CEEL - ISSN 2596-2221
Universidade Federal de Uberlândia
06 a 10 de Novembro de 2023

ANÁLISE E DESENVOLVIMENTO DE MÉTRICAS DE EFICIÊNCIA PARA SISTEMAS DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA

Leandro dos Reis Pedrosa de Oliveira

UFU - Universidade Federal de Uberlândia

Murillo Guimarães Carneiro

FACOM - UFU - Universidade Federal de Uberlândia

Kil Jin Brandini Park

FEELT - UFU - Universidade Federal de Uberlândia

Rodrigo Sanches Miani

FACOM - UFU - Universidade Federal de Uberlândia

Resumo **- Este artigo propõe um método para caracterizar a eficiência dos Sistemas de Gerenciamento de Eventos e Informações de Segurança (SIEMs), por meio de um conjunto de métricas propostas. Tais métricas foram criadas com base na experiência adquirida durante a atuação direta em diversos ambientes corporativos geradores de milhares de eventos por segundo devido aos seus ambientes compostos de várias máquinas, ambientes em nuvem, Diretórios Ativos (ADs), Sistemas de Prevenção de Perda de Dados (DLPs), Proxies e sistemas antivírus. O estudo considera dados sobre o número de eventos por segundo (EPS) e as ofensas criadas pelo SIEM, de forma que as métricas desenvolvidas possam ser aplicadas independentemente do SIEM e do ambiente empresarial. Essa abordagem permitirá que empresas com ambientes complexos monitorem facilmente a eficiência de seus SIEMs em tempo real, agilizando o processo de identificação e resposta a ameaças. Além disso, o método proposto poderá ser adotado pelos fornecedores de SIEM para demonstrar a eficiência real de suas ferramentas em ambientes simulados.**

Palavras-Chave**- Avaliação de SIEMs, Gerenciamento de Eventos de Segurança da Informação, Identificação de Ameaças, SIEMs**

ANALYSIS AND DEVELOPMENT OF EFFICIENCY METRICS FOR SIEM

Abstract **- This article details the development of a method for characterizing Security Information and Event Management systems (SIEM) efficiency using a set of metrics. These metrics are based on direct experience in various corporate environments, dealing with thousands of events per second from multiple machines, cloud environments, Active Directories (ADs), Data Loss Prevention Systems (DLPs), Proxies, and antiviruses. The study considers data on the number of Events per Second (EPS) and the offenses created by the SIEM, allowing the developed metrics to be applied independently of the SIEM and corporate environment. This approach will enable companies with complex environments to monitor the efficiency of their SIEMs in real time easily, streamlining the process of threat identification and response. Moreover, the proposed method can be adopted by SIEM vendors to demonstrate the real efficiency of their tools in simulated environments.**

Keywords **- Evaluation of SIEMs, Information Security Event Management, Threat Identification, SIEMs.**

NOMENCLATURAS

ADs	Diretórios Ativos.
AQL	Linguagem de consulta a banco de dados Ariel.
DLPs	Sistemas de Prevenção de Perda de Dados.
EPS	Eventos por segundo.
IDS	Sistema de Detecção de Intrusão.
IOCs	Indicadores de compromissos.

SIEM Sistema de Gerenciamento de Eventos e Informações de Segurança.

SOC Centro de Operações de Segurança.

I. INTRODUÇÃO

A segurança da informação é fundamentada em três pilares essenciais: confidencialidade, integridade e disponibilidade. Garantir a manutenção desses pilares é uma tarefa desafiadora no atual cenário em que os dados se tornaram valiosos e os ataques cibernéticos são incessantes, ameaçando corporações com danos significativos. A perda de reputação, sequestro de informações e prejuízos milionários tornam a proteção das infraestruturas de rede uma prioridade para as empresas.

No âmbito dessa crescente preocupação, surge a questão de como as empresas conseguem monitorar em tempo real suas extensas infraestruturas de rede. Para enfrentar esse desafio, muitas organizações adotam uma abordagem proativa, contando com equipes de segurança bem estruturadas, como o SOC (Security Operations Center), responsáveis pelo monitoramento ininterrupto dos eventos de segurança da informação. Nesse contexto, são empregadas diversas ferramentas, e uma das mais importantes é o SIEM (Security Information and Event Management).

Os SIEMs são capazes de realizar o gerenciamento de eventos e identificar em tempo real possíveis ameaças por meio da análise e correlação de milhares de eventos por segundo. Sendo assim, eles se tornam aliados essenciais das equipes de segurança defensiva, agilizando a detecção de ataques e possibilitando a mitigação antes que os atacantes avancem em suas explorações.

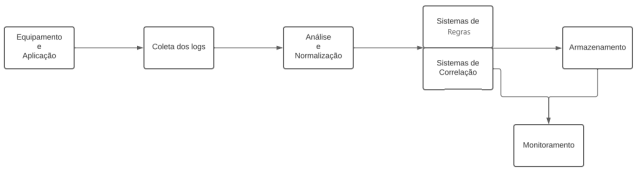
Os Sistemas SIEMs, que abrangem o campo em constante expansão da segurança cibernética, enfrentam o desafio frequente de incorporar novos componentes de armazenamento à infraestrutura computacional. Nesse contexto, administradores de sistemas devem determinar os recursos necessários para cada componente específico do SIEM [2].

No mercado atual, uma variedade de opções de SIEMs está disponível, incluindo nomes como IBM QRadar, Splunk Enterprise Security, AlienVault Unified Security Management, Sumo Logic e SolarWinds Security Event Manager, entre outros. O SIEM QRadar se destaca como líder do mercado, caracterizando-se por sua análise inteligente, notavelmente aprimorada na correlação de eventos.

O funcionamento desses sistemas é baseado na gestão de eventos de segurança, que coleta informações provenientes de diversas soluções de segurança, como firewalls, sistemas de detecção de intrusões IDS, IPs e antivírus [3]. O resultado é uma visão abrangente e direta da infraestrutura de TI da organização, beneficiando a equipe de segurança. A capacidade de relacionar eventos previamente registrados em outros sistemas de infraestrutura permite a detecção, prevenção de ataques e vulnerabilidades, além de simplificar a administração e relatórios de incidentes.

Portanto, o trabalho de um analista de sistemas é monitorar as redes em busca de possíveis ameaças e violações, sob um gerenciamento de imagens de vigilância. Isso permite detecção imediata de ameaças e resposta a incidentes de forma mais eficiente e inteligente. Dessa forma, o SIEM desempenha um papel crucial na detecção e resposta a possíveis ataques cibernéticos de maneira inteligente. A evolução tecnológica, especialmente no uso de inteligência artificial, transformou os SIEMs ao longo da última década, tornando-os mais ágeis e eficientes na resposta a incidentes [7]. Como resultado, os analistas de sistemas têm a responsabilidade de monitorar redes em busca de ameaças e violações, enquanto supervisionam a vigilância por meio de imagens. Essa abordagem proporciona detecção imediata de ameaças e respostas mais eficazes e inteligentes a incidentes.

Figura 1: Fluxograma adaptado sobre o funcionamento básico de um SIEM



Fonte: Autor (2022)

Desse modo, forma-se um "conjunto complexo de tecnologias projetadas para fornecer a visão e clareza sobre o sistema de TI da empresa como um todo, beneficiando os analistas de segurança e administradores de TI" [3]. Portanto, o SIEM atua como sistema para centralizar e correlacionar as informações de uma infraestrutura de TI, a partir das funções principais listadas por [6]:

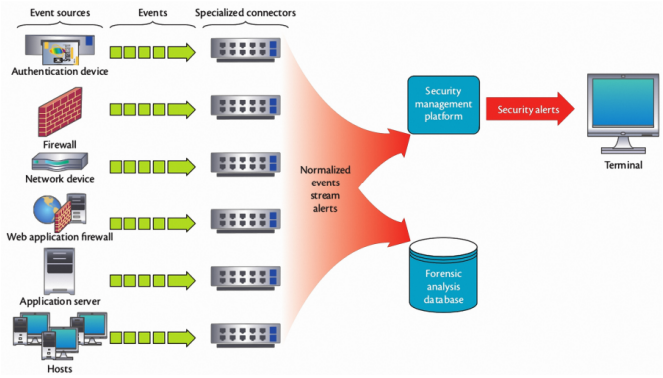
- Consolidação de logs: serviço que armazena de forma centralizada eventos de sistemas e equipamentos.
- Correlação de ameaças: utilização de inteligência artificial para analisar e combinar vários tipos de eventos e assim aumentar a capacidade de detecção de ataques e agressores.
- Gerenciamento de incidentes: o sistema deve indicar o que fazer quando detectar uma ameaça. Esta ação pode ser, por exemplo, uma notificação por email ou uma resposta automática com a execução de scripts de instrumentação.
- Relatórios: um SIEM pode emitir relatórios de eficiência/eficácia operacional, forenses ou até mesmo de conformidade com normas como PCI-DSS e ISO 27001.

Como visto, o SIEM está atrelado à capacidade de identificação de um ataque. Ao localizar tal possibilidade, é necessário, gerar o alerta e, em tempo real, gerar respostas automáticas previamente configuradas para cada caso, como apontado por [5].

Uma arquitetura geral para SIEMs é composta por diversos componentes, sendo os mais comuns, segundo [4]: geradores de eventos, bases de dados, componentes de normalização, componentes de gerenciamento e componentes de monitoramento. Desse modo, um SIEM deve receber logs de várias fontes, incluindo redes, dispositivos de segurança, sensores, firewalls, IDS, aplicativos, aplicativos da Web, servidores de autenticação e outros servidores, como explicado por [1]. Os

dados adquiridos são armazendos em um banco de dados, podendo ser utilizados quando houver necessidade de investigação digital, para rever acontecimentos e relatórios de atividade. Os SIEM dispõem normalmente de um interface com o utilizador, como exibido por [5], permitindo a monitorização em tempo-real. Ainda, é comum o uso de dashboards, para facilitar a vida do utilizador e ou administrador de rede, como o exemplo de arquitetura genérica de um SIEM na imagem abaixo:

Figura 2: Fluxo de coleta e processamento de eventos



Fonte: Bhatt (2014) [1]

Essa ferramenta depende do conhecimento da infraestrutura e integração com dispositivos de segurança, considerando os aspectos teóricos e práticos de sua programação. Assim, a arquitetura de um SIEM pode ser organizada, conforme [7], por detectores, coletores, SIEM, front-end para gerenciamento (para recolher os eventos gerados nos sistemas, para normalizá-los e correlacionados): Detectores: consiste nos sistemas que geram eventos;

- Coletores: permite agrupar as informações dos detectores, para aplicar a interpretação dos dados, classificá-los e, por fim, enviar ao SIEM. A coleta dos eventos de cada detector ocorre através dos métodos Push e Pull;
- Correlação de Eventos: após o recebimento de dados tratados pelos coletores, o SIEM classifica um grau de risco (na escala de 0 a 3 para cada evento), realizando a correlação e permitindo detectar ataques e novos padrões para reduzir o número de falsos positivos e negativos;
- Gerenciamento: ao adquirir as informações, elas são armazenadas no banco de dados.

Desse modo, torna-se possível consultar os eventos e alarmes gerados, permitindo a geração de relatórios, gerenciamento de vulnerabilidades e a configuração do sistema.

O SIEM precisa ser compatível com o maior número de fontes de informação. A partir de [5] fica evidente que a primeira tarefa de um SIEM é normalizar os dados. As diferentes representações de logs, obtidas de diferentes dispositivos e de diferentes fabricantes, requerem a conversão deles para um formato comum. Após a normalização, os dados são transferidos para outras partes do SIEM, como um processo de conversão de todos os logs de diferentes dispositivos em um formato comum. Assim, a plataforma de gestão de um SIEM, mantém e analisa os eventos, sendo responsável pelo mecanismo de correlação baseado em regras. Com base nas regras existentes no SIEM e nos eventos que foram registrados, alertas são enviados ao usuário.

No entanto, a efetividade do SIEM está diretamente ligada à sua correta implementação e adequação ao ambiente em que é utilizado. Além disso, é fundamental que o SIEM seja eficiente e eficaz na identificação de ameaças, proporcionando uma visibilidade abrangente da infraestrutura da organização. Isso é especialmente relevante para ambientes complexos, com um alto volume de eventos gerados a cada segundo.

Diante dessa necessidade de avaliar e caracterizar a eficiência dos SIEMs, independentemente de modelos e infraestruturas, este estudo tem como objetivo desenvolver um método baseado em um conjunto de métricas projetadas especificamente para essa finalidade. Por meio dessa abordagem, empresas com infraestruturas complexas no qual possuem sistemas, redes e tecnologias altamente elaborados e interconectados para sustentar suas operações. Isso pode incluir uma ampla gama de componentes, como servidores, data centers, sistemas de armazenamento, redes de comunicação, segurança cibernética e software especializado, logo, poderão facilmente monitorar a eficiência de seus SIEMs, permitindo uma rápida identificação de brechas na segurança e, assim, fortalecendo a postura de defesa contra as ameaças cibernéticas.

II. MATERIAIS E MÉTODOS

Nesta seção serão apresentados os métodos utilizados para aquisição dos dados de eventos de segurança da informação dentro dos SIEMs bem como a metodologia a ser ser aplicada para a avaliação dos dados supracitados dada a necessidade de demostrar a validade do experimento com relação a influência das métricas de eficiência para SIEM, considerando os resultados. Os métodos utilizados para validar a hipótese se aplicaram através das medidas de avaliação, conjunto de parâmetros, bases de dados e testes nas plataformas dos SIEMs da IBM. Deste modo, visando construir uma arquitetura de diferentes componentes e métricas que implementam o SIEM e suas interconexões, avaliou-se a eficiência do SIEM por meio dos seguintes indicadores:

- totEPS - Total de EPS contratados
- medEPS - Média de EPS diária utilizada
- totOfensas - Total de ofensas diárias
- totOfensasFP - Ofensas diárias categorizadas como falsos positivos

Para isso, utilizou-se por 30 dias as equações (1) a (9) descritas mais adiante nesta seção nos processos de teste: porcentagem de EPS utilizado; porcentagem de cases válidos, média diária; média mensal; e somatório de EPS. Da mesma forma, a normalização considerou como valor mínimo a menor média de EPS diária; o valor máximo sendo o total de EPS encontrados; permitindo chegar a média mensal (x). Logo obteve-se um valor entre 0 e 1, onde quanto mais próximo de 1 maior o consumo de EPS de maneira eficiente.

A pesquisa proposta, ou seja, o processo de criação e avaliação da fórmulação proposta para medir eficiência do SIEM,

foi dividida em quatro passos. No primeiro passo, houve a preparação do ambiente de testes, composta da implantação do IBM QRadar SIEM em um servidor on-premise, do envio de logs para uma máquina com o sistema operacional Ubuntu e outra com o sistema operacional Windows, onde ocorreram testes básicos com o intuito de construir o arcabouço de caracterização do SIEM, e por fim a realização dos testes em um ambiente corporativo, contendo milhares de máquinas heterogêneas com diversos sistemas operacionais e configurações de hardware, ambientes Cloud distintos, DLPs, Proxies e antivírus. No segundo passo, promoveu-se a criação de uma dashboard para obter a média de EPS (eventos por segundo) que são processado em 24h. Assim, a AQL criada para obter a informação sobre os eventos foi a seguinte:

```
SELECT sum(EPS) FROM
( SELECT starttime/(1000*60) as minute,
DATEFORMAT(starttime,'YYYY MM dd HH:mm:ss')
as showTime,
(minute * (1000 * 60)) as 'tsTime',
"Events per Second Raw - Average 1 Min"
as EPS,
parent as a Parent from events where
logsourceid=65 and aParent IN
(select aParent
FROM
(select parent as aParent,"Events
per Second Raw - Average 1 Min"
as EPS from events where parent
<> NULL and logsourceid=65 group
by Parent order by EPS desc limit 5
last 24 HOURS))
group by parent order by minute ASC
last 24 HOURS)
GROUP BY minute
```

No terceiro passo ocorreu a observação dos ambientes, a fim de descobrir dados importante para medir a eficiência, diante disso, observou-se a possibilidade de incluir o número total de EPS contratados, o número total de ofensas criadas no SIEM e o número de falsos positivos, tudo isso dentro do intervalo de um mês, com o intuito de se obter uma amostragem de dados robusta e garantir solidez para a base a ser usada no cálculo sobre a eficiência do SIEM.

Por fim, no quarto passo promoveu-se a criação da fórmula para medir eficiência considerando o intervalo de 0 a 1, ou seja, de forma normalizada, tal como apresentado a seguir.

A Porcentagem de EPS (pEPS) se caracteriza pela média de EPS utilizada diariamente e é dada pela equação abaixo, obtida a partir da média de EPS diária utilizada (medEPS) e do total de EPS contratados (totEPS):

$$pEPS = \frac{medEPS \cdot 100}{totEPS} \ . \tag{1}$$

Para mOfensasVal, iremos obter o número de ofensas válidas tendo a porcentagem de ofensas válidas e o total de ofensas diárias, obtida a partir do total de ofensas e do total de ofensas categorizadas como falso positivo:

$$mOfensasVal = totOfensas - totOfensasFP \tag{2}$$

Diante dos cálculos realizados acima, podemos obter as seguintes somas a fim de simplificar as fórmulas finais:

$$m = medEPS + mOfensasVal \tag{3}$$

$$n = totEPS + totOfensas \tag{4}$$

Para média diária de eficiência (MD):

$$MD = \frac{m}{n} \cdot 100 \tag{5}$$

Para obter a média mensal de eficiência (MM) será realizada a média da média diária de eficiência no período de um mês:

$$MM = \frac{1}{nd_{ms}} \sum_{i \in ms} MD_i \ , \tag{6}$$

em que nd_{ms} refere-se ao número de dias do mês.

Por outro lado, a média diária de EPS por mês (medEPSMes) é dada por:

$$medEPSMes = \frac{1}{nd_{ms}} \sum_{i \in ms} medEPS_i \ , \tag{7}$$

Por fim, tem-se a fórmula para calcularmos a eficiência do SIEM.

$$resSIEM = \frac{MM}{medEPSMes}. \tag{8}$$

Após o cálculo do resultado obtido da fórmula final, onde tem-se a eficiência, realiza-se a normalização dos dados, com o intuito de facilitar a compreensão e análise da métrica:

$$avSIEM = \frac{resSIEM - min(medEPS)}{totEPS - min(medEPS)} \ , \tag{9}$$

em que min(medEPS) refere-se a menor média de EPS diário e totEPS ao total de EPS contratados.

Com os dados normalizados tem-se o resultado final, sendo que quanto mais próximo de 1, maior a eficiência na aplicação do SIEM e quanto mais próximo de 0, menor sua eficiência.

III. EXPERIMENTOS

De acordo com o que foi descrito na Seção II, realizou-se o experimento ao longo de 30 dias. Desse modo, o estudo foi realizado em ambiente de produção utilizando dados reais de um ambiente corporativo com EPS (totEPS) = 10000, recém contratados, e com hardware abaixo do mínimo recomendado pela IBM, considerando que o processo para realizar expansão de recursos do SIEM encontrava-se em curso. O ambiente de produção conta com milhares de máquinas heterogêneas com com sistemas operacionais Windows, Linux e Mac OS, além de ambientes Cloud, DLPs, proxies, antivírus e controles de e-mails.

Durante o período de um mês, obteve-se os resultados apresentados na Tabela 1.

Tabela 1: Resultados obtidos nos experimentos por dia.

Dia	medEPS	totOfensas	totOfensasFP	pEPS (%)	medEPS+mOfensasVal	totEPS+totOfensas	média diária (%)
1	9591	21	3	85.71	9953.0	10021	99.32
2	9238	22	5	77.27	9255.0	10022	92.34
3	9834	19	3	84.21	9850.0	10019	98.31
4	9965	22	5	77.27	9982.0	10022	99.60
5	9076	20	2	90.00	9094.0	10020	90.75
6	9510	19	2	89.47	9527.0	10019	95.08
7	8644	17	2	88.23	8659.0	10017	86.44
8	9114	16	4	75.0	9126.0	10016	91.113
9	8625	15	2	86.66	8638.0	10015	86.25
10	8020	21	2	90.47	8039.0	10021	80.22
11	9753	20	2	90.00	9771.0	10020	97.51
12	8456	15	4	73.33	8467.0	10015	84.54
13	8905	20	6	70.00	8919.0	10020	89.01
14	7837	21	2	90.47	7856.0	10021	78.39
15	8889	19	6	68.42	8902.0	10019	88.85
16	7766	17	5	70.58	7778.0	10017	77.64
17	9059	15	3	80.00	9071.0	10015	90.57
18	8958	21	6	71.42	8973.0	10021	89.54
19	9016	21	5	76.19	9032.0	10021	90.13
20	87.19	18	3	83.33	8734.0	10018	87.18
21	8956	19	2	89.47	8973.0	10019	89.55
22	8859	15	3	80.00	8871.0	10015	88.57
23	8997	15	5	66.66	9007.0	10015	89.93
24	8917	17	3	82.35	8931.0	10017	89.15
25	8621	18	6	66.66	8633.0	10018	86.17
26	8614	21	6	71.42	8629.0	10021	86.10
27	9343	17	4	76.47	9356.0	10017	93.40
28	9772	16	5	68.75	9783.0	10016	97.67
29	9573	22	2	90.90	9593.0	10022	95.71
30	9591	20	6	70.00	9605.0	10020	95.85

Fonte: Autor (2022)

A avaliação dos resultados foi aplicada a partir dos experimentos realizados durantes trinta dias, conforme exibido na Tabela 1. Desse modo, a partir de 10.000 de EPS total contratados pelo ambiente empresarial, foram realizados os testes finais, e também houve a implantação do IBM QRadar SIEM no servidor on-premise, com envio de logs de uma máquina com sistema operacional Ubuntu e outra com sistema operacional Windows para que fossem realizados testes de baixa complexidade no SIEM.

De começo, o QRadar agrupou e priorizou todos os eventos relacionados em uma única ofensa, fornecendo uma visão de um cenário de ataque potencialmente em evolução. A análise de investigação cruzada forneceu um rico contexto sobre alertas ao vincular automaticamente as investigações por meio de incidentes conectados, reduzindo a duplicação de esforços e estendendo a investigação além do provável incidente e alerta atuais.

Após levantar os EPS diários obteve-se uma média de EPS diária utilizada de 8606.324. Também houve uma mínima de 7447.21. A partir disso, considerou-se o total de ofensas diárias e as ofensas diárias categorizados como falso positivo, com testes em um ambiente de produção real. Assim, o uso de registro de ações do usuário foi estabelecido em produção e afetou significativamente a carga no processador do servidor já que o ambiente estava em processo de expansão de recursos considerando a recém realizada contratação de mais EPS para o SIEM. Tal fato explicitou uma fragilidade na eficiência dado que, dentro do intervalo de medição de 0 a 1, obteve-se o valor de 0.45.

Portanto, nota-se que as métricas SIEM foram essenciais para indicar uma possível fragilidade do sistema. A partir desta informação seria possível traçar novos métodos e alterações para ampliar a segurança e uso eficiente da plataforma. Concomitantemente, os testes indicaram a confiabilidade de utilizar as métricas propostas para testes de segurança, pois foi corretamente apontada a média de EPS baixa em relação a quantidade contratada. Ademais, conforme previamente indicado, foi levada em consideração a falta de recursos de hardware para proporcionar o aumento de recebimento de logs, a fim de tornar o SIEM mais eficiente.

Tabela 2: Média dos Resultados obtidos nos experimentos.

Média dos resultados obtidos			
Mínimo (EPS)	**Máximo (EPS)**	**Classificação de eficiência entre 0 e 1**	**x (Média mensal)**
7447.219526804431	A (Total de EPS contratados)	0.4540556798229514	8606.324 EPS

Fonte: Autor (2022)

IV. CONCLUSÃO

Ao longo da pesquisa, foi possível traçar o panorama teórico e conceitual de um SIEM sob diferentes ambientes de segurança, iniciando com análises do número de ofensas geradas e a quantidade de falsos positivos, além da quantidade de eventos ocorridos por tempo de resposta por tipo de incidentes.

Consequentemente, o trabalho considerou a tarefa de selecionar soluções a partir das métricas sobre eficiência de recursos para construir uma arquitetura de sistema computacional para serviços web. O escopo dos sistemas SIEM tem sido estudado como uma área importante no campo da segurança de computadores.

O impacto dos componentes SIEM na eficiência de recursos mostrou ser mensurável utilizando um ambiente de produção em expansão. Os resultados podem ser úteis para aprender os impactos na eficiência de recursos de vários componentes SIEM e outras soluções de arquitetura para sistemas de TI.

Entre suas vantagens, observou-se a facilidade de uso e a relativa amplitude de variação. Particularmente no que diz respeito à quantidade de EPS contratados e a diferença entre a quantidade de eventos recebidos, dado que em diversos dias tem-se os EPS registrados bem abaixo da quantia contratada. Por fim, também foi observado que é aconselhado integrar a interface de gerenciamento e otimizar os processos de métricas para facilitar seu uso de modo intuitivo [1]. Entre suas vantagens, observou-se a facilidade de uso e a relativa amplitude de variação. Particularmente no que diz respeito à quantidade de EPS contratados e diferença entre a quantidade de eventos recebidos, dado que em diversos dias tem-se os EPS registrados bem abaixo da quantia contratada, por fim, também foi observado que é aconselhado integrar a interface de gerenciamento e otimizar os processos de métricas para facilitar seu uso de modo intuitivo [1].

Como sugestão para futuros trabalhos, torna-se relevante elaborar pesquisas aplicando as métricas aqui consideradas em diferentes SIEMs. Também, será possível elaborar o desenvolvimento de estruturas e ferramentas de automação para estudos de eficiência de recursos da SIEM.

Os resultados podem ser benéficos para estudar os impactos de eficiência de recursos de vários componentes SIEM e outras soluções de arquitetura para sistemas de computação. Assim, também seria possível estudar um método de desenvolvimento de frameworks para a eficiência de recursos.

REFERÊNCIAS

[1] BHATT, S.; MANADHATA, P. K.; ZOMLOT, L. The operational role of security information and event management systems. *IEEE Security Privacy*, v. 12, n. 5, p. 35–41 https://doi.org/10.1109/MSP.2014.103, 2014.

[2] CONCEIÇÃO, J. P. S. d. Implementação de um sistema siem: estudo de caso. 2017.

[3] MILLER, D. R.*Security information and event management (SIEM) implementation.* [S.l.]: McGraw-Hill Higher Education, 2011.

[4] PAVLIK, J.; KOMAREK, A.; SOBESLAV, V. Security information and event management in the cloud computing infrastructure. In: IEEE. *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*.[S.l.], 2014. p. 209–21 https://doi.org/10.1109/CINTI.2014.7028677.

[5] SOUSA, L. M. M. d. *Sonorização de eventos gerados por um SIEM*. Tese (Doutorado) — Instituto Politécnico do Porto. Escola Superior de Tecnologia e Gestão, 2016.

[6] SWIFT, D. A practical application of sim/sem/siem automating threat identification.*Paper, SANS Infosec Reading Room, The SANS*, p. 8, 2006.

[7] VERDE, J. V. d. A. Utilização do siem para detecção de ciberataque. 2017.