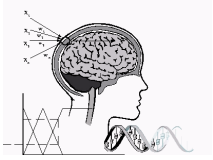
International
Innovation in Knowledge Based and Intelligent Engineering Systems



INVITED SESSION SUMMARY

Title of Session:
Agentic AI and Retrieval-Augmented NLP for Intelligent Intrusion Detection and Next-Generation SIEM (Privacy and LLM Security Included)

Name, Title and Affiliation of Chair: Associate Professor Dr. Yessine Hadj Kacem
PMP® Certified || ISTQB® Certified
University of Sfax, Tunisia-Faculty of Economics and Management
LinkedIn | dblp | Google Scholar:

Details of Session (including aim and scope):

The growing complexity of modern IT infrastructures and the explosion of heterogeneous security data, largely textual and semi-structured (logs, alerts, incident tickets, threat reports, playbooks, chatops messages, vulnerability advisories, CTI feeds, and darknet content), have made traditional IDS (Intrusion Detection System) and SIEM (Security Information and Event Management) correlation approaches increasingly limited. While Deep Learning and Large Language Models (LLMs) offer powerful capabilities for semantic understanding and reasoning, their deployment in security operations raises new challenges related to reliability, evidence grounding, privacy, and adversarial manipulation.

Recent progress in Retrieval-Augmented Generation (RAG) enables LLMs to ground outputs in verifiable sources such as enterprise knowledge bases, SIEM indices, asset inventories, and threat intelligence repositories. Beyond this, Agentic AI, LLM systems that plan, use tools, and execute multi-step workflows, creates opportunities for end-to-end automation and decision support in the SOC, including alert triage, threat hunting, incident reconstruction, and response orchestration. Agentic RAG combines planning and tool-use with retrieval to support complex investigations while improving traceability through citations, provenance, and audit logs.

This invited session aims to bring together researchers and practitioners at the intersection of NLP/LLMs, agentic systems, IDS, and SIEM/SOAR platforms. We invite contributions on novel methods, architectures, and evaluations that leverage agentic reasoning, retrieval grounding, and multimodal security telemetry to enhance detection, correlation, prediction, and incident response. Emphasis will be placed on privacy-preserving and trustworthy deployment, as well as the emerging landscape of attacks on LLMs and generative AI in

operational cybersecurity (e.g., prompt injection, data leakage, poisoned retrieval corpora, tool hijacking, and model backdoors). Topics of interest include, but are not limited to:

- NLP for log analysis, alert triage, and anomaly detection
- IDS enhanced by deep learning, transformers, and foundation models
- Retrieval-Augmented Generation (RAG) for evidence-grounded detection and reporting
- Agentic AI for SOC automation: planning, tool use, and multi-step workflows
- Agentic RAG for threat hunting, incident reconstruction, and cross-source reasoning
- LLM-based assistants for SIEM/SOAR: query translation, playbook generation, and safe automation
- Text mining of threat reports, vulnerability advisories, CTI feeds, and darknet data
- Semantic similarity and retrieval-based detection of suspicious behaviors
- Multimodal security analytics combining textual and telemetry data
- Generative models for synthetic attack data and scenario simulation
- Explainable and auditable IDS powered by NLP/LLMs
- Privacy and governance for LLMs in security pipelines
- Security of LLMs and generative AI: prompt injection, jailbreaks, poisoned retrieval, backdoors
- Robustness and evaluation: adversarial stress tests, drift, and trustworthy benchmarks
- Applications to cloud, IoT, and critical infrastructures, including real-world deployments

Main Contributing Researchers / Research Centres (tentative, if known at this stage):

Associate Professor Dr. Yessine Hadj Kacem
Laboratory on Development and Control of Distributed Applications (ReDCAD)
University of Sfax, Tunisia-Faculty of Economics and Management

Associate Professor Dr. Maha Charfeddine Hamza
REGIM Lab.: REsearch Groups on Intelligent Machines
National Engineering School of Sfax, University of Sfax, Department of Computer Engineering and Applied Mathematics, BP 1173, Sfax, 3038, Tunisia

Assistant Professor Dr. Houda Abadlia
LARIA Research Unit (UR22ES01), National School of computer science, University of Manouba, Tunisia

Assistant Professor Dr. Nadia Smairi
LARIA Research Unit (UR22ES01), National School of computer science, University of Manouba, Tunisia

Website URL of Call for Papers (if any):
Email & Contact Details: Dr. Yessine Hadj Kacem : yessine.hadjkacem@enis.tn (**Tel**: (+216) 22535395--(+216) 98762850) Dr. Maha Charefeddine Hamza: maha.charfeddine@enis.tn Dr. Houda Abadlia: houdaabadlia@gmail.com Dr. Nadia Smairi: nadia.smairi@gmail.com