Cybersecurity Readiness Podcast Series

Episode Title: AI vs. AI: Automating Defense to Outpace Automated Attacks

Host: Dave Chatterjee, Ph.D. — https://dchatte.com

Guest: Roi Cohen, CEO and Co-Founder of Vicarius

Summary Pitch

In this episode, Dr. Dave Chatterjee speaks with Roi Cohen, CEO and Co-Founder of Vicarius, about the urgent need to counter AI-driven attacks with equally automated defenses. Cohen, who began his career managing mission-critical systems in the Israeli military at age 18, shares his journey through leadership roles at CyberArk to launching Vicarius. Drawing from real-world penetration tests at hospitals and Ivy League institutions, he illustrates how attackers exploit simple misconfigurations to access sensitive data. Together, they examine why defenders must move beyond manual, ticket-based remediation to keep pace with adversaries leveraging agentic AI.

The conversation underscores that automation, while essential, is not sufficient without human oversight and governance discipline. Anchored in Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) framework, the discussion highlights the organizational mindsets and technological building blocks needed to sustain resilience. Cohen emphasizes the hybrid future of AI and human collaboration, where transparent reasoning and flexible control are vital for trust.

Discussion Highlights

• Automated offense is a present reality—AI agents can autonomously find and exploit vulnerabilities at scale.

• Field anecdotes: hospital breach via a misconfigured network printer; Ivy League penetration test exposing domain admin credentials.

• Why manual remediation fails—average time to exploit has shrunk from months to hours.

• Five components of automated defense: asset discovery, AI-driven risk prioritization, automated patch deployment, remediation playbooks, and continuous testing.

• Beyond patching: configuration changes and alternative mitigations can delay or prevent exploits.

• The CPD framework applied: commitment from leadership, preparedness through automation architecture, and discipline via monitoring and validation.

• Hybrid future: AI-enhanced automation with human oversight to build transparency and trust.

Actionable Recommendations

- Eliminate manual, ticket-based remediation—scale defenses with AI-driven automation.

- Continuously validate segmentation, patching, and remediation effectiveness.

- Educate executives to dispel myths (e.g., only Microsoft vulnerabilities matter) and secure buy-in for automation.

- Adopt hybrid models where automation is complemented by red-team validation and human-in-the-loop oversight.

- Apply the CPD framework: leadership commitment, architectural preparedness, and governance discipline.

Time Stamps

- 0:49 — Roi Cohen's career journey: Israeli military to CyberArk to Vicarius

- 3:32 — The CPD framework and its military inspiration

- 7:46 — Rise of automated offense with agentic AI

- 9:38 — Field anecdotes: hospital penetration test

- 14:19 — Ivy League penetration test case

- 17:07 — Why manual remediation fails in today's threat landscape

- 19:35 — Shrinking time-to-exploit: months to hours

- 23:52 — Five components of automated defense infrastructure

- 27:07 — Patching difficulties and alternatives

- 30:01 — Hybrid future: AI + human oversight

- 34:48 — Transparency, reasoning, and trust in AI-driven security

- 39:16 — Closing reflections: AI as an enabler, not a replacement

Memorable Quotes

- "Automatic offense is not science fiction. This is the reality we must face." — Roi Cohen

- "You cannot fix what you don't know is there—automated asset discovery is the foundation." — Dr. Dave Chatterjee

- "Automation without discipline will backfire—human oversight remains critical." — Dr. Dave Chatterjee

- "AI is an enabler, but people are not dispensable. The future is hybrid." — Roi Cohen