The Millenium Alliance – Breakfast Keynote Panel

October 23rd at 8 AM

"Cybersecurity Jujutsu: Harnessing the Power of Adversity for Resilience and Recovery

Moderated by:

Dave Chatterjee, Ph.D.

Visiting Professor, Pratt School of Engineering, Duke University

Author: Cybersecurity Readiness: The Holistic and High-Performance Approach

Host, The Cybersecurity Readiness Podcast

https://www.dchatte.com

https://www.linkedin.com/in/dchatte/

Agenda and Discussion Plan

I. Introduction (5-10 min)

II. Cybersecurity Lessons from Brazilian Jujutsu

1. Close the distance (5-10 min)

"Closing the gap between you and the attacker is the best way to keep them at bay."

Q. How do we close the distance and keep the organization and its partners safe from malicious attacks?

2. Keep your friends close, but your elbows closer (5-10 min)

"When rolling or competing against someone, you learn that elbows and arms are vulnerable and can be used against you. This can lead to submissions such as shoulder locks, wrist locks, and armbars."

Q. How do you identify and manage your security vulnerabilities?

3. Size doesn't matter (5-10 min)

"Size thankfully doesn't matter. What's most important is the techniques that you use and how you apply them. The most vital part is feeling the opponent's movements and predicting their steps prior to them taking it – like chess."

Q. How proactive is your approach to cybersecurity? How do you judiciously and effectively utilize your resources?

4. ***When you know how to defend, you know how to attack (5-10 min)***

   "Coach Mariusz G. says his focus wasn't to attack when he was a white belt. It was to defend, to simply survive. Whilst doing this, he was able to learn and feel the way the opponent reacted to different things, ultimately teaching him areas of weakness and vulnerability that can be exploited."

   Q. How do you keep up with the evolving attack methods and techniques?

5. ***Everything in life changes, but Jujutsu stays the same (5-10 min)***

   "Regardless of the school of training, the coaches you have, even your personal style, the foundations of Brazilian jiu-jitsu remain the same. Reduce the gap, keep your body ready and in check so it cannot betray you, proactively plan for attack and how to defend and put the hours in on the mat."

   Q. Cybersecurity fundamentals don't change. What are these fundamentals and how do you adhere to them?

III. Closing Thoughts (5-10 min)

Recommendations and Takeaways

Q. How do we close the distance and keep the organization and its partners safe from malicious attacks?

- Continuous monitoring
- Prompt processing and acting on intelligence alerts
- Periodic Penetration testing
- Inventory applications and dependencies to understand risk exposure.
- Conduct risk assessment to quantify risk and start with highest priority applications.
- Identify single points of failure.
- Trust but verify. You want to test things repeatedly so that when that inevitable outage happens, you're confident that the incident will not have drastic consequences.
- Consider implementing identity orchestration and continuity solutions to introduce redundancy after evaluating cost vs risk.
- Create a culture of resilience that is not surprised when an outage happens but can handle it with grace and confidence.

Q. How do you identify and manage your security vulnerabilities?

- There are three main LLM attack vectors: a) Attacking the LLM Model directly, b) Attacking the infrastructure and integrations, and c)Attacking the application.
- Prevention and mitigation strategies include a) Strict input validation and sanitization, b) Isolating the LLM environment from other critical systems and resources, c) Restricting the LLM's access to sensitive resources and limiting its capabilities to the minimum required for its intended purpose; d) Regularly audit and review the LLM's environment and access controls; e) Implement real-time monitoring to promptly detect and respond to unusual or unauthorized activities; and f) Establish robust governance around ethical development and use of LLMs.
- Establish specific use cases and indicators for identifying potential insider threat incidents.

- Monitor for suspicious activities like outside of scheduled hours logins and unusual login locations.
- Take a proactive approach to insider risk management, focusing on user behavior and indicators rather than just incident response.
- Consider incorporating the expertise of behavioral psychologists and researchers into the organization's insider threat program.

Q. How proactive is your approach to cybersecurity? How do you judiciously and effectively utilize your resources?

- Treat cybersecurity as a strategic opportunity and invest adequate resources to build and sustain this competency.
- Proactively determining different disaster scenarios and stress testing organizational resilience in dealing with those situations.
- Consider establishing key metrics to measure the effectiveness and maturity of cybersecurity operations.
- Invest in automation to gather and maintain compliance evidence.
- Implement "compliance as code" to bake compliance into the software development lifecycle.
- Automate change management processes to speed up compliance reviews.
- Conduct regular manual reviews to validate automated compliance processes and findings.
- Ensure prompt action on compliance alerts and issues to avoid consequences.

Q. How do you keep up with the evolving attack methods and techniques?

- "Bypassing the human verification is something super critical we need to address. It's something we can't afford to wait on, and it's low-hanging fruit."
- Implement a driver's license validation solution to authenticate callers to the IT help desk.
- Explore expanding the use of identity verification technologies beyond the IT help desk, such as for wire transfers and other high-risk financial transactions.
- Adopt a layered approach to establishing a robust defense. "You need a good tech stack, user entity behavior analytics, conditional access policies, MFA, and security awareness training."
- Educate IT support staff on identifying potential social engineering attempts, even when the caller appears to be using advanced techniques like voice cloning.
- Implement a policy instructing employees to hang up and call back when they receive requests for sensitive information or transactions.
- Stay vigilant and continue to explore new solutions to combat the evolving threat of social engineering attacks.

Q. Cybersecurity fundamentals don’t change. What are these fundamentals and how do you adhere to them?

- Treat cybersecurity as a strategic opportunity and invest adequate resources to build and sustain this competency.
- Establishing fail-safe software development practices.
- Software testing and rollout models must be continuously and rigorously tested.
- Proactively determining different disaster scenarios and stress testing organizational resilience in dealing with those situations.
- Consider establishing key metrics to measure the effectiveness and maturity of cybersecurity operations.
- Demand visibility and transparency into the specific activities a managed service provider is conducting to protect the organization, such as vulnerabilities remediated, security incidents handled, and training completed. Regular reporting should be provided.
- Conduct thorough due diligence when selecting a cybersecurity [1]service provider, including validating the qualifications and expertise of the individuals who will be responsible for security, the technologies used, and references from other customers.