Jurnal Teknologi Terpadu

https://journal.nurulfikri.ac.id/index.php/jtt
ISSN : 2477-0043 ISSN ONLINE : 2460-7908

STRATEGI IMPLEMENTASI SIEM UNTUK MENGURANGI RISIKO TERHADAP KEBOCORAN INFORMASI

Taufik Rendi Anggara[1]

[1] Teknik Informatika, Universitas Esa Unggul
Jakarta Selatan, DKI Jakarta, Indonesia 11510
taufik.anggara@esaunggul.ac.id

Abstract

More than 100 instances of information leakage brought on by unauthorized access occurred in 2022. This study used case studies in conjunction with system development. Early Warning Systems (EWS) are intended to give current information on event violations. When the worker goes to the console, EWS will warn and ask for verification. In Centralised Log Management (CLM), data logs were filtered with a policy-based Correlation setup approach. Network Security devices are configured for Rule-Based Correlations, and log data will be forwarded to CLM. In the case of an occurrence, logs are crucial to the inquiry. We used the CLM model to secure log data. EWS can filter harmful activity and malicious events from all current devices using this CLM. EWS will send any malicious activities or events it detects through telegram and email. Applying CLM and EWS with IT risk measurement can assist in reducing the risk of information leakage and offer quick information for breaches or incidents, according to this study. Evaluation, which lasted for two weeks, produced outcomes including less unauthorized activity, outstanding performance in the notification system that may assist in verifying access to the proper privileges for accessing the device, and simple detection of unauthorized access and file modifications, among other things.

Keywords: *Centralized Log Management, Early Warning Systems, IT Risk, Rule and Policy Based Correlations, SIEM*

Abstrak

Pada tahun 2022 terdapat lebih dari 100 kasus kebocoran informasi yang diakibatkan dari *illegal* akses. Penelitian ini, menggunakan metode System Development yang dikombinasikan dengan studi kasus. *Early Warning Systems* (EWS) dirancang untuk memberikan informasi secara *realtime* dari pelanggaran kejadian yang berlangsung. EWS juga membantu dalam verifikasi saat personil masuk ke dalam *Console* Perangkat. Teknik konfigurasi *Policy Based Correlation* dilakukan untuk mempermudah filter log yang masuk ke dalam *Centralized Log Management* (CLM). Konfigurasi *Rule Based Correlation* dilakukan pada perangkat *Network Security* dan log dari perangkat tersebut dikirimkan ke CLM. Log menjadi kunci dalam investigasi jika terjadi insiden. Teknik Pengamanan log yang dilakukan adalah dengan model CLM. Dari CLM inilah EWS dapat melakukan filter *malicious activity* dan *malicious event* dari seluruh perangkat. *Malicious Activity* dan Event yang ditangkap oleh EWS akan diteruskan informasinya melalui telegram dan email. Pengukuran Risiko IT dilakukan untuk mengukur seberapa jauh tingkat keamanan yang telah diterapkan dan dapat membantu mitigasi jika terjadi kebocoran data, informasi maupun pelanggaran dan insiden. Evaluasi dilakukan selama dua minggu dan mendapatkan hasil seperti berkurangnya aktivitas tanpa izin, kinerja maksimal pada sistem notifikasi yang dapat membantu verifikasi akses izin masuk ke dalam perangkat dan mudahnya pendeteksian jika terjadi ilegal akses, perubahan *file* dll.

Kata kunci: *Centralized Log Management*, *Early Warning Systems*, Risiko IT, *Rule and Policy Based Correlations*, SIEM

1. PENDAHULUAN

Kebocoran informasi dapat memiliki konsekuensi yang sangat merugikan bagi individu, organisasi, atau bahkan negara. Di bidang bisnis, kebocoran informasi dapat merusak reputasi perusahaan dan mengakibatkan kerugian finansial yang besar. Misalnya, ketika informasi rahasia perusahaan bocor ke pesaing, pesaing tersebut dapat menggunakan informasi tersebut untuk mengalahkan perusahaan tersebut di pasar. Di bidang politik, kebocoran informasi dapat mengganggu hubungan antar negara dan membahayakan keamanan nasional. Hal ini terlihat pada kasus-kasus seperti Wikileaks dan Edward Snowden.

Seperti halnya pada kasus tahun 2022, baik dari pemerintahan, lembaga – lembaga sampai dengan perusahaan besar yang tertimpa permasalahan kebocoran

Diterima 18 Mei 2023, Direvisi 4 Juli 2023, Diterima untuk publikasi 25 Juli 2023

data [2-3]. Penyebab dari kebocoran data ini beragam mulai dari gangguan sistem sampai dengan akses *illegal* terhadap sistem [4]. Pada tahun 2022 [4] terjadi 138 kasus yang dilaporkan ke pihak yang berwajib mengenai *illegal* akses ke sebuah sistem.

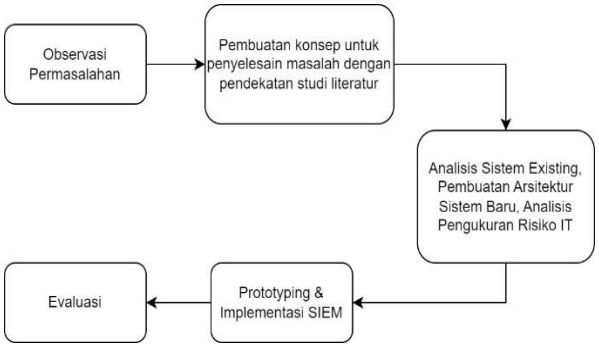
Untuk mencegah kebocoran informasi, perusahaan dan organisasi harus mengambil langkah-langkah keamanan yang tepat, seperti menggunakan enkripsi data, memperkuat akses ke data rahasia, dan memastikan bahwa karyawan terlatih dan memahami pentingnya menjaga kerahasiaan data. Pada tingkat individu, penggunaan teknologi yang aman, seperti penggunaan *password* yang kuat dan tidak membagikan informasi pribadi secara sembarangan, juga dapat membantu mencegah kebocoran informasi. Untuk dapat mencegah kebocoran informasi maka dapat dilakukan dengan tindakan preventif seperti mengikuti standar keamanan informasi [1].

SIEM *(Security Information and Event Management)* adalah solusi keamanan yang digunakan oleh organisasi untuk mendeteksi dan merespons ancaman keamanan pada sistem informasi [5]. SIEM mengumpulkan dan menganalisis data dari berbagai sumber, termasuk *log* keamanan, aktivitas pengguna, dan lalu lintas jaringan, untuk mendeteksi aktivitas mencurigakan atau serangan yang terjadi. SIEM juga memungkinkan organisasi untuk mempercepat respons terhadap ancaman dan mengurangi risiko kerentanan keamanan pada sistem informasi.

Risiko IT merupakan tantangan penting yang dihadapi oleh organisasi. Peningkatan penggunaan teknologi informasi memberikan peluang bisnis baru bagi organisasi, tetapi juga membawa risiko yang signifikan. Risiko IT dapat timbul dari berbagai faktor seperti kesalahan manusia, perubahan teknologi, kegagalan sistem, dan serangan siber. Oleh karena itu, penting bagi organisasi untuk memiliki strategi manajemen risiko IT yang efektif. Pendekatan yang paling mudah dalam mengukur *RISK IT* dengan menggunakan *COBIT 5 For RISK* [8]. *COBIT 5 For RISK* adalah kerangka kerja manajemen risiko IT yang dikembangkan oleh ISACA. *COBIT 5 For RISK* menawarkan pendekatan terstruktur untuk manajemen risiko IT yang berbasis pada prinsip-prinsip manajemen risiko ISO dan ISO/IEC 27005. Kerangka kerja ini membantu organisasi untuk mengidentifikasi, mengevaluasi, dan mengendalikan risiko IT.

2. METODE PENELITIAN

Secara garis besar penelitian ini menggunakan pendekatan *System Development* dan Studi Kasus [6-7]. Studi kasus yang dipadukan dengan *System Development* diharapkan akan mendapatkan hasil yang obyektif dan mendapatkan hasil yang tepat guna dalam strategi implementasi SIEM. Oleh karena itu metode ini dapat digambarkan pada Gambar 1 di bawah ini:



Gambar 1. Metode Penelitian

Pada Gambar 1 langkah awal penelitian ini adalah dengan observasi. Observasi permasalahan dilakukan untuk mengetahui permasalahan apa saja yang sedang terjadi. Dari observasi ini didapatkan beberapa permasalahan yaitu:

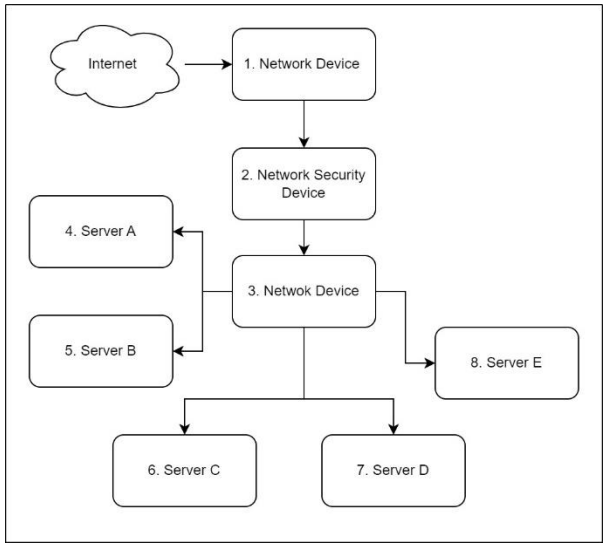
1. Belum terdapat metode yang efektif untuk mengetahui pengaksesan sistem & infrastruktur IT sesuai dengan prosedur yang ada.
2. Belum terdapat pengukuran risiko untuk *Event Management* dari sistem yang sudah ada.
3. Didapatkannya risiko IT yang masih tinggi dalam pengaksesan sistem & infrastruktur IT.
4. Belum terdapat *Early Warning Systems* (EWS) terhadap pengaksesan sistem dan infrastruktur IT yang tidak sesuai prosedur.
5. Belum terdapat pengamanan terhadap data *log system.*

3. ANALISIS, HASIL DAN EVALUASI

Penyelesaian permasalahan yang ada dimulai dari pendekatan studi literatur. Dari studi literatur [5, 9, 10, 11, 12] mengenai SIEM, didapatkan kesimpulan bahwa implementasi SIEM dilakukan dengan cara:

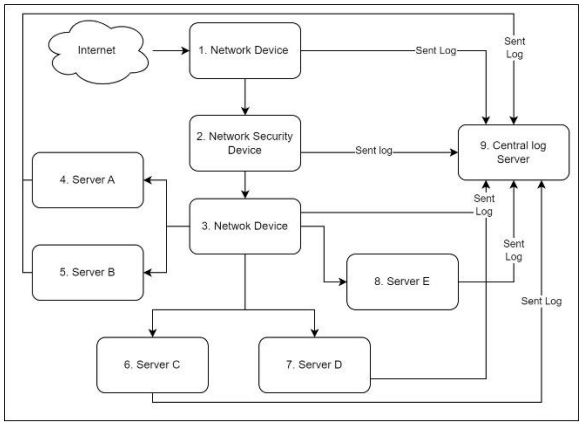
1. Mengetahui model arsitektur infrastruktur IT secara keseluruhan.
2. Melakukan pengumpulan *log* dari seluruh *device* / *hardware* yang digunakan *Centralized Log Management* (CLM).
3. Melakukan konfigurasi *Rule Engine Correlation* dan *Policy Based Correlation* untuk mendeteksi peristiwa maupun kejadian diluar kendali pihak yang berwenang.
4. Melakukan konfigurasi notifikasi peristiwa untuk *early warning systems* (EWS) / sistem notifikasi.
5. Menentukan lokasi perubahan *file* pada *Operating Systems* yang akan dilakukan pemantauan.

Dari observasi yang dilakukan, arsitektur yang digunakan perusahaan rekenan ini dapat digambarkan pada Gambar 2 sebagai berikut:



Gambar 2. Arsitektur Hasil Observasi

Dari Gambar 2 mengenai arsitektur hasil observasi, diketahui bahwa informasi yang didapat dari sistem dimulai dari *Network Device* No. 1 sampai dengan *Server* No. 8 dan belum terdapat CLM, EWS, serta *Monitoring System* untuk mengumpulkan semua peristiwa yang terjadi di Infrastruktur dan Sistem dan memberikan notifikasi peristiwa secara *Realtime*. Oleh karena itu diperlukannya perbaikan maupun perubahan di arsitektur infrastruktur dan sistem seperti pada Gambar 3.



Gambar 3. Perbaikan / Penambahan *Central log Server* Pada *Architecture Existing*

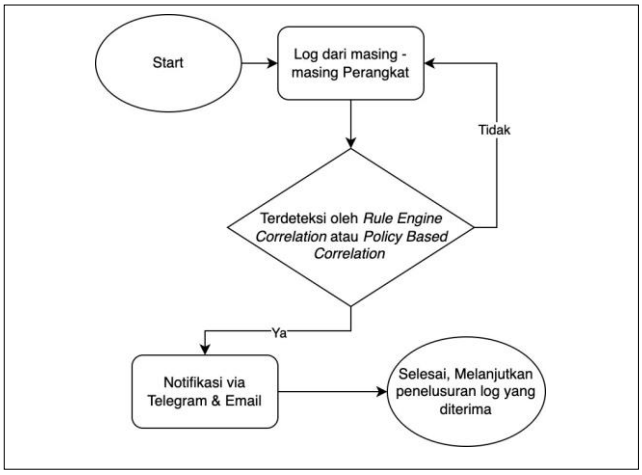
Perbaikan arsitektur yang dilakukan pada Gambar 3 adalah dengan menambahkan perangkat *server* dan jalur komunikasi ke perangkat tersebut. Jalur komunikasi ini dibangun dengan tujuan untuk mengirimkan maupun mengamankan *log* dari berbagai macam perangkat ke CLM No. 9. Selain untuk mengamankan CLM, teknik ini juga akan memudahkan dalam melakukan *filter* semua *log* yang ada. *Filter* ini ditujukan untuk memberitahu staf Keamanan IT bahwa telah terjadi pelanggaran akses pada infrastruktur IT (EWS).

Setelah dilakukannya penambahan perangkat untuk CLM, maka perlu ditambahkannya konfigurasi untuk *Policy Based Correlation* (seperti Gambar 4) pada masing-masing *server*. Hal ini bertujuan untuk melindungi *filepath* terpenting yang berada didalam *server*, tujuan lainnya adalah sistem dapat melakukan *filter* dengan cepat dan memberi notifikasi kepada staf Keamanan IT. Untuk *Rule Based Correlation* dapat dilakukan konfigurasi langsung di perangkat *Network Security* dengan mengaktifkan *rule IPS, IDS, Endpoint Security* dan melakukan pembaharuan piranti lunak secara berkala pada setiap perangkat.

```
/etc/passwd => change passwd
/etc/group => change group
/etc/shadow => add shadow root user
/etc/sudoers => add sudo user
/etc/ssh/sshd_config => change sshd_conf
/var/www/html => default folder path untuk web application
....
```

Gambar 4. *Policy Based Correlation*

Gambar 5. menggambarkan sistem notifikasi yang dibuat. Pada *flow* tersebut dapat diketahui bahwa sistem ini dirancang untuk melakukan penelusuran *log* yang diterima dari berbagai macam perangkat secara terus - menerus (*continue*). Oleh karena itu *EWS* ini dapat membantu staf Keamanan IT dalam melakukan pemantauan setiap aktivitas dan kejadian. *Flow notification system* ini dibuat dengan pendekatan teori [13,14,15,16].



Gambar 5. *Flow* Untuk Notifikasi pelanggaran pada Infrastruktur IT

Untuk menambah keamanan pada infrastruktur sistem, maka diperlukannya pengukuran dan mitigasi risiko. Pengukuran dan mitigasi dilakukan dengan cara pendekatan teoritis [8,17,18,19,20]. Dari studi literatur ini didapatkan kesimpulan yaitu untuk mengukur nilai risiko yang ada maka diperlukan tabel acuan pengukuran risiko. Pada penelitian ini, acuan pengukuran nilai risiko dapat dilihat pada Tabel 1. Pengendalian Risiko, Tabel 2 Risiko Tingkat Kerusakan (*Risk Severity*), Tabel 3 Kemungkinan Risiko Terjadi (*Risk Frequency*). Tabel ini akan menjadi acuan dalam melakukan pengelolaan risiko yang ada di infrastruktur sistem.

Tabel 1. Tabel Pengendalian Risiko

Kategori Risiko	Metode Pengendalian	Nilai Korelasi *Severity & Frequency*
Tinggi	*Risk Mitigation*	Nilai > 11
Sedang	*Risk Mitigation / Transfer*	Nilai diantara 6 – 10
Rendah	*Risk Acceptance / Avoidance*	Nilai < 6

Pada tabel pengendalian risiko dilakukan pembagian dalam kategori risiko, dimulai dari risiko yang tinggi sampai dengan risiko yang rendah. Pengelompokan kategori ini dilakukan untuk mempermudah dalam melakukan pengendalian terhadap risiko yang akan terjadi.

Tabel 2. Tabel Risiko Tingkat Kerusakan (*Risk Severity)*

Nilai	Klasifikasi	Konsekuensi
1	Ringan	aktivitas Operasional Terganggu lebih dari 6 jam
2	Sedang	aktivitas Operasional Terganggu lebih dari 12 jam
3	Berat	aktivitas Operasional Terganggu lebih dari 1 Hari
4	Sangat Berat	aktivitas Operasional Terganggu lebih dari 2 Hari

Tingkat kerusakan pada risiko perlu dilakukan klasifikasi. Tujuan pengklasifikasian ini dilakukan untuk mengetahui konsekuensi apa saja yang dapat terjadi. Klasifikasi dibagi mulai dari yang ringan sampai dengan sangat berat dan dilakukan pengukuran terhadap konsekuensi dari masing-masing klasifikasinya.

Tabel 3. Tabel Kemungkinan Risiko Terjadi (*Risk Frequency)*

Nilai	Tingkat Kemungkinan	Deskripsi
1	Sangat Kecil Kemungkinan	Terjadi < 2x dalam 1 tahun
2	Kecil Kemungkinan	Terjadi 3 – 6x dalam 1 tahun
3	Mungkin	Terjadi 7 – 12x dalam 1 tahun
4	Sangat Mungkin	Terjadi lebih dari 12 dalam 1 tahun

Tingkat kemungkinan risiko terjadi dibuat mulai dari risiko terjadi sangat kecil kemungkinan sampai dengan sangat mungkin terjadi. Dari tingkat kemungkinan risiko ini, kemudian dilakukan pendeskripsian agar tingkat kemungkinan risiko ini mudah dikategorikan sesuai dengan kondisi yang *real* terjadi. Setelah pengendalian, tingkat kerusakan, dan kemungkinan risiko ini terjadi dibuat, maka dapat dilanjutkan untuk melakukan pengukuran skor profil risiko sesuai pada Tabel 4.

Tabel 4. Tabel Nilai Korelasi Antara *Severity & Frequency*

	SEVERITY			
	Correlation Score	1	2	3	4
Frequency	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Penetapan nilai risiko, dilakukan dengan cara mempertemukan nilai *Severity* dengan *Frequency*, seperti pada Tabel 4, mengenai nilai korelasi antara *severity* & *frequency*. Pertemuan nilai ini memudahkan peneliti dan staf Keamanan IT untuk mengukur tingkat risiko yang terjadi. Pemberian warna merah, kuning dan hijau berelasi dengan Tabel 1. Pengendalian Risiko, relasi ini akan mempermudah membaca risiko dan mitigasi apa saja yang sudah dilakukan pada Tabel 5, Tabel 6, Tabel 7, mengenai daftar risiko IT.

Tabel 5. Tabel Daftar Risiko IT (Identifikasi Risiko IT)

No	Aset / Aktivitas	Identifikasi Risiko		
		Ancaman	Kerawanan	Dampak
1	*Server Device*	Akses Tanpa Izin	Manipulasi dan mencuri isi *server*	Kehilangan data, perubahan data tanpa izin
2	*Network Device*	Akses Tanpa Izin	Manipulasi konfigurasi	Gangguan layanan, dapat terjadi pencurian data
3	*Network Security Device*	Akses Tanpa Izin	Manipulasi konfigurasi	Gangguan layanan dan dapat terjadi pencurian data
4.	Terjadi Serangan	Gangguan Layanan	Akses ke sistem melambat	Layanan Tidak bisa di akses
5	Log dihapus	Aktivitas perangkat tidak bisa di pantau	Jika Terjadi *fraud* Tidak bisa dilakukan identifikasi kejadian	Jika terjadi *fraud*, tidak terdapat catatan kejadian untuk pembuktian
6	Terkena *Malware / Virus*	Data Hilang & Gangguan Layanan	Melumpuh-kan seluruh perangkat karena penyebaran cepat	Data Tidak Dapat diakses

Pada tabel 5 mengenai daftar risiko IT menjelaskan identifikasi risiko yang akan terjadi. Identifikasi dilakukan dengan cara memetakan ancaman, kerawanan dan dampak yang terjadi dari risiko pada aset maupun aktivitas operasional.

Tabel 6. Tabel Lanjutan Daftar Risiko IT (Analisis Risiko IT)

No.	Aset / Aktivitas	Analisis Risiko		
		Nilai *Severity*	**Nilai *Frequency***	**Nilai korelasi**
1	*Server Device*	4	2	8
2	*Network Device*	4	2	8
3	*Network Security Device*	4	2	8
4	Terjadi Serangan	2	4	8
5	*Log* dihapus	4	2	8
6	Terkena *Malware / Virus*	4	2	8

Tabel 6 merupakan lanjutan dari tabel 5 mengenai daftar risiko. Pada tabel ini menjelaskan analisis risiko berbasis skor pada *severity*, *frequency* dan nilai korelasinya. Penetapan skor pada analisis risiko ini dilakukan berdasarkan data dan informasi dari kejadian sebelumnya. Jika skor yang didapatkan memiliki nilai lebih tinggi dari lima maka akan dilakukan mitigasi/pengendalian risiko yang sesuai pada Tabel 7.

Tabel 7. Tabel Lanjutan Daftar Risiko (Mitigasi dan Pengendalian)

No.	Aset / Aktivitas	Mitigasi Pengendalian Risiko	Pengendalian Risiko Setelah di Mitigasi
1	*Server Device*	Akses Menggunakan *Dual Control*, notifikasi penggunaan *root account*	*Risk Acceptance*
2	*Network Device*	Akses Menggunakan *Dual Control*, notifikasi penggunaan *root account*	*Risk Acceptance*
3	*Network Security Device*	Akses Menggunakan *Dual Control*, notifikasi penggunaan *root account*	*Risk Acceptance*
4	Terjadi Serangan	Notifikasi terjadi serangan, melakukan *block IP permanent*, membuat catatan kejadian, *update patch* secara berakala	*Risk Acceptance*
5	*Log* dihapus	Pengiriman *log* ke *CLM*, notifikasi perubahan *file* pada *device*, *log* yang berada di *CLM* dilakukan *signing*	*Risk Acceptance*
6	Terkena *Malware / Virus*	Notifikasi penyebaran *malware*, memisahkan konfigurasi per-*subnet* dan *vlan*, *update patch* secara berakala	*Risk Acceptance*

Tabel 5, Tabel 6, Tabel 7 menjelaskan bahwa penilaian risiko dilalukan per - aset maupun aktivitas yang dilakukan. Penilaian ini juga dilakukan secara objektif dengan menggunakan Teknik FGD (*Focus Group Disccussion*). Seluruh risiko ini juga telah dilakukan mitigasi, sehingga risiko yang telah dimitigasi dan disepakati pengendaliannya menjadi *Risk Acceptance.* Pada Tabel 5, peneliti dan Tim mengidentifikasi risiko dengan cara mendaftarkan aset dan aktivitas yang memiliki nilai risiko menengah dan tinggi ke dalam daftar risiko. Pada Tabel 6 nilai *severity* dan *frequency* yang diberikan adalah hasil catatan kejadian sebelumnya. Pada Tabel 7 Mitigasi pengendalian risiko yang dilakukan adalah dengan membuat daftar aktivitas apa saja yang harus dilakukan ketika risiko ini terjadi, sehingga tim yang menangani insiden tersebut akan dengan mudah menanganinya.

Evaluasi setelah dilakukan implementasi dilakukan secara berkala dengan model pemantauan harian dengan jangka waktu dua minggu. Hasil yang didapatkan dari pemantauan ini yaitu:

- Berkurangnya aktivitas tanpa izin dalam melakukan akses ke perangkat (*Hardware*).
- Belum pernah terjadi insiden dari risiko yang telah didaftarkan.
- Pemantauan terhadap kinerja dari CLM adalah sistem bekerja dengan maksimal
- Sistem notifikasi juga bekerja dengan maksimal dan sangat membantu dalam melakukan verifikasi akses izin masuk ke dalam perangkat dan sistem ini juga dapat melakukan pendeteksian jika terjadi *illegal* akses, perubahan *file*, serangan terhadap perangkat dan lainnya sesuai dengan konfigurasi yang telah dilakukan.

4. KESIMPULAN

Penelitian ini dilakukan dengan pendekatan metode *System Development* yang dikombinasikan dengan studi kasus. Langkah pertama pada penelitian ini adalah observasi. Observasi yang dilakukan untuk mengetahui permasalahan yang ada pada objek penelitian. Untuk menjawab

permasalahan tersebut, maka dilakukan dengan pendekatan studi literatur. Hasil dari studi literatur didapatkan, dalam implementasi SIEM dengan baik maka diperlukan lima tahapan yang dimulai dari mengetahui model arsitektur infrastruktur yang kemudian akan dilakukan perbaikan. Tahapan ini dilakukan sampai dengan penentuan lokasi perubahan *file* pada *Operating Systems* yang akan dilakukan pemantauan. Perbaikan arsitektur infrastruktur IT menjadi kunci utama dalam melakukan pengamanan sistem dan implementasi SIEM.

Penambahan konfigurasi *Policy & Rule Based Correlation* memudahkan EWS / Sistem notifikasi peristiwa dalam memberikan peringatan terjadinya *illegal* akses / insiden lainnya. Pengamanan catatan peristiwa (*log*) dilakukan dengan cara mengirimkan seluruh *log* dimasing – masing perangkat ke CLM dan dilakukan pemantauan terhadap *path* pada *log* tersebut. Selain itu pengukuran terhadap risiko dilakukan, pengukuran ini ditujukan untuk membantu memetakan konsekuensi apa saja yang akan terjadi jika insiden tersebut benar terjadi. Daftar risiko juga akan membantu dalam melakukan mitigasi dari insiden yang terjadi. Evaluasi dilakukan waktu dua minggu. Hasil evaluasi menujukan bahwa implementasi SIEM berjalan dengan baik, dan belum pernah terjadi insiden.

Implementasi SIEM dan mitigasi risiko yang telah dilakukan, diharapkan dapat menjadi contoh untuk berkontribusi di berbagai macam industri. Sehingga kasus kebocoran informasi akibat dari ilegal akses dapat berkurang secara signifikan dan pengelolaan terhadap akses ke perangkat fisik maupun perangkat *virtual (cloud)* dapat dengan mudah dilakukan pengendaliannya. Selain SIEM, implementasi EWS juga mempercepat tindakan jika terjadi pelanggaran maupun penanganan insiden. Jika terjadi insiden / pelanggaran, maka tim investigator akan dengan mudah melakukan investigasi dari catatan peristiwa yang telah diamankan melalui implementasi CLM.

DAFTAR PUSTAKA

[1] ISO/IEC, Information Security – Cyber Security and Privacy Protection – Information Security Management Systems – Requirement (27001), 2022

[2] Berita kebocoran informasi di Indonesia dari Kompas.com, https://tekno.kompas.com/read/2022/12/29/09020067/kasus-data-bocor-di-indonesia-sepanjang-2022-dari-pln-pertamina-hingga-aksi?page=all – diakses pada tanggal 3 April 2023

[3] Berita kebocoran informasi di Indonesia dari CNN Indonesia, https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah diakses pada tanggal 3 April 2023

[4] Rekapitulasi daftar kejahatan siber tahun 2022 dari katadata.com, https://databoks.katadata.co.id/datapublish/2020/09/08/daftar-kejahatan-siber-yang-paling-banyak-dilaporkan-ke-polisi diakses pada tanggal 3 April 2023

[5] Adabi Raihan Muhammad, et-al, Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning, Procedia Computer Science, Volume 217, Pages 1406-1415, 2023

[6] Van der Merwe A, et-al, Guidelines for Conducting Design Science Research in Information Systems, Communications in Computer and Information Science book series (CCIS), pp. 163-178, 2020.

[7] Kirsty Williamson, Graeme Johanson, Research Methods Information, Systems and Context (Second Edition), Chandos Publishing, 2018

[8] ISACA. COBIT 5 for RISK. United States of America: ISACA, 2013

[9] Miloslavskaya, Natalia. Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. Conference: First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures, Agustus 2018

[10] Lipilini, J and Baiardi F, A Simulation Based SIEM Framework to Attribute and Predict Attacks, Pisa University Press, Oct 2015

[11] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors Vol. 21, 2021

[12] A. Vazão, L. Santos, M. B. Piedade and C. Rabadão, "SIEM Open Source Solutions: A Comparative Study," Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019

[13] Ahmadian Ramaki, Ali & Ebrahimi Atani, Reza. A survey of IT early warning systems: architectures, challenges, and solutions. Security and Communication Networks. 2016

[14] Baneres, D.; Guerrero-Roldán, A.E.; Rodríguez-González, M.E.; Karadeniz, A. A Predictive Analytics Infrastructure to Support a Trustworthy Early Warning System. MDPI, Journal Applied. Scinces. 2021

[15] Abhinav Mehrotra, Mirco Musolesi, Intelligent Notification Systems: A Survey of the State of the Art and Research Challenges, ArXiv, Computer Science, 2017

[16] Joshi M, Hadi T, A Review of Network Traffic Analysis and Prediction Techniques, CoRR (2015).

[17] Sulaman, Sardar & Weyns, Kim & Höst, Martin. A Review of Research on Risk Analysis Methods for IT Systems. ACM International Conference Proceeding Series, 2013.

[18] Mohammad, Sikender Mohsienuddin, Risk Management in Information Technology, SSRN 2020.

[19] ISACA, RISK IT Framework, 2015

[20] Barret, Shaun. Effects of Information Technology Risk Management and Institution Size on Financial Performance, Dissertation Doctoral Thesis, Walden Universtiy, 2016