

**PENERAPAN QRADAR *SECURITY INFORMATION*
AND *EVENT MANAGEMENT (SIEM)* UNTUK MENINGKATKAN
KETAHANAN KEAMANAN DATA TERHADAP SERANGAN *CYBER*
PADA APLIKASI KEUANGAN DIGITAL OVO**

Shely Alfiana

**Program Studi Akuntansi Fakultas Ekonomi dan Bisnis Univeristas
Muhammadiyah Metro. Kota Metro, Lampung, Indonesia**

E-mail: shely.alfiana@gmail.com

Abstrak

Penelitian ini bertujuan untuk meneliti penerapan Qradar *Security Information And Event Management (SIEM)* untuk meningkatkan ketahanan keamanan data terhadap serangan *cyber* pada aplikasi keuangan digital OVO. Penelitian ini metode yang digunakan adalah metode kualitatif deskriptif. Dengan menerapkan model Agile, proyek penerapan QRADAR dapat dilakukan secara iteratif dan inkremental. Instrument pengumpulan data yang digunakan yaitu wawancara, pengumpulan log data, dan studi pustaka. Teknik analisis data yang digunakan meliputi, pengumpulan data, normalisasi data, pengidentifikasian ancaman, korrelasi peristiwa, pengelompokan dan prioritas ancaman, investigasi dan respon, notifikasi dan pelaporan. Hasil penelitian ini menunjukkan bahwa penerapan QRadar dalam aplikasi keuangan digital secara signifikan meningkatkan ketahanan keamanan data terhadap serangan *cyber*. QRadar memungkinkan deteksi, analisis, dan respons terhadap ancaman keamanan secara *real-time*, yang memperkuat perlindungan terhadap informasi sensitif dan meningkatkan kepercayaan pengguna terhadap platform tersebut.

Kata Kunci: QRADAR *Security Information And Event Management (SIEM)* (1); Ketahanan Keamanan Data (2); Serangan *Cyber* (3); Aplikasi Keuangan Digital (4)

**IMPLEMENTATION OF QRADAR *SECURITY INFORMATION*
AND *EVENT MANAGEMENT (SIEM)* TO INCREASE DATA SECURITY
RESILIENCE AGAINST CYBER ATTACKS ON OVO DIGITAL APPLICATIONS**

Shely Alfiana

**Accounting Study Program, Faculty of Economics and Business
Muhammadiyah Metro University. Metro City, Lampung, Indonesia**

E-mail: shely.alfiana@gmail.com

Abstract

This research aims to examine the application of Qradar (SIEM) to increase data security resilience against cyber attacks on OVO digital financial applications. This research method used is a descriptive qualitative method. By applying the Agile model, the QRADAR implementation project can be carried out iteratively and incrementally. The data collection instruments used were interviews, data log collection, and literature study. Data analysis techniques used include data collection, data normalization, threat identification, event correlation, threat grouping and prioritization, investigation and response, notification and reporting. The results of this research show that the application of QRadar in digital financial applications significantly increases data security resilience against cyber attacks. QRadar enables detection, analysis and response to security threats in real-time, which strengthens the protection of sensitive information and increases user trust in the platform.

Keywords: QRADAR *Security Information And Event Management (SIEM)* (1); Data Security Resilience (2); Cyber Attacks (3); Digital Finance Applications (4)