

The Cybersecurity Readiness Podcast Series

Episode Title	Detecting Malicious Insider Threats by Monitoring User Journeys
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	Doron Hendler, CEO, and Co-Founder at RevealSecurity
Summary Pitch	Insider threats are often considered the biggest risk for organizations because they can cause the most destruction. Survey reports, and studies, have found that organizations have spent millions of dollars to recover from insider threat attacks. Proactively detecting and thwarting such threats is a critical aspect of robust information security governance. Doron Hendler, CEO, and Co-Founder at RevealSecurity , sheds light on a context-based detection model that analyzes activity sequences performed when using an application. According to Doron, this User Journey Analytics method is a ubiquitous detection model that can be applied to any SaaS and custom-built application. Since no rules are required, it eliminates the need to fully understand the application business logic.
Time Stamps	01:23 First, let's talk about your professional journey before we get into the details of insider threats, detection challenges, and solutions. 03:27

	<p>Doron, would you like to add to the reasons why we are having this discussion?</p> <p>07:29</p> <p>So, Doron, going back to monitoring using technology, share with the listeners what was the traditional method, what were some of the weaknesses of the traditional method, and what you and your company are offering by way of your platform.</p> <p>12:23</p> <p>So given this move to these more advanced, more sophisticated solutions, for folks who are listening in on this conversation, CISOs of companies who have the authority to make purchasing decisions, how do they go about evaluating the different products out there? What should they be looking for in terms of what would work best for their context for their environment? Any advice? Any suggestions?</p> <p>14:34</p> <p>What could be possible shortcomings of the user journey analytics approach?</p> <p>17:26</p> <p>If a company was going to adopt this (User Journey Analytics) technology platform, what kind of changes does it require? From a change management standpoint, what should an organization be prepared for?</p> <p>19:13</p> <p>When the user journey is different from the normal user journey, let's say abnormal user journeys are detected, how does the alert system work? Who is alerted? And is there a way of capturing or documenting whether organizations respond to those alerts?</p>
--	---

	<p>21:57</p> <p>How do you convince a potential buyer or potential customer to adopt this new technology solution? What does it take to convince them? What have you experienced when you have engaged with prospective customers? What are their concerns when they're evaluating such platforms?</p> <p>24:53</p> <p>I'd like to give you the opportunity to wrap it up for us with some final thoughts and advice.</p>
<p>Memorable Doron Hendler Quotes/Statements</p>	<p>"The highest risk in today's organizations, in our digital transformation, is our identities."</p> <p>"If you cannot trust anyone, you have to monitor, you have to track, and you have to learn how to do this quickly, accurately, and automatically."</p> <p>"Today's solution around detections, which are based on rules, basically provide very, very limited, ineffective detection, in the application layer."</p> <p>"Accuracy comes with context, if you understand the context, you will have much better accuracy."</p>