IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN SPLUNK UNTUK ANALISIS TREN ANCAMAN SIBER PADA JARINGAN UII

Disusun Oleh:

N a m a : Muhammad Rijal Kamal
NIM : 17523098

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2022

HALAMAN PENGESAHAN DOSEN PEMBIMBING

IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN SPLUNK UNTUK ANALISIS TREN SERANGAN SIBER PADA JARINGAN UII

TUGAS AKHIR

Disusun Oleh:

N a m a : Muhammad Rijal Kamal
NIM : 17523098

Yogyakarta, 22 Juli 2022
Pembimbing,

(Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D.)

HALAMAN PENGESAHAN DOSEN PENGUJI

IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN SPLUNK UNTUK ANALISIS TREN SERANGAN SIBER PADA JARINGAN UII

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia
Yogyakarta, Juli 2022

Tim Penguji

Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D. _____

Anggota 1

Dr. Ahmad Luthfi, S.Kom., M.Kom. _____

Anggota 2

Erika Ramadhani, S.T., M.Eng. _____

Mengetahui,
Ketua Program Studi Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Muhammad Rijal Kamal
NIM : 17523098

Tugas akhir dengan judul:

IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) DENGAN SPLUNK UNTUK ANALISIS TREN SERANGAN SIBER PADA JARINGAN UII

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, Juli 2022

(Muhammad Rijal Kamal)

HALAMAN PERSEMBAHAN

Laporan tugas akhir ini saya persembahkan untuk:

Yang Maha Pengasih lagi Maha Penyayang,
Allah ta'ala

Kedua orang tua saya,
Bapak Agus Sulastomo dan (Almh) Ibu Siti Arofatus Syangidah

Adik-adik saya,
Raisya Dyah Yumna dan Riasta Rahma Hayati

HALAMAN MOTO

“Barangsiapa yang menempuh suatu jalan untuk menempuh ilmu, Allah akan mudahkan baginya jalan ke surga” (HR Muslim)

“Maka sesungguhnya beserta kesulitan ada kemudahan” (QS al-Insyirah ayat 5)

“Berpikirlah positif, tidak peduli seberapa keras hidupmu” (Ali bin Abi Thalib)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Alhamdulillah, puji dan syukur penulis panjatkan ke hadirat Allah ta'ala yang telah memberikan rahmat, hidayah, serta karunia-Nya, sehingga laporan tugas akhir yang berjudul "Implementasi *Security Information and Event Management* (SIEM) dengan Splunk untuk Analisis Tren Serangan Siber pada Jaringan UII" dapat diselesaikan.

Laporan tugas akhir ini merupakan salah satu syarat untuk memperoleh gelas Sarjana Strata-1 (S1) pada Program Studi Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia. Penulis mendapatkan bimbingan, motivasi, dukungan, semangat, dan doa dalam penyusunannya. Oleh karena itu, penulis ucapkan terima kasih kepada:

1. Bapak Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D. selaku dosen pembimbing penelitian yang telah banyak memberikan bantuan, arahan, dan bimbingan untuk penelitian tugas akhir ini.
2. Orang tua penulis, Bapak Agus Sulastomo dan Almarhumah Ibu Siti Arofatus Syangidah atas segala hal yang telah diberikan kepada penulis.
3. Kedua saudara, Raisya Dyah Yumna dan Riasta Rahma Hayati atas dukungan dan doa yang diberikan.
4. Teman-teman Program Studi Informatika angkatan 2017.
5. Serta teman-teman dan saudara-saudara saya yang tidak dapat saya sebutkan satu per satu.

Penulis memohon maaf karena laporan tugas akhir ini masih jauh dari kata sempurna. Akan tetapi, penulis harap dengan adanya laporan tugas akhir ini dapat bermanfaat bagi banyak orang.

Yogyakarta, 20 Juli 2022

(Muhammad Rijal Kamal)

SARI

Ancaman serangan siber semakin meningkat seiring berkembangnya teknologi informasi. Pada bulan Februari 2022 lalu, ditemukan celah keamanan pada salah satu situs web UII yang kemudian disalahgunakan oleh pihak yang tidak bertanggung jawab. Hal tersebut membuat nama UII mendapat reputasi buruk karena salah satu situsnya digunakan untuk menyerang situs lain di luar UII. Badan Sistem Informasi UII memiliki *next-generation firewall (*NGFW*)* sebagai salah satu usaha pengamanan jaringan. Firewall mencatatkan setiap ancaman dan serangan yang masuk ke jaringan UII pada *log firewall*. Perlu adanya analisis terhadap tren ancaman siber dengan mengolah *log* data *firewall*. Implementasi *Security Information and Management System* (SIEM) ditawarkan sebagai solusi untuk membantu menganalisis tren ancaman dan serangan siber yang ada pada UII dengan cara mengolah *log firewall* dengan tipe *threat*. Log tersebut diolah menggunakan SIEM yaitu Splunk yang mendukung pengolahan data secara besar karena log yang dihasilkan firewall UII cukup besar. Log diunggah dan dilakukan pencarian data sesuai *rules*, kemudian hasil pencarian akan divisualisasikan dan ditampilkan pada *dashboard*. Adanya analisis tren ancaman siber diharapkan akan membantu mengetahui bahaya apa saja yang sering mengancam jaringan UII dan juga sebagai alat untuk memprediksi ancaman dan serangan yang akan datang.

Kata kunci: SIEM, threat, firewall, log, vulnerability.

GLOSARIUM

Event	sebuah data catatan aktivitas atau peristiwa pada log firewall atau Splunk
Firewall	sistem keamanan jaringan yang melindungi jaringan computer dari ancaman dan serangan siber serta mengatur setiap trafik yang keluar dan masuk jaringan
Log	*file* data yang berisi catatan aktivitas atau operasi yang dilakukan oleh sebuah aplikasi, sistem, server, dan perangkat lainnya
Rules	seperangkat aturan yang digunakan untuk melakukan sebuah tindakan tertentu pada perangkat *firewall* maupun Splunk
SIEM	*Security Information and Event Management* (SIEM) adalah sistem informasi terpusat yang digunakan untuk mengmpulkan *log* data, mengolah data, serta menampilkan hasil pengolahan *log* data untuk membantu manajemen dan pemantauan *log* data
Threat	ancaman terhadap keamanan jaringan akibat adanya celah keamanan
Vulnerability	celah keamanan pada sebuah program atau sistem yang memungkinkan adanya akses tanpa izin dengan mengekploitasi celah yang ada

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

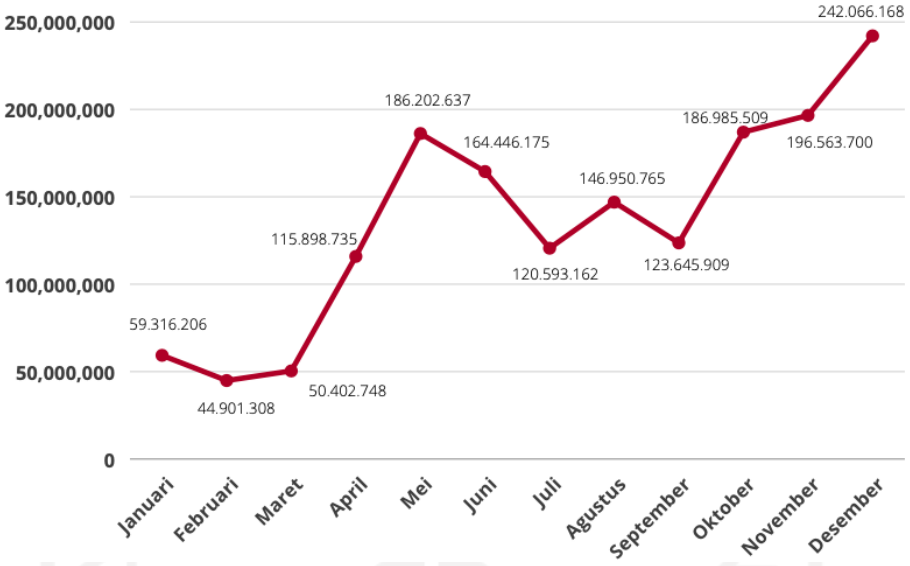
BAB I
PENDAHULUAN

1.1 Latar Belakang

Ancaman serangan siber semakin besar seiring berkembangnya teknologi informasi. *Malicious software* (*malware*) adalah salah satu ancaman keamanan siber yang berupa kode berbahaya yang ditanam dan digunakan untuk mengeksploitasi celah keamanan pada sistem, situs web, aplikasi, maupun jaringan. Vulnerability atau celah keamanan merupakan kesalahan kode atau konfigurasi pada sistem operasi maupun perangkat lunak. Celah inilah yang nantinya dieksploitasi oleh orang yang tidak bertanggungjawab untuk tujuan yang dapat merugikan.

Di Universitas Islam Indonesia (UII) setidaknya terdapat sekitar 200 situs web. Pada sekitar bulan februari 2022, ditemukan celah keamanan pada salah satu situs web yang ada di UII. Celah keamanan tersebut digunakan oleh orang yang tidak bertanggungjawab untuk menyerang web lain di luar UII sehingga domain uii.ac.id diblokir oleh vendor karena telah dilaporkan atas tindak kejahatan oleh pemilik web yang diserang dan menyebabkan beberapa layanan di UII tidak dapat berjalan dengan lancar. Oleh karena itu, UII mendapat reputasi buruk karena salah satu alamat web-nya digunakan untuk menyerang situs web lain.

Menurut Laporan Tahunan Monitoring Keamanan Siber 2021 yang dikeluarkan oleh Badan Siber dan Sandi Negara, terjadi tren kenaikan pada statistik *monitoring* trafik anomali selama tahun 2021 seperti yang dapat dilihat pada gambar 1.1. Dari hasil tersebut didapatkan alamat IP sumber dan tujuan anomali. Anomali yang sangat masif hingga mencapai jutaan trafik dalam waktu satu bulan ditunjukan oleh aktivitas beberapa alamat IP. Banyaknya anomali ini dalam waktu singkat ini dapat disebabkan oleh aktivitas ZBot, trojan, dan malware lainnya.



Gambar 1.1Trafik anomali di Indonesia

Melihat jumlah ancaman serangan siber dan perkembangan jenis ancaman yang sangat cepat, sangat penting bagi penyedia layanan dengan teknologi informasi untuk selalu update tren ancaman dan serangan siber. Khususnya di UII yang menaungi 30.000 pengguna layanan teknologi informasi yang dikelola oleh Badan Sistem Informasi (BSI), untuk dapat menjaga dan menjamin kerahasiaan, integritas, dan ketersediaan data. Hal tersebut dimaksudkan untuk meminimalisir risiko ancaman serangan siber yang ada di jaringan UII. Menurut Peraturan Rektor UII no 15 tahun 2020 tentang kebijakan teknologi informasi di lingkungan UII, menyatakan prinsip pada bagian kebijakan keamanan bahwa pemangku kepentingan berkewajiban turut serta dalam memastikan lingkungan kerja berbantuan teknologi agar tetap aman dan nyaman dengan melaporkan setiap celah keamanan di dalam sistem yang ditemukan, risiko-risiko terhadap sistem dan peretasan sistem keamanan sesuai dengan ketentuan dalam peraturan, dan UII memberikan jaminan ketersediaan sistem dan asset informasi yang diperlukan oleh pemangku kepentingan sesuai dengan peraturan.

Sebagai upaya menjaga keamanan jaringannya, BSI telah mengimplementasikan *Next-Generation Firewall* (NGFW) yaitu dari Palo Alto Network. *Firewall* merupakan sistem keamanan yang melindungi jaringan komputer dari berbagai ancaman dan serangan siber. *Firewall* inilah yang mengatur informasi, data, dan kegiatan yang boleh masuk atau keluar jaringan dan mencatatkan setiap kegiatannya pada log data. *Firewall* Palo Alto mencatatkan setiap ancaman serangan, waktu dan *URL* serangan, sumber dan tujuan serangan, *IP address*, aturan keamanan, dan *severity level* setiap serangan pada log dengan tipe *threat*. Perlu adanya

analisis terhadap *threat log* ini untuk mengetahui tren ancaman dan serangan yang masuk ke jaringan UII. Hal ini dimaksudkan untuk memprediksi serangan yang akan terjadi di masa yang akan datang, sekaligus menjadi langkah meminimalisir risiko, pencegahan dan mitigasi serangan siber.

Pada penelitian ini, penulis bermaksud untuk mengolah *threat log* yang dihasilkan *firewall* milik BSI UII untuk membantu analisis tren ancaman serangan siber. Log ini akan diolah dengan mengimplementasikan *Security Information and Event Management* (SIEM). SIEM merupakan sistem informasi terpusat dan digunakan untuk mengumpulkan log yang nantinya memberikan hasil berupa visualisasi log monitoring untuk mempermudah pembacaan informasi pada log. *Tools* SIEM yang akan digunakan pada penelitian ini adalah Splunk. Splunk merupakan *next-generation* SIEM *product* yang mendukung penerapan data mining untuk mengelola log firewall sehingga visualisasi data dalam jumlah besar mudah untuk dipahami.

1.2 Rumusan Masalah

Dari latar belakang yang telah diuraikan, maka didapatkan rumusan masalah pada penelitian ini adalah bagaimana implementasi SIEM untuk membantu menganalisis tren ancaman serangan siber berdasarkan *log firewall* pada jaringan UII?

1.3 Tujuan Penelitian

Tujuan yang dicapai pada penelitian ini adalah:

a. Mengimplementasikan *Security Information and Event Management* (SIEM) Splunk untuk membangun *dashboard* visualisasi dari *log firewall threat type* jaringan UII.
b. Menganalisis tren serangan siber pada jaringan UII.

1.4 Manfaat Penelitian

Dengan adanya penelitian diharapkan akan memberikan manfaat untuk:

a. Membantu proses pengolahan *log firewall*.
b. Mempermudah pembacaan *log firewall* dan analisis tren serangan siber.

1.5 Batasan Penelitian

Pada penelitian ini terdapat beberapa batasan masalah, antara lain:

a. SIEM yang digunakan pada penelitian ini adalah Splunk.

b. Data penelitian berasal dari *Log Firewall* yang diberikan oleh Badan Sistem Informasi (BSI) Universitas Islam Indonesia.
c. *Log Firewall* yang digunakan adalah log Palo Alto Network dengan tipe *threat*.

1.6 Metode Penelitian

Metode penelitian yang digunakan pada penelitian ini sebagai berikut:

1.6.1 Kajian Pustaka

Kajian pustaka dilakukan untuk mengidentifikasi masalah, mencari referensi dan landasan teori pada penelitian ini. Kajian pustaka dilakukan dengan cara mencari dan mengkaji jurnal, makalah, artikel, maupun penelitian yang sejenis.

1.6.2 Perencanaan Penelitian

Perencanaan penelitian dilakukan secara mendalam untuk mendapatkan solusi dari permasalahan. Proses perencanaan ini meliputi pencarian serta pemilihan sumber dan pustaka, teknologi yang digunakan, serta alat yang digunakan dalam penelitian.

1.6.3 Pengumpulan Data

Data yang digunakan dalam penelitian merupakan data sekunder yang berasal dari data yang tercatat pada *log firewall* yang diberikan oleh Badan Sistem Informasi (BSI) Universitas Islam Indonesia selama satu bulan penuh. Data *log firewall* yang digunakan bertipe *threat log*.

1.6.4 Implementasi

Implementasi dimulai dengan instalasi alat dan aplikasi yang dibutuhkan, mengunggah data *log firewall*, melakukan konfigurasi serta pencarian pada data *log firewall* dan membangun *dashboard* untuk menampilkan hasil pencarian.

1.6.5 Pengujian

Menguji kesesuaian hasil konfigurasi SIEM, pencarian dan pengolahan data, serta tampilan dashboard.

1.6.6 Analisis

Analisis dilakukan dengan mengamati hasil pencarian yang sudah ditampilkan pada dashboard.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir disusun menjadi lima bagian yang terdiri dari:

BAB I PENDAHULUAN, berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian,

BAB II LANDASAN TEORI, berisi teori dasar dan kajian pustaka yang berkaitan dengan tema penelitian untuk merancang dan membangun konsep penelitian.

BAB III METODOLOGI PENELITIAN, berisi proses yang dilakukan pada penelitian mulai dari mengkaji pustaka, melakukan perencanan, mengumpulkan data penelitian, serta analisis dari hasil penelitian.

BAB IV HASIL DAN PEMBAHASAN, berisi hasil dan pembahasan dari penelitian.

BAB V KESIMPULAN DAN SARAN, berisi kesimpulan dari hasil penelitian dan saran untuk penelitian sejenis.

BAB II
LANDASAN TEORI

2.1 Landasan Teori

2.1.1 Keamanan Informasi

Keamanan informasi merupakan aktivitas pengamanan yang ditujukan untuk melindungi informasi dan rahasia perusahaan dari berbagai ancaman serta menjamin kelangsungan bisnis dan meminimalisir resiko yang ada. Tujuan utama dari adanya keamanan informasi adalah untuk mengamankan segala informasi yang ada pada infrastruktur teknologi informasi maupun sistem informasi dari berbagai macam serangan agar tidak disalahgunakan.

Semakin banyak data yang dimiliki oleh suatu perusahaan maka semakin besar pula ancaman dan resiko yang dapat mengakibatkan informasi tersebut diakses oleh pihak yang tidak sah, penyalahgunaan informasi, kehilangan informasi, kerusakan informasi, dan modifikasi informasi. Terdapat 3 aspek penting yang dalam keamanan informasi, yaitu:

a. Kerahasiaan (*Confidentiality*)

   Rahasia atau privasi hendaknya hanya pihak tertentu saja yang mengetahui rahasia itu. Dalam keamanan informasi, aspek kerahasiaan ini adalah bagaimana suatu data atau informasi hanya dapat diakses oleh pihak yang berwenang atau memiliki akses terhadap informasi tersebut. Untuk menjaga kerahasiaan informasi, suatu perusahaan bisa menggunakan berbagai cara seperti meminimalisir penyebaran informasi sensitif, melakukan enkripsi data, memberi ID dan kata sandi untuk pengguna, menggunakan autentikasi beberapa factor. Meskipun demikian, informasi masih dapat diakses oleh pihak yang tidak berwenang karena kelalaian atau kecerobohan pengguna serta tingkat pengamanan yang lemah.

b. Integritas (Integrity)

   Integritas atau keandalan adalah bagaimana menjaga keutuhan, kualitas, dan keaslian data. Data atau informasi tidak boleh diubah atau dimanipulasi oleh pihak yang tidak berwenang. Dalam menjaga integritas data tidak hanya menjaganya dari serangan yang dilakukan pihak lain tapi juga mencegah perubahan data akibat dari kesalahan pengguna. Beberapa cara yang dapat digunakan untuk mencegah data diubah oleh pihak yang tidak berwenang atau mengembalikan data yang diubah oleh pihak yang

tidak berwenang bisa dilakukan dengan cara memperketat autentikasi, melakukan validasi saat memasukan data, mengecek dan mengontrol akses pengguna.

c. Ketersediaan (Availability)

Ketersediaan adalah menjamin data atau informasi tetap bisa diakses pihak yang berwenang saat dibutuhkan. Untuk menjaga ketersediaan data maka suatu perusahaan perlu memerlukan pemeliharaan terhadap perangkat dan peralatan, melakukan *update* perangkat lunak, memasang perangkat pengamanan baik perangkat keras maupun perangkat lunak.

2.1.2 Keamanan Siber

Keamanan siber adalah aktivitas yang ditujukan untuk melindungi sistem jaringan dari penyusupan, akuisisi maupun eksploitasi berbahaya. Keamanan siber ini bisa dimulai dari tingkat individu dengan mengamankan data atau perangkat pribadi. Kemudian pada tingkat perusahaan, perusahaan wajib menyediakan perlindungan data konsumen dan memastikan keberlangsungan bisnisnya. Sampai pada tingkat pemerintah atau negara, maka pemerintah harus menjamin keamanan data milik setiap warga dan mencegah tersebarnya informasi yang tidak valid ke masyarakat.

Keamanan siber merupakan bagian dari keamanan informasi. Mulai dari individu, perusahaan, dan negara tentu akan menghadapi ancaman dan risiko yang beragam tergantung informasi apa yang mereka miliki dan proses serta apa maksud tujuannya dan bagaimana caranya. Misalnya risiko dalam bidang pelayanan masyarakat seperti rumah sakit, data riwayat kesehatan pasien memiliki risiko penyalahgunaan pada keamanan siber daripada data pribadi karyawannya. Atau pada perusahaan investasi keuangan risiki tertinggi yang ada bisa jadi pada pencurian atau manipulasi pasar investasi bukan pada kebocoran data karyawan.

2.1.3 Ancaman Siber

Jaringan komputer merupakan kumpulan komponen-komponen IT yang saling terhubung satu sama lain dan membuat layanan IT dapat berjalan dalam suatu organisasi atau perusahaan. Jaringan inilah yang menjalankan segala macam proses bisnis yang ada pada perusahaan. Infrastruktur jaringan memiliki nilai dan informasi penting yang harus dilindungi dari ancaman serangan siber. Berikut merupakan beberapa contoh Iancaman serangan siber:

a. Distributed Denial of Service (DDoS Attack)

DDos Attack merupakan ancaman siber yang dirancang untuk membajiri trafik atau sumber daya jaringan sehingga dampaknya jaringan akan mengalami *down*.

b. Ransomware

Ransomware merupakan salah satu jenis malicious software yang menyerang perangkat korban dengan cara menenkripsi data informasi pada file sehingga file tidak dapat dibaca maupun diakses oleh pemiliknya.

c. Phising

Serangan siber yang dilakukan dengan cara mengelabui korban dengan memanipulasi psikologisnya untuk mendapatkan informasi atau data penting dari korban. Data yang menjadi sasaran ini dapat berupa data pribadi, data suatu akun, maupun data untuk finansial.

d. Vulnerability Exploitation

Serangan dengan memanfaatkan suatu kerentanan pada sistem untuk dieksploitasi dengan *malware*, *script*, maupun *open-source exploit kit*.

e. Cryptojacking

Cryptojacking atau malicious cryptomining merupakan ancaman jaringan yang bersembunyi pada perangkat korban dengan tujuan untuk menjadikan computer perangkat sebagai mesin penambang mata uang digital

2.1.4 IT Security Risk Management

Risiko adalah ukuran sejauh mana sumber daya informasi terekspos berdasarkan eksploitasi celah keamanan oleh potensi ancaman. Manajemen risiko pada keamanan IT adalah proses mengidentifikasi risiko keamanan yang ada pada suatu organisasi dan mengambil tindakan untuk meminimalisir risiko tersebut. Tindakan yang diambil mulai dari pada penggunaan perangkat keras, perangkat lunak, maupun memberikan pelatihan pekerja untuk menjaga lingkungan siber aman dari berbagai macam ancaman. Manajemen risiko pada teknologi informasi dilakukan untuk menjaga *Confidentiality*, *Integrity*, dan *Availability* dengan meminimalisir dampak yang akan muncul dan memberikan efek pada *Confidentiality* dari informasi, *Integrity* dari data yang ada pada sistem, dan *Availability* yang berasal dari infrastruktur sistem.

2.1.5 Risk Assesment

Penilaian risiko atau risk assessment pada keamanan siber merupakan bagian penting dari proses manajemen risiko suatu perusahaan. Risiko memiliki dua komponen yaitu dampak celah keamanan yang dieksploitasi terhadap jalannya bisnis perusahaan dan kemungkinan terjadinya serangan atau eksploitasi tersebut. Proses ini bertujuan untuk menganalisis dan menguraikan risiko terkait dengan potensi ancaman dan celah keamanan yang ada.

A. Membangun Konteks Penilaian Risiko

Selama penilaian risiko sangat penting untuk menentukan konteks bisnis maupun teknis dari sistem informasi yang ditinjau. Menetapkan konteks penilaian risiko ditujukan untuk memastikan bahwa tujuan dari bisnis sudah dipahami dengan baik serta mempertimbangkan faktor internal dan eksternal yang bisa mempengaruhi risiko. Proses ini juga ditujukan untuk mengetahui lingkup dan batasan dari proses penilaian risiko.

B. Mengidentifikiasi Risiko (*Risk Identification*)

Tahap identifikasi risiko bertujuan untuk membuat daftar lengkap mengenai kejadian-kejadian yang dapat mencegah, menurunkan, atau menunda tercapainya tujuan bisnis. Identifikasi yang komprehensif sangat dibutuhkan karena risiko yang tidak teridentifikasi pada tahap ini tidak akan dimasukkan pada tahap analisis risiko. Untuk mengelola risiko yang ada juga perlu dilakukan identifikasi terhadap potensi ancaman yang ada pada sistem informasi yang ada. Identifikasi ancaman dapat dilakukan dengan mendefinisikan scenario risiko. Scenario risiko adalah sebuah metode yang dapat menentukan ada atau tidaknya risiko yang dapat mempengaruhi *confidentiality*, *integrity*, dan *availability* pada sistem informasi dan oleh karenanya dapat mempengaruhi tujuan dari bisnis.

C. Menganalisis Risiko (*Risk Analysis*)

Setelah risiko yang relevan dapat teridentifikasi, kemungkinan dan dampak yang akan terjadi diberi nilai dan peringkat atau level. Biasanya kemungkinan dan dampak dari suatu risiko dinilai dengan menggunakan skala kualitatif.

D. Mengevaluasi Risiko (*Risk Evaluation*)

Evaluasi risiko bertujuan untuk membantu pemilik dari suatu bisnis atau perusahaan dalam membuat keputusan terkait risiko mana saja yang memerlukan perlakuan khusus dan menentukan prioritas untuk penerapan tindakan terhadap risiko yang ada.

E. Perlakuan terhadap Risiko (*Risk Treatment*)

Pemilik bisnis atau pihak yang berwenang dapat memilih tindakan untuk menghindari, menangani, mentransfer, atau menerima risiko yang ada. Maksud dari tindakan tersebut adalah:

Menghindari risiko (*Avoid*) – menghentikan aktivitas yang menimbulkan risiko atau bahkan menghilangkan risiko yang ada.

Memperlakukan risiko (*Treat*) – menerapkan suatu aturan atau control untuk mengurangi kemungkinan dan/atau dampak dari risiko yang ada.

Mengalihkan risiko (*Transfer*) – mentransfer atau membagi sebagian atau seluruh dampak dari risiko yang ada kepada pihak ketiga.

Menerima risiko (*Accept*) – pelaku bisnis dapat memilih untuk menerima risiko yang ada. Risiko biasanya diterima ketika dinilai masih dalam tingkat toleransi yang ditetapkan.

F. Pemantauan Risiko (*Monitoring*)

Risiko yang ada akan terus berubah dan berkembang, faktor-faktor yang mempengaruhi kemungkinan dan dampak dari risiko yang terjadi dapat berubah. Oleh karena itu, tinjauan risiko yang berkelanjutan sangat diperlukan sangat penting untuk memastikan bahwa penanganan risiko yang ada tetap efektif. Pemantauan dan peninjauan kembali risiko dilakukan untuk memastikan bahwa kemungkinan dan dampak risiko tidak meningkat. Hasil dari pemantauan dan peninjauan ulang risiko harus menjadi masukan untuk proses manajemen risiko.

2.1.6 *Next-Generation Firewall*

Firewall adalah sistem keamanan yang melindungi jaringan computer dari berbagai ancaman dan serangan siber. *Firewall* inilah yang mengatur informasi, data, dan kegiatan yang boleh masuk dan keluar jaringan. Sedangkan *Next-Generation Firewall* (NGFW) adalah hasil evolusi dari *firewall* generasi pertama. NGFW dibuat karena kebutuhan pada era saat ini, seiring dengan serangan *malware* yang berkembang dalam hal kompleksitas, kekuatan, dan juga metode untuk memanfaatkan celah yang ada pada *firewall* generasi pertama. Karena firewall adalah pertahanan utama terhadap serangan semacam itu dan keberlangsungan sistem sangat penting untuk berjalannya suatu bisnis, maka firewall juga telah maju dan berkembang untuk menghadapi ancaman tersebut. Berikut adalah beberapa perbedaan yang menjadi kelebihan dari NGFW:

a. Pengaturan *non-disruptive*, *in-line*, *bump-in-the-wire* (BITW), maksudnya firewall dapat secara sembunyi-sembunyi hidup di dalam *subnet* sehingga dapat menyaring aktivitas saluran lalu lintas antar *host*.
b. *Intrusion Prevention System* (IPS) dengan *signature-base* yang terintegrasi, yang dapat menunjukkan jenis serangan mana yang harus disaring dan dilaporkan.
c. Dekripsi *Secure Socket Layer* (SSL) untuk memperkuat bukti yang dapat dikenali dari aplikasi tidak diinginkan.
d. Kemampuan untuk memasukkan informasi dari luar, termasuk susunan dengan indeks dan juga pencatatannya.
e. Membuktikan aplikasi yang pernah dikenali sebelumnya menggunakan *signature* aplikasi, memeriksa muatan paket data dan *header inspection*, serta penerapan strategi keamanan jaringan di tingkat aplikasi.

2.1.7 Palo Alto Networks

Palo Alto Networks adalah salah satu penyedia layanan *next-generation firewall*. Palo Alto memberikan solusi untuk mengamankan jaringan melalui aplikasi *firewall* dengan cara:

a. Memblokir ancaman yang diketahui dengan IPS dan *anti-virus/anti-spyware* jaringan.
b. *Malware* yang tidak dikenal diidentifikasi dan dianalisis oleh WildFire, yang secara langsung mengeksekusi dan mengamati file yang tidak dikenal di lingkungan *sandbox* virtual bebasis awan.
c. Mengidentifikasi *host* yang terinfeksi *bot*.
d. Membatasi tranfser file dan data yang tidak terotorisasi.
e. Mengontrol *web surfing*.

Firewall Palo Alto melaporkan dan mencatatkan setiap kegiatannya pada log yang dapat di-*export* ke file CSV atau diteruskan ke *syslog server*. Terdapat beberapa tipe *log* yang dicatatkan oleh *firewall* Palo Alto berdasarkan fungsinya masing-masing, antara lain:

1. *Traffic* – menampilkan catatan untuk setiap awal dan akhir sesi. Setiap catatan mencakup tanggal dan waktu, zona sumber dan tujuan, alamat dan port, nama aturan keamanan yang diterapkan pada trafik (*allow*, *deny*, *drop*), antarmuka keluar dan masuk, jumlah *byte*, dan alasan sesi berakhir.
2. *Threat* – menampilkan catatan alarm keamanan yang dihasilkan *firewall*. Setiap catatan mencakup tanggal dan waktu, zona sumber dan tujuan, alamat dan port, nama

aturan keamanan yang diterapkan pada trafik, tindakan alarm (*allow, block*) dan tingkat bahayanya.

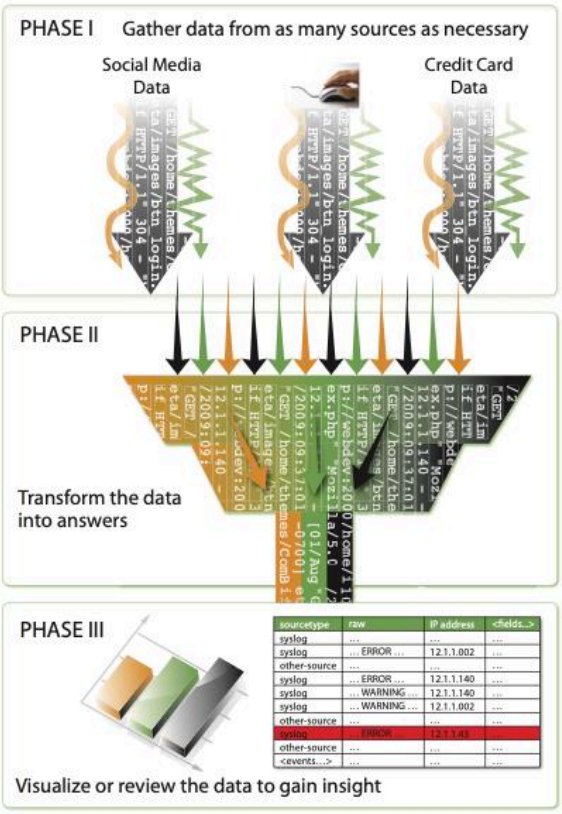
3. *URL Filtering* – menampilkan *log* untuk filter URL yang mengontrol akses ke situs web dan apakah pengguna dapat mengirimkan kredensial ke situs web.
4. *WildFire Submissions* – menampilkan log untuk file dan tautan surel yang diteruskan *firewall* untuk analisis WildFire. WildFire Cloud menganalisis sampel dan mengembalikan hasil analisis, yang mencakup putusan WildFire yang ditetapkan ke sampel (*benign*, *malware*, *greyware*, atau *phishing*). Firewall bisa mengizinkan atau memblokir file berdasarkan aturan kebijakan keamanan dengan melihat kolom *Action*.
5. *Data Filtering* – menampilkan log untuk kebijakan keamanan dengan profil *Data Filtering* yang terlampir, untuk membantu mencegah informasi sensitif seperti kartu kredit atau nomor jaminan sosial meninggalkan area yang dilindungi oleh firewall, dan profil *File Blocking*, yang mencegah jenis file tertentu diunggah atau diunduh.

2.1.8 *Security Information and Event Management*

Security Information and Event Management (SIEM) bertanggung jawab untuk mengumpulkan yang data relevan dengan keamanan secara terpusat untuk mendeteksi adanya ancaman atau insiden serangan. Dengan demikian, SIEM dapat memberikan kemampuan analitik pada keamanan secara *real-time* maupun historis pada kejadian masa lampau dengan menghubungkan beberapa log. Fungsi lebih lanjut dari SIEM adalah untuk pengayaan konteks data, menormalisasi sumber data heterogen, pelaporan, peringatan, dan kemampuan untuk merespons suatu insiden secara otomatis. SIEM memungkinkan pertukaran informasi ancaman maupun serangan siber dengan menyediakan koneksi ke platform yang lain, serta dapat memberikan visualisasi dari analisis jaringan untuk penggunanya. SIEM juga menyediakan kemampuan untuk manajemen log dengan penyimpanan data suatu peristiwa dalam jangka Panjang.

2.1.9 Splunk

Splunk merupakan platform untuk mengolah data, melakukan pencarian, memeriksa, menganalisis, visualisasi data, dan membedah informasi dari kumpulan data. Splunk mendukung pengolahan data dalam skala besar atau *big data*. Selain itu, Splunk juga dapat diintegrasikan dengan aplikasi pendukung lainnya. Gambar 2.1 menunjukkan Langkah atau fase implementasi Splunk.



Gambar 2.1 Tahap Implementasi Splunk

2.2 Kajian Pustaka

Kajian terhadap beberapa pustaka yang disajikan pada Tabel 2.1 berisi tentang uraian singkat mengenai masalah yang ada pada beberapa penelitian dan juga hasil atau solusi yang didapatkan.

Tabel 2.1 Kajian Pustaka

No	Nama Penulis	Uraian Singkat	Hasil
1	Pratama, A. & Wijaya, A (2016)	Peneliti menerapkan SIEM yaitu *OSSIM AlienVault* untuk *monitoring* server jaringan di Universitas Bina Dharma Palembang	Penerapan dapat berjalan dengan baik dan dapat melaporkan ancaman serangan dan dapat dipantau secara *real-time*.
2	Bachane, I. & Adsi, Y.I.K. & Adsi, H.C (2016)	Peneliti bertujuan untuk menyelesaikan kebutuhan forensik pada komputasi awan dengan menerapkan SIEM serta melakukan perbandingan kinerja antara penggunaan SIEM dan *server syslog*.	Investigasi forensik dengan SIEM lebih efektif dibandingkan dengan *server syslog*.

3	Erwinsyah, Y.B (2019)	Penerapan log management system berbasis sumber terbuka, ELK Stack. ELK Stack digunakan untuk manajemen log dan visualisasi log data.	Penerapan ELK Stack untuk manajemen log dan visualisasi log data sudah berhasil dilakuakan.
4	Rakhmadani (2019)	Peneliti melakukan penerapan SIEM Splunk untuk memantu log Modern Honey Network	Hasil penelitian sesuai yang diharapkan yaitu peneliti dapat mengintegrasikan Splunk dengan Honeypot dan hasilnya dapat divisualisasikan serta dapat dipantau untuk setiap serangan yang ada.
5	Arnafudin, C (2019)	Peneliti bermaksud untuk melihat implikasi penerapan SIEM terhadap nilai indeks KAMI. Peneliti juga melakukan simulasi serangan kepada router.	Hasilnya SIEM dapat memberi informasi terkait serangan yang dilakukan, tapi beberapa serangan tidak dapat dikenali oleh SIEM dan penggunaan SIEM ini terbukti menaikkan indeks KAMI.
6	Al-Duwairi, B., Al-Kahla, W., AlRefai, M. A., Abedalqader, Y., Rawash, A., & Fahmawi, R. (2020)	Perangkat IoT memiliki beberapa celah keamanan yang dapat dieksploitasi oleh Botnet IoT. Peneliti coba mengimplementasikan SIEM untuk sistem deteksi dan mitigasi serangan DDoS oleh Botnet IoT. Sistem SIEM dibangun dengan menggunakan Splunk.	Hasil dari penerapan SIEM yang dilakukan menunjukkan bahwa sistem berhasil untuk mengidentifikasi dan memblokir trafik berbahaya yang berasal dari perangkat IoT yang telah disusupi.
7	Abidian, W (2021)	Peneliti mengimplementasikan SIEM yaitu Splunk untuk mengolah *log firewall*, memvisualisasikan data, dan mengintegrasikan dengan *bot telegram*. Penelitian ini menggunakan studi kasus di Universitas Islam Indonesia	*Log* data berhasil diolah dengan dengan SIEM. Peneliti juga berhasil melakuakan klasterisasi data serta menampilkannya di *dashboard* dan mengintegrasikan pelaporan ke *bot telegram*.
8	Dewantara, R & Sugiantoro, B (2021)	Penelitian ini bertujuan untuk menerapkan infrastruktur OSSIM, memantau indeks keamanan menggunakan OSSIM serta mengidentifikasi hasil sebelum dan sesudah penerapan OSSIM terkait indeks KAMI	Indeks KAMI meningkat 25 poin menjadi lebih baik setelah adanya OSSIM.
9	Alfandi, M (2022)	Peneliti mencoba membandingkan performa SIEM yaitu Elasticsearch dan	Simulasi berhasil dilakukan, kedua SIEM dapat melihat informasi serangan yang dilakukan. Dari

		Splunk dengan membuat suatu simulasi serangan	perbandingan performa keduanya, Splunk lebih unggul daripada Elasticsearch dalam *alerting event*.
10	Iqbal, M (2022)	Implementasi Honeypot dan SIEM untuk mendeteksi serangan pada jaringan serta mengkorelasi log dan peristiwa serangan.	Implementasi Honeypot berhasil diimplementasikan untuk mendeteksi serangan yang kemudian log dari serangan tersebut ditampilkan pada SIEM

Dari beberapa jurnal penelitian yang sudah dikaji, didapatkan sebuah solusi dari permasalahan pengolahan data *log firewall* untuk menganalisis tren ancaman serangan siber yaitu dengan penerapan teknologi *Security Information and Event Management* (SIEM). Dan aplikasi atau alat yang dipilih untuk penerapan SIEM ini adalah Splunk yang memungkinkan pengolahan data dalam jumlah besar karena jumlah data untuk *log firewall* Palo Alto dengan tipe *threat* sekitar 2-5 *gigabyte* setiap bulannya.

BAB III
METODOLOGI PENELITIAN

3.1 Sumber Data

Pada penelitian ini menggunakan data sekunder yang merupakan data internal yang dikumpulkan oleh Badan Sistem Informasi Universitas Islam Indonesia. Data yang digunakan berupa *log firewall* dari Palo Alto Network dengan tipe *Threat* yang dikumpulkan selama satu bulan penuh.

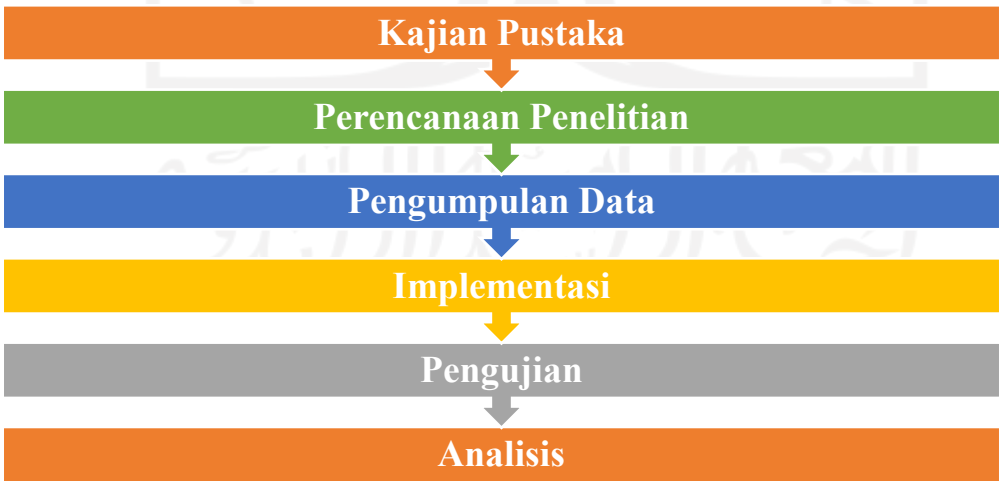
3.2 Indikator Keberhasilan

Penelitian ini memeiliki indicator keberhasilan sebagai berikut:

a. SIEM Splunk dapat mengunggah dan mengolah data log firewall serta mengimplementasikan konfigurasi yang dibuat.
b. Dashboard dapat menampilkan hasil analisis tren serangan siber yang dapat dengan mudah dibaca dan dipahami.

3.3 Metode Penelitian

Pada gambar 3.1 menunjukkan langkah-langkah yang ditempuh pada penelitian ini. Tahapannya dimulai dari kajian pustaka, perencanaan penelitian, pengumpulan data, implementasi, dan analisis hasil.



Gambar 3.1 Metode Penelitian

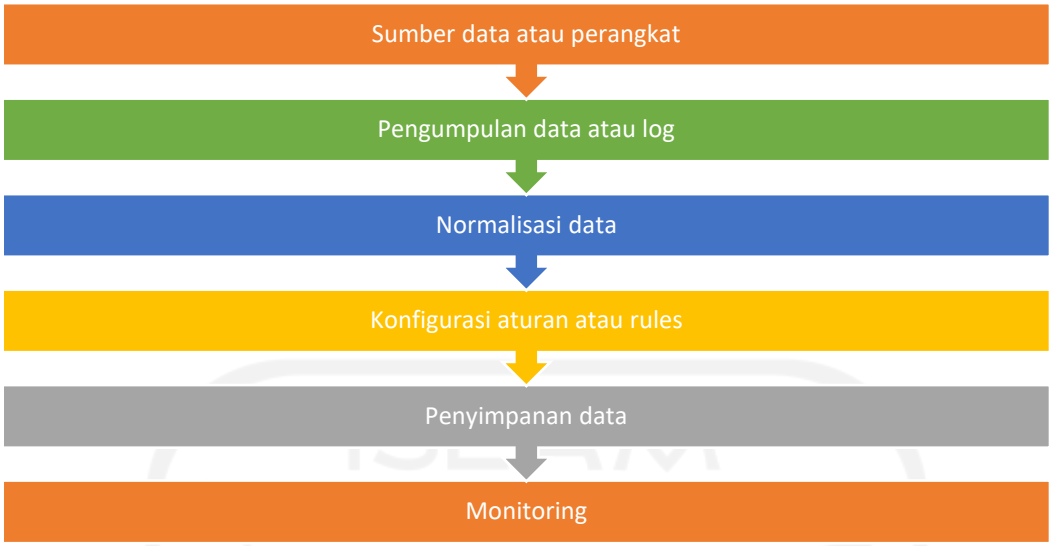
3.3.1 Kajian Pustaka

Penelitian ini dimulai dengan kajian pustaka sebagai langkah awal untuk menentukan permasalahan, mencari referensi terkait permasalahan yang ada, dan juga sebagai dasar landasan teori untuk penelitian. Kajian pustaka juga bertujuan untuk mencari solusi terkait permasalahan yang ada dan menentukan teknologi atau alat yang digunakan untuk pemecahan masalah. Tahapan ini dilakukan dengan cara mengkaji jurnal ilmiah, makalah, artikel, dan penelitian sejenisnya.

3.3.2 Perencanaan Penelitian

Pada tahap ini dilakukan penyusunan rencana untuk pemecahan masalah yang ada, meliputi solusi dari permasalahan, pustaka yang dipakai untuk referensi, teknologi dan alat yang akan digunakan.

Pada penelitian ini, implementasi SIEM ditujukan untuk membantu mengolah *threat log* yang dihasilkan oleh *firewall* milik BSI UII sehingga dapat membantu analisis ancaman serangan pada jaringan. Secara umum, SIEM memiliki kemampuan untuk mengumpulkan, agregasi, menyimpan, dan mengorelasikan *events* yang dihasilkan oleh infrastruktur terkait yang kemudian membentuk suatu platform terpusat untuk sistem keamanan dengan mengumpulkan *events* atau data dari beberapa sumber, mengorelasikan *events* atau data, dan kemudian memberikan suatu *alert* untuk penanganan ancaman serangan dan laporan keamanan. Alur kerja SIEM ditunjukkan pada gambar 3.2, mulai dari sumber data, pengumpulan data, normalisasi data, konfigurasi aturan atau *rules*, penyimpanan data, dan pemantauan data atau *monitoring*.



Gambar 3.2 Alur kerja SIEM

Alat bantu SIEM yang diimplementasikan pada penelitian ini adalah Splunk. Splunk dipilih setelah melakukan kajian terhadap beberapa literatur dengan membandingkan penggunaan SIEM untuk keperluan keamanan jaringan pada beberapa penelitian. Splunk juga memungkinkan untuk melakukan pengolahan data dalam jumlah besar atau *big data* yang memuat jutaan *events* karena log data yang dihasilkan oleh firewall BSI UII berjumlah jutaan dan memiliki ukuran yang besar.

Data yang digunakan berasal dari *threat log* yang dicatatkan oleh firewall milik BSI UII. Log dikumpulkan menggunakan agent yang terinstall pada sistem firewall selama bulan Mei 2022. Pengumpulan data dengan cara forwarding atau mengumpulkan langsung secara real-time tidak dimungkinkan karena akses khusus untuk sistem firewall milik BSI UII. Data *threat log* yang terkumpul berukuran 2,6 *gigabyte* memuat 3.511.236 *events threat*.

Proses normalisasi data dilakukan dengan memecah *log* ke ukuran di bawah 500 *megabyte* karena Splunk Enterprise versi ujicoba hanya memungkinkan mengunggah data atau *log* dengan ukuran maksimal 500 *megabyte* dalam sekali unggah. Proses ini dilakukan dengan menggunakan *tools* "*Split*" yang terdapat pada aplikasi terminal MacOS.

Data yang sudah dinormalisasi atau dipecah kemudian diunggah ke aplikasi Splunk Enterprise. Selanjutnya melakukan konfigurasi aturan dan penyusunan rules yang digunakan untuk analisis ancaman serangan siber. Kebutuhan analisis pada penelitian ini merujuk pada Laporan Kuarter 2 Publik: Monitor Keamanan Cyber yang disusun oleh *Security Operation Center* Badan Sistem Informasi UII.

Hasil pengolahan disimpan dan visualisasi dari rules ditampilkan pada dashboard untuk mempermudah proses pemantauan terkait ancaman serangan siber.

3.3.3 Pengumpulan Data

Data yang digunakan merupakan data sekunder yang diperoleh dari pencatatan *log firewall* dari Palo Alto Network oleh Badan Sistem Informasi Universitas Islam Indonesia. Data *log firewall* yang digunakan dalam penelitian adalah *log* dengan tipe *Threat* yang sudah tercatat selama bulan Mei 2022. Selama bulan Mei 2022, firewall jaringan UII telah mencatatkan 3.511.236 *events threat* yang kemudian dikumpulkan dalam format *.csv*.

3.3.4 Implementasi

Tahap selanjutnya adalah implementasi *Security Information and Event Management* (SIEM) Splunk untuk menganalisis tren serangan siber pada jaringan UII dengan mengolah log firewall. Pada tahap ini terdiri dari beberapa langkah kerja sebagai berikut:

G. Instalasi Splunk Enterprise

Pada penelitian ini, *tools* SIEM yang digunakan adalah Splunk Enterprise versi percobaan yang hanya dapat digunakan selama 60 hari. Untuk kebutuhan jangka panjang aplikasi Splunk wajib untuk berlangganan. Kebutuhan sistem untuk dapat melakukan instalasi Splunk Enterprise adalah sebagaimana ditunjukkan pada Tabel 3.1

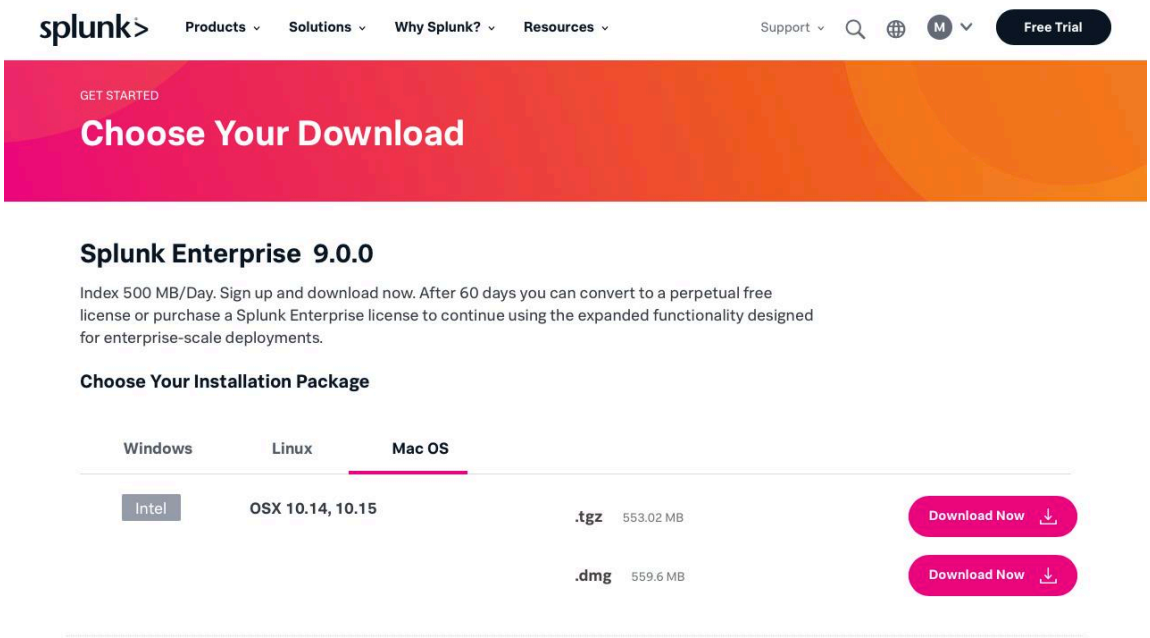
Tabel 3.1 *System Requirements Splunk*

Operating System	macOS / Linux / Windows
Minimum Processing	1,5 GHz
Minimum RAM	512 megabyte
Free Disk Space	5 gigabyte
Web browser	Versi terbaru dari Firefox / Safari / Chrome / Microsoft Edge: Chromunium
Port	8000

Langkah-langkah instalasi Splunk Enterprise adalah sebagai berikut:

6. Mendaftar akun Splunk di situs web splunk.com. Jika sudah masuk dengan akun yang terdaftar.
7. Pilih menu “Free Trial” dan kemudian pilih paket instalasi Splunk Enterprise yang akan diunduh. Pada penelitian ini menggunakan laptop dengan sistem operasi macOS Catalina dengan processor 2,5 GHz Dual-Core Intel Core i5, RAM sebesar 8gigabyte,

dan web browser Safari sehingga menggunakan paket instalasi untuk macOS. Gambar 3.2 menunjukkan halaman web untuk mengunduh paket instalasi Splunk Enterprise.

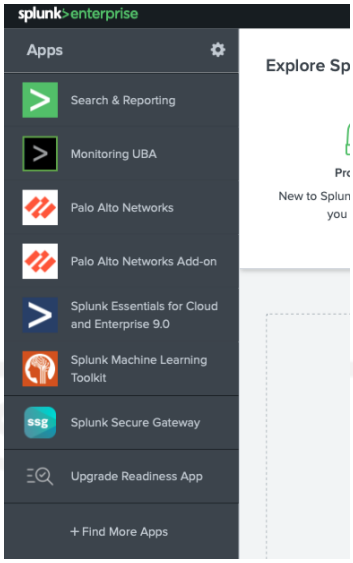


Gambar 3.3 Halaman unduh instalasi Splunk

8. Paket instalasi yang sudah diunduh bisa langsung diinstal dan buat akun untuk administrator. Kemudian akan diarahkan ke halaman utama Splunk dengan alamat http://localhost:8000 pada web browser.

H. Instalasi Palo Alto Network Add-On pada Splunk

Instalasi Palo Alto Network Add-On pada Splunk ini dimaksudkan untuk memperluas pembacaan *fields* pada log firewall Palo Alto agar lebih banyak fields yang terdeteksi oleh Splunk. *Add-on* ini dapat ditambahkan dengan memilih menu "*Apps*" kemudian cari dan *install* Palo Alto Network Add-On. Aplikasi tambahan yang sudah terpasang akan muncul pada daftar aplikasi tambahan Splunk seperti gambar 3.3.



Gambar 3.4 Daftar aplikasi tambahan pada Splunk

I. Mengunggah Data Threat Log Firewall

Data *threat log* yang dihasilkan *firewall* Palo Alto selama bulan Mei 2022 berukuran 2,3 *gigabyte* dan terdapat 3.511.236 *events threat* yang disimpan dalam format csv. Splunk Enterprise memiliki batasan ukuran unggah data sebesar 500 *megabyte* dalam sekali unggah. Maka dari itu, data *threat log firewall* dibagi menjadi beberapa bagian dengan ukuran di bawah 500 *megabyte* agar data dapat diolah oleh Splunk.

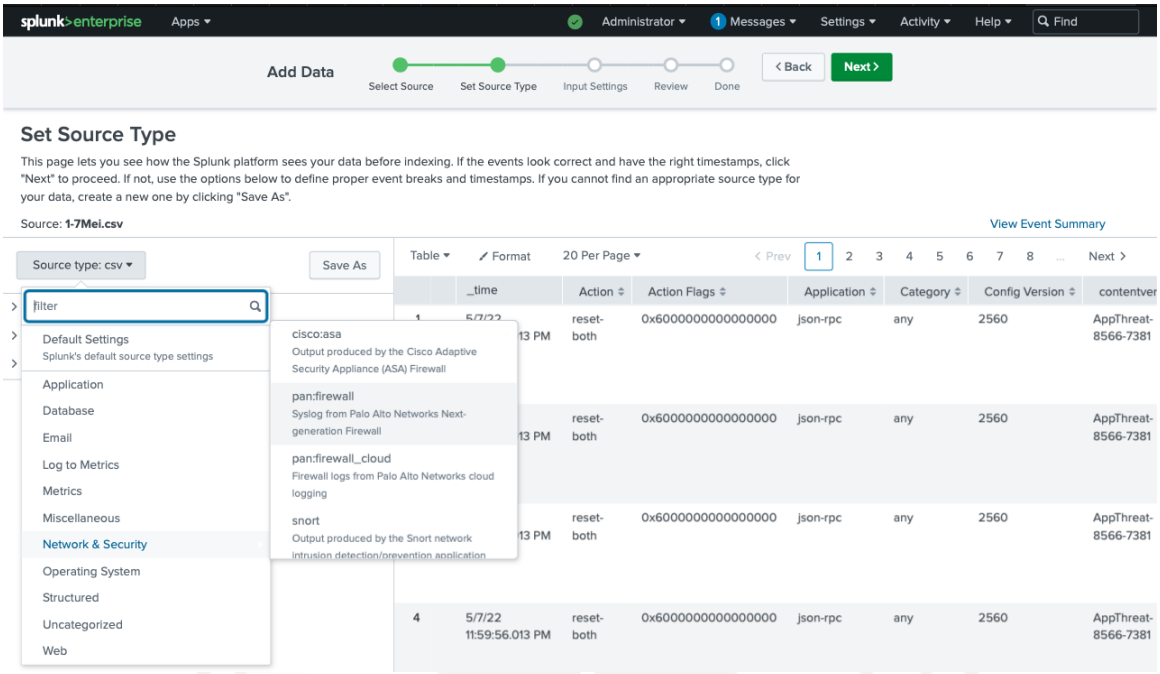
Data *log* dipecah menggunakan *tools* "*Split*" yang ada pada aplikasi Terminal macOS. Gambar 3.4 menunjukkan sintaks penggunaan "*Split*" untuk memecah file.

```
split [-b byte_count[k|m]] [-l line_count] [file[name]]
```

Gambar 3.5 Sintaks memecah file dengan Split

Data yang sudah dipecah kemudian diunggah ke Splunk dengan cara sebagai berikut:

1. Pilih menu "*Add Data*" pada halaman awal Splunk. Kemudian pilih metode "*Upload*" untuk mengunggah data dari file yang berasal dari komputer pengguna.
2. Pada bagian "*Select Source*" tekan "*Select File*" untuk memilih file data *log* yang akan diunggah. Kemudian tekan "*Next*" jika file sudah dipilih.
3. Selanjutnya pada "*Set Source Type*" pilih tipe sumber data yang sesuai, yaitu dengan memilih pada bagian "*Network & Security*" kemudian pilih "*pan:firewall*" karena data yang digunakan berasal dari *syslog firewall* Palo Alto seperti yang ditunjukkan pada gambar 3.5. kemudian tekan "*Next*" jika sudah memiih tipe sumber data.

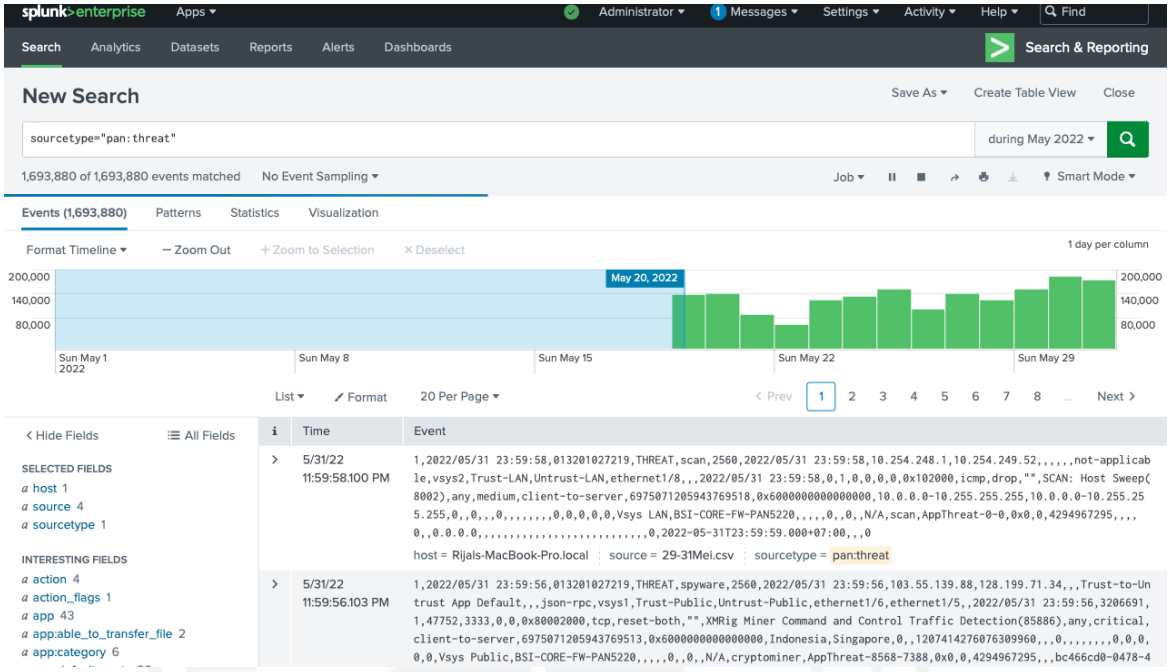


Gambar 3.6 Memilih tipe data sumber

4. Selanjutnya tidak ada perubahan konfigurasi pada bagian "*Input Settings*" dan membiarkan kondisi default pada opsi "*Index*". Kemudian tekan "*Review*".
5. Kemudian pada bagian "*Review*" pastikan bahwa data yang akan diunggah telah sesuai, jika sudah sesuai lalu tekan "*Submit*" untuk mengunggah data.
6. Data berhasil diunggah lalu ulangi proses di atas dengan memilih "*Add More Data*" untuk menambahkan data sampai semua data yang dibutuhkan selesai diunggah ke Splunk.

J. Search & Reporting Splunk

Pada tahap ini dilakukan pembuatan "*rules*" untuk mengolah data log firewall dan menampilkannya pada dashboard Splunk supaya mudah dibaca dan dipahami sehingga membantu proses analisis tren serangan siber pada jaringan UII. Tahapan ini dimulai dengan membuka aplikasi *Search & Reporting* pada Splunk. Gambar 3.6 menunjukkan halaman Search & Reporting.

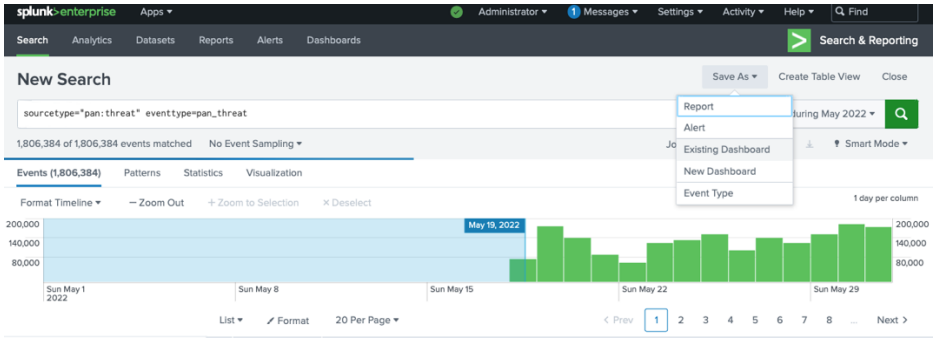


Gambar 3.7 Halaman *Search & Reporting* pada Splunk

Penulisan "*rules*" pada Splunk mengikuti kaidah "*Search Processing Language*". Komponen penulisan dengan Search Processing Language pada Spunk memiliki komponen sebagai berikut:

a. *Search Terms*, yaitu kata kunci atau frasa yang akan dicari.
b. *Command*, yaitu perintah yang diberikan kepada kumpulan data atau hasil pencarian.
c. *Functions*, yaitu komputasi atau perhitungan yang diterapkan pada data atau hasil pencarian.
d. *Clauses*, yaitu cara untuk mengelompokkan atau memberi nama *fields* pada suatu data atau hasil.

Setelah rules disusun dan dilakukan pencarian serta pengolahan data, hasil yang didapatkan disimpan dan ditampilkan ke *dashboard* untuk mempermudah pembacaan hasil pengolahan data. Gambar 3.7 menunjukkan langkah untuk menyimpan hasil pencarian ke dalam *dashboard*.



Gambar 3.8 Menyimpan hasil ke *dashboard*

3.3.5 Pengujian

Tahap ini dilakukan untuk menguji kesesuaian antara hasil implementasi dengan poin **3.2 Indikator Keberhasilan**. Indikator keberhasilan yang pertama yaitu menguji kesesuaian rules yang dibuat dengan temuan hasil *Search & Reporting*. Kemudian indikator keberhasilan yang kedua yaitu menguji apakah hasil temuan yang ditampilkan pada dashboard dapat tetap berjalan dengan baik atau tidak. Jika kedua indikator keberhasilan tersebut terpenuhi, maka rules yang digunakan bersifat universal dan dapat digunakan untuk implementasi jangka panjang atau secara *real-time*.

3.3.6 Analisis

Tahap analisis dilakukan untuk mengamati temuan hasil dari proses implementasi dan pengujian pada penelitian ini dan sebagai dasar untuk menarik kesimpulan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil dan Analisis

Berdasarkan hasil implementasi Security Information and Event Management (SIEM) Splunk untuk analisis tren ancaman pada jaringan UII, maka hasil temuan dan analisis yang diperoleh diuraikan sebagai berikut.

4.1.1 *Rules* untuk *Search & Reporting*

Menampilkan jumlah ancaman per hari

```
(index=* OR index=_*) (sourcetype="pan:threat") (date_mday="*")
| rename date_mday AS RootObject.date_mday log_subtype AS
RootObject.log_subtype
| fields "_time" "host" "source" "sourcetype" "RootObject.date_mday"
"RootObject.log_subtype"
| eval _time='_time'
| timechart dedup_splitvals=t count AS "Jumlah Threat per Hari" span=1d
format=$VAL$:::$AGG$
| sort limit=0 _time
| fields _time, "Jumlah Threat per Hari"
```

Gambar 4.1 *Rules Threat per day*

Menampilkan Threat Chart untuk setiap kategori ancaman

```
| pivot ThreatChart RootObject count(RootObject) AS "Count of
1657214316.599" SPLITROW _time AS _time PERIOD day SPLITCOL threat_category
SORT 0 _time ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 100 SHOWOTHER 1
```

Gambar 4.2 *Threat Chart by Category*

Menampilkan 10 *threat* teratas

```
sourcetype="pan:threat"
| top limit=10 threat_name
```

Gambar 4.3 *Top 10 Threat*

Menampilkan 10 *vulnerability* teratas

```
sourcetype="pan:threat" log_subtype=vulnerability
| top limit=10 threat_name
```

Gambar 4.4 *Top 10 Vulnerability*

Menampilkan *threat severity*

```
sourcetype="pan:threat"
| top limit=5 severity
```

Gambar 4.5 *Threat Severity*

Menampilkan *5 threat* dengan *critical severity*

```
sourcetype="pan:threat" severity=critical
| top limit=5 threat_name
```

Gambar 4.6 Top 5 *threat by critical severity*

Menampilkan 10 pengguna teratas dengan *protocol-anomaly*

```
sourcetype="pan:threat" category="protocol-anomaly" user!=unknown
| top limit=10 user
```

Gambar 4.7 *Top 10 users with protocol-anomaly*

Menampilkan 10 IP address teratas dengan *protocol-anomaly*

```
sourcetype="pan:threat" category="protocol-anomaly"
| top limit=10 src_ip
```

Gambar 4.8 *Top 10 IP address with protocol-anomaly*

Menampilkan *vendor (Palo Alto Network) action* terhadap *threat*

```
sourcetype="pan:threat"
| top limit=10 vendor_action
```

Gambar 4.9 *Vendor (PAN Firewall) Action*

Menampilkan lokasi *IP address* dari *threat*

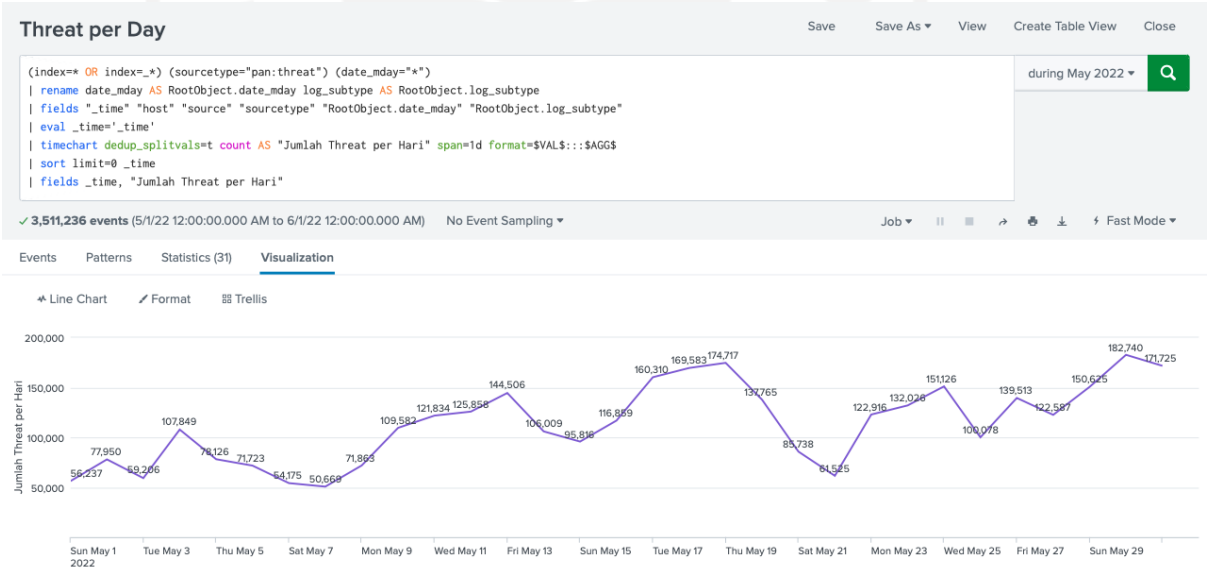
```
sourcetype="pan:threat"
| iplocation src_ip
| geostats distinct_count(src_ip) by src_location globallimit=10
```

Gambar 4.10 *Source IP Address location*

4.1.2 Statistik dan Visualisasi Hasil dari Proses *Search & Reporting*

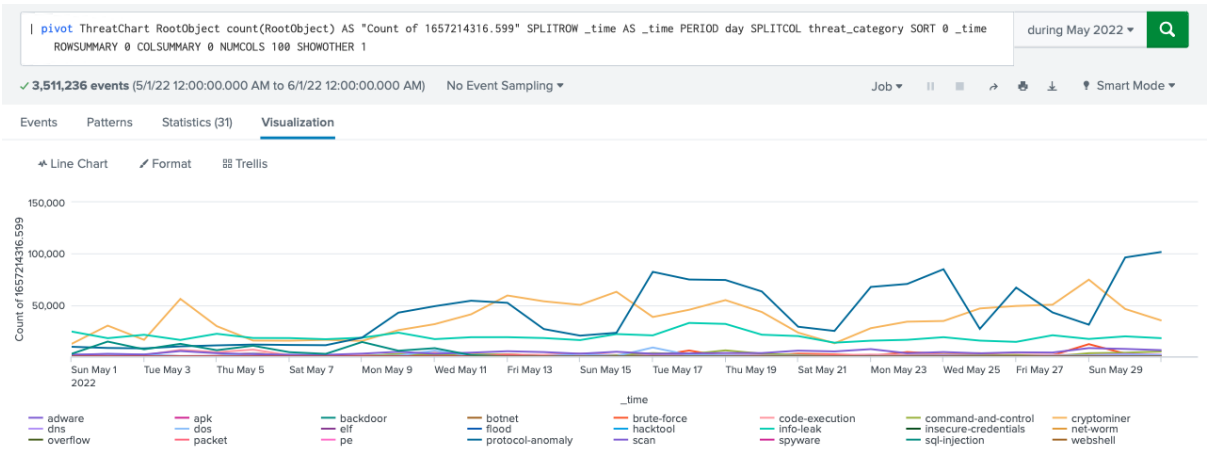
Berikut merupakan statistik dan visualisasi data dari rules yang sudah diimplementasikan.

Hasil dari *rules* pada gambar 4.1 menampilkan grafik jumlah ancaman per hari yang masuk ke jaringan UII dengan jenis visualisasi "*Line Chart*" seperti pada gambar 4.11. Tampilan ini digunakan untuk memudahkan pembacaan grafik jumlah ancaman per hari dalam kurun waktu tertentu. Dari grafik tesebut juga dapat dilihat kenaikan atau turunnya jumlah ancaman.



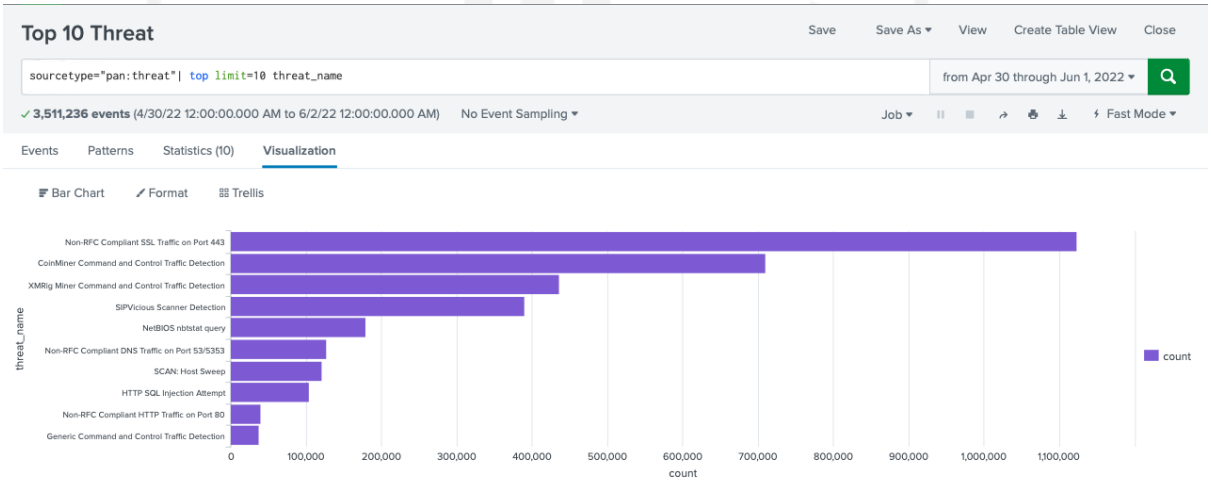
Gambar 4.11 *Line Chart – Threat per Day*

Hasil dari *rules* pada gambar 4.2 menampilkan grafik jumlah ancaman per hari berdasarkan *threat category* dari *firewall* Palo Alto dengan jenis visualisasi "*Line Chart*" seperti pada gambar 4.12. Tampilan ini digunakan untuk memudahkan pembacaan grafik jumlah *threat* per hari dan membandingkan grafik dari tiap jenis ancaman. Dari grafik tersebut dapat dilihat bahwa jumlah *threat* dengan kategori *protocol-anomaly* dan *cryptominer* mengalami kenaikan mulai pada minggu kedua pada bulan Mei 2022



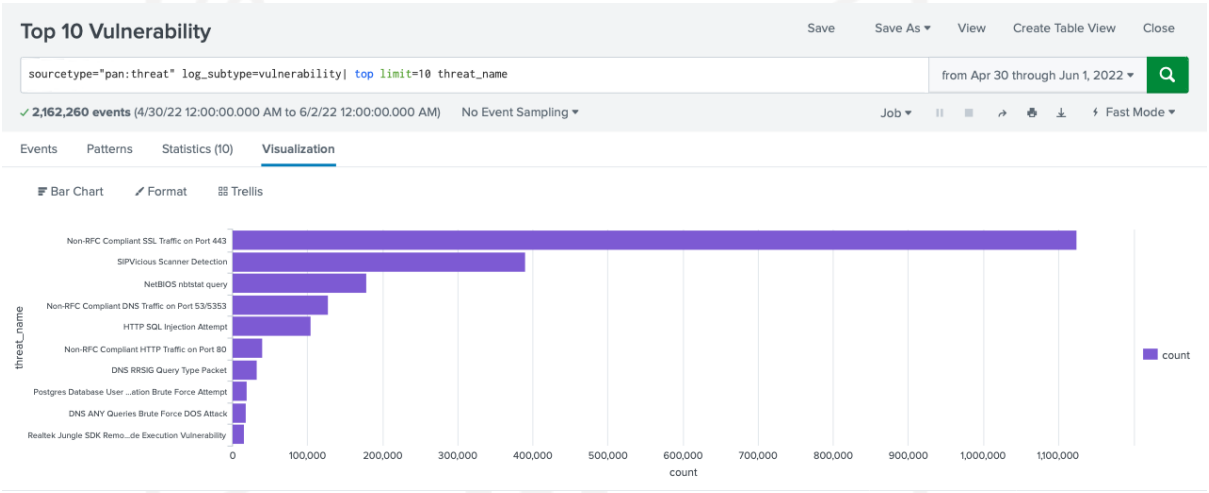
Gambar 4.12 *Line Chart – Threat Chart by Category*

Hasil dari *rules* pada gambar 4.3 menampilkan 10 *threat* teratas dengan jenis visualisasi "*Bar Chart*" seperti pada gambar 4.13. Tampilan ini dipilih untuk menunjukkan 10 nama *threat* yang sering masuk ke jaringan UII beserta jumlah kejadian dalam kurun waktu tertentu. Dari visualisasi tersebut dapat dilihat bahwa dari 3.511.236 *events threat* menunjukkan bahwa *NON-RFC Compliant SSL Traffic on Port 443* merupakan *threat* yang paling sering ditemukan di jaringan UII dengan jumlah 1.124.058 *events*, disusul *Coinminer Command and Control Traffic Detection* dengan 709.857 *events*, dan *XMRig Miner Command and Control Traffic Detection* dengan 436.267 *events* selama bulan Mei 2022.



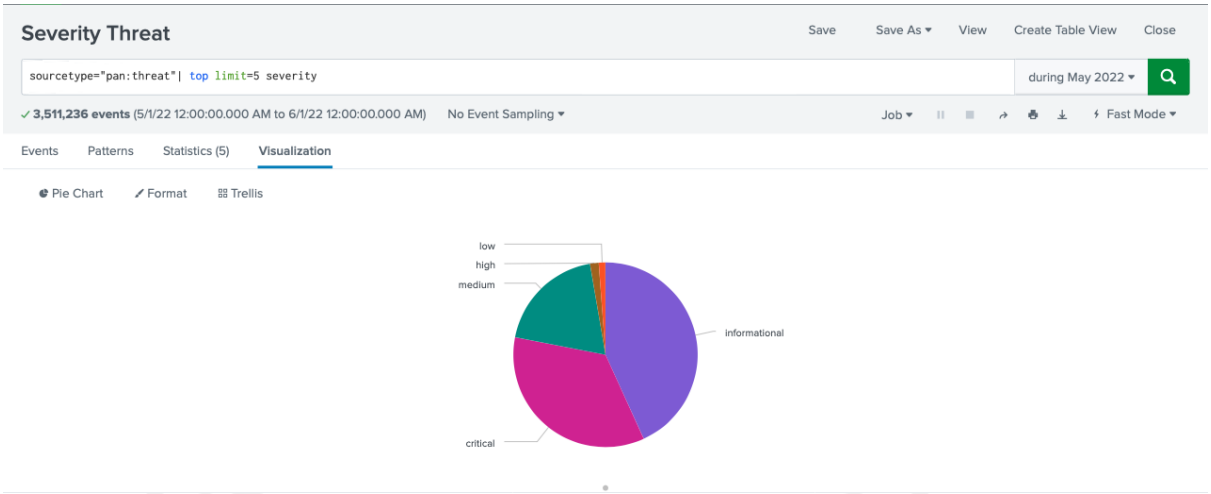
Gambar 4.13 *Bar Chart – Top 10 Threat*

Hasil dari *rules* pada gambar 4.4 menampilkan 10 *vulnerability* teratas dengan visualisasi "*Bar Chart*" seperti pada gambar 4.14. Tampilan ini dipilih untuk menunjukkan 10 nama *vulnerability* teratas yang ada pada jaringan UII beserta jumlah kejadian dalam kurun waktu tertentu. Dari visualisasi tersebut dapat dilihat bahwa dari 2.162.260 *events vulnerability* menunjukkan bahwa *NON-RFC Compliant SSL Traffic on Port 443* merupakan *vulnerability* yang sering ditemukan di jaringan UII dengan jumlah 1.124.058 *events*, disusul *SIPVicious Scanner Detection* dengan 390.037 *events*, dan *NetBIOS nbstat query* dengan 178.802 *events* selama bulan Mei 2022.



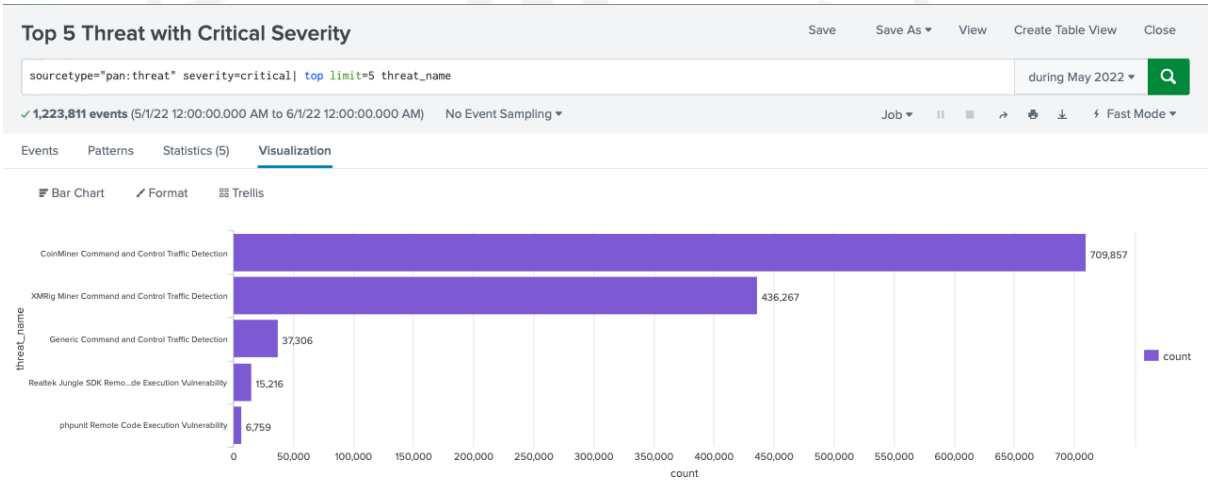
Gambar 4.14 *Bar Chart – Top 10 Vulnerability*

Hasil dari *rules* pada gambar 4.5 menampilkan persentase *threat severity* dengan visualisasi "*Pie Chart*" seperti pada gambar 4.15. Tampilan ini dipilih untuk memudahkan pembacaan jumlah dan persentase *threat* berdasarkan *severity level*. Dari visualisasi tersebut dapat dilihat bahwa 43,195% *threat* dengan level *informational*, 34,854% *threat* dengan level *critical*, 19,251% *threat* dengan level *medium*, 1,531% *threat* dengan level *high*, dan 1,168% *threat* dengan level *low*.



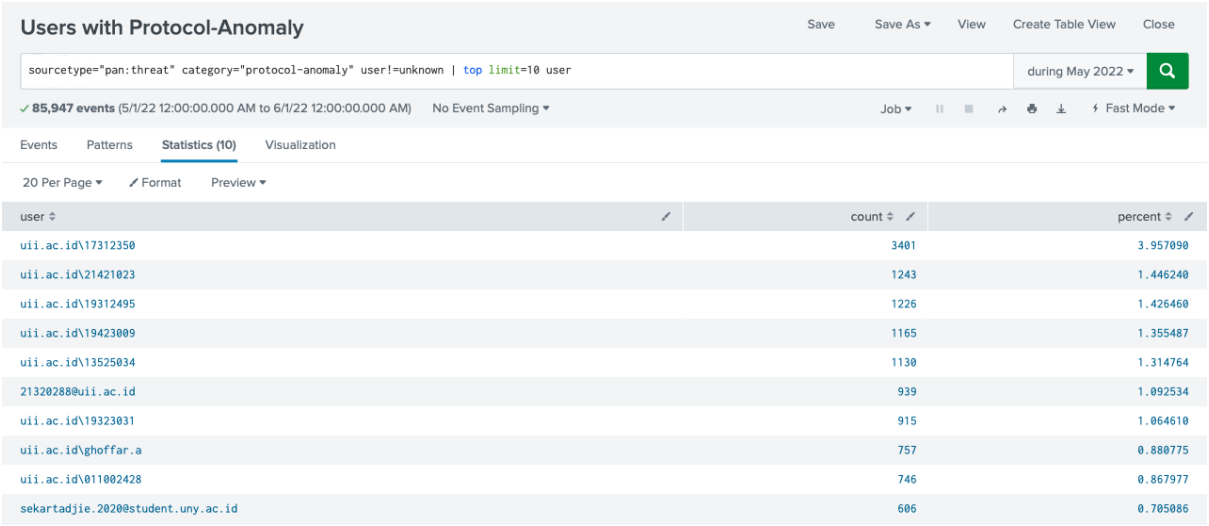
Gambar 4.15 Pie Chart – Severity Level

Hasil dari *rules* pada gambar 4.6 menampilkan 5 *threat* teratas yang memiliki *severity level* yaitu *critical* dengan jenis visualisasi "*Bar Chart*" yang ditunjukkan pada gambar 4.16 untuk memudahkan pembacaannya. Dari visualisasi tersebut terlihat bahwa dari 1.223.811 *events threat* dengan level *critical* menunjukkan bahwa *Coinminer Command and Control Traffic Detection* merupakan *threat* yang paling banyak ditemukan dengan jumlah 709.857 *events*, disusul *XMRig Miner Command and Control Traffic Detection* dengan 436.267 *events*.



Gambar 4.16 *Bar Chart – Top 5 Threat with Critical Severity*

Hasil dari *rules* pada gambar 4.7 menampilkan 10 pengguna teratas yang terindikasi dengan *protocol-anomaly*. Visualisasi dengan tabel data statistik seperti pada gambar 4.17 dipilih untuk memudahkan pembacaan terkait nama pengguna yang *terindikasi protocol-anomaly* dan jumlah kejadiannya.



Users with Protocol-Anomaly

Save | Save As | View | Create Table View | Close

sourcetype="pan:threat" category="protocol-anomaly" user!=unknown | top limit=10 user

during May 2022

✓ 85,947 events (5/1/22 12:00:00.000 AM to 6/1/22 12:00:00.000 AM) No Event Sampling | Job | Fast Mode

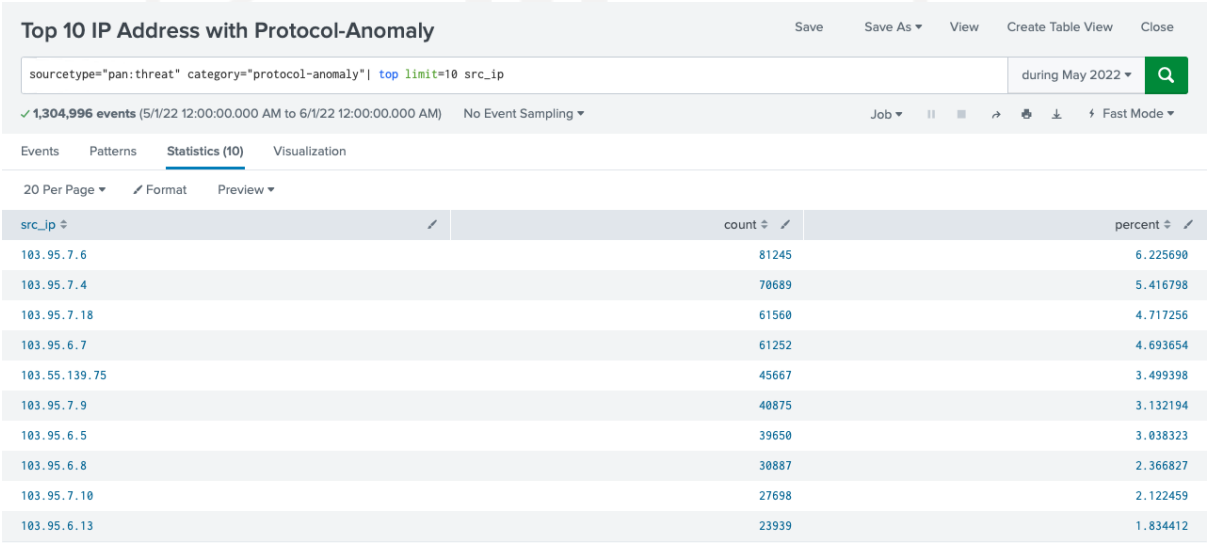
Events | Patterns | Statistics (10) | Visualization

20 Per Page | Format | Preview

user	count	percent
uii.ac.id\17312350	3401	3.957090
uii.ac.id\21421023	1243	1.446240
uii.ac.id\19312495	1226	1.426460
uii.ac.id\19423009	1165	1.355487
uii.ac.id\13525034	1130	1.314764
21320288@uii.ac.id	939	1.092534
uii.ac.id\19323031	915	1.064610
uii.ac.id\ghoffar.a	757	0.880775
uii.ac.id\011002428	746	0.867977
sekartadjie.2020@student.uny.ac.id	606	0.705086

Gambar 4.17 *Data Table – Top 10 Users with Protocol Anomaly*

Hasil dari *rules* pada gambar 4.8 menampilkan 10 *IP address* teratas yang terindikasi dengan *protocol-anomaly*. Visualisasi dengan tabel data statistik seperti pada gambar 4.18 dipilih untuk memudahkan pembacaan terkait *IP address* yang terindikasi *protocol-anomaly* dan jumlah kejadiannya.



Top 10 IP Address with Protocol-Anomaly

Save | Save As | View | Create Table View | Close

sourcetype="pan:threat" category="protocol-anomaly"| top limit=10 src_ip

during May 2022

✓ 1,304,996 events (5/1/22 12:00:00.000 AM to 6/1/22 12:00:00.000 AM) No Event Sampling | Job | Fast Mode

Events | Patterns | Statistics (10) | Visualization

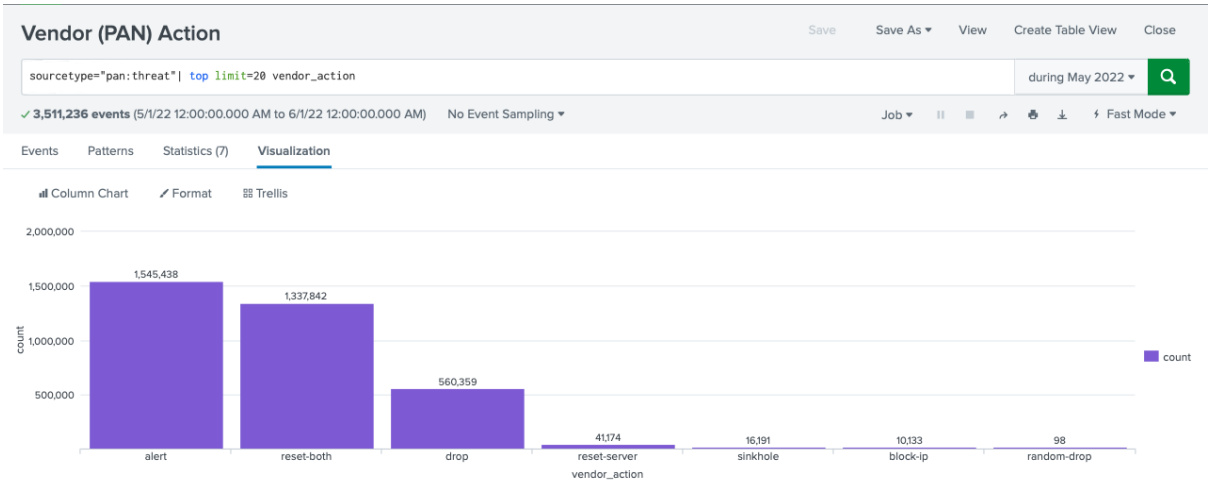
20 Per Page | Format | Preview

src_ip	count	percent
103.95.7.6	81245	6.225690
103.95.7.4	70689	5.416798
103.95.7.18	61560	4.717256
103.95.6.7	61252	4.693654
103.55.139.75	45667	3.499398
103.95.7.9	40875	3.132194
103.95.6.5	39650	3.038323
103.95.6.8	30887	2.366827
103.95.7.10	27698	2.122459
103.95.6.13	23939	1.834412

Gambar 4.18 *Data Table – Top 10 IP Address with Protocol Anomaly*

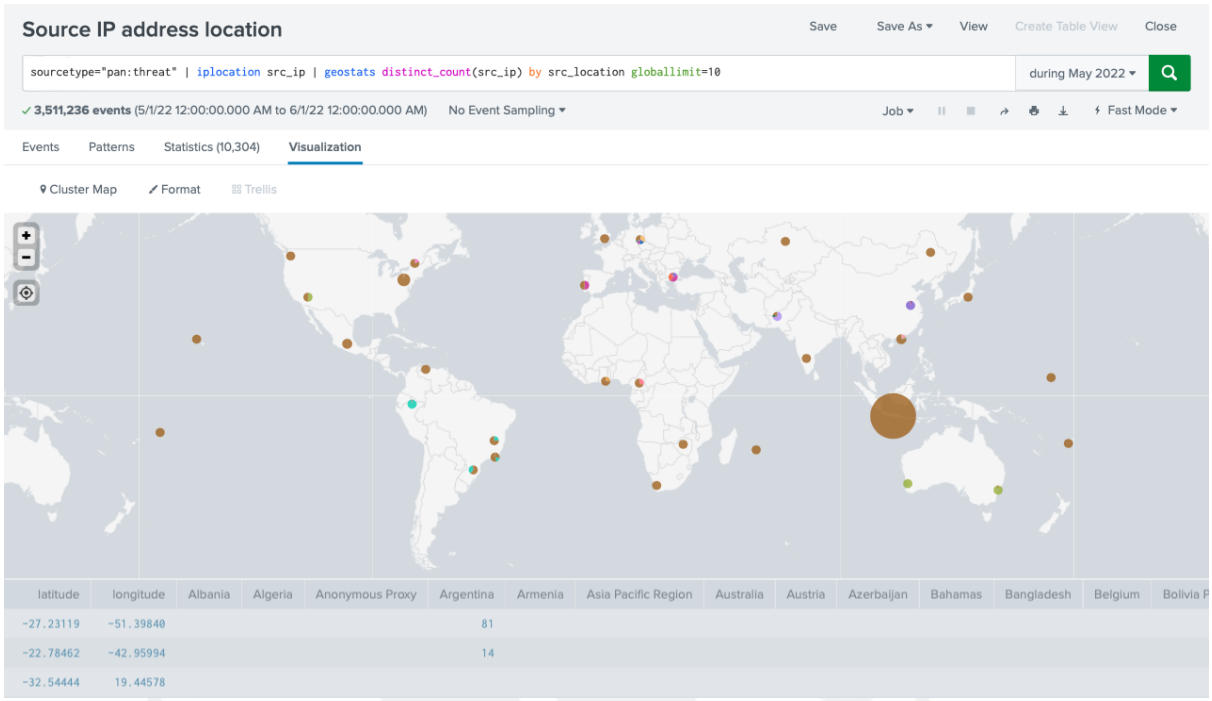
Hasil dari *rules* pada gambar 4.9 menampilkan tindakan yang dilakukan *vendor* dalam hal ini *firewall Palo Alto* terhadap *threat* yang ada pada jaringan UII seperti pada gambar 4.19.

Visualisasi yang dipilih yaitu dengan jenis "*Column Chart*" yang ditujukan untuk memudahkan pembacaan dan pembanding tindakan yang sudah dilakukan terhadap *threat* yang ada pada jaringan UII.



Gambar 4.19 *Column Chart – Vendor (PAN) Action*

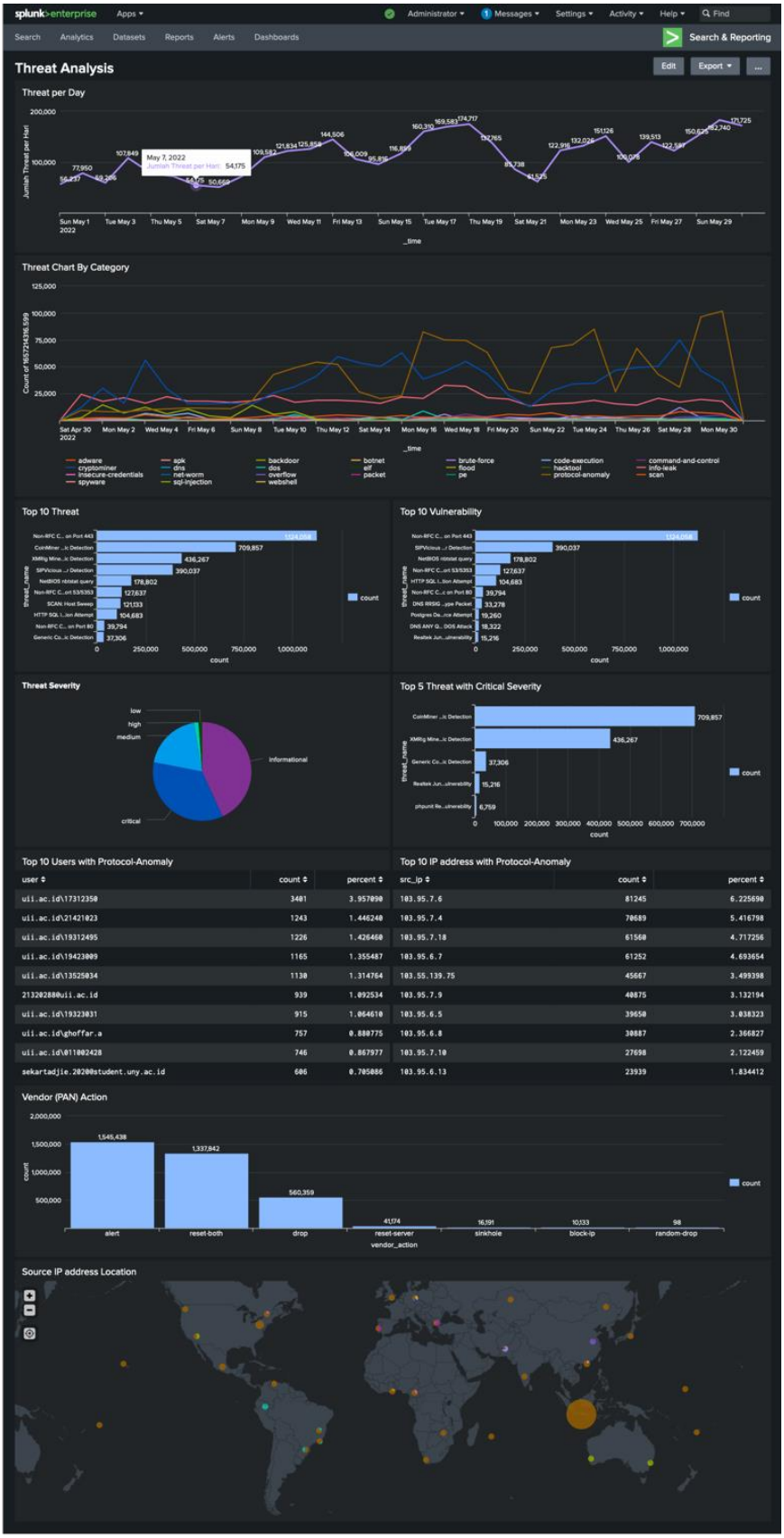
Hasil dari *rules* pada gambar 4.10 menampilkan lokasi asal dari *IP address* dari ancaman serangan siber seperti pada gambar 4.20 dengan visualisasi "*Cluster Map*" agar lebih memudahkan pencarian lokasi asal ancaman karena bisa langsung mengarahkan kursor ke titik tertentu dan bisa langsung melihat darimana ancaman berasal beserta jumlahnya.



Gambar 4.20 *Cluster Map – Source IP Address Location*

4.1.3 Tampilan Dashboard

Hasil temuan berupa tabel statistik maupun visualisasi dari proses pencarian dengan *rules* disimpan dan disatukan dalam satu *dashboard*. *Dashboard* ini ditujukan untuk membantu proses pembacaan dan analisis tren ancaman. Tampilan *dashboard* dapat dilihat pada gambar 4.21.



Gambar 4.21 *Dashboard – Threat Analysis*

Dashboard di atas dapat di-*export* ke file PDF jika diperlukan untuk laporan dalam periode tertentu.

4.2 Pembahasan

Dari hasil implementasi *Security Information and Event Management* (SIEM) Splunk untuk analisis tren ancaman siber, data dari *log firewall* dapat diolah dengan baik oleh Splunk. *Rules* yang dibuat disusun berdasarkan Laporan Kuarter 2 Publik: Monitor Keamanan Cyber yang disusun oleh *Security Operation Center* Badan Sistem Informasi UII. Data analisis yang dibutuhkan untuk laporan tersebut antara lain:

a. Grafik jumlah ancaman serangan berdasarkan tipe serangan. *Rules* yang dibuat sudah diimplementasikan dengan SIEM Splunk seperti pada gambar 4.11 dan 4.12 dan bisa ditampilkan dan dibaca di *dashboard* seperti pada gambar 4.21.
b. Grafik persentase ancaman serangan berdasarkan *severity level*. *Rules* yang dibuat sudah diimplementasikan dengan SIEM Splunk seperti pada gambar 4.15 dan bisa ditampilkan dan dibaca di *dashboard* seperti pada gambar 4.21.
c. Data statistik untuk 10 ancaman serangan. Rules yang dibuat sudah diimplementasikan dengan SIEM Splunk seperti pada gambar 4.13 dan gambar 4.16 dan bisa ditampilkan dan dibaca di *dashboard* seperti pada gambar 4.21.
d. Data trafik anomali dari pengguna dan IP addres. Rules yang dibuat sudah diimplementasikan dengan SIEM Splunk seperti pada gambar 4.17 dan gambar 4.18 dan bisa ditampilkan dan dibaca di *dashboard* seperti pada gambar 4.21.

Selain rules yang disusun berdasarkan laporan kuartal BSI UII, *rules* juga disusun berdasarkan hasil *review* beberapa laporan ancaman dan serangan siber dari pihak lain.

Hasil penelitian ini menunjukkan bahwa implementasi *Security Information and Event Management* (SIEM) dengan Splunk dapat membantu proses analisis ancaman serangan siber, menentukan respon dan mitigasi pada suatu kejadian baik ancaman maupun serangan, serta menjadi bahan evaluasi untuk setiap aturan yang diterapkan pada jaringan UII.

1. *Rules* pada gambar 4.1 yang menghasilkan tampilan gambar 4.11 yaitu laporan jumlah ancaman serangan per hari yang masuk ke jaringan UII. Dari laporan ini, pihak yang berwenang yaitu BSI UII bisa melihat kenaikan atau penurunan jumlah serangan sehingga dapat melihat trennya untuk memprediksi jumlah serangan di masa yang akan datang. Misalnya jika terdapat suatu lonjakan kenaikan jumlah serangan secara drastis dalam waktu singkat atau tidak normal maka analis keamanan dapat

melaporkan dan berkoordinasi dengan tim yang lain untuk mencari tau serangan apa yang terjadi dan celah keamanan mana yang dieksploitasi oleh penyerang sehingga ancaman atau serangan yang terjadi dapat segera teratasi.

2. *Rules* pada gambar 4.2 yang menghasilkan tampilan gambar 4.12 yaitu laporan jumlah ancaman serangan berdasarkan kategori ancaman. Analis keamanan dapat melihat tren jenis ancaman yang banyak terjadi di jaringan UII. Misalnya terjadi kenaikan jumlah serangan pada pertengah bulan Mei 2022 dengan jenis *protocol-anomaly* dan *cryptominer*, maka analis keamanan beserta tim dapat segera mencari tau siapa saja pengguna yang terindikasi dengan serangan tersebut atau *IP address* mana saja yang digunakan oleh serangan tersebut.

3. *Rules* pada gambar 4.3 yang menghasilkan tampilan gambar 4.13 yaitu laporan mengenai 10 ancaman teratas pada jaringan UII. Tim keamanan siber dapat mengetahui ancaman yang ada di jaringan UII. Misalnya *NON-RFC Compliant SSL Traffic on Port 443* menjadi ancaman yang paling banyak selama bulan Mei 2022, tim keamanan bisa segera mengambil tindakan untuk pencegahan dan penanganan pada celah keamanan yang dieksploitasi oleh ancaman tersebut.

4. *Rules* pada gambar 4.4 yang menghasilkan tampilan gambar 4.14 yaitu laporan mengenai 10 celah keamanan yang paling banyak terekspos. Dengan mengetahui celah keamanan mana saja yang paling banyak terekspos, tim keamanan dapat segera menutup celah tersebut sehingga serangan yang mengakibatkan kerugian pada jaringan dan perusahaan dapat dicegah atau diminimalisir.

5. *Rules* pada gambar 4.5 yang menghasilkan tampilan gambar 4.15 yaitu laporan jumlah ancaman siber berdasarkan *severity level* atau tingkat bahaya suatu ancaman. Misalnya pada bulan Mei 2022 sebanyak 35% dari ancaman serangan bersifat *critical*, maka tim keamanan dapat segera melakukan pengecekan pada *firewall*, apakah ancaman serangan tersebut sudah dapat diatasi oleh *firewall* atau perlu adanya penanganan khusus karena dalam ancaman serangan dengan level *critical* biasanya penyerang tidak memerlukan autentikasi kredensial khusus atau informasi mengenai target dan korban tidak perlu dimanipulasi lagi untuk melakukan fungsi-fungsi khusus. Laporan

ini juga bisa menjadi bahan pertimbangan untuk melakukan evaluasi terkait aturan-aturan keamanan yang diterapkan baik pada perangkat jaringan maupun pengguna jaringan.

6. *Rules* pada gambar 4.6 yang menghasilkan tampilan gambar 4.16 yaitu laporan mengenai 5 ancaman serangan yang bersifat *critical*. Ancaman yang bersifat *critical* harus segera ditangani dan celah keamanan yang diindikasi dengan ancaman tersebut harus segera ditutup karena dampak buruk yang diakibatkan akan sangat merugikan. Dengan adanya informasi tersebut, tim keamanan dapat mengetahui ancaman yang bersifat *critical* apa saja yang paling banyak terekspos pada jaringan UII dan tim keamanan dapat segera melakukan penanganan dan mitigasi ancaman serangan tersebut.

7. *Rules* pada gambar 4.7 yang menghasilkan tampilan gambar 4.17 yaitu laporan pengguna yang terindikasi dengan ancaman jenis *protocol-anomaly*. Dari laporan tersebut dapat diketahui siapa saja pengguna yang paling sering terindikasi dengan tindak ancaman jenis *protocol-anomaly*. *Protocol-anomaly* tejadi ketika perilaku dari protocol menyimpang dari standar dan penggunaan yang seharusnya. Misalnya terdapat paket yang tidak sesuai bentuknya, aplikasi yang ditulis dengan buruk, atau aplikasi yang berjalan tidak pada port standar maka akan dianggap sebagai *protocol-anomaly*. Dengan adanya informasi tersebut, tim keamanan perlu melakukan penanganan untuk pengguna yang sering terindikasi dengan ancaman tersebut atau melakukan evaluasi terkait aturan yang diterapkan pada *firewall*.

8. *Rules* pada gambar 4.8 yang menghasilkan tampilan gambar 4.18 yaitu laporan *IP address* yang terindikasi dengan ancaman jenis *protocol-anomaly*. Dari laporan tersebut dapat diketahui IP address mana saja yang paling sering terindikasi dengan ancaman jenis protocol-anomaly. Dengan adanya informasi tersebut, tim keamanan perlu melakukan penanganan untuk IP address yang sering terindikasi dengan ancaman tersebut atau melakukan evaluasi terkait aturan yang diterapkan pada *firewall*.

9. *Rules* pada gambar 4.9 yang menghasilkan tampilan gambar 4.19 yaitu laporan tindakan yang sudah dilakukan *firewall* Palo Alto Network terhadap ancaman yang ada pada jaringan UII. Beberapa tindakan yang dilakukan firewall terhadap ancaman yang ada adalah:
    - *Allow* – menghasilkan *alert* atau peringatan untuk setiap ancaman pada trafik aplikasi. Pada data *log* bulan Mei 2022 sebanyak 1.545.348 *alert* dihasilkan.
    - *Drop* – melarang atau membatasi trafik aplikasi. Sebanyak 560.359 trafik di-*drop* oleh *firewall* pada bulan Mei 2022.
    - *Reset Server* – untuk protokol TCP akan dilakukan *reset* di sisi koneksi *server*, sedangkan pada protokol UDP koneksi yang terjalin akan di-*drop*. Sebanyak 41.174 trafik dilakukan tindakan *reset-server* oleh *firewall* pada bulan Mei 2022.
    - *Reset Both* – untuk protokol TCP akan dilakukan *reset* konek di sisi *client* dan *server*, sedangkan pada protokol UDP koneksi yang terjalin akan di-*drop*. Sebanyak 1.337.842 trafik dilakukan tindakan *reset-both* oleh *firewall* pada bulan Mei 2022.
    - *Sinkhole* – mengarahkan *DNS query* yang terindikasi dengan domain berbahaya ke *sinkhole IP address*. Sebanyak 16.191 trafik dialihkan ke *DNS sinkhole* pada bulan Mei 2022.
    - *Block IP* – memblokir trafik baik dari *source* maupun *source-destination* trafik. Sebanyak 10.133 trafik diblokir oleh *firewall* pada bulan Mei 2022.
    - *Random-drop* – dilakukan *drop* pada trafik secara acak saat jumlah trafik mencapai ambang batas *Activate Rate* untuk melindungi sistem dari serangan DoS. Sebanyak 98 trafik di-*drop* oleh *firewall* secara acak pada bulan Mei 2022. Dari hasil laporan tersebut dapat dijadikan bahan evaluasi terkait aturan-aturan keamanan yang diterapkan pada *firewall*.

10. *Rules* pada gambar 4.10 yang menghasilkan tampilan gambar 4.20 yaitu laporan mengenai lokasi asal ancaman serangan siber pada jaringan UII. Dari laporan ini, tim keamanan dapat mengetahui darimana ancaman serangan berasal dan dapat digunakan untuk mengidentifikasi karakteristik ancaman serangan dari wilayah tertentu.

Dari hasil penerapan *rules* untuk pencarian ancaman serangan dengan *level critical* diperoleh beberapa ancaman atau *threats* yang paling banyak dicatatkan oleh *firewall* Palo Alto milik BSI UII, antara lain:

- *Cryptojacking*

Cryptojacking adalah serangan siber yang memungkinkan peretas dapat mengkooptasi sumber daya komputasi dan menggunakannya untuk menambang berbagai mata uang kripto. Ancaman jenis ini menjadi ancaman dengan level *critical* yang paling banyak terekspos yaitu *CoinMiner Command and Control Traffic Detection* sebanyak 709.857 *events* dan *XMRig Miner Command and Control Traffic Detection* sebanyak 436.267 *events* pada bulan Mei 2022 dan menjadi 2 ancaman dengan level *critical* teratas.

Dampak dari adanya serangan jenis ini bisa menyebabkan perangkat menjadi lebih lamban dari biasanya dan juga membahayakan data pribadi karena ada orang yang tidak berwenang masuk ke dalam komputer. Ada beberapa cara "*Coin Miner*" ini masuk ke sistem, antara lain penyerang dapat mengeksploitasi aplikasi yang terekspos ke publik yang rentan terhadap kerentanan *remote code execution* (RCE) untuk menyebarkan penambang kripto, mengkompromi kunci akses ke sistem, dan melakukan *phising* surel maupun perangkat USB.

Langkah mitigasi yang dapat dilakukan antara lain dengan selalu memperbarui aplikasi dan perangkat lunak, memastikan bahwa kunci akses tidak terekspos ke publik, dan mematikan *autorun* pada komputer serta mengedukasi pengguna akan bahaya surel penipuan.

- *Command and Control*

Serangan ini dimulai dengan menginfeksi komputer yang berada di belakang firewall dengan cara menggunakan *phising* surel yang mengarahkan pengguna untuk membuka suatu web dan menjalankan kode berbahaya, melalui kerentanan pada web plugins, atau aplikasi yang sudah terinfeksi kode berbahaya lainnya. Setelah kode berbahaya dijalankan, penyerang bisa mendapat akses penuh ke jaringan dan dapat menjalankan botnet atau kode apapun di dalamnya. Dampak dari serangan ini penyerang dapat mencuri data pengguna maupun organisasi, mematikan sistem atau komputer, melakukan *reboot* sistem, dan juga serangan *Distributed Denial of Services* (DDoS) yang dapat merugikan organisasi.

Langkah pencegahan terhadap serangan ini bisa dengan mengedukasi pengguna akan surel penipuan serta memastikan aplikasi yang digunakan aman dan tetap terbarui. Pada

bulan Mei 2022, ancaman serangan banyak terekspos oleh firewall milik BSI UII antara lain *CoinMiner Command and Control Traffic Detection*, *XMRig Miner Command and Control Traffic Detection*, dan *General Command and Control Traffic Detection.*

- *Command Injection*

Serangan ini ditujukan untuk mengeksekusi perintah secara sewenang-wenang pada sistem operasi host melalui aplikasi yang memiliki kerentanan. Serangan ini mungkin terjadi saat aplikasi melewati data yang disediakan pengguna yang tidak aman (*form*, *cookie*, *header HTTP*, dan lainnya) ke shell sistem.

Dampak dari serangan ini adalah penyerang dapat menjalankan perintah sistem operasi dengan hak istimewa dari aplikasi yang rentan. Bergantung dari hak istimewanya, kerentanan ini dapat mengakibatkan peretas mendapat hak akses ke sistem, mengekstrak data yang sensitif, dan bisa mengambil alih control penuh dari sistem. Pada bulan Mei 2022, kerentanan pada aplikasi yang banyak terekspos adalah *Realtek Jungle SDK Remote Code Execution Vulnerability* sebanyak 15.216 *events*.

Beberapa langkah mitigasi yang dapat dilakukan adalah dengan menghindari penggunaan fungsi shell atau membatasi penggunaan untuk kasus yang spesifik, melakukan validasi masukan ke dalam perintah eksekusi *shell*, dan menggunakan API yang aman saat menerima masukan dari pengguna.

- *Vulnerability*

Vulnerability atau kerentanan pada sistem dapat dieksploitasi dengan *malware*, *script*, maupun *open-source exploit kit* oleh pihak yang tidak bertanggung jawab. Celah keamanan yang terekspos oleh firewall milik BSI UII pada bulan Mei 2022 adalah *Realtek Jungle SDK Remote Code Execution Vulnerability* sebanyak 15.216 *events* dan *phpunit Remote Code Execution Vulnerability* sebanyak 6.759 *events*. Langkah mitigasi dari setiap celah keamanan berdasarkan kerentanan yang terdapat setiap aplikasi atau sistem akan berbeda.

4.3 Keterbatasan Penelitian

Penelitian ini hanya mengolah log firewall dengan tipe threat yang terkumpul selama satu bulan. Untuk penerapan secara langsung pada lingkup jaringan UII perlu adanya persiapan terkait komputer yang memadai dan memenuhi kebutuhan pengolahan data yang lebih besar dan diproses secara *real-time*.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan dari hasil temuan, pembahasan, dan analisis yang sudah dilakukan penulis, dapat ditarik kesimpulan bahwa implementasi Security Information and Event Management (SIEM) dengan aplikasi Splunk sudah berhasil dilakukan. *Rules* yang dibuat dapat diterapkan dengan baik serta menghasilkan data statistik dan visualisasi yang dibutuhkan untuk analisis tren ancaman serangan siber dan ditampilkan pada *dashboard* untuk memudahkan pembacaan. Dengan adanya penelitian ini diharapkan dapat membantu *Security Operation Center* Badan Sistem Informasi UII untuk menganalisis tren serangan siber pada jaringan UII dan juga pembuatan laporan ancaman siber serta bahan pertimbangan untuk manajemen risiko dari ancaman serangan dan mitigasi serangan siber.

5.2 Saran

Peneliti menyadari masih banyak kekurangan pada penelitian ini, ada beberapa saran agar penelitian selanjutnya menjadi lebih baik sebagai berikut:

1. Perlu melakukan eksplorasi terkait dampak dan risiko yang ada pada serangan serta penggunaan hasil analisis tren siber untuk tahap penanganan dan mitigasi serangan siber.
2. Melakukan simulasi serangan atau deteksi secara *real-time* untuk membandingkan performa dan hasil yang didapat.
3. Menerapkan *rules* pencarian Splunk untuk mempredikasi yang akan datang menggunakan *trendline* atau melakukan pencarian *threat* yang belum terdapat pada *signature-base* Palo Alto dengan Splunk.

DAFTAR PUSTAKA

Al-Duwairi, B., Al-Kahla, W., AlRefai, M. A., Abdelqader, Y., Rawash, A., & Fahmawi, R. (2020). SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *International Journal of Electrical and Computer Engineering*, *10*(2), 2182–2191. https://doi.org/10.11591/ijece.v10i2.pp2182-2191

Bachane, I., Adsi, Y. I. K., & Adsi, H. C. (2016). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. *2016 Third International Conference on Systems of Collaboration (SysCo)*, 1–3. https://doi.org/10.1109/SYSCO.2016.7831327

Badan Siber dan Sandi Negara. (2021). *Laporan Tahunan Monitoring Keamanan Siber 2021*.

Badan Sistem Informasi Universitas Islam Indonesia. (n.d.). *Sekilas Tentang BSI*. Retrieved July 20, 2022, from https://bsi.uii.ac.id/sekilas-bsi/

Citra, A. (2019). *REAL TIME ANALISIS KEAMANAN ROUTER DI JARINGAN DENGAN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI (KAMI) Studi Kasus : Dinas Komunikasi dan Informatika Kota Tegal*.

Dewantara, R., Sugiantoro, B., & Korespondensi, P. (2021). EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA JARINGAN (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*, 1137–1148. https://doi.org/10.25126/jtiik.202183123

Erwinsyah, Y. B. (2019). *KONSOLIDASI DAN VISUALISASI LOG SERVER BSI UII MENGGUNAKAN ELK STACK*. http://hdl.handle.net/123456789/17428

Mohamad, I. (2022). *UJI COBA SISTEM KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT DAN SIEM PADA JARINGAN KOMPUTER PT. GLORIA MAJU CAHAYA*. https://repository.mercubuana.ac.id/id/eprint/60364

Muhammad Alfandi. (2022). *Analisa Security Information and Event Managemet (SIEM) menggunakan Elasticsearch dan Splunk*.

Palo Alto. (2022). *Palo Alto Network Documentation*. https://docs.paloaltonetworks.com

Peraturan Rektor UII. (2020). *PR No 15 2020 Kebijakan Teknologi Informasi di UII*.

Pratama, A., Wijaya, A., & Nasrul Halim, R. D. (2016). *PENERAPAN NETWORK MONITORING MENGGUNAKAN SECURITY INFORMATION AND EVENT*

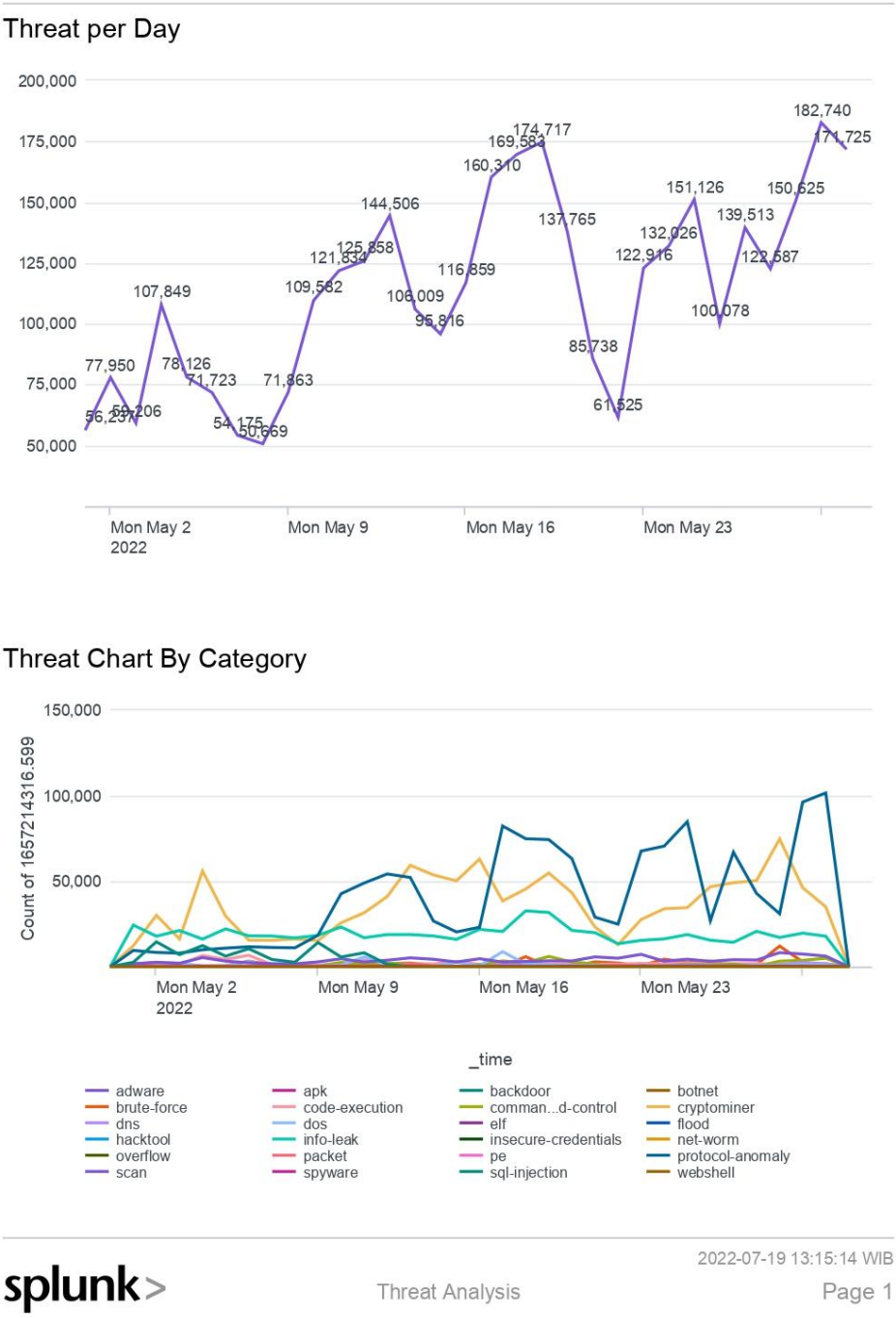
MANAGEMENT (SIEM) BERBASIS OPEN SOURCE DI UNIVERSITAS BINA DARMA PALEMBANG.

Rakhmadani, Syaifudin, & Sari, Z. (2019). *INTEGRASI VISUALISASI MODERN HONEY NETWORK (MHN) DENGAN SPLUNK*.

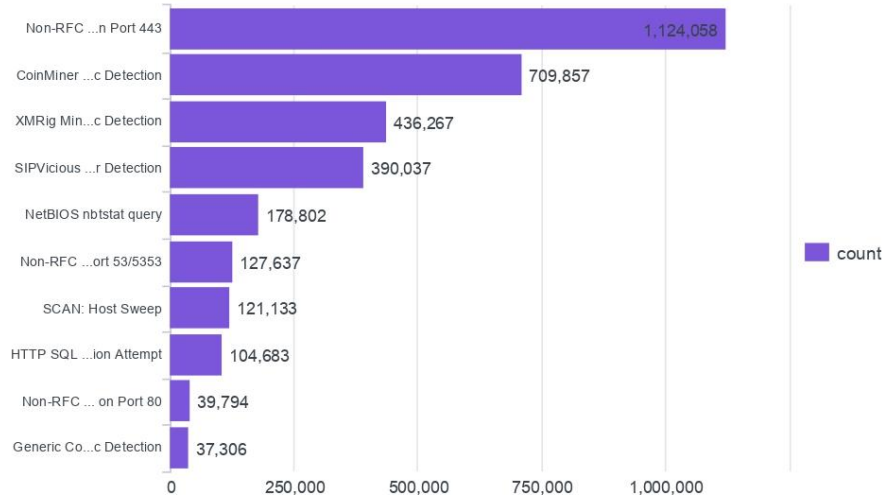
Wahluf, A. (2021). *IMPLEMENTASI SPLUNK DALAM MEMBANGUN SECURITY INFORMATION AND EVENT MANAGEMENT BERDASARKAN LOG FIREWALL TRAFFIC TYPE (STUDI KASUS: JARINGAN UII)*. https://dspace.uii.ac.id/handle/123456789/29642

LAMPIRAN

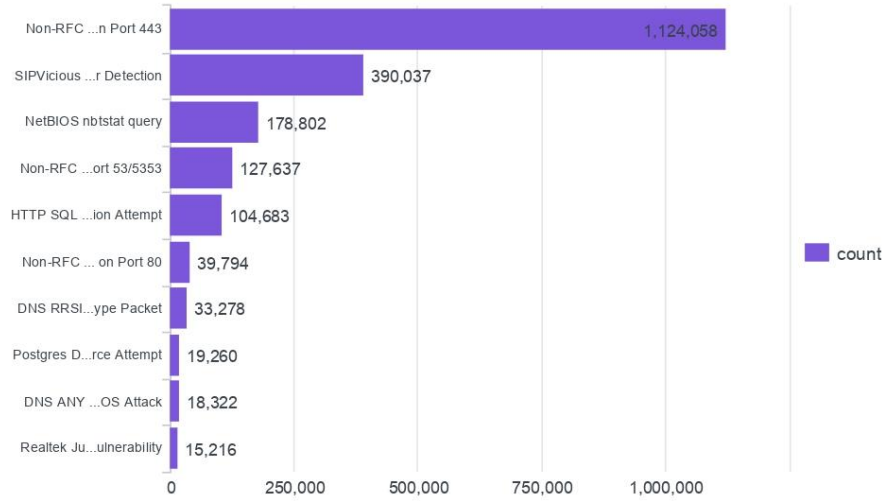
Hasil export dashboard ke file PDF



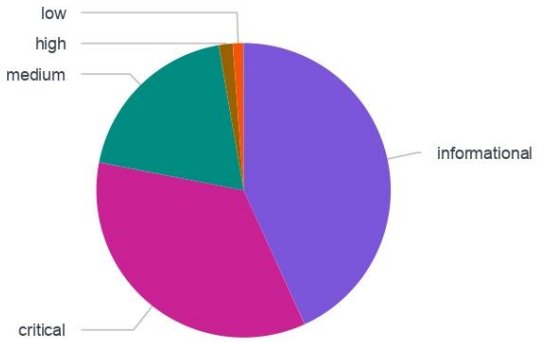
Top 10 Threat



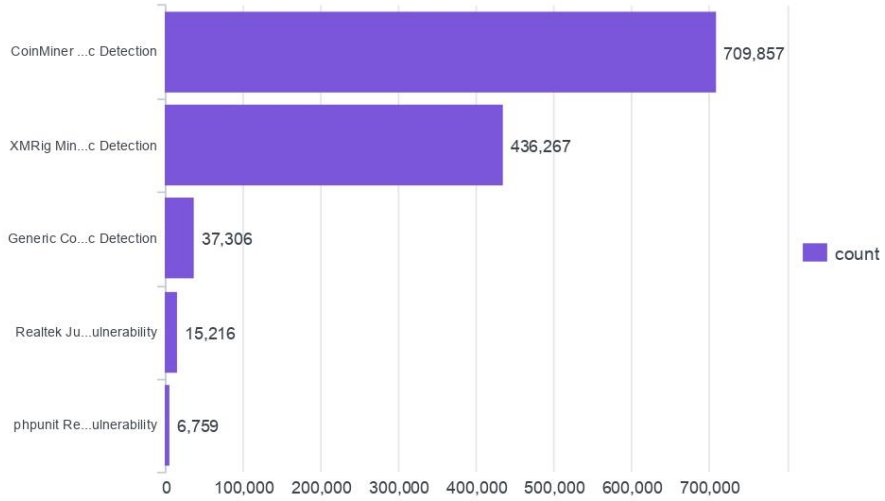
Top 10 Vulnerability



Threat Severity



Top 5 Threat with Critical Severity



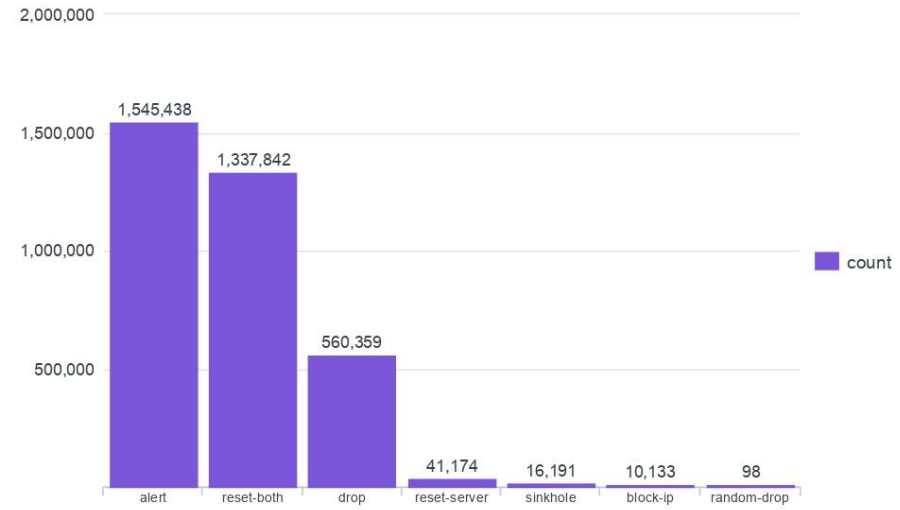
Top 10 Users with Protocol-Anomaly

user	count	percent
uii.ac.id\17312350	3401	3.957090
uii.ac.id\21421023	1243	1.446240
uii.ac.id\19312495	1226	1.426460
uii.ac.id\19423009	1165	1.355487
uii.ac.id\13525034	1130	1.314764
21320288@uii.ac.id	939	1.092534
uii.ac.id\19323031	915	1.064610
uii.ac.id\ghoffar.a	757	0.880775
uii.ac.id\011002428	746	0.867977
sekartadjie.2020@student.uny.ac.id	606	0.705086

Top 10 IP address with Protocol-Anomaly

src_ip	count	percent
103.95.7.6	81245	6.225690
103.95.7.4	70689	5.416798
103.95.7.18	61560	4.717256
103.95.6.7	61252	4.693654
103.55.139.75	45667	3.499398
103.95.7.9	40875	3.132194
103.95.6.5	39650	3.038323
103.95.6.8	30887	2.366827
103.95.7.10	27698	2.122459
103.95.6.13	23939	1.834412

Vendor (PAN) Action



Source IP address Location