IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PADA APLIKASI SMS CENTER PEMERINTAH DAERAH PROVINSI NUSA TENGGARA BARAT

(*Implementation of Security Information And Event Management (SIEM) in The SMS Center Application for The West Nusa Tenggara Provincial Government***)**

Husnul Khotimah [1], Fitri Bimantoro [1], Robert Silas Kabanga [2], Ida Bagus Ketut Widiartha [1]
[1]Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
[2] Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat
Jl. Udayana No. 14 Mataram, Lombok, NTB, INDONESIA
Email: husnulhk31@gmail.com, bimo@unram.ac,id, kominfotik@ntbprov.go.id, widi@unram.ac,id

Abstrak

Seiring dengan pesatnya penggunaan teknologi informasi dan komunikasi, ancaman siber juga turut mengalami peningkatan. Bertolak dari beberapa permasalahan keamanan siber diperlukan suatu sistem yang dapat mengantisipasi banyaknya serangan dan atau insiden siber atas sistem di pemerintahan. Solusi yang bisa digunakan untuk memonitor serangan yang ada adalah penggunaan Security Information and Event Management (SIEM). Penggunaan plaform wazuh yang mengimplementasikan teknologi SIEM dapat mengumpulkan informasi keamanan yang berasal dari data log. Berdasarkan hasil implementasi dan analisis log yang dilakukan menunjukkan bahwa teknologi SIEM dapat mempermudah dalam memonitoring serangan yang dapat mengancam keamanan sistem.

Keywords: *Cyber Security, Aplikasi, Log, Monitor, Informasi.*

1. PENDAHULUAN

1.1. Latar Belakang

Era digital merupakan era teknologi dengan perkembangan yang sangat pesat. Seiring dengan pesatnya penggunaan teknologi informasi dan komunikasi, ancaman siber pun juga turut mengalami peningkatan. Beberapa dari ancaman siber ditujukan pada infrastruktur teknologi informasi dan komunikasi, yang menyebabkan runtuhnya sistem tatanan sosial, kelumpuhan ekonomi nasional dan melemahnya sistem pertahanan.

Bertolak dari beberapa permasalahan keamanan siber tersebut diperlukan suatu sistem yang dapat mengantisipasi banyaknya serangan dan atau insiden siber atas sistem di pemerintahan. Maka dari diperlukan pendeteksian terhadap anomali sistem keamanan yang digunakan pada sistem pemerintah. Deteksi anomali merupakan kegiatan analisis terhadap data signifikan pada sistem yang berguna untuk menemukan data yang tidak normal sehingga dapat membantu menanggulangi permasalahan keamanan sistem [1].

Solusi yang bisa digunakan untuk memonitor serangan yang ada adalah penggunaan *Security Information and Event Management* (SIEM). Teknologi SIEM ini dapat digunakan untuk mengumpulkan informasi keamanan yang berasal dari data *log* pada jaringan, aplikasi, dan hardware. Teknologi SIEM mampu mengumpulkan data dalam jumlah yang cukup besar dan mampu menghubungkan dan menganalisis peristiwa dari berbagai sumber.

Berdasarkan uraian yang disampaikan diatas, maka pada pengabdian masyarakat kali ini akan dilakukan pengimplementasian SIEM pada salah satu aplikasi SMS Center Pemerintah Daerah Provinsi NTB. SMS Center merupakan sebuah aplikasi yang menyediakan layanan SMS *Gateway* Pemerntah Provinsi NTB yang digunakan untuk *broadcast* dan mengirim pesan berbasis sms. Tools yang akan digunakan sebagai solusi yang ditawarkan adalah menggunakan aplikasi Wazuh. Wazuh merupakan perangkat berbasis *Open Source* yang menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat dan mengumpulkan *log* dari suatu sistem.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan dari pokok permasalahan tersebut adalah "Bagaimana menerapkan *Security information and Event Management* (SIEM) pada aplikasi SMS Center Pemerintah Daerah Provinsi Nusa Tenggara Barat".

1.3. Batasan Masalah

Adapun untuk batasan masalah, penulis membatasi pembahasan yang akan disampaikan agar memiliki batasan dan ukuran sesuai dengan bagian yang dikerjakan. Adapun batasan masalah yang akan dibahas dalam laporan ini, yaitu :

1. Sistem ini merupakan *security* sistem yang dibangun menggunakan platform Wazuh.
2. *Security Information and Event Management* (SIEM) diterapkan pada sistem pemerintah Provinsi Nusa Tenggara Barat.
3. Keamanan jaringan dilakukan dengan memantau aktifitas *log* dan analisis terhadap serangan yang berpotensi sebagai ancaman pada host atau aplikasi SMS Center.

1.4. Tujuan Masalah

Berdasarkan latar belakang yang telah dijelaskan, tujuan kegiatan pengabdian masyarakat yang dilakukan yaitu penerapan *Security Information and Event Management* (SIEM) pada aplikasi SMS Center yang dapat membantu memonitoring keamanan komputer dan anomali perubahan sistem aplikasi.

2. TINJAUAN PUSTAKA

2.1. Profil Singkat Diskominfotik Provinsi NTB

Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat merupakan perangkat daerah yang memiliki tugas pokok menyelenggarakan Urusan Pemerintahan Bidang Komunikasi dan Informatika, Urusan Pemerintahan Bidang Statistik serta Urusan Pemerintahan Bidang Persandian yang menjadi kewenangan Daerah Provinsi dan Tugas Pembantuan yang ditugaskan kepada Daerah Provinsi. Dalam menyelenggarakan Tugas Pokok sebagaimana dimaksud, Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat mempunyai fungsi :

1. Perumusan kebijakan strategis dibidang Komunikasi, Informatika dan Statistik.
2. Pelaksanaan koordinasi, fasilitasi, monitoring, evaluasi dan pelaporan dibidang Komunikasi, Informatika dan Statistik.
3. Pelaksanaan administrasi dinas dan Pembinaan dibidang Komunikasi, Informatika dan Statistik.
4. Pelaksanaan fungsi lain yang diberikan oleh pimpinan sesuai dengan bidang tugas.

2.2. Keamanan Komputer (*Cybersecurity*)

Cybersecurity terdiri dari dua kata yaitu *cyber* yang berarti dunia maya dan *security* yang berarti keamanan sehingga jika digabungkan *cybersecurity* memiliki arti keamanan siber. *Cybersecurity* atau keamanan siber berperan dalam mendeteksi, memperbaiki, atau menurunkan tingkatan risiko dari ancaman siber (*cyber threat*) dan serangan siber (*cyber attack*) serta seluruh kegiatan yang memberi ancaman terhadap keamanan seluruh komponen sistem siber[2]. Konsep dasar *cybersecurity* atau yang disebut sebagai The CIA *Triad* terdiri dari 3 unsur dasar yaitu [3]:

1. *Confidentiality* atau kerahasiaan merupakan sebuah aturan yang membatasi akses yang dimiliki seseorang atau organisasi agar informasi tersebut tidak dapat diakses oleh orang lain.
2. *Integrity* atau integritas yaitu memastikan data yang dimiliki seseorang atau organisasi konsisten, akurat, dan dapat dipercaya selama periode tertentu.
3. *Availability* atau ketersediaan, yaitu ketersediaan perangkat keras, perangkat lunak, dan jaringan yang harus dipelihara dan ditingkatkan performanya agar bisa melindungi data kita secara maksimal.

2.3. CSIRT (Gov CSIRT : csirt.ntbprov.go.id)

CSIRT (*Computer Security Insiden Response Team*) merupakan suatu organisasi atau tim yang menyediakan pelayanan dalam mencegah, menanggulangi dan menanggapi insiden keamanan siber [4]. *Computer Security Incident Response Team* (CSIRT) pada sektor pemerintah daerah Provinsi Nusa Tenggara Barat atau disebut NTB-PROV CSIRT diketuai oleh Kepala Dinas Diskominfotik Provinsi NTB. Pembentukan NTB-PROV CSIRT memilliki visi terwujudnya ketahanan siber pada sektor Pemerintah Daerah Provinsi NTB yang andal dan professional. Beberapa misi yang dijalankan NTB-PROV CSIRT yaitu mengkoordinasikan dan mengolaborasikan layanan keamanan siber serta membangun kapasitas sumber daya keamanan siber pada sektor Pemerintah Daerah Provinsi NTB. NTB-PROV CSIRT akan melakukan kerjasama dan berbagi informasi dengan Gov-CSIRT Indonesia (BSSN) atau organisasi lain dalam lingkup keamanan siber.

Beberapa layanan yang diberikan oleh NTB-PROV CSIRT yaitu:

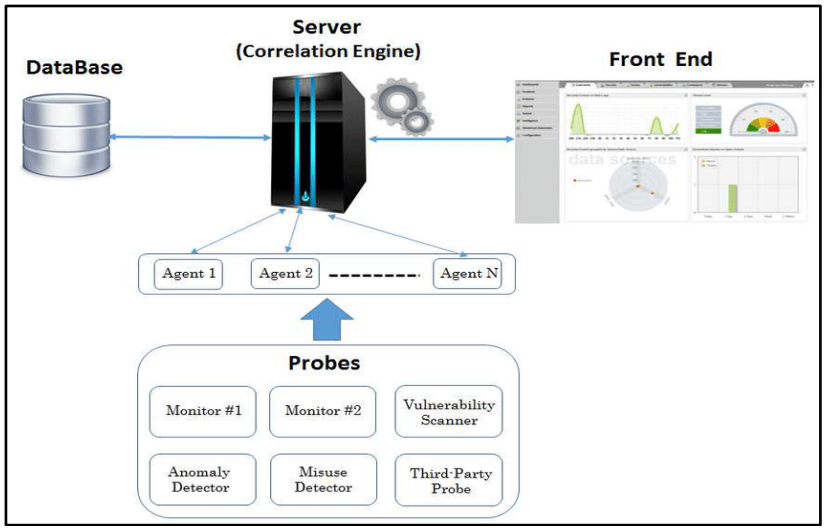
1. Layanan Reaktif
   Layanan reaktif dari NTB-PROV CSIRT merupakan layanan utama dan bersifat prioritas yaitu :
   a. Layanan pemberian peringatan terkait dengan laporan insiden siber.
   b. Layanan penanggulangan dan pemulihan Insiden.
   c. Layanan penanganan kerawanan.
   d. Layanan penanganan artifak.
2. Layanan Proaktif
   NTB-PROV CSIRT secara aktif membangun kapasitas sumber daya keamanan siber melalui aktivitas :
   a. Pemberitahuan hasil pengamatan terkait dengan ancaman baru.
   b. Layanan sosialisasi ancaman siber.
3. Layanan Manajemen Kualitas Keamanan
   NTB-PROV CSIRT meningkatkan kualitas keamanan melalui aktivitas :
   a. Konsultasi terkait kesiapan penanggulangan dan pemulihan Insiden.
   b. Pembangunan kesadaran dan kepedulian terhadap keamanan siber.
   c. Pembinaan terkait kesiapan penanggulangan dan pemulihan insiden.

2.4. Aplikasi SMS Center

SMS Center merupakan suatu aplikasi yang memberikan layanan SMS Gateway yang dapat digunakan oleh internal pemerintah Provinsi NTB untuk melakukan broadcast dan mengirim pesan berbasis sms. Setiap SMS yang masuk akan dikelola dan diklasifikasi dengan baik oleh Bidang Persandian dan Keamanan Informasi Dinas Komunikasi Informatika dan Statistik Provinsi NTB.

2.5. SIEM

Security Information and Event Management (SIEM) merupakan sistem monitoring yang mampu mendeteksi serangan dan *respons* sistem keamanan terhadap serangan melalui analisis *log* dari berbagai event-*log* yang bersumber dari data secara *real-time* [5]. *Log* merupakan informasi dari perangkat yang berisi kegiatan dari *log* tersebut, mulai dari lalu lintas jaringan, status dari perangkat dan lainnya.



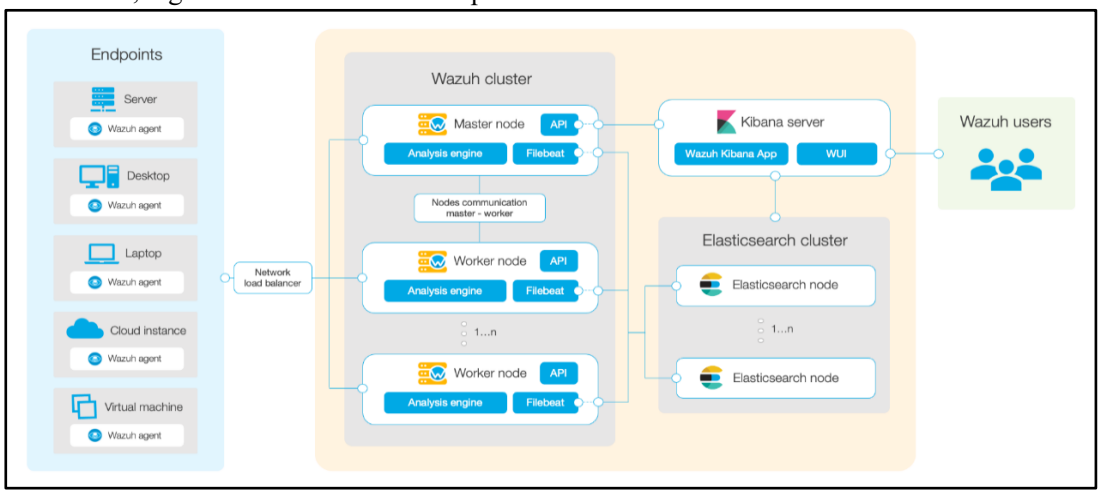
Gambar 3.1 *Architecture of a SIEM System*

Sistem SIEM bekerja dengan mengumpulkan data dari berbagai sumber dalam infrastruktur jaringan, termasuk dari jaringan, *security*, server, database, dan aplikasi untuk mengidentifikasi potensi ancaman, baik yang berasal dari eksternal ataupun internal. Perangkat-perangkat pemberi *input* SIEM dianggap sebagai sensor yang menangkap kejadian sesuai dengan tempatnya berada. Data yang berhasil dikumpulkan akan ditampilkan pada *dashboard* dalam bentuk *chart* sehingga lebih mudah dibaca dan dimengerti, ataupun lebih mudah menemukan suatu pola khusus. SIEM menyediakan penyimpanan jangka panjang, sehingga dapat dilakukan korelasi data dalam jangka waktu yang cukup lama. Teknologi SIEM dapat melakukan teknik korelasi yang terintegrasi dengan berbagai sumber data, sehingga data dapat diproses menjadi informasi yang bermanfaat.

2.6. Wazuh

Wazuh merupakan *platform open source* yang berfungsi sebagai sistem deteksi ancaman, pemantauan keamanan dan respons insiden. *Platform* Wazuh merupakan implementasi dari *Security Information and Event Management* (SIEM). Wazuh menyediakan berbagai fitur yang dapat menganalisis data *log*, intruksi dan deteksi malware, pemantauan integritas file, penilaian konfigurasi dan deteksi kerentanan sistem. Wazuh memiliki 3 buah komponen yaitu :

1. Wazuh *Agent*, merupakah sebuah *end points* seperti desktop, server, instans *cloud* atau mesin virtual, yang dapat melakukan pencegahan, deteksi, dan respons.
2. Wazuh Server, merupakan server yang bertugas menganalisis data yang diterima oleh *agent* dan memprosesnya melalui *decoder* dan aturan.
3. Elastis Stack , digunakan untuk melakukan pencarian dan analisis.



Gambar 3.2 Wazuh *Architecture*

Wazuh *agent* akan mengirimkan *log* yang didapatkan ke Wazuh server untuk dilakukan analisis dan deteksi ancaman. Sebelum itu, wazuh *agent* akan membuat sebuah koneksi dengan layanan server. Kemudian wazuh server akan menerjemahkan *log* yang diterima menggunakan *analysis engine*. *Log* yang terdeteksi sebagai ancaman akan dibuatkan suatu *alert* yang menyimpan *rule id* dan *rule name*. Kemudian *log* tersebut akan ditampung ke dalam penyimpanan wazuh. *Filebeat* digunakan untuk mengirimkan *alert* dan *log* ke server *Elasticsearch*. Setelah data diterima oleh *Elasticsearch*, Kibana akan memvisualisaskan informasi yang didapatkan. *Interface* dari wazuh berjalan pada Kibana, sebagai *plugin*.

3. METODE PENGABDIAN MASYARAKAT

3.1. Tahap Persiapan

Kegiatan implementasi *Scurity Information and Event Management* (SIEM) pada aplikasi SMS Center Provinsi Nusa Tenggara Barat ini dilaksanakan secara bertahap diawali dengan pengumpulan materi yang berkaitan dengan *Cyber Security* dan *Scurity Information and Event Management* (SIEM). Selanjutnya secara teknis pelaksanaan kegiatan ini berupa instalasi beberapa komponen wazuh seperti Wazuh Manager dan Wazuh Agent untuk menjalankan fungsi perlindungan pada Aplikasi SMS Center Provinsi Nusa Tenggara Barat dari ancaman siber. Beberapa peralatan yang dibutuhkan untuk mendukung kegiatan ini berlangsung adalah sebagai berikut:

1. Seperangkat komputer yang terhubung ke jaringan internet.
2. Materi dokumentasi instalasi Wazuh Manager dan Wazuh Agent.

3.2. Tahap Pelaksanaan

Kegiatan pengabdian masyarakat di kantor Dinas Komunikasi Informasi dan Statistika Provinsi Nusa Tenggara Barat dilaksanakan selama 2 dimulai sejak tanggal tanggal 24 Januari 2022 sampai dengan 24 Maret 2022. Dengan waktu kerja sebanyak lima hari (Senin-Jum'at) dalam seminggu. Adapun beberapa pelaksanaan kegiatan pengabdian yang dilakukan yaitu :

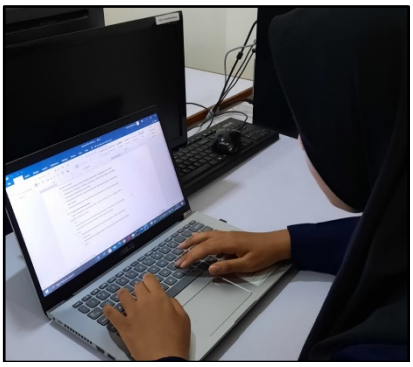
1. Pengumpulan dan pendalaman materi berkaitan dengan *Cyber Security* dan *Security Information and Event Management* (SIEM).
2. Pembuatan Wazuh Manager dan Wazuh *Agent* pada aplikasi SMS Center.
3. Analisis jenis serangan yang ditangkap oleh Wazuh Agent aplikasi SMS Center.

3.3. Tahap Evaluasi

Evaluasi kegiatan dilaksanakan pada saat pelaksanaan kegiatan berlangsung seperti saat pengujian terhadap pemahaman materi, serta pada saat proses instalasi komponen Wazuh yang digunakan. Selain itu evaluasi juga dilakukan saat analisis log yang dihasilkan oleh sistem berlangsung. Beberapa hal lain juga dikomunikasikan melalui grup Telegram dan Whatsapp untuk mendiskusikan kendala yang dialami saat proses analisis sistem berlangsung.

4. HASIL DAN PEMBAHASAN

Kegiatan pengabdian masyarakat ini telah dilaksanakan selama 2 bulan bertempat di kantor Dinas Komunikasi Informasi dan Statistika Provinsi Nusa Tenggara Barat yakni pada tanggal 24 Januari 2022 hingga 24 Maret 2022. Kegiatan pengabdian masyarakat ini diawali dengan pengumpulan informasi mengenai *Cyber Security* dan *Security Information and Event Management* (SIEM). Informasi-informasi yang didapatkan kemudian dipelajari serta dipahami sebagai bahan pembelajaran mengenai kegiatan implementasi SIEM pada Aplikasi SMS Center Provinsi NTB. Materi pembelajaran tidak hanya berasal dari hasil pengumpulan informasi yang dilakukan individu, tetapi juga berasal dari materi yang diberikan oleh pembimbing lapangan sebagai tambahan bahan pembelajaran yang berkaitan dengan *Cyber Security* dan SIEM.



Gambar 4.1 Pengumpulan dan pemahaman materi mengenai *Cyber Security* dan SIEM

Setelah mempelajari materi *Cyber Security* dan SIEM, kegiatan pengabdian dilanjutkan dengan penginstalan Wazuh Manager dan Wazuh Agent pada aplikasi SMS Center Provinsi NTB. Pengistalan komponen wazuh tersebut dilaksanakan pada tanggal 8 Februari 2022. Sebelum proses instalasi Wazuh Agent dilakukan, terlebih dahulu terdapat proses konfigurasi agar perangkat terhubung dengan server SMS Center. Setiap tahap proses penginstalan bersumber dari dokumentasi pada *platform* Wazuh yang tersedia. Setelah proses instalasi berhasil dilakukan, Wazuh Agent SMS Center telah aktif sehingga dapat menyimpan log yang dihasilkan oleh aplikasi SMS Center Provinsi NTB.

Gambar 4.2 Proses Instalasi Wazuh

Selanjutnya dilakukan analisis terhadap *log* yang berhasil ditangkap oleh Wazuh Agent SMS Center. Analisis dilakukan pada halaman *Security Event* pada Dashboard Wazuh. Beberapa hal yang ada pada *dashboard* Wazuh antara lain total *log* yang dihasilkan oleh Wazuh Agent SMS Center dari sejak pertama dibuat yaitu tanggal 8 Februari 2022, beberapa grafik yang menyajikan 5 data tertinggi dari beberapa kategori dan detail dari setiap *log*. Analisis *log* tersebut dibagi ke dalam beberapa kategori yaitu berdasarkan jumlah *alert*, jumlah *rule groups*, jumlah

PCI DSS, dan tingkatan level dari *log* tersebut. *Log* dengan data tertinggi pada setiap kategori diberi penjelasan dari setiap bagian dari informasi yang ada pada *log* tersebut.

Gambar 4.3 Analisis *Log* pada Wazuh

Hasil analisis terhadap log yang ditangkap oleh Wazuh Agent SMS Center ini dapat membantu tim yang memiliki tugas yang berkaitan dengan keamanan Teknologi Informasi pemerintah provinsi NTB untuk mengetahui serangan apa saja yang ada pada aplikasi SMS Center. Selain itu tim tersebut juga dapat dimudahkan dalam memberikan penanganan yang sesuai terhadap jenis serangan yang ada pada aplikasi SMS Center. Dengan begitu kedepannya aplikasi SMS Center juga dapat berjalan lebih baik dan terhindar dari serangan yang dapat merusak sistem keamanannya serta informasi yang diterima oleh masyarakat juga dapat lebih maksimal.

4.1 Faktor Pendukung

1. Dukungan dari Dosen Pembimbing dan Pembimbing Lapangan yang mengarahkan dalam penyediaan materi dan kegiatan.
2. Kerja sama yang baik dengan rekan pengabdian masyarakat.
3. Pihak Diskominfotik yang memberikan fasilitas berupa ruang kerja, perangkat komputer dan akses jaringan internet.

4.2 Faktor Penghambat

1. Membagi fokus antara pengerjaan tugas pada kegiatan pengabdian masyarakat dengan perkuliahan.
2. Kurang memahami penggunaan *Open Source* Wazuh sehingga mengalami kesulitan dalam mengenal jenis serangan siber yang ada.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil kegiatan pengabdian masyarakat di Dinas Komunikasi Informatika dan Statistik Provinsi Nusa Tenggara Barat didapatkan kesimpulan yaitu pengimplementasian *System Information and Event Management* (SIEM) pada Aplikasi SMS Center Provinsi Nusa Tenggara Barat dapat mempermudah tim keamanan Teknologi Informasi pemerintah provinsi NTB pemerintah provinsi dalam memonitoring serangan yang dapat mengancam keamanan sistem. Untuk memakasimalkan penganalisian terhadap SIEM pada aplikasi perlu dilakukan analisis terhadap bagian lain pada SIEM (*Security Inormation anda Event Management*) selain pada *security events.* Selain itu penggunaan SIEM (*Security Inormation anda Event Management*) dapat didampingi dengan pengembangan OSINT (*Open Source Intelligence*) agar monitoring terhadap keamanan dan serangan pada sistem dapat berjalan lebih maksimal.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada seluruh pihak yang telah berperan dalam kegiatan pengabdian masyarakat dengan kegiatan pengimplementasian *Security Information and Event Management* (SIEM) pada aplikasi SMS Center Provinsi NTB. Ucapan terimakasih juga disampaikan kepada pihak yang telah membantu agar hasil dari kegiatan pengabdian masyarakat ini dapat dituangkan ke dalam bentuk tulisan. Dan ucapan terimakasih juga diberikan kepada pegawai Diskominfotik NTB yang telah menyiapkan sarana dan prasarana yang yang mendukung kegiatan pengabdian masyarakat ini.

DAFTAR PUSTAKA

[1] M. R. Kamal and M. A. Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," *Automata*, no. 4, 2021.
[2] M. R. Ramadhani and A. R. Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," *Journal.Uii.Ac.Id*, vol. 1, no. 2, pp. 1–8, 2020.
[3] R. Riyandhika and R. Pratama, "Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia," *Uii*, vol. 1, no. 2, p. 1, 2020.
[4] R. Kurniawan and B. Rahardjo, "STUDI MODEL ORGANISASI CSIRTs (COMPUTER SECURITY INCIDENT RESPONSE TEAMS) PADA PERUSAHAAN BERSKALA BESAR," *Semin. Nas. Apl. Teknol. Inf.*, vol. 2007, no. Snati, pp. 1907–5022, 2007.
[5] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, "Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 1, pp. 1–7, 2019.