Seminar

ECU COMPUTER SCIENCE

Co-Modeler: AI-Driven Threat Modeling

Abstract. Traditional threat modeling is a critical component of secure software development, yet it remains a severe bottleneck due to the slow, manual, and inconsistent process of decomposing architecture diagrams and mapping them to enterprise security controls. To address this scalability challenge, this presentation discusses Co-Modeler: an AI-driven threat modeling engine that leverages the advanced multimodal capabilities of Google's Gemini Flash. By utilizing an end-to-end "Vision-to-Reasoning" approach, Co-Modeler directly ingests complex architecture diagrams to instantly extract key system components (Actors, Processes, Datastores, and Dataflows) and intelligently correlate them with applicable STRIDE threats and configurable security frameworks, such as NIST CSF and ISO 27001. This paradigm shift from a purely manual pipeline to an AI-assisted workflow reduces initial threat identification time from days to mere minutes. Ultimately, by automating the repetitive data mapping process, Co-Modeler ensures consistent, high-frequency security assessments while maintaining a strategic Human-in-the-Loop (HITL) architecture, empowering security professionals to focus their expertise exclusively on validating complex edge cases and high-impact risk scenarios.

Biography. Dr. Shankar Chebrolu, Director of Security Architecture at Red Hat, leads risk assessments for crown jewel systems hosting sensitive data. With an IT PhD, Dr. Chebrolu combines deep academic rigor with extensive practical experience, backed by elite industry certifications spanning cybersecurity, data privacy, and enterprise risk management. Passionate about advancing the practice of secure system design, he is a founding member of the Threat Modeling Connect community. Furthermore, Dr. Chebrolu actively bridges the gap between industry and academia; he serves as guest faculty and the Vice-Chair of the Advisory Board for Duke University's Global Executive Cybersecurity Certificate Programs, where he helps shape the curriculum for the next generation of cybersecurity leaders.

Dr. Shankar Chebrolu
Director of Security Architecture
Red Hat, Inc.

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

Friday March 20, 2026
Time: 2:00 – 3:00pm

Microsoft Teams
Join the meeting now
Meeting ID: 213 708 622 023 28
Passcode: yy2tW7kT

Contact: Dr. Kamran Sartipi
Dept. of Computer Science, ECU
https://cs.ecu.edu/sartipik16/CSseminar/