Implementasi Splunk dalam Membangun Security Information and Event Management Berdasarkan Log Firewall (studi kasus: Jaringan UII)

by John Doe

Submission date: 24-Nov-2020 01:57AM (UTC+0700)
Submission ID: 1455287210
File name: 17523141.pdf (1.25M)
Word count: 4058
Character count: 26327

Implementasi Splunk dalam Membangun *Security Information and Event Management* Berdasarkan *Log Firewall (studi kasus: Jaringan UII)*

***Abstrak*— Universitas Islam Indonesia adalah salah satu perguruan tinggi yang berkomitmen meningkatkan teknologi informasi dengan mendirikan Badan Sistem Informasi atau disingkat BSI. UII saat ini sedang dalam tahap menerapkan teknologi *enterprise*. Salah satunya pada bidang keamanan, UII telah menerapkan *Next-Generation Firewall* (NGFW) yang merupakan teknologi mutakhir dari *Firewall*. Namun apabila hanya mengandalkan *Firewall* saja, maka hal belum dapat menjamin keamanan. Terlebih ternyata data yang dihasilkan oleh NGFW memiliki ukuran masuk dalam kategori *big data*. Data yang besar tentunya menyimpan informasi yang besar pula. Sebagai bentuk upaya untuk menambah pengamanan pada jaringan UII serta memanfaatkan data yang telah dimiliki. Maka peneliti mengusulkan sebuah penelitian yang bertujuan untuk memberikan gambaran apabila BSI UII melakukan implementasi sebuah teknologi yang dapat digunakan untuk melakukan orkestrasi dari data-data *Log* yang dihasilkan banyak perangkat, teknologi tersebut bernama *Security Information and Event Management*. Tentunya untuk mengimbangi teknologi *enterprise* yang ada, maka penulis mambawa *tools* yang merupakan *next-generation* dari SIEM yaitu Splunk. Dalam penelitian ini penulis akan mengolah data *Log Firewall* yang berasal dari NGFW menjadi sebuah *dashboard* dengan pendekatan *Data Mining*. Visualisasi pada *dashboard* akan berupa visualisasi *cluster* dan non-*cluster*. Selain itu juga akan diterapkan *alert* yang diintegrasikan dengan *Both* Telegram.**

Kata Kunci—log; firewall; SIEM; NGFW; cluster; dashboard; Alert; Data Mining

1 PENDAHULUAN

Universitas Islam Indonesia adalah salah satu perguruan tinggi yang berkomitmen meningkatkan teknologi informasi dengan mendirikan Badan Sistem Informasi atau disingkat BSI. Secara umum BSI bertugas mengawal perencanaan, pengembangan, operasi, serta layanan sistem dan teknologi informasi untuk kurang lebih 30.000 pengguna [1]. Agar dapat memberikan layanan secara profesional, hendaknya BSI berfokus untuk menjamin *confidentiality* (kerahasiaan), *integrity* (konsistensi, akurasi, dan validitas data), *availability* (ketersediaan) atau biasa disebut CIA. Ketiga komponen tersebut merupakan dasar dari keamanan informasi [2].

Dalam menjaga kerahasiaan data, BSI telah mengimplementasikan *next-generation firewall* (NGFW) dari perusahaan *Palo Alto Network*. Teknologi *next-generation firewall* (NGFW) merupakan penerus dari *firewall* tradisional yang memiliki banyak kekurangan. Fitur pada NGFW mencakup segala fitur yang terdapat pada *firewall* tradisional dan terdapat fitur tambahan seperti *Intrusion Prevention System* (IPS), *Deep Packet Inspection* (DPI), *Application Control*, *Directory Integration*, dan *Encrypted Traffic Inspection* [3]. Dengan jumlah pengguna yang kurang lebih mencapai 30.000 pengguna, tentu saja catatan log pada *firewall* memiliki jumlah data berjumlah besar.

Untuk membantu administrator BSI UII dalam membaca *Log Firewall* dengan jumlah yang besar, solusi yang dapat ditawarkan adalah membuat *Log Monitoring System*. *Security Information Event and Management* atau disingkat SIEM merupakan sistem informasi terpusat dan digunakan untuk mengumpulkan *log* yang nantinya memberikan hasil berupa visualisasi *Log Monitoring* guna mempermudah pembacaan informasi *Log* [4]. Namun, akan timbul masalah dalam visualisasi *Log Monitoring* apabila jumlah data log berukuran besar. Informasi yang ditampilkan akan memiliki persebaran acak sehingga cenderung sulit untuk dibaca maupun dipahami.

Solusi untuk menangani jumlah data yang besar atau saat ini biasa disebut *big data* salah satunya adalah dengan pendekatan *data mining*. Data yang besar nantinya akan dikelompokkan atau dikluster dengan hitungan secara matematika dan statistik sebelum data ditampilkan. Sehingga visualisasi *Log Monitoring* akan dapat lebih mudah dipahami [5]. Dalam menerapkan *data mining* salah satu teknik yang digunakan adalah menggunakan *machine learning*. Dalam melakukan pengelompokan atau *cluster* dibutuhkan algoritma sebagai dasar dari penerapan teknik *machine learning*. Pemilihan algoritma salah satunya harus didasarkan dengan *tools* yang digunakan dalam mengimplementasikan teknologi *Security Information and Event Management* (SIEM) [6]. Pada penelitian kali ini alat yang akan digunakan sebagai solusi yang penulis tawarkan adalah menggunakan aplikasi Splunk yang merupakan *next-generation* SIEM *product*. Splunk mendukung penerapan *data mining* dengan teknik *machine learning* yang dibutuhkan untuk mengelola *Log Firewall* dalam melakukan klasterisasi agar visualisasi *Log Firewall* mudah untuk dipahami. Splunk juga memiliki fitur penyaringan, pencarian, masukkan, modifikasi, pelaporan, dan penghapusan data.

Pada Splunk terdapat *add-on* berupa aplikasi, salah satunya adalah *Splunk Machine Learning Toolkit* yang memiliki fitur untuk melakukan kegiatan *machine learning*, yaitu *clustering*. Pada bagian *clustering* yang terdapat pada *add-on* Splunk, terdapat dua variasi untuk melakukan eksperimen *clustering* yaitu *smart clustering* dan *cluster number events*. Pada variasi *clustering* tersebut, Splunk memberikan 4 pilihan algortima

machine learning yaitu DBSCAN, Birch, K-means, dan SpectralClustering [7]. Setelah melakukan perbandingan dari keempat algoritma tersebut, pada penelitian kali ini algoritma yang akan digunakan adalah K-means. K-means merupakan algoritma *machine learning* dengan type *Unsupervised Learning*. Algoritma K-means dipilih karena dalam hal melakukan komputasi, lebih cepat dibanding dengan algoritma klustering lainnya, hasil algoritma ini juga sederhana untuk menjelaskan dan memahami, dan algoritma ini biasanya menghasilkan *cluster* yang lebih *tighter* dibanding *hierarchical clustering* [7].

Splunk memiliki fitur *alert real-time* yang dapat digunakan untuk membantu memantau *event* atau serangan yang terjadi. Menyiapkan *alert* berdasarkan *critical control* keamanan dapat memberi informasi keamanan ketika penyerang mencoba melewati kontrol atau ketika perangkat yang berpotensi tidak aman atau tidak sah memasuki jaringan [8]. Dalam menerapkan *alert*, sebaiknya pemberitahuan *alert* dapat diketahui tidak hanya saat sedang memantau Splunk saja. Sebab *administrator* tidak mungkin selalu berada ditempat yang sama. Oleh karena itu dibutuhkan integrasi *alert* dengan sebuah aplikasi yang dapat memberikan kemudahan penerimaan informasi saat *alert* muncul. Telegram merupakan sebuah aplikasi yang dapat diakses pada *smartphone* ataupun perangkat komputer. Telegram memiliki fitur *both* yang dapat diintegrasikan dengan Splunk untuk membantu kemudahan menerima informasi saat *alert* muncul. Penggunaan *both* Telegram juga telah diadopsi oleh *team* BSI UII untuk melakukan pemantauan suhu *server*, Sehingga penerapan *both* Telegram sudah sangat familiar dilingkungan BSI UII.

2 LANDASAN TEORI

2.1 Landasan Teori

Pemanfaatan IT salah satunya sebagai tempat mengumpulkan sumber informasi serta berbagai data penting yang merupakan aset dari organisasi. Informasi ataupun aset yang terkumpul merupakan sebuah nilai (*Value*) yang berharga dari suatu organisasi yang harus dilindungi. Semakin besar sebuah organisasi tentunya akan semakin besar dalam memanfaatkan infrastruktur IT, hal ini akan membuat sistem IT semakin kompleks dan terdistribusi sehingga akan membuat departemen IT mengalami kesulitan dalam melakukan pengelolaan serta kegiatan *monitoring*. Penerapan teknologi mutakhir tentunya diperlukan untuk mempermudah departemen IT dalam melakukan pekerjaannya.

2.1.1 Keamanan Informasi

Keamanan Informasi merupakan bidang serta aktifitas profesional multidisiplin yang berkaitan dengan pengembangan dan juga implementasi mengenai mekanisme keamanan dari berbagai aspek secara teknis maupun organisional. Tindakan minimal yang harus diterapkan oleh organisasi untuk mengamankan informasi saat ini biasa dikenal dengan Kerahasiaan, Integritas, dan Ketersediaan atau biasa disebut dengan CIA. Kerahasiaan bertugas memastikan privasi dari data dengan membatasi akses melalui enkripsi yang terotentikasi. Integritas bertugas menjamin bahwa informasi tepat dan akurat serta terpercaya. Ketersediaan bertugas memastikan informasi selalu dapat diakses oleh pihak atau pengakses yang berwenang [9].

2.1.1.1 Confidentiality (Kerahasiaan)

Kerahasiaan memiliki istilah lain yaitu privasi. Sebuah perusahaan hendaknya memiliki kebijakan untuk membatasi akses ke informasi atau data yang hanya dapat diakses oleh pihak atau staf yang berwenang. Salah satu solusi dari hal tersebut adalah membagi data menurut tingkat keamanan atau sensitivitas dari informasi tersebut. Terdapat metode untuk memastikan kerahasiaan yang mencakup enkripsi data, ID nama pengguna dan kata sandi, otentikasi dua faktor, dan meminimalisir dalam menyebarkan informasi yang sensitif.

2.1.1.2 Integrity (Integritas)

Integritas merupakan keakuratan, konsistensi, dan keandalan dari data selama masa pakainya. Data yang dikirimkan tidak boleh berubah dan juga tidak dapat diubah oleh seseorang atau entitas yang tidak berwenang ataupun tidak sah. Perizinan pada file serta kontrol untuk akses pengguna dapat mencegah dari pengakses yang tidak sah. Selain itu, kontrol versi juga dapat digunakan untuk mencegah perubahan dari ketidaksengajaan pengguna yang berwenang. Cadangan data diperlukan untuk membantu apabila data ingin dikembalikan dari resiko kerusakan seluruh data, dan *hashing checksum* dapat digunakan untuk memverifikasi integritas data selama data dalam pengiriman.

2.1.1.3 Availability (Ketersediaan)

Memelihara peralatan, memperbaiki perangkat keras, selalu update sistem operasi dan perangkat lunak, serta mencadangkan data untuk memastikan ketersediaan jaringan dan data bagi pengguna yang berwenang. Rencana yang telah disusun hendaknya dijalankan degan cepat misalnya dalam hal memulihkan dari bencana alami atau akibat perbuatan manusia. Peralatan (*tools*) atau perangkat lunak (*software*) keamanan, seperti *Firewall* akan berguna untuk melindungi dari gangguan akibat serangan seperti DoS (penolakan layanan). DoS terjadi apabila penyerang mencoba membuat sumber daya tidak berdaya dalam memberikan respon yang mengakibatkan layanan tidak tersedia bagi pengguna.

2.1.2 IT Security Risk Management

Risk Management atau manajemen risiko merupakan proses untuk melakukan identifikasi celah keamanan (*vulnerabilities*) serta ancaman yang mengancam sumber informasi yang biasanya digunakan oleh organisasi dalam upaya mencapai tujuan bisnisnya dan untuk menentukan respon/tindakan pencegahan apa saja yang diperlukan apabila resiko tersebut terjadi atau bahkan dapat mengurangi risiko dengan catatan tingkatnya dapat diterima didasarkan pada nilai dari sumber informasi organisasi tersebut [5].

IT risk management berupaya untuk mencoba melindugi *Confidentiality*, *Integrity*, dan *Availability* (CIA) dengan meminimalisir dampak yang nantinya mungkin akan muncul

dan memberikan efek pada *Confidentiality* dari informasi, *Integrity* dari data yang terdapat pada sistem, dan *Availability* yang berasal dari infrastruktur sistem [10].

2.1.3 *Security Information and Event Management (SIEM)*

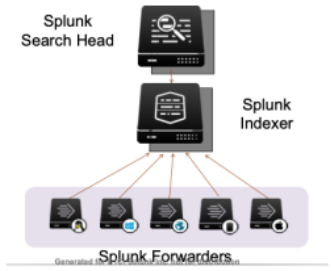
Security Information and Event Management atau biasa disebut dengan SIEM merupakan sebuah teknologi yang dapat mendeteksi berbagai ancaman dan insiden dari keamanan dengan mengumpulkan *Log real-time* dan melakukan analisa sejarah *Log* keamanan dari berbagai jenis tipe log dan berasal dari berbagai sumber data dari perangkat yang berbeda-beda.

SIEM mendukung analisa dan juga investigasi pada insiden melalui analaisis dari data historis dan berbagai alat keamananan dari organisasi seperti Router, IDS/IPS, UTM, Firewall, Server, dan lain-lain. Inti dari kemampuan teknologi SIEM yaitu cakupan yang luas dalam mengumpulkan *Log* dan juga kemampuan dalam melakukan korelasi dan melakukan analisis kejadian dari berbagai sumber jenis log atau perangkat yang berbeda-beda [11].

2.1.4 *Splunk*

Splunk adalah *platform* perangkat lunak untuk melakukan pencarian, menganalisis, dan memvisualisasikan data yang dihasilkan mesin dan biasanya berasal dari *computers, network device, logs, sensor, databases*, dan lain-lain yang menyusun infrastruktur IT suatu organisasi.

Splunk bekerja melalui 3 perangkat penyusun dasarnya, pertama adalah setiap perangkat yang meghasilkan data dipasang alat bernama Splunk *Forwarders* yang berfungsi untuk menghimpun data dari perangkat dan mengirimnya menuju Splunk *Indexer* yang merupakan tempat berkumpulnya data dari berbagai perangkat. Untuk kebutuhan tingkat atas yaitu berkaitan dengan klien dan visualisasi maka alat yang bekerja adalah Splunk *Search Head*.



Gambar 1. Cara Kerja Splunk

2.1.5 *Next-Generation Firewall (NGFW)*

Next-Generation Firewall atau biasa disebut NGFW lebih kuat dibandingkan dengan Traditional *Firewall*. NGFW memiliki kemampuan Traditional *Firewall* dan juga memiliki sejumlah fitur tambahan untuk menangani lebih banyak variasi kebutuhan organisasi dan memblokir lebih banyak potensi ancaman. *Firewall* ini disebut dengan "*Next-Generation*" untuk membedakan dari *Firewall* lama (Traditional *Firewall*) yang tidak memiliki kemampuan tambahan tersebut [12]. Segala macam *Firewall* mencatat segala macam jenis kegiatan kedalam *Log Firewall*. Karena terdapat fitur tambahan pada NGFW, maka ukuran dari *Log Firewall* cenderung lebih besar dibanding Traditional *Firewall*.

2.1.6 *Data Mining*

Data mining merupakan proses dalam menggunakan teknik metematik, statistik, kecerdasan buatan, dan *machine learning* dalam melakukan ekstrasi dan melakukan identifikasi yang bermanfaat serta pengetahuan yang terkait dari berbagai *big data* atau maha data [11]. Tujuan dari dilakukannya *data mining* adalah untuk memahami lebih jauh terkait perilaku data yang sedang diamati (deskripsi) dan sebagai acuan untuk memperkirakan kondisi yang nantinya akan terjadi (prediksi).

2.2 *Penelitian Terkait*

[5] dalam penelitiannya melakukan konsolidasi dan visualisasi *Log Server* yang berasal dari Badan Sistem Informasi, Universitas Islam Indonesia. Dalam melakukan penelitainnya penulis memanfaatkan *Log Management System* berbasiskan sumber terbuka (open source) yaitu ELK Stack yang terdiri dari empat aplikasi berbeda yaitu Kibana, Beats, Elasticsearch, dan Logstash. Hasil dari penelitian ini adalah *Log* dapat dikonsolidasi dan terkumpul menjadi satu dengan bantuan Filebeat, *Log* dapat dipecah untuk disesuaikan dengan kebutuhan administrator menggunakan Logstash, dan *Log* yang telah dipecah berhasil divisualisasikan dengan memanfaatkan aplikasi Kibana. Namun peneliti memberikan saran untuk penelitian berikutnya agar menambahkan variasi dari *Log* yang dikelola dan pemanfaatan fitur *machine learning* yang tersedia pada pada aplikasi Kibana

[13] dalam penelitiannya yang melakukan klasifikasi *Alert* pada *Intrusion Detection System* dengan menggunakan algoritma K-means. Penulis menggunakan *tools* IDS yaitu Snort dalam proses identifikasi serangan dan menggunakan *tools* Matlab untuk proses *clustering* dengan algoritma K-means memanfaatkan perhitungan *Euclidean Distance* untuk menentukan jarak terdekat antara data dengan *centroid*. Hasilnya peneliti mendapatkan hasil nilai klasifikasi serangan menggunakan algoritma tersebut, namun penulis mencatat beberapa kelemahan dari algoritma K-means dalam penelitiannya yaitu kurangnya kejelasan mengenai bagaimana menentukan jumlah kluster (k) yang terbaik. Penulis memberikan saran untuk dapat memanfaatkan segala jenis serangan dalam proses klasifikasi *alert*, sehingga IDS dapat bekerja lebih optimal

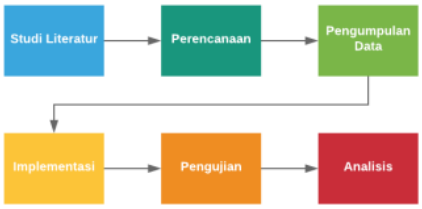
[14] dalam penelitiannya melakukan integrasi untuk visualisasi *Log* dari *honeypot* dengan sistem manajemen *honeypot* paling mutakhir yaitu *Modern Honey Network* (MHN) dengan memanfaatkan *tools* Splunk. Peneliti mendapatkan hasil bahwa MHN mudah diterapkan karena telah memiliki API untuk membaca data penyerang. Hasil yang diperoleh pun mempermudah keterbacaan aktivitas yang telah tercatat pada *Log*.

[15] dalam penelitiannya, peneliti membuat sebuah usulan dalam penggunaan model dan arsitektur baru dalam melakukan implementasi *Security Information and Event Management*

(SIEM) yaitu dengan menggunakan *Hierarchical* SIEM *manager,* sebuah mekanisme yang tujuannya adalah untuk tipe perusahaan dengan tipe organisasi yang telah terdistribusi. Peneliti menyebutkan bahwa telah berhasil dalam mengunakan *ArchSight ESM* dalam melakukan implementasi keamanan jaringan dengan skala besar dan terdistribusi.

3 METODOLOGI

Penelitian ini menggunakan metode penelitian sebagai berikut:



Gambar 2. Metode Penelitian

3.1 *Studi Literatur*

Tahapan pertama dalam penelitian ini adalah studi literatur untuk pencarian masalah, pencarian referensi, dan landasan teori sebagai dasar untuk melakukan penelitian. Studi literatur dilakukan guna melakukan *review* terhadap makalah, jurnal ataupun hasil penelitian yang sejenis, mengeksplorasi sumber pustaka yang dikutip oleh tulisan yang dibaca dengan bahasan yang sejenis. Penulis mengadopsi beberapa teknologi yang digunakan dan mengambil beberapa saran penelitian dari studi literatur sebagai masukan dalam meneliti.

3.2 *Perencanaan*

Setelah melakukan studi literatur, penulis melakukan perencanaan secara mendalam untuk solusi ditawarkan. Perencanaan meliputi sumber atau literatur yang penulis adopsi, pemilihan teknologi yang akan digunakan, dan pemilihan *tools* yang akan digunakan.

3.3 *Pengumpulan Data*

Data yang akan digunakan merupakan data yang tercatat pada *log firewall* Badan Sistem Informasi, Universitas Islam Indonesia data dalam waktu satu hari secara penuh yang merupakan hasil pilihan dari hari-hari lainnya di Universitas Islam Indonesia. Data *Log Firewall* yang digunakan adalah type *Traffic* dan merupakan data sekunder.

3.4 *Implementasi*

Pada bagian implementasi akan terdiri dari beberapa metode sebagai berikut,

3.4.1 *Instalasi Splunk Web*

Dalam penelitian kali ini, penulis menggunakan versi *trial* dari Splunk dan merupakan Splunk Web, sebab penggunaan aplikasi Splunk untuk kebutuhan jangka panjang adalah berbayar. Adapun kebutuhan system untuk dapat menggunakan versi *Trial* dari Splunk Enterprise adalah,

Tabel 1. KEBUTUHAN SISTEM

Sistem Operasi	Windows / Linux / Mac Os
Processor	Minimal 2-core 64-bit CPU at 2GHz
RAM	Minimal 4 GB
Web Browser	Versi paling update dari Chrome / Firefox / Safari
Port Splunk Web	8000

3.4.2 *Instalasi Add-on Aplikasi Palo Alto Firewall*

Data yang akan diteliti merupakan data yang berasal dari *Firewall Palo Alto Network*. Oleh karena itu, untuk menambah keterbacaan *fields* dari data *log firewall* (*traffic type*) sehingga fields yang terdeteksi akan lebih banyak. Maka dibutuhkan instalasi *Add-on* Aplikasi *Palo Alto Network*.

3.4.3 *Instalasi Aplikasi Splunk Machine Learning Toolkit*

Untuk proses klasterisasi dengan pendekatan *machine learning,* dibutuhkan aplikasi yang dapat melakukan proses komputasi dengan *machine learning.* pada Splunk telah terdapat aplikasi berupa *Add-on* untuk pengolahan tersebut yang bernama "*Splunk Machine Learning Toolkit"*.

3.4.4 *Instalasi Aplikasi Telegram Alert Action*

Dalam *alert system* yang akan diterapkan dan akan diintegrasikan dengan *both* Telegram. Maka instalasi aplikasi "*Telegram Alert Action*" bertujuan untuk memudahkan dalam melakukan integrasi tersebut.

3.4.5 *Upload Data*

Splunk Web versi *trial* memberikan pembatasan untuk upload data yaitu sebesar 500 mb untuk satu waktu upload. Data *traffic log firewall* dalam satu hari memiliki ukuran 25 – 35 gb. Maka salah satu solusi agar data dapat diolah adalah dengan membagi data menjadi bagian-bagian yang berukuran dibawah 500 mb. Penulis melakukan pemecahan data dengan memanfaatkan *tools* dari linux yaitu tools "Split".

```
Split -b <ukuran file>m -additional-suffix=<ekstensi
file> <Nama File> <nama file setelah dipecah> --verbose
```

Gambar 3. *Syntax Split* File

3.4.6 *Search & Reporting*

Pada bagian ini, hal yang dilakukan adalah membuat "*Rule*" untuk menampilkan visualisasi dari data Log Firewall agar mudah dipahami atau dibaca. Untuk melakukan hal ini, yang harus dilakukan adalah masuk pada bagian "*Search & Reporting*" dari tampilan awal Splunk Web. Berikut merupakan *Rule* yang akan digunakan:

```
index=* sourcetype="pan:traffic"
| chart count over app:technology by action
```

Gambar 4. *Rule Detection Traffic by Action*

```
index=* sourcetype="pan:traffic"
| stats  dc(user) as total_pengguna
```

Gambar 5. *Rule Detection All User by User*

```
index=* sourcetype="pan:traffic"
client_location=Indonesia
| stats  dc(user) as total_pengguna
```

Gambar 6. *Rule Detection Indoneisan User from client_location by user*

```
index=* sourcetype="pan:traffic"
| iplocation client_ip
| stats dc(user) as Pengguna by client_location
| geom geo_countries featureIdField=client_location
```

Gambar 7. *Rule Detection Count User in Country by client_location*

```
index=* sourcetype="pan:traffic"
| chart count over app:technology by action
```

Gambar 8. *Rule Splunk Web Login Attemps*

```
index=* sourcetype="pan:traffic" user=* user!=""
| stats count(eval(action="success")) as successes
count(eval(action="failure")) as failures by user,
app
| where successes>0 AND failures>100
```

Gambar 9. *Rule Detection Brute Force Attack*

3.4.7 *Klasterisasi*

Pada bagian ini, hal yang dilakukan adalah mencoba melakukan klasterisasi dari data "*Log Firewall*". Kegiatan ini dilakukan dengan menggunakan aplikasi *Splunk Machine Learning Toolkit* yang sebelumnya telah diinstal. Algoritma yang digunakan adalah K-means.

3.4.8 *Membuat Alert dan Integrasi ke Telegram*

Setelah tahapan-tahapan sebelumnya selesai dilakukan, tahapan paling akhir adalah membuat laporan berdasarkan temuan-temuan yang didapatkan dari hasil visualisasi. Laporan dibuat diawali dengan melakukan *Search dan Reporting*.

3.5 *Pengujian*

Kegiatan utama dari penelitian ini adalah menghasilkan tiga macam keluaran, ketiga keluaran tersebut yaitu pertama Visualisasi non-*Clustering.* Kedua Visualisasi dengan *Clustering,* Ketiga Integrasi *Alert* dengan *both* Telegram. Pengujian dilakukan dengan menguji *Rule* pada data *log firewall* pada hari yang berbeda.

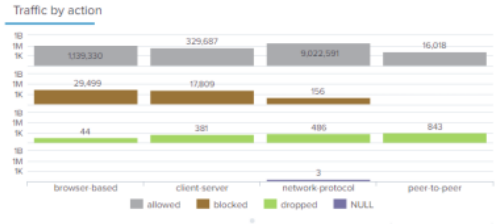
3.6 *Analisis*

Tahapan analisis akan dilaksanakan setelah pengujian dilakukan. Analisis dilakukan untuk mengamati hasil dari visualisasi non-*cluster* dan visualisasi dengan *cluster.* Hasil dari analisis ini yang nantinya akan menjadi acuan bagi penulis untuk menuliskan kesimpulan.

4 PEMAPARAN HASIL

4.1 *Visualisasi Log Firewal non-Clustering*

Dari *Rule* yang telah diterapkan, maka hasil visualisasi adalah sebagai berikut:

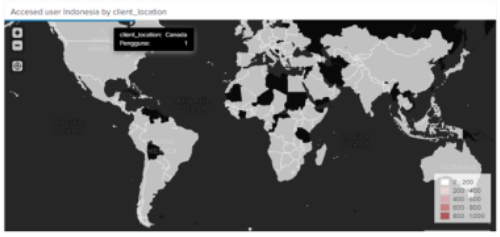


Gambar 10. *Visualitation Traffic by Action*

Gambar 11. *Visualitation All User by user*

Gambar 12. *Visualitation Indonesian User by user*

Gambar 13. *Visualitation User in Country by client_location*

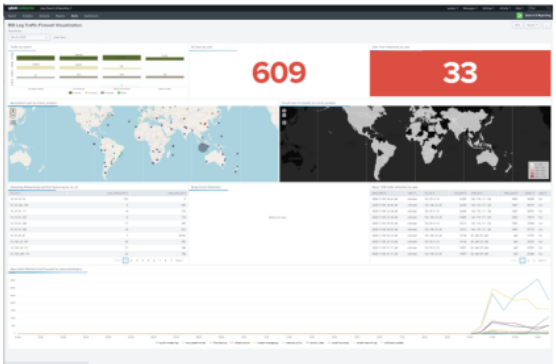


Gambar 14. *Visualitation Count User in Country by client_location*

Dalam proses pengujian, penulis melakukan pengujian *Rule* yang telah ditetapkan. Penulis menguji apakah Rule bersifat *universal* sehingga dapat digunakan pada data *Log Firewall* di setiap harinya. Karena keterbatasan waktu dan ruang penyimpanan. Sebab data *Log Firewall* setiap harinya berukuran lebih dari 30 GB. Maka penulis melakukan pengujian pada dua hari yang berbeda. Hari ditentukan berdasarkan ukuran *Log Firewall* yang lebih besar dibanding hari-hari lainnya. Hari yang pertama adalah pada Rabu, 28 Oktober 2020. Kemudian hari yang kedua adalah pada Jum'at 06 November 2020. Berikut tabel perbandingan dari kedua hari tersebut:

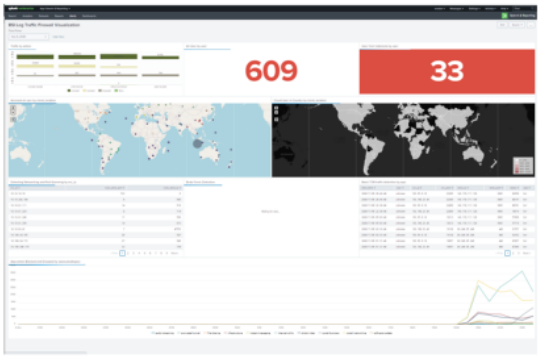
Tabel 2. DASHBOARD RABU, 28 OKTOBER 2020

Waktu	Rabu, 28 Oktober 2020
Data Size	40.8 GB
Total Events	104.484.528 events
Problems	Tidak ada



Tabel 3. DASHBOARD JUM'AT 06 NOVEMBER 2020

Waktu	Jum'at, 06 November 2020
Data Size	43,3 GB
Total Events	111.866.547 events
Problems	Tidak ada



Dari hasil pengujian, dapat disimpulkan bahwa *Rule* yang telah ditetapkan telah bersifat *universal*. Karena dapat diintegrasikan pada hari yang berbeda dan tidak memiliki masalah. Menurut penulis, hal ini terjadi karena proses yang dilakukan hanya sekedar melakukan pencarian data yang telah ada kemudain ditampilkan dalam bentuk visualisasi, tidak ada proses perhitungan matematika ataupun statistika.

4.2 Visualisasi Log Firewall dengan Clustering

Penulis membuat klasterisasi untuk visualisasi dengan *cluster* dari *Log Firewall* berdasarkan field "_time" dan "app:subcategory". Kedua bagian tersebut dipilih dengan harapan penulis akan mendapatkan kecenderungan user dalam menggunakan aplikasi berdasarkan waktu membukanya. Pada *field* "app:subcategory" hanya dipilih 4 kategori dari aplikasi yang dianggap mewakili untuk tujuan mempermudah dalam mengetahui kecenderungan *user*. Dalam penerapan *cluster* memanfaatkan fitur *Smart Cluster*, berikut merupakan *Rule* yang digunakan:

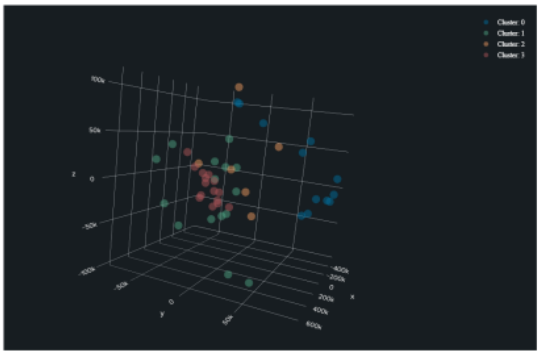
```
index=* sourcetype="pan:traffic"
| chart count over app:technology by action
```

Gambar 15. Rule Splunk Web Login Attemps

Dari hasil *Rule* tersebut, berikut merupakan visualisasi yang dihasilkan pada dua hari yang berbeda:

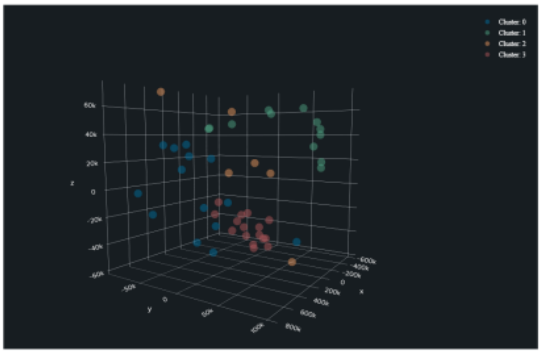
Tabel 4. CLUSTER PADA RABU, 28 OKTOBER 2020

Waktu	Rabu, 28 Oktober 2020
Data Size	40.8 GB
Total Events	104.484.528 events
Problems	Tidak ada



Tabel 5. CLUSTER PADA JUM'AT, 06 NOVEMBER 2020

Waktu	Jum'at, 06 November 2020
Data Size	43,3 GB
Total Events	111.866.547 events
Problems	*Missing Value*



Dari hasil pengujian, dapat disimpulkan bahwa *Rule* yang telah ditetapkan tidak bersifat *universal*. Karena tidak dapat diintegrasikan pada hari yang berbeda dan memiliki masalah yaitu terdapat *field* yang tidak tersedia. Menurut penulis, fields yang ditampilkan adalah sesuai dengan data yang terbesar. Sehingga apabila *fields* yang diinginkan tidak terdapat pada pembacaan data saat pengolahan dengan *machine learning*. Maka akan terjadi error berupa *missing value*.

4.3 Integrasi Alert dengan both Telegram

Untuk integrasi *Alert* dengan *Both* Telegram, penulis membuat tiga Jenis *Alert*. Bagian *Alert* yang pertama adalah mendeteksi upaya masuk yang tidak sah pada akun *Splunk Web*. Bagian *Alert* yang kedua adalah memberitahu informasi jumlah pengguna apabila melebihi batas dari pengguna seharusnya dalam kurun waktu yang telah ditentukan. Bagian *Alert* yang ketiga adalah mendeteksi serangan *Brute Force*. Berikut merupakan *Rule* yang digunakan pada bagian pertama:

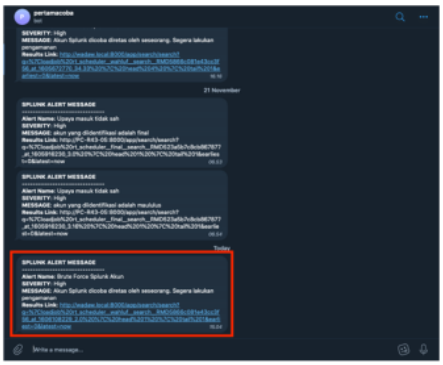
```
index=* sourcetype="pan:traffic"
| chart count over app:technology by action
```

Gambar 16. Rule Splunk Web Login Attemps

Berikut merupakan *Rule* yang memicu kapan *Alert* akan dikirimkan pada bagian pertama:

Gambar 17. *Rule* pemicu agar *Alert terkirim*

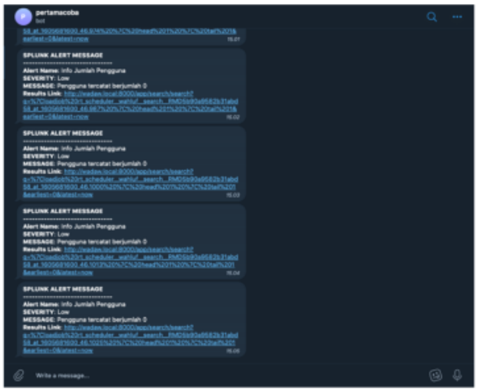
Kemudian penulis mencoba melakukan kesalahan selama empat kali dalam kurun waktu satu menit saat melakukan *log-in*, Hasil dari percobaan tersebut adalah:



Gambar 18. *Notifikasi* pada *both* Telegram

Pada bagian *Alert* yang kedua, hasilnya tidak muncul. Hal ini terjadi karena data yang akan dibaca adalah bersifat saat ini (*present)* dan yang akan datang (*future*). Karena data *Log*

Firewall yang penulis gunakan merupakan data yang telah lalu, maka penulis merubah pengaturan pada bagian "*Trigger Alert When*" menjadi "*Per-result*", hasilnya sebagai berikut:



Gambar 19. Notifikasi Jumlah Pengguna

Alert memberikan notifikasi ke *both* Telegram, namun user yang terdeteksi adalah nol. Hal tersebut terjadi karena deteksi dilakukan secara *Real-Time*, maka tidak ada data yang dibaca sehingga data *user* berjumlah nol. Untuk pengujian pada bagian *Alert* yang ketiga adalah hampir sama seperti kasus pada bagian kedua. Mendapatkan hasil nol.

5 Kesimpulan

Berdasarkan hasil penelitian yang telah penulis lakukan, masih banyak sekali kekurangan yang dilakukan oleh penulis. Namun penulis dapat menarik kesimpulan bahwa penerapan teknologi *Security Information and Event Management* dengan *tools* Splunk pada level organisasi yang telah menerapkan sistem *enterprise* sangatlah dibutuhkan. Selain dapat memudahkan *administrator* dalam memahami dan menerima informasi mengenai *traffic* yang terjadi secara *real-time.* Penerapan teknologi SIEM akan dapat memberi banyak masukkan bagi pihak-pihak yang memiliki kepentingan dalam menentukan kebijakan, sebab trend penggunaan perangkat pintar kian meningkat. Hal ini menyebabkan informasi-informasi terkait kebiasaan pengguna dapat lebih banyak diperoleh pada jaringan UII.

6 References

[1] A. BSI, "Sekilas Tentang BSI," 2017. https://bsi.uii.ac.id/sekilas-bsi/ (accessed Sep. 10, 2020).

[2] H. Azaim and W. Nuryanto, "Mengenal Confidentiality, Integrity, dan Availability Pada Keamanan Informasi," *Netsec.Id*, 2017. https://netsec.id/confidentiality-integrity-availability-keamanan-informasi/ (accessed Nov. 10, 2020).

[3] Cloudflare, "What Is a Next-Generation Firewall (NGFW)? | NGFW vs. FWaaS," *CloudFlare*, 2020. https://www.cloudflare.com/learning/cloud/what-is-a-next-generation-firewall/ (accessed Nov. 10, 2020).

[4] S. Perciballi, "Design Correlation Rules to Get the Most Out of Your SIEM," *Paloalto Network*, 2015. https://blog.paloaltonetworks.com/2015/08/design-correlation-rules-to-get-the-most-out-of-your-siem/ (accessed Sep. 10, 2020).

[5] Y. B. Erwinsyah, "KONSOLIDASI dan VISUALISASI LOG SERVER BSI UII MENGGUNAKAN ELK STACK," p. 15523249, 2019.

[6] J. Chancey and J. Penn, "ANALYTICSDRIVEN SECURITY POWERS NEXT GENERATION SIEMS," Accenture, Dublin, 2018.

[7] Splunk, "Splunk® Machine Learning Toolkit User Guide 5.2.0," *Splunk Inc*, 2020. https://docs.splunk.com/Documentation/MLApp/5.2.0/User/WelcometoMLTK (accessed Sep. 10, 2020).

[8] D. Brown, "Finding Bad with Splunk," *SANS.edu*, 2016.

[9] N. Cisco, "Pendahuluan Tentang Keamanan Cyber," 2020. http://static-course-assets.s3.amazonaws.com/CyberSec2.1/id/index.html#1.2.1.2 (accessed Nov. 12, 2020).

[10] A. Haikal, "Pentingnya IT Risk Management Dalam Mendukung Keberlangsungan Bisnis," 2017. https://netsec.id/pentingnya-it-risk-management/ (accessed Nov. 13, 2020).

[11] T. Efrain, J. E. Aronson, and T. P. Lian, *Decision Support Systems and Intelligent Systems Edisi Bahasa Indonesia Jilid 1*. Yogyakarta: Andi, 2005.

[12] Cloudflare, "What Is a Next-Generation Firewall (NGFW)? | NGFW vs. FWaaS," 2020. https://www.cloudflare.com/learning/cloud/what-is-a-next-generation-firewall/ (accessed Nov. 13, 2020).

[13] F. C. Wulur and I. Sembiring, "Klasifikasi Alert pada Intrusion Detection System Menggunakan Algoritma K-Means," no. December, pp. 2–4, 2015.

[14] Rakhmadhani, Syaifuddin, and Z. Sari, "INTEGRASI VISUALISASI MODERN HONEY NETWORK (MHN) DENGAN SPLUNK," *SENTRA 2019*, pp. 167–172, 2019.

[15] I. Anastasov and D. Davcev, "SIEM implementation for global and distributed environments," *2014 World Congr. Comput. Appl. Inf. Syst. WCCAIS 2014*, 2014, doi: 10.1109/WCCAIS.2014.6916651.

Implementasi Splunk dalam Membangun Security Information and Event Management Berdasarkan Log Firewall (studi kasus: Jaringan UII)

ORIGINALITY REPORT

8%	8%	1%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	medium.com Internet Source	3%
2	sistemasi.ftik.unisi.ac.id Internet Source	1%
3	www.thepcinsider.com Internet Source	<1%
4	dspace.uii.ac.id Internet Source	<1%
5	accounting.binus.ac.id Internet Source	<1%
6	bsi.uii.ac.id Internet Source	<1%
7	aliyhafiz.com Internet Source	<1%
8	repository.its.ac.id Internet Source	<1%

9	repository.uksw.edu Internet Source	<1%
10	Muhammad Rafi Muttaqin, Meriska Defriani. "Algoritma K-Means untuk Pengelompokan Topik Skripsi Mahasiswa", ILKOM Jurnal Ilmiah, 2020 Publication	<1%
11	underpapers.blogspot.com Internet Source	<1%
12	pitajepang.wordpress.com Internet Source	<1%
13	iia-indonesia.org Internet Source	<1%
14	software.10terbaik.com Internet Source	<1%
15	www.scribd.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		