Increased Focus on AI and Machine Learning in Cybersecurity

Eric L. Harris Jr.

CISO, Charlie Norwood VA Medical Center, Department of Veterans Affairs

Something to think about…

“AI’s growing role in cyber crime is undeniable. By 2025, AI will not only enhance the scale of attacks but also their sophistication. Phishing attacks will be harder to detect, with AI continuously learning and adapting.”

“As AI tools like ChatGPT and Google Gemini become deeply integrated into business operations, the risk of accidental data exposure skyrockets with new data privacy challenges.”

- Jeremy Fuchs, Cyber Security Evangelist at Check Point Software Technologies.

Key AI Considerations

- AI as a Change Catalyst
- Balancing Innovation and Risk
- Tools for Success
- Future Resilience

AI as a Change Catalyst

- Threat Detection/Prevention
- Predictive Analytics
- Process Automation

Balancing Innovation and Risk

- Advantages
  - Speed and Accuracy
  - Scalability
  - Real-time Learning

- Disadvantages
  - Adversarial AI
  - Data Quality and Biases
  - Ethical Considerations

Tools for Success

- For Security Leaders:
  - Security Information and Event Management (SIEM)
  - Threat Intelligence Platforms (TIP)
- For Technical Teams:
  - Endpoint Detection and Response (EDR)
  - Vulnerability Management Tools
- For Developers:
  - Static Application Security Testing (SAST)
  - Software Composition Analysis (SCA)

Future Resilience

- Staying Current with Emerging Trends
- Building/Updating AI Governance
- Investment in Talent Development
- Innovators and Security Teams Collaboration

Let’s Wrap Up…

- Key Takeaways:
  - AI is a powerful tool…for BOTH sides
  - Master the Balancing Act
  - Collaboration is Key

- Call to Action:
  - Explore AI Tools that HELP your organization
  - Stay Current and Informed
  - Be the Cultural Change Agent for your Organization

Thank you!