

# **Building a mini SOC system for monitoring, detecting, and responding to cybersecurity incidents.**

**Le Huu Toan**

**Abstract:** In the current context, information security and cybersecurity management are increasingly receiving attention. This topic focuses on building a mini SOC (Security Operation Center) system to serve the purpose of monitoring, detecting, and responding promptly to cybersecurity incidents. Through theoretical research combined with experimentation, the topic aims to provide an effective solution to support organizations in enhancing their ability to protect critical information. The expected results will contribute significantly to the field of cybersecurity management and can be widely applied in various organizations.

**Keywords:** SOC mini, network security monitoring, incident detection, rapid response, information security