Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи бакалавра *Використання штучного інтелекту для ефективного реагування на інциденти у SIEM системі*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Using Artificial Intelligence for Effective Incident Response in the SIEM*
переклад англійською

Освітній ступінь : магістр

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

Екзаменаційна комісія: Екзаменаційна комісія № 41
напр.: Екзаменаційна комісія №1

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

Дата захисту: 26 грудня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 98

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Кубарич Захар Петрович
розкривати ініціали

Прізвище, ім'я (англ.): Kubarych Zakhar
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.): Скарга-Бандурова Інна Сергіївна
повністю

Прізвище, ім'я (англ.): Skarga-Bandurova Inna
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: доктор технічних наук, професор кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Боднарчук Ігор Орестович
повністю

Прізвище, ім'я (англ.): Ihor Bodnarchuk
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): кандидат технічних наук, зав. кафедри КН

Ключові слова
українською кібербезпека, SIEM, штучний інтелект, Wazuh, Nmap, LLM
до 10 слів

англійською cybersecurity, SIEM, artificial intelligence, Wazuh, Nmap, LLM
до 10 слів

Анотація

українською:

Штучний інтелект розширює можливості SIEM-систем в управлінні інформацією та подіями безпеки, пропонуючи безпрецедентну автоматизацію, точність і швидкість.

Традиційні заходи безпеки еволюціонують, а штучний інтелект надає можливості для проактивного виявлення загроз і реалізації прогностичних моделей безпеки.

У дослідженні були розглянуті основні теорії штучного інтелекту, які можуть бути застосовні до SIEM систем і підкреслено баланс між використанням можливостей штучного інтелекту та усуненням пов'язаних з ним ризиків, таких як: якість даних і конфіденційність.

Було продемонстровано процес впровадження мовленнєвої моделі штучного інтелекту до SIEM системи для надання інформації про наявні загрози у системі.

англійською:

Artificial intelligence expands the capabilities of SIEM systems in managing security information and events by offering unprecedented automation, accuracy, and speed.

Traditional security measures are evolving, and artificial intelligence provides opportunities for proactive threat detection and the implementation of predictive security models.

The study reviewed the main theories of artificial intelligence that can be applied to SIEM systems and emphasized the balance between using the capabilities of artificial intelligence and eliminating the associated risks, such as data quality and privacy.

The process of implementing a speech model of artificial intelligence into a SIEM system to provide information about existing threats in the system was demonstrated.

Бібліографічний опис:

1. Bandr Siraj Fakiha. 2020. Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness. International Journal of Forensic Medical and Toxicological Sciences. [online] Available at: https://medicopublication.com/index.php/ijfmt/article/view/11587/10679.

2. National Institute of Standards and Technology (NIST). 2020. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. [online] Available at: https://csrc.nist.gov/pubs/ir/8219/final