RIDER UNIVERSITY

Department of Computer Science & Physics
College of Liberal Arts and Sciences, Rider University
2083 Lawrenceville Road Lawrenceville, NJ 08648

Enhancing NVISO's Cybersecurity LLM Agents with Open-Source Threat Intelligence Feeds for Improved Intrusion Detection

1 Introduction

Large language models are very popular[6]. NVISO's Cybersecurity LLM Agents represent a pioneering advancement in the application of Large Language Models (LLMs) for automating and optimizing cybersecurity operations.[7] Built atop the AutoGen framework, these agents are designed to perform critical security tasks such as threat detection, incident response, and threat analysis by leveraging the natural language understanding and generation capabilities of LLMs [8]. Their modular and extensible architecture enables easy customization and integration into diverse organizational environments, allowing security teams to automate repetitive workflows and enhance analytical efficiency.[3]

In today's threat landscape, where adversaries continuously adapt and evolve, NVISO's LLM agents are increasingly used to streamline complex security operations and reduce the manual workload on cybersecurity professionals.[9] These agents can rapidly process large volumes of threat data, detect behavioral patterns, and produce actionable insights, thus supporting faster and more informed decision-making[1].

However, a notable limitation of the current implementation is its reliance on static, preloaded knowledge.[2] In an age of fast-evolving cyberattacks, static models may lack the adaptability needed to recognize and respond to emerging threats.[4] This research aims to bridge that gap by integrating real-time, open-source threat intelligence feeds—specifically AbuseIPDB and the Malware Information Sharing Platform (MISP)—into the NVISO framework. This enhancement will enable the agents to dynamically validate Indicators of Compromise (IoCs), such as suspicious IPs and domains, significantly improving the agents' accuracy and responsiveness in detecting contemporary threats.

2 Hypothesis/Objectives

NVISO's Cybersecurity LLM Agents currently rely on static data, limiting their ability to detect and respond to evolving cyber threats. This static approach reduces detection accuracy, increases false negatives, and weakens defense against emerging threats such as zero-day attacks.[5] Integrating real-time threat intelligence feeds is necessary to enhance the agents' adaptability and effectiveness in dynamic threat environments.

- To integrate real-time, open-source threat intelligence feeds into NVISO's Cybersecurity LLM Agents.
- To enrich agent decision-making by cross-referencing active Indicators of Compromise.
- To evaluate improvements in detection accuracy, reduction of false positive/negative rates, and system responsiveness.

3 Proposed methods and procedures

To achieve the research objectives, the project will follow a structured methodology that progresses from integration to evaluation. The steps are designed to ensure that the enhancements made to NVISO's Cybersecurity LLM Agents are both practical and verifiable.

First, the focus will be on connecting the agents with real-time threat intelligence feeds. This will include integrating AbuseIPDB, which provides dynamic IP reputation data, and MISP, which supports structured sharing of Indicators of Compromise (IoCs). Next, development will concentrate on building connectors and normalization layers to ensure that data from these feeds can be properly parsed, formatted, and used within NVISO's agent workflows. After successful integration, enhancements will be made to the agent decision-making logic, allowing the agents to actively reference updated intelligence during threat detection. Finally, the improved system will be tested and evaluated using established cybersecurity datasets to assess its accuracy, adaptability, and responsiveness. The procedures will be listed in detail below:

- **Stage 1:** Integrate AbuseIPDB and MISP feeds into NVISO's Cybersecurity LLM Agents to provide real-time validation of suspicious IPs, domains, and IoCs.
- **Stage 2:** Develop API connectors and implement data normalization so that intelligence feeds are compatible with NVISO's AutoGen-based workflows.
- **Stage 3:** Enhance agent workflows by modifying decision-making logic to incorporate real-time intelligence during detection and analysis.
- **Stage 4:** Test and evaluate the system using benchmark datasets such as NSL-KDD and CICIDS2017, measuring detection accuracy, false positive/negative rates, and response time.
- **Stage 5:** Review and analyze the results with the supervisor, refine methods if necessary, and prepare the paper for final submission.

4 Project timetable/Faculty meeting

This independent study will be conducted during the Fall semester of 2025. The participated student will work with the supervisor and meet once a week for progress reports. The detailed weekly schedule is shown below:

Time	Task
Weeks 1-2	Begin the research on real-time threat intelligence feeds (AbuseIPDB and MISP) while reviewing outside resources that explain their structure, functionality, and integration methods.
Weeks 3-4	Continue researching the NVISO Cybersecurity LLM Agents framework and collect academic papers supporting the use of LLMs in cybersecurity and intrusion detection..
Weeks 5-6	Develop API connectors and implement data normalization techniques to ensure compatibility between the threat intelligence feeds and NVISO's agent workflows.
Weeks 7-8	Enhance the agent decision-making logic so that the system actively references real-time intelligence during detection and event analysis..
Weeks 9-10	Begin testing the enhanced agents using benchmark datasets (NSL-KDD, CICIDS2017). Record detection accuracy, false positive/negative rates, and system response times.
Weeks 11-12	Complete testing and analyze the results to identify strengths, weaknesses, and areas for improvement. Work with the supervisor to finalize findings and prepare the paper for submission.

5 Project evaluation

The independent study will be evaluated from multiple perspectives. They include but not limited to:

- **Knowledge:** The student are required to understand the fundamentals of machine learning and LLM, and NVISO's agent.
- **Programming skills:** The participated student will be required to programming and debugging Large Language Models.
- **Research experience:** The student will cooperate with the supervisor on researching the field of large language models and proposing new ideas novel to this field.

- **Academic Writing:** The student will cooperate and work with the supervisor on getting the potential new ideas or findings published in academic conferences/journals. The student will help the writing process and other tasks capable of.

The final grade of the independent study will be decided upon the following components with the regarding weight:

- Advisor meeting (10%)
- Programming implementation (30%)
- Results/Data analysis (30%)
- Poster and paper writing (30%)

6 Relevant bibliography

References

[1] Agrawal, Prerna and Trivedi, Bhushan. "Analysis of android malware scanning tools". *International Journal of Computer Sciences and Engineering* 7(3) (n.d.): 807–810.

[2] Alharbi, Mohammed and Huang, Shihong. "A survey of incorporating affective computing for human-system co-adaptation". In: *Proceedings of the 2nd World Symposium on Software Engineering*. n.d.: 72–79.

[3] Friha, Othmane et al. "Llm-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness". *IEEE Open Journal of the Communications Society* (n.d.).

[4] Haase, Jennifer and Pokutta, Sebastian. "Beyond Static Responses: Multi-Agent LLM Systems as a New Paradigm for Social Science Research". *arXiv preprint arXiv:2506.01839* (n.d.).

[5] Kamberi, Shahnaz. "A cross-case analysis of possible facial emotion extraction methods that could be used in second life-pre experimental work". *Journal of Virtual Worlds Research* 5(3) (n.d.).

[6] Naveed, Humza et al. "A comprehensive overview of large language models". *ACM Transactions on Intelligent Systems and Technology* (n.d.).

[7] Shrestha, Yash Raj and He, Vivianna Fang. "Integrating multimodal data and machine learning for entrepreneurship research". *Strategic Entrepreneurship Journal* (n.d.).

[8] Tuma, Katja, Calikli, Gül, and Scandariato, Riccardo. "Threat analysis of software systems: A systematic literature review". *Journal of Systems and Software* 144 (n.d.): 275–294.

[9] Van Buggenhout, Erik. “Purple Teaming: A comprehensive and collaborative approach to cyber security”. *Cyber Security: A Peer-Reviewed Journal* 7(3) (n.d.): 207–216.