BAB III

METODE PENGEMBANGAN

A. Model Pengembangan

Pada penelitian ini metode yang digunakan adalah metode kualitatif deskriptif. Menurut (Hanyfah et al., 2022) dalam (Djam'an Satori, 2011: 23) metode penelitian yang berdasarkan pada pengolahan data yang sifatnya deskriptif Penelitian kualitatif deskriptif dilakukan untuk menjelaskan penelitian yang ada tanpa memberikan manipulasi data variable yang diteliti dengan cara melakukan wawancara langsung (Bahri, 2017: 73).

Dalam rangka penerapan QRADAR SIEM untuk meningkatkan ketahanan keamanan data terhadap serangan *cyber* pada aplikasi keuangan digital OVO, model pengembangan Agile dipilih sebagai pendekatan utama dalam pengembangan skripsi ini. Keputusan ini didasarkan pada kebutuhan akan fleksibilitas dan adaptabilitas dalam menghadapi dinamika yang mungkin muncul selama pengembangan sistem keamanan data. Agile memberikan kerangka kerja yang sesuai dengan sifat proyek yang terus berkembang dan dapat memberikan solusi yang responsif terhadap perubahan kebutuhan keamanan yang mungkin timbul seiring waktu.

Dengan menerapkan model Agile, proyek penerapan QRADAR dapat dilakukan secara iteratif dan inkremental. Hal ini memungkinkan tim pengembang untuk secara teratur menghasilkan produk yang dapat diuji dan diimplementasikan, sehingga memfasilitasi evaluasi berkelanjutan terhadap tingkat ketaatan terhadap keamanan data. Pendekatan ini juga memungkinkan tim untuk berkolaborasi secara erat dengan pemangku kepentingan dan pengguna, memastikan bahwa prioritas berbasis nilai bisnis diberikan perhatian tinggi dalam setiap tahap pengembangan.

Selain itu, model Agile memberikan ruang bagi pengujian yang berkelanjutan sepanjang siklus pengembangan. Pengujian terus-menerus ini memastikan bahwa solusi keamanan yang diimplementasikan tidak hanya efektif secara teoritis tetapi juga dapat mempertahankan tingkat keamanan yang tinggi dalam menghadapi berbagai skenario serangan *cyber* yang mungkin terjadi. Melalui retrospektif dan pembelajaran berkelanjutan yang terintegrasi dalam model Agile, tim dapat secara efisien memperbaiki dan meningkatkan proses pengembangan sepanjang waktu, menciptakan

lingkungan yang adaptif dan responsif terhadap perkembangan ancaman keamanan data. Dengan demikian, penggunaan model Agile bukan hanya sebagai alat pengembangan, tetapi juga sebagai strategi integral untuk mencapai tujuan penguatan keamanan data yang dijelaskan dalam penelitian ini.

B. Instrument Pengumpulan Data

Instrument pengumpulan data adalah alat atau metode yang digunakan peneliti untuk mengumpulkan informasi yang relevan dan diperlukan dalam rangka menjawab pertanyaan penelitian dan mencapai tujuan penelitian. Instrument pengumpulan data menjadi bagian penting untuk mendukung penelitian yang berfokus pada penerapan Qradar SIEM untuk meningkatkan ketahanan keamanan data terhadap serangan cyber pada aplikasi keuangan digital OVO. Berikut adalah penjelasan mengenai instrument pengumpulan data yang dapat digunakan dalam skripsi ini:

1. Wawancara: Melibatkan pihak terkait seperti sesorang yang paham mengenai keamanan informasi dan administrator keamanan data untuk mendapatkan wawasan mendalam tentang kebutuhan keamanan data dan implementasi Qradar SIEM. Maka, disusun kisi-kisi pedoman wawancara sebagai berikut:

   Tabel 3. Pedoman Wawancara Mengenai Keamanan Informasi Data dan Implementasi Qradar SIEM

	Fokus/Sub Fokus yang Ditanyakan	Petikan Wawancara
1	Meningkatkan ketahanan keamanan data pada aplikasi keuangan digital melalui penerapan IBM QRadar (SIEM).	Wawancara
2	Risiko dan tantangan yang dihadapi oleh aplikasi keuangan digital terkait dengan serangan cyber.	Wawancara
3	Dampak penerapan IBM Qradar terhadap mitigasi risiko dan peningkatan keamanan data pada aplikasi keuangan digital.	Wawancara
4.	Implementasi Qradar (SEM) pada Aplikasi Keaunagn Digital.	Wawancara

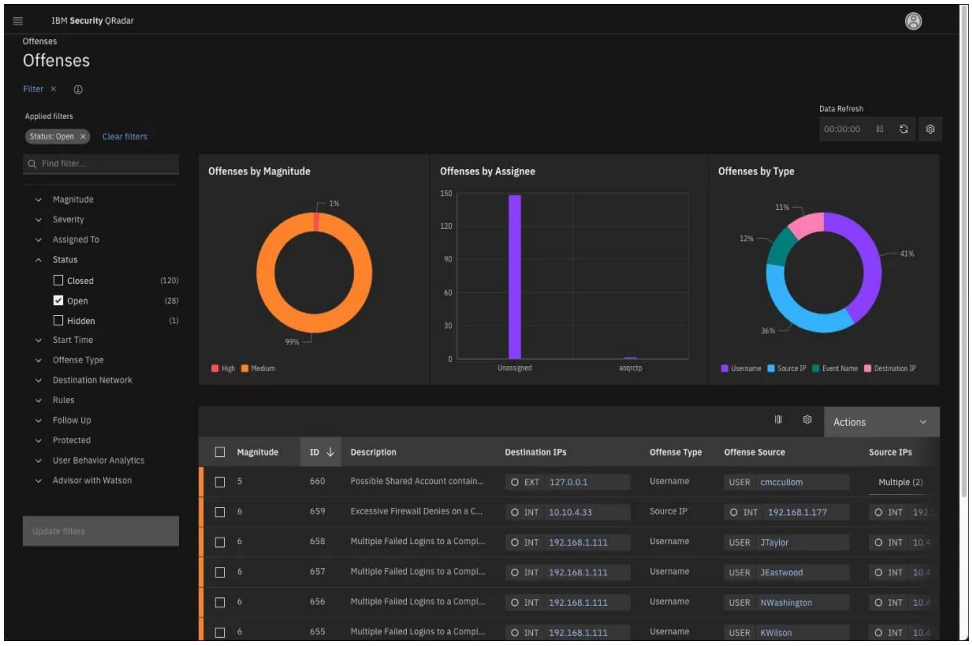
2. Pengumpulan Log Data: Mencakup pengumpulan data log dari sistem yang diintegrasikan dengan IBM QRadar. Data log dapat memberikan informasi penting tentang aktivitas keamanan, deteksi ancaman, dan respons terhadap serangan.
3. Studi Pustaka: Melibatkan analisis literatur tentang keamanan data, serangan cyber, dan implementasi SIEM *(Security Information and Event Management)* untuk mendukung landasan teoritis dan konseptual penelitian.

C. Prosedur Penelitian

Langkah-Langkah Penelitian menggunakan metode eksperimental, dengan menguji efektivitas penerapan Qradar *Security Information And Event Management* (SIEM).

1. Memantau Dasbor Untuk Potensi Ancaman

   Cara tercepat dan termudah untuk memulai adalah dengan berfokus pada ancaman yang paling penting menggunakan tab Pelanggaran:



Gambar 2. Dasbor Potensi Ancaman

Cara tercepat dan termudah untuk memulai adalah dengan berfokus pada ancaman yang paling penting menggunakan tab Pelanggaran:

Dasbor ikhtisar di atas menunjukkan statistik penting tentang peringatan terkini di lingkungan TI perusahaan ini, yang disebut “pelanggaran” di

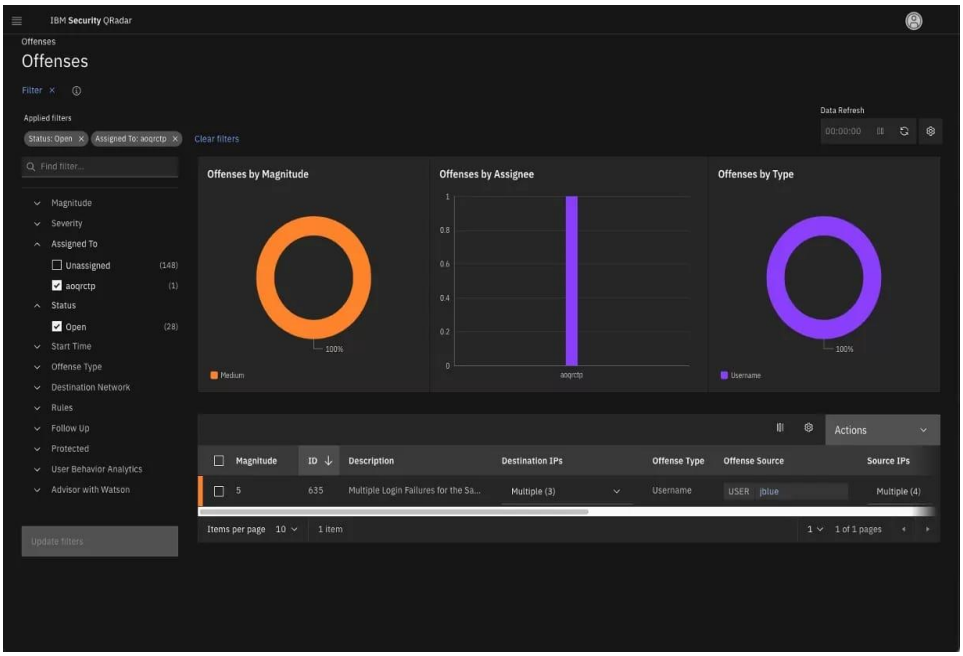
QRadar SIEM. Melihat tabel pelanggaran, kolom pertama menunjukkan pelanggaran berdasarkan prioritas atau besaran skor. Pelanggaran terjadi melalui proses deteksi ancaman otomatis QRadar, yang menganalisis peristiwa hampir secara real-time untuk mengetahui apa yang terjadi. QRadar SIEM dapat menganalisis peristiwa dari dua jenis sumber:

- Log: Ini adalah peristiwa yang terjadi pada titik waktu tertentu dan ditulis ke file log oleh aplikasi. QRadar SIEM dapat menganalisis file log dari lebih dari 700 sumber data.
- Arus atau aliran jaringan: Ini adalah aktivitas jaringan antara dua host di jaringan.

Kedua jenis sumber tersebut ditangkap oleh add-on Deteksi dan Respons Jaringan (NDR) bawaan QRadar SIEM. Aliran lebih dapat diandalkan dibandingkan data log karena mewakili data real-time aktual dan tidak dapat diubah.

2. Menyelidiki dan Menghubungkan Berbagai Peristiwa

Dari halaman deskripsi pelanggaran, saya dapat melihat segala sesuatu yang telah dikorelasikan dan diprioritaskan oleh QRadar SIEM:

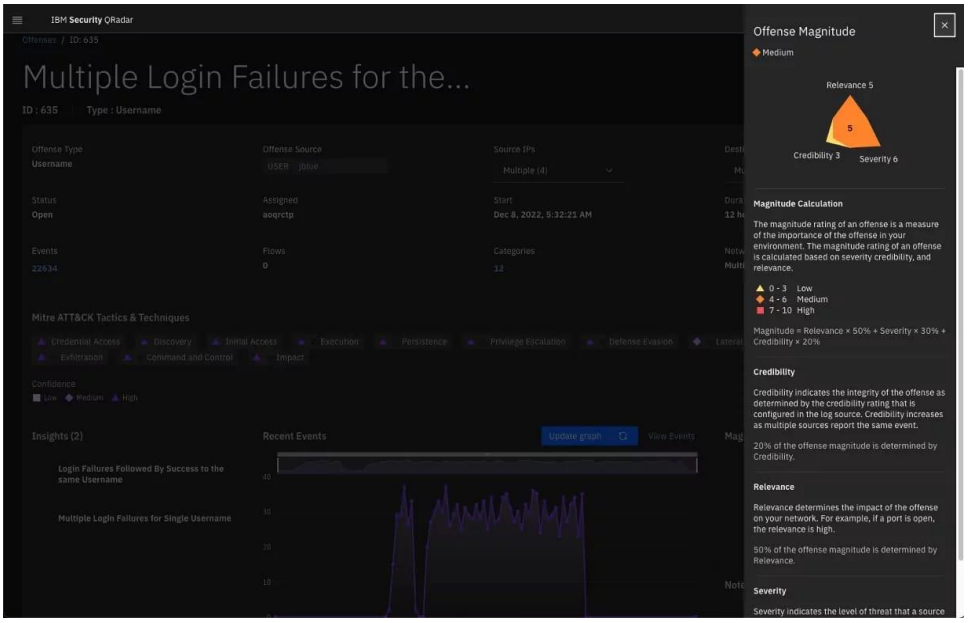


Gambar 3. Halaman Deskripsi Pelanggaran

3. Menilai Besarnya Suatu Pelanggaran

Hal ini mencakup IP sumber dan tujuan, taktik dan teknik MITRE ATT dan CK mana yang telah terdeteksi, dan kasus penggunaan apa yang dipicu sehubungan dengan pelanggaran ini, serta rincian skor besarnya. Skor besarnya adalah bagaimana QRadar SIEM secara unik menghitung prioritas pelanggaran, yang membantu analis keamanan fokus pada pelanggaran yang paling penting terlebih dahulu. Seperti yang ditunjukkan pada layar di bawah, ini terdiri dari tiga faktor:

1) Kredibilitas: Seberapa besar saya mempercayai sumbernya? (20% dari skor besarnya).
2) Relevansi: Seberapa relevankah hal ini secara spesifik dengan lingkungan saya? (50% dari skor besarnya).
3) Tingkat Keparahan: Seberapa buruk dampaknya jika hal ini benar-benar terjadi? (30% dari skor besarnya).



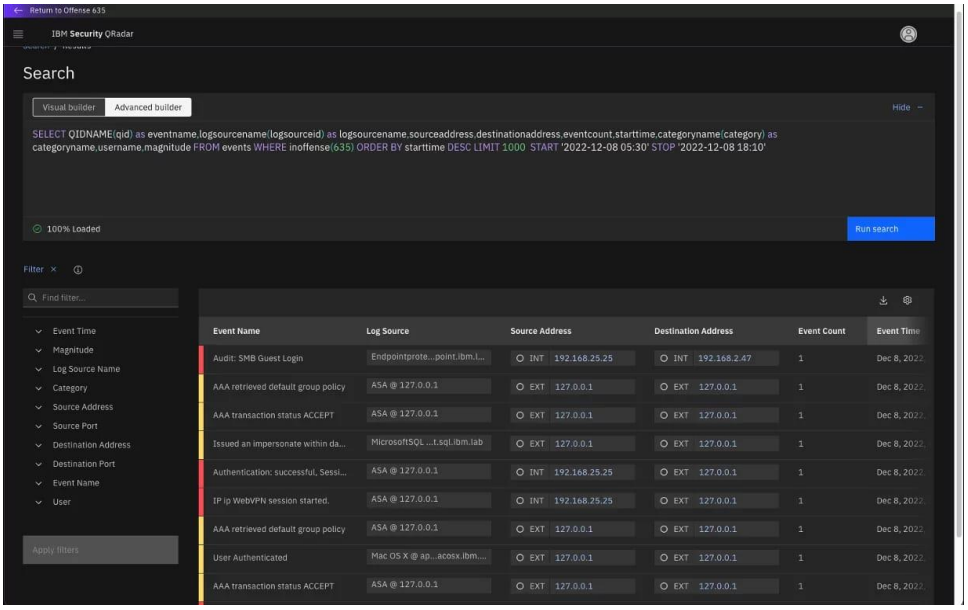
Gambar 4. Perhitugan Prioritas Pelanggaran

Pelanggaran ini mempunyai nilai besaran lima yang merupakan pelanggaran sedang. Jadi, saya ingin melanjutkan penyelidikan dengan meninjau kejadiannya. Mari kita lihat apakah QRadar SIEM menemukan nama pengguna yang terkait dengan semua ini.

4. Mencari Dan Memfilter Peristiwa

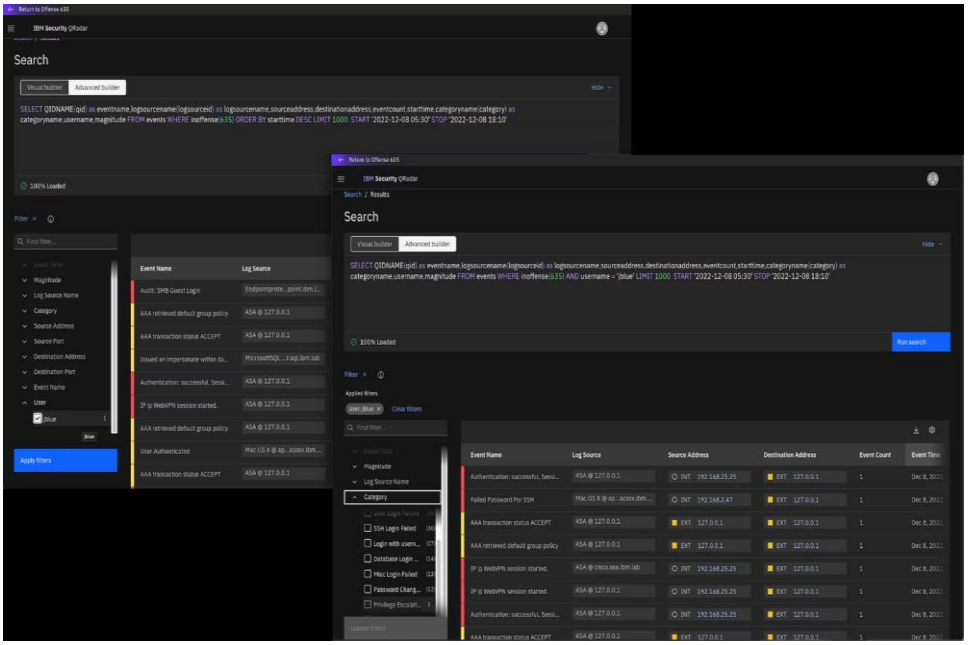
Dengan mengklik peristiwa tersebut, QRadar SIEM menunjukkan kepada saya alat pembuat kueri tempat saya melihat tampilan berisi

peristiwa yang terkait dengan pelanggaran ini. Di sini saya dapat terus menelusuri peristiwa, memfilternya atau jika perlu memodifikasi kueri AQL untuk memperluas atau mempersempit jumlah peristiwa.



Gambar 5. Tampilan Mencari dan Memfilter Peristiwa

Saya sekarang akan menggunakan beberapa kemampuan filter cepat di sebelah kiri untuk melihat apakah ada nama pengguna yang terdeteksi dalam peristiwa yang terkait dengan pelanggaran ini. Saya dapat melihat ada beberapa nama. Mari kita lihat penggunanya, JBlue:

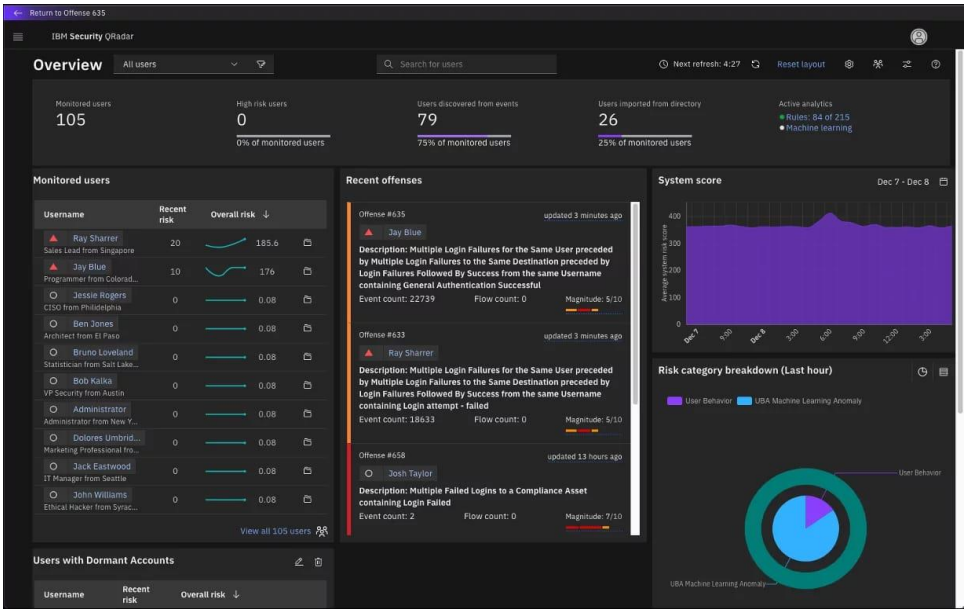


Gambar 6. Tampilan Mendeteksi Suatu Peristiwa

Seperti yang terlihat di atas, saya sekarang dapat melihat aktivitas Jblue. Saya segera melihat peningkatan hak istimewa, login gagal dan berhasil, dan sebagainya. Sepertinya Jblue merencanakan sesuatu. Saya akan beralih ke alat Analisis Perilaku Pengguna (UBA).

5. Menjalankan Analisis Perilaku Pengguna (UBA)

Pada halaman UBA atau *User Behavior Analytics* di bawah ini, saya dapat melihat informasi khususnya seputar risiko ancaman.



Gambar 7. Halaman UBA *(User Behavior Analytics)*

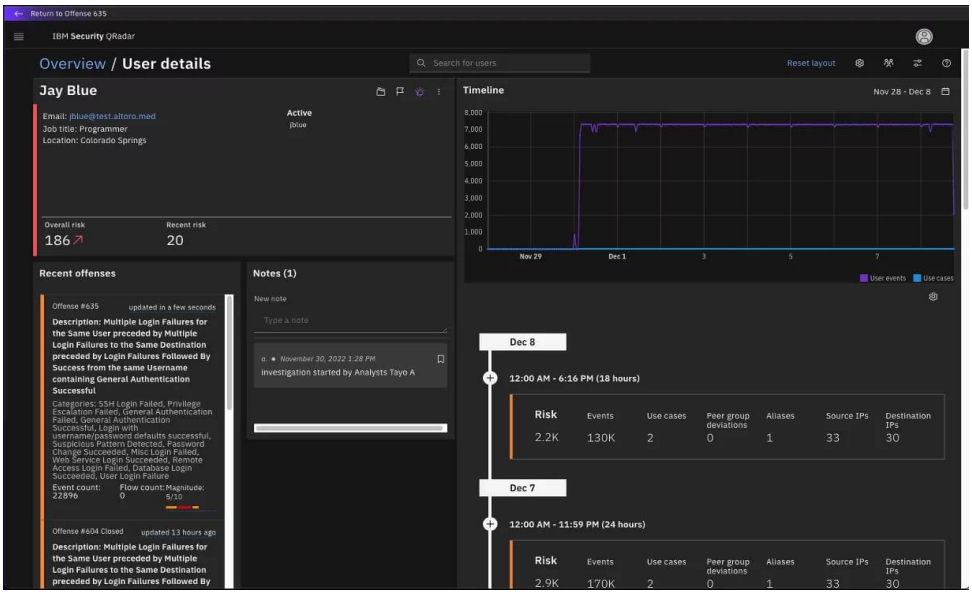
Di sebelah kiri adalah daftar Pengguna yang dipantau dan berisiko. Di sini, UBA diberi peringkat berdasarkan skor risiko tertinggi (yang didasarkan pada beberapa analisis di Qradar SIEM). Beberapa model pembelajaran mesin (ML) khusus menentukan perilaku normal versus anomali untuk setiap pengguna berdasarkan aktivitas mereka sendiri dan aktivitas kelompok rekan yang mereka pelajari. Model ML kelompok sejawat membantu UBA mendeteksi perilaku di luar apa yang dianggap sebagai perilaku kelompok sejawat yang normal.

Di bagian atas adalah status lingkungan saya, berapa banyak pengguna yang dipantau dan bagaimana UBA menemukan mereka (pengguna yang diimpor atau ditemukan melalui analisis peristiwa). Saya dapat mengimpor pengguna melalui CSV (*Comma Separated Values*) tradisional atau menggunakan LDAP (*Lightweight Directory Access Protocol*) untuk mengidentifikasi pengguna berdasarkan atribut terkait di seluruh sumber log. Di area paling kanan atas, UBA menunjukkan berapa

banyak aturan (kasus penggunaan) terkait UBA yang saat ini saya aktifkan, dan status model ML saya. Jadi sekarang, mari klik dua kali untuk mengetahui apa yang terjadi dengan pengguna Jblue.

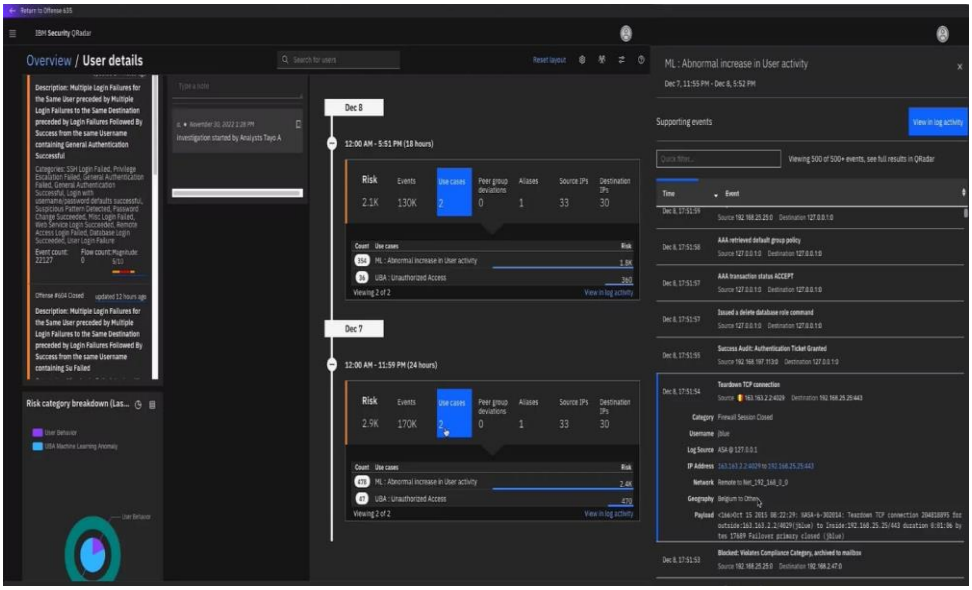
6. Menyelesaikan Penyelidikan Dengan Cepat Untuk Memicu Respons yang Efektif

Di bawah ini adalah halaman rincian Pengguna Jblue, yang memberi saya rincian tentang apa yang telah dilakukan Jblue:



Gambar 8. Tampilan penyelidikan *cyber*

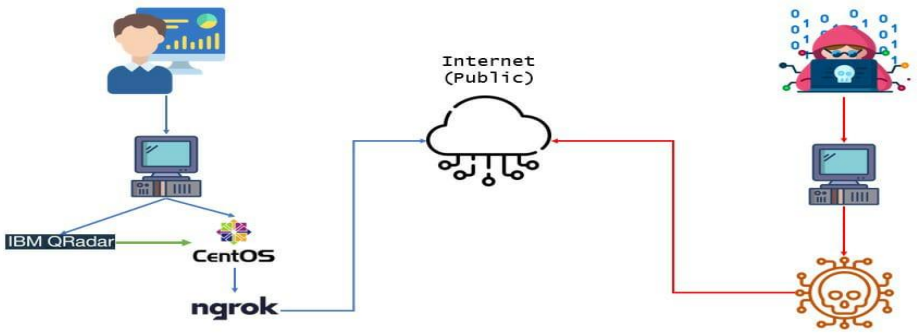
Saya langsung melihat dua kasus penggunaan pada layar di bawah yang cocok untuk sesi ini, yang merupakan tanda bahaya bagi saya:



Gambar 9. Halaman Status Penggunaan

Ketika saya dapat mengklik kasus penggunaan pertama ini ”akun tidak aktif digunakan” saya melihat ada peristiwa TCP yang terkait dengan IP Jerman. Untuk skenario ini, saya tahu bahwa saya tidak ada di sana.

Jadi, QRadar SIEM dapat membantu dalam deteksi ancaman secara real-time dan pada saat yang sama mengurangi beban kerja analis keamanan.



Gambar 10. Ilustrasi Serangan *Cyber*

Pada gambar diatas menunjukan bahwa haker menggunakan alat atau perangkat komputer yang digunakan untuk menyerang suatu user melalui internet. Kemudian serangan tersebut akan melewati ngrok dan cetos. Pada cetos, jika pengamanan melalui Qradar dilakukan dengan tepat maka data akan aman. Namun, jika pada cetos tidak dilakukan dengan tepat pengamanan data melalui Qradarnya, maka data akan dengan mudah diambil oleh haker.

D. Teknik Analisis Data

Analisis data akan melibatkan evaluasi efektivitas penerapan QRADAR SIEM dengan melihat tingkat keamanan sebelum dan setelah implementasi. Analisis juga akan melibatkan pengukuran respons terhadap serangan *cyber*. Langkah - langkah yang akan dilakukan proses analisis data adalah:

1. Pengumpulan Data

   QRadar mengumpulkan data dari berbagai sumber, termasuk log keamanan, aliran jaringan, dan aktivitas pengguna. Data ini diterima sebagai peristiwa atau kejadian dan dikirim ke pusat keamanan untuk analisis lebih lanjut.

2. Normalisasi Data

   Data yang diterima dari berbagai sumber dapat memiliki format dan struktur yang berbeda. Langkah normalisasi digunakan untuk

mengubah data ke dalam format standar sehingga dapat diintegrasikan dan dianalisis dengan lebih efektif.

3. Pengidentifikasian Ancaman

   QRadar melakukan analisis terhadap peristiwa-peristiwa yang terjadi untuk mengidentifikasi potensi ancaman keamanan. Ini melibatkan deteksi pola, tanda-tanda serangan, atau perilaku yang mencurigakan.

4. Korrelasi Peristiwa

   Proses korrelasi digunakan untuk menghubungkan peristiwa terkait dan mengidentifikasi serangan atau ancaman yang lebih kompleks yang mungkin terlihat biasa-biasa saja jika dilihat secara terpisah.

5. Pengelompokan dan Prioritisasi Ancaman

   Data yang dikumpulkan dianalisis untuk memprioritaskan ancaman berdasarkan tingkat keparahan dan dampak potensial terhadap sistem. QRadar dapat memberikan nilai risiko terhadap setiap ancaman.

6. Investigasi dan Respon

   Melakukan investigasi lebih lanjut terhadap ancaman yang diidentifikasi. QRadar menyediakan alat untuk menyelidiki peristiwa, menggali lebih dalam informasi terkait, dan merinci aktivitas yang mencurigakan.

7. Notifikasi dan Pelaporan

   Sistem ini memberikan kemampuan untuk memberikan notifikasi segera tentang kejadian yang memerlukan perhatian, serta menyediakan laporan keamanan yang dapat digunakan untuk audit dan pemantauan jangka panjang.