UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

WESLEY FRANCO FERREIRA

APLICAÇÃO DE CONCEITOS DE SOC: IMPLEMENTAÇÃO DE SIEM COM ELASTICSEARCH

CAMPO MOURÃO

2023

WESLEY FRANCO FERREIRA

APLICAÇÃO DE CONCEITOS DE SOC: IMPLEMENTAÇÃO DE SIEM COM ELASTICSEARCH

APPLICATION OF SOC CONCEPTS: IMPLEMENTATION OF SIEM WITH ELASTICSEARCH

Trabalho de conclusão de curso de graduação apresentado como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação do Curso de Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná (UTFPR). Orientador(a): Prof. Dr. Luiz Arthur Feitosa dos Santos.

CAMPO MOURÃO

2023

WESLEY FRANCO FERREIRA

APLICAÇÃO DE CONCEITOS DE SOC: IMPLEMENTAÇÃO DE SIEM COM ELASTICSEARCH

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Ciência da Computação do Curso de Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 15/junho/2023

Geazzy Brasilino Marçal Zanoni
Especialização em redes de computadores
Link para o currículo Lattes: http://lattes.cnpq.br/5907422406993028
Universidade Tecnológica Federal do Paraná

Rodrigo Campiolo
Doutorado em Ciência da Computação
Link para o currículo Lattes: http://lattes.cnpq.br/2822469089227391
Universidade Tecnológica Federal do Paraná

Luiz Arthur Feitosa dos Santos
Doutorado em Ciência da Computação
Link para o currículo Lattes: http://lattes.cnpq.br/3725232561617394
Universidade Tecnológica Federal do Paraná

CAMPO MOURÃO

2023

RESUMO

FERREIRA, Wesley Franco. **Aplicação de conceitos de SOC**: implementação de SIEM com Elasticsearch. 2023. Trabalho de conclusão de curso (Bacharelado em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2023.

Com o cenário atual de cibersegurança, empresas são invadidas no dia a dia em questão de segundos, porém podendo demorar entre dias e até semanas para detectar essas invasões. Esse défice de detecções acontece mesmo entre empresas de grande porte onde existem grandes orçamentos exclusivos para equipes de segurança, ferramentas e criação de processos. No caso de empresas de pequeno e médio porte a utilização de equipes de segurança se torna inviável devido ao seu alto custo de implantação com pessoas especializadas, ferramentas e processos. O principal objetivo deste trabalho foi desenvolver um sistema utilizando ferramentas *open source* que possibilite a detecção de eventos de segurança de forma automatizada em tempo real. Juntamente com o monitoramento de eventos de segurança, um dos objetivos é a centralização de logs, possibilitando centralizar a utilização de uma interface de visualização que permite uma melhor análise dos dados, assim contribuindo com uma melhora na investigação de possíveis incidentes. Primeiramente definiram-se as ferramentas que seriam utilizadas, definindo a utilização do pacote de software *Elk Stack*. Em seguida foi definido a linguagem de programação para o desenvolvimento de um script para consulta e análise dos dados. Durante o desenvolvimento do script foi definido a criação de regras utilizadas para analisar as informações em busca de eventos específicos. Por fim a definição do fluxo de envio de alertas informativos contendo informações sobre os eventos detectados. A geração de logs utilizando o *framework* de auditoria do Linux foi possível coletar 2.071.123 de eventos sobre um *host*, consumindo cerca de 1,4 Gigabytes em espaço de disco. Diariamente foram coletados em média 49.312 eventos. Com a execução do script de monitoração a cada 1 hora, foi possível identificar 124 eventos do uso de comandos com elevação de privilégios administrativos. Com a centralização dos dados, foi implantada uma interface de visualização de dados permitindo a realização de consultas de simples até complexas facilitando a análise dos dados, além da possibilidade de extração de relatórios com uma infinidade de filtros. O desenvolvimento deste trabalho foi possível implementar uma monitoração de ativos baseada em eventos pré-definidos, criando e enviando alertas informativos. Outra contribuição é a melhora na forma de análise de grandes volumes de dados, extração de relatórios e identificação de padrões.

Palavras-chave: cibersegurança; detecção; incidentes; elasticsearch; SIEM.

( ) Não autorizo a disponibilização de endereço de correio eletrônico para contato.

(x) Autorizo a disponibilização do seguinte correio eletrônico para contato:

wesley2ff@gmail.com

ABSTRACT

FERREIRA, Wesley Franco. **Application of SOC concepts**: SIEM implementation with Elasticsearch. 2023. Trabalho de conclusão de curso (Bacharelado em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2023. Título original: Aplicação de conceitos de SOC: implementação de SIEM com Elasticsearch.

With the current cybersecurity scenario, companies are invaded on a daily basis in a matter of seconds, but it can take between days and even weeks to detect these invasions. This detection deficit happens even among large enterprises where there are large budgets dedicated to security teams, tools and process creation. In the case of small and medium-sized companies, the use of security teams becomes unfeasible due to their high cost of implementation with specialized people, tools and processes. The main objective of this work was to develop a system using open source tools that allows the detection of security events in an automated way in real time. Along with the monitoring of security events, one of the objectives is the centralization of logs, making it possible to centralize the use of a visualization interface that allows a better analysis of the data, thus contributing to an improvement in the investigation of possible incidents. First, the tools that would be used were defined, defining the use of the Elk Stack software package. Next, the programming language was defined for the development of a script for querying and analyzing the data. During the development of the script, the creation of rules used to analyze the information in search of specific events was defined. Finally, the definition of the flow of sending informative alerts containing information about the detected events. Generating logs using the Linux auditing framework was able to collect 2,071,123 events on a host, consuming about 1.4 Gigabytes of disk space. An average of 49,312 events were collected daily. By running the monitoring script every hour, it was possible to identify 124 events involving the use of commands with elevation of administrative privileges. With the centralization of data, a data visualization interface was implemented, allowing queries from simple to complex, facilitating data analysis, in addition to the possibility of extracting reports with an infinity of filters. The development of this work made it possible to implement asset monitoring based on predefined events, creating and sending informative alerts. Another contribution is the improvement in the way of analyzing large volumes of data, extracting reports and identifying patterns.

Keywords: cybersecurity; detection; incidents; elasticsearch; SIEM.