

Design and Implementation of a Conversational AI Chatbot for Security Insights in Cisco Cyber Vision

Auteur : Hoorelbeke, Jordi

Promoteur(s) : Geurts, Pierre

Faculté : Faculté des Sciences appliquées

Diplôme : Master en sciences informatiques, à finalité spécialisée en "computer systems security"

Année académique : 2024-2025

URI/URL : <http://hdl.handle.net/2268.2/23371>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

University of Liège
School of Engineering and Computer Science

Design and Implementation of a Conversational AI Chatbot for Security Insights in Cisco Cyber Vision

Enabling Natural Language Interaction Through Cisco Webex Integration

Author: Jordi Hoorelbeke

Supervisors:

Prof. Pierre Geurts
Emmanuel Tychon

Academic Year 2024-2025

Abstract

The concept of natural human-computer interaction has long inspired both science fiction and early AI research. Thanks to advances in conversational AI, this vision is becoming increasingly practical, enabling more accessible and intuitive ways to interact with complex systems. Building on this progress, this thesis presents a chatbot designed to interface with Cisco Cyber Vision (CCV), a security platform for Operational Technology (OT) environments.

The chatbot empowers users to retrieve security insights through natural, intuitive messages. Integrated into Cisco Webex, it offers a familiar, text-based environment for questions like “What activities occurred between devices *X* and *Y* this week?”, “Explain vulnerability *Z*,” or for receiving timely updates on the industrial network’s security posture. Its purpose is to streamline information access and reduce reliance on rigid web user interfaces.

This work’s key contributions include an integration environment assessment encompassing Cisco Webex, CCV, and the OT environment; the definition of conversational requirements for specifically tailored use cases; and the design and implementation of the chatbot’s architecture, primarily focusing on its conversational AI logic as the central contribution. To this end, we provide a detailed comparison of conventional machine learning models and modern Large Language Models (LLMs) for natural language understanding, detail how the chatbot adapts to non-standard language and typographical errors, and examine how generative AI and prompt engineering foster richer, more explanatory responses, enabling innovative use cases.

This work conclusively highlights the feasibility and benefits of augmenting CCV with a natural language interface via Webex. It also acknowledges and addresses inherent limitations introduced by specific design choices and the constraints of the Webex integration model.