ABSTRAK

Nama : **Aprido Syawindra Pratama**
Program Studi : **Teknik Informatika**
Judul : **Implementasi Ibm Qradar System Information And Event Management (Siem) Dalam Mendeteksi Ancaman Keamanan Jaringan Pada Infinite Learning Indonesia.**
Dosen Pembimbing : **Husni, ST., M.Kom., MSc.**

Penerapan teknologi keamanan jaringan semestinya sudah menjadi fokus terutama pada sebuah perusahaan yang sangat rawan terjadinya sebuah serangan data melalui sebuah jaringan. Terlepas pada tahun 2023 ini ancaman jaringan sudah maraknya terjadi, khususnya pada Indonesia. Penggunaan sistem deteksi jaringan sudah semestinya di lakukan terutama pada *Infinite Learning*, bergerak pada bidang pendidikan yang fokus utamanya memberikan fasilitas *online* kepada pengguna. Terfokus penyelesaian masalah yang di hadapi untuk memantau traffic jaringan yang terjadi maka di butuhkannya sistem pemantau jaringan secara realtime guna mencegah permasalahan jaringan yang terjadi. Pada penelitian ini akan menggunakan penerapan teknologi keamanan jaringan yaitu *IBM Qradar SIEM* sebagai *platform* yang dapat mendeteksi ancaman jaringan secara *realtime* dan menanggapi ancaman tersebut pada lingkungan perusahaan khususnya *Infinite Learning*. Penelitian ini merupakan perancangan serta implementasi sistem untuk mendapatkan hasil percobaan sehingga dapat mengevaluasi sebagai hasil dan menanggapi respon ancaman yang terjadi. Dengan menggunakan bantuan teknik virtualisasi server dengan Vmware sehingga dapat mengaplikasikan metode percobaan penelitian ini dan mendapatkan hasil yang di inginkan. Dengan melibatkan *IBM Qradar SIEM* pada teknik virtualisasi dan dilakukannya pengujian serangan sehingga mendapatkan hasil serangan yang terjadi masuk dalam pendeteksian sistem dan mendapatkan visualisasi dengan jelas oleh *IBM Qradar*. Harapan dari hasil penelitian ini dapat meningkatkan strategi keamanan jaringan pada perusahaan khususnya *Infinite Learning*.

Kata Kunci : Ancaman Keamanan Jaringan, *Infinite Learning, SIEM, IBM QRadar, Vmware*.

ABSTRACT

The application of network security technology should have become a focus, especially in a company that is very prone to data attacks through a network. Regardless of the year 2023, network threats have been rampant, especially in Indonesia. The use of a network detection system should be done, especially at Infinite Learning, engaged in the field of education whose main focus is to provide online facilities to users. Focused on solving the problems faced to monitor network traffic that occurs, a realtime network monitoring system is needed to prevent network problems that occur. This research will use the application of network security technology, namely IBM Qradar SIEM as a platform that can detect network threats in real time and respond to these threats in the corporate environment, especially Infinite Learning. This research is a system design and implementation to get experimental results so that it can evaluate as a result and respond to the threat response that occurs. By using the help of server virtualization techniques with Vmware so that it can apply this research experiment method and get the desired results. By involving IBM Qradar SIEM in virtualization techniques and testing attacks so as to get the results of attacks that occur in system detection and get visualization clearly by IBM Qradar. The hope of the results of this study can improve network security strategies in companies, especially Infinite Learning.

Keywords: *Network Security Threats, Infinite Learning, SIEM, IBM QRadar, Vmware.*