BAB V

PENUTUP

A. Simpulan

Berdasarkan pada hasil penelitian diatas, bisa disimpulkan antara lain:

1. Penelitian 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.
2. Aplikasi keuangan digital menghadapi berbagai risiko serius terkait serangan *cyber*, termasuk pencurian data pengguna, penipuan keuangan, gangguan layanan, *malware*, dan *phishing*. Penting bagi perusahaan untuk mengimplementasikan strategi keamanan yang kuat untuk melindungi data dan mematuhi regulasi keamanan data serta privasi pengguna.
3. Penerapan QRadar memiliki dampak positif terhadap mitigasi risiko dan peningkatan keamanan data pada aplikasi keuangan digital. Visibilitas yang lebih baik terhadap aktivitas dan ancaman keamanan memungkinkan tim keamanan untuk mendeteksi dan menanggapi serangan dengan lebih efisien. Integrasi dengan perangkat lunak keamanan lainnya juga meningkatkan lapisan perlindungan aplikasi keuangan.
4. Implementasi QRADAR pada aplikasi keuangan digital OVO menjanjikan solusi keamanan yang komprehensif dan adaptif. Dengan fitur-fitur seperti pemantauan pelanggaran, analisis peristiwa, identifikasi ancaman, dan respons terhadap serangan, produk ini memiliki potensi untuk meningkatkan ketahanan keamanan data OVO secara signifikan. Alamat keberadaan produk yang mencakup pusat keamanan operasional, pilihan infrastruktur, dan integrasi dengan infrastruktur OVO menunjukkan komitmen untuk mendukung efektivitas produk secara keseluruhan.

B. Saran

Berdasarkan hasil penelitian, sejumlah saran dapat diajukan untuk mengoptimalkan implementasi QRADAR SIEM *(Security Information And Event Management)* pada aplikasi keuangan digital OVO:

1. Perlu dilakukan pengembangan lebih lanjut pada model Agile dengan mengeksplorasi elemen tambahan yang dapat meningkatkan fleksibilitas dan responsivitas terhadap perubahan kebutuhan keamanan. Pemantauan pelanggaran dapat ditingkatkan melalui integrasi dengan teknologi dan alat pemantauan terkini, bahkan dengan pertimbangan penerapan kecerdasan buatan atau machine learning.
2. Proses respons terhadap serangan juga perlu dievaluasi dan diperbarui secara berkala, termasuk penyelidikan penerapan respons otomatis lebih lanjut. Optimalisasi penggunaan data log, peningkatan kapabilitas analisis data dengan memanfaatkan teknologi analitika canggih, dan kerjasama dengan pihak eksternal, seperti penyedia layanan keamanan cyber, juga perlu dipertimbangkan. Pelatihan dan kesadaran keamanan pengguna secara teratur dapat meningkatkan lapisan pertahanan tambahan.
3. Evaluasi ulang berkala terhadap kebutuhan keamanan akan memastikan keselarasan dengan perkembangan teknologi dan perubahan dalam ancaman *cyber*. Semua saran ini diharapkan dapat memberikan panduan untuk pengembangan selanjutnya dan memastikan keberlanjutan serta peningkatan dalam upaya penguatan keamanan data pada aplikasi keuangan digital OVO.
4. Untuk meningkatkan efektivitas implementasi produk ini, disarankanuntuk memberikan perhatian khusus pada pelatihan dan pendidikanpersonel di pusat keamanan operasional (SOC), sehingga mereka dapat memanfaatkan fitur-fitur produk secara optimal. Selain itu memperbarui secara berkala database ancaman dan melakukan evaluasi rutin terhadap keamanan infrastruktur. Kolaborasi dengan tim pengembangan OVO juga diperlukan untuk integrasi yang lebih baik. Dengan langkah-langkah ini, diharapkan produk dapat lebih efisien dalam melindungi data keuangan digital OVO dari ancaman keamanan.