

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

SKRIPSI



OLEH :

SHELY ALFIANA

20630040

**PROGRAM STUDY AKUNTANSI
FAKULTAS EKONOMI DAN BISNIS
UNIVERSITAS MUHAMMADIYAH METRO
2024**



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

SKRIPSI

Diajukan

Untuk Memenuhi Salah Satu Persyaratan Dalam Menyelesaikan Program
Sarjana Akuntansi (S1)

SHELY ALFIANA

20630040

**PROGRAM STUDY AKUNTANSI
FAKULTAS EKONOMI DAN BISNIS
UNIVERSITAS MUHAMMADIYAH METRO
2024**

**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.alfianaa@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, pungumpulan data, normalisasi data, pengidentifikasi ancaman, korrelasi peristiwa, pengelompokan dan prioritisas 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.alfianaa@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)

RINGKASAN

Shely Alfiana. 2024. *Penerapan Qradar Security Information And Event Management (SIEM) Untuk Meningkatkan Ketahanan Keamanan Data Terhadap Serangan Cyber Pada Aplikasi Keuangan Digital OVO*. Skripsi. Program Studi Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Metro. Pembimbing (1) Nedi Hendri, S.E. M.Si., Akt., CA., ACPA., CPA., CRA. (2) Elmira Febri Darmayanti, S.E., M.A.B.

Kata Kunci: Qradar *Security Information And Event Management (SIEM)*, Ketahanan Keamanan Data, Serangan *Cyber*, Aplikasi Keuangan Digital.

Paragraf pertama berisi tentang latar belakang masalah. Penerapan IBM Qradar *Security Information And Event Management (SIEM)* untuk meningkatkan ketahanan keamanan data terhadap serangan *cyber* pada aplikasi keuangan digital OVO. Kemudian didukung oleh kemajuan teknologi informasi yang memberi manfaat untuk meningkatkan keamanan data.

Paragraf kedua berisi tentang tujuan penelitian. Penelitian ini bertujuan untuk memberikan pemahaman yang mendalam tentang keamanan data dalam konteks aplikasi keuangan digital dan kontribusi solusi yang diusulkan dalam menghadapi berbagai risiko serangan *cyber*.

Paragraf ketiga berisi tentang metode penelitian. Metode penelitian 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, pengidentifikasi ancaman, korrelasi peristiwa, pengelompokan dan prioritas ancaman, investigasi dan respon, notifikasi dan pelaporan.

Paragraf keempat berisi tentang hasil penelitian dan kesimpulan. Berdasarkan hasil penelitian maka dapat disimpulkan 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.

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

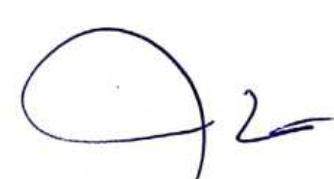
SHELY ALFIANA

20630040

Metro, 28 Maret 2024
Pembimbing I,


Nedi Hendri, S.E. M.Si., Akt., CA., ACPA., CPA., CRA.
NIDN. 0020048101

Pembimbing II,


Elmira Febri Darmayanti, S.E., M.A.B.
NIDN. 0211028002

Mengetahui,
Ketua Program Studi S1 Akuntansi


Elmira Febri Darmayanti, S.E., M.A.B
NIDN. 0211028002

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

SHELY ALFIANA

20630040

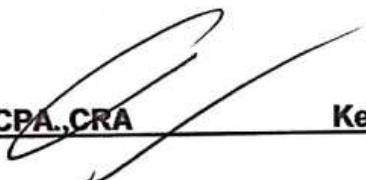
Skripsi telah diuji dan dinyatakan lulus pada

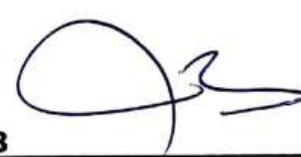
Hari : Selasa

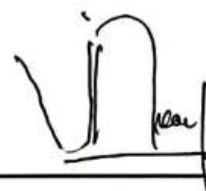
Tanggal : 02 April 2024

Tempat Ujian : Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Metro

Tim Penguji :


Nedi Hendri, S.E., M.Si., Akt., CA., ACPA., CPA., CRA Ketua
NIDN. 0219127001


Elmira Febri Darmayanti, S.E., M.A.B Sekertaris
NIDN. 0211028002


H. Jawoto Nusantoro, S.E., M.Si Penguji Utama
NIDN. 0219127001

Mengetahui,
Dekan Fakultas Ekonomi dan Bisnis



H. Siwarto, S.E., M.M
NIDN. 0210036801

MOTTO

“Kamu tidak harus menjadi hebat untuk memulai, tetapi kamu harus memulai untuk menjadi hebat.”

(Zig Ziglar)

“Usahakan yang terbaik untuk orang tuamu, orang-orang yang selalu ada untukmu dan terutama untuk dirimu sediri”

(Shely Alfiana)

PERSEMBAHAN

Dengan mengucap Syukur Alhamdulillah kepada Allah SWT yang telah memberikan kasih sayang serta rahmat-Nya dan memberikan kemudahan maupun kelancaran kepada penulis. Skripsi ini kupersembahkan sebagai ungkapan rasa syukur dan cinta kasih kepada:

1. Kepada kedua orang tua bapak Kasjo Haryanto dan ibu Sumarmi yang telah memberikan kasih sayang, senantiasa yang selalu memberikan doa tulus dan ikhlas kepada saya dan memberikan bimbingan, motivasi untuk menjadi yang terbaik.
2. Kepada diri sendiri (Shely Alfiana), karena telah mampu berusaha dengan keras tanpa mengenal waktu dan beruang sejauh ini. Mampu mengendalikan diri dari berbagai tekanan diluar keadaan dan tak pernah memutuskan menyerah sesulit apapun proses penyusunan skripsi ini dengan menyelesaikan sebaik dan semaksimal mungkin.
3. Kepada Mbaku Dwi Martinawati yang sudah memberikan semangat untuk menyelesaikan skripsi ini.
4. Sahabatku yang selalu membantu, memberikan semangat dan motivasi sehingga dalam menyelesaikan skripsi ini, Lita Anjani.
5. Kepada Dina dan Manda yang sudah saling menguatkan, memberi semangat dan berjuang bersama untuk menyelesaikan skripsi ini, dengan melalui proses yang panjang dan selalu menjunjung tinggi kalimat (kuat sampai tamat).
6. Kepada kucing-kucingku yang sudah menemani dan menjadi penghilang stres dalam proses penulisan skripsi ini.
7. Almameter tercinta Universitas Muhammadiyah Metro sebagai tempat untuk mengemban ilmu dan memberikan pengalaman sampai proses saat ini khususnya untuk Fakultas Ekonomi dan Bisnis progaram studi Akuntansi terimakasih atas ilmu yang diperoleh selama ini.

KATA PENGANTAR

Segala puji dan syukur kehadirat Allah Swt. yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi ini yang berjudul "**PENERAPAN QRADAR SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK MENINGKATKAN KETAHANAN KEAMANAN DATA TERHADAP SERANGAN CYBER PADA APLIKASI KEUANGAN DIGITAL OVO**" skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan Program Strata-1 Jurusan Akuntansi, Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Metro.

Penulis merasa bahwa dalam penyusunan skripsi ini masih menemui beberapa kesulitan dan hambatan. Namun dengan selesainya penulisan skripsi ini diperlukan ketekunan, kesabaran dan kerja keras serta tidak terlepas dari bantuan berbagai pihak, maka pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Dr. H. Nyoto Suseno, M.Si. selaku Rektor Universitas Muhammadiyah Metro.
2. Bapak H. Suwarto, S.E., M.M. selaku Dekan Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Metro.
3. Bapak H. Jawoto Nusantoro, S.E., M.Si. selaku Ketua Program Studi Akuntansi Fakultas Ekonomi Universitas Muhammadiyah Metro dan selaku dosen pembimbing 2 dalam penyusunan penulisan skripsi.
4. Bapak Nedi Hendri, S.E., M.Si., Akt., CA., ACPA., CRA. selaku dosen pembimbing 1 yang telah memberi arahan dalam penyusunan penulisan skripsi.
5. Ibu Elmira Febri Darmayanti, S.E., M.A.B. selaku dosen pembimbing 2 yang telah memberi arahan dalam penyusunan penulisan skripsi.
6. Bapak dan Ibu Dosen Fakultas Ekonomi dan Bisnis Universitas Muhammadiyah Metro yang telah memberikan ilmu yang bermanfaat bagi penulis.
7. Bapak dan ibuku tercinta yang selalu memberi semangat dalam penyusunan penulisan skripsi selama ini.
8. Semua pihak yang telah membantu, baik secara langsung maupun tidak langsung, serta pihak-pihak lain yang tidak bisa penulis sebutkan satu persatu.

Akhir kata, semoga ALLAH SWT senantiasa melimpahkan karunianya dan membalas segala amal budi serta kebaikan pihak-pihak yang telah membantu penulis dalam penyusunan skripsi ini. Semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Metro, 13 Desember 2023

Penulis



Shely Alfiana

NPM. 20630040

PERNYATAAN TIDAK PLAGIAT

Yang bertanda tangan dibawah ini:

Nama : Shely Alfiana
NPM : 20630040
Fakultas : Ekonomi dan Bisnis
Program Studi : Akuntansi

Menyatakan bahwa skripsi yang berjudul "**PENERAPAN QRADAR SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK MENINGKATKAN KETAHANAN KEAMANAN DATA TERHADAP SERANGAN CYBER PADA APLIKASI KEUANGAN DIGITAL OVO**" merupakan karya saya dan bukan hasil plagiat. Apalagi dikemudian hari terdapat unsur plagiat dalam skripsi tersebut, maka saya bersedia menerima sanksi. Demikian surat pernyataan ini dibuat dengan sesungguhnya.

Metro, 27 Maret 2024

Yang membuat pernyataan,



NPM.20630040



UNIT PUBLIKASI ILMIAH
UNIVERSITAS MUHAMMADIYAH
METRO



SURAT KETERANGAN UJI KESAMAAN (SIMILARITY CHECK)

Nomor: 153/II.3.AU/F/UPI-UK/2024

Unit Publikasi Ilmiah Universitas Muhammadiyah Metro dengan ini menerangkan bahwa:

Nama : SHELY ALFIANA
Npm : 20630040
Jenis Dokumen : SKRIPSI

Judul:

ANALISIS PENERAPAN IBM QRADAR (SIEM) UNTUK MENINGKATKAN KETAHANAN KEAMANAN DATA TERHADAP SERANGAN CYBER PADA APLIKASI KEUANGAN DIGITAL OVO

Telah dilakukan validasi berupa Uji Kesamaan (*Similarity Check*) dengan menggunakan aplikasi *Tumitin*. Dokumen telah diperiksa dan dinyatakan telah memenuhi syarat bebas uji kesamaan (*similarity check*) dengan persentase $\leq 20\%$. Hasil pemeriksaan uji kesamaan terlampir.

Demikian kami sampaikan untuk digunakan sebagaimana mestinya.



Alamat

Jl. Ki Hajar Dewantara No.116
Iringmulyo, Kec. Metro Timur Kota Metro,
Lampung, Indonesia

Website: upi.ummetro.ac.id
E-mail: help.upi@ummetro.ac.id

DAFTAR ISI

HALAMAN SAMPUL.....	i
LEMBAR LOGO.....	ii
HALAMAN JUDUL.....	iii
ABSTRAK.....	iv
RINGKASAN.....	vi
HALAMAN PERSETUJUAN	vii
HALAMAN PENGESAHAN.....	viii
MOTTO	ix
HALAMAN PERSEMAHAN.....	x
KATA PENGANTAR	xi
PERNYATAAN TIDAK PLAGIAT.....	xiii
SURAT KETERANGAN UJI KESAMAAN (SIMILARITY CHECK).....	xiv
DAFTAR ISI	xv
DAFTAR TABEL	xvii
DAFTAR GAMBAR.....	xviii
DAFTAR LAMPIRAN	xix
BAB 1 PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	5
C. Tujuan Pengembangan Produk.....	6
D. Kegunaan Pengembangan Produk	6
E. Spesifikasi Pengembangan Produk.....	7
F. Urgensi Pengembangan Produk.....	7
G. Keterbatasan Pengembangan Produk	7
BAB II KAJIAN LITERATUR.....	8
A. Landasan Teori	8
1. Teori Keamanan Jaringan.....	8
2. Teori Keamanan Data.....	8
3. Pengertian Serangan Cyber	9

4. <i>Security Information and Event Management (SIEM)</i>	10
5. IBM Qradar.....	12
6. <i>Financial Technology (E-wallet OVO)</i>	13
B. Hasil Penelitian Relevan.....	14
C. Kerangka Pemikiran.....	19
BAB III METODE PENGEMBANGAN.....	22
A. Medel Pengembangan	22
B. Prosedur Penelitian	23
C. Instrument Pengumpulan Data.....	29
D. Teknik Analisis Data.....	28
BAB IV HASIL DAN PEMBAHASAN.....	30
A. Gambaran Umum.....	32
B. Penyajian Hasil Pengembangan.....	34
C. Pembahasan Hasil	37
BAB V PENUTUP	40
A. Simpulan	40
B. Saran	40
DAFTAR PUSTAKA.....	42
DAFTAR LAMPIRAN	44

DAFTAR TABEL

Tabel 1. Jumlah Serangan Cyber di Indonesia	3
Tabel 2. Hasil Penelitian Relevan	16
Tabel 3. Pedoman Wawancara Mengenai Keamanan Informasi Data dan Implementasi IBM Qradar (SIEM).....	30
Tabel 4. Penyajian Hasil Pengembangan Penerapan IBM Qradar (SIEM) Untuk Meningkatkan Ketahanan Keamanan Data Terhadap Serangan Cyber	34

DAFTAR GAMBAR

Gambar 1. Kerangka Pemikiran.....	21
Gambar 2. Dasbor Potensi Ancaman.....	23
Gambar 3. Halaman Deskripsi Pelanggaran	24
Gambar 4. Perhitungan Prioritas Pelanggaran.....	25
Gambar 5. Tampilan Mencari Dan Memfilter Peristiwa	26
Gambar 6. Tampilan Mendeteksi Suatu Peristiwa.....	26
Gambar 7. Tampilan UBA (<i>User Behavior Analytics</i>).....	27
Gambar 8. Tampilan Penyelidikan <i>Cyber</i>	28
Gambar 9. Halaman Status Penggunaan.....	28
Gambar 10. Ilustrasi Serangan <i>Cyber</i>	29

DAFTAR LAMPIRAN

Lampiran

1. Prosedur Penerapan Qradar (SIEM)
2. Daftar Pertanyaan Wawancara
3. Daftar Wawancara
4. Pengajuan Judul
5. Surat Keputusan Pembimbing
6. Surat Keputusan Ujian Skripsi
7. Lembar Bimbingan
8. Rekap Hasil Nilai Ujian Skripsi
9. Berita Acara Ujian Skripsi
10. Nilai Ujian Skripsi