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

Авторська довідка

(кваліфікаційної роботи магістра)

Назва кваліфікаційної роботи бакалавра *Аналіз методик виявлення вторгнень у системах інформаційної безпеки*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Analysis of Intrusion Detection Methods in Information Security Systems*
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: 83

УДК: 004.42

Автор роботи
Прізвище, ім'я, по батькові (укр.): Микитишин Артур Андрійович
розкривати ініціали

Прізвище, ім'я (англ.): Mykytyshyn Artur Andriyovych
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.): Лечаченко Тарас Анатолійович
повністю

Прізвище, ім'я (англ.): Lechachenko Taras
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: Ph.D, старший викладач кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Дуда Олексій Михайлович
повністю

Прізвище, ім'я (англ.): Duda Oleksii
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: к. т. н., доцент, доцент кафедри комп'ютерних наук

Ключові слова
українською лог-аналіз, ids, система захисту, filebeat, rusthound, jinja, elasticsearch, python, інцидент-

виявлення

до 10 слів

англійською log analysis, ids, defense system, filebeat, rusthound, jinja, elasticsearch, python, incident detection

до 10 слів

Анотація

українською:

Кваліфікаційна робота презентує комплексний підхід до виявлення порушень безпеки в інформаційних системах, використовуючи методи лог-аналізу та інтеграції різних джерел інформації. У дослідженні наведено висновки щодо ефективності методу виявлення порушень та його загальної корисності, з врахуванням Elasticsearch та Python.

Ключовою складовою системи є використання Filebeat для отримання та передачі логів від агентів безпеки Defender у систему Elasticsearch. Rusthound, у свою чергу, виступає як додаткове джерело контекстної інформації, що допомагає збагачувати дані, отримані від Defender, і розширювати їхню інтерпретацію.

Процес виявлення порушень у роботі здійснюється із використанням Python для реалізації скриптів та автоматизації ряду завдань. Для генерації повідомлень про інциденти використано Jinja, що уможливило генерування індивідуалізованих повідомлень.

Використання інтегрованого підходу у дослідженні до аналізу логів забезпечує глибоке та повне розуміння стану безпеки системи. Комбінація Filebeat, Rusthound, Elasticsearch, Python і Jinja створює потужний інструментарій для виявлення, аналізу та реагування на потенційні порушення безпеки, роблячи інформаційні системи більш стійкими та захищеними.

англійською:

The qualification work presents a comprehensive approach to detecting security breaches in information systems using log analysis methods and integration of various information sources. The study provides conclusions about the effectiveness of the method of detecting violations and its overall usefulness, taking into account Elasticsearch and Python.

A key component of the system is the use of Filebeat to receive and transfer logs from Defender security agents to Elasticsearch. Rusthound, in turn, acts as an additional source of contextual information that helps enrich the data received from Defender and expand its interpretation.

The process of detecting operational irregularities is carried out using Python to implement scripts and automate a number of tasks. Jinja is used to generate incident notifications, which makes it possible to generate customized messages.

Using an integrated approach to log analysis in the study provides a deep and complete understanding of the system's security status. The combination of Filebeat, Rusthound, Elasticsearch, Python, and Jinja creates a powerful toolkit for detecting, analyzing, and responding to potential security breaches, making information systems more resilient and secure.

Бібліографічний опис:

Микитишин А. А. Аналіз методик виявлення вторгнень у системах інформаційної безпеки: кваліфікаційна робота магістра за спеціальністю 125 — Кібербезпека / Микитишин Артур Андрійович. – Тернопіль : ТНТУ, 2023. – С. 83