BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan teknologi informasi, khususnya dalam bidang aplikasi keuangan digital, telah mengubah cara layanan keuangan diakses dan digunakan secara signifikan. Saat ini, aplikasi keuangan digital menjadi landasan penting dalam menyediakan kemudahan akses, mempercepat proses transaksi, serta meningkatkan pengalaman pengguna dalam hal keuangan (Soesanto et al., 2023).

Aplikasi keuangan digital, seperti OVO telah menjadi bagian penting dari kehidupan. Transaksi keuangan yang cepat dan efisien melalui platform digital menunjukkan tren peningkatan ketergantungan. OVO, sebagai penyedia layanan keuangan digital, dihadapkan pada tantangan keamanan data yang signifikan. Informasi sensitif seperti data transaksi, detail akun dan informasi pribadi pengguna perlu dilindungi dengan sangat ketat. Oleh karena itu, perlu adanya langkah-langkah proaktif untuk meningkatkan ketahanan sistem terhadap potensi ancaman.

OVO adalah produk *e-money* yang dikeluarkan oleh PT. Visionet Data Internasional. VisioNet atau PT. Visionet Data Internasional adalah anak perusahaan PT. Multipolar Tbk yang didirikan pada tahun 2006. OVO merupakan platform pembayaran digital dan layanan finansial di Indonesia. OVO mengakses berbagai persepsi kemudahan yang ditawarkan dalam bentuk aplikasi, seperti pembayaran, transfer, beli ulang, dan tarik dana. Untuk dapat mengeluarkan produk layanan *e-money* PT. Visionet Data Internasional sebagai penyedia layanan OVO harus memiliki lisensi penyelenggara *e-money* untuk Bank dan Lembaga Selain Bank (LSB) dari Bank Indonesia. Bank Indonesia selaku lembaga yang memiliki hak untuk mengeluarkan Perizinan Penyelenggara dan Pendukung Jasa Sistem Pembayaran per 31 Agustus 2017 telah memberikan lisensi kepada perusahaan penyedia produk *e-money*.

Namun, berdasarkan data dan penelitian terdahulu diketahui bahwa terdapat beberapa masalah yang membuat konsumen berpikir ulang terkait Keputusan. OVO merupakan salah satu aplikasi keuangan digital yang paling populer dan luas digunakan di masyarakat, mencakup berbagai transaksi

keuangan dan data sensitif pengguna. Keberadaannya sebagai subjek penelitian memberikan keuntungan signifikan karena mencerminkan relevansi dengan tren industri keuangan digital saat ini. Selain itu, aplikasi OVO juga rentan terhadap berbagai bentuk serangan *cyber* yang dapat merugikan tidak hanya pengguna individual tetapi juga stabilitas sistem keuangan secara keseluruhan. Penggunaan OVO, salah satunya yang tertinggi ialah perasaan khawatir karena isu keamanan data OVO yang cenderung rentan (Iliyin & Widiartanto, 2020).

Dengan pertumbuhan digitalisasi keuangan muncul risiko keamanan yang signifikan, terutama terkait dengan serangan *cyber* yang dapat merugikan integritas dan kerahasiaan data pengguna. Aplikasi keuangan digital menyimpan banyak data yang tidak terhingga jumlahnya, menyimpan informasi pribadi, finansial dan transaksional dari jutaan pengguna. Data tersebut menjadi target yang sangat menguntungkan bagi para pelaku serangan *cyber* yang terus meningkatkan kecanggihan teknik mereka.

Di masa lalu, keamanan *cyber* sangat bergantung pada teknik berbasis tanda tangan untuk mendeteksi ancaman. Teknik-teknik ini secara efektif memerangi ancaman yang diketahui dengan mengidentifikasi pola berulang atau 'tanda tangan' yang terkait dengan kategori serangan *cyber* tertentu (Kumar et al., 2023).

Sedangkan, dalam beberapa tahun terakhir serangan *cyber* terus meningkat baik dari segi frekuensi maupun kompleksitasnya. Pelaku serangan semakin canggih dalam menggunakan teknik-teknik baru untuk mengakses dan mengeksploitasi data sensitif. Aplikasi keuangan digital, seperti OVO menjadi target yang menarik bagi para pelaku serangan *cyber* karena mengandung informasi finansial yang berharga.

Menurut Babys (2021) Negara yang paling rentan terhadap perang *cyber* adalah negara pengguna jasa internet, dan Indonesia termasuk dalam daftar negara paling rentan terhadap serangan *cyber* tersebut bahkan menjadi target utama para hacker karena Indonesia masuk dalam daftar Negara pengguna internet terbesar di dunia (dengan jumlah pengguna internet mencapai 82 juta orang) dan Indonesia sebagai negara yang lemah dalam manajemen keamanan *cyber*.

Berikut merupakan data Jumlah Serangan Cyber di Indonesia (2018-2023) :

Tabel 1. Jumlah Serangan Cyber di Indonesia (2018-2023)

No.	Tahun	Serangan *Cyber*
1.	2019	290.381.283
2.	2020	316.167.753
3.	2021	266.741.784
4.	2022	370.022.283
5.	Januari - September 2023	305.000.000

Sumber: Badan *Cyber* dan Sandi Negara (BSSN)

Dari data diatas menunjukan bahwa pada tahun 2019 terjadi serangan *cyber* sebanyak 290.381.283 kasus. Pada tahun 2020 mengalami peningkatan sebanyak 25.786.470 kasus. Pada tahun 2021 mengalami penurunan dari tahun sebelumnya sebanyak 49.425.969 kasus dan pada tahun 2022 mengalami peningkatan secara signifikan sebanyak 103.280.499 kasus. Kemudian dari data terakhir yang didapat pada bulan januari-september 2023 terjadi serangan *cyber* sebanyak 305.000.000 kasus. Dari data tersebut menunjukan Indonesia masih rentan terhadap serangan *cyber*.

Analisis dari data tersebut menunjukkan bahwa langkah-langkah pengamanan yang diambil oleh sistem di Indonesia masih belum mencukupi untuk melawan serangan *cyber*. Masih ada kekurangan dalam infrastruktur dan strategi keamanan yang mengakibatkan tingginya tingkat kerentanan terhadap serangan tersebut. Tingginya jumlah kasus pencurian data yang dilakukan oleh para *hacker* menunjukkan bahwa data sensitif masih belum sepenuhnya terlindungi. Diperlukan tindakan lebih lanjut untuk memperkuat kemampuan pertahanan keamanan data di Indonesia. Tindakan ini melibatkan peningkatan infrastruktur keamanan dan peningkatan kesadaran keamanan *cyber* di seluruh lapisan masyarakat. Hal ini perlu dilakukan guna mengatasi kerentanan yang masih tinggi terhadap serangan *cyber* dan untuk melindungi data sensitif dari upaya pencurian oleh para *hacker*.

Berdasarkan berbagai kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah *cyber security*nya. Hal ini dapat diketahui dari maraknya berbagai kejadian, salah satunya adalah peretasan terhadap data kartu debit nasabah sebuah bank karena *hacker* berusaha menyusup ke sistem pengamanan kartu nasabah bank (Ardiyanti, 2014).

Kasus *cyber* yang sering terjadi pada aplikasi keuangan digital di Indonesia yaitu pengguna terpengaruh oleh serangan *phishing* dan secara tidak sengaja memberikan informasi *login* atau rahasia kepada pihak yang tidak sah, hal ini dapat menyebabkan akses lain masuk ke akun mereka. Kemudian, pengguna yang memakai kata sandi yang lemah atau tidak menjaga keamanan perangkat mereka juga dapat menjadi risiko bagi keamanan sistem.

Menurut Bagus Artiadi Soewardi, M.,Si, dalam Babys (2021) Indonesia pernah mengalami serangan *cyber* berupa *worm stuxnet*, dengan pelaku di duga oleh Amerika Serikat dan Israel akibat sikap Indonesia dalam kasus nuklir Iran. Tidak hanya itu, Indonesia juga pernah mengalami perang cyber dengan Malaysia. *Cybercrime* merujuk pada tindakan yang melanggar hukum yang dilakukan melalui jaringan komputer dengan tujuan memperoleh keuntungan dari kerugian pihak lain, dengan menggunakan komputer sebagai sarana. Di Indonesia, kesadaran dan pemahaman masyarakat terhadap ancaman serangan *cyber* yang melibatkan kecerdasan buatan (AI) terhadap keamanan data mereka masih kurang. (Anastasya Zalsabilla Hermawan et al., 2023).

Dalam menghadapi serangan *cyber* yang semakin kompleks, solusi seperti Qradar *Security Information And Event Management* (SIEM) menawarkan pendekatan yang efektifdan dapat memberikan visibilitas yang lebih baik terhadap aktivitas keamanan di dalam jaringan, mendeteksi potensi ancaman, dan memberikan respons cepat terhadap insiden keamanan.

Salah satu cara untuk meningkatkan keamanan siber adalah dengan menganalisis peralatan TI dengan memantau log yang dihasilkan dari peralatan tersebut. Menganalisis log yang dihasilkan dari setiap peralatan membutuhkan waktu lama dan sulit. Pengelolaan sistem keamanan siber yang tidak berjalan dengan baik akan menyebabkan kegagalan sistem keamanan siber. Oleh karena itu, diperlukan mekanisme pertahanan untuk mengelola log yang disebut *Security Information and Event Management* (SIEM) (Anama et al., 2023).

Menurut González, granadillo et al.,(2021) secara umum, SIEM memiliki kapasitas untuk mengumpulkan, menyimpan dan menghubungkan peristiwa yang dihasilkan oleh sistem yang dikelola. IBM QRadar merupakan salah satu platform SIEM yang canggih dan terpercaya yang dirancang untuk

mendeteksi, melacak dan menanggapi ancaman keamanan secara efisien. Penggunaan QRadar sebagai bagian dari strategi keamanan dapat memberikan keuntungan signifikan dalam memperkuat ketahanan terhadap serangan *cyber* pada aplikasi keuangan digital. Dengan mempertimbangkan kompleksitas dan tingginya nilai data dalam aplikasi keuangan digital OVO, penerapan Qradar *Security Information And Event Management* (SIEM) diharapkan dapat memberikan manfaat signifikan. Integrasi solusi keamanan ini diharapkan dapat meningkatkan kesiapan dan respons terhadap serangan *cyber*, menjadikannya langkah proaktif untuk menjaga keamanan data pengguna OVO.

Penelitian ini dilatarbelakangi oleh berbagai faktor penting. Pertama, keamanan data menjadi aspek penting mengingat OVO menyimpan dan memproses informasi keuangan serta data pribadi pelanggan dalam skala besar. Kedua, ancaman *cyber* semakin kompleks dan canggih, mendorong perlunya solusi keamanan yang dapat memberikan respons cepat terhadap serangan tersebut. Selain itu, kekhawatiran terhadap ketidakpastian keamanan aplikasi keuangan digital dan kepatuhan terhadap regulasi yang ketat juga dapat menjadi motivasi bagi penelitian ini. Perkembangan teknologi SIEM, seperti IBM Qradar yang semakin efektif dalam mendeteksi ancaman *cyber*, juga menjadi pemicu penelitian ini. Selain itu, pengalaman serangan *cyber* sebelumnya, menjadi dorongan untuk mengambil tindakan lebih lanjut guna mencegah kejadian serupa di masa depan.

Dengan demikian, peneliti tertarik untuk melakukan penelitian lebih lanjut terkait kemampuan IBM Qradar *Security Information And Event Management* (SIEM) sebagai pedeteksi, pelacak dan menanggapi ancaman keamanan data secara efisien dan diharapkan dari penelitian ini dapat memberikan pemahaman yang mendalam tentang keamanan data dalam konteks aplikasi keuangan digital dan solusi yang diusulkan, seperti penerapan QRADAR *Security Information and Event Management* (SIEM), diharapkan dapat memberikan kontribusi signifikan untuk menghadapi berbagai risiko serangan *cyber*.

Berdasarkan latar belakang yang telah diuraikan diatas, maka peneliti tertarik untuk melakukan penelitian ilmiah dalam bentuk skripsi dengan judul **“PENERAPAN QRADAR *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) UNTUK MENINGKATKAN KETAHANAN**

KEAMANAN DATA TERHADAP SERANGAN *CYBER* PADA APLIKASI KEUANGAN DIGITAL OVO"

B. Rumusan Masalah

Berdasarkan identifikasi masalah diatas, maka diperoleh rumusan masalah dalam penelitian ini adalah:

1. Bagaimana meningkatkan ketahanan keamanan data pada aplikasi keuangan digital melalui penerapan Qradar *Security Information And Event Management* (SIEM)?
2. Apa saja risiko dan tantangan yang dihadapi oleh aplikasi keuangan digital terkait dengan serangan *cyber*?
3. Bagaimana dampak penerapan QRadar terhadap mitigasi risiko dan peningkatan keamanan data pada aplikasi keuangan digital?
4. Bagaimana implementasi Qradar *Security Information And Event Management* (SIEM) pada Aplikasi Keuangan Digital?

C. Tujuan Pengembangan Produk

Tujuan dari pengembangan produk ini adalah meningkatkan ketahanan keamanan data pada aplikasi keuangan digital OVO melalui penerapan Qradar *Security Information And Event Management* (SIEM). Dengan demikian, tujuan khususnya meliputi:

1. Meningkatkan deteksi dini terhadap potensi serangan cyber.
2. Memperkuat respons terhadap serangan *cyber* untuk mengurangi dampak yang mungkin terjadi.
3. Merancang solusi yang dapat secara efektif menggunakan QRadar untuk mengurangi risiko keamanan dan meningkatkan keamanan data pada aplikasi keuangan digital.
4. Mengetahui implementasi Qradar *Security Information And Event Management* (SIEM) pada Aplikasi Keuangan Digital.

D. Kegunaan Pengembangan Produk

Penerapan QRadar *Security Information And Event Management* (SIEM) diharapkan dapat memberikan manfaat sebagai berikut:

1. Meningkatkan Keamanan Data:

   Pengembangan produk, seperti penerapan QRadar *Security Information And Event Management* (SIEM) dapat meningkatkan keamanan data

pada aplikasi keuangan digital seperti OVO. Ini mencakup deteksi dini, analisis perilaku abnormal, dan manajemen insiden yang dapat memberikan lapisan pertahanan tambahan terhadap serangan *cyber*.

2. Peningkatan Ketahanan Terhadap Serangan *Cyber*:
   Melalui pengembangan teknologi keamanan, terutama dengan memanfaatkan platform SIEM seperti IBM QRadar, aplikasi keuangan digital dapat meningkatkan ketahanannya terhadap serangan *cyber*. Hal ini termasuk kemampuan untuk mengumpulkan, menyimpan, dan menghubungkan peristiwa yang dihasilkan oleh sistem, serta memberikan respons yang efisien terhadap ancaman.
3. Meningkatkan Kepercayaan Pengguna dan Mitra Bisnis:
   Keamanan data yang ditingkatkan dapat membantu mempertahankan reputasi bisnis dan meningkatkan kepercayaan pelanggan serta mitra bisnis. Dengan memberikan perlindungan yang baik terhadap informasi sensitif, seperti data keuangan dan informasi pribadi, aplikasi keuangan digital seperti OVO dapat memperoleh dukungan yang lebih kuat dari pengguna dan mitra bisnis.

E. Spesifikasi Pengembangan Produk

Spesifikasi pengembangan produk melibatkan detail teknis terkait implementasi QRadar *Security Information And Event Management* (SIEM) pada infrastruktur OVO, termasuk integrasi, konfigurasi, dan pemeliharaan.

F. Urgensi Pengembangan Produk

Pengembangan ini mendesak mengingat tingginya ancaman serangan *cyber* pada aplikasi keuangan digital dan urgensi perlindungan data pengguna. Keamanan yang ditingkatkan akan memperkuat kepercayaan pengguna terhadap layanan OVO.

G. Keterbatasan Pengembangan Produk

Pada pengembangan ini, beberapa keterbatasan yang dihadapi meliputi keterbatasan anggaran, sumber daya manusia, dan waktu yang diberikan untuk mengerjakan implementasi penerapan Qradar *Security Information And Event Management* (SIEM) dilakukan hanya dalam waktu 2 minggu. Keterbatasan-keterbatasan ini perlu dipertimbangkan untuk memastikan keberhasilan implementasi yang lebih maksimal.