Análise e desenvolvimento de métricas de eficiência para SIEM

Leandro dos Reis Pedrosa de Oliveira

Universidade Federal de Uberlândia
Faculdade de Computação
Bacharelado em Sistemas de Informação

Monte Carmelo - MG
2023

Leandro dos Reis Pedrosa de Oliveira

Análise e desenvolvimento de métricas de eficiência para SIEM

Trabalho de Conclusão de Curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito exigido parcial à obtenção do grau de Bacharel em Sistemas de Informação.

Área de concentração: Sistemas de Informação

Orientador: Murillo Guimarães Carneiro

Monte Carmelo - MG
2023

Dedicado a mim mesmo, por ter coragem e determinação para seguir meus estudos. Ao meu orientador TCC, por me orientar durante o processo e fornecer um apoio inestimável. E à minha família, pelo amor e apoio inabaláveis durante toda a minha jornada. Obrigado a todos por acreditarem em mim e me ajudarem a alcançar este marco.

Agradecimentos

Aos meus pais, Fernanda Ferreira Pedrosa dos Reis Oliveira e Vanderlei dos Reis Oliveira, que sempre estiveram ao meu lado fornecendo todo apoio possível.

E ao meu orientador de T.C.C. Dr. Murillo Carneiro, por acompanhar todo meu desenvolvimento profissional, pela confiança, apoio e amizade.

"Se A é o sucesso, então A é igual a X mais Y mais Z. O trabalho é X; Y é o lazer; e Z é manter a boca fechada."

(Albert Einstein)

Resumo

SIEMs são responsáveis pelo gerenciamento de eventos e são capazes de identificar em tempo real possíveis ameaças correlacionando e analisando milhares de eventos por segundo. Atualmente, o grande desafio está em manter um sistema de gerenciamento e correlação de eventos de segurança da informação (SIEM) que seja eficiente e eficaz trazendo muito mais visibilidade para a infraestrutura da organização e tendo um maior ganho de eficiência, principalmente envolvendo a identificação de ameaças. Assim, o objetivo deste estudo é desenvolver um método para caracterizar a eficiência dos SIEMs, independente do modelo e infraestrutura, por meio de um conjunto de métricas a serem projetadas com base na experiência obtida com a atuação direta com SIEMs em diversos ambientes distintos. Com base na experiência profissional e estudos realizados em um ambiente corporativo contendo milhares EPS (eventos por segundo) gerados devido ao grande número de máquinas utilizados, ambiente Cloud, ADs, DLPs, Proxies e antivírus. Será realizada a criação das métricas levando em consideração dados sobre EPS (eventos por segundo) e ofensas criadas pelo SIEM, que poderão vir a ser utilizados independente do SIEM e ambiente empresarial. Assim, empresas com ambientes complexos, com milhares de eventos gerados por segundo, podem realmente monitorar sua eficiência de forma fácil e rápida, além de que o método poderá ser adotado pelos fornecedores de SIEM para demonstrar a eficiência real de sua ferramenta em vários ambientes simulados, bem como aumentar o desempenho dos SOCs ao utilizar o método para melhorar continuamente seu SIEM, verificando sua eficiência na rotina testes.

Palavras-chave: SIEM, IBM QRadar, Segurança da Informação, Eficiência, SOC.

Abstract

SIEMs are responsible for managing events and are able to identify potential threats in real time by correlating and analyzing thousands of events per second. Currently, the great challenge is to maintain an information security event management and correlation system (SIEM) that is efficient and effective, bringing much more visibility to the organization's infrastructure and having a greater efficiency gain, mainly involving threat identification. Thus, the aim of this study is to develop a method to characterize the efficiency of SIEMs, independent of the model and infrastructure, through a set of metrics to be projected based on the experience obtained with the direct action with SIEMs in different environments. Based on professional experience and studies carried out in a corporate environment containing thousands of EPS (events per second) generated due to the large number of machines used, Cloud environment, ADs, DLPs, Proxies and antivirus. Metrics will be created taking into account data on EPS (events per second) and offenses created by the SIEM, which may be used regardless of the SIEM and business environment. Thus, companies with complex environments, with thousands of events generated by second, they can really monitor their efficiency easily and quickly, and the method could be adopted by suppliers of SIEM to demonstrate the real efficiency of your tool in various simulated environments, as well as increase the performance of SOCs by use the method to continuously improve your SIEM, verifying its efficiency in routine tests.

Keywords: SIEM, IBM QRadar, Efficiency, Information security, SOC.

Lista de ilustrações

Lista de tabelas

Lista de siglas

AQL Linguagem de consulta a banco de dados Ariel

EPS Eventos por segundo

IDS Sistema de Detecção de Intrusão

IOCs Indicadores de compromissos

SIEM Gerenciamento de eventos e informações de segurança

SOC Centro de Operações de Segurança

Sumário

Capítulo 1

Introdução

Confidencialidade, integridade e disponibilidade são pilares da segurança da informação. Manter a segurança e garantir que esses pilares estejam sendo cumpridos é um grande desafio, já que hoje dados valem ouro e os atacantes estão a todo momento em busca de apenas uma pequena brecha para realizar a invasão e trazer danos absurdos as corporações. Tais danos envolvem a imagem, perca ou sequestro de informações e até mesmo causar danos aos softwares e sistemas da empresa, trazendo prejuízos milionários.

Neste momento, considera-se a seguinte pergunta: Mas como as empresas conseguem monitorar infraestruturas de rede gigantescas em tempo real?

Geralmente, empresas bem estruturadas possuem equipes de segurança, como por exemplo o Centro de Operações de Segurança (SOC) (*Security Operations Center*) que cuidam do monitoramento de segurança atuando 24 horas por dia. Essas equipes utilizam diversas ferramentas para automatizar e agilizar a análise e detecção de ataques e incidentes, como por exemplo os SIEMs, podendo até mesmo identificar um possível ataque e mitigar antes que o atacante evolua ou obtenha sucesso na sua exploração.

Os SIEMs (*Security Information and Event Management*) são responsáveis pelo gerenciamento de eventos, são capazes de realizar a identificação em tempo real de possíveis ameaças a partir da correlação e análise de milhares de eventos por segundo. Logo, o Gerenciamento de eventos e informações de segurança (SIEM) é um grande aliado no dia a dia das equipes de segurança defensiva, já que seria impossível uma equipe acompanhar e identificar ataques analisando milhares de eventos por segundo.

O grande desafio atualmente é ter um SIEM implementado corretamente de acordo com o ambiente e ser eficiente e eficaz, trazendo muito mais visibilidade sobre a infraestrutura da organização e tendo um maior ganho na eficiência principalmente envolvendo a identificação de ameaças. Desta forma, o objetivo desse estudo é desenvolver um método para caracterizar a eficiência de SIEMs, independente de modelo e infraestrutura, através de um conjunto de métricas a serem projetadas. Logo, empresas que possuem ambientes complexos, com milhares de eventos gerados por segundo, poderão realmente monitorar a sua eficiência de uma maneira fácil e rápida.

1.1 Motivação

Grandes empresas precisam se manter seguras diante de milhares de ataques realizados diariamente e explorando diferentes tipos de falhas. Logo, devem buscar monitorar seus ativos 24h, com ótimas ferramentas de logs e gerar as ofensas sobre as diversas vulnerabilidades que podem ser exploradas no ambiente corporativo. Portanto, a ferramenta deve ter um ótimo nível de eficiência principalmente na detecção de ofensas para obter um resultado rápido e com o menor número de falsos positivos, mantendo as empresas mais seguras.

1.2 Problema

Um grande desafio da atualidade é saber o quão eficiente o SIEM está sendo para o ambiente empresarial, onde o mesmo recebe milhares de logs por segundo e tem o papel de encontrar possíveis ataques.

1.3 Objetivos

O objetivo desse estudo é o desenvolimento e análise de conjuntos de métricas para realizar a avaliação da eficiência de um SIEM em diferentes ambientes de segurança, iniciando com análises do número de ofensas geradas e a quantidade de falsos positivos, e considerendo também a quantidade de eventos ocorridos por tempo de resposta por tipo de incidentes.

1.4 Contribuições

Busca-se garantir a adoção do método pelos fornecedores de SIEM a fim de demonstrar a real eficiência da sua ferramenta em diversos tipos de ambientes simulados, além do aumento de desempenho dos SOCs ao utilizarem o método para obter uma melhoria contínua do seu SIEM verificando sua eficiência em testes de rotina.

1.5 Organização da Monografia

Este estudo será divido em 4 partes. Primeiramente, será apresentada a introdução, exibindo os motivos, justificativas e afins da pesquisa. Posteriormente, será exibido um embasamento teórico onde será apresentado um pouco sobre SIEM, como a descrição das atividades onde será citado o planejamento do ambiente em que será testado, as métricas que serão utilizadas para medir a eficiência do SIEM nos testes e, por fim, as considerações finais onde será feito um levantamento geral e as conclusões do estudo.

Capítulo 2

Fundamentação Teórica

Neste capítulo, será apresentado o referencial teórico da introdução SIEM, arquitetura e funcionamento, desenvolvimento das métricas de eficiência, testes das métricas em um ambiente controlado e por fim as considerações finais.

2.1 Introdução ao SIEM

Os sistemas SIEM, (ou gerenciamento de eventos e informações de segurança), são um campo em constante expansão na segurança cibernética. No entanto, muitas vezes é difícil incorporar um novo componente de armazenamento na infraestrutura de computação. Nessa situação, um administrador do sistema deve saber a quantidade de recursos necessários para um determinado componente do SIEM (CONCEIÇÃO, 2017).

Atualmente temos diversas opções de SIEM no mercado, como IBM QRadar, Splunk Enterprise Security, AlienVault Unified Security Management, Sumo Logic, SolarWinds Security Event Manager, dentre outros... Sendo o principal do mercado o SIEM QRadar, com inteligência na análise como principal diferencial, realizando correlação dos eventos muito bem otimizado.

Seu funcionamento ocorre a partir do gerenciamento de eventos de segurança que coleta informações de diversas soluções de segurança, incluindo firewalls, Sistema de Detecção de Intrusão (IDS), IPs, antivírus, entre outros. Miller (2011) fornece uma visão clara de toda a infraestrutura de TI da corporação de forma direta para a equipe de segurança. Desse modo, o software deve ser capaz de vincular eventos já registrados em outros sistemas da infraestrutura para realizar a detecção e prevenção de ataques e vulnerabilidades, bem como facilitar o gerenciamento e o reporte de incidentes.

Portanto, o SIEM é usado para detectar e responder a possíveis ataques cibernéticos de maneira inteligente. A tecnologia SIEM mudou na última década graças à inteligência artificial, permitindo que seja mais inteligente e rápido ao responder a incidentes, como apontado por Verde (2017). 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.

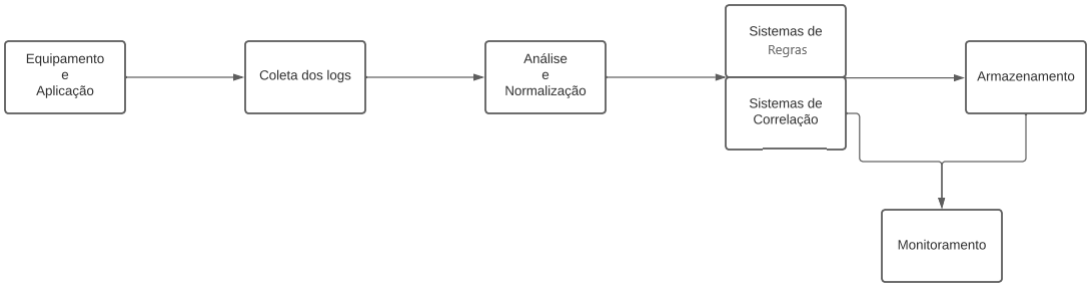


Figura 1 – Fluxograma adaptado sobre o funcionamento básico de um SIEM

Adaptado pelo 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" (MILLER, 2011). Portanto, o SIEM atua como sistema para centralizar e correlacionar as informações de uma infraestrutura de TI, a partir das funções principais listadas por Swift (2006):

a) Consolidação de logs: serviço que armazena de forma centralizada eventos de sistemas e equipamentos.

b) 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.

c) Gerenciamento de incidentes: o sistema deve 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.

d) Relatórios: um SIEM pode emitir relatórios de eficiência/eficácia operacional, forenses ou até mesmo de conformidade com normas como PCI-DSS e ISO 27001.

Conforme a citação presente na figura 1, proposta por Miller (2011) e a imagem acima, observa-se que é imprescindível deixar todos os dados organizados para garantir a determinação de etapas da política de segurança, tráfegos no firewall e o cumprimento das normas da empresa. Portanto, o sistema deste tipo, atua no monitoramento, identificação, documentação e registro de ameaças de segurança.

Conforme AZEVEDO (2016) a correlação de eventos é o cruzamento que um SIEM faz em todas as informações disponibilizadas nos sensores. Desse modo, torna-se possível a identificação de uma ameaça que poderá passar despercebida, caso seja analisada apenas uma fonte de dados. Logo abaixo, a figura 2 exibe uma estrutura básica em SIEM de camadas:

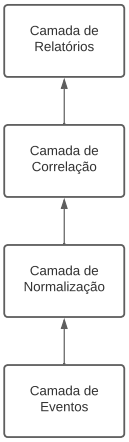


Figura 2 – Estrutura básica de um SIEM em camadas

Adaptado pelo Autor (2022)

Na camada de eventos, ocorre a coleta dos logs e mensagens utilizando outras ferramentas. Já na camada de normalização, a informação coletada é convertida para uma sintaxe comum AZEVEDO (2016). A camada de correlação classifica os eventos relacionados, visando localizar quaisquer ameaças. Por fim, nos relatórios, criam-se as saídas e ações que serão necessárias para cada dado levantado. Nota-se então, que o SIEM traz inúmeras vantagens para a otimização do trabalho, como citado por Verde (2017), Conceição (2017), reduz consideravelmente o número de falso-positivos, falso-negativos e atua na identificação de ataques desconhecidos.

Portanto, o SIEM é usado para detectar e responder de forma inteligente a possíveis ataques cibernéticos. Conforme observado por Verde (2017), a tecnologia SIEM foi sendo aprimorada principalmente com a introdução da inteligência artificial, permitindo o incremento da velocidade de resposta. Logo, é importante saber os mecanismos de monitoramento da tecnologia para a detecção instantânea de ameaças e resposta eficiente para incidentes.

2.2 Arquitetura e Funcionamento

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 Sousa (2016).

Uma arquitetura geral para SIEMs, é composta por diversos componentes, sendo os mais comuns, segundo Pavlik, Komarek e Sobeslav (2014): 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 Bhatt, Manadhata e Zomlot (2014). Os dados adquiridos são armazendo num 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 Sousa (2016), 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:

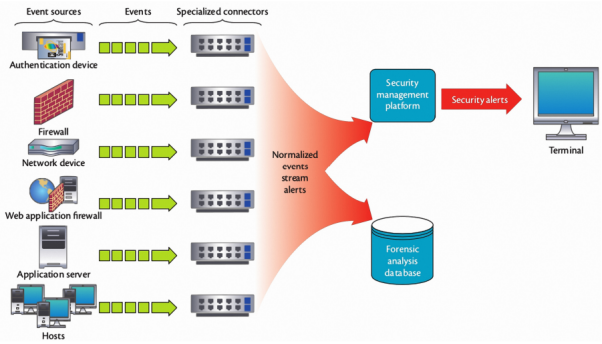


Figura 3 – Fluxo de coleta e processamento de eventos

Bhatt, Manadhata e Zomlot (2014)

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 Verde (2017) por detectores, coletores, SIEM, front-end para gerenciamento (para recolher os eventos gerados nos sistemas, para normalizá-los e correlacionados):

a) Detectores: consiste nos sistemas que geram eventos

b) 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.

c) 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.

d) 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 Souza (2017) 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 dos mesmos 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.

A lista de recursos fornecidos por um SIEM dependerá do fabricante e da arquitetura. No entanto, há um conjunto de recursos encontrados na maioria, particular, os recursos mais comuns são os apontados por Pavlik, Komarek e Sobeslav (2014): agregação de dados, correlação de eventos, geração de alertas, apresentação de informações, reconhecimento de padrões, resposta a incidentes de segurança da informação manutenção de registros e geração de relatórios.

Ainda, um SIEM deve ser capaz de agregar dados de diferentes fontes, redes de computadores, equipamentos de segurança de perímetro, servidores, bancos de dados e até aplicativos importantes, como mencionado por Sousa (2016). Esses dados devem ser apresentados de forma simples e coerente. Neles, poderá haver a correlação de eventos, um recurso fundamental dos SIEM, consistindo em formas de processamento de informações que conectam diferentes eventos (sejam físicos quanto de redes). Com isso, após realizar as técnicas de correlação, é possível integrar diferentes fontes, com o objetivo de transmutar os dados coletados em informações úteis.

A análise automática de eventos relevantes deve realizar alertas em caso de ataque. Estas notificações, tem como objetivo informar o administrador da rede ou responsável, que nela está acontecendo algo anormal, como a existência de possíveis vulnerabilidades no equipamento, a existência de intrusos ou a existência de outros problemas. Os alertas devem ser categorizados numericamente ou não de acordo com o risco prioridade e outras características que o evento apresenta à rede, como explicado por Sousa (2016) e Detken et al. (2015).

Concomitantemente, as informações coletadas e obtidas pelo agrupamento de informações devem ser expostas de forma concisa, preferencialmente em uma única tela. As informações devem ser expostas, de forma sintética, para permitir um melhor entendimento por parte de quem utiliza o SIEM. As informações devem ser agrupadas conforme o nível de risco, prioridade e data. Ainda, podem ser representadas textualmente e graficamente.

Ainda, Novikova e Kotenko (2013) acreditam que é crucial utilizar diferentes técnicas e diferentes tecnologias conjuntas para aumentar a percepção e a extensão das informações fornecidas por um SIEM. Um SIEM deve ser capaz de identificar um ataque e gerar

um alerta, após isso, ser capaz de responder automaticamente às respostas previamente configuradas para cada instância. Todos os dados gerados através do monitoramento da rede devem ser registrados para poder acessá-los a qualquer momento. Isso também facilita a correlação de dados ao longo do tempo. Finalmente, um SIEM deve produzir relatórios sobre as informações obtidas e correlacionadas, sobre os eventos detectados, sobre os alertas gerados e sobre as ações tomadas em resposta a incidentes de segurança. Isso facilita o entendimento de situações críticas ocorridas na rede e ensina como resolvê-las ou evitá-las.

2.3 Desenvolvimento de Métricas de Eficiência

A eficácia do SIEM na redução do tempo de resposta e da gravidade do incidente também é evidente por meio da medição do MTTR e da gravidade. Assim, o número de casos abertos para investigação devido ao SIEM e os possíveis incidentes resolvidos nos estágios iniciais também são métricas úteis, porque o número de alertas tratados por cada analista permite que a organização acompanhe o desempenho da equipe e não apenas o desempenho da ferramenta (DODGE; HOLZ; CHUVAKIN, 2014).

Como resultado, o software SIEM está entre os mais complexos de gerenciamento e operação, como explicado por entre as principais métricas para aumentar a eficácia do SIEM, são: diminuição na porcentagem de falsos positivos/negativos ao longo de um período de tempo; número de regras SIEM redundantes/desatualizadas; a proporção de alertas acionados para alertas corrigidos; o número de regras não documentadas; o tempo médio de resposta a incidentes de segurança; o número de incidentes abertos relacionados aos seus ativos críticos (dispositivos, sistemas, aplicativos e usuários).

As ferramentas SIEM podem classificar alertas e eventos com base em sua criticidade. Se um alerta de incidente for emitido e o dispositivo, usuário, terminal e aplicativo relevante estiver lidando com operações ou dados críticos de negócios, isso deve ser corrigido como uma questão de prioridade, como explicado por Dodge, Holz e Chuvakin (2014). Essa métrica informa sobre eventos críticos. De preferência, essa métrica deve ser zero, pois deixa sua organização vulnerável a grandes interrupções ou violações de dados como explicado por Magomedov, Ilin e Nikulchev (2021 https://doi.org/10.3390/app11114718)

Um SIEM deve ser capaz de combinar informações de várias fontes, redes de computadores, dispositivos de segurança, servidores, bancos de dados e até mesmo seus aplicativos críticos. Tais informações podem ser apresentadas de forma simples e consistente. A correlação de eventos é um recurso chave que deve estar presente em um SIEM. Consiste em uma forma de processamento de dados que combina diferentes transações de diferentes partes físicas e/ou elementos de rede. Com isso, após a realização de técnicas de correlação, é possível integrar diferentes fontes com o objetivo de converter os dados coletados em informações úteis, conforme explica Sousa (2016).

Com a crescente necessidade de inteligência de segurança em tempo real impulsionada por SOCs, há uma variedade de desafios operacionais e técnicos que precisam ser resolvidos por meio de uma implantação abrangente de SIEM. Assim, é necessário aumentar a visibilidade de suas operações diárias, permitindo que eles entendem totalmente o impacto e o contexto dos ataques.

2.4 Testes das Métricas

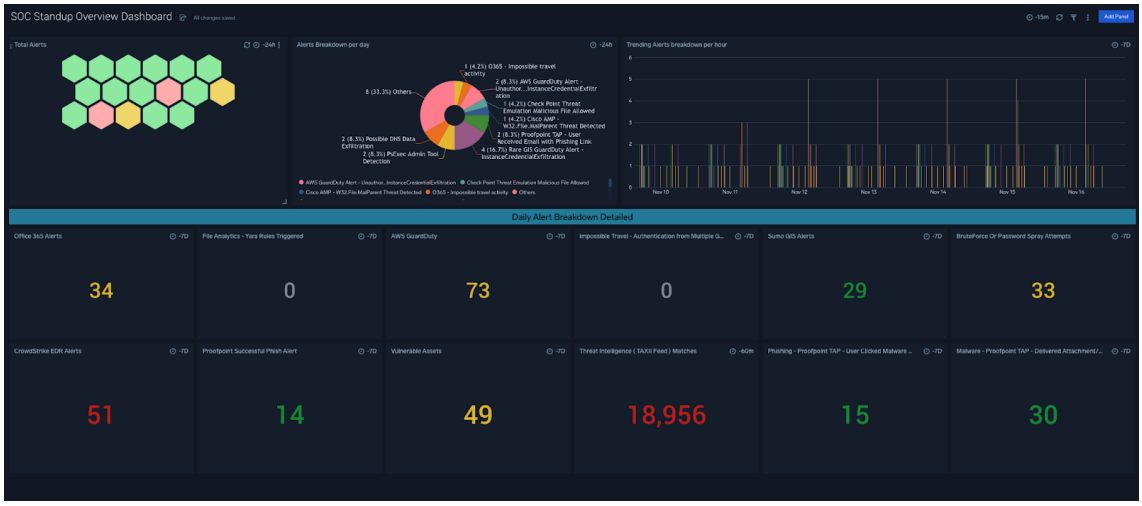
É recomendado modelar um sistema bem estruturado de métricas de segurança com definições e objetivos precisos, organizados em torno da Taxonomia de Capacidades SOC (Centro de operações de segurança), conforme explicado por Alvesa et al. (2017). Essas métricas destinam-se a monitorar a postura de risco e segurança de uma organização de acordo com os vários recursos SOC e vários sistemas SIEM usados pelo consórcio. Além disso, a relevância desses indicadores no contexto das atividades do consórcio será avaliada por meio de questionários.

O aplicativo SOC Daily Standup, disponível mediante solicitação para clientes do Sumo, é a solução da Sumo Logic para facilitar o trabalho de executar uma operação diária do SOC. Com uma única dashboard é possível verificar todas as correlações importantes e exibe tendências e falhas de alerta em uma determinada janela de tempo. Cada entrada fornece visibilidade em um caso de uso de detecção em nível organizacional. A exibição de favo de mel consolida as correlações, a exibição de alerta e a divisão de alerta correspondente por dia. A análise de tendências pode rastrear todos os alertas em janelas de hora em hora. As informações sobre cada alerta são codificadas por cores com base nas linhas de base de alerta. Antes de decidir criar um aplicativo autônomo SOC como este, é necessário levar alguns pontos em consideração, incluindo sua infraestrutura de segurança, a fonte e a natureza de sua lógica,

O Sumo Logic não apenas fornece uma visão de 40.000 pés de todas as correlações, mas também fornece uma análise por resumo de alerta, resumo de incidente e KPIs SOC. Todos eles são divididos em painéis separados para facilitar a leitura e o consumo. Todos os painéis são alimentados por correlações geradas pelo Cloud SIEM e também contabilizam o analista responsável, bem como as respostas para os KPIs de rastreamento.

Isso exibe o total de insights de alertas triados e priorizados para investigação, incluindo insights gerados pelo sistema (que são adaptados dos algoritmos de agrupamento de sinal por padrão), insights gerados pelo usuário (que são escalonados manualmente a partir de alertas por um analista) e detalhes do insight (que consiste em um resumo dos insights gerados no Cloud SIEM).

Também, o IBM Qradar pode ser empregado como uma plataforma de gerenciamento de segurança de rede para o reconhecimento situacional e suporte de conformidade. O processo ocorre pela rede em fluxo, correlação de eventos de segurança e avaliação de



Cua et al. (2010)

Figura 4 – Dashboard principal do SIEM

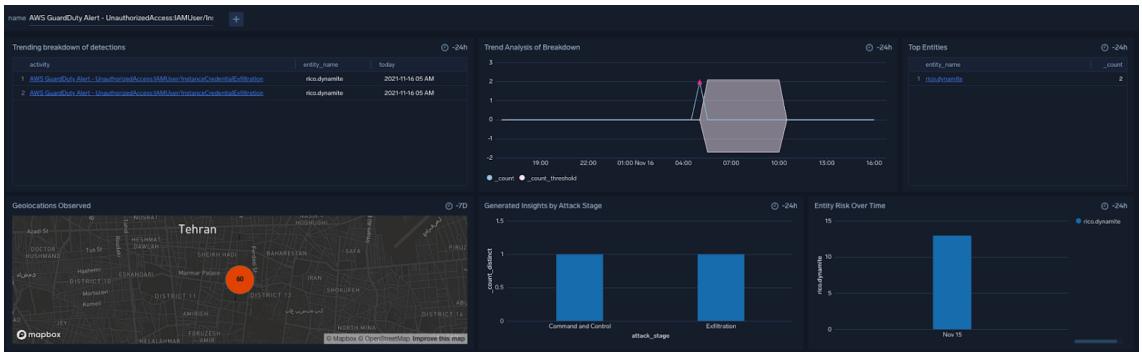


Figura 5 – Dashboard com informções de um alerta

Cua et al. (2010)

vulnerabilidade baseada em ativo. Destaca-se que a recomendação de seu uso é apenas para ambientes de testes, de modo que seja disponibilizado:

a) Atividade de log: permite monitorar e exibir eventos de rede em tempo real ou executar pesquisas avançadas.

b) Atividade de Rede: para investigar as sessões de comunicação entre dois hosts.

c) Ativos: permite criar automaticamente perfis de ativos usando dados de fluxo passivo e dados de vulnerabilidade para descobrir seus servidores e hosts de rede.

d) Ofensas: é possível investigar ofensas para determinar a causa raiz de um problema de rede.

e) Relatórios: criação de relatórios customizados ou usar relatórios padrão.

f) Coleta de Dados O: permite aceitar informações em vários formatos e de uma ampla variedade de dispositivos, como eventos de segurança, tráfego de rede e resultados de varredura.

g) Regras: executam testes em eventos, fluxos ou ofensas.Dependendo das condições de um teste, caso sejam atendidas, a regra gerará uma resposta.

h) Navegadores da Web Suportados: Para que os recursos funcionem corretamente, deve-se utilizar um navegador da web suportado.

i) Aplicativos: Para melhorar o fluxo de trabalho, alguns aplicativos que anteriormente estavam disponíveis apenas no IBM Security App Exchange são instalados por padrão.

Levando em consideração o objetivo do estudo, não foi encontrado trabalhos relacionados sobre efiência ou até mesmo eficácia focados especificamente para um SIEM. Portanto, a definição das métricas foram definidas baseadas totalmente na experiência profissional do Autor.

Capítulo 3

Materiais e Métodos

Neste capítulo, serão apresentados os métodos utilizados para a avaliação e os resultados dos experimentos. A partir da necessidade de demostrar a eficiência do experimento para a influência das métricas de eficiência para SIEM, considerando os resultados. Por fim, será apontado a avaliação do resultado adquirido.

3.1 Método para a Avaliação

Os métodos utilizados para validar a hipótese se deu através as medidas de avaliação, conjunto de parâmetros, bases de dados e testes nas plataformas SIEM da IBM. Deste modo, visando construir uma arquitetura de diferentes componentes e métricas que implementam o SIEM e suas interconexões, avaliou-se a oportunidade eficiência das métricas de seus recursos. Em outras palavras, é possível estimar:

- totEPS - Total de EPS contratados
- medEPS - Média de EPS diária utilizada
- totOfensas - Total de ofensas diárias
- totOfensasFP - Ofensas diárias categorizados como falso positivo

Para isso, utilizou-se por 30 dias as fórmulas da seção "3.2 Expressões matemáticas"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 mais o consumo de EPS bem utilizado de forma eficiente.

A pesquisa (Processo de criação da fórmula para medir eficiência do SIEM), foi dividida em quatro passos. No primeiro passo, houve a preparação do ambiente de testes, feita implantação do IBM QRadar SIEM em um servidor on-primess, feito envio de logs de

uma máquina ubuntu e outra Windows, onde tivemos testes básicos para conhecer melhor o SIEM, e por fim a realização dos testes em um ambiente corporativo, contendo milhares de máquinas, ambientes Cloud, 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 Linguagem de consulta a banco de dados Ariel (AQL) criada para obter a informação:

```
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, será elaborado 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 de 1 mês a fim de ter uma boa média dos dados e garantir que teremos um bom cálculo sobre a eficiência do SIEM. Por fim, no quarto passo promoveu-se a criação da fórmula para medir eficiência em um range de 0 a 1 ou seja normalizada.

3.2 Expressões matemáticas

A Porcentagem de EPS (pEPS) caracteriza pelo 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:

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

Diante dos cálculos realizados acima, podemos obter as seguintes somas afim de simplicar nas 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 obtermos a média mensal de eficiência (MM) será realizada a média da média diária de eficiência no período de um mês:

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

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

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

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

Por fim, temos a fórmula para calcularmos a eficiência do SIEM.

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

Após termos o resultado obtido da fórmula final onde temos a eficiência, realizamos a normalização do dado, para facilitarmos 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 temos o resultado final, onde quanto mais próximo de 1, mais eficiente está o SIEM e quanto mais próximo de 0, menor a eficiência do mesmo.

Capítulo 4

Experimentos e Análise dos Resultados

Neste capítulo, serão apresentados os métodos utilizados para a avaliação e os resultados dos experimentos. A partir da necessidade de demostrar a eficiência do experimento para a influência das métricas de eficiência para SIEM, considerando os resultados. Por fim, será apontado a avaliação do resultado adquirido.

4.1 Experimentos

De acordo com o que foi descrito na Seção 3.1, 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 já que estava em processo para realizar expansão de recursos do SIEM. O ambiente de produção conta com milhares de máquinas 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

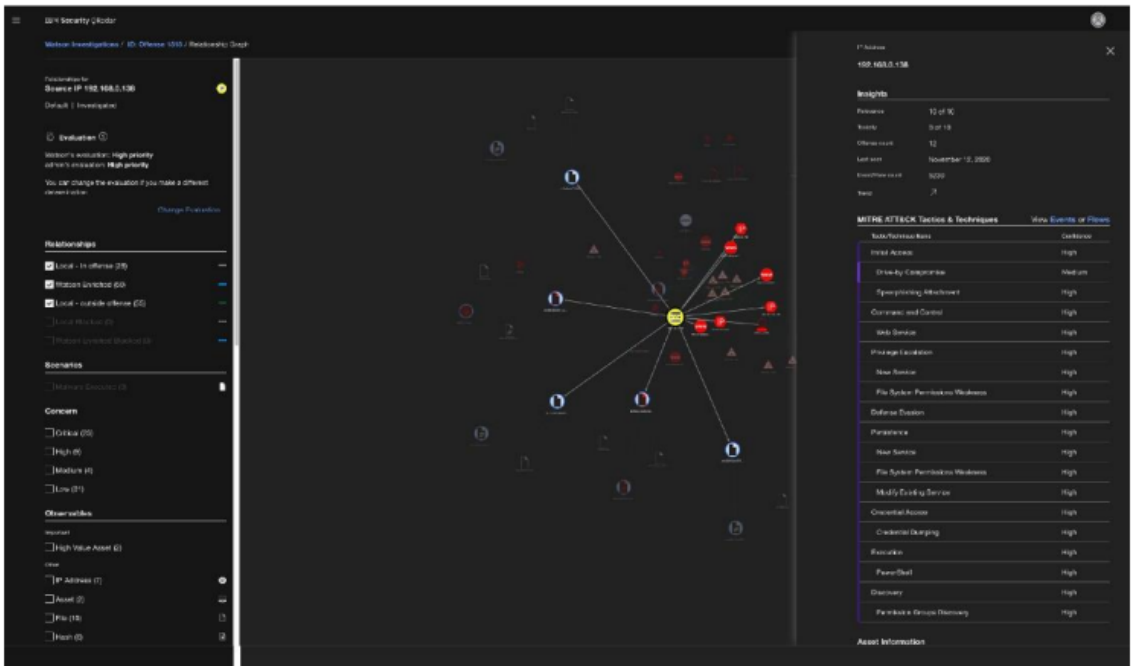
Fonte: Autor (2022)

4.2 Avaliação dos Resultados

A avaliação dos resultados foi aplicada a partir dos experimentos realizados durantes trinta dias, conforme exibido no tópico anterior. Desse modo, a partir de 10.000 de Eventos por segundo (EPS) total contratados pelo ambiente empresarial, foi realizados os testes finais, e também houve a implantação do IBM QRadar SIEM em no servidor on-primess, com envio de logs de uma máquina ubuntu e outra Windows para que fosse 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 fornece um rico contexto sobre alertas ao vincular automaticamente as investigações por meio de incidentes conectados, reduzindo a duplicação de esforços e estende a investigação além do provável incidente e alerta atuais.

Após, ao levantar os EPS diários, obteve-se uma média de EPS diária utilizada de 8606.324 EPS. Também, houve uma mínima de 7447.219526804431 EPS. A partir disso, considerou-se o total de ofensas diários e as ofensas diárias categorizados como falso positivo, onde foi testado 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 já que havia acabado de realizar a contratação de mais EPS para o SIEM, mostrando uma



IBM

Figura 6 – Relações estabelecidas no QRadar entre a IOCs, ativos, usuários, e outras investigações

fragilidade na eficiência que, numa medida de 0 a 1, apenas obteve-se 0.4540556798229514.

Portanto, nota-se que as métricas SIEM foram essenciais para indicar uma possível fragilidade do sistema onde, a partir de então, seria possível traçar novos métodos e alterações para ampliar a segurança. Concomitantemente, os testes indicaram a confiabilidade de utilizar as métricas para testes de segurança, onde podemos notar que temos e média de EPS baixa em relação a quantidade contratada e levando em consideração a falta de recursos de hardware para levar ao aumento de recebimento de logs, afim de deixar 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)

Capítulo 5

Conclusão

Neste capítulo será exposto as conclusões tomadas do objetivo desse estudo, isto é, a análise geral dos conjuntos de métricas levantadas durante os experimentos e resultados. 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 com 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 arquitetônicas 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 diferença entre a quantidade de eventos recebidos, no qual em diversos dias temos os EPS bem abaixo da quantia contratada, por fim, também foi observado que é melhor integrar a interface de gerenciamento e otimizar os processos de métricas para facilitar o uso intuitivo.

5.1 Principais Contribuições

As contribuições da pesquisa, mostraram as seguintes validações dos experimentos executados.

- ❏ Apresentar uma proposta para análise e avaliação de eficiência de SIEM;
- ❏ Modelagem da proposta para implementar uma solução plausível;

- ❑ A simulação da ferramenta utilizando a solução proposta gera um alerta de detecção de intrusão do sistema;
- ❑ Fortalecer a confiança na tomada de decisões em relação a incidentes de segurança.

5.2 Trabalhos Futuros

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

ALVESA, J. et al. Threat intelligence. **Analysis of using equivalent instructions at the hidden embedding of information into the executable files**, 2017. Citado na página 19.

AZEVEDO, D. C. N. d. **Estimação de banda disponível em redes sem fio padrão IEEE 802.11 N: uma análise experimental sobre os efeitos de seus novos mecanismos em técnicas ativas**. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2016. Citado 2 vezes nas páginas 14 e 15.

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. Citado na página 16.

CONCEIÇÃO, J. P. S. d. Implementação de um sistema siem: estudo de caso. 2017. Citado 2 vezes nas páginas 13 e 15.

CUA, J. et al. Representing story plans in sumo. In: **Proceedings of the NAACL HLT 2010 Second Workshop on Computational Approaches to Linguistic Creativity**. [S.l.: s.n.], 2010. p. 40–48. Citado na página 20.

DETKEN, K.-O. et al. Siem approach for a higher level of it security in enterprise networks. In: IEEE. **2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)**. [S.l.], 2015. v. 1, p. 322–327 https://doi.org/10.1109/IDAACS.2015.7340752. Citado na página 17.

DODGE, R. C.; HOLZ, T.; CHUVAKIN, A. Advanced attacker detection and understanding with emerging honeynet technologies. **Wiley Handbook of Science and Technology for Homeland Security**, 2014. Citado na página 18.

MAGOMEDOV, S.; ILIN, D.; NIKULCHEV, E. Resource analysis of the log files storage based on simulation models in a virtual environment. **Applied Sciences**, MDPI, v. 11, n. 11, p. 4718, 2021 https://doi.org/10.3390/app11114718. Citado na página 18.

MILLER, D. R. **Security information and event management (SIEM) implementation**. [S.l.]: McGraw-Hill Higher Education, 2011. Citado 2 vezes nas páginas 13 e 14.

NOVIKOVA, E.; KOTENKO, I. Analytical visualization techniques for security information and event management. In: IEEE. **2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing**. [S.l.], 2013. p. 519–525 https://doi.org/10.1109/PDP.2013.84. Citado na página 17.

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. 209–214 https://doi.org/10.1109/CINTI.2014.7028677. Citado 2 vezes nas páginas 15 e 17.

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. Citado 4 vezes nas páginas 15, 16, 17 e 18.

SWIFT, D. A practical application of sim/sem/siem automating threat identification. **Paper, SANS Infosec Reading Room, The SANS**, p. 8, 2006. Citado na página 14.

VERDE, J. V. d. A. Utilização do siem para detecção de ciberataque. 2017. Citado 3 vezes nas páginas 13, 15 e 16.