

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2024

Безпека інформаційних технологій

МАТЕРІАЛИ

XIII Міжнародної науково-технічної
конференції

9-11 травня 2024
м. Львів (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 257 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XIII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека та захист інформації, а також всім зацікавленим.

3MICT

Methodology for choosing a consensus algorithm for blockchain technology.....	12
<i>Tetiana Bazhan¹, Viktoriia Zhebka², Serhii Zhebka³</i>	12
Software Vulnerability Detection Using Large Language Models.....	14
<i>Beliaiev Igor¹, Peleshko Dmytro²</i>	14
Analysis of methods and models for assessing the consequences of the loss of information with limited access, its value and aging.....	16
<i>Yurii Dreis¹, Oleksandr Korchenko²</i>	16
On the semigroup of monoid endomorphisms of a some extension of a bicyclic semigroup.....	19
<i>Oleg Gutik¹, Inna Pozdniakova²</i>	19
Lagrangian approach for Navier-Stokes Equations.....	20
<i>Ostap Hrytsyshyn¹, Valeriy Trushevskyy²</i>	20
Unveiling Privacy Risks in the Data-Driven Urban Landscape of the Smart Cities.....	22
<i>Pavlo Ihnatolia¹, Yaroslav Syvokhop², Vasyl Rizak³</i>	22
Detection of LDAP Reconnaissance or Kerberoasting attacks using machine learning.....	24
<i>Roman Karpiuk¹, Petro Venherskyi², Michael Kropyva³</i>	24
Emerging research directions in post-quantum cryptographic primitives based on group cryptography.....	27
<i>Yevgen Kotukh¹, Gennady Khalimov², Volodymyr Liubchak³</i>	27
Correlation of Strategic Decisions of NATO and the USA With the Amounts and Origins of Cyber Threats.....	31
<i>Oleksandr Kuchyk¹, Danylo Shcherbyna²</i>	31
Vulnerabilities Detection in Smart Contracts.....	33
<i>Sundas Munir</i>	33
Heat-driven changes in dielectric layers for aircraft fairings.....	34
<i>Oleksii Nimych¹, Ihor Makieiev²</i>	34
SQL Injection Vulnerabilities in C# Applications.....	37
<i>Orest Onyshchenko¹, Yaryna Kokovska², Petro Venherskyi³</i>	37
Design and analysis of Walsh-Tukey function systems of any order.....	39
<i>Dmytro Poltoratskyi</i>	39
Using artificial intelligence to predict cyberattacks.....	41
<i>Anton Shantyri¹, Vyacheslav Zinchenko²</i>	41
Rhino IMS CDR APV fields for network and subscriber identification.....	42
<i>Storchak Kamila, Sahaidak Viktor</i>	42
Head Harnessing Skills and Fostering Innovation: The Role of Ethical Hacking CTF Competitions in Cybersecurity Education.....	44
<i>Olga Torstenson</i>	44
Social media: from communication to security threats.....	46
<i>Olha Vasylieva</i>	46

Конкурентна розвідка як основа інформаційно-аналітичного забезпечення безпеки організації.....	49
<i>Ірина Аксьонова¹, Тетяна Мілевська²</i>	49
Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України	51
<i>Валерія Балацька¹, Василь Побережний², Іван Опірський³</i>	51
Підвищення стійкості ідентифікації вторгнень у комп'ютерну систему за рахунок глибинної нейромережі	53
<i>Кирило Безпалий¹, Вячеслав Гуменюк², Павло Павловський³</i>	53
Основні аспекти безпеки при виконанні польотів безпілотними авіаційними комплексами.....	55
<i>Блаженний Назарій</i>	55
Ефективність захисту персональних комп'ютерів через телеграм-бот	56
<i>Любомир Боценюк¹</i>	56
Вплив користувацьких інтерфейсів на безпеку інформації.....	58
<i>Буковецький Василь¹, Михайло Різак²</i>	58
Генерація зображень в завданнях стеганографічного захисту	60
<i>Андрій Варениця¹, Дмитро Пелешко^{1,2}, Олена Винокурова²</i>	60
Методи та засоби мінімізації ризиків привілейованих облікових засобів в інформаційних системах.....	62
<i>Петро Венгеський¹, Андрій Ребець²</i>	62
Підхід до вибору стратегії застосування методів протидії кібератакам	64
<i>Сергій Веретюк¹, Катерина Молодецька²</i>	64
Обмін шифрованими повідомленнями в командному рядку.....	66
<i>Віталій Власов¹</i>	66
З історії української авіаційної промисловості. 1919–1926 рр	67
<i>Валерій Ворожко</i>	67
Використання алгоритмів CCC/UMAC для вдосконалення протоколу SSL/TLS.....	69
<i>Алла Гаврилова¹, Ірина Аксьонова²</i>	69
Система моніторингу периметра об'єкта критичної інфраструктури.....	71
<i>Олександр Галущенко¹, Володимир Дужецький²</i>	71
Аналіз методів оцінки кібербезпеки програмного забезпечення	73
<i>Роман Гамрецький¹, Віктор Гнатюк²</i>	73
Частота оновлення маркерів доступу при використанні OAuth 2.0 технології.....	75
<i>Микола Герцюк¹, Дмитро Новостройний²</i>	75
Кібербезпека колісних транспортних засобів: регламенти ООН.....	77
<i>Віктор Горицький, Анна Дорошенко</i>	77
Задачі кібербезпеки в хмарних обчисленнях	79
<i>Давиденко А.М.</i>	79

Тенденції та виклики у навчанні з кібербезпеки	81
<i>Максим Делембовський¹, Денис Калениченко²</i>	81
Параметрична оптимізація законів руху порталного маніпуляційного робота	83
<i>Мирослав Демидюк^{1,2}, Богдан Проць²</i>	83
Методи виявлення вторгнення в ІТ інфраструктуру	86
<i>Дмитро Денисюк¹, Олег Савенко², Антоніна Каїталія³</i>	86
Математична модель для аналізу інформаційних потоків в соціокіберфізичних системах	88
<i>Наталія Дженюк¹, Максим Толкачов²</i>	88
Розробка алгоритму автентифікації на основі криптокової конструкції Мак-Еліса	90
<i>Сергій Дунаєв¹, Вадим Стеценко²</i>	90
Розробка методу генерації зображень на основі заданого текстового опису для обходу водяних знаків	92
<i>Максим Житніков¹, Дмитро Пелешко^{1,2}, Олена Винокурова²</i>	92
Автоматизоване керування та планування маршрутів для БпЛА	95
<i>Ігор Жуков¹, Сергій Балакін², Богдан Долінець³</i>	95
Використання блокчейн-технології для підвищення безпеки від SQL ін'єкцій	98
<i>Ірина Замрій¹, Іван Шахматов²</i>	98
Математична модель оцінки захищеності хмарних сервісів	102
<i>Євгенія Іванченко¹, Ірина Лозова², Євгеній Педченко³, Марі Петровська⁴, Ігор Іванченко⁵</i>	102
Аналіз поняття кіберстійкості критичної інфраструктури	106
<i>Євгенія Іванченко¹, Олександр Корченко², Наталія Вишневіська³, Ігор Іванченко⁴</i>	106
Афінний шифр зсуву в системі залишкових класів	114
<i>Михайло Касянчук¹, Микола Карпінський², Михайло Голембійовський³</i>	114
Метод захищеного зберігання медичних даних за допомогою розмежування прав доступу та блокчейну	115
<i>Вікторія Клиш, Владислава Ланова, Юрій Баршиєв</i>	115
Метод ідентифікації вторгнень на основі алгоритму визначення самоподібності трафіку та алгоритмів нечіткої логіки	117
<i>Юрій Кльоц¹, Наталія Петляк²</i>	117
Протидія витоку конфіденційної інформації шляхом аналізу та виявлення програм-шпигунів	119
<i>Олександр Ковальов¹, Тетяна Матьовка²</i>	119
Використання узагальнених матриць Галуа і Фібоначчі у потокових шифрах	121
<i>Арсен Ковальчук¹, Анатолій Білецький²</i>	121
Сучасні методи соціотехнічних атак	123
<i>Анна Корченко¹, Кирило Давиденко²</i>	123
Створення захищеного протоколу передачі даних для БПЛА	126
<i>Віктор Котетунов</i>	126

Модель пірингової мережі для захищеної корпоративної комунікації.....	127
<i>Михайло Кренцін¹, Леонід Куперштейн²</i>	127
Особливості застосування методів протидії змагальним атакам в системах виявлення вторгнень	130
<i>Олександр Кручинін¹, Володимир Святошенко², Дмитро Тимофєєв³</i>	130
Визначення важливих параметрів систем захисту інформації у захищених інформаційних мережах передачі даних	132
<i>Олександр Лаптєв, Юлія Хохлачова, Абдуллах Аль-Далваш, Наталія Вишневецька</i>	132
Ефективність та проблеми використання кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів	140
<i>Марина Ларченко</i>	140
Вплив соціальних мереж на інформаційну безпеку	142
<i>Світлана Легомінова¹, Юрій Якименко², Михайло Запорожченко³</i>	142
Ефективність алгоритмів машинного навчання для виявлення аномалій у фінансових операціях	144
<i>Юрій Лісовський¹</i>	144
Кіберполігон кафедри твердотіЛЬНОї електроніки та інформаційної безпеки УжНУ	146
<i>Богдан Маліцький¹, Сергій Калкутін², Василь Різак¹</i>	146
Шифрування з надійними ключами в асиметричних алгоритмах.....	147
<i>Юлія Мисло¹, Михайло Пагіря²</i>	147
Методологія побудови багатоконтурної системи безпеки у соціокіберфізичних системах .	149
<i>Станіслав Мілевський¹, Сергій Євсєєв², Ірина Аксьонова³</i>	149
Тенденція до змінювання парадигми забезпечування кібербезпеки.....	152
<i>Володимир Мохор¹, Олександр Бакалинський¹, Ярослав Дорогий^{2,3}, Василь Цуркан^{1,3}</i>	152
Проекти Європейського Союзу для безпеки Інтернету речей.....	153
<i>Тетяна Мужанова¹, Віталій Тищенко²</i>	153
Виклики та стратегії кібербезпеки цифрових послуг для широкого застосування	155
<i>Марія Навитка</i>	155
Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах	157
<i>Олена Негоденко¹, Віталій Негоденко²</i>	157
Дослідження методів апроксимації неявно заданих кривих в комп'ютерній графіці	159
<i>Михайло Олексин¹, Петро Венгерський²</i>	159
Поширення радіохвиль та його особливості як методика подолання природніх перешкод для телекомунікаційних систем	161
<i>Володимир Пархоменко¹, Андрій Щепак², В'ячеслав Пархоменко³</i>	161
Антенна протидії роботі радіомережі в діапазоні 2,4 ГГц.....	163
<i>Юрій Пена¹, Володимир Бичков²</i>	163

Аналіз кібератак на елементи інфраструктури об'єктів смарт технологій.....	165
<i>Дмитро Печериця</i>	165
Кібербезпека системи "Connected Car"	167
<i>Підлісний Ю.І.</i>	167
Виявлення безпекових аномалій інформаційно-комунікаційних мереж за допомогою моніторингових систем	169
<i>Василь Пограничний¹, Сергій Заблоцький², Мар'ян Кирик³</i>	169
Актуальні клептографічні загрози та потенційні методи протидії	171
<i>Олександр Полевод</i>	171
Дослідження загроз інформаційної безпеки Wi-Fi мереж	173
<i>Орест Полотай¹, Наталія Фединець²</i>	173
Критерії виявлення повільних DDoS-атак	175
<i>Петро Поночовний¹, Ігор Аверічев²</i>	175
Оцінювання та оптимізація ризику для консервативних систем захисту інформації.....	177
<i>Іван Прокопишин^{1,2}</i>	177
Динамічне емулювання як засіб виявлення поліморфних вірусів із маскувальними техніками	179
<i>Павло Резіда¹, Марія Капустян², Лигун Олексій³</i>	179
Удосконалення методу малоресурсного гешування HDG.....	181
<i>Віталій Селезньов¹, Володимир Лужецький²</i>	181
Дослідження log-файлів засобами платформи Elastic Stack	184
<i>Ольга Смотров¹, Микита Куріков²</i>	184
Модифікація методу вибору контейнера для зменшення чутливості стеганоповідомлення до збурних дій	188
<i>Сокальський Сергій</i>	188
Аналіз проблем кібербезпеки при використанні програмного забезпечення з відкритим кодом	192
<i>Андрій Тарасенко¹, Мар'ян Кирик²</i>	192
Оптимізація повного суматора у квантовій моделі обчислень.....	194
<i>Андрій Терещенко¹, Валерій Задірака²</i>	194
Розробка програмного забезпечення для симуляції акустичних хвиль за допомогою трасування променів.....	196
<i>Олександр Терлецький¹, Валерій Трушевський²</i>	196
Побудова нелінійних криптосистем та криптографічних протоколів	198
<i>Вера Тітова¹, Володимир Анікін², Наталія Петляк³</i>	198
Розроблення та застосування експлойтів з подальшою інтеграцією в ботнет	200
<i>Ростислав Ткачук, Артур Ткаченко, Роман Андрійв</i>	200
Анонімізація користувача в мережі інтернет за допомогою WHONIX	203
<i>Ростислав Ткачук, Богдан Філіпчук, Богдана Федина</i>	203

Дослідження log-файлів засобами платформи Elastic Stack

УДК 004.4:004.896

Ольга Смотров¹, Микита Купріков²

*Львівський державний університет безпеки життєдіяльності,
¹olgasmotr@gmail.com, ²nkuprikov@ldubgd.edu.ua*

Однією з найбільш поширених загроз для даних є несанкціонований доступ, що може призвести до втрати конфіденційності, цілісності та доступності інформації. Адже у сучасному світі, де взаємозв'язки набувають все більшого значення, конфіденційність інформації про продукти, процеси, клієнтів та постачальників є критично важливою для будь-якої компанії. Особливо відчутною ця необхідність стає в контексті спалаху інформаційної війни, що супроводжує повномасштабне вторгнення російських військ на територію України у 2022 році. Відповідно до прогнозів спеціалістів Cybersecurity Ventures на 2024 рік витрати світової спільноти на кіберзлочинність становитимуть близько 9,5 трильйонів доларів США. [1]. В свою чергу, кількість кібератак з метою заволодіння даними зростає більш ніж на 18%, середня вартість збитків від витоку даних становитиме понад 4,5 млн доларів США. [2].

Для розв'язання цих проблем на передньому краї технологічного розвитку стоїть аналіз log-файлів. Log-файли представляють собою записи подій, які відбуваються в системі або програмі, і є важливим інструментом для виявлення аномальних або підозрілих активностей. Аналіз log-файлів допомагає розуміти, як функціонує система та виявляти аномальну поведінку, що може свідчити про зловживання доступом або зловмисну діяльність. Це може бути корисно при розслідуванні інцидентів безпеки та при виявленні вразливостей, які можуть бути використані для атак на систему. Однак, аналіз log-файлів є трудомістким завданням, що, як правило, є складним для ручного аналізу, зважаючи на їх значний розмір та різні формати, залежно від того, яка система їх генерує. Адже log-файли можуть бути текстовими, бінарними або ж представленими у інших спеціальних форматах для зберігання даних. Для ефективного аналізу log-файлів доречно використовувати методіку структурного аналізу даних, з метою відокремити корисну інформацію від зайвої та виявити можливі загрози безпеці даних та алгоритми машинного навчання для виявлення аномальної активності в системі.

На сьогодні на ринку існує ряд платформ з інструментарієм аналізу log-файлів. Це такі як Elastic Stack, Splunk, Graylog, Fluentd тощо. Для подальшої роботи з log-файлами використовуватимемо Elastic Stack. Elastic Stack (ELK) складається з таких компонентів як: Elasticsearch, Logstash, Kibana та Beats, і забезпечує комплексне рішення для збору, аналізу та візуалізації даних. Вона має ряд переваг: висока швидкість, масштабованість, а також розширені можливості візуалізації та аналізу даних [3-6]. Однак, слід зазначити, що вона також має свої недоліки, зокрема, складність налаштування та використання для не досвідчених користувачів. Зокрема продемонструємо процес розробки фільтрів для Logstash.

Розробка фільтрів для Logstash є одним із вирішальних етапів у створенні системи аналізу log-файлів. Фільтри дозволяють трансформувати та розбирати вхідні дані на більш деталізовані складові, що спрощує подальший аналіз. Одним з

основних типів фільтрів, які будуть розроблені в рамках даної роботи, є фільтр "grok". Фільтр grok дозволяє структурувати неструктуровані log-файли, шляхом використання шаблонів. Цей інструмент ідеально підходить для обробки логів syslog, Apache та інших веб-серверів, MySQL та, загалом, будь-якого формату логів, який зазвичай пишуть для людей, а не для обробки комп'ютерами.

Основа роботи з Grok полягає в комбінуванні текстових шаблонів у такий, що відповідає вашим логам. Синтаксис для шаблону grok виглядає так:

```
%{SYNTAX:SEMANTIC}
```

де SYNTAX - це назва шаблону, який буде збігатися з вашим текстом. Наприклад, число 3.44 буде збігатися з шаблоном NUMBER, а IP-адреса 55.3.244.1 - з шаблоном IP. SEMANTIC - це ідентифікатор, який ви задаєте частині тексту, яка збігається. Наприклад, число 3.44 може бути тривалістю події, тому ви можете іменувати його просто "duration". Рядок "55.3.244.1" може ідентифікувати клієнта, який робить запит. У цьому випадку наш фільтр grok міг би виглядати так:

```
%{NUMBER:duration} %{IP:client}
```

Також можемо додати до свого шаблону grok перетворення типів даних. За замовчуванням, всі семантичні складові зберігаються як рядки. Якщо ви хочете змінити тип даних семантичної складової, наприклад, змінити рядок на ціле число, додайте до нього цільовий тип даних. Наприклад, %{NUMBER:num:int}, який конвертує семантичну складову "num" з рядка в ціле число. На даний момент підтримуються тільки перетворення в int і float.

Розглянемо, як за допомогою синтаксису і семантики можна витягти корисні поля, для прикладу, з такого логу HTTP-запиту:

```
55.3.244.1 GET /index.html 15824 0.043
```

Шаблон для цього логу може бути наступним:

```
%{IP:client} %{WORD:method}
%{URIPATHPARAM:request}
%{NUMBER:bytes} %{NUMBER:duration}
```

У кінцевому результаті наш файл конфігурації виглядатиме так (рис. 1).

```
input {
  stdin { } # Вихідний потік для отримання даних з консоліfile {
    path => "/var/log/http.log" # Шлях до файлу журналу, який потрібно обробити
  }
}
filter {
  grok {
    match => { "message" => "%{IP:client} %{WORD:method}
%{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}" }
  }
}
output {
  stdout {
    codec => rubydebug # Вивід даних у форматі Ruby-відладки
  }
  elasticsearch {
    hosts => ["http://localhost:9200"] # Адреси серверівElasticsearch
    index => "test.logstash" # Індекс, у який будуть зберігатися
дані
    user => "elastic" # Користувач Elasticsearch
    password => "3gu2Vh6K1wJCh*gvEQfp" # Пароль користувача
Elasticsearch
  }
}
```

Рис.1. Лістинг - Конфігурація Logstash-файлу «learn.conf» для обробки журналу HTTP

Наш запит можемо здійснити через командний рядок або ж у Kibana. Результат запиту з командного рядка та Kibana відображено на рисунках 2 та 3 відповідно.

```
55.3.244.1 GET /index.html 15824 0.043
{
  "@timestamp" => 2023-06-12T18:50:23.167602700Z,
  "client" => "55.3.244.1",
  "request" => "/index.html",
  "duration" => "0.043",
  "method" => "GET",
  "bytes" => "15824",
  "host" => {
    "hostname" => "WIN-AEAR2C9HGUN"
  },
  "message" => "55.3.244.1 GET /index.html 15824 0.043\r",
  "@version" => "1",
  "event" => {
    "original" => "55.3.244.1 GET /index.html 15824 0.043\r"
  }
}
```

Рисунок 2 - Результат зчитування log-файлу у командному рядку

Запит "55.3.244.1 GET /index.html 15824 0.043" був оброблений Logstash і вивід результату показує, що дані були успішно розпізнані і відформатовані за допомогою grok-виразу. Кожен елемент запиту відображений відповідним полем, наприклад, IP-адреса ("client"), HTTP-метод ("method"), URL-шлях ("request"), обсяг байтів ("bytes") та тривалість ("duration"). Додаткові поля, такі як "@timestamp" та "host.hostname", також відображаються. Загальний результат містить ключі та значення для кожного поля, яке було оброблено. Ці дані можна використовувати для подальшої аналітики, візуалізації та зберігання у Elasticsearch для подальшого використання.

У Kibana, в розділі "Expanded document" ми також можемо побачити розширені дані документу, які були збережені у Elasticsearch після обробки Logstash (див. рис. 3).

Expanded document

View: [Single document](#) [Surrounding documents](#)

Search new matches

Actions	Field	Value
🔍 🔗 🗑️ 🔍 🔍	* _id	mmxkIgtbPk1Rvk_8ku7
	* _index	test.logstash
	# _score	-
	📅 @timestamp	Jun 12, 2023 @ 21:50:23.167
	f @version	1
	📄 bytes	15824
	📄 bytes.keyword	15824
	📄 client	55.3.244.1
	📄 client.keyword	55.3.244.1
	📄 duration	0.043
	📄 duration.keyword	0.043
	f event.original	55.3.244.1 GET /index.html 15824 0.043
	f host.hostname	WIN-AEAR2C9HGUN
	f message	55.3.244.1 GET /index.html 15824 0.043
	📄 method	GET
	📄 method.keyword	GET
	📄 request	/index.html
	📄 request.keyword	/index.html

Rows per page: 25

Рисунок 3 - Результати нашого запиту у Kibana

Тепер за допомогою Kibana можна встановлювати фільтри за різними полями, такими як "client", "method" або "request", і швидко отримувати підсумкові дані для конкретних сегментів інформації. Окрім того, Kibana пропонує нам розширені можливості фільтрування та пошуку. Ми можемо виконувати розширені пошукові запити, використовуючи синтаксис Elasticsearch Query DSL, щоб знайти конкретні документи або аналізувати дані за певними умовами. Як наслідок, ми можемо точно налаштувати свої запити та отримувати результати, які відповідають конкретним потребам користувача. Наприклад, можна налаштувати систему моніторингу трафіку на мережевому рівні, щоб виявляти незвичайну активність, таку як велика кількість запитів від одного IP-адреси або незвичайні шаблони поведінки.

Висновок. Застосування системи Elastic Stack для аналізу log-файлів є доволі ефективним засобом виявлення потенційних загроз безпеці інформації. Даний підхід дозволяє підвищити рівень захисту інформації та забезпечити вчасне виявлення можливих загроз. Під час аналізу загроз безпеці інформації в системі ELK, можливо виявити різноманітні типи атак, такі як діяльність шпигунів, спам-атаки, фішингові атаки, вторгнення в систему, DDOS-атаки та інші. Для виявлення таких атак можна використовувати різноманітні техніки та методи, такі як: машинне навчання, статистичний аналіз, розробка правил або комбінування цих підходів.

Аналіз log-файлів надає можливість виявляти та вирішувати проблеми безпеки, що виникають в системі, а також розгорнути проактивні заходи безпеки, щоб запобігти майбутнім інцидентам. Розробка шаблонів та фільтрів для аналізу log-файлів є ключовою складовою налаштуванню Elasticsearch. Вона передбачає створення шаблонів для Elasticsearch, які визначають структуру даних та надають змогу ефективно зберігати та швидко отримувати доступ до них. Розробка фільтрів для Logstash допомагає приймати, обробляти та передавати дані в Elasticsearch для подальшого аналізу. Налаштування та впровадження системи ELK для аналізу log-файлів вимагає ретельного планування і налаштування, але при цьому дозволяє здійснювати ефективний моніторинг та виявлення потенційних загроз безпеки.

1. eSentire. Офіційний звіт про кіберзлочинність за 2023 рік. URL: <https://www.esentire.com/resources/library/2023-official-cybercrime-report> (дата звернення: 12.04.2024).
2. H-X Technologies. Прогнози на 2024 рік. URL: <https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua> (дата звернення: 12.04.2024).
3. Elastic N.V., "Elastic Stack Documentation." - [Електронний ресурс]. - Режим доступу : <https://www.elastic.co/guide/index.html> (дата звернення: 01.04.2024)
4. Kuprikov M, Smotr O. Monitoring and analysis of large amounts of data using the elastic stack platform. Information security and information technologies IBIT-2023: collection of abstracts of the VI All-Ukrainian scientific and practical conference, November 30, 2023. - Lviv, LSU of Life Safety, 2023. - P.341-343.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ

XIII Міжнародної науково-технічної конференції
«ITSec: Безпека інформаційних технологій»

9-11 травня 2024 року

м. Львів (Україна)

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних (у тому числі класифікаційного індексу УДК) уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі кібербезпеки
Львівського національного університету імені Івана Франка