Insights from Zack's Journey: A Path to Cybersecurity

Zack’s journey into cybersecurity highlights the value of curiosity, adaptability, and continuous learning. His non-traditional path and reflections offer valuable lessons for anyone considering a career in cybersecurity or transitioning into the field.

Key Takeaways from Zack's Story

1. Non-Traditional Backgrounds Can Thrive in Cybersecurity
   * Zack didn’t begin his career in tech or security. He started in recruiting, pivoted to strategy work, and later transitioned into software engineering at Google.
   * His story underscores that a technical background isn’t a prerequisite for success in cybersecurity. Skills can be learned, and passion for problem-solving can lead the way.
2. The Power of Playbooks
   * Playbooks provide structured solutions for addressing security incidents like data leaks, denial of service attacks, and privacy issues.
   * For someone new to the field, playbooks are an indispensable resource. They encapsulate the wisdom of experienced professionals, offering step-by-step guidance for tackling vulnerabilities and incidents effectively.
3. Continuous Learning and Adaptability
   * Zack learned web scraping through self-teaching and took Google’s internal training to transition into engineering. His example highlights the importance of upskilling and seeking opportunities to grow.
   * Tackling his first externally reported vulnerability felt overwhelming, but the remediation guidance and playbook support made the process manageable.
4. Cybersecurity Is a Team Effort
   * Zack’s insight into the role of communication is eye-opening: 50% of his time is spent collaborating, reviewing designs, and discussing ideas.
   * This emphasizes that cybersecurity isn't just technical—it’s also about teamwork, problem-solving, and clear communication.
5. Security Teams Are Always Relevant
   * Zack notes that while some tech roles come in and out of fashion, cybersecurity remains essential and is growing in importance.
   * For those seeking stability and purpose in their careers, security teams are a great place to contribute to critical work that protects people and data.
6. Advice for Aspiring Cybersecurity Professionals
   * Talk to industry professionals to learn about job roles, open positions, and workplace cultures.
   * Recognize that coding isn’t just about long hours of solitude—it’s a collaborative, creative process that involves working closely with others.
   * Cybersecurity offers both a meaningful mission and job security, making it an appealing career path.

Final Thoughts

Zack’s experience illustrates that cybersecurity is accessible, dynamic, and rewarding. Whether you’re new to the field or looking for a career change, following his advice to stay curious, network, and embrace teamwork can open doors to a fulfilling role in this ever-evolving industry.

What Does a Privacy Engineer Do?

* Focus: Erin works on speculative and emerging technologies—innovations expected to emerge in the next 2–5 years.
* Responsibilities:
  + Embedding privacy into new technologies before they even reach users.
  + Ensuring users trust products by protecting their privacy and informing them about how their data is used.
  + Addressing potential privacy risks proactively, long before a product is launched.