Research and deployment of a network attack monitoring and detection system using Wazuh integrated with Snort in an enterprise network system.

Nguyen Ngoc Quy

Abstract: In the context of cybersecurity increasingly becoming a global focus, this paper aims to research and develop a network attack monitoring and detection system based on the integration of Wazuh and Snort. This project conducts an in-depth analysis of security threats in enterprise network environments and validates its effectiveness through actual deployment and experimentation. Combining theoretical research with practical application, the system can provide real-time and accurate reports of network intrusion events, thereby enhancing the overall level of network security. The expected outcomes not only offer an effective supplement to existing protection mechanisms but also make a positive contribution to the development of enterprises in the field of network information security.

Keywords: Cybersecurity, Wazuh, Snort, network attack detection, enterprise network security