Chatbot For Incident Response

Department of Computer Science, Cal Poly Pomona Cybersecurity and Awareness Fair 2024

Armin Erika Polanco
Jerold Manansala
Kenneth Pham
Trung Vu

Abstract

Operational technology (OT) is hardware/software that detects or causes a change through direct monitoring. OT networks comprise of devices responsible for roles from temperature control to monitoring nuclear radiation, but they are significantly more vulnerable than IT networks. Incident response teams help protect these networks from adversaries, however, one of the most common challenges incident response (IR) teams face is the sheer volume of alerts received, most of which are false positives. The time spent on false positives prevents incident handlers from better addressing real threats. Developing a method to efficiently filter false positives is critical. Our team has developed an AI-driven chatbot focused on operational technology incident response to efficiently filter false positives and enhance IR workflows. The chatbot is capable of classifying alerts as true or false positives, creating Splunk alerts to enhance detection systems, generating formatted IR reports for alerts, and answering general OT, CVE, and cybersecurity questions. The chatbot can be integrated into IR team workflows to reduce time spent analyzing alerts so IR teams across the industry can spend more time tackling real threats and reinforcing their detection systems.

Introduction

Incident response (IR) is the process organizations use to identify and respond to cyberattacks and breaches, usually involving identification, containment, eradication, recovery, and post-incident review. IR prevents adversaries from stealing critical information from organizations, however, most daily alerts are false positives which keep incident handlers from spending more time on real threats.

Problem Statement:
Filtering false positives is an industry-wide problem that, if solved, will be ground-breaking for all IR teams, especially enterprise cyber OT teams. OT devices include SCADA and ICS their lack of security has resulted in OT networks being more vulnerable than IT networks. Securing OT networks is important though as OT devices range from controlling temperatures of households to maintaining critical infrastructure.

Objective:
LLMs have changed the cybersecurity landscape, assisting IR teams in triaging alerts and enhancing responses by providing quick explanations for unknown concepts and creating frameworks for security patches. Our team attempts to develop an AI-drive chatbot that leverages Meta's Llama LLM and continuously pulls CVE information from MITRE and CISA to assist IR teams respond to OT network incidents. The chatbot will be capable of answering IR, OT, and cybersecurity questions via the pre-trained Llama model and generate updates on the latest OT-related CVEs reported by MITRE and CISA. More importantly, the chatbot will be capable of ingesting incident alerts, generating a formatted report, and classifying whether the incident is a false or true positive. Lastly, the chatbot will have the capability of helping IR teams enhance current detection systems by improving current rules on platforms like Suricata and Splunk.

Methods

Natural Language Processing (NLP):

- Used to process unstructured text data
- Needed to extract information quickly, reducing time spent on data interpretation

Machine Learning:

- Utilized to predict and categorize cyber threats based on historical data; trained on past incidents and responses

LLaMA:

- Enhances chatbot conversational capabilities for incident response and general queries
- Trained with historical and recent data for contextually relevant responses regarding IR, OT, and cybersecurity

Results

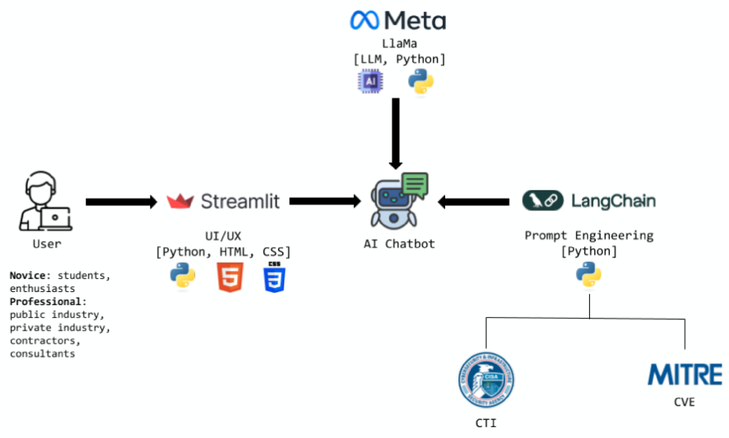

Figure 1. System Architecture of Chatbot

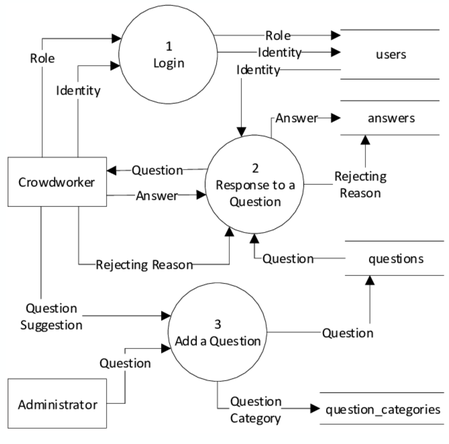

Figure 2. Data Flow Diagram of Chatbot Model (ResearchGate, 2020)

Results (Continued)

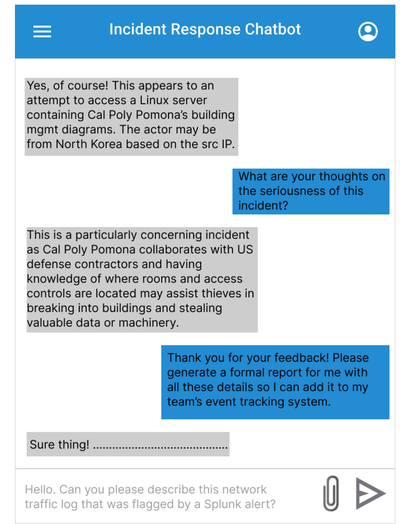

Figure 3. GUI of Chatbot

Conclusion

- Increased productivity by moving from manual to automated methods
- Provided a boost in OT cyber defense for all cyber teams
- Chatbot can
  - Answer questions about OT, IR, and cybersecurity
  - Produce daily updates on OT-related CVEs
  - Classify false positive incident alerts such as spam mail
  - Generate IR reports for OT-related incidents
  - Enhance and create new Suricata or Splunk rules to flag suspicious network activity
- Cybersecurity students triaged simulated incidents 30% faster and with a 15% lower error rate using chatbot

References

Chahal, Sunil. (2023). AI-Enhanced Cyber Incident Response and Recovery. International Journal of Science and Research (IJSR). 12. 1795-1801. 10.21275/SR231003163025.

Stouffer et al., (2023). Guide to Operational Technology (OT) security. National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/nist.sp.800-82r3

Acknowledgement

We want to thank Professor Abdelfattah Amamra for his mentorship and John Jarocki PhD from Sandia National Laboratories for providing his feedback and insight!