "I think it's first and foremost the mindset. And the mindset is, are you reactive or proactive? Unfortunately, in many organizations, security is very reactive. You rarely see organizations building a security practice from the ground up." "There is usually a trigger. There's a trigger that causes organizations to build security practices. And that trigger is usually, a regulatory requirement, a breach, and requirements from clients." "Once the organization has the fundamentals in place such as vulnerability management, access controls, and compliance, the next step is to test if they are working and effective. That's where offensive security can help, because not only can you simulate, but also empirically test how well are the defenses working. How well they hold? Where do we need to improve? And basically, how do we measure our program?" "You have to continuously practice, you have to continuously train, you have to continuously improve, because things are changing all the time. I can't emphasize enough the importance of this continuous improvement and recognize the fact that you're never done." "We don't have a standard way of doing security."

	"How do we define harm that is caused by cyber security? This is still, I would say, an unresolved question." "Start with what you know, the known attack patterns, and continuously improve from there." "I don't like to call it the basics, only because, when people hear basics, they think easy, and it's not easy. I think those foundational controls, knowing your inventory, manage it into a large scale, managing your identity is, you know, patching your systems, all of that, again, that hygiene, it's a lot of work, and it's not easy." "So, leverage people, process, and technology, do it intentionally, do it thoughtfully, do it pragmatically. And at some point, you will have to decide, okay, based on everything we have, what is good enough for us?"