Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Аналіз лог-файлів з використанням ELK для виявлення потенційних загроз безпеці*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Analysis of log files using ELK for detecting potential security threats*
переклад англійською

Освітній ступінь : бакалавр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 40
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 21 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 84

УДК:

Автор роботи
Прізвище, ім'я, по батькові (укр.): Чурбаков Константин Олексійович
розкривати ініціали

Прізвище, ім'я (англ.): Churbakov Konstantyn
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Козак Руслан Орестович
повністю

Прізвище, ім'я (англ.): Kozak Ruslan
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Михалик Дмитро Михайлович
повністю

Прізвище, ім'я (англ.): Mykhalyk Dmytro
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: канд. техн. наук, доц.

Ключові слова:
українською: ELK, лог-файли, безпека, загрози, аналіз даних.
до 10 слів

англійською: ELK, log files, security, threats, data analysis.
до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена аналізу лог-файлів за допомогою ELK для виявлення потенційних загроз безпеки. Робота охоплює теоретичні аспекти аналізу лог-файлів та систем ELK, включаючи розгляд видів лог-файлів, їх значення в інформаційній безпеці, особливостей зберігання та аналізу лог-файлів. Порівнюються відмінності логів у Windows та Linux. Детально розглядаються принципи збору та аналізу лог-файлів з використанням ELK, включаючи Elasticsearch, Logstash та Kibana.

В роботі проаналізовано статистику та атаки, класифіковані загрози безпеки інформації та розглянуто практичні приклади використання аналізу лог-файлів для виявлення загроз. Впроваджено систему для аналізу лог-файлів з використанням ELK, включаючи встановлення Elasticsearch, Logstash і Kibana, а також розробку шаблонів та фільтрів для аналізу лог-файлів.

англійською:

The qualification thesis is dedicated to the analysis of log files using ELK to identify potential security threats. The work covers theoretical aspects of log file analysis and ELK systems, including the review of types of log files, their significance in information security, and peculiarities of storage and analysis of log files. The differences between logs in Windows and Linux are compared. The principles of collecting and analyzing log files using ELK, including Elasticsearch, Logstash, and Kibana, are considered in detail.

The work analyzes statistics and attacks, classifies information security threats, and considers practical examples of using log file analysis to detect threats. The system for analyzing log files using ELK is implemented, including the installation of Elasticsearch, Logstash, and Kibana, as well as the development of templates and filters for log file analysis.

Чурбаков К. О. Аналіз лог-файлів з використанням ELK для виявлення потенційних загроз безпеці: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / К. О. Чурбаков. – Тернопіль: ТНТУ, 2023. – 84 с.