Building a comprehensive security monitoring system for the network system based on the open-source Osquery combined with Kolide Fleet and ELK.

Tran Ba Quan

Abstract: This topic addresses the necessity of improving security monitoring capabilities in network systems through the development of a comprehensive solution. The main objective is to build and deploy an overall security monitoring system based on the open-source Osquery, integrated with Kolide Fleet for device management and the ELK Stack for real-time data collection, storage, and analysis. The research methodology includes both theoretical and experimental approaches, aiming to provide a flexible and effective solution. The expected outcome is to create a robust security monitoring system that enhances security and the ability to respond quickly to cyber threats.

Keywords: Security monitoring, Osquery, Kolide Fleet, ELK Stack, Network system