ORCHESTRATING SECURITY OPERATIONS WITH AI AGENTS

Event Details

- Date and day: 21st February 2026 (Saturday)
- Venue: Offline (Chemical AV Room, SCET)
- Time: 10:30 AM – 12:30 PM IST
- Professional Volunteers: Dr. Gayatri Kapadia, Prof. Zankhana Vaishnav
- Student Coordinators: Hamdan Siddiki, Chaitanya Chavda, Kalp Shah
- Student Volunteers: IEEE SCET Student Branch, MCA Tech Club "Techverse"
- Total no. of Participants: 70

Objective

The expert session on "Orchestrating Security Operations with AI Agents" was organized to introduce participants to AI-driven techniques used in modern digital investigations and to enhance their understanding of integrating Artificial Intelligence into security operations and digital forensic workflows. The session focused on enabling students to evaluate and apply AI-based tools to improve the accuracy, efficiency, and speed of forensic analysis, while also addressing ethical considerations, legal responsibilities, and the responsible use of AI in cybersecurity. Additionally, it highlighted emerging challenges in conducting digital investigations within complex and evolving technological environments, preparing students for real-world cybersecurity scenarios.

Summary

The event commenced at 10:30 AM with registration, followed by the felicitation of Dr. Nikunj Tahilramani by Prof. (Dr.) Gayatri Kapadia. The speaker addressed the evolution of AI-driven enterprise ecosystems, highlighting the integration of AI agents in corporate workflows, recruitment processes, and decision-making frameworks. The session established the relevance of Artificial Intelligence in modern security operations and digital investigation environments.

The technical discussion covered AI-enhanced cybersecurity practices, including Vulnerability Assessment and Penetration Testing (VAPT), enterprise security analytics, and AI-driven threat intelligence. The concepts of Red Teaming with AI and Red Teaming for AI were explained, along with adversarial testing, prompt manipulation, prompt injection risks, and secure AI deployment frameworks. Key topics such as Retrieval-Augmented Generation (RAG), Large Language Model (LLM) deployment strategies (cloud and on-premise), and the comparison between traditional SOC (SIEM and SOAR) and Autonomous SOC

powered by Agentic AI were presented, supported by a case study demonstrating large-scale alert management and operational efficiency.

The session further included a live demonstration using the n8n platform to illustrate AI-driven workflow automation (Trigger → Action → Output) for cybersecurity use cases such as URL spam detection, DNS tracing, credential verification, and risk assessment. The program concluded with an interactive discussion on career opportunities in AI-driven security domains, followed by a vote of thanks. A memento and certificate were presented to Dr. Nikunj Tahilramani by Prof. Zankhana Vaishnav as a token of appreciation. The event also featured an IEEE membership promotion segment highlighting professional networking, technical resources, research and travel grants, and development opportunities for students. The organizing team sincerely expressed gratitude to Dr. Chirag Paunwala, Chair – IEEE Gujarat Section, for his guidance and support in making the initiative successful.

Photographs

Compiled By:

- Name: Jainim Jariwala, Secretary - IEEE SCET SB CS Chapter
- Facilitated by:
  Faculty Advisor: Dr. Chirag Paunwala
  Email: cpaunwala@gmail.com
  Chair- Masoom Parekh
  Vice Chair- Aryan Sariya