# IMPLEMENTASI *MINI SECURITY OPERATIONS CENTER* (SOC) BERBASIS *WAZUH-SURICATA* UNTUK DETEKSI DINI DAN ANALISIS INSIDEN KEAMANAN JARINGAN

(Studi Kasus: Laboratorium Jaringan Komputer)


Nama Mahasiswa : Mutia Zahra Anindya

NIM : 6103230039

Dosen Pembimbing : Wahyat, S.Kom., M.Kom.


## ABSTRAK


Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis belum memiliki sistem keamanan jaringan yang terpusat untuk melakukan *monitoring* dan deteksi insiden keamanan. Penelitian ini mengimplementasikan *Mini Security Operations Center* (SOC) berbasis *Wazuh* dan *Suricata* untuk *monitoring*, deteksi, dan respons terhadap ancaman keamanan jaringan. Pengujian dilakukan menggunakan skenario serangan *port scanning*, *brute force* SSH, SQL *Injection*, ICMP *Flood*, dan HTTP *Flood*, yang masing-masing dilakukan sebanyak 10 kali. Hasil pengujian menunjukkan rata-rata waktu respons sistem terhadap serangan *port scanning* sebesar 1,9 detik, *brute force* SSH 3,2 detik, SQL *Injection* 5 detik, ICMP *Flood* 1,5 detik, dan HTTP *Flood* 2,7 detik. Selain itu, Sistem berhasil mendeteksi seluruh serangan, menampilkan *log* keamanan pada *Wazuh Dashboard*, serta menjalankan respons otomatis melalui *Suricata* IPS dan *Wazuh Active Response*. Implementasi *Mini* SOC ini membantu meningkatkan *monitoring* keamanan jaringan di Laboratorium Jaringan Komputer Jurusan Teknik Informatika Politeknik Negeri Bengkalis.



**Kata kunci:** SOC, *monitoring*, deteksi intrusi, keamanan jaringan

# *IMPLEMENTATION OF A MINI SECURITY OPERATIONS CENTER (SOC) BASED ON WAZUH-SURICATA FOR EARLY DETECTION AND ANALYSIS OF NETWORK SECURITY INCIDENTS*

(*Study Case*: Laboratorium Jaringan Komputer)


| | |
|---|---|
| Student Name | : Mutia Zahra Anindya |
| Student ID | : 6103230039 |
| Supervisor | : Wahyat, S.Kom., M.Kom. |


## ABSTRACT


*The Computer Network Laboratory of the Department of Informatics Engineering at Politeknik Negeri Bengkalis does not yet have a centralized network security system for monitoring and detecting security incidents. This research implements a Mini Security Operations Center (SOC) based on Wazuh and Suricata to perform network security monitoring, threat detection, and response. The system was evaluated using five attack scenarios, namely port scanning, SSH brute force, SQL Injection, ICMP Flood, and HTTP Flood, with each scenario conducted ten times. The results showed that the average system response time was 1.9 seconds for port scanning, 3.2 seconds for SSH brute force, 5.0 seconds for SQL Injection, 1.5 seconds for ICMP Flood, and 2.7 seconds for HTTP Flood. In addition, the system successfully detected all attack scenarios, displayed security logs through the Wazuh Dashboard, and automatically responded to threats using Suricata IPS and Wazuh Active Response. The implementation of the Mini SOC helps improve network security monitoring in the Computer Network Laboratory of the Department of Informatics Engineering at Politeknik Negeri Bengkalis.*



***Keywords****: SOC, monitoring, intrusion detection, network security*