INTISARI

HYBRID INTRUSION DETECTION SYSTEM UNTUK KEAMANAN SIBER PADA JARINGAN INDUSTRI

Oleh:

Danendra Azriel Ramdhany

21/478295/PA/20739

Perkembangan teknologi jaringan komputer dan penggunaan internet telah mengubah berbagai aspek kehidupan, termasuk sektor industri. Internet memungkinkan kontrol jarak jauh dalam proses produksi, tetapi juga meningkatkan risiko keamanan siber pada *Industrial Control System* (ICS) dan *Supervisory Control and Data Acquisition* (SCADA). Penelitian ini mengkaji ancaman terhadap ICS/SCADA dan mengusulkan penggunaan *Intrusion Detection System* (IDS).

Penelitian ini mengimplementasikan *hybrid intrusion detection system* dengan menggabungkan metode *anomaly-based detection* berbasis *machine learning* algoritme *random forest* dan *signature-based detection* menggunakan Suricata. Hasil analisis dari sistem divisualisasikan dalam *dashboard* serta dilakukan tindakan saat terjadi serangan.

Hasil dari penelitian ini menunjukkan bahwa metode *hybrid* efektif dalam mendeteksi serangan dan mengatasi kekurangan masing-masing metode. Proses deteksi divisualisasikan dengan baik melalui *dashboard*, memudahkan pemantauan secara *real-time*. Selain itu, sistem berhasil memblokir alamat IP penyerang yang menunjukkan potensi implementasi untuk meningkatkan keamanan siber di sektor industri.

Kata kunci: Industri, Keamanan Siber, *Intrusion Detection System, Machine Learning, Random Forest,* Suricata.

ABSTRACT

HYBRID INTRUSION DETECTION SYSTEM FOR CYBERSECURITY IN INDUSTRIAL NETWORKS

By:

Danendra Azriel Ramdhany

21/478295/PA/20739

The advancement of computer network technology and internet usage has transformed various aspects of life, including the industrial sector. The internet enables remote control in production processes but also heightens cybersecurity risks within Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. This research examines threats to ICS/SCADA and proposes the implementation of an Intrusion Detection System (IDS).

This study implements a hybrid intrusion detection system by combining anomaly-based detection using the random forest machine learning algorithm and signature-based detection through Suricata. The analysis results from the system are visualized on a dashboard, and actions are taken when an attack occurs.

The results of this study demonstrate that the hybrid method is effective in detecting attacks and addressing the limitations of each individual method. The detection process is well-visualized through a dashboard, facilitating real-time monitoring. Furthermore, the system successfully blocks attacker IP addresses, indicating the potential for practical implementation to enhance cybersecurity within the industrial sector.

Keywords: Industry, Cybersecurity, Intrusion Detection System, Machine Learning, Random Forest, Suricata.