Rancang Bangun Rekomendasi Strategi Cybersecurity Indonesia Berdasarkan Perbandingan Cyber Threat Intelligence Global Menggunakan Metode Osint = Design And Development Of Indonesia'S Cybersecurity Strategy Recomendation Based On Global Cyber Threat Intellegence Comparison Using Osint

Satriyo Adipratomo, author

Abstrak

Data World Bank menunjukkan bahwa dari tahun 2010 hingga 2021 terjadi kenaikan sebesar 51% pada angka persentase populasi yang menggunakan akses internet di Indonesia. Kondisi ini belum dibarengi dengan penjagaan cybersecurity yang maksimal. Salah satu cara untuk menanggulangi masalah ini adalah dengan perumusan strategi cybersecurity berdasarkan cyber threat intelligence. Salah satu metode yang dapat dimanfaatkan untuk mencari cyber threat intelligence adalah melalui open source intelligence atau OSINT. OSINT merupakan suatu metode pengumpulan dan analisis data yang tersedia secara terbuka; artinya sumber informasi dan datanya harus dapat diakses oleh siapapun, kapanpun. Pada penelitian ini, Twitter dipilih sebagai sumber OSINT dengan pertimbangan kemampuan Twitter untuk menghasilkan data yang volumenya besar, jumlah akun yang banyak dan beragam, aksesibilitas, dan popularitas di komunitas cybersecurity. Data dari Twitter akan diproses melalui enam skenario untuk menghasilkan cyber threat intelligence. Hal ini dilakukan dengan menghitung persentase jumlah kemunculan istilah terkait cyber threat dan threat actor atau software yang sering dibicarakan di Twitter. Kemudian hasil dari tiap skenario akan dibandingkan. Didapatkan hasil bahwa isu paling berbahaya di Indonesia adalah dark web: 40,12%, kebocoran data: 31,48%, dan ransomware: 12,35%; dnegan LockBit sebagai threat group yang paling berbahaya dengan persentase kemunculan 27,27%. Informasi tersebut digabungkan dengan hasil banding strategi cybersecurity dari negara Malaysia, Belgia, Inggris, dan Amerika Serikat menjadi dasar perancangan rekomendasi Strategi Cybersecurity Indonesia yang terbagi menjadi sebuah narasi, 4 komitmen, dan 17 tugas untuk mencapai tujuan tersebut.

.....World Bank data shows that from 2010 to 2021 there will be an increase of 51% in the percentage of the population using internet access in Indonesia. This condition has not been accompanied by maximum cybersecurity. One way to overcome this problem is to formulate a cybersecurity strategy based on cyber threat intelligence. One method that can be used to search for cyber threat intelligence is through open source intelligence or OSINT. OSINT is an openly available data collection and analysis method; meaning that sources of information and data must be accessible to anyone, at any time. In this study, Twitter was chosen as the OSINT source by considering Twitter's ability to generate large volumes of data, the large and varied number of accounts, accessibility, and popularity in the cybersecurity community. Data from Twitter will be processed through six scenarios to generate cyber threat intelligence. This is carried out by calculating the percentage of terms related to cyber threats and threat actors or software that are frequently discussed on Twitter. Then the results of each scenario will be analyzed and compared with each other. The results show that the most dangerous issues in Indonesia are the dark web: 40.12% occurrence, data breach: 31.48% occurrence, and ransomware: 12.35% occurrence; with LockBit being the most dangerous threat group with an occurrence percentage of 27.27%. This information is combined with the results of a

comparison of cybersecurity strategies from Malaysia, Belgium, the United Kingdom, and the United States of America to form the basis for designing the recommendations for the Indonesian Cybersecurity Strategy which are divided into a narrative, 4 commitments, and 17 tasks to achieve this goal.