SEI Bulletin

Trouble reading this email? View in browser.

Machine Learning for Cybersecurity Needs Two-Way Explainability

November 22, 2023—Machine learning (ML) seems a natural fit for data-rich cybersecurity operations, but a lack of explainability--from ML models to humans and the other way around--is standing in the way. A new SEI Blog post illustrates both directions of explainability and recommends the research needed to advance cybersecurity ML.

"On a very basic level, explainable cybersecurity ML can be achieved now, but there are opportunities for significant improvement," wrote Jeffrey Mellon and Clarence Worrell in *Explainability in Cybersecurity Data Science*. "Significantly strengthening the human-machine team through explainable cybersecurity ML is one of the biggest steps we can take to encourage broader adoption of data science into cybersecurity organizations and systems."

Read the post »

SEI News

Generative AI Presents Key Opportunities and Challenges for Defense Department
The stakes are high for adopting generative AI in national defense, according to a cross-domain group convened by the SEI and DoD.

See more news »

Latest Blogs

Explainability in Cybersecurity Data Science
Jeffrey Mellon and Clarence Worrell provide an overview of explainability in machine learning and illustrate model-to-human and human-to-model explainability.

Generative AI Q&A: Applications in Software Engineering
John Robert and Douglas Schmidt explore the transformative impacts of generative AI on software engineering as well as its practical implications and adaptability in mission-critical environments.

The OSATE Slicer: Fast Reachability Query Support for Architectural Models
Sam Procter introduces the OSATE Slicer, a new extension to the Open Source AADL Tool Environment that adapts a concept called slicing to architectural models of embedded, critical systems.

See more blogs »

Latest Podcasts

User-Centric Metrics for Agile
Will Hayes, Patrick Place, and Suzanne Miller discuss how user stories can help put development in the context of who is using the system and lead to a conversation about why a specific metric is being collected.

The Product Manager's Evolving Role in Software and Systems Development
Judy Hwang and Suzanne Miller talk about implementing foundational product management principles in software and systems development and offer resources for strengthening Agile product delivery practices.

Measuring the Trustworthiness of AI Systems
Carol Smith, Katie Robinson, and Alex Steiner discuss how to measure the trustworthiness of an AI system as well as questions that organizations should ask before determining if they want to employ a new AI technology.

See more podcasts »

Latest Publications

Assessing Opportunities for LLMs in Software Engineering and Acquisition
This white paper examines how decision makers can assess the fitness of large language models (LLMs) to address software engineering and acquisition needs.

Mixed-Trust Computing for Real-Time Systems
This paper proposes a real-time mixed-trust computing framework that combines verification and protection.

See more publications »

Latest Videos

Connecting Stakeholders for DoD Software Systems
Hasan Yasar highlights how the upcoming DoD Weapon Systems Software Summit will play a pivotal role in creating effective solutions for securely delivering robust software capabilities on time and on budget.

Cyber Supply Chain Risk Management: No Silver Bullet
Brett Tucker emphasizes using robust enterprise risk management to achieve operational resilience in the cyber supply chain.

Upcoming Events

FloCon 2024, January 9-11, 2024
FloCon centers on improving network security by analyzing a variety of data supported by innovative machine learning, hardware, and network storage.

See more events »

Upcoming Training

Cybersecurity Oversight for the Business Executive
January 17-18, 2024 (SEI Live Online)

Software Architecture Design and Analysis
March 5-8, 2024 (SEI Live Online)

See more courses »

Employment Opportunities

Senior AI Workforce Development Engineer

Senior Cybersecurity Engineer

Cyber Readiness Software Developer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute