# The Cybersecurity Readiness Podcast Series

| | |
|---|---|
| **Episode Title** | Securing Application Programming Interfaces (APIs) |
| **Podcast Series** | The Cybersecurity Readiness Podcast Series<br><br>https://www.cybersecurityreadinesspodcast.com/ |
| **Host and Producer** | Dave Chatterjee, Ph.D.<br><br>https://dchatte.com |
| **Guest** | Jeremy Snyder, Founder & CEO, Firetail.io |
| **Summary Pitch** | Application Programming Interfaces (APIs) play a vital role in modern software development, enabling the integration of services and facilitating the exchange of information. The ubiquity of APIs is a testament to their success in supporting a vast number of functions. However, their prominence has also made APIs a target for cyberattacks. **Jeremy Snyder, Founder & CEO, Firetail.io**, joins me in discussing how to effectively secure APIs. Our discussion revolves around the following questions:<br><br>• What do we need APIs for? Why do we need API security? What are the consequences of lax of API security?<br><br>• What are the risks of APIs today? How can we remedy current API security issues? |
| **Time Stamps** | 00:02 -- Introduction<br><br>00:49 -- Setting the Stage and Context for the Discussion<br><br>02:26 -- Guest's Professional Highlights<br><br>04:37 -- Overview of APIs |

| | |
|---|---|
| | 09:12 -- Common API Security Risks and Vulnerabilities<br><br>12:29 -- Design with security in mind<br><br>13:23 -- Securing APIs<br><br>13:36 -- Integrating Security into the Development Process<br><br>13:52 -- Different Ways of Security Testing APIs<br><br>17:08 -- Vulnerability Monitoring and Promptly Acting on Alerts<br><br>19:22 -- Role of Humans in Acting on Vulnerability Alerts<br><br>21:33 -- Staying on the Right Side of the Law<br><br>23:37 -- Significance of Maintaining Logs<br><br>25:36 -- Selecting Robust APIs<br><br>27:59 -- Key Takeaways<br><br>28:57 -- API Governance<br><br>30:25 -- Zero Trust Approach<br><br>32:10 -- Use of APIs in Leveraging Large Language Models (AI)<br><br>33:41 -- API Governance and Taking Ownership<br><br>36:12 -- Final Thoughts |
| **Memorable Jeremy Snyder Quotes/Statements** | "Application Programming Interface (API) -- It's basically the way two pieces of software talk to each other, that can be to send data from system A to system B, or that can be for system A to request system B to process something for it." |

| | |
|---|---|
| | "We've got sensitive data crossing the wires over an API, but we've also got critical business functions like processing credit card transactions over an API."<br><br>"API's are pretty much happening behind the scenes, they enable a huge volume of interactions and transactions every day."<br><br>"So we've been cataloging the API data breaches for the last couple of years, these breaches go back about a decade or started about a decade ago, or let me say started to be recognized about a decade ago. And as we've catalogued them, we've kind of categorized them as well, to try to understand in each of these breach scenarios, what was the primary error or breach vector? How was the API breached? And if there's a secondary cause, or things like that, we look at that as well. Two of the main things that we see are are really authentication and authorization."<br><br>"Authorization turns out to be the number one root cause of data breaches around API's. And this has been true for many years now."<br><br>"Proactive security is always much cheaper than reactive security."<br><br>"From the proactive standpoint, the number one thing that any provider of an API can do is actually just check the API's before they go live."<br><br>"You should actually pen test your API's before they go live."<br><br>"Very often, we find that API's get shipped into production environments without going through either the static code analysis, or the pre launch testing." |

| | |
|---|---|
| | "The average time that a vulnerability existed in a production environment before being patched and updated, was around 180 days."<br><br>"The best practice that we recommend to customers about reacting to the logs or the alerts or the suspicious conditions that you're seeing in your logs is to do it with automation."<br><br>"The human has to come into play as soon as there is any reason to suspect a data breach."<br><br>"If you find an organization that has a lot of undocumented stuff, or poorly documented stuff, that's kind of an indicator that they don't have good governance over the API's that they themselves are providing. And so I would have concerns about what other API functions might be out there that are not documented or publicly disclosed, that could also be used by third parties or bad actors to breach that organization."<br><br>"Right now, more than 50% of all internet requests are API requests."<br><br>"If you can't see it, you can't protect it."<br><br>"From a governance perspective, do you know all the API's that you have? Do you know the versions of API's?"<br><br>"From the kind of cultural perspective, having organizational guidelines for what acceptable usage of API's is, and having that documented and communicated to the team somewhere, is always very important."<br><br>"One of the fastest areas of API usage growth right now is AI."<br><br>"What I'm seeing in a very small percentage of organizations right now are API centers of excellence. And it tends to be right now at the |

| | |
|---|---|
| | largest organizations that have 1000s of applications that they might have built and run." |