The Intersection of Cyber and AI for Computational Modeling of Biological Agents

NASEM Navigating the Benefits and Risks of Publishing Studies of In Silico Modeling and Computational Approaches of Biological Agents and Organisms – A Workshop

April 4, 2025

Nandi Leslie, Ph.D.

Relevant Professional Experiences

- Published over 60 R&D papers, edited books, and patents on AI/machine learning (ML) and cyber
- Presented over 50 R&D talks at conferences and workshops
- Served as board member, conference chair, panelist, and program committees on 10+ conferences
  - Princeton University, Board of Trustees
  - Howard University, Center of Excellence in AI and Machine Learning Advisory Board
  - Principal Technical Fellow, RTX/Raytheon
  - Chief Data Scientist, Raytheon
  - Raytheon R&D Chief Engineer
  - Raytheon Technology Solutions Director, Cyber
  - National Academies Study on Biotechnology Capabilities for National Security Needs
  - President's National Security Telecommunications Advisory Committee, Strategy for Increasing Trust in the Information and Communications Technology and Services
  - National Academies Army Board on Army R&D on AI and Justified Confidence Committee
  - National Academies on AI Test and Evaluation for the Air Force Committee
  - Society of Industrial and Applied Mathematics (SIAM), Industry Committee
  - SIAM Committee on Programs and Conferences

Signatures vs. Anomalies

- Having the best signatures is inadequate
- Anomaly detection presents its own issues
- Many approaches exist for anomaly detection
- Need to organize intrusion detection to improve predictions

Challenges & Opportunities for the Use of AI/ML in Cybersecurity: Considerations for In Silico Biological Studies

Data Quality and Availability

- AI applications require volumes data

Implementation Complexity

- Deep understanding of ML and cyber

Privacy Issues

- Data privacy requirements and laws

Adversarial Attacks

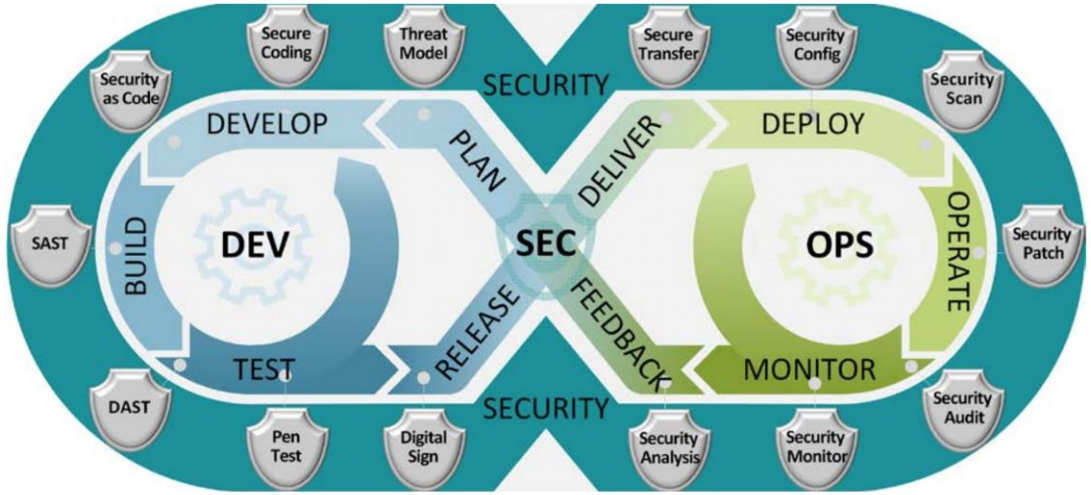
- Adversarial AI

Unsupervised Learning Challenges

- Analyze unlabeled data
- Predict clusters in feature space
- Observe distance from normal data
- Measure similarity and dissimilarity between clusters
- Visualize patterns
- Examine predictions from clustering

Opportunities for the Use of AI/ML for DevSecOps

- Feedback Loop Automation
- Automation and Autonomy using AI/ML
- AI-Enhanced Performance Optimization
- AI/ML-based security
- Automation of AI-based Code Reviews
- MLOps Implementation for Event/Messaging Streams



Excerpt Nichols, B. (2021) The Current State of DevSecOps Metrics

Questions

- Any questions?