

RINGKASAN

ARIEF NURRACHMAN. Implementasi IBM QRadar SIEM *Community Edition* untuk Manajemen Keamanan Jaringan di HSPNET. *Implementation of IBM QRadar SIEM Community Edition for Network Security Management in HSPNET*. Dibimbing oleh HENDRA RAHMAWAN.

HSPNet, *Internet Service Provider* yang dikelola oleh PT. Parsaoran Global Daratrans, saat ini telah memiliki banyak pelanggan yang tersebar di Jakarta, sehingga memungkinkan banyaknya serangan yang ingin menyerang server atau jaringan yang dimiliki oleh HSPNet. Di HSPNet belum ada pemantauan jaringan secara otomatis dengan sistem SIEM. Akibat dari belum adanya skema pemantauan otomatis adalah munculnya potensi serangan yang tidak terdeteksi oleh administrator jaringan. Jaringan tersebut perlu dilakukan pemantauan jika ada serangan yang masuk ke dalam jaringan HSPNet. Pemantauan jaringan ini sangat penting dilakukan guna mengetahui jenis serangan dan *IP Address* yang digunakan oleh penyerang.

Tidak adanya pemantauan keamanan jaringan akan menyulitkan administrator jaringan untuk mengetahui masalah atau jika adanya serangan yang terjadi pada jaringan di sebuah perusahaan HSPNet. Jaringan tersebut perlu dilakukan tambahan keamanan seperti *Security Information and Event Management* (SIEM). Untuk melakukan pemantauan terhadap adanya aktivitas serangan ke server-server HSPNet dan digunakan salah satu aplikasi SIEM yaitu *IBM QRadar Security Intelligence*. *IBM QRadar Security Intelligence* membantu mendeteksi keamanan dan memprioritaskan ancaman secara akurat didalam suatu perusahaan dan memberikan wawasan yang memungkinkan administrator untuk merespon dengan cepat untuk mengurangi dampak dari sebuah serangan yang terjadi dengan menggunakan gabungan sebuah *log* dan aliran data jaringan dari berbagai perangkat yang berada di suatu jaringan. Berdasarkan hasil dari pengujian dapat disimpulkan bahwa IBM QRadar SIEM berhasil mendeteksi potensi-potensi serangan yang masuk ke HSPNet.

Kata kunci: *IBM QRadar Security Intelligence*, Keamanan Jaringan, SIEM.

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumumkannya sebagai atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.