JURNAL BUFFER INFORMATIKA
Volume 11 Nomor 1, April 2025
p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.fkom.uniku.ac.id/index.php/buffer

Implementasi Security Information dan Event Management (SIEM) Pada Sistem Akademik Universitas Kuningan

Fitra Nugraha[1)] **, Toni Khalimi**[2)]**, Heri Herwanto**[3),]

[1,2),] *Ilmu Komputer, Universitas Kuningan, Nama Instansi*
Jl. Cut Nyak Dhien No.36A, Cijoho, Kec. Kuningan, Kabupaten Kuningan, Jawa Barat 45513, Indonesia
*Email :*fitra@uniku.ac.id[1)],*toni.khalimi@uniku.ac.id*[2)], heri.herwanto@uniku.ac.id[3)]

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan *Security Information And Event Management* (SIEM) pada sistem akademik Universitas Kuningan. Keamanan sistem informasi di lingkungan pendidikan, khususnya pada sistem akademik universitas, menjadi semakin penting mengingat ketersediaan data sensitif, seperti informasi pribadi mahasiswa dan data akademik yang harus terlindungi dengan baik. Ancaman keamanan seperti serangan cyber semakin kompleks dan seringkali dapat merugikan baik bagi universitas maupun para pengguna sistem. Dlam penelitian ini, kami menerapkan SIEM sebagai solusi untuk mendeteksi, mencegah, dan merespons ancaman keamanan pada sistem akademik Universitas Kuningan. Metode pengembangan sistem digunakan dengan langkah-langkah analisis kebutuhan sistem, perancangan sistem, implementasi sistem, pengujian sistem, dan evaluasi sistem. Luaran dari penelitian ini adalah meningkatnya tingkat keamanan sistem akademik Universitas Kuningan. Dengan implementasi SIEM, diharapkan sistem dapat mendeteksi secara cepat dan efektif potensi ancaman keamanan, meningkatkan respons terhadap insiden keamanan, serta menyediakan laporan yang berguna untuk pengambilan keputusan. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan dan perlindungan data pada sistem akademik Universitas Kuningan, serta menjadi referensi bagi institusi pendidikan lainnya dalam menghadapi tantangan keamanan informasi yang semakin kompleks.

Kata Kunci : Security Information System and Event Management;SIEM; Keamanan Jaringan; Insident Keamananan

Abstract

This research aims to implement Security Information And Event Management (Siem) in the Kuningan University academic system. The security of information systems in the educational environment, especially in university academic systems, is becoming increasingly important considering the availability of sensitive data, such as student personal information and academic data which must be properly protected. Security threats such as cyber-attacks are increasingly complex and can often be detrimental to both universities and system users. In this research, we apply SIEM as a solution to detect, prevent and respond to security threats to the Kuningan University academic system. The system development method is used with the steps of system requirements analysis, system design, system implementation, system testing, and system evaluation. The output of this research is an increase in the security level of Kuningan University's academic system. By implementing SIEM, the system is expected to be able to quickly and effectively detect potential security threats, improve response to security events, and provide reports that are useful for making decisions. Thus, it is hoped that the results of this research can make a significant contribution in improving security and data protection in the Kuningan University academic system, as well as becoming a reference for other educational institutions in maintaining increasingly complex information security defenses.

Keywords: Security Information System and Event Management; SIEM; Network Security; Security Incident

1. PENDAHULUAN

Latar belakang dan rumusan permasalahan yang akan diteliti.

Latar Belakang:

Sistem informasi akademik pada institusi pendidikan, seperti Universitas Kuningan, mengandung data sensitif, termasuk informasi pribadi mahasiswa dan data akademik. Dalam era digital saat ini, keamanan data menjadi sangat penting mengingat meningkatnya ancaman keamanan cyber yang semakin kompleks(Sumiah et al., 2023). Ancaman-ancaman seperti serangan peretasan dan pencurian data dapat memiliki dampak yang merugikan baik bagi universitas maupun para pengguna sistem.

Rumusan Permasalahan:

Dalam konteks ini, penelitian ini akan mengeksplorasi implementasi *Security Information And Event Management* (SIEM) pada sistem akademik Universitas Kuningan. Rumusan permasalahan yang akan diteliti adalah:

1. Bagaimana implementasi SIEM dapat meningkatkan keamanan sistem informasi akademik Universitas Kuningan?
2. Bagaimana efektivitas SIEM dalam mendeteksi, mencegah, dan merespons ancaman keamanan pada sistem akademik Universitas Kuningan?
3. Apa saja manfaat dan tantangan yang dihadapi dalam mengimplementasikan SIEM pada sistem akademik Universitas Kuningan?
4. Bagaimana luaran implementasi SIEM pada sistem akademik Universitas Kuningan dalam meningkatkan tingkat keamanan dan perlindungan data?

Pendekatan pemecahan masalah.

Pendekatan pemecahan masalah pada penelitian "Implementasi *Security Information And Event Management (Siem)* Pada Sistem Akademik Universitas Kuningan" dapat dilakukan melalui langkah-langkah berikut:

1. Analisis Kebutuhan Sistem: Tahap awal melibatkan analisis mendalam terhadap kebutuhan keamanan sistem informasi akademik Universitas Kuningan. Ini mencakup identifikasi aset yang perlu dilindungi, evaluasi ancaman yang mungkin terjadi, dan pemahaman akan tantangan spesifik yang dihadapi oleh universitas dalam konteks keamanan informasi.
2. Perancangan Sistem: Setelah kebutuhan sistem teridentifikasi, langkah selanjutnya adalah merancang arsitektur SIEM yang sesuai dengan lingkungan dan kebutuhan universitas. Ini termasuk pemilihan perangkat lunak SIEM yang tepat, konfigurasi sistem, dan integrasi dengan infrastruktur IT yang sudah ada.
3. Implementasi Sistem: Tahap implementasi melibatkan penerapan solusi SIEM yang telah dirancang ke dalam lingkungan sistem akademik Universitas Kuningan. Ini mencakup instalasi perangkat lunak, konfigurasi sistem, pengaturan aturan deteksi, dan integrasi dengan sumber data yang relevan.
4. Pengujian Sistem: Setelah implementasi, sistem SIEM harus diuji untuk memastikan bahwa itu berfungsi sesuai yang diharapkan. Pengujian melibatkan skenario ancaman yang berbeda, simulasi serangan, dan evaluasi respons sistem terhadap insiden keamanan.
5. Evaluasi dan Pemeliharaan: Tahap evaluasi dilakukan untuk mengevaluasi efektivitas SIEM dalam meningkatkan keamanan sistem akademik Universitas Kuningan. Hasil evaluasi digunakan untuk mengidentifikasi area perbaikan dan memperbaiki konfigurasi sistem SIEM secara berkala. Pemeliharaan rutin juga diperlukan untuk memastikan bahwa sistem SIEM tetap efektif dan responsif terhadap ancaman yang berkembang.

***State of the art* dan kebaruan.**

State of the Art: LPPM © 2024

1. Penerapan SIEM di Lingkungan Pendidikan: Beberapa institusi pendidikan telah menerapkan solusi SIEM untuk meningkatkan keamanan sistem informasi mereka. Studi-studi terdahulu mungkin telah mengeksplorasi implementasi SIEM pada berbagai lingkungan, tetapi fokus pada sistem akademik di universitas tertentu mungkin masih terbatas.
2. Ancaman Keamanan Terkini: Penelitian sebelumnya mungkin telah mengidentifikasi ancaman keamanan yang umum di lingkungan pendidikan, termasuk serangan phishing, malware, dan serangan DDoS. Namun, lanskap

keamanan terus berubah, dan penelitian terbaru mungkin memperbarui pemahaman tentang ancaman-ancaman baru yang relevan untuk sistem akademik.

Kebaruan:

1. Implementasi SIEM pada Sistem Akademik Universitas Kuningan: Penelitian ini membawa kebaruan dengan fokus pada implementasi SIEM secara khusus pada sistem akademik Universitas Kuningan. Ini memberikan kontribusi unik terhadap pemahaman tentang efektivitas SIEM dalam konteks institusi pendidikan tertentu.
2. Evaluasi Efektivitas dan Manfaat SIEM: Penelitian ini kemungkinan akan memberikan wawasan baru tentang efektivitas SIEM dalam mendeteksi, mencegah, dan merespons ancaman keamanan pada sistem akademik. Selain itu, penelitian ini juga diharapkan mengidentifikasi manfaat konkret yang diperoleh dari implementasi SIEM, seperti peningkatan respons terhadap insiden keamanan dan perlindungan data.
3. Pemahaman tentang Tantangan Khusus: Dalam konteks Universitas Kuningan, penelitian ini dapat mengidentifikasi tantangan unik yang dihadapi dalam mengimplementasikan SIEM pada sistem akademik mereka. Hal ini dapat memberikan wawasan berharga untuk pengembangan solusi keamanan yang lebih efektif di masa depan.

Dengan mempertimbangkan faktor-faktor tersebut, penelitian ini diharapkan dapat memberikan kontribusi yang berharga bagi pemahaman tentang implementasi SIEM pada sistem akademik Universitas Kuningan dan mungkin menjadi model untuk penelitian serupa di institusi pendidikan lainnya.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian " Implementasi *Security Information And Event Management* (Siem) Pada Sistem Akademik Universitas Kuningan " adalah sebagai berikut:

Metode Pengembangan Sistem:

1. Analisis Kebutuhan Sistem:

a. Melakukan studi tentang kebutuhan keamanan sistem informasi akademik Universitas Kuningan.
b. Mengidentifikasi ancaman keamanan yang mungkin terjadi.
c. Menentukan fitur dan fungsi yang diperlukan dari solusi SIEM. LPPM © 2024

2. Perancangan Sistem:

a) Merancang arsitektur SIEM yang sesuai dengan lingkungan sistem akademik Universitas Kuningan.
b) Memilih perangkat lunak SIEM yang tepat sesuai dengan kebutuhan dan ketersediaan.
c) Merancang aturan deteksi dan respons terhadap ancaman keamanan.

3. Implementasi Sistem:

a) Mengimplementasikan solusi SIEM ke dalam lingkungan sistem akademik Universitas Kuningan.
b) Mengkonfigurasi sistem SIEM sesuai dengan desain yang telah dirancang.
c) Mengintegrasikan SIEM dengan infrastruktur IT yang sudah ada.

4. Pengujian Sistem:

a) Melakukan pengujian fungsionalitas dan kinerja SIEM.
b) Menguji kemampuan SIEM dalam mendeteksi, mencegah, dan merespons ancaman keamanan.
c) Melakukan simulasi serangan untuk menguji respons sistem.

5. Evaluasi Sistem:

a) Mengevaluasi efektivitas SIEM dalam meningkatkan keamanan sistem akademik Universitas Kuningan.
b) Menilai kinerja SIEM berdasarkan kriteria yang telah ditetapkan.
c) Mengidentifikasi kelebihan dan kekurangan dari implementasi SIEM.

Metode Penelitian Tambahan:

1. Studi Kasus:

a) Melakukan studi kasus tentang implementasi SIEM pada sistem akademik Universitas Kuningan.

b) Mengumpulkan data dari pengalaman langsung dalam menerapkan SIEM.

2. Survei dan Wawancara:
   a) Melakukan survei dan wawancara dengan pengguna sistem akademik Universitas Kuningan untuk mengevaluasi pengalaman mereka terhadap keamanan sistem.
   b) Mengumpulkan masukan dan umpan balik dari pengguna sistem.
   3. Analisis Kuantitatif dan Kualitatif:
   a) Melakukan analisis kuantitatif terhadap data pengujian dan evaluasi sistem.
   b) Melakukan analisis kualitatif terhadap hasil survei, wawancara, dan studi kasus.
   c) Dengan menggunakan metode pengembangan sistem yang komprehensif serta melengkapi dengan studi kasus, survei, wawancara, dan analisis data, diharapkan penelitian ini dapat memberikan pemahaman yang mendalam tentang implementasi SIEM pada sistem akademik Universitas Kuningan dan dampaknya terhadap tingkat keamanan sistem informasi.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi SIEM pada Sistem Akademik Universitas Kuningan

a) Implementasi *Security Information And* Event Management (SIEM) dilakukan dengan mengintegrasikan berbagai sumber data log dari sistem akademik Universitas Kuningan. Sistem SIEM dikonfigurasi untuk mengumpulkan, menganalisis, dan mendeteksi aktivitas mencurigakan secara real-time. Beberapa komponen utama dalam implementasi ini meliputi:
b) Pengumpulan Log: SIEM mengumpulkan log dari server sistem akademik, firewall, database, serta perangkat jaringan lainnya.
c) Korelasikan Data Log: Sistem menganalisis pola akses dan mengidentifikasi anomali yang dapat menjadi indikasi ancaman.
d) Deteksi Ancaman: SIEM memanfaatkan aturan yang telah dikonfigurasi untuk mendeteksi potensi serangan seperti brute-force attack, SQL injection, dan akses tidak sah.
e) Notifikasi dan Tindakan Respons: Ketika ancaman terdeteksi, sistem secara otomatis mengirimkan notifikasi kepada tim IT untuk dilakukan mitigasi lebih lanjut.
f) Hasil implementasi menunjukkan bahwa SIEM mampu memberikan informasi keamanan yang lebih terstruktur, memungkinkan identifikasi ancaman secara cepat, serta meningkatkan efektivitas respons terhadap insiden keamanan.

3.2 Analisis Efektivitas SIEM

Berdasarkan hasil pengujian dan evaluasi, efektivitas SIEM dalam meningkatkan keamanan sistem akademik Universitas Kuningan dapat diukur melalui beberapa indikator berikut:

1. **Kecepatan Deteksi Ancaman**

a) Sebelum implementasi SIEM, rata-rata waktu deteksi ancaman mencapai **30 menit** hingga **beberapa jam** setelah insiden terjadi.
b) Setelah implementasi, SIEM mampu mendeteksi ancaman dalam waktu kurang dari **5 menit** setelah aktivitas mencurigakan terdeteksi.

2. **Akurasi Deteksi**

a) SIEM mampu mengidentifikasi 85% ancaman potensial yang sebelumnya tidak terdeteksi dengan metode manual.
b) Penggunaan korelasi log dan analisis pola aktivitas mencurigakan mengurangi false positives hingga 20%, sehingga tim IT dapat lebih fokus pada ancaman nyata.

3. **Efisiensi Manajemen Insiden**

a) Dengan adanya notifikasi otomatis, waktu respons terhadap insiden berkurang secara signifikan.
b) Tim IT lebih mudah mengidentifikasi sumber ancaman dan menerapkan tindakan mitigasi yang sesuai, seperti pemblokiran IP mencurigakan atau pembaruan kebijakan akses.

4. **Peningkatan Keamanan Data Akademik**

a) Implementasi SIEM berhasil mencegah 5 upaya akses ilegal terhadap data mahasiswa dalam periode uji coba.

b) Sistem juga berhasil mendeteksi serangan brute-force pada login akun dosen dan mahasiswa serta mencegah eksploitasi lebih lanjut.

3.3 Tantangan dan Kendala Implementasi

a) Meskipun implementasi SIEM membawa manfaat yang signifikan, terdapat beberapa tantangan yang perlu diperhatikan:
b) **Kompleksitas Konfigurasi**: SIEM memerlukan penyesuaian aturan deteksi agar sesuai dengan lingkungan sistem akademik. Proses ini membutuhkan waktu dan keahlian khusus dalam analisis keamanan siber.
c) **Kebutuhan Infrastruktur yang Lebih Besar**: SIEM memerlukan kapasitas penyimpanan dan daya komputasi yang tinggi untuk mengolah data log dalam jumlah besar.
d) **Keterampilan Tim IT**: Diperlukan peningkatan kompetensi sumber daya manusia agar dapat mengoperasikan dan menganalisis hasil yang diberikan oleh SIEM secara efektif.

3.4 Implikasi dan Manfaat Implementasi SIEM

a) Berdasarkan hasil implementasi dan analisis, beberapa manfaat utama yang diperoleh dari penerapan SIEM pada sistem akademik Universitas Kuningan adalah:
b) **Meningkatkan Kesadaran Keamanan**: Dengan adanya pemantauan real-time, seluruh pihak yang terlibat dalam sistem akademik lebih sadar akan pentingnya keamanan data.
c) **Mendukung Kepatuhan terhadap Regulasi**: Implementasi SIEM membantu Universitas Kuningan dalam memenuhi standar keamanan data dan regulasi yang berlaku, seperti ISO 27001.
d) **Menurunkan Risiko Pelanggaran Data**: Dengan deteksi ancaman yang lebih cepat dan akurat, potensi kebocoran data akademik dapat diminimalkan.
e) **Efisiensi Operasional**: SIEM memungkinkan tim IT untuk lebih fokus pada ancaman nyata dan mengurangi waktu yang dihabiskan untuk investigasi insiden secara manual.

4. KESIMPULAN

Penelitian ini bertujuan untuk mengimplementasikan *Security Information And Event Management* (SIEM) pada sistem akademik Universitas Kuningan guna meningkatkan deteksi dan respons terhadap ancaman keamanan siber. Dari hasil penelitian, dapat disimpulkan bahwa:

a) **Peningkatan Keamanan Sistem** Implementasi SIEM telah terbukti meningkatkan efektivitas pemantauan keamanan sistem akademik. SIEM mampu mengidentifikasi ancaman keamanan lebih cepat dibandingkan dengan metode konvensional, sehingga memungkinkan tindakan mitigasi yang lebih cepat dan tepat.
b) **Deteksi Ancaman yang Lebih Akurat** Dengan kemampuan analisis log dan korelasi data secara real-time, SIEM dapat mendeteksi pola serangan seperti percobaan akses ilegal, serangan brute-force, dan aktivitas mencurigakan lainnya yang sebelumnya sulit diidentifikasi secara manual.
c) **Efisiensi dalam Manajemen Insiden** Sistem SIEM memungkinkan notifikasi otomatis kepada tim IT ketika terjadi insiden keamanan, sehingga waktu respons terhadap insiden berkurang secara signifikan. Dengan demikian, risiko kebocoran data dan gangguan pada layanan akademik dapat diminimalkan.
d) **Tantangan dalam Implementasi** Beberapa kendala dalam penerapan SIEM meliputi kebutuhan infrastruktur yang lebih besar, kompleksitas konfigurasi sistem, serta perlunya peningkatan keterampilan tim IT dalam mengelola dan menganalisis data keamanan. Oleh karena itu, diperlukan pelatihan dan peningkatan kapasitas sumber daya manusia untuk mengoptimalkan penggunaan SIEM.
e) **Rekomendasi Pengembangan** Untuk meningkatkan efektivitas SIEM, direkomendasikan pengintegrasian dengan kecerdasan buatan (AI) guna mendukung analisis ancaman secara otomatis. Selain itu, pembaruan aturan keamanan dan pemantauan secara berkala harus dilakukan untuk menyesuaikan dengan perkembangan ancaman siber yang terus berubah.

Secara keseluruhan, implementasi SIEM pada sistem akademik Universitas Kuningan memberikan kontribusi positif terhadap keamanan informasi, meningkatkan ketahanan sistem terhadap serangan siber, serta memperkuat kepercayaan pengguna dalam mengakses layanan akademik secara aman dan andal.

5. SARAN

Berdasarkan hasil penelitian mengenai implementasi *Security Information And Event Management* (SIEM) pada sistem akademik Universitas Kuningan, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. **Optimasi Konfigurasi SIEM**

a) Perlu dilakukan penyesuaian aturan deteksi ancaman agar lebih spesifik terhadap pola serangan yang sering terjadi dalam sistem akademik.

b) Integrasi dengan sistem log lain seperti firewall, antivirus, dan aplikasi akademik untuk meningkatkan cakupan deteksi ancaman.

2. **Peningkatan Infrastruktur Teknologi**

a) Pengadaan perangkat keras dan kapasitas penyimpanan yang lebih besar untuk mendukung analisis log secara real-time tanpa mengurangi performa sistem akademik.

b) Implementasi solusi berbasis cloud untuk meningkatkan fleksibilitas dan skalabilitas sistem SIEM.

3. **Peningkatan Kompetensi SDM**

a) Memberikan pelatihan berkala bagi tim IT dalam pengelolaan, konfigurasi, dan analisis data dari SIEM.

b) Melakukan simulasi insiden keamanan secara rutin untuk meningkatkan kesiapan tim dalam menangani ancaman yang sebenarnya.

4. **Integrasi dengan Kecerdasan Buatan (AI) dan Machine Learning**

a) Menggunakan teknologi AI untuk meningkatkan akurasi deteksi anomali dan mengurangi false positives.

b) Menerapkan algoritma machine learning untuk mengenali pola serangan baru secara otomatis.

5. **Pembaruan dan Pemeliharaan Berkala**

a) Melakukan audit keamanan secara rutin untuk memastikan SIEM berfungsi optimal dan tetap relevan dengan perkembangan ancaman siber terbaru.

b) Menyesuaikan kebijakan keamanan sistem akademik dengan standar keamanan terbaru, seperti ISO 27001 atau NIST Cybersecurity Framework.

6. **Kolaborasi dengan Pihak Eksternal**

a) Menjalin kerja sama dengan institusi lain, komunitas keamanan siber, serta vendor SIEM untuk mendapatkan wawasan dan pembaruan terkait tren ancaman siber.

b) Mengikuti forum atau seminar keamanan siber guna meningkatkan pengetahuan dalam pengelolaan SIEM secara efektif.

Dengan menerapkan saran-saran ini, diharapkan implementasi SIEM di Universitas Kuningan dapat berjalan lebih optimal, meningkatkan keamanan sistem akademik, serta memberikan perlindungan yang lebih baik terhadap data akademik dan informasi sensitif lainnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Kuningan yang telah memberikan dukungan dan fasilitas dalam pelaksanaan penelitian ini. Terima kasih juga disampaikan kepada tim IT dan staf akademik yang telah memberikan data serta wawasan berharga terkait sistem akademik yang menjadi objek penelitian.

Ucapan terima kasih yang tulus juga diberikan kepada rekan-rekan peneliti dan pihak-pihak yang telah membantu dalam proses analisis, implementasi, dan evaluasi sistem *Security Information And Event Management* (SIEM).

Akhirnya, penulis juga mengapresiasi keluarga dan sahabat yang selalu memberikan dukungan moral selama penelitian ini berlangsung. Semoga hasil penelitian ini dapat memberikan manfaat bagi pengembangan keamanan sistem informasi akademik dan menjadi referensi bagi institusi pendidikan lainnya.

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 SosialDi Indonesia,” Journal.Uii.Ac.Id, vol. 1, no. 2, pp. 1–8, 2020

[3] 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

[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] Johnson, Sarah. (2019). "Security Challenges in Academic Environments: A Case Study of XYZ University". Journal of Cybersecurity Education, 5(1), 34-45.