BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Information Secruity event merupakan sebuah kejadian yang teridenttifikasi(diamati) dari suatu keadaan sistem, *service*, atau *network* yang mengindikasikan konsekuensi negatif seperti pelanggaran *policies*, pelanggaran standar security practice atau kegagalan control, atau situasi yang sebelumnya tidak diketahui yang mungkin berkaitan dengan keamanan[1]. Salah satu jenis Information Security Event adalah anomali *traffic*. Anomali traffic merupakan keaadan abnormalitas yang terjadi pada lalu lintas *network* sehingga dapat menyebabkan penurunan performa jaringan bahkan hingga melumpuhkan jaringan[2].

Bedasarkan data-data yang dipublikasi oleh BSSN, setiap tahunnya terjadi peningkatan anomali traffic yang muncul di Indonesia. Pada bulan Agustus 2023, tercatat 78.464.384 anomali *traffic* yang terjadi di Indonesia. Terjadi 75% peningkatan munculnya anomali dibulan Agustus 2023 daripada satu tahun sebelumnya yaitu pada bulan Agustus 2022 yang hanya terdapat 44.776.891. Oleh sebab itu, organisasi maupun instansi baik swasta atupun pemerintah haruslah mengimplementasikan Security Operation Center (SOC) agar mengurangi resiko yang berkaitan dengan *cybersecurity*[3]. SOC sendiri merupakan sebuah pusat pengendalian operasi *cybersecurity* dari suatu organisasi[4]. Tujuan utama diimplementasikannya SOC adalah untuk memonitor, menganalisis, dan mitigasi *information security event* sehingga *confidentiality*, *intergrity*, dan *availability* dari informasi teknologi suatu organisasi atau perusahaan dapat terlindungi. Sistem yang berjalan pada SOC haruslah berkerja secara efektif dalam hal mendeteksi, menganalisis, dan merespon terhadap ancaman cybersecurity. Hal tersebut mencakup kombinasi dari ketiga aspek yaitu manusia, proses, dan teknologi yang berkerja sama untuk mengelola postur keamanan suatu organisasi yang mana merupakan syarat minimal untuk suatu SOC dikatakan baik[4].

Pada diskusi panel di Workshop persiapan pembentukan CSIRT 2024, Adi Himawan Plt. Direktur Keamanan Siber Dan Sandi Pembangunan Manusia Badan Siber Sandi Negara memberikan kesimpulan bahwa tingkat penerapan tata kelola, pengelolaan insiden, dan penerapan kontrol keamanan siber di perguruan tinggi masih belum optimal. Ditambah dengan kurangnya pemenuhan kebutuhan SDM keamanan siber di perguruan tinggi sehingga adanya insiden keamanan siber ini berdampak signifikan pada layanan di perguruan tinggi. Menanggapi hal ini pemerintah melalui Kementrian Pendidikan, Kebudayaan, Riset, dan Teknologi (KEMENDIKBUDRISTEK) telah mengeluarkan PERSEJEN NO. 11 Tahun 2022 tentang Sistem Manajemen Keamanan Informasi pada SPBE KEMENDIKBUDRISTEK. Sehingga terbentuklah EDUCSIRT yang melakukan koordinasi dalam pembentukan SOC dan Cyber Security Incident Respond Team (CSIRT) di perguruan tinggi.

Universitas Komputer Indonesia (UNIKOM) sebagai salah satu perguruan tinggi swasta berakreditasi unggul di Indonesia juga didorong oleh EDUCSIRT untuk memiliki SOCnya sendiri. Selain itu salah satu jobdesk dari divisi INFRANET UNIKOM bedasarkan SK REKTOR NO 3168/SK/REKTOR/UNIKOM/XII/2022 adalah membuat sistem yang mampu terjaga keamaanannya, tidak dapat dihack atau dicuri datanya oleh pihak luar. Oleh karena itu dibutuhkan SOC untuk membuat sistem yang berjalan di UNIKOM dapat terjaga keamanannya. Saat ini UNIKOM memiliki 2 dari 3 aspek yang menjadi syarat minimal suatu SOC dikatakan baik, yaitu manusia dan teknologi. Aspek proses belum dimiliki oleh UNIKOM dan juga pada aspek teknologi, teknologi yang dimiliki UNIKOM belum terintergrasi secara terpusat dalam hal pencatatan *information security event*. Selain itu dikarenakan monitoring *security event* belum terpusat, maka tidak memungkinkan untuk melakukan *reporting* terhadap *security event* yang terjadi di lingkungan UNIKOM.

Bedasarkan Rahman[5], suatu SOC membutuhkan *Security Information* and *Event Management* (SIEM) untuk menjadi bagian intergral dari sistem yang berjalan. SIEM digunakan untuk menyelesaikan masalah *flow control*, dari

Information Security Event yang datang dari *Information Protection Tools* serta mengkomputerasikan proses pengelolaan *Information Security Incident*. Tujuan dari SIEM adalah untuk membantu organisasi agar dapat lebih cepat merespon dan menghubungkan seluruh *security event* yang terjadi menjadi sebuah rangkaian yang bermakna[6].

Salah satu *tools* SIEM yang dapat digunakan adalah Wazuh. Wazuh sendiri merupakan sebuah security platform gratis dan opensource. Wazuh terdiri dari *single-universal agent* dan 3 komponen pusat yaitu Indexes, Server, dan Dashboard. Wazuh berfungsi untuk melindungi beban kerja dari cloud, container, atau server.

Kelebihan dari Wazuh adalah *setup* dan *user interface* yang lebih sederhana dibandingkan dengan *tools* SIEM lainnya. Hal tersebut memungkinkan Wazuh untuk diterapkan secara cepat. Dengan *interface* yang sederhana tersebut, maka waktu yang digunakan untuk memahami dan mempelajari penggunaan *interface* Wazuh menjadi lebih sedikit. Kekurangan dari Wazuh ada pada saat proses skalabilitas, konfigurasi yang dilakukan masihlah manual dibandingan dengan *tools* SIEM lainnya. Dari kelebihan dan kekurangan yang telah disampaikan, penggunaan *tools* Wazuh sebagai SIEM sangatlah cocok untuk organisasi yang tidak terlalu besar dan budget yang dikeluarkan tidak terlalu berfokus kepada solusi keamanan[7].

Bedasarkan uraian masalah diatas, penilit membuat topik penelitian dengan judul “Implementasi *Security Information and Event Managemen*t (SIEM) di Lingkungan UNIKOM”.

1.2 Rumusan Masalah

Adapun masalah yang dapat dirumuskan adalah:

1. Belum adanya suatu sistem yang mengendalikan operasi *cybersecurity* secara terpusat di lingkungan UNIKOM
2. Belum adanya teknologi untuk monitoring dan reporting secara terpusat event security yang terjadi terhadap sumber daya digital UNIKOM.

1.3 Tujuan

Adapun Tujuan dari penelitian sebagai berikut:

1. Terbentuknya SOC di UNIKOM.
2. SIEM melakukan monitoring dan reporting terhadap event security di lingkungan UNIKOM.

1.4 Batasan Masalah

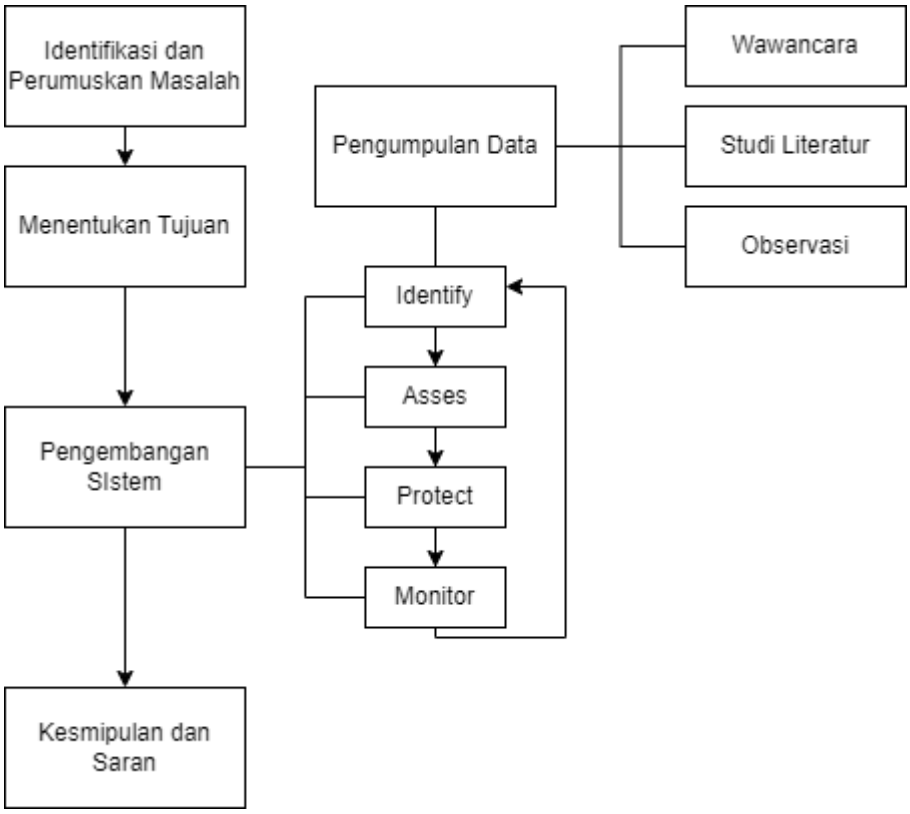
Adapun batasan masalah dari penelitian ini sebagai berikut:

1. Penelitian ini menggunakan tools SIEM yang *open source*.
2. Penelitian ini menggunakan sistem Operasi Ubuntu sebagai Wazuh server.
3. Penelitian ini hanya menggunakan 8 *endpoint* di Universitas Komputer Indonesia sebagai tempat di distribusikannya agent.
4. Endpoint yang digunakan sebagai tempat didistribusikannya agent hanya endpoint yang berlokasi pada Server Host 2 di Node 1 dan Node 2.
5. Penelitian ini hanya menggunakan Agent Collection untuk melaksanakan operasi Security Event Collection.
6. Penelitian ini menggunakan sistem operasi Kali Linux sebagai komputer penyerang.

1.5 Metodelogi Penelitian

Metode Penelitian merupakan kumpulan kegiatan berurutan dalam mencari kebenaran suatu studi penelitian, yang dimulai dengan bantuan dan persepsi penelitian terdahulu, guna membentuk suatu kesimpulan melalui tahap pengolahan dan analisis[8]. Adapun metodelogi penelitian yang digunakan adalah metode analisis deskriptif. Metode analisis deskriptif merupakan sebuah metodelogi penelitian yang berusaha mendeskripsikan suatu gejala, peristiwa, kejadian yang terjadi pada saat sekarang. Metode anallisis deskriptif memusatkan perhatian kepada pemecahan masalah aktual sebagaimana adanya pada saat penelitian dilaksanakan. Kemudian hasilnya akan diambil dan dianilis untuk

menghasilkan sebuah kesimpulan. Berikut ini Gambar 1.1 merupakan alur penelitian:



Gambar 1.1 Alur Penelitian

Berikut ini penjelasan dari masing-masing tahapan yang ada pada alur penelitian sesuai dengan Gambar 1.1:

1.5.1 Identifikasi dan Perumusan Masalah

Pada tahap ini dilakukan pengidentifikasian masalah dan perumusan masalah. Identifikasi masalah merupakan pencarian masalah yang relevan melalui observasi, dedukasi, rekomendasi hasil penelitian, masalah sosial, serta pengalaman pribadi. Masalah merupakan kesengjangan yang antara harapan dengan kenyataan, antara kebutuhan dengan yang tersedia, antara yang seharusnya dengan yang ada[9]. Adapun tempat masalah yang diidentifikasi berlokasi di

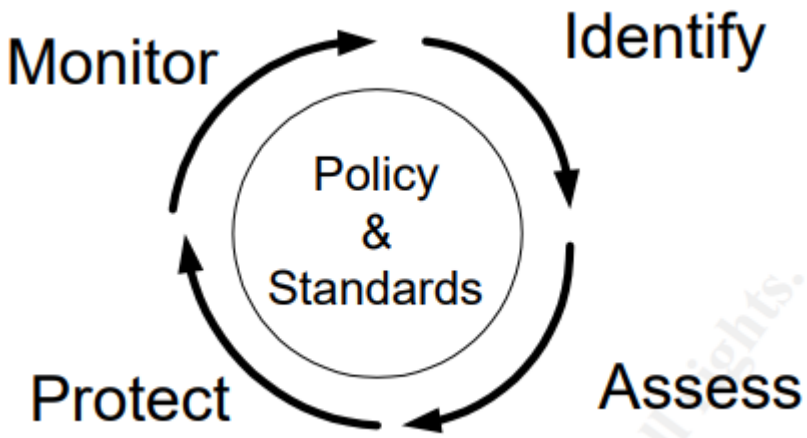
Universitas Komputer Indonesia. Setelah masalah diidentifikasi selanjutnya dilakukan perumusan masalah

1.5.2 Menentukan Tujuan

Pada tahap ini, dilakukan perumusan tujuan penelitian bedasarkan identifikasi dan rumusan masalah yang dilakukan pada tahap ke 1.

1.5.3 Pengembangan Sistem

Pada tahap ke 3, dilakukan tahap pengembangan sistem. Adapun Model pengembangan sistem yang digunakan adalah model Security Lifecycle versi dari Robert Pfau yang publikasi oleh SANS institute.



Gambar 1.2 Security Life Cycle (Robert Pfau 2003)

Pada model Security Lifecylce terdapat beberapa tahapan yaitu Identify, Assess, Protect, Monitor. Adapun penjelasan dari masing-masing tahapan sebagai berikut:

1. Identify

   Tahap awal dari program keamanan adalah mengetahui apa yang ingin dilindungi. Pada tahap ini dilakukan pengumpulan data dan infromasi terhadap jaringan, server, dan informasi terkait lainnya.

   a. Pengumpulan Data

Pada tahap identify ini, dilakukan pengumpulan data yang relevan yang digunakan untuk mencapai tujuan yang telah ditentukan pada tahap 2. Adapun beberapa metode yang digunakan untuk pengumpulan data terbagi menjadi:

i. Wawancara

Metode wawancara adalah metode pengumpulan data yang dilakukan untuk menggali pemahaman, pandangan atupun pengalaman seseorang terkati suatu topik melalui tanya jawab langsung antara peneliti dan narasumber. Pada penelitian ini, peneliti akan melakukan wawancara terhadap staf infrastruktur Universitas Komputer Indonesia.

ii. Studi Literatur

Metode studi literatur adalah metode pengumpulan data yang berfokus pada analissi literatur yang telah dipublikasi. Metode ini dilakukan dengan cara mencari, membaca, dan mereview literatur mengenai Security Operation Center, Security Information and Event Management, Wazuh, dan berbagai jenis serangan.

iii. Observasi

Metode observasi adalah metode pengumpulan data yang melibatkan pengamatan langsung terhadap objek peneltiana secara sistematis. Observasi akan dilakukan terhadap perangkat-perangkat yang digunakan pada jaringan unikom serta server Wazuh.

2. Assess

Tahap Assess pada model Security Lifecycle dibuat bedasarkan tahap identify. Pada tahap Assess ini dilakukan peninjauan terhadap proses dan prosedur pada organisasi serta perencanaan untuk mengamankan sistem. Pada tahap ini juga dilakukan penjabaran kebutuhan pengamanan sistem seperti kebutuhan akan software, hardware, dan regulation.

3. Protect

Tahap protect ini didasarkan pada tahap Assess. Pada tahap ini dilakukan implementasi security resources tambahan sesuai dengan rencana yang telah dibuat ditahap sebelumnya.

4. Monitor

Pada tahap ini dilakukan pemantauan terhadap keamanan yang telah diimplementasi. Perlu dilakukan pengujian untuk memvalidasi keefektifan dari peningkatan keamanan.[10]

1.5.4 Kesimpulan dan Saran

Pada tahap ini, dilakukan pembuatan kesimpulan terhadap hasil penelitian yang dilakukan. Diikuti dengan perumusan saran bedasarkan hasil kesimpulan yang dibuat agar penelitian selanjutnya dapat menberikan hasil yang yang lebih baik.

1.6 Sistematika Penulisan

Sistematika penulisan memberikan susunan agar bisa lebih dipahami dengan menyusunnya menjadi beberapa BAB yaitu

BAB 1 PENDAHULUAN

BAB 1 menguraikan penjelasan singkat mengenai latar belakang masalah , rumusan masalah, tujuan, batasan masalah dan penjelasan mengenai metodelogi penelitian yang cocok untuk masalah yang sedanag dihadapi. Serta sistematika penulisan yang akan dibuat.

BAB 2 LANDASAN TEORI

BAB 2 membahas mengenai teori-teori pendukung yang behubungan erat dengan masalah yang dibahas.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

BAB 3 membahas mengenai analisis dan perancangan dari sistem yang akan dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

BAB 4 membahas mengenai implementasi dan pengujian dari sistem yang telah dibangun.

BAB 5 KESIMPULAN DAN SARAN

BAB 5 menguraikan kesimpulan yang diperoleh dari hasil pengujian sistem serta saran untuk pengembangan sistem selanjutnya.