Research and development of an endpoint security monitoring system (EDR) integrated with an AI assistant to support incident handling.

Dao Duy Thanh

Abstract: This topic aims to research and develop an endpoint detection and response (EDR) system with the ability to integrate an AI assistant to support handling security-related incidents. In the context of increasing cyberattack risks, the demand for automation solutions and enhanced security monitoring efficiency has become urgent. This topic applies a combined method of theoretical research and experimentation to design and deploy the EDR system, aiming to provide a robust platform for early detection and rapid handling of attacks through the integration of artificial intelligence. The expected results will expand automation capabilities in the field of network security, contributing to improving the safety level of information systems.

Keywords: Information security monitoring, EDR system, AI Assistant, Incident handling, Network security