Implantação de um sistema de gerenciamento de eventos e informações de segurança em uma Universidade Pública

Jean Caminha[1], **Renan Heiji Susuki**[1]

[1]Instituto de Computação - Universidade Federal de Mato Grosso (UFMT)
Cuiabá – MT – Brasil

{jean.caminha,renan.susuki}@ufmt.br

Resumo. *O número de ataques cibernéticos tem aumentado significativamente no mundo, fazendo com que as organizações devam enfrentar uma ampla gama de riscos, desde ataques de phishing, negação de serviços, ransomwares e outras formas de malware. Incidentes de cibersegurança são muitas vezes resultado de vulnerabilidades em sistemas e falta de monitoramento. Neste cenário é crucial que as instituições invistam em tecnologias de segurança avançadas. Entretanto, as universidades públicas vem sofrendo cortes de investimentos que também impactam nas medidas de proteção. O presente artigo relata a implantação de um sistema de gerenciamento de eventos e informações de segurança (SIEM) baseado em software livre e uma unidade de cibersegurança em uma universidade pública federal. O SIEM detectou 782 eventos que resultaram em mudanças de configurações e políticas de uso, visando a proteção da infraestrutura e sistemas.*

Abstract. *The number of cyber attacks has increased significantly around the world, leaving organizations facing a wide range of risks from phishing and denial of service attacks, ransomware and other forms of malware. Cybersecurity incidents are often results of systems vulnerabilities and lack of monitoring. In this scenario it is crucial institutions to invest in modern security technologies. However, public universities have been suffering from investment cuts which also impact protection initiatives. This paper reports an implementation of a free software-based security information and event management system (SIEM) and a cybersecurity unit at a public university. The SIEM detected 782 events that resulted in configuration and usage policy changes aimed at protecting the infrastructure and systems.*

1. Introdução

O número de ataques cibernéticos tem aumentado significativamente no mundo, fazendo com que as organizações devam enfrentar uma ampla gama de riscos, desde ataques de phishing, negação de serviços, ransomwares e outras formas de malware. Incidentes de cibersegurança são muitas vezes resultado de vulnerabilidades em sistemas e falta de monitoramento[Mijwil et al. 2023].

Monitorar manualmente uma quantidade crescente de ameaças complexas não é trivial. Os Security Information and Event Management - SIEM, são sistemas de monitoramento automatizados são utilizados como alternativas para a coleta e triagem de alertas

para as equipes de cibersegurança. Os SIEM agregam os dados de evento que são produzidos por soluções de monitoramento, avaliação, detecção e resposta implantadas em aplicativos, rede, pontos finais e ambientes de nuvem. Podem ser capazes de realizarem detecção de ameaças, por meio de correlação e análise de comportamento de usuários e entidades. Estes sistemas podem funcionar baseado em nuvem ou suportar implantação local (on-premises) [Shoard et al. 2023].

O presente artigo relata a implantação de um sistema de gerenciamento de eventos e informações de segurança (SIEM) baseado em software livre e uma unidade de cibersegurança em uma universidade pública federal.

2. Contexto

A proteção das informações nos sistemas e infraestrutura demandam investimentos pelas organizações nos aspectos de pessoas, processos e tecnologias. Entretanto, as universidades públicas brasileiras vem sofrendo cortes em seus orçamentos. Os recursos destinados a investimentos, que incluem obras e compras de equipamentos sofreram uma redução de 87,8% no período de 2014 a 2022 [Sou Ciência 2024].

Ferramentas proprietárias de SIEM possuem um alto custo de uso. A solução líder de mercado Splunk, por exemplo, pode chegar a cerca de mil e oitocentos dólares por gigabyte de dados coletados[Tariq et al. 2023]. Isso pode ser um desafio para organizações que buscam soluções de segurança de TI eficientes, mas que também precisam manter um orçamento controlado[Manzoor et al. 2024].

Organizações públicas como as universidades precisam se proteger contra ameaças cibernéticas e garantir a segurança de seus dados, bem como atender às legislações específicas, como a Lei Geral de Proteção de Dados (LGPD) e as auditorias dos órgãos de controle[Lima et al. 2022]. Como essas instituições lidam com um grande volume de informações sensíveis, é fundamental que elas adotem medidas eficazes de segurança cibernética, mesmo em um cenário de restrição de recursos financeiros e humanos[Manzoor et al. 2024].

A implementação de um SIEM auxilia a identificar possíveis ameaças e vulnerabilidades, além de permitir que a equipe de segurança possa agir rapidamente para mitigar qualquer risco[Tariq et al. 2023]. Além disso, o SIEM também pode ajudar na gestão de incidentes e na análise forense de possíveis violações de dados, para atender às regulamentações e manter a confiança dos usuários e da sociedade em geral[Lima et al. 2022].

3. Ações realizadas

A implantação do SIEM fez parte do projeto de estabelecimento técnico da unidade de gestão de segurança cibernética da universidade. O projeto foi gerenciando utilizando as melhores práticas de propostas pelo Project Management Body of Knowledge (PMBoK)[Project Management Institute 2017], sendo realizado no período de maio a setembro de 2022.

O processo de avaliação e escolha da ferramenta foi composto pelos seguintes passos: 1) Definição do problema, escopo e critérios de seleção; 2) Pesquisa de mercado e análise preliminar das ferramentas; 3) Condução de prova de conceito; 4) Implantação em

ambiente de produção e 5) Análise e validação dos resultados. A lista inicial de ferramentas alvo de avaliação seguiu a classificação disponibilizada nos quadrantes de ferramentas líderes e visionárias da consultoria especializada Gartner[Davies and Schneider 2024].

Os critérios utilizados para a escolha basearam-se nos recursos necessários mínimos este tipo de ferramenta [Davies and Schneider 2024], acrescidos da exigência de possuir uma versão *software* livre e persistir os *logs* em formato aberto. Os requisitos avaliados foram: 1) Coleta de detalhes da infraestrutura e dados relevantes de segurança de uma ampla gama de ativos localizados em ambientes locais e/ou na infraestrutura em nuvem; 2) Capacidade para que os usuários finais desenvolvam, modifiquem e mantenham casos de uso de detecção de ameaças utilizando métodos baseados em correlação, análise e assinatura; 3) Fornecimento de conteúdo do fornecedor de SIEM e facilidades para conteúdo criado pelo cliente, em áreas como: análises, normalização de dados, coleta e enriquecimento; 4) Provisão de gerenciamento de casos e suporte a atividades de resposta a incidentes; e 5) Geração de relatórios para apoiar necessidades de negócios, conformidade e auditoria conforme necessário.

4. Resultados

A ferramenta escolhida para dar suporte ao SIEM foi a plataforma Elastic Stack[Elastic 2024]. Após uma análise de outras ferramentas, proprietárias e abertas, a solução escolhida atendeu os requisitos principais do projeto: conjunto de ferramentas integradas, compatibilidade com a infraestrutura, software livre e padrões abertos.

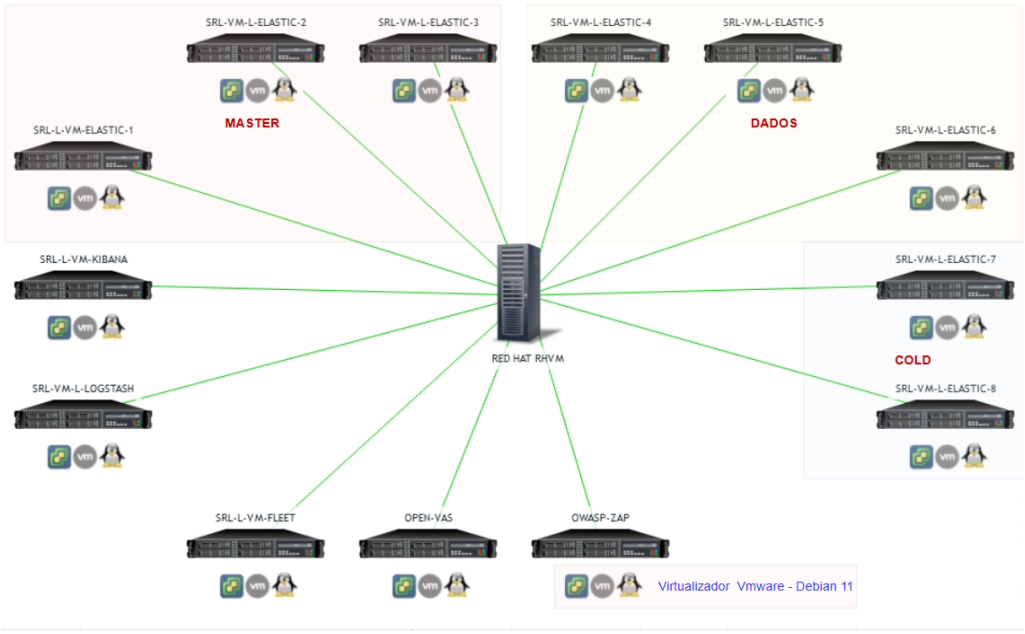
A plataforma Elastic Stack é um conjunto de softwares desenvolvidos pela empresa Elastic e é composta por quatro produtos: Elasticsearch, Logstash, Kibana e Beats. O Elasticsearch é um mecanismo de busca e análise distribuído que permite o armazenamento, recuperação e análise de grandes quantidades de dados de forma escalável e em tempo real. O Logstash é um agente de coleta de dados, que permite a ingestão e o processamento de diferentes tipos de dados em diversos formatos. O Kibana é uma interface de usuário que permite a visualização, a análise e a exploração de dados coletados pelo Elasticsearch. Por fim, o Beats é uma ferramenta que permite a coleta e o envio de dados para o Elasticsearch e o Logstash.

Outras três soluções também foram disponibilizadas para o projeto. O OpenVAS e o OwaspZAP[Arvindpdmn 2020], para a análise de vulnerabilidades de infraestrutura e aplicações respectivamente, além do Fleet[Elastic 2024], para automatizar a configuração dos coletores instalados nos *end-points*.

A infraestrutura do projeto SIEM (Figura 1) conta com 14 máquinas virtuais que executam as tarefas de coleta e análise de dados, além de persistir os dados de *logs* em duas temporalidades: 1) *Hot*, para acesso imediato e 2) *Cold* para registros históricos (30 dias).

A Figura 2 ilustra um exemplo de configuração de uma regra customizada para alertar sobre um possível ataque de força bruta no serviço SSH. A regra utiliza o software Logstash para coletar os dados de logs do serviço SSH e processá-los. Em seguida, a regra aplica filtros para identificar padrões suspeitos de acesso, como múltiplas tentativas de login malsucedidas a partir de um mesmo endereço IP em um curto intervalo de tempo. Quando a regra detecta esses padrões, ela dispara um alerta para uma equipe de segurança,

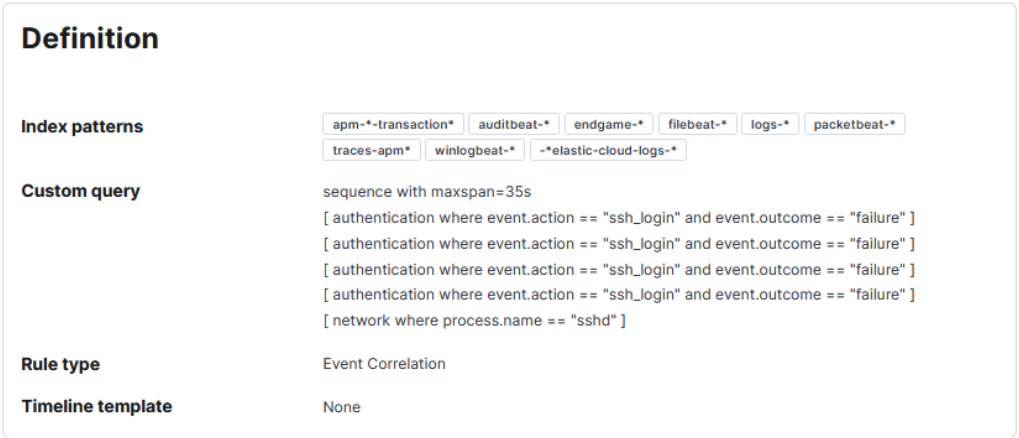
Figura 1. Infraestrutura do projeto SIEM.



Fonte: Elaborado pelos autores (2024).

indicando a possibilidade de um ataque em andamento. Essa configuração exemplifica a importância de se personalizar as regras do sistema de detecção de ameaças, de forma a adaptá-las às particularidades do ambiente de TI da organização e aumentar a eficácia na detecção de ameaças em tempo real.

Figura 2. Interface de configuração de regras.

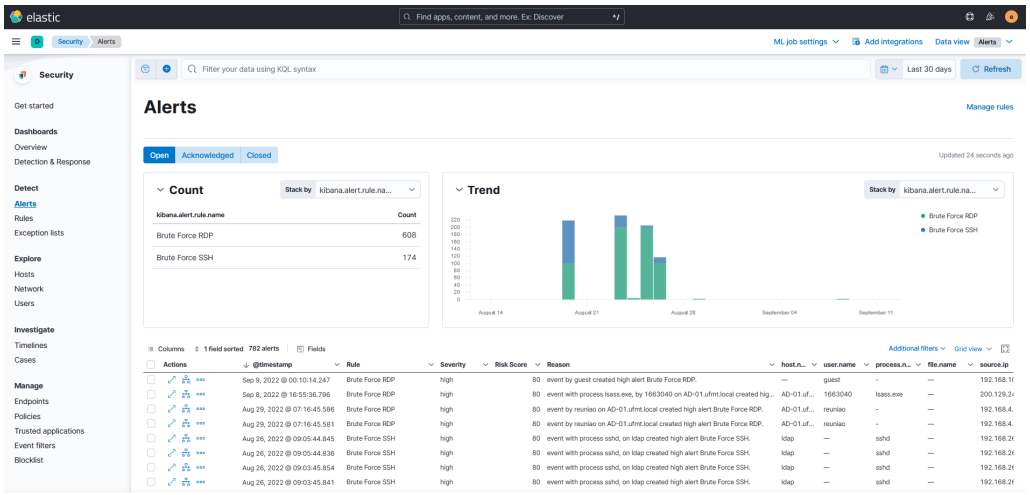


Fonte: Elaborado pelos autores (2024).

Um painel web específico (Figura 3) exibe o monitoramento de dados de *logs* de diversas fontes, como também identificar tendências de ataques ao longo do tempo, permitindo que os administradores visualizem e analisem informações e ajustem as estratégias de defesa.

Além do acompanhamento dos servidores de aplicação, foi implementado também o monitoramento dos acessos dos *end-points wi-fi*. Com essa funcionalidade, é possível

Figura 3. Painel de monitoramento de alertas.



Fonte: Elaborado pelos autores (2024).

detectar possíveis ameaças e identificar comportamentos suspeitos de usuários conectados à rede sem fio, como por exemplo a tentativa de se conectar uma grande quantidade de dispositivos na rede pelo mesmo dispositivo.

Em sete meses de funcionamento até março de 2024, o SIEM detectou 782 eventos que resultaram em mudanças de configurações e políticas de uso, visando a proteção da infraestrutura e sistemas. Um exemplo dessas mudanças foi a implantação da política de acesso apenas durante o dia para aos sistemas no decorrer dos recessos acadêmicos. A supervisão de segurança comprovou com dados do SIEM o aumento de tentativas de invasão durante as festas de finais de ano e o mês de janeiro.

5. Lições aprendidas

O desenvolvimento deste projeto proporcionou algumas lições para a equipe. Foi observado que em apenas um mês a quantidade de registros de eventos *logs* já havia ultrapassado a capacidade de armazenamento projetada para um ano. Considera-se importante realizar uma gestão eficiente dos *logs* e a necessidade de se estabelecer critérios claros para retenção.

A implementação de um SIEM pode ser bastante complexa, devido à quantidade de componentes que fazem parte do sistema, bem como aos desafios envolvidos na integração desses elementos entre si e com os sistemas e infraestrutura existentes na instituição. Além disso, a necessidade de personalização das regras para detecção de eventos, de acordo com as particularidades do ambiente de TI demanda esforço e especialização da equipe técnica.

O monitoramento de alertas é uma funcionalidade importante do SIEM, entretanto sua eficácia depende do monitoramento contínuo de um técnico capacitado. A detecção de eventos suspeitos exige uma análise mais aprofundada, para que se possa distinguir situações relevantes de alertas ou falsos positivos. No entanto, é possível configurar o sistema para que sejam disparadas ações automáticas em determinados cenários, o que pode ajudar a minimizar o tempo de resposta em situações críticas.

Por fim, foi identificada uma limitação relacionada à integridade dos dados em situações de falha no sistema. Quando ocorria a queda de um nó do *cluster*, houve corrupção dos arquivos de *log*, o que podia comprometer a confiabilidade do SIEM como um todo. Essa limitação demandou a importância de se contar com um sistema de backup adequado e com protocolos de contingência bem definidos.

6. Conclusão

O presente artigo relatou a implantação de um sistema de gerenciamento de eventos e informações de segurança (SIEM) baseado em software livre e uma unidade de cibersegurança em uma universidade pública federal.

A plataforma instalada monitora tentativas de acesso indevidas, tanto por agentes externos quanto pela infraestrutura de rede sem-fio local. O SEIM detectou em sete meses de operação 782 eventos que resultaram em mudanças de configurações e políticas de uso, visando a proteção da infraestrutura e sistemas.

Como trabalhos futuros, serão realizado estudos dos dados coletados pela plataforma SIEM o treinamento de modelos de Inteligência Artificial para a análise automatizada dos incidentes.

Referências

Arvindpdmn, N. (2020). Owasp zap. https://devopedia.org/owasp-zap.

Davies, A. and Schneider, M. (2024). Magic quadrant for security information and event management. *Gartner RAS Core Reasearch Note (May 2024)*.

Elastic (2024). Elastic observability and security - built on elasticsearch. https://www.elastic.com/.

Lima, P. R. S., Ferreira, L. M. M., and de Albuquerque Peixoto, A. L. V. (2022). Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. *P2P E INOVAÇÃO*, 9(1):206–221.

Manzoor, J., Waleed, A., Jamali, A. F., and Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source siem solutions for smes. *Plos one*, 19(3):e0301183.

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., Al-Shahwani, H., et al. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. *Mesopotamian journal of cybersecurity*, 2023:1–6.

Project Management Institute (2017). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. Project Management Institute, sixth edition.

Shoard, P., Davies, A., and Schneider, M. (2023). Magic quadrant for security information and event management. https://www.gartner.com/doc/reprints?id=1-2BDC4CDWamp;ct=221010amp;st=sb.

Sou Ciência, Centro de Estudos Sociedade, U. e. C. (2024). Orçamento das universidades federais. https://souciencia.unifesp.br/dados-fctesp/orcamento-universidades-federais.

Tariq, A., Manzoor, J., Aziz, M. A., Tariq, Z. U. A., and Masood, A. (2023). Open source siem solutions for an enterprise. *Information & Computer Security*, 31(1):88–107.