ABSTRAK

Nama : Mohamad Reza Al Fatah

NIM : 41520010183

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Implementasi IBM QRadar Community Edition Sebagai Security Information and Event Management (SIEM) Untuk Deteksi Ancaman dan Serangan Siber

Pembimbing : Lukman Hakim, ST., M. Kom

Keamanan siber adalah elemen penting dalam manajemen infrastruktur teknologi informasi, terutama dengan meningkatnya frekuensi dan kompleksitas serangan siber. Penelitian ini bertujuan untuk mengaplikasikan IBM QRadar *Community Edition* sebagai platform *Security Information and Event Management* (SIEM) untuk mendeteksi ancaman dan serangan siber pada server. IBM QRadar *Community Edition* menawarkan solusi yang terintegrasi untuk mengumpulkan, menganalisis, dan mengkorelasikan data log dari berbagai sumber guna mengidentifikasi aktivitas mencurigakan dan memberikan peringatan dini. Metode penelitian ini meliputi instalasi dan konfigurasi IBM QRadar *Community Edition* pada mesin virtual, pengaturan sumber aliran data untuk mengumpulkan data dari server Linux, serta pembuatan aturan untuk mendeteksi ancaman tertentu. Pengujian dilakukan dengan mensimulasikan serangan siber untuk menilai efektivitas deteksi dan respons SIEM. Hasil penelitian menunjukkan bahwa IBM QRadar *Community Edition* dapat mendeteksi berbagai jenis serangan siber secara *real-time* dan memberikan peringatan yang dapat digunakan oleh administrator untuk mengambil tindakan mitigasi. Implementasi SIEM menggunakan IBM QRadar *Community Edition* terbukti meningkatkan visibilitas dan respons terhadap ancaman siber, serta membantu organisasi dalam mengelola keamanan jaringan dengan lebih proaktif dan efisien. Penelitian ini memberikan kontribusi yang signifikan dalam bidang keamanan siber, khususnya dalam penerapan solusi SIEM untuk mendeteksi dan merespons ancaman di lingkungan server.

Kata Kunci: Keamanan Siber, IBM QRadar *Community Edition*, *Security Information and Event Management* (SIEM), Deteksi Ancaman, Serangan Siber, Analisis Keamanan.

ABSTRACT

Nama : Mohamad Reza Al Fatah

NIM : 41520010183

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Implementasi IBM QRadar Community Edition Sebagai Security Information and Event Management (SIEM) Untuk Deteksi Ancaman dan Serangan Siber

Pembimbing : Lukman Hakim, ST., M. Kom

Cybersecurity is a crucial element in managing information technology infrastructure, especially with the increasing frequency and complexity of cyberattacks. This study aims to apply IBM QRadar Community Edition as a Security Information and Event Management (SIEM) platform to detect threats and cyberattacks on servers. IBM QRadar Community Edition offers an integrated solution to collect, analyze, and correlate log data from various sources to identify suspicious activity and provide early warnings. The research methodology includes the installation and configuration of IBM QRadar Community Edition on a virtual machine, setting up data flow sources to collect data from Linux servers, and creating rules to detect specific threats. Testing was conducted by simulating cyberattacks to evaluate the effectiveness of SIEM's detection and response capabilities. The study results show that IBM QRadar Community Edition can detect various types of cyberattacks in real-time and provide alerts that administrators can use to take mitigation actions. Implementing SIEM using IBM QRadar Community Edition has proven to enhance visibility and response to cyber threats, helping organizations manage network security more proactively and efficiently. This study makes a significant contribution to the field of cybersecurity, particularly in the application of SIEM solutions to detect and respond to threats in server environments.

Keywords: ***Cybersecurity, IBM QRadar Community Edition, Security Information and Event Management (SIEM), Threat Detection, Cyber Attacks, Security Analysis*.**