

Building an information security operations system (SOC) using open source.

Nguyen Tuan Anh

Abstract: This topic focuses on building a Security Operations Center (SOC) based on open-source software to meet the growing needs of enterprises in protecting their network environment. Through a combination of theoretical research and experimentation, the topic will introduce a method for designing and deploying an effective information security system. The main objective is to build a flexible, customizable, and optimized solution to support the monitoring and protection of enterprise information networks. The expected results from this topic will affirm the applicability of open-source technology in the field of information security, while providing technology organizations with a cost-effective and flexible alternative solution.

Keywords: Security Operations Center (SOC), Open Source, Network Protection, Network Control, Security Monitoring