Workshop on AI for cyber Threat Intelligence (WAITI)

The AI for Cyber Threat Intelligence (WAITI) Workshop will be held on Monday, December 9, 2024, in conjunction with the Annual Computer Security Applications Conference (ACSAC) in Hybrid mode. ACSAC will be held in Hawaii, USA. We have merged the IoT Security and Cyber Threat Intelligence (IoT-SCTI) Workshop with WAITI to cater to a wider audience.

Official Website: https://waiti-workshop.github.io/

Call for Papers

The cybersecurity landscape constantly shifts, throwing a never-ending data stream at security professionals. Valuable threat intelligence is hidden within this large stream, including text reported in social media, technical reports, and dark web forums. Traditionally, Cyber Threat Intelligence (CTI) relied on manual analysis or basic keyword matching, leading to bottlenecks and missed opportunities. Security analysts face limitations in the sheer volume of data, sophistication in tactics like code obfuscation and social engineering, and the rapid evolution of threats necessitates real-time processing to stay ahead of attackers. In today's digital landscape, where the volume and complexity of data continue to escalate, Natural Language Processing (NLP) techniques and large language models have emerged as indispensable tools for deciphering and mitigating cyber threats. NLP empowers machines to understand and process human language, offering significant benefits for CTI such as automated processing, advanced threat detection, and real-time analysis, allowing immediate threat identification and response. Thus, extracting and analyzing this information efficiently is critical for proactive defense strategies. This workshop explores the exciting potential of Artificial Intelligence/Generative AI to revolutionize cybersecurity, particularly CTI gathering and analysis. The workshops will provide a platform for researchers, practitioners, and enthusiasts to delve deeper into specialized topics related to NLP, Large Language Models (LLMs), and, more in general, artificial intelligence techniques in the context of cybersecurity and cyber threat intelligence.

We encourage original and high-quality contributions, preliminary work, and novel ideas on topics, including but not limited to:

- Information extraction in cyber threat intelligence
- Deep learning architectures for threat detection and analysis
- Visualization techniques for CTI
- Large Language Models for CTI
- Intelligence-driven threat-hunting
- Attribution
- Sharing of CTI
- Hunting and Tracking Adversaries
- Threat Quantification & Prioritization
- Explainable AI in Cybersecurity
- Dynamic Threat Adaptation with LLMs
- Multimodal Threat Intelligence Fusion
- LLMs for Malware Detection
- Bias Mitigation in LLMs for Cyber Threat Intelligence
- Federated Learning for Threat Detection
- LLMs for Social Media Threat Analysis
- LLMs and Visual Content
- Multimodal Large Language Models (MLLMs)
- Understanding Technical Language for CTI
- Cross-lingual Threat Intelligence using LLMs
- Misinformation Detection in CTI with LLMs
- LLM-powered Threat Scenario Generation
- Human-in-the-loop systems for LLM-based CTI
- Explainable Threat Intelligence Reports with LLMs
- Benchmarking LLM Performance
- Legal and Ethical Considerations for AI
- Zero Trust and CTI
- CTI in the IoT domain
- AI/GenAI for users' behavior analysis and inference
- GenAI for mobility management and network control
- AI/GenAI within 6G networks
- Blockchain-based approaches for CTI
- Applying CTI/Case Studies
- CTI for IoT Systems
- Using IoT for sourcing CTI

Submissions should be a maximum of 6 pages, using the double-column ACM proceedings format (acmart) template available at https://www.acm.org/publications/taps/word-template-workflow, with the [sigconf, anonymous] options.
Two additional pages can be used for the Appendix. Note that the reviewers are not expected to read the Appendix. All submissions must be anonymous.
We also encourage submission of Systemization-of-Knowledege (SoK) papers which distill the intersection of LLM and Cyber security of previously published articles.

The submission website is at: [Available soon]

Publication

We are currently negotiating with major publishers for the workshop proceedings.

Important Dates

Submission Deadline	September 20, 2024
Acceptance Notification	October 1, 2024
Final Manuscript due	November 15, 2024
Workshop Date	December 9, 2024

Further details about the workshop can be found on the workshop website: https://waiti-workshop.github.io/

For any questions, please contact the Workshop Chairs at: vinod.puthuvath@unipd.it; serena.nicolazzo@unimi.it

Organizing Committee

Program Chairs

- Omar Alrawi - Georgia Tech, USA.
- Mauro Conti - University of Padua, Italy and TU Delft, The Netherlands.
- Antonino Nocera - University of Pavia, Italy.
- V.S. Subrahmanian - McCormick School of Engineering, Northwestern University, USA.

Workshop/ General Chairs

- Alessandro Brighente - University of Padua, Italy.
- Serena Nicolazzo - University of Milan, Italy.
- Vinod P. - University of Padua, Italy, and Cochin University of Science and Technology, Kochi, India.

Publicity Chairs

- Marco Arazzi - University of Pavia, Italy.
- Serena Nicolazzo - University of Milan, Italy.
- Vinod P. - University of Padua, Italy, and Cochin University of Science and Technology, Kochi, India.

Program Committee

1. Basant Agarwal - Central University of Rajasthan, India.
2. Marco Arazzi - University of Pavia, Italy.
3. Zalán Bodó - Babeş-Bolyai University, Romania.
4. Alessandro Brighente - University of Padua, Italy.

5. Fabio De Gaspari - Sapienza University of Rome, Italy.
6. Andrea Di Sorbo - University of Sannio, Italy.
7. Earlence Fernandes - University of California San Diego, USA.
8. Alessandro Galeazzi - University of Padua, Italy.
9. Ankit Gangwal - International Institute of Information Technology, Hyderabad, India.
10. Sarada Prasad Gochhayat - India Institute of Technology, Jammu, India.
11. Meng Li - Hefei University of Technology, China.
12. Eleonora Losiouk - University of Padua, Italy.
13. Alejandro Guerra Manzanares - Center for Interacting Urban Networks, New York University Abu Dhabi, United Arab Emirates.
14. Francesco Marchiori - University of Padua, Italy.
15. Weizi Meng - Technical University of Denmark, Denmark.
16. Francesco Mercaldo - University of Molise, Italy.
17. Preeti Mishra - Doon University Dehradun (State Government University), India.
18. Smita Naval - Malaviya National Institute of Technology, India.
19. Serena Nicolazzo - University of Milan, Italy.
20. Antonino Nocera - University of Pavia, Italy.
21. Stjepan Picek - Radboud University, The Netherlands.
22. Vinod P. - University of Padua, Italy, and Cochin University of Science and Technology Kochi, India.
23. Andrea Saracino - Scuola Universitaria Superiore Sant'Anna di Pisa, Italy.
24. Simone Soderi - Scuola IMT Alti Studi Lucca, Italy.
25. Shrikant Tangadi - Christ University, India.
26. Aaron Visaggio - University of Sannio, Italy.
27. Suleiman Y. Yerima - The British University in Dubai, United Arab Emirates.
28. Chia-Mu Yu - National Taiwan University, Taiwan.

Workshop Registration

If you are interested in attending, please check off the appropriate box on the conference registration form and add in the AI for cyber Threat Intelligence (WAITI) Workshop fee.

For accepted papers, at least one author must register and attend. Remote presentation is allowed subject to approval from PC. We generally encourage in-person attendance, however authors with adequate motivation can present remotely.