НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри
_____ **Дмитро ЛАНДЕ**
(підпис)
«_____»_____2024 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Методи оптимізації "false positives" в системах виявлення вторгнень, засновані на комплексному використання даних про інформаційну систему.

Виконала: здобувачка вищої освіти **VI** курсу, групи ФБ-21мп
(шифр групи)

Григор'єва Ольга Олександрівна
(прізвище, ім'я, по батькові) (підпис)

Керівниця к.т.н., доцент кафедри ІБ Світлана Олександрівна Носок
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Науковий консультант д.т.н., с.н.с професор кафедри ММЗІ Кудін Антон Михайлович
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Рецензент заступник начальника управління безпеки інформації Національного банку України к.т.н., доцент Проскуровський Роман Васильович
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувачка вищої освіти
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський)
Спеціальність– 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ ДмитроЛАНДЕ
(підпис)
«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачці вищої освіти

Григор'єва Ольга Олександрівна _____
(прізвище, ім'я, по батькові)

1. Тема роботи: Методи оптимізації "false positives" в системах виявлення вторгнень, засновані на комплексному використання даних про інформаційну систему,
керівниця роботи к.т.н., доцент кафедри ІБ Світлана Олександрівна Носок
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «10» листопада 2024 р. №5236-с

2. Термін подання здобувачкою вищої освіти роботи 9 січня 2024 р.

3. Вихідні дані до роботи: наукова література та відкриті джерела за темою; попередні дослідження за темою; документація SIEM Wazuh та Splunk, існуючі правила виявлення вторгнень та напрацювання спільноти користувачів.

4. Зміст роботи: опис загальноприйнятих методів виявлення вторгнень, їх класифікація, переваги та недоліки; огляд існуючих методів оптимізації кількості FP; запропонована методика оптимізації кількості FP; пояснення щодо запроваджених практичних дій для підвищення ефективності виявлення.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація на тему «Методи оптимізації "false positives" в системах виявлення вторгнень, засновані на комплексному використання даних про інформаційну систему».

6. Дата видачі завдання 20 березня 2023 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вибір теми роботи	06.02.2023 – 17.03.2023	
2	Отримання завдання	20.03.2023	
3	Вивчення літератури за темою, вибір літературних джерел	21.03.2023 – 31.05.2023	
4	Проходження переддипломної практики, написання практики	01.09.2023 – 27.10.2023	
5	Вивчення проблем існуючих метрик виявлення, написання першого розділу	01.09.2023 – 29.09.2023	
6	Дослідження існуючих способів оптимізації, написання другого розділу	02.10.2023 – 31.10.2023	
7	Проведення експериментів, розгортання лабораторії, написання третього розділу	01.11.2023 – 01.12.2023	
8	Аналіз отриманих знань та результатів	04.12.2023 – 28.12.2023	
9	Отримання допуску до захисту	29.12.2023	
10	Створення презентації для захисту дипломної роботи	01.01.2024 – 08.01.2024	
11	Передзахист дипломної роботи	09.01.2024	
12	Доопрацювання дипломної роботи та презентації	09.01.2024 – 15.01.2024	
13	Захист дипломної роботи	16.01.2024	

Здобувачка вищої освіти  Ольга ГРИГОР’ЄВА

(підпис) (**Власне ім’я, ПРІЗВИЩЕ**)

Керівниця роботи  Світлана НОСОК

(підпис) (**Власне ім’я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Робота складається з 3 розділів, містить 21 іллюстрацій, 2 таблиці, 1 додаток та 33 літературні посилання, обсяг роботи – 76 сторінок.

Завданням роботи є аналіз загальноприйнятих методів виявлення вторгнень, оцінка їх ефективності, переваг та недоліків, вивчення способів оптимізації кількості хибнопозитивних спрацювань, розгортання лабораторного середовища з встановленими SIEM Wazuh та Splunk, тестування у них запропонованих методів оптимізації на основі збирання комплексних даних про події у системі.

Метою роботи є підвищення ефективності виявлення вторгнень за допомогою комплексного аналізу даних про функціонування системи та зменшення кількості хибнопозитивних спрацювань, а також розробка універсальної методики такої оптимізації.

Предметом дослідження є: методи виявлення вторгнень та оптимізації кількості false positives. Об’єктом дослідження є: системні події, що збираються SIEM системами.

Наукова новизна полягає у тому, що не існує універсального підходу до оптимізації ефективності виявлення вторгнень, заснованого на комплексному використанні даних про інформаційну систему.

Ключові слова: Оптимізація Кількості False Positive; Системи Виявлення Вторгнень; Виявлення Аномалій; Комплексний Аналіз Поведінки; Керування Інформацією та Подіями Безпеки; Без Сигнатурні Методи Виявлення Вторгнень.

ABSTACT

The work consists of 3 sections, contains 21 illustrations, 2 tablesб 1 appendix and 33 references, the volume of work – 76 сторінок.

The task of the work is to analyze the generally accepted methods of intrusion detection, evaluate their effectiveness, advantages and disadvantages, study ways to optimize the number of false positives, deploy a laboratory environment with installed SIEMs Wazuh and Splunk, test the proposed optimization methods based on the collection of complex data about events in the system.

The aim of the work is to increase the efficiency of intrusion detection by means of comprehensive analysis of system functioning data by reducing the number of false positives, as well as the development of a universal technique for such optimization.

The subject of research are: intrusion detection methods and false positives optimization. The object of research are: system events collected by SIEM systems.

The scientific novelty is that there is no universal approach to optimizing the effectiveness of intrusion detection based on the comprehensive use of information system data.

Keywords: False Positives Optimization; Intrusion Detection Systems (IDS); Anomalies Detection; Comprehensive Behavioral Analysis; Security Information And Event Management (SIEM); Signatureless Intrusion Detection Methods.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS – Intrusion Detection Systems

IPS – Intrusion Prevention Systems

SIEM – Security Information and Event Management

FP – false positive

FN – false negative

FPR – False Positives Rate

FNR – False Negative Rate

APT – Advanced Persistent Threat

WS – Work Station

ВСТУП

Збір інформації про події у системі є ключовим та відправним етапом у проблемі виявлення факту вторгнення, протидії йому та майбутнього попередження. Природним чином, від якості та повноти зібраних даних напряму залежить здатність системи та спеціалістів з безпеки виконати ці критичні операції. На SIEM систему, окрім збору та зберігання подій, покладається і механізм виявлення вторгнень, а на експертів, що з нею працюють – вкладення до неї ефективних методів рішення цієї задачі. Серед класичних методів можна виділити дві групи: сигнатурні та такі, що засновані на аномаліях, проте ні разом, ні поодинці, вони не дають бажаного рівня ефективності виявлення, створюючи хибнопозитивні спрацювання чи пропускаючи реальні атаки. Перед фахівцями таким чином, лежить завдання не тільки покращення вже існуючих, але і задача розробки нових систем чи методів виявлення, адже як проблема перенавантаження SIEM подіями, так і пропуск вторгнення є не прийнятними для інформаційних систем захисту.

Актуальність роботи полягає у тому, що від питання оптимізації FPR напряму залежить ефективність системи виявлення вторгнень, а аналіз сучасних тенденцій у сфері інформаційних технологій дає підстави вважати, що кількість FP за часом буде лише зростати, що негативним чином впливатиме на здатність системи захисту виявляти та протистояти вторгненням. З іншого боку дані телеметрії, отримані від систем моніторингу функціонування інформаційних систем та систем захисту інформації не використовуються в повному обсязі для зниження рівня FP. До того ж, використання для вирішення задачі методів лише однієї групи (наприклад, статистичних) вимагає значного збільшення об’єму даних для аналізу, тому комплексне використання як даних телеметрії так і методів виявлення аномалій різних типів є вельми перспективним напрямком досліджень.

Перший розділ роботи присвячено огляду загальноприйнятих методів виявлення вторгнень, аналізу їх переваг та недоліків, другий розділ має на меті

вивчити існуючи методи оптимізації FPR та запропонувати такий, що буде універсальним та кращим за інші, а третій розділ окрім демонстрації функцій та можливостей двох популярних сучасних SIEM Wazuh та Splunk, буде виділено для практичного втілення запропонованої методики у правилах виявлення цих систем та тестуванню написаних правил на прикладі мережевої атаки, що експлуатує віддалений доступ до робочих станцій та підбір паролів.

Мета роботи: дослідження існуючих напрацювань у галузі виявлення вторгнень, у тому числі їх класифікація та існуючі методи оптимізації ефективності даних підходів; створення універсальної методики на базі комплексного використання даних про інформаційну систему і методів виявлення аномалій різного типу та її практичне запровадження та тестування ефективності.

Мета роботи реалізується за допомогою наступних **задач дослідження**:

1. Визначити та описати загальноприйняті методи виявлення вторгнень, знайти їх слабкі та сильні сторони;
2. Зробити висновки щодо їх ефективності та галузі кращого застосування;
3. Дослідити яким чином у тематичній літературі вирішується задача оптимізації FPR, з акцентом на універсальність підходу;
4. Запропонувати та описати підхід на базі комплексного використання даних про інформаційну систему та методів виявлення аномалій різного типу;
5. Розгорнути лабораторне тестове середовище у VMware Workstation зі встановленими на хостах SIEM Wazuh та Splunk, продемонструвати їх функціонал та специфіку задач, які вони вирішують найкращим чином;

6. Провести симуляцію атаки зі спробою віддаленого доступу засобами SSH на робочі станції, що працюють на базі операційних систем Windows та Linux;
7. Розробити правила виявлення наведеного типу мережевих атак, що використовуватимуть дані про події комплексно;
8. Протестувати ефективність виявлення;
9. Надати алгоритм універсального підходу до оптимізації FPR з урахуванням отриманих теоретичних та практичних знань.

Предметом дослідження є: методи виявлення вторгнень на основі аналізу аномалій та оптимізації кількості false positives. **Об'єктом дослідження** є: системні події, що збираються SIEM системами.

Методом дослідження є аналіз наявних теоретичних та практичних напрацювань з питання виявлення вторгнень та оптимізації FPR; критичний підхід до оцінки можливості їх універсального прикладного запровадження; побудова лабораторного середовища для тестування запропонованих методів з метою подальшого зведення результатів та висновків до єдиного підходу вирішення проблеми оптимізації FPR з використанням комплексних даних про інформаційну систему.

Наукова новизна полягає у тому, що не існує універсального підходу до оптимізації ефективності виявлення вторгнень, заснованого на комплексному використанні даних про інформаційну систему та комплексного використання методів виявлення аномалій різних типів для зниження значень FP.

Практичне значення одержаних результатів полягає в тому, що запропонований алгоритм підвищення ефективності виявлення вторгнень підходить для інфраструктури будь-якої складності та направленості і окрім головної мети також може позитивним чином вплинути на ресурси, що потрібні для її функціонування, а також підвищити рівень обізнаності щодо її стану для фахівця з безпеки.

1 ЗАГАЛЬНОПРИЙНЯТІ МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Будь-яка SIEM система має на своїй меті збір інформації про всі події у дослідному середовищі, їх зручний аналіз та агрегування або ж іншими словами – моніторинг подій безпеки. З точки зору інформаційної безпеки, цікавими є ті події, що пов’язані з певною зловмисною активністю у системі, тобто свідчать про її компрометацію. Сама по собі SIEM з налаштуваннями за замовчуванням, на відміну від наприклад IPS чи IDS, не здатна ані виявити загрозу, ані запобігти її експлуатації, адже потужним інструментом вона стає лише у руках спеціаліста з кібербезпеки, який налаштовує її та правила виявлення загроз в залежності від певної конкретної ситуації, інфраструктури, яку має бути захищено, та профілю зловмисника. Правила виявлення вторгнень – певні синтаксично-логічні кореляції, що автоматично шукають серед усіх подій підозрілі шаблони поведінки або певні зловмисні рядки, тобто сигнатури, та сповіщають фахівця про вірогідну атаку. Оскільки досконалих правил для виявлення вторгнень не буває, часто подібні сповіщення (security alerts) виявляються хибними, тобто та активність, яка спричинила реагування правила, насправді була легітимною, просто наприклад не зовсім типовою, що призвело до створення, як це прийнято називати у галузі SIEM та математичної статистики, false positive, тобто помилки першого роду. Ще гірше, коли умови правила виявлення не були розраховані на незвичайну атаку та звісно не створили сповіщення про неї, що вже називається статистичною помилкою другого роду або ж false negative.

Самі значення false positive чи false negative не є інформативними, адже будуть різні для кожної системи, тому у математичній статистиці для порівняння ефективності роботи системи виявлення використовують поняття FPR та FNR, які обраховуються за наступними формулами:

False Positive Rate (FPR) = $\frac{FP}{FP+TN}$,

False Negative Rate (FNR) = $\frac{FN}{FN+TP}$,

де FP – кількість false positive, TP – true positive, FN – false negative TN – true negative.

Ці два поняття невідривно пов’язані один з одним, адже покращення показників одного призводить до аналогічного погіршення іншого. Для прикладу, намагаючись не пропустити серед великої кількості дозволеного трафіку зловмисний, умови правил виявлення вторгнень можуть бути надто широкими, що звісно допоможе виявити більше можливих атак, проте створить додатковий шум для аналітиків, що будуть переглядати сповіщення. Таким чином, окрім важливих задач збору та зберігання подій безпеки, SIEM також має бути спроможним балансувати значення FP та FN. Проблема генерації більшої, аніж можливо обробити, кількості FP і є головною у даній роботі. Оптимізація їх значень допомогла б не лише фахівцям витрачати менше часу на розгляд хибних спрацювань, але й зняла б зайве навантаження з SIEM систем, а отже, їх ефективність виявлення реальних вторгнень зросла б.

Методи написання правил для виявлення вторгнень переважно використовують один типовий підхід або комбінацію для досягнення своєї мети, серед яких:

1. Сигнатурний
2. Поведінковий (виявлення аномалій поведінки)
3. Статистичний
4. Машинного навчання

Глобально виділяють тільки **сигнатурний** (signature-based) та метод, **заснований на аномаліях** (anomaly-based), адже інші є їх варіаціями або комбінаціями [1]. Так, поведінковий метод можна розглядати з боку аномальних шаблонів поведінки, статистичний – з боку аномальної кількості певних подій, машинне навчання ж взагалі саме для виявлення аномалій у часових рядах в контексті питання і використовується. Усі вони мають свої переваги та недоліки, чому буде приділено увагу у першому розділі даної роботи, причому буде показано, як жоден з них не спроможний забезпечити бажану ефективність поодинці. Сигнатурний метод у більш широкому розумінні також називається **шаблонним виявленням**, а заснований на аномаліях – **безшаблонним**. Причому останній включає в себе також методи, що працюють на основі

ймовірнісних моделей, тобто не потребують готового шаблону. Саме їх застосування і вважається у даній роботі перспективним рішенням проблеми надмірної кількості false positive.

Питання виявлення загроз та вторгнень також часто згадується разом з поняттям аномалій, проте треба розуміти, що аномальна активність у системі не завжди є чимось зловмисним, на відміну від терміну вторгнення, який обов'язково пов'язаний з деякою атакою. Виявити реальну природу аномалії – легітимну чи ні – також частина оптимізації ефективності роботи SIEM, проте оскільки у процесі виявлення аномалії, тобто відхилення від норми, неможливо заздалегідь знати відповідь на це питання, умовно усі нетипові події вважаються загрозами до моменту розгляду, тому часто у літературі та у даній роботі ці два поняття можуть бути синонімічними.

Доволі повна класифікація методів виявлення наведена у роботі [2, ст.76] та приведена на Рисунку 1.1:

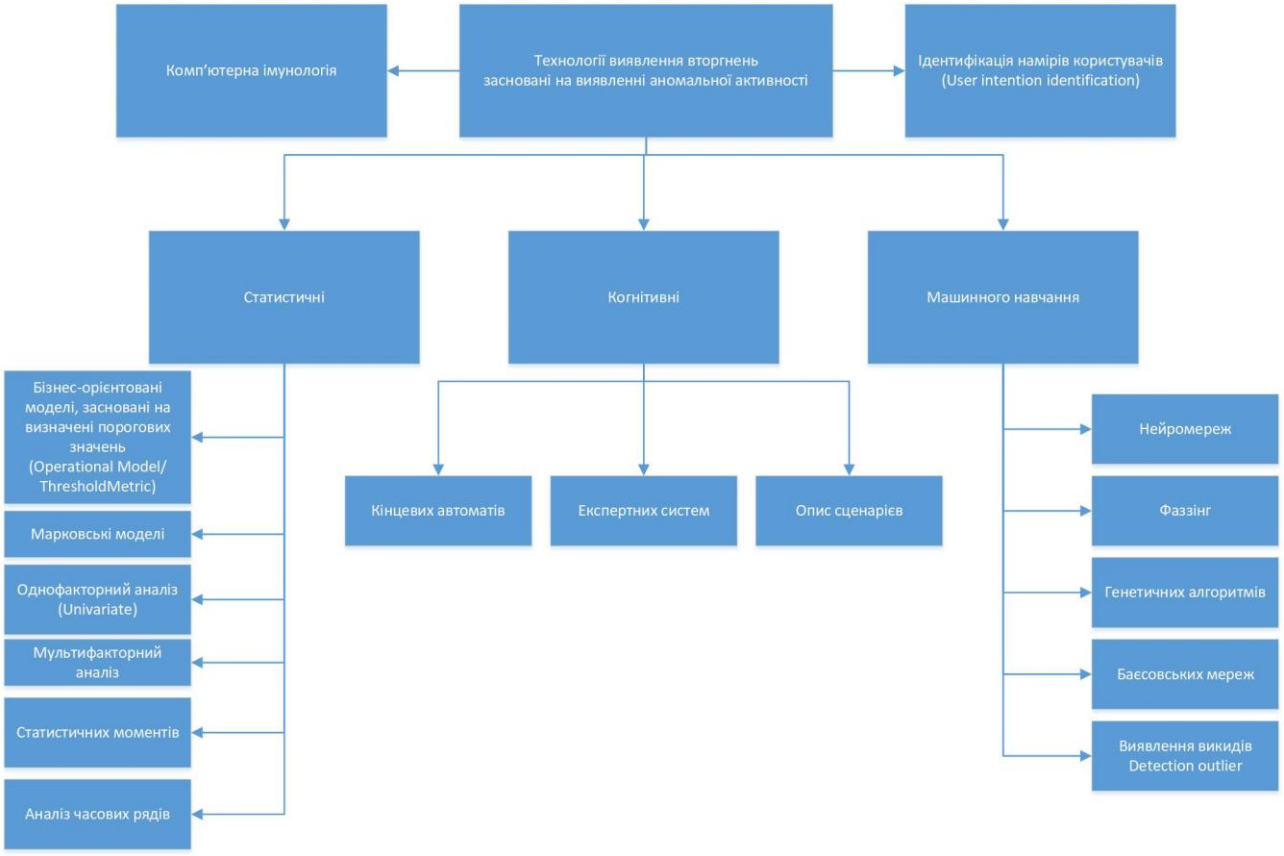


Рисунок 1.1 – Класифікація методів виявлення вторгнення [2, ст.76]

1.1 Сигнатурні та поведінкових методи виявлення вторгнень

1.1.1 Сигнатурні методи виявлення вторгнень

Найпершим та найбільш інтуїтивним методом для побудови системи виявлення аномалій є збір інформації про вже скоєні атаки. Природним чином, якщо певна зловмисна дія колись призвела до успішної атаки, то зібравши сліди та артефакти, що залишили по собі злодії, можна буде швидко зв’язати можливі наступні підозрілі дії з ними. Оскільки абстрактний підхід до опису характеру дій хакерів важче формалізувати у єдиний алгоритм (хоча і такі спроси звісно існують), ніж виділити “відбитки” у вигляді IP адрес, хешів файлів чи доменних імен, більшість SIEM використовують саме сигнатурний підхід до вирішення задачі знаходження серед безлічі звичайних подій деяких аномальних або ж зловмисних.

Сигнатурний метод доволі простий у реалізації: зібрані артефакти додаються до різних списків та фільтрів, які використовуються для “просіювання” через них загальної маси подій, що збирають SIEM системи [3]. Окрім очевидного недоліку з неповнотою списку чи динамічністю даних, постає проблема ресурсів, людських та цифрових. Для підтримання сигнатурних баз у більш-менш актуальному стані потрібні спільні зусилля великої кількості спеціалістів з безпеки з усього світу та допомога небайдужих користувачів, але ніхто з них все рівно не зможе напевно сказати, чи потрібно зважати у своїх перевірках наприклад на IP адресу, з якої вже три роки не було зареєстровано ніяких шкідливих дій, чи вона вже давно належить цілком легітимному сервісу. Така проблема потребує додаткової складної математичної системи для оцінки актуальності даних, яка все рівно не дасть 100% гарантії. Бази ж баз хешів взагалі вражають своїми розмірами та марністю, адже для зловмисника набагато легше змінити один символ свого ескплойту, ніж сервісу для перевірки репутації файлів внести всі варіації до бази. Порівняння хешів підозрілих файлів з базами дозволяє лише з впевненістю судити про легітимність файлу (констатувати true

negative), якщо його хеш має відмітку “чистий”, особливо у поєднанні з надійним цифровим підписом, проте ніяк не допомагає у ситуації, коли хеш не міститься у базі [4]. Цифрові ж ресурси, потрібні для проведення операцій пошуку сумнівних артефактів у списках дозволених чи зловмисних, важко уявити з огляду на те, скільки мільйонів подій може надходити до SIEM системи у великій компанії лише за одну секунду. Часто такі ресурси просто не виправдовують витрат на них, беручи до уваги їх низьку ефективність виявлення реальних аномалій, тобто true positive, та проблему атак нульового дня – неможливо виявити те, чого немає у базі.

Важливою проблемою є також той факт, що сигнатурні методи безсилі перед складними атаками, що мають декілька стадій, адже принципово не розглядають події як ланцюжок, перевіряючи кожну з них окремо [5, ст.4]. Проте потрібно визнати, що за умови актуальної бази сигнатур, визначити типову атаку буде доволі легко, враховуючи, що окрім хешу, може бути використано ще багато інших сигнатур. Сигнатурами можуть бути:

- Мережеві артефакти: IP адреси, домени, порти
- Файлові: хеш, нетипове розширення, ім’я, атрибути
- Певний набір ключових слів, знаків або бітів у командах
- Відомі командні рядки, що часто використовують зловмисники

Беззаперечною силою сигнатурних методів, проте, являється їх простота та швидкість роботи: складання та підтримання баз все ж таки не така складна задача, як побудова нового довершеного автоматизованого алгоритму, що буде самостійно приймати рішення про природу аномалії, а пошук серед “словника” сигнатур – операція швидша за навчання поведінкової моделі. Також варто визнати, що за обставин, коли атака відома базі, її однозначно і легко буде виявлено.

1.1.2 Поведінкові методи виявлення вторгнень

Перш ніж пояснити причину недосяжності бажаної ефективності сигнатурними методами, потрібно розглянути також поведінкові – сучасніший та більш комплексний підхід до виявлення аномалій. Аналіз поведінки певної системи це принципово більш абстрактний процес і сучасною практикою для його реалізації є різноманітні використання машинного навчання та нейронних мереж. Загальний процес виглядає просто та перспективно: алгоритм навчається на великій кількості “нормальної поведінки” користувача, можливо отримує певні дані щодо можливих аномальних дій і далі легко відрізняє одну поведінку від іншої [6]. На практиці часто важко однозначно сказати, що є нормальною поведінкою, адже користувач може вирішити попрацювати у вихідні, випадково відкрити сумнівний сайт, зробити друкарську помилку та взагалі безліччю способів змусити алгоритм виявити його дії як небезпечні і – згенерувати false positive. Також не варто забувати, що дані про поведінку кожного окремого користувача можуть бути невеликими та відносно простими, але у масштабах великої організації хибне навчання системи автоматичного виявлення аномалій неминуче. Ба більше, погано навчений алгоритм буде пропускати реальні атаки, адже не матиме інформації про схожу поведінку, а хакери, як відомо, можуть бути дуже винахідливими. Дуже узагальнено, можна сказати, що поведінковий аналіз – автоматизована комплексна база сигнатур, але сигнатур поведінки.

Аналогічним до минулого, але повністю інакшим за виконанням, є підхід до виявлення аномалій через аналіз тактик та технік зловмисників – всім відома матриця MITRE [7]. Існує можливість налаштувати SIEM шукати у подіях послідовності дій, які можуть бути трактованими як звична поведінка хакерів. У тому, аби виділити та корелювати між собою такі ланцюжки, і допомагає матриця MITRE. Зрозуміло, що такий підхід не повною мірою вирішує проблеми двох згаданих раніше, адже з одного боку він може бути більш точним, проте потребує обережного налаштування, бо матриця MITRE дає загальні поради як

виявити ту чи іншу зловмисну активність, але кожна система унікальна і потрібно зважати на її особливості.

Перевагою поведінкового методу над сигнатурним однозначно можна назвати його можливість виявляти потенційні інсайдерські атаки, адже якщо сформовано профіль поведінки користувача (які типові операції, коли і як він виконує), то вірогідно відхилення від нього можна вважати аномалією та виконувати більш докладний аналіз подій [8, ст.2]. Такий підхід не захистить від FP, зате дозволить з більшою вірогідністю не пропустити реальну атаку.

1.1.3 Проблеми сигнатурних та поведінкових методів

Отже, якщо повернутися до питання **“Чому сигнатурні та поведінкові методи не дають високого відсотку ефективності та мають високий рівень помилок першого чи другого роду?”,** то основна причина такої ситуації - люди. Залишаючи на розсуд фахівця з безпеки не тільки процес налаштування SIEM системи, а й докладний розгляд кожної виявленої аномалії окремо, з одного боку, можливо серед FP з більшою вірогідністю знайти реальну аномалію, але так само вірогідно її і пропустити, бо судження спеціаліста врешті-решт, також схильне до пошуку шаблонів поведінки користувача, які він формує з досвідом. Від налаштувань SIEM системи якраз і залежить у більшій мірі чи буде вона ефективно працювати, навіть за використання згаданих методів. У цьому питанні не можна вдаватися до крайнощів: надто точні умови виявлення аномалії підвищать рівень FN, надто широкі – FP. Часто роблять вибір у бік всеохоплюючих критеріїв та запроваджують ручну перевірку, що потребує певної кількості спеціалістів.

На ефективність звісно впливають і доступні компанії ресурси: грошові та цифрові. Як вже було згадано, за великих можливостей використання сигнатурних баз не зашкодить, але не варто покладатися лише на них. Як і в більшості питань кібербезпеки, для виявлення аномалій найкраще працюватимуть комплексні методи, що будуть брати краще від кожного з

підходів та нівелювати помилки, які виникають через недоліки, порівнюючи вердикти та приймаючи рішення щодо аномалій за встановленим алгоритмом [9]. Якщо ж підбивати підсумки, то можна виділити такі недоліки описаних вище методів, спочатку для сигнатурних:

- Неповнота та великий об’єм сигнатурних баз
- Значна кількість ресурсів для підтримання в актуальному стані та обробки операцій пошуку зловмисних сигнатур
- Неможливість виявити zero-day атаки
- Помилкові спрацювання за умови застарілої бази сигнатур
- Сигнатури не є універсальними для будь-якої системи чи атаки

І тепер для поведінкових:

- Великий об’єм даних для навчання
- Помилкове навчання для складних систем
- Велика кількість помилкових спрацювань
- Складний процес налаштування
- Зловмисні дії, що імітують легітимну поведінку

1.2 Статистичний метод виявлення аномалій

Принцип дії статистичних методів базується на кількісних знаннях про роботу системи, так наприклад, мережева система, що використовує такий підхід для виявлення аномалій працює приблизно так: «Кожному пакету присвоюється рейтинг його «аномальності», який вказує на ступінь його відхилення від нормального профілю. Якщо рейтинг вище певного порогу «нормальної» поведінки, виконується заздалегідь визначена дія» [10]. За такого алгоритму дій, експерти отримують сповіщення про можливі вторгнення лише якщо їх “рівень підозри” достатньо високий, що підвищує шанс того, що виявлено дійсну атаку, а отже менше часу витрачається на розгляд “шуму” – false positive.

Статистичний метод також можна з одного боку вважати поведінковим, проте він дозволяє створювати більш складні правила виявлення у SIEM. Зрозумілим чином, коли у системі трапляється аномальна подія, це не завжди щось погане. Для прикладу візьмемо неуспішний вхід користувача. Він може бути спричинений низкою факторів: пароль нещодавно було змінено, користувач зробив помилку при введенні, якийсь застосунок продовжує автоматично використовувати старий захешований пароль або ж дійсно відбувається атака з підбором паролей. Аби відкинути випадкові причини, правила SIEM часто можуть встановлювати граничне допустиме значення неуспішних входів, за якого створюється сповіщення безпеки, адже реальний брутфорс навряд чи буде обмежуватися кількома спробами. Окрім такого варіанту, може відбуватися також моніторинг кількості інших подій, наприклад для веб-ресурсу притаманний трафік певних об’ємів і за умови його аномального зменшення або збільшення, також можна підозрювати атаку. Статистичні методи враховують типові кількісні метрики подій у системі, аби виявляти аномалії. До цього типу правил виявлення також можна віднести такі, що базуються на кількості спрацювань на певному хості: якщо за деякий проміжок часу відбулося кілька підозрілих подій, можна стверджувати, що вірогідність зловмисних дій за таких обставин вища.

Окрім більш складних статистичних шаблонів, можуть враховуватися і очевидні: більша кількість подій щодо наприклад вже згаданих невдалих входів у систему, буде спостерігатися на початку робочого дня та після обідньої перерви, адже у ці інтервали більша кількість людей буде здійснювати вхід зі зрозумілих причин, аніж десь серед дня. Аби досягнути більш точного рішення про аномальність певної кількості трафіку у визначений момент, його можна порівнювати не тільки з учорашнім, а і з більш довгими інтервалами у ретроспективі, причому за такого способу ефективність та точність напряму залежить від наявних ресурсів зберігання. Якщо подібна активність ніколи не була виявлена, вона може бути аномальною.

Статистичні методи аналізу даних використовують теоретико-ймовірнісні моделі статистики, такі як дерева рішень, аналіз часового ряду та ентропій. Робота [11] показує на основі відкритого набору мережевих даних ефективність різних підходів для виявлення аномалій та значення FP спрацювань, так, за результатами згаданої роботи, метод дерева рішень має 94% ефективності, і всього 8% хибнипозитивних рішень. Схожі експерименти проводяться з застосуванням і машинного навчання, у тому числі на базі кластерного аналізу.

1.3 Методи виявлення вторгнень за допомогою машинного навчання

Машинне навчання у питанні виявлення аномалій виконує суміжну зі статистичними методами задачу: маючи вибірку легітимних та зловмисних даних з системи, можливо використати зручний алгоритм для навчання на тестових даних, який має бути приблизно у співвідношенні 1:5 до реального трафіку, з тим, аби пізніше навчена модель самостійно класифікувала події на нормальні та підозрілі. Звичайно, різні алгоритми та підходи даватимуть не однакові відповіді та матимуть різну ефективність. Складність для спеціаліста з машинного навчання якраз і полягає у тому, що не існує єдиного вірного підходу для окремих задач і чим влучніше буде підібрано не лише алгоритм, а і його параметри, тим краще працюватиме система виявлення вторгнень.

Загалом, у літературі більше прийнято застосовувати машинне навчання або нейронні мережі на етапі IDS/IPS, дослідження ж для SIEM проводяться рідше. Це можна пояснити більшою кількістю функцій, що виконує SIEM, порівняно зі здебільше однопрофільним завданням систем виявлення атак, які природним чином мають ту саму мету, що і методи класифікації чи кластерізації машинного навчання: відділити від дозволеного трафіку підозрілий. Перекладання відповідальності щодо визначення легітимності ще й мережевих подій на SIEM може створити додаткове навантаження, що має шанс у свою чергу виснажити ресурси системи. Але й перевага такого комплексного рішення може себе виправдати, адже якщо IDS/IPS пропустять шкідливу подію, SIEM

матиме шанс це виправити на своєму етапі роботи, створивши сповіщення безпеки. Не зайвим буде також додати, що SIEM переважно в ідеалі позиціонується як достатнє комплексне рішення, що не потребує інших механізмів, проте якщо ресурси дозволяють, то кращим рішенням буде все-таки обрати поєднання систем.

Щодо конкретних засобів машинного навчання, то для задачі виявлення вторгнень застосовують широкий спектр алгоритмів. Все також залежить і від вхідних даних для навчання, адже якщо наявний трафік, де чітко відомо, що є аномальним, а що ні, то можна говорити про кероване навчання, а якщо наприклад є приклади тільки легітимних подій, то це вже напів кероване навчання, і відповідно усе, що не виглядає схоже на відомі дані буде класифікуватися як аномалія. Також існує і навчання без вчителя, коли алгоритм сам визначає на базі припущення, що дозволених подій більше, природу даних. За такого виду можлива велика кількість FP, якщо тестова вибірка усе-таки містила вагому кількість зловмисних дій [12, ст.2]. У фаховій літературі за проблематикою даної роботи наводяться безлічі варіантів рішення питання пошуку аномалій, тому для більш ґрунтовного огляду було обрано найбільш повне з наразі наявних систематизованих досліджень – [12], за даними якого найпопулярнішими техніками машинного навчання є алгоритм Support Vector Machine, кластерний аналіз, різні варіації нейронних мереж. Цікавим є також той факт, що у більшості робіт, розглянутих у згаданому вище джерелі, у якості датасету використовується або застарілі загальнодоступні дані, або трафік з реальних приватних систем, що ще раз свідчить про недостатнє освітлення теми у фаховій літературі. [13] також стверджує, що один із найкращих рішень для пошуку вторгнень саме в галузі кібербезпеки є одно класовий Support Vector Machine та алгоритм Bayesian Online Changepoint Detection (BOCD), причому перший добре підходить для пошуку аномального мережевого трафіку, а другий – для аналізу складних даних, які погано піддаються класифікації традиційними статистичними методами.

Для даних про події безпеки у виді часових рядів часто використовують рекурентні нейронні мережі з довгою короткотривалою пам’яттю або long short-term memory – LSTM; хоча їх традиційне застосування – розпізнавання мовлення, можна знайти роботи, де демонструється їх вдале використання до задач пошуку аномальної активності, як наприклад у [14]. Можливі також виявлення вторгнень у часових рядах за допомогою кластеризації такими популярними методами як k-найближчих сусідів (k-Nearest Neighbors) або методом k-середніх – k-Means.

Так само, як і зі статистичними та поведінковими методами, не останнім недоліком машинного навчання у питанні виявлення зловмисного трафіку є відсутність універсального єдиного способу, який би однаково добре працював принаймні на різних операційних системах, не кажучи вже про різної складності та налаштувань інфраструктури. Переважно, дослідження з застосуванням машинного навчання показують добрі результати підвищення ефективності тільки на окремому датасеті, що є серйозним недоліком.

1.4 Тенденції у питанні false positives

Враховуючи наведені вище методи та їх різнобарв’я, стає зрозумілим, що питання оптимізації FP займає вагоме місце у переліку актуальних проблем серед фахівців з безпеки. Проте чи мають вони інші підстави, окрім бажання покращити ефективність виявлення своїх систем, витрачати багато часу на рішення згаданого питання? Виявляється, що дослідження трендів у кібербезпеці та цифрових даних свідчить лише про майбутнє підвищення кількості FP, а отже немає підстав вважати, що воно вирішиться саме або перестане бути актуальним. Розглянемо тенденції , які було виявлено під час роботи над темою.

Через зростаючу популярність хмарних центрів обробки даних та аутсорсингу SOC послуг, у питаннях виявлення аномалій з’явилися нові виклики. Період пандемії спричинив стрімке зростання попиту на сторонні послуги безпеки, але, як показують деякі опитування, порівняно з 37% компаній,

які користувалися послугами аутсорсингу у 2021 році, поточні 22% виглядають менш привабливо [15]. Якою б не була статистика, також безсумнівно, що як малі, так і неспеціалізовані компанії продовжуватимуть використовувати таку допомогу SOC для управління своєю безпекою через економію коштів і персоналу. Часто легше використовувати вже налаштований механізм, ніж створювати його з нуля, і хоча стороннім фахівцям може знадобитися більше часу, щоб ознайомитися з новою інфраструктурою та працювати з усіма конфіденційними даними в компанії, переваги SOC на аутсорс можуть компенсувати це. Процес налаштування систем безпеки для ефективного виявлення аномалій і вторгнень може бути складнішим із аутсорс-версією SOC, ніж з його внутрішньою версією, але в будь-якому випадку цей процес, очевидно, створить величезну кількість помилкових спрацьовувань. Хоча кваліфіковані штатні експерти, швидше за все, подолають цю проблему шляхом ретельного налаштування, це не завжди варіант.

Не дивно, що ключовою метою кожної системи безпеки, яка покладається на SIEM у справі пошуку аномалій, є зменшення рівня шуму або помилкового спрацьовування. Таким чином, **говорячи про ефективність будь-якої установки виявлення, ми маємо на увазі рівень помилкових спрацьовувань, які вона створює**. Чим менше помилкових спрацьовувань, тим краща система.

Аналіз фактів виявлення вторгнень дозволяє виявити наступні свіжі тенденції:

1. Зростання важливості каналів зв'язку в хмарі

Якщо здебільшого покладатися на хмарні служби для безпеки чи інших проблем, потрібно розуміти, що якщо з будь-якої причини хмара недоступна, вся робота неминуче припиняється. Серед таких причин, звичайно, DDoS-атаки, які шкодять доступності ресурсів компанії, завдаючи не тільки фінансової, але й репутаційної шкоди. За даними [16], DDoS-атаки залишаються в топ-10 ризиків хмарної безпеки, тому захист каналів зв’язку між хмарою та її клієнтами має велике значення. Щоб пом’якшити їх, можна запропонувати використання IDS та перевірку трафіку брандмауера, а також пошук аномалій та блокування IP-

адрес, що також принесе більше помилкових спрацьовувань. На жаль, навіть такі респектабельні компанії, як Cloudflare, не можуть запропонувати нічого краще, ніж вручну додавати винятки або змінювати чутливий рівень правила виявлення для випадків, коли легітимний трафік класифікується як шкідливий [17].

2. Підвищення вимог до автентичності джерела IOC-ів

Довіряючи величезним спискам IOC сумнівного походження, компанія знижує ефективність виявлення та змушує експертів і системні ресурси бути постійно перевантаженими. Бази даних IOC слід не тільки часто оновлювати, але й перевіряти на предмет достовірності та авторитетного походження. Для оцінки значущості IOC можна використовувати різні методології, наприклад, як описано в [18] або інші рішення, засновані на ML. Іншим варіантом є аналіз cyber kill chain [19], який насправді також можна автоматизувати за допомогою ML. Незважаючи на те, що багато компаній не дуже щедрі, коли справа доходить до обміну досить цінним досвідом боротьби з кіберзагрозами, деякі платформи з відкритим кодом для обліку IOC існують. Кілька прикладів включають OpenIOC Framework, MISP, IBM X-FORCE, SANS Internet Storm Center, численні відкриті рішення Github тощо.

3. Довірений зловмисник

Оскільки хмарні сервіси набули популярності, вони стали корисними не лише для звичайних користувачів, але й для хакерів, що призвело до того, що зловмисник користується тими ж привілеями в хмарному сервісі, що й законний користувач. Більше того, система навряд чи перевіряє так само поглиблено, наприклад внутрішній трафік, як той, що надходить ззовні. Як стверджується [20], «понад 35% інцидентів безпеки хмари сталися через використання зловмисниками дійсних, скомпрометованих облікових даних». Ці статистичні дані розкривають значну проблему інсайдерських атак, особливо беручи до уваги той факт, що такі дії можуть бути не такими явно злими, як інші інциденти. Виникає питання: як відрізнити таку діяльність користувача від звичайної? Найкращі практики включають надання найменш необхідних привілеїв користувачам, впровадження деяких поведінкових алгоритмів виявлення та

використання підходу DSPM (Data Security Posture Management), який може запобігти витоку конфіденційних даних [21]. Так само як пошук аномалій може бути виходом із ситуації, це також створить більше шуму виявлення.

4. Комплексний аналіз поведінки користувачів

Через передовий характер сучасних кібератак традиційне ставлення до виявлення відхилень від нормальної поведінки користувачів, засноване на сигнатурах, потребує більш комплексного розгляду. Хакери більше не загрожують лише обліковим записам із високими привілейованими правами, вони вважають за краще перестрахуватися й поступово отримувати все більше й більше доступу до системи, починаючи з користувачів із низьким рівнем доступу, які часто не отримують захисту та уваги, якої вони потребують. На щастя, розробникам засобів захисту відомо про описані ризики, і деякі рішення вже представлені. Наприклад, хмарна служба CASB (Cloud Access Security Broker) від Oracle має модуль User Behavior Analytics (UBA), який може виконувати «динамічну оцінку ризиків користувача на основі постійної оцінки поведінки користувачів», створювати шаблони доступу та контролювати використання додатків користувачами [22]. Інші зміни, включно з будь-якими привілеями чи конфігурацією безпеки, також мають вирішальне значення для моніторингу та перевірки. IBM QRadar також пропонує подібний сервіс UBA [23], який використовує можливості ML для вилучення моделі поведінки користувача з вже наявних логів. Іншим чудовим прикладом впровадження UBA є Exabeam, який також за допомогою ML може виявляти відхилення від встановлених базових показників.

5. Збільшення обсягів даних телеметрії

У відповідь на нові атаки спеціалісти змушені додавати більше правил виявлення, джерел журналів, перевірок, які щорічно множать телеметричні дані. У якийсь момент ресурси компанії вичерпуються, і вона вже не має повного контролю над ситуацією. «38% компаній працюють з обмеженою обізнаністю про те, що відбувається в їхньому програмному забезпеченні», — йдеться в [24]. Інакшими словами, надмірний збір журналів означає, що не всі вони фактично

використовуються або корисні в розслідуваннях. Серед уже згаданих проблем [24] також зауважує, що «телеметричні дані є неструктурованими; різні формати ускладнюють використання; підготовка даних займає багато часу, а конфіденційні дані в журналах можуть призвести до порушення відповідності вимогам».

6. Комплексно слід розглядати окрім IOC, й інші дані телеметрії

З попереднього абзацу випливає, що всі дані можуть бути зібрані даремно, якщо використовувати їх бездумно. Щоб досягти раннього виявлення аномалій, ніколи не буде достатньо проводити лише моніторинг IOC або інше виявлення на основі сигнатур, оскільки слід брати до уваги весь ландшафт. Фахівці з безпеки повинні спостерігати не просто за одним сповіщенням, а за послідовністю, здавалося б, законних дій, які призводять до атаки. Це можна зробити за допомогою складних правил виявлення, заснованих на знанні попередніх схем атак, наприклад таких, як пропонує MITRE. Крім того, алгоритми ML або нейронні мережі можуть навчатися на нормальній системній діяльності і, таким чином, стати здатними виявляти такі підозрілі моделі.

З дослідження сучасних тенденцій можна зробити однозначний висновок, що надмірна кількість FP є викликом для спеціалістів та за такого шляху розвитку, яким зараз йдуть цифрові технології, не має сумнівів, що їх кількість буде лише зростати у відповідь на спроби впровадження загального моніторингу та атак зловмисників, які лише ускладняються з часом. Тому вирішення даної проблеми є надзвичайно актуальним на цей день.

1.5 Актуальність проблеми надмірних FP спрацювань

Враховуючи усі недоліки шаблонних методів виявлення вторгнень, стає зрозумілим, чому не дивлячись на простоту та швидкість традиційних методів, спеціалісти постійно знаходяться в пошуках способів оптимізації FP: ефективність прийнятих підходів велика, але ресурси, потрібні на їх підтримання і проблема нових загроз постійно стимулюють до розвитку. Актуальність

питання оптимізації кількості FP, а значить і підвищення ефективності роботи SIEM чи IDS/IPS – запорука якості послуг, які надають ці системи. Ринок засобів кібербезпеки доволі конкурентний, на додачу до цього атаки також не зупиняють свого ускладнення, тому без розвитку система захисту існувати не може.

Підсумовуючи, основні причини, які роблять дослідження цієї теми і корисним, і актуальним, такі:

1. Дана галузь все ще недостатньо розвинена, причому це стосується як впевненої теоретичної бази, так і вдалих універсальних практичних рішень
2. Системи SIEM та IDS/IPS наразі є важливою частиною будь-якої системи захисту, отже покращення їх роботи також є важливою задачею для спеціалістів з безпеки
3. Залежність між захищеністю інфраструктури та ефективністю системи виявлення вторгнень пряма, отже не можна нехтувати будь-яким напрямком її підвищення
4. Оптимізація кількості FP звільнить ресурси як фахівців, так і системи захисту
5. Наявні практичні способи рішення проблеми не є ані універсальними, ані достатньо ефективними, аби подальше покращення не мало сенсу
6. Традиційні підходи шаблонного виявлення не здатні надати самі по собі задовільного рівня виявлення вторгнень та часто безсилі перед окремими типами атак (APT, zero-day)
7. Світові тренди у сфері кібербезпеки не дають жодних підстав вважати, що проблема надмірної кількості FP вирішиться сама собою, навпаки, прогнозується лише їх ріст

Висновки до розділу 1

Сигнатурні методи виявлення вторгнень, так само як статистичні та прості поведінкові, не в змозі забезпечити необхідної ефективності показників – false positives, через що системи часто перенавантажені та вже не можуть реагувати навіть на успішно виявлені загрози. Мета сучасних систем виявлення – вже не тільки пошук аномалій, а й побудова складних комплексних підходів та алгоритмів, що будуть враховувати не лише очевидні дані, а й кореляційні зв'язки між ними. Машинне навчання дає деякі можливості для оптимізації, проте йому бракує універсальності та простоти застосування.

Беручи до уваги поточні тенденції в хмарних службах, ми можемо лише зробити висновок, що всі вони вимагають більш комплексного підходу до виявлення аномалій і розширення інформації, яку ми збираємо з систем, що, у свою чергу, звісно створить більше false positive сповіщень, якщо ми не зможемо налаштувати системи виявлення обережніше або скористатися розширеними автоматизованими алгоритмами виявлення.

Було зроблено висновок, що враховуючи сучасний стан кіберпростору та тенденції, питання оптимізації FP є і буде актуальним. Одним із головних викликів у його рішенні є універсальність, адже запропонований вихід має бути можливо застосувати до будь-якої системи та її конфігурації. Зауважимо, як відомо з теорії математичної статистики, універсальними методами зниження рівня помилки першого роду є збільшення обсягу експериментальних даних, а отже збільшення комплексності збору даних про події в системи неодмінно приведе до зниження false positive, адже їх можна буде досліджувати на єдиній канві.

2 МЕТОДИ ЗМЕНШЕННЯ КІЛЬКОСТІ FALSE POSITIVES

З огляду на всі наведені у першому розділі цієї роботи аргументи щодо важливості рішення проблеми надмірної кількості FP, треба також оговорити, що завдання зменшення їх кількості є важливим не лише з точки зору фахівця з безпеки. З одного боку, на питання: «**Що гірше: пропустити вторгнення чи витратити зайвий час на розгляд легітимного трафіку?»**, спеціаліст з кібербезпеки матиме чітку відповідь, що звісно не знати про атаку критичніше, ніж мати перенавантажену систему, адже це можна вирішити збільшенням обчислювальних ресурсів та штату аналітиків. Така ситуація розглядається по-різному за різних обставин, адже ризики різнопланових інфраструктур мають не тільки окрему природу, але і збитковість. Тому приймається рішення на базі всіх присутніх факторів щодо доцільності ніяких чином не допустити незнання про вторгнення, аби не зазнати репутаційних та фінансових збитків, чи зняти навантаження з системи, припускаючи, що потенційна атака не буде фатальною чи буде виявлена іншими засобами, що також має місце бути.

Але важливо розуміти, що з точки зору користувача, наявність FN – реально присутньої атаки – не така критична, як можливість блокування його легітимних запитів чи дій через надто широкі умови правил спрацювання та реагування на інциденти [25, ст.147]. Факт того, що SIEM пропустив атаку, може дратувати користувача набагато менше, коли це не повторюється надто часто, ніж ситуація, коли його нормальній роботі будуть заважати системи захисту, наприклад як IPS, що може заблокувати його віддалене підключення чи перегляд сторінки у браузеру. Оскільки з точки зору спеціаліста FP більш припустимі за FN, не дивно що їх часто генерується рази більше, проте як показують результати аналізу, зокрема [25, ст.151], не дивлячись на те, що відношення FP:FN≈13:1, «кількість видів атак у випадках FN – 27, тобто близька до кількості видів атак у випадках FP – 35». Це свідчить про різноманітність способів атак у порівнянні з їх кількістю та про можливість узагальнити більшу частину FP до деякої кінцевої кількості груп, а отже ефективніше їх фільтрувати.

2.1 Організаційні та конфігураційні методи

Найперша реакція на велику кількість FP – перегляд та валідація доцільності прийнятих політик безпеки та існуючих правил виявлення. Якщо умови правила доволі легко піддаються калібруванню, чи було виявлено факт недостатньої кваліфікації працівника, що їх створював, достатньо буде змінити або правила, або команду, або усе одразу, проте навіть найдосвідченіші спеціалісти світу не в змозі написати ідеальні умови спрацювань, тому варто бути обачним у своїх діях. Дуже часто наявність FP навіть не викликана нетиповою підозрілою поведінкою користувача чи слабкими правилами, а як [25, ст.151] наприклад стверджує, «91 відсоток сповіщень FP, що дорівнює приблизно 85 відсоткам помилкових випадків, пов’язано не з проблемами безпеки, а з політикою управління». Це означає, що в інфраструктурі немає чітких прав доступу: ніде не прописано, хто і які права має, на які об’єкти та дії на ними присутні дозволи, які команди нормальні лише для працівників IT-відділу, а які для – інших. Усе це призводить логічним чином до потреби кожен незрозумілий випадок досліджувати окремо, навіть іноді з отриманням підтвердження від користувача, який здійснив дії, що викликали підозру, про їх природу та легітимність. Дуже погано відбивається на роботі системи не лише відволікання працівників на такі звернення, але й потреба адміністратора чи фахівця з безпеки витрачати на це час.

Замість цього зваженим та ефективним рішенням буде за відсутності – створення, а за наявності – розширення та уточнення правил політики управління на основі діючих або потрібних у системі правил доступу. Такі чіткі інструкції не лише довозлять додати відомі виключення до правил виявлення, чим значно знімуть навантаження з аналітиків, але й дозволять використовувати можливості SIEM системи повною мірою. До того ж така система хоча і потребуватиме схожого з сигнатурними базами оновлення, проте її актуалізація набагато простіша через те, що кожну нову зміну у політиці безпеки треба буде внести до виключень лише один раз, і після цього спрацювань, викликаних нею, вже не

буде. Для прикладу можна уявити собі користувача, який підключається через VPN до корпоративної мережі: кожного разу IP адреса такого користувача буде різною і не є доцільним вносити їх всі, зате у налаштуваннях VPN може бути виставлено певну країну, і тільки її адреси буде у майбутньому при підключенні отримувати користувач, тоді комбінація імені користувача та потрібної країни, звісно за успішної двофакторної автентифікації, буде вважатися дозволеним виключенням. Зрозуміло, що це не виключатиме можливих спроб зловмисника заволодіти легітимними даними для входу, проте зробить цю задачу ще складнішою. Врешті-решт, комплексний підхід до автентифікації, так само як і до аналізу подій у системі, здатний приносити плоди.

Повертаючись до проблеми внесення всіх можливих винятків щодо дозволених користувачам операцій, варто визнати, що їх також не завжди можна виділити, адже є і такі випадки, коли варіантів легітимних команд може бути так само багато, як хешів у зловмисній хакерській програмі. Але все рівно не потрібно нехтувати можливістю знизити за допомогою організаційних змін кількість оброблюваних загроз, адже одна така дозволена дія лише в один день може генерувати доволі багато спрацювань, а виключаючи з перегляду SIEM-ом певні відомі дії, ми потенційно знижуємо навантаження на систему захисту.

2.2 Методи пошуку ланцюжків false positives подій

Як було з’ясовано, доволі часто про регулярні та типові FP може бути відомо фахівцю з безпеки. За можливості всі правила та виключення до них, у системі, що прагне до високої ефективності виявлення вторгнень, вже налаштовані. Коли ж не вдається знайти виключення, яке б задовольняло вимогам політики безпеки, чи іншим міркуванням, фахівці можуть застосувати своє знання про інфраструктуру для пошуку серед загальної маси подій такі, що не просто повторюються раз за разом, але і є пов’язаними між собою певними логічними причинно-наслідковими зв’язками. Такі речі неодмінно помічаються коли довгий час маєш справу з однією системою.

Уявімо, що є мережевий адміністратор, робота якого полягає у контролі правильного функціонування мережі та допомозі у налаштуванні нового обладнання чи програми. Його типові дії, окрім логіну, неодмінно будуть включати у себе рутинні операції: віддалений доступ до комп'ютера, який потрібно налаштувати, перевірка актуального користувача, перевірка досяжності певної мережевої одиниці (ping), аналіз стану мережевих інтерфейсів, їх зміна і тому подібне. Всі ці операції по одинці можуть свідчити і про вторгнення, проте разом, на єдиній площині та за умови довіреної автентифікації, що максимально виключає спробу компрометації легітимного облікового запису, є звичайною активністю цього працівника. Для SIEM – це декілька потенційних FP, для аналітика, що працює зі спрацюваннями SIEM-у – зайва робота з аналізу типової нормальної поведінки. Нажаль, написання таких складних прав, що включають у себе багато операцій, які ще й можуть відбуватись у довільній формі, у різний (але робочий) час та не обов'язково усі по черзі та за один день, є неймовірним викликом. Алгоритми машинного навчання мають потенціал для слушного реагування і в таких випадках, але більш доцільно не сподіватися, що алгоритм успішно пройде навчання та виявить цей ланцюжок як легітимний, а змістити фокус з усього трафіку одразу на більш конкретні епізоди.

У математичній статистиці існує поняття частих епізодів (frequent episode): «Епізоди — це сукупність подій, які відбуваються відносно близько одна до одної в заданому частковому порядку», як описуються правилами виду: «Якщо певна комбінація подій відбувається протягом періоду часу, то інша комбінація подій відбудеться протягом періоду часу» [26]. Відповідно, аби стати частим, епізод має повторюватись деяку кількість разів, яка є різною для кожної системи. Епізоди один відносно інших можуть бути лінійними, паралельними чи комбінацією. Характеризуються епізоди частотою появи та вірогідністю настання, якщо виконано умови. Загалом очевидно, що подібна схема легко вписується у логіку роботи SIEM, адже агрегуючи та зберігаючи велику кількість логів, вони мають більше шансів знайти деякі послідовності подій, які часто зустрічаються разом.

На базі теорії про часті епізоди розроблена окрема математика, (у тому числі у роботі [27] вона представлена формалізовано), яка описує визначення того, що вважається епізодом, які правила мають виконуватися, аби певний ланцюжок чи сукупність подій відбувалась і класифікувалась як епізод, адже важливий не лише набір подій, а і їх порядок, причому якщо за визначенням епізоду потрібно буде дві конкретні події, аби настала наступна, то всі ці умови має бути виконано, інакше класифікація не відбудеться. Аналізуючи події, за певним алгоритмом спочатку виділяються часті епізоди, а потім відбувається виявлення правил, за якими ці епізоди генеруються. Теорія частих епізодів також оперує поняттям вірогідності настання деякої події, що є частиною частого епізоду, за умови, що попередні відбулися, що може бути дуже корисно у сфері кіберзахисту, адже захищеність системи також є хоча і дуже складним, але все-таки ймовірнісним процесом. Запровадження аналізу подій як ланцюжків активностей, що за певними правилами виявляються та складаються у епізоди, може бути відповіддю на те, як з більшою вірогідністю відрізнити зловмисний трафік, що імітує легітимний від справді такого, чи як не генерувати FP, коли користувач виконує набір дій, що звичайні системи виявлення вторгнень однозначно відмітили б як підозрілий, а система, здатна до виявлення частих епізодів – ні, саме через її здатність до навчання на таких складних шаблонах.

Думка про те, що подібність трафіка і є головною причиною появи великої кількості FP згадується також і у [25]. Зрозумілим чином, коли події мають складену природу, межа між дозволеним і ненормальним трафіком не є достатньо чіткою не те що для алгоритмів, а й подекуди і для досвідчених експертів. Щодо FN, думка [25] така: «відсутність сигнатур атаки в базі сигнатур є причиною випадків FN», що доволі логічно та очевидно, на противагу до рішення питання, адже мова про сигнатурне виявлення не може йти, коли ми маємо справу з APT атаками чи zero-day. Проте, повертаючись до FP, зрозуміло, що певним чином впровадження складного алгоритму з використанням машинного навчання, що б навчався на основі частих епізодів, є доволі перспективним напрямком та може бути досліджене в наступних роботах. У

раніше згаданій роботі [27] окрім теоретичного обґрунтування теорії частих епізодів надано також алгоритм їх виявлення на псевдокоді, який може слугувати базою для покращеної та універсальної методики.

Таке навчання окрім дбайливого налаштування потребувало б і великого якісного набору даних, адже від цього напряму б залежала його ефективність. Як часто буває у сфері кібербезпеки, важливим є не тільки скільки даних ми збираємо, а наскільки повно вони описують поведінку системи, чому буде присвячено пункт 2.5 даної роботи.

2.3 Методи збільшення даних та Data Augmentation

Необхідність збільшення обсягу вибірки (даних, що аналізуються) для зменшення похибки першого роду прямо витикає з теореми Чебишова (або закону великих чисел) [28, ст.141, 29, ст.137], а саме зі збільшенням числа спостережень різні випадкові відхилення випадкових величин нівелюється, отже з ймовірністю, що прямує до 1 арифметична середня результатів спостережень буде довільно мало відрізнятись від арифметичної середньої признаку, що досліджується, в усієї статистичної генеральної сукупності.

Маємо:

Теорема Чебишова. *Нехай* $X_1, \dots X_n$ *– незалежні однаково розподілені випадкові величини, яка мають математичне очікування та дисперсію. Позначимо загальне значення математичного очікування як* M *. Тоді для кожного* $\varepsilon > 0$ *за умови* $n \to \infty$ *ймовірність*

$$P\left(\left|\frac{X_1+\dots+X_n}{n} - M\right| < \varepsilon\right) \to 1.$$

Навіть більше, ми можемо оцінити розмір вибірки n з центральної граничної теореми, яка стверджує, що розподіл випадкової величини $\sqrt{n}(\theta_n - \theta)$ (де θ_n – деяка характеристика випадкової величини, отримана за вибіркою розміром n, а θ – її теоретичний аналог) має асимптотичне нормальний розподіл з деякими параметрами (a, σ^2). Звідти маємо чітку постановку задачі оптимізації

для визначення необхідного обсягу даних спостережень при певних значеннях false/positive.

Вплив збільшення кількості різних типів даних, що спостерігаються, на зниження рівня false/positive вимагає більшого пояснення. По-перше, таке збільшення дозволяє більш чітко визначити теоретичний закон розподілу випадкових величин, що спостерігаються. По-друге, як правило, це дозволяє в певних випадках переходити від статистичних методів виявлення вторгнень (див. Рисунок 1.1 Класифікація методів виявлення вторгнень, заснованих на аналізі аномалій [2]) до детермінованих, що в свою чергу, різко знижує рівень false/positive. Простим прикладом може бути додатковий аналіз розташування суб'єктів аналізу (IP-адрес) при статистичній границі числа хибних спроб авторизації. Цей факт ми будемо використовувати в наших методах далі.

У машинному навчанні для ситуацій, коли розмір датасету не є достатнім, аби виключити можливість перенавчання моделі, а також підвисити її точність прогнозів, використовують метод під назвою Data Augmentation, що можна перекласти як нарощування даних для навчання. Суть методу полягає у штучному збільшенні датасету шляхом генерування додаткових даних на базі існуючих, проте у зміненому вигляді. І хоча такий підхід більш поширений для випадків з розпізнаванням мови та у медицині, його можна загальним чином застосувати до будь-якої задачі бінарної класифікації, як от з визначенням вторгнень.

Робота [30] підкреслює, що для збільшення ефективності виявлення певного класу (тобто або вторгнення, або ж легітимної активності), потрібно проводити нарощування даних саме за цим класом. У медицині, зрозумілим чином, важливіше передбачити хворобу, аніж визнати її відсутність, а з точки зору фахівця з безпеки аналогічним чином потрібно збільшити кількість атак у наборі даних для навчання. Проте за такого підходу, кількість FP навпаки зросте. Отже, якщо наша ціль – оптимізувати FPR, потрібно робити протилежні дії – згенерувати ще більше прикладів легітимного трафіку, серед якого буде і нетиповий. У згаданій вище роботі для зменшення кількості FN було змінено

мітки приналежності до класу хвороби у деякої кількості FP, скориставшись тим фактом, що часто для моделі FP та FN може бути важко відрізнити один від одного, тим самим отримавши не тільки меншу кількість FN, але і піднявши загальну ефективність. Використавши протилежний підхід до системних подій, теоретично можливим є аналогічне зменшення кількості FP, що може бути темою для наступних досліджень.

2.4 Пошук першопричин-джерел більшості false positives

Як уже було згадано на початку другого розділу, велика кількість FP спрацювань часто не означає їх такої самої різноманітності, як же притаманно FN, і якщо відкинути організаційні та конфігураційні причини, яким було присвячено пункт 2.1, все рівно можна знайти деякі їх першопричини. Дослідження такого плану у загальному випадку має назву root causes analysis, а про його застосування до проблеми хибних спрацювань відомо з 2003 року, а саме з роботи [31], де окрім термінології, було також запропоновано низку практичних підходів.

Праця [31] розповідає яким чином можна застосувати пошук неочевидних кореляційних зв’язків Data Mining, а саме його підвид alarm clustering для завдання пошуку серед загальної маси подій так званих першопричин (root causes), адже «кілька десятків першопричин загалом становлять понад 90% спрацювань у журналі тривог». Зрозумілим чином, якщо їх не усунути, спрацювання будуть продовжувати з’являтись. Для вирішення задачі alarm clustering відбувається майнінг усіх логів, виявляються потрібні атрибути, що будуть характеризувати спрацювання, такі як source ip, destination ip, тип спрацювання та звісно мітка часу. Окрім конкретних атрибутів, можуть бути більш корисними і узагальнені («узагальнений сигнал тривоги – це стислий і зрозумілий людині шаблон, якому сигнал тривоги повинен відповідати, щоб належати до відповідного кластера» [31, ст.16]), адже завжди краще внести у правило не усі можливі конкретні значення, а знайти загальну ідею, що їх

об’єднує. Так з ір адресами можна обрати певний проміжок адрес та присвоїти їм відповідну мітку, як наприклад легко відрізнити приватну адресу від публічної, так само і деякий набір адрес може вважатися таким, що є нормальних для веб-серверів, або ж можна виділити перелік непривілейованих. Ба більше: навіть мітку часу можна представити словом – робочий час чи позаробочий. Для звичайного SIEM побудова правила на кшалт “підключення до привілейованих портів з приватних адрес дозволено лише у робочий час” є чимось фантастичним, проте приблизно так виглядають політики безпеки. Але виділивши кластери спрацювань та описавши їх узагальненими атрибутами, фахівець значно спростить собі пошук першопричини або причин, адже нажаль їх може бути і декілька, що ускладнює пошук.

Результат alarm clustering за ідеальних обставин має повертати чітке розбиття спрацювань на кластери і не допускати ситуації, коли одне з них належить декільком типам. Алгоритм шукає лінійні, послідовні, періодичні шаблони у наборі даних, які вказують на певний тип спрацювань, а отже і визначену першопричину.

Правила фільтрації, що будуть відсіювати спрацювання з відомими легітимними першоджерелами, як наголошено у згаданій вище роботі, мають бути конкретними, аби випадково не пропустити true positive. Не варто забувати, що коли мова йде про пошук першоджерел деякої групи спрацювань та на основі цього створюється правило, в залежності від динамічності системи пройде деякий час і правило перестане бути актуальним, адже причина подій може зникнути чи змінити вигляд, а саме правило залишиться і буде не лише навантажувати систему зайвий раз, але і можливо пропускати вже не дозволений трафік. Тому перегляд правил спрацювань, як і інших питань захисту має бути регулярним.

2.5 Використання комплексних показників для виявлення вторгнень

2.5.1 Загальноприйняті показники

Ідея комплексного підходу до виявлення вторгнень має значні переваги над звичним сигнатурним чи аномальним методами, проте і у “загального” цілісного підходу немає чітко прописаних вимог та алгоритмів. Дуже багато залежить від конкретної інфраструктури, а отже фахівці вимушені підбирати влучний спосіб знаходити небажані події не лише з боку вибору SIEM, алгоритму виявлення чи взагалі наявних ресурсів або моделі загроз, а і з боку того, які показники збирати, аби виявлення відбувалось найбільш ефективним чином. Від якості зібраних логів напряму залежить і показники системи захисту. Не доцільно збирати просто всі можливі логи, чи навпаки – обмежуватись лише критичними, бо якщо на меті покращення захисту та реагування, вибір даних для аналізу може грати роль, не меншу за інші згадані вибори.

Кожен SIEM має свій набір ключових полів у подіях, причому для різних їх видів і поля будуть різними, проте деякі речі все рівно є загальноприйнятими. Це стосується і всіх літературних джерел, приведених вище, автори яких у своїх дослідженнях обирати певних зручний набір показників, серед яких майже незмінно були: source&destination ip address, source&destination port, мережевий протокол, мітка часу, тип спрацювання, контекст події, командний рядок і т.п. Проте велика кількість показників не лише ускладнює аналіз та наприклад ті самі згадані процеси кластеризації чи класифікації, адже пошук кореляційних зв’язків між купою параметрів вже не може бути таким само ефективним, але і роздуває бази логів до неймовірних розмірів та сповільнює всі операції над ними. Варто намагатися зберегти баланс між повним розумінням того, що відбувається у системі та надмірністю.

Отже, у пошуках оптимальної повної та достатньої кількості параметрів для аналізу, дослідники часто звертаються до концепції Situation Awareness, яку можна розуміти як *обізнаність щодо стану системи*. Прийнятими етапами цієї

обізнаності є сприйняття, розуміння та проекція. У праці [32] ціль автора була у тому, щоб «створити нову техніку для мінімізації хибних спрацьовувань за допомогою багатообіцяючих нових досліджень ELM (Extreme learning machine) як класифікатора, у поєднанні з HMM (hidden Markov model), у системі усвідомлення ситуації». Перший етап виконувався засобами ELM, а другий – HMM, що дозволило дивитися не тільки на кожну окрему подію поодинці, але і знаходити взаємозв'язок між ними, що дуже допомагає підняти рівень розуміння ситуації, як вже не раз було згадано у цій роботі. Проекція ж реалізується за допомогою схеми одностайного голосування за результатами роботи перших двох етапів. Таким чином, у наведеному процесі система здатна сама приймати рішення про природу події і виконувати певні дії в залежності від рішення. Прийняття рішення на другому етапі залежить від вірогідностей переходів між станами у Марковому ланцюгу, а отже чим точніше вони будуть визначені, що залежить від рівня обізнаності щодо стану системи, тип точнішим буде прогноз природи події.

Метрики часу грають не останню роль у питанні відрізнення легітимного трафіку від зловмисного: будь-яка типова чи ні подія, що відбувається у нетиповий час є автоматично підозрілою та має бути окремо досліджена фахівцем з безпеки. У кожній компанії є чітко визначені рамки робочого дня, тому активність поза ними викликає занепокоєння. Окрім того, що це може бути просто деякий адміністратор, що вирішив затриматись на роботі і виконати свої задачі, це може і яскраво сигналізувати про вторгнення. Однозначно, що зловмисники можуть діяти і у робочий час, проте не варто ігнорувати доступний та легкий спосіб виявити однозначно недозволені операції серед просто підозрілих. **Таким чином для IDS/IPS чи SIEM має працювати така логіка: "підозріла подія у підозрілий час має рівень більш критичний за таку саму подію у нормальний час".**

Для зменшення кількості false positives можливо також враховувати інші часові показники, окрім таких, що є однозначно підозрілими, як було згадано вище (робота у вихідні, вночі), у тому числі можливим є розгляд таких часових

метрик, як типові логічні рамки для деякої події: «врахування часових характеристик окремої доби, днів тижня, числа місяця, та дня року… під час обідньої перерви на підприємстві, активність користувачів стає мінімальною» [10]. Тобто у святкові дні, чи дні перед ними звична активність може відхилятися від норми, причому у обох напрямках: працівники або ж будуть більше відпочивати, чи навпаки енергійно завершувати потрібні справи.

Хоча більшість робіт за темою виявлення вторгнень і написані на прикладі різних IDS/IPS, SIEM має над ними одну значну перевагу, яка дуже допомагає у процесі більш ґрунтовного аналізу подій, а саме можливість досліджувати активність, яка відбувалась у минулому, що особливо важливо для APT та zero-day атак, а також розтягнутих у часі атак, через їх здатність маскуватися серед легітимного трафіку, а також «повільно вилучати дані протягом тривалого періоду часу, щоб уникнути виявлення та використовувати шифрування, яке часто перешкоджає IDS, що покладаються на сигнатури» [32, ст.60]. Там, де IDS/IPS аналізують трафік у моменті, SIEM бачить картину у цілому, а значить ймовірність виявити складну атаку зростає. Навіть з простими подіями, що повторюються, SIEM має всі шанси це виявити та на основі цього зробити висновок про їх вірогідну легітимну природу, адже «Очікується, що помилкові спрацьовування від звичайного трафіку кілька разів викликатимуть одні й ті самі сповіщення» [26, ст.37]. Відсіявши декілька груп повторюваних сповіщень, можна отримати великий вплив на ефективність виявлення.

2.5.2 Метрики, що пропонуються у роботі

Щоб досягнути повноти показників та бажаної ефективності виявлення вторгнень, потрібно в ідеалі винайти загальний метод з універсальними показниками, який буде працювати однаково добре у будь-якій інфраструктурі з різними налаштуваннями та правилами безпеки. З усіх цих вимог найреалістичнішою є потреба у єдиній метриці, що описуватиме будь-яку мережеву подію достатнім чином. Оскільки системи IDS/IPS та SIEM мають і

різний вид обробки сирих логів, різні ключові поля, а джерела, з яких надходять події взагалі дуже різноманітні, не можна у цьому питанні опиратися на будь-що специфічне, треба знайти те, без чого жодна мережева подія не може бути проаналізована, в незалежності від її природи. Найперше, що приходить на думку: час події або ж часова мітка (timestamp) – без неї не можна уявити логи. Але одного того, що ми знаємо коли відбулась подія звісно мало. Бажано ще розуміти звідки вона прийшла, і мова не про засіб мережевого зв'язку чи комп'ютер, а про адресу, звідки її було "відправлено", тобто source IP адресу. Ці два показники хоча і здаються простими, але можуть багато чого розповісти про природу події як самі по собі, так і особливо у комбінації, а саме:

1. Подія з нетиповою source IP адресою може з деякою вірогідністю бути зловмисною
2. Подія, що трапилась у нетиповий час з деякою вірогідністю може свідчити про її не легітимне походження
3. Подія, що трапилась у нетиповий час та прийшла з нетипової адреси з більшою вірогідністю є вторгненням

Оскільки аби автоматизувати рішення SIEM чи IDS/IPS про природу події на базі статистичних моделей, потрібно визначитись з ймовірністю їх належності певному класу, треба також розуміти, що в залежності від їх комбінацій, і вірогідність класифікації події як вторгнення має бути різною. Наприклад, якщо подія трапилась у не робочий час, то з ймовірністю 0.3 вона є вторгненням, а якщо адреса, з якої прийшла подія – нова, то шанс вже 0.5, а коли такі події трапляються одночасно – 0.7. Ці значення звісно будуть різні для кожної системи та в залежності від способу їх отримання (експертний, автоматизований). Але запровадження контролю за цими показниками потенційно має покращати ситуацію з кількістю false positives, чому і буде присвячено третій розділ.

Висновки до розділу 2

Фахівці з безпеки постійно знаходяться у пошуку нових способів підвищення ефективності роботи системи виявлення вторгнень. У другому розділі даної роботи було показано, як цього певною мірою можна досягти за допомогою різних методів: організаційних, статистичних, кластеризації, пошуку першопричин (root causes), частих епізодів (frequent episode). Жоден з варіантів вирішення питання оптимізації досі не є однозначно ефективнішим за інші чи універсальним: усі вони мають потенціал у комплексі давати значно вищі результати, ніж поодинці. Було зроблено висновок, що повнота логів, що збираються, стала б на нагоді за будь-якого з цих методів, а гарна обізнаність щодо стану системи допомагає в питанні оцінки їх результатів.

Було показано, що серед фахівців та розробників систем виявлення відсутня єдність щодо ключових показників, а тому запропоновано єдині метрики показників, контролю за якими має бути достатньо, у поєднанні з іншими доступними засобами, для зменшення рівню FP спрацювань серед загальної маси мережевих подій, а саме показники часу (timestamp) та походження (source IP адресою).

3 ВПРОВАДЖЕННЯ МЕТОДІВ, ЗАСНОВАНИХ НА КОМПЛЕКСНОМУ ВИКОРИСТАННІ ДАНИХ ПРО СИСТЕМУ

3.1 Вибір тестових даних та побудова лабораторії

3.1.1 Проблема пошуку тестових даних

Аби виконати адекватну реальності перевірку ефективності будь-яких оптимізації, потрібен набір даних, тобто датасет, який буде достатньою мірою відображати реальний трафік з атаками. Нажаль, у відкритому доступі майже неможливо знайти такий, що відповідав би усім критеріям, а саме:

- Об’єм, достатній для якісного навчання моделі
- Збалансованість не тільки легітимного та шкідливого трафіку, але і типів вторгнень, що у ньому наявні
- Актуальність загроз, методів захисту, мережевих комунікацій
- Зручні ключові поля та повнота зібраної інформації

Доступні широкому колу дослідників датасети, наприклад KDD98, KDDCUP99, DARPA 1999, NSLKDD та інші, якраз не відповідають вимогам, наведеним вище. Вони застарілі, а отже не показують сучасні приклади подій, а тим більше атак; їх розмір може бути недостатнім; кількість типів атак та їх збалансованість залишає бажати кращого; інформації може бути недостатньо або вона може бути погано придатною для обробки потрібними способами. До того ж аби помістити логи у обрані SIEM знадобився б складний процес парсингу, який до того ж був би не завжди можливим, адже датасети, що використовуються для машинного навчання вже були перероблені з певного набору подій.

Застосувати для дослідження логи з будь-яких реальних систем було б ідеальним рішенням, проте політика безпеки не дозволяє ані отримувати, ані розповсюджувати приватні дані. Тому хоча дослідники все рівно вимушені використовувати такі датасети, які є, частіше все рівно обирають створити власний [26, ст.60], у деякій тестовій мережі. Не виключенням є і ця робота.

3.1.2 Структура побудованого лабораторного середовища

Для проведення усіх дослідів та експериментів було обрано використати платформу для віртуалізації VMware Workstation 17 Pro, де у повністю контрольованому тестовому середовищі було розгорнуто такі віртуальні машини:

1. Ubuntu 22.04.3, яка виступає у ролі сервера, де будуть розміщуватись база даних з логами та всі три компоненти SIEM Wazuh (indexer + dashboard + manager) та сервер Splunk (далі – сервер)
2. Ubuntu 22.04.3, на якій встановлено агенти Wazuh та Splunk, у ролі комп'ютера адміністратора (далі – Ubuntu WS)
3. Windows 10 Home, на якій встановлено агенти Wazuh та Splunk, у ролі звичайної робочої станції (далі – Windows WS)
4. Kali 2022.2, яка буде джерелом атаки, тобто комп'ютер зловмисника, агенти Wazuh та Splunk на даній машині відсутні (далі – зловмисник)

Загалом тестова мережа зображена на Рисунку 3.1, де можна також побачити які IP адреси мають кожна з машин та іншу інформацію у візуальному вигляді, що була наведена вище:

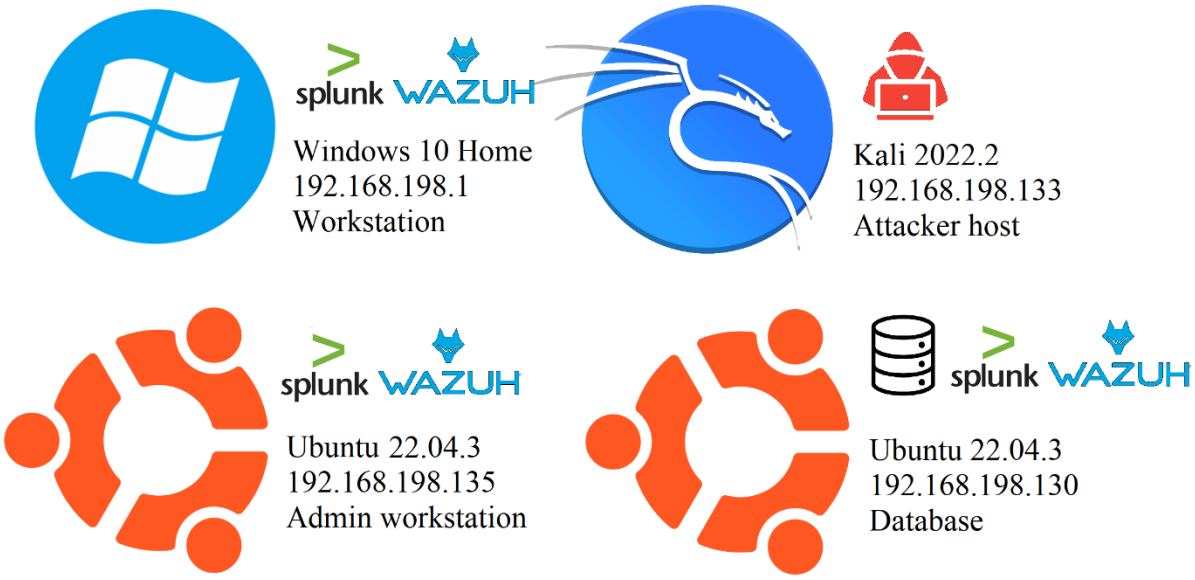


Рисунок 3.1 – Вигляд тестового середовища та параметри його компонент

Для досягнення мети дослідження дані про визначені типи подій з Ubuntu WS та Windows WS постійно збираються встановленими агентами двох SIEM:

Wazuh та Splunk, передаються ними на сервер, де зберігаються та аналізуються, а з комп'ютера зловмисника будуть надходити спроби атак.

3.2 Огляд SIEM Splunk та Wazuh

У даній роботи у якості SIEM обрані Wazuh та Splunk, вибір яких зумовлено низкою факторів: їх наявність у відкритому безкоштовному доступі (обидва, але Splunk з обмеженнями на об'єм трафіку за день), популярність та активні форуми з підтримки (обидва), здатність виконувати усі потрібні операції (обидва, проте інтерфейси дуже розрізняються), деякі цікаві особливості, про які буде згадано далі. Різноманіття SIEM окрім обраних є великим, проте головною перепоною логічним чином є їх відсутність у вільному доступі. Аби перейти до практичного використання, потрібно коротко навести основні відомості про кожен з SIEM.

Wazuh – це open source SIEM платформа з підтримкою технології XDR (Extended detection and response), яка з'явилась у 2015 році і досі завойовує популярність серед експертів з безпеки. За даними розробників [33], їх платформа використовується на більше ніж 15 мільйонах комп'ютерів, і ця цифра постійно зростає. Таку поширеність – найбільшу серед усіх open source рішень – Wazuh здобув завдяки широким можливостям, а саме: аналітика безпеки, виявлення вторгнень, аналіз логів, моніторинг цілісності файлів, виявлення вразливостей, оцінка конфігурацій та відповідності вимогам, відповідь на інциденти, хмарна безпека – тобто платформа позиціонує себе як єдине рішення, здатне покрити усі потреби інфраструктури у сфері інформаційної безпеки. Wazuh підтримує різні варіанти встановлення: як на одній ноді, так і у розподіленому вигляді. Оскільки тестова середа у даній роботі не є надто складною, для зручності було обрано процес встановлення усіх трьох компонентів платформи на одному комп'ютері – сервері. Три згадані частини Wazuh – це indexer (пошуковий двигун, який індексує та зберігає сповіщення, що генеруються після аналізу логів з агентів), dashboard (веб інтерфейс для роботи з

зібраними даними у браузері) та manager (сервер, що управляє агентами та аналізує логи, пропускаючи їх через правила виявлення). Разом вони забезпечують роботу платформи та зручне її використання для спеціаліста.

Процес встановлення компонентів на сервер не є легким навіть за спрощеного виду, що є однозначним мінусом платформи, порівняно з іншими SIEM, у тому числі зі Splunk. Wazuh потребує ручного виконання багатьох операцій, які частіше за все подібні системи проводять автоматично, проте це також дає спеціалісту можливість повнішого контролю та конфігурації. Зате агенти, які підходять для більшості існуючих операційних систем, не потребують особливих зусиль для розгортання: декілька команд і комп'ютер з'являться на екрані моніторингу веб інтерфейса на сервері, а сирі логи з нього відображаються (у рамках даної роботи) у веб консолі GrayLog – ще одному важливому компоненті, який по суті може існувати як окреме рішення для управління логами або ж працювати у комбінації з SIEM, у нашому випадку – з Wazuh.

Splunk Enterprise Security – SIEM з закритим кодом, який надає класичні послуги для даного типу систем, історія якої розпочалась ще у 2003 році. Splunk забезпечує аналіз великих об'ємів логів у режимі реального часу, працює з широким спектром типів логів та здатен приводити їх до спільного формату, з яким можна працювати спеціалісту, має вбудований пошуковий двигун з дуже гнучкими параметрами та шаблонами пошуку, дає потужні можливісті для візуалізації даних та розслідування інцидентів. Він підтримує також бізнес аналітику за рахунок гнучкості вхідних даних та пошуку.

Процес встановлення як самого серверу Splunk, так і його агентів, дуже простий та майже не потребує втручання фахівця, до дозволяє почати роботу з ним дуже швидко та перейти безпосередньо до створення правил виявлення вторгнень, візуалізації результатів та глибокого аналізу подій.

Під час роботи також було виділено основні сильні та слабкі сторони двох SIEM, що використовувалися. Таким чином критичний аналіз Splunk наведений у Таблиці 3.1:

Таблиця 3.1 – Переваги та недоліки Splunk

Переваги	Недоліки
Збір великих об’ємів логів з безлічі різних джерел	Безкоштовне використання з обмеженою кількістю даних (до 500Мб на день)
Аналіз історичних логів та у режимі реального часу	Важкість налаштування
Гнучкість пошуку (без жорстких шаблонів)	Splunk – не open source проект
Потужна візуалізація даних	У безкоштовній версії обмежено функціонал
Легке масштабування	

Аналогічні порівняння для Wazuh представлені у Таблиці 3.2:

Таблиця 3.2 – Переваги та недоліки Wazuh

Переваги	Недоліки
Безкоштовний open source проект	Важкий процес встановлення та налаштування правил, аби не створювалося забагато FP
Гнучкі можливості для створення правил виявлення	Потребує багато ресурсів для роботи
Потужні вбудовані модулі	Бракує підтримки від розробників
Можливість інтеграції з іншими засобами захисту	Парсинг подій доволі важкий
Великий асортимент дефолтних правил та функцій	Масштабованість часто призводить до втрати у продуктивності

3.3 Симуляція атаки та демонстрація виявлення

3.3.1 Опис сценарію атаки

За ідеєю експерименту, зловмисник намагається здійснити віддалений мережевий доступ засобами SSH до Ubuntu WS та Windows WS, це можна зробити за допомогою простої аналогічної команди для обох комп’ютерів-жертв, за умови, що зловмисник вже деяким чином отримав знання про їх IP адреси та присутні облікові записи, потім спробував вгадати пароль, проте безуспішно, як це видно на Рисунку 3.2:

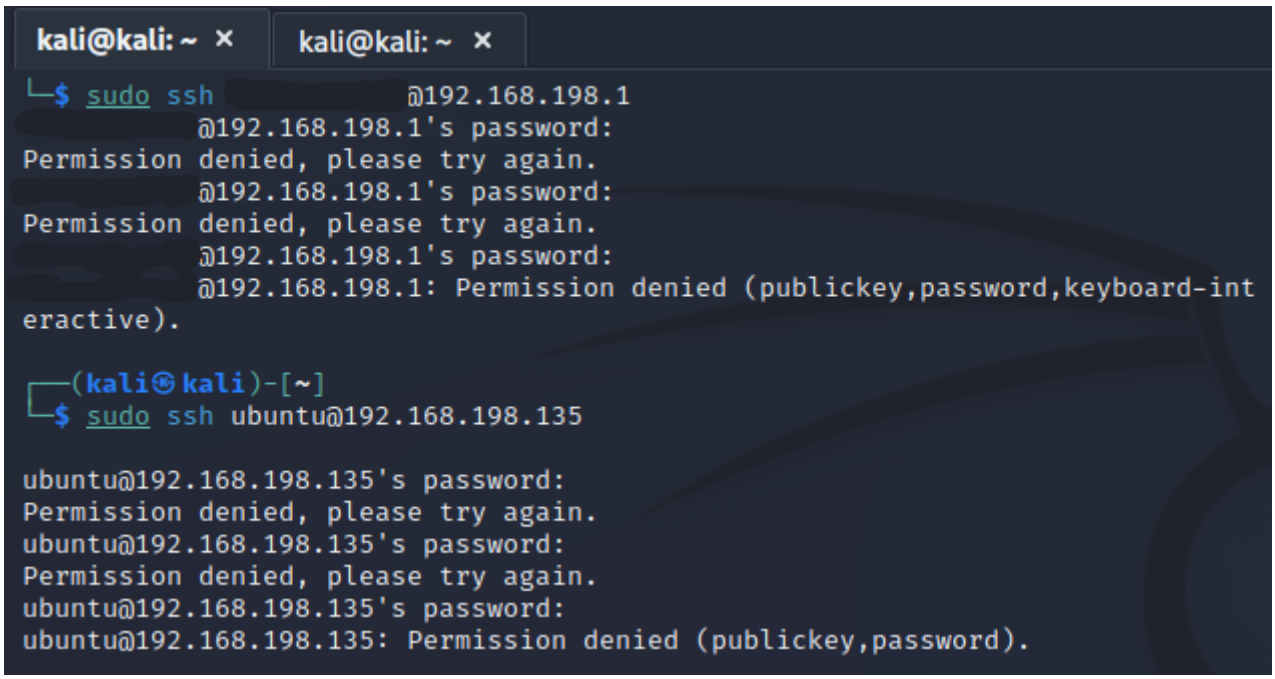


Рисунок 3.2 – Типовий приклад неуспішних спроб віддаленого входу

Відповідно, на стороні зловмисника він отримує помилку про неправильний пароль, а отже продовжує певними засобами подібні спроби, можливо за допомогою автоматизованих програм, проте на стороні фахівця з безпеки це все рівно виглядає як неуспішна спроба віддаленого підключення до комп'ютера з використанням існуючого облікового запису, але невірним паролем. Аби прийняти рішення про природу події, потрібен контекст: звідки і коли було підключення, скільки разів відбувалась подія, за який проміжок часу, чи були успішні входи врешті-решт. Це буде продемонстровано далі.

3.3.2 Виявлення підозрілої активності віддаленого входу за допомогою SSH засобами Wazuh

Перед початком безпосереднього виконання завдань роботи потрібно продемонструвати як виглядає типова робота з обраними SIEM. Розпочнемо з Wazuh, а саме з вигляду основної панелі, де показуються усі комп'ютери, на яких встановлено агенти, час їх останнього підключення, стан та загальна інформація, як можна побачити на Рисунку 3.3:

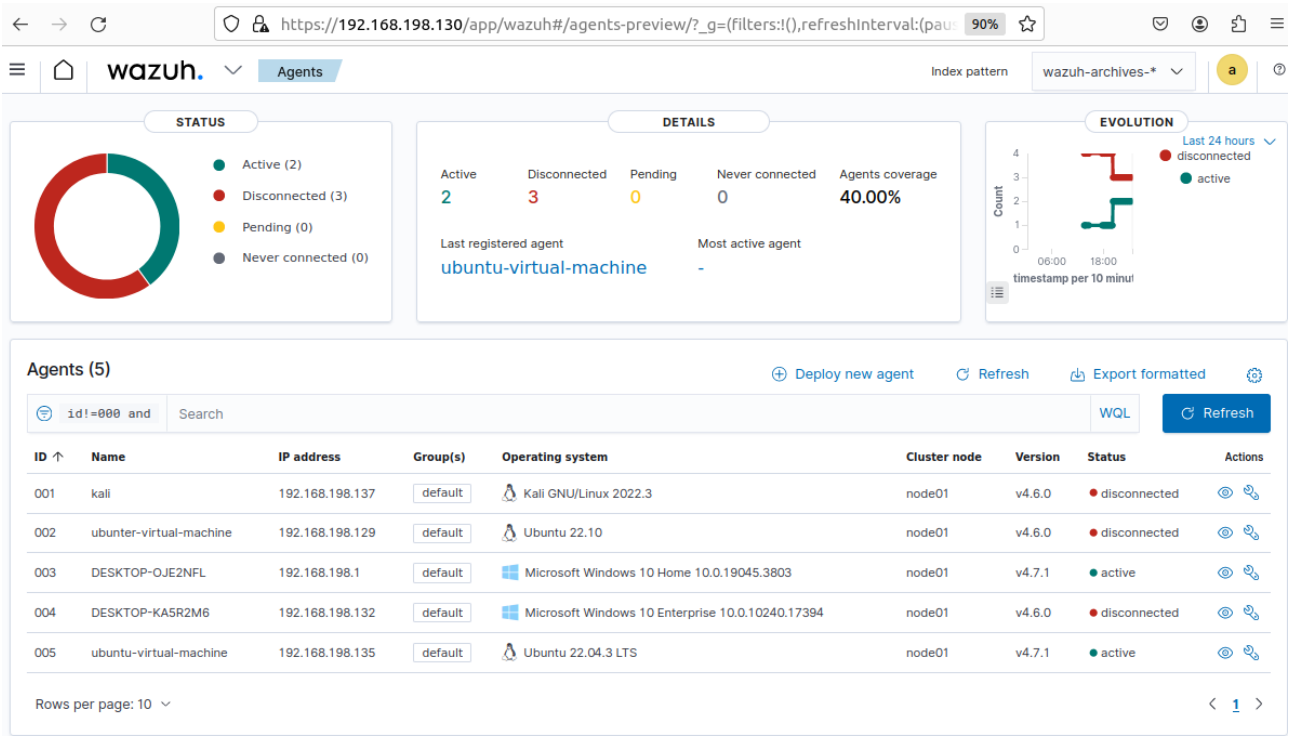


Рисунок 3.3 – Вигляд основної панелі агентів Wazuh

Усі агенти мають постійно надсилати логи на сервер, для цього вони звертаються до нього за IP адресою та портом, який можна побачити на Рисунку 3.4, видно що менеджером є хост, на якому встановлено сервер, а саме olga-virtual-machine:

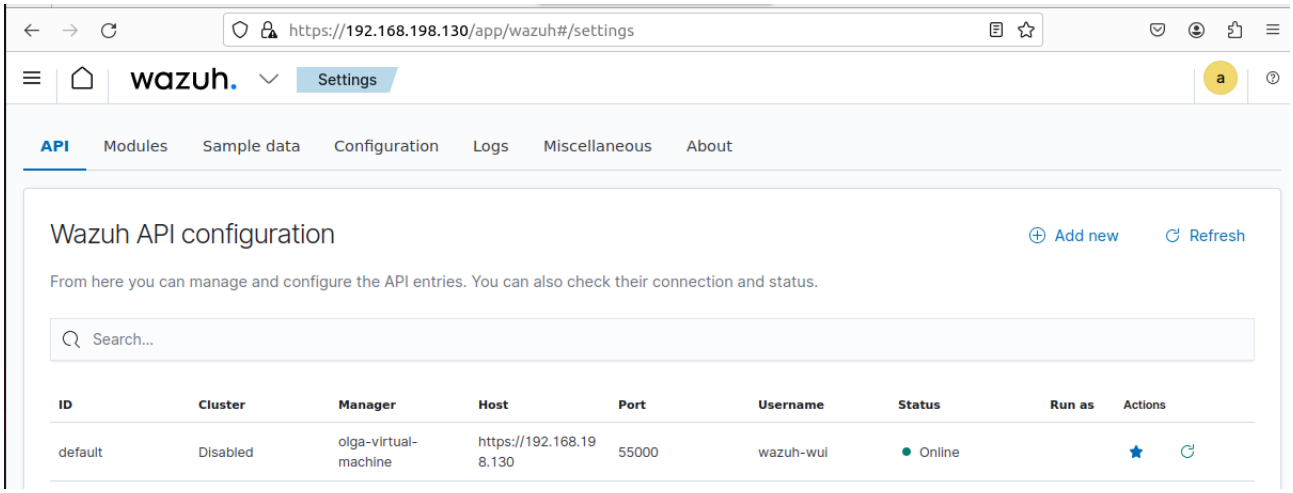


Рисунок 3.4 – Вигляд панелі з даними про веб консоль Wazuh dashboard

Для того, аби Graylog працював коректно у зв’язку з Wazuh, між ними має існувати канал комунікації, мають бути налаштовані сертифікати для безпечного обміну даними, тоді у веб консолі Graylog можна бути побачити канал вхідних даних, як видно на Рисунку 3.5:

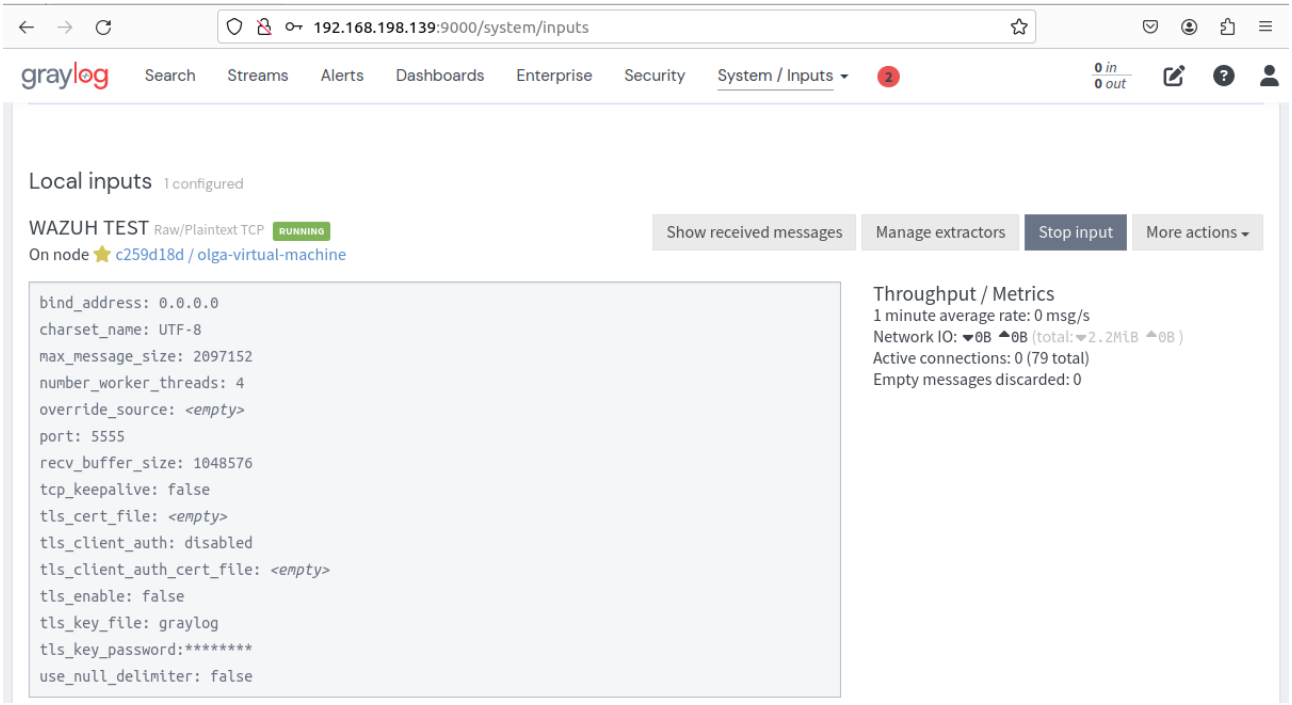


Рисунок 3.5 – Вид вхідного каналу даних для Graylog

Основний плюс Wazuh, який активно використовується у даній роботі це широка база готових правил виявлення за замовчуванням. Треба взагалі відмітити, що індексуються у базу Wazuh , та відповідно потім пересилаються до Graylog, лише ті події, що описані певним правилами, що знаходяться у директорії /var/ossec/ruleset/rules на системі, де встановлено сервер Wazuh. Цей факт ніяким чином не впливає на ефективність чи повноту роботи Wazuh, адже його правила не тільки покривають усі можливі стандартін події на популярних операційних системах, але і дуже легко піддаються зміні чи доповленню. Неомінною перевагою є і те, що всі вони інтегровані з базою даних MITRE ATT&CK, тому окрім даних про подію, що призвела до спрацювання правила, є інформація щодо того, якою частиною ланцюжка атаки це може бути. Для Windows машини також буде присутній код події, як це видно на Рисунку 3.6, а для Linux інформації буде менше, проте кожне правило всередині Wazuh також має свій код, що допомагає з його ідентифікацією:

Рисунок 3.6 – Вигляд дефолтного правила виявлення неуспішної спроби віддаленого входу за SSH для Windows

Іноді все ж таки готових правил не вистачає і потрібно створювати власні, як це сталось у рамках даної роботи, коли дійшло до проблеми відсутності у стандартному полі потрібного для ґрунтовного аналізу події ключового поля, для чого окрім правила, наведеного на Рисунку 3.7, на Windows машині довелося встановити Sysmon, тобто системний монітор для цієї операційно системи, що дає ще повніший контроль за подіями у системі, дає можливість вносити винятки до того, що потрібно логувати, а головне легко може впоратися з підозрілою мережевою активністю, у нашому випадку засобами SSH:

Рисунок 3.7 – Доповнене правило для виявлення неуспішних входів у Windows

Нажаль, Graylog потребує доволі великої кількості додаткових операцій, аби можна було від отримання події, перейти до її аналізу. Знайти у ручному порядку серед загальної маси потрібно може бути не так і складно, проте автоматизація цієї операції, на відміну від, як ми побачимо згодом, Splunk, є багатоетапною задачею. Для початку відбувається парсинг за набором ключових полей, потім потрібно створити потік даних (stream), в який будуть потрапляти усі події неуспішного віддаленого входу засобами SSH, тоді конвеєр за

специфічними правилами (тими, що засновані на виявленні аномального походження чи часу події, чи разом) вже з усіх будуть обирати найбільш підозрілі, за інструкціями, які йому вказані. Отже, для початку ми маємо справу з сирим логом, а після парсингу можемо легше відрізняти одне поле від іншого, а отже провести аналіз щодо того які наслідки у журналі викликали дії зловмисника, стає простіше. Саме на базі вивчення структури логу неуспішного входу, звісно створюються і правила виявлення, а сам вигляд події для Windows можна побачити на Рисунку 3.8, а для Linux на Рисунку 3.9:

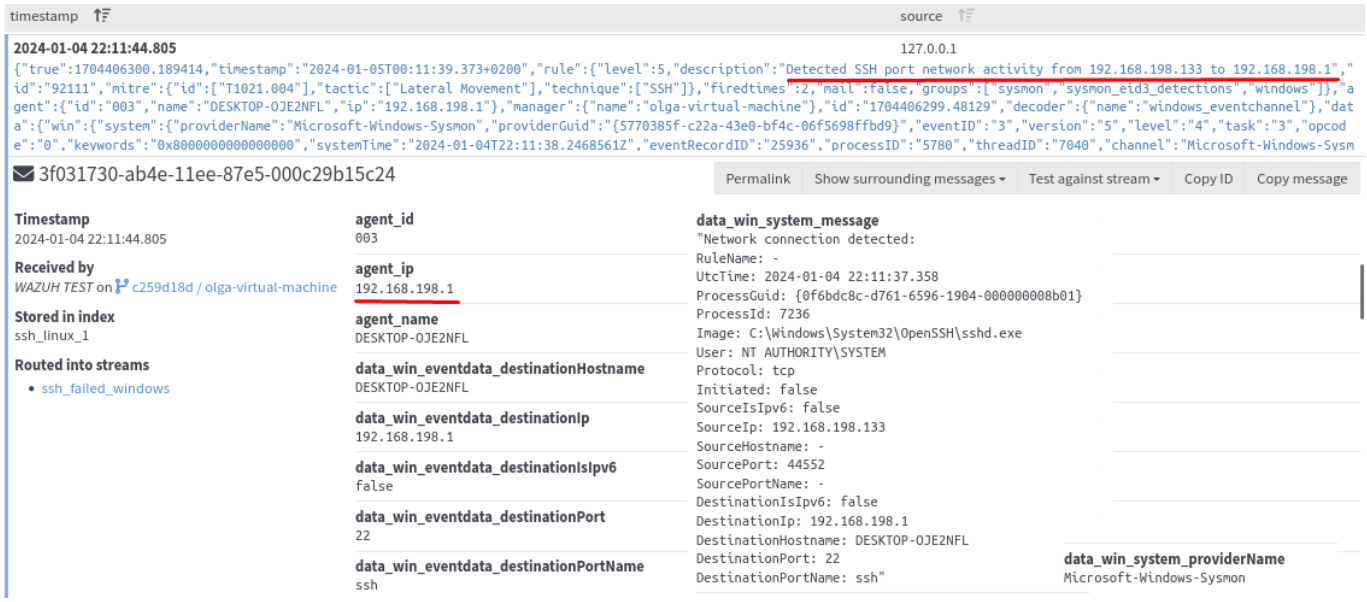


Рисунок 3.8 – Лог події неуспішного віддаленого входу через SSH у Windows

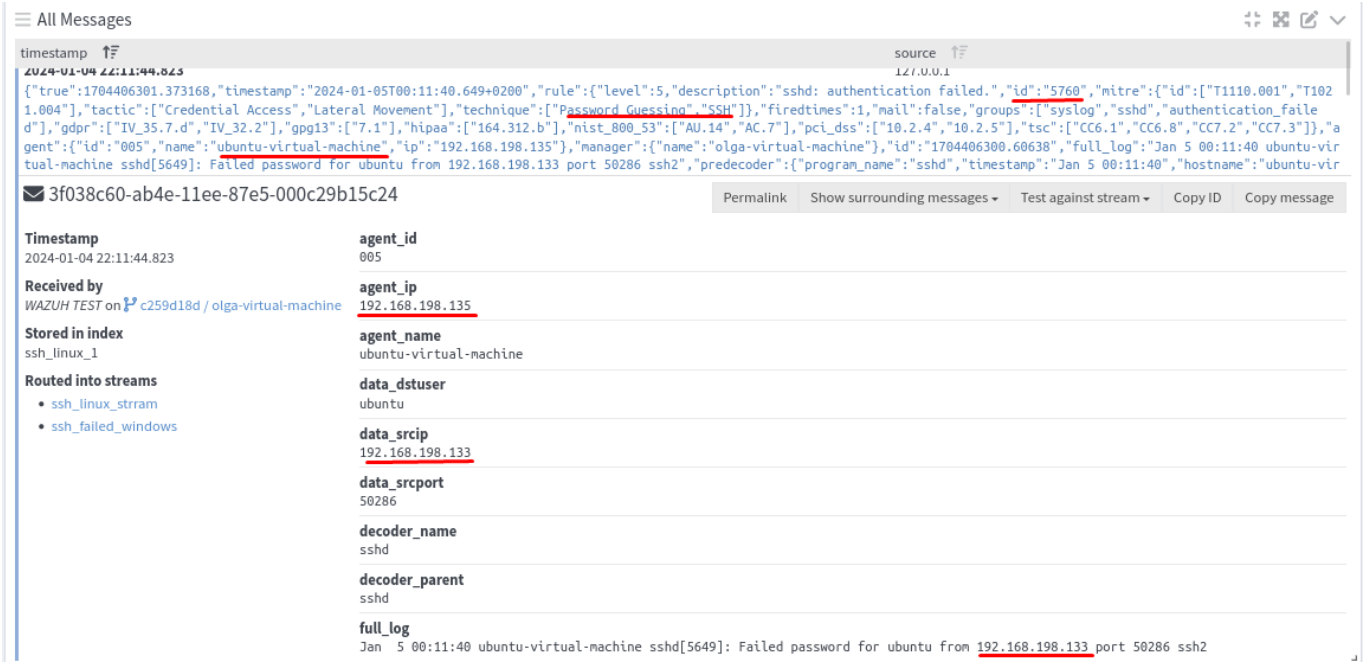


Рисунок 3.9 – Лог події неуспішного віддаленого входу через SSH у Linux

Щодо того, які правила для конвеєрів було визначено, то оскільки нам потрібно приділити більшу увагу аномальним подіям, потрібно кожен неуспішний вхід перевірити за двома критеріями: чи є час події таким, що не входить до загальноприйнятих робочих часів (до 6 ранку, після 18 вечора, у вихідні) або чи IP адреса є нам невідомою. Отже, правила, визначені у конвеєрі мають відповідні до цілі назви: ssh_failed_{windows\linux}_{anomaly_hours\unknown_ip}.

Конвеєр вичитує потрібну інформацію: для часу перевіряє мітку та звіряє з дозволеними (будні дні з 6 до 18), для IP адреси перевіряє на базі whitelist-а, тобто якщо адреса не була додана до відомих – вона вважається новою. Далі результат перевірки (true\false) вноситься у додатково створене поле, що додається до подій у потоці: triggered_workhours_off та unknown_ip. Усі створені для конвеєру правила наведено на Рисунку 3.10:

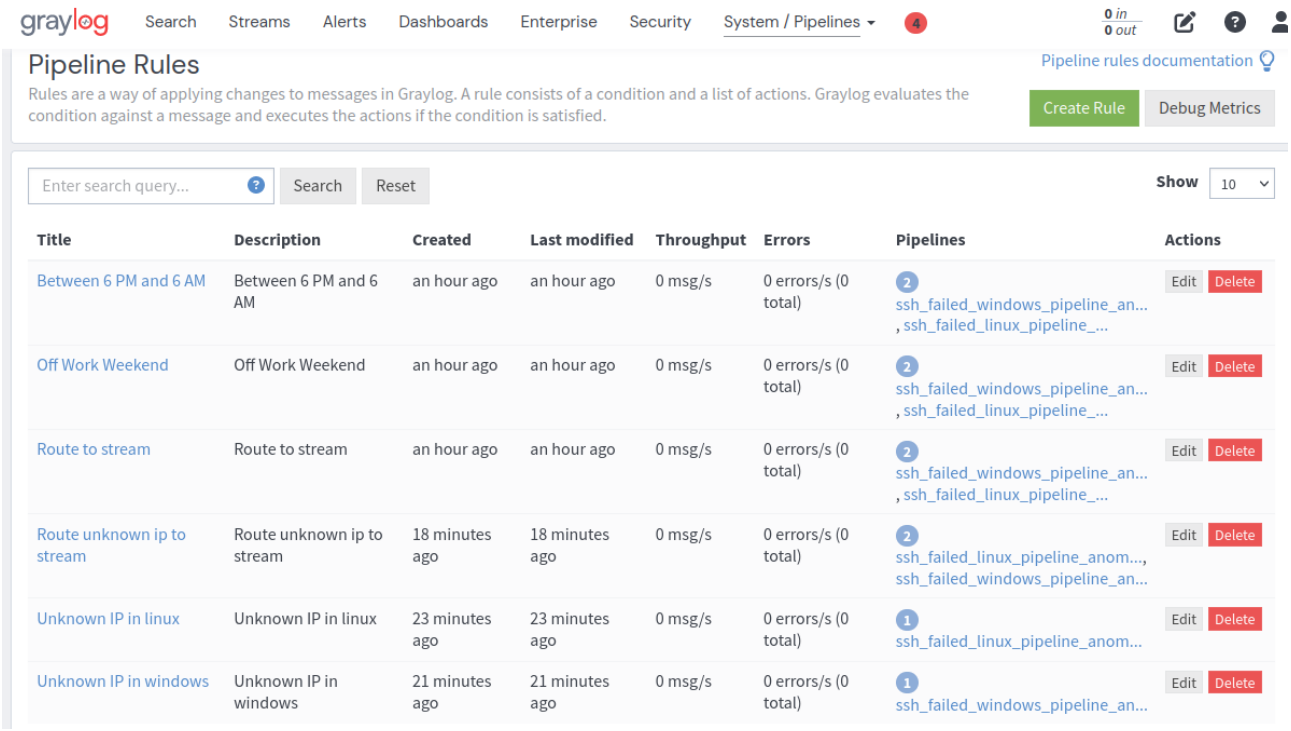


Рисунок 3.10 – Правила перевірки полей події для конвеєру

Graylog оперує поняттям «визначення події» (event definition), яке у класичному розумінні SIEM і прийнято називати правилами виявлення. Як і у інших системах, Graylog здатен будувати складні взаємозв’язки між подіями для більш точного та автоматизованого виявлення вторгнень, чого від добивається

комбінацією наведених вище кроків, кореляціями (лише у платній версії), агрегуванням подій за пороговим значенням (threshold), аби не створювати зайвого шуму із спрацювань. Тому у рамках виявлення неуспішного віддаленого входу через SSH у Windows було створено 4 правила, що за спрацювання створюють події:

1. ssh_failed_WIN : спрацьовує, якщо за 5 хвилин було принаймні 5 неуспішних входів, критичніть Low
2. ssh_failed_WIN_anomaly_hours : спрацьовує, якщо за 5 хвилин було принаймні 3 неуспішних входа, причому у неробочі часи, критичніть Medium
3. ssh_failed_WIN_anomaly_ip : спрацьовує, якщо за 5 хвилин було принаймні 3 неуспішних входа, причому з невідомої адреси, критичніть Medium
4. ssh_failed_WIN_anomaly_hours_and_ip : спрацьовує, якщо за 5 хвилин було принаймні 2 неуспішних входа, причому у неробочі часи, критичніть High

Абсолютно аналогічні event definition створені і для Linux.

Припущення про час і порогове значення є індивідуальним для кожної окремої інфраструктури, наведені краще підійдуть для малої мережі, яка і є у даній роботі, до того ж повноцінний brute force не буде обмежуватися кількома спробами, за умови складного паролю, звісно. Для моніторингу можливих успішних спроб у аномальний час чи з дивної адреси працює аналогічний підхід, лише коди подій мають бути різними та порогове значення. У рамках даного експерименту, присутність одного індикатору вторгнення вважається більш критичним, за просто неуспішний вхід, а обох – критичнішим за попередній випадок. Розподіл важливості реагування також допомагає знизити навантаження на фахівця з безпеки, а комплексний підхід до аналізу показників події – до зниження кількості FP спрацювань та загального підвищення ефективності виявлення, бо з такими правилами шанс не пропустити дійсну нетипову атаку стає вищим: тобто false negative теж буде менше.

Коли умови спрацювання event definition виконано, відбувається поява alert-ів, які зображено на Рисунку 3.11, де вказано коротку загальну інформацію: назва правила, за яким полем була агрегація, на прикладі це IP адреса зловмисника, адже коли система велика, важливо враховувати, що легітимних неуспішних логінів теж буде багато, а агрегація за IP адресою дає можливість зменшити кількість alert-ів, а схожі події об'єднати в один:

Description	Key	Type	Event Definition	Timestamp
ssh_failed_WIN_anomaly_ip: 192.168.198.133|DESKTOP-OJE2NFL|NT AUTHORITY\\SYSTEM|true - count()=2.0	*none*	Event	ssh_failed_WIN_anomaly_ip	2024-01-04 22:21:17
ssh_failed_WIN_anomaly_hours_and_ip: 192.168.198.133|NT AUTHORITY\\SYSTEM|DESKTOP-OJE2NFL|true|true - count()=2.0	*none*	Event	ssh_failed_WIN_anomaly_hours_and_ip	2024-01-04 22:20:33
ssh_failed_linux_anomaly_hours: 192.168.198.133|ubuntu|ubuntu-virtual-machine|true - count()=7.0	*none*	Event	ssh_failed_linux_anomaly_hours	2024-01-04 22:20:09
ssh_failed_linux_anomaly_hours_and_ip: 192.168.198.133|ubuntu|ubuntu-virtual-machine|true|true - count()=4.0	*none*	Event	ssh_failed_linux_anomaly_hours_and_ip	2024-01-04 22:19:35
ssh_failed_linux: 192.168.198.133|ubuntu|ubuntu-virtual-machine - count()=7.0	*none*	Event	ssh_failed_linux	2024-01-04 22:19:23
ssh_failed_WIN_anomaly_hours: 192.168.198.133|NT AUTHORITY\\SYSTEM|DESKTOP-OJE2NFL|true - count()=4.0	*none*	Event	ssh_failed_WIN_anomaly_hours	2024-01-04 22:19:15
ssh_failed_WIN: 192.168.198.133|DESKTOP-OJE2NFL|NT AUTHORITY\\SYSTEM - count()=4.0	*none*	Event	ssh_failed_WIN	2024-01-04 22:18:26
ssh_failed_linux_anomaly_ip: 192.168.198.133|ubuntu|ubuntu-virtual-machine|true - count()=4.0	*none*	Event	ssh_failed_linux_anomaly_ip	2024-01-04 22:17:54

Рисунок 3.11 – Загальний вигляд сторінки зі спрацюваннями

За промислового тестування сповіщення про спрацювання приходять до спеціаліста за налаштованим каналом зв'язку: пошта, Microsoft Teams, Slack, проте у рамках даної роботи це не було доцільно. До того ж, не про всі спрацювання, наприклад такі, що не є критичними, потрібно повідомляти таким оперативним методом, загалом достатньо палені моніторингу самого Wazuh. До кожного спрацювання можливо також налаштувати додавання інформації, що дозволить швидко розібратися що і де відбулося, як от час події, адреса та назва комп'ютера-жертви, акаунт, до якого було спробувано отримати доступ, значення перевірок triggered_workhours_off та unknown_ip і т.п, бо все залежить від типу події. Приклад для Linux та Windows показано на Рисунку 3.12.

Як було показано, пара Wazuh + Graylog дає фахівцю гнучкі способи для досягнення цілі оптимізації ефективності виявлення вторгнень, проте її інтуїтивність використання не є високою, проте це компенсується розвиненою спільнотою користувачів.

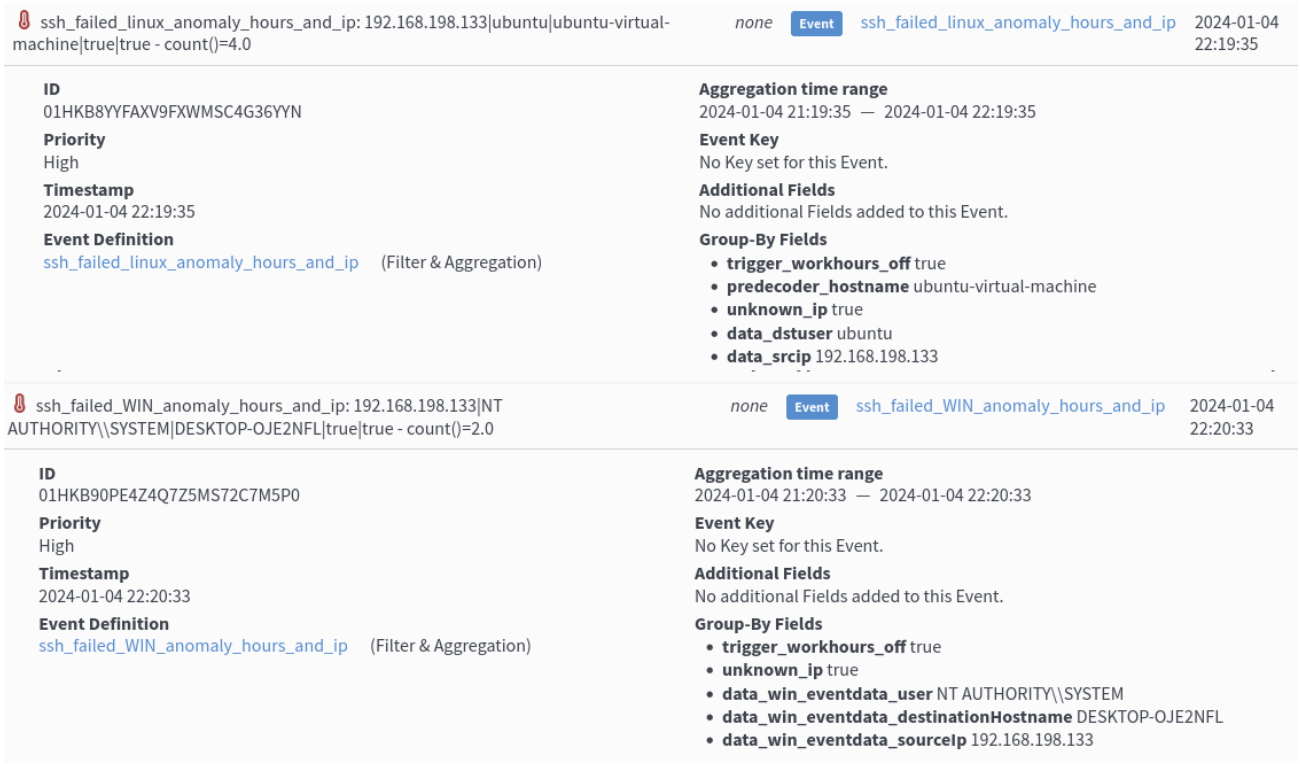


Рисунок 3.12 – Детальна інформація про подію всередині спрацювання

3.3.3 Виявлення підозрілої активності віддаленого входу за допомогою засобами Splunk

Після додавання агентів на сервер Splunk вони з’являються як джерела логів у зведеному вигляді, разом з джерелами логів як показано на Рисунку 3.13:

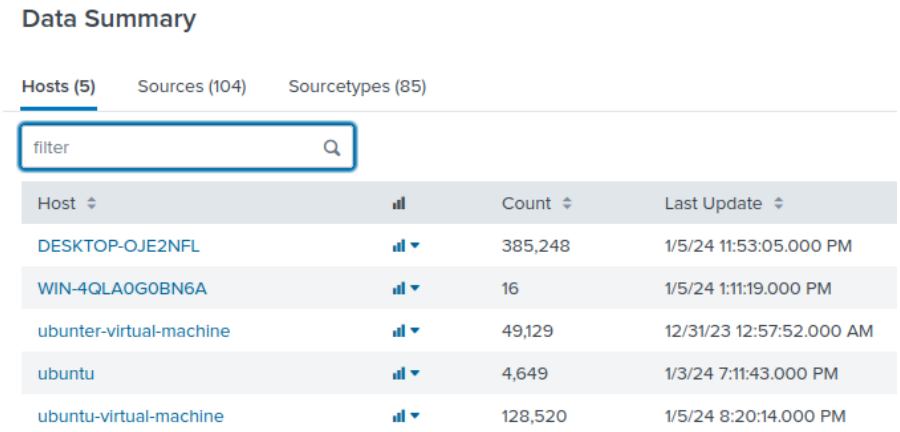


Рисунок 3.13 – Перелік доступних джерел логів у Splunk

Splunk, як вже було зазначено, має здатність аналізу подій у режимі реального часу і пошук, наприклад за певним комп’ютером, у випадку пошуку, наведеного на Рисунку 3.14 – Ubuntu WS, виглядатиме приблизно так:

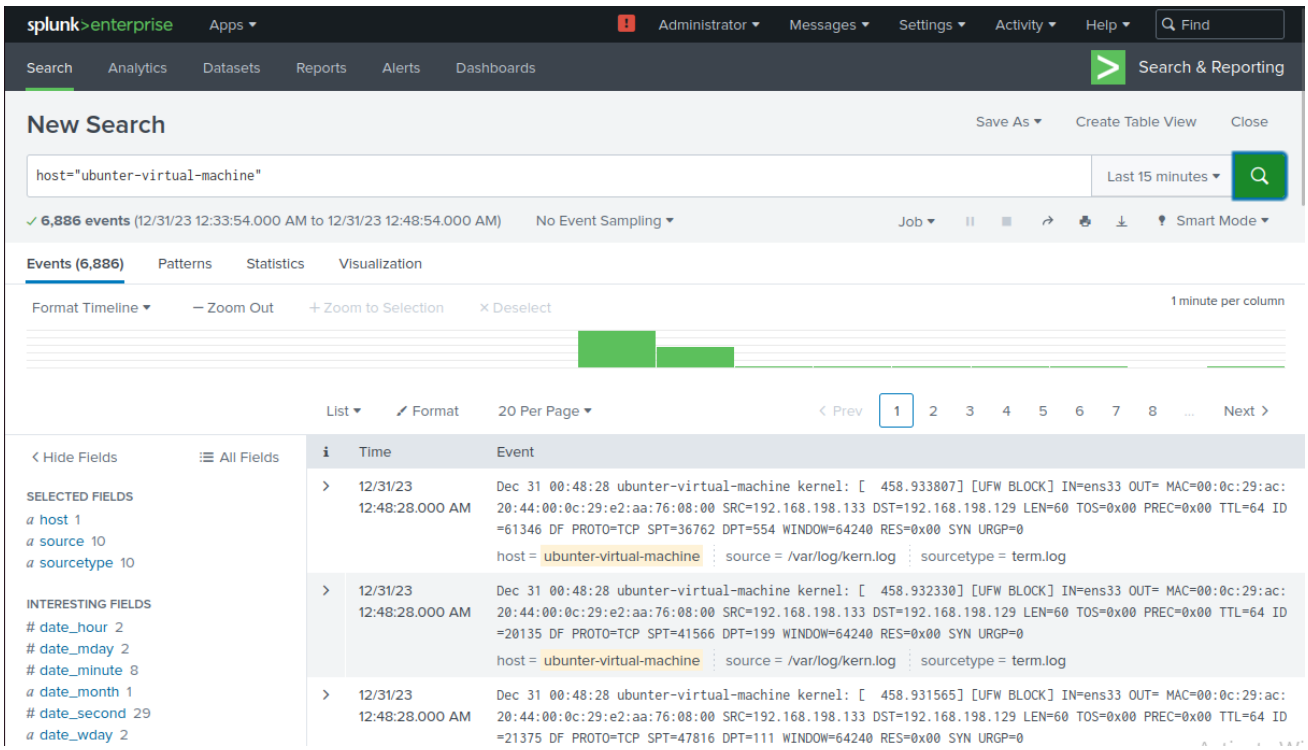


Рисунок 3.14 – Приклад пошуку подій за іменем комп’ютера у Splunk

Оскільки процедура атаки вже була описана, можна одразу перейти до того, як виглядають події від тієї самої зловмисної активності у Splunk. На Рисунку 3.15 – спроба доступу до Ubuntu WS:

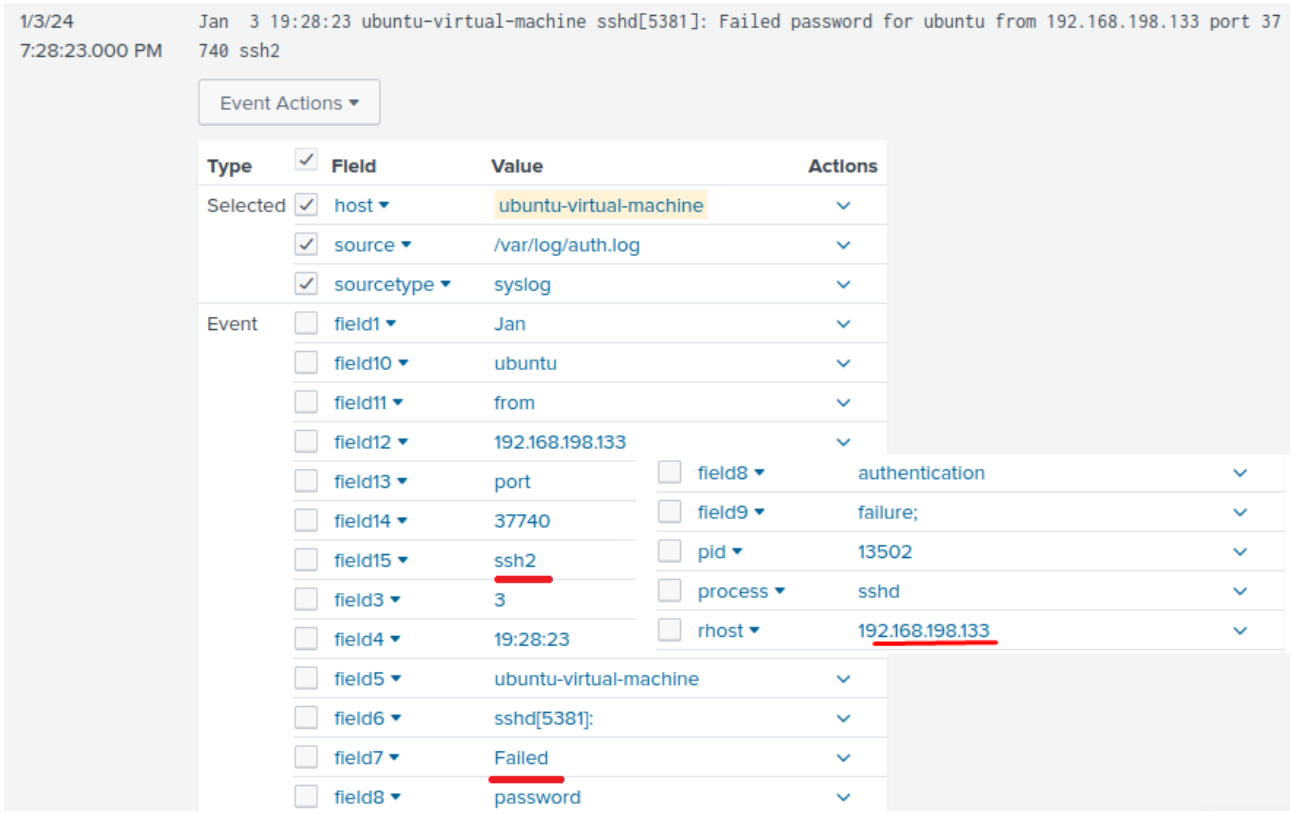


Рисунок 3.15 – Вигляд логів після неуспішного SSH доступу до Ubuntu WS

Для Windows WS ті самі події виглядають вигляду інакше, як видно з Рисунку 3.16:

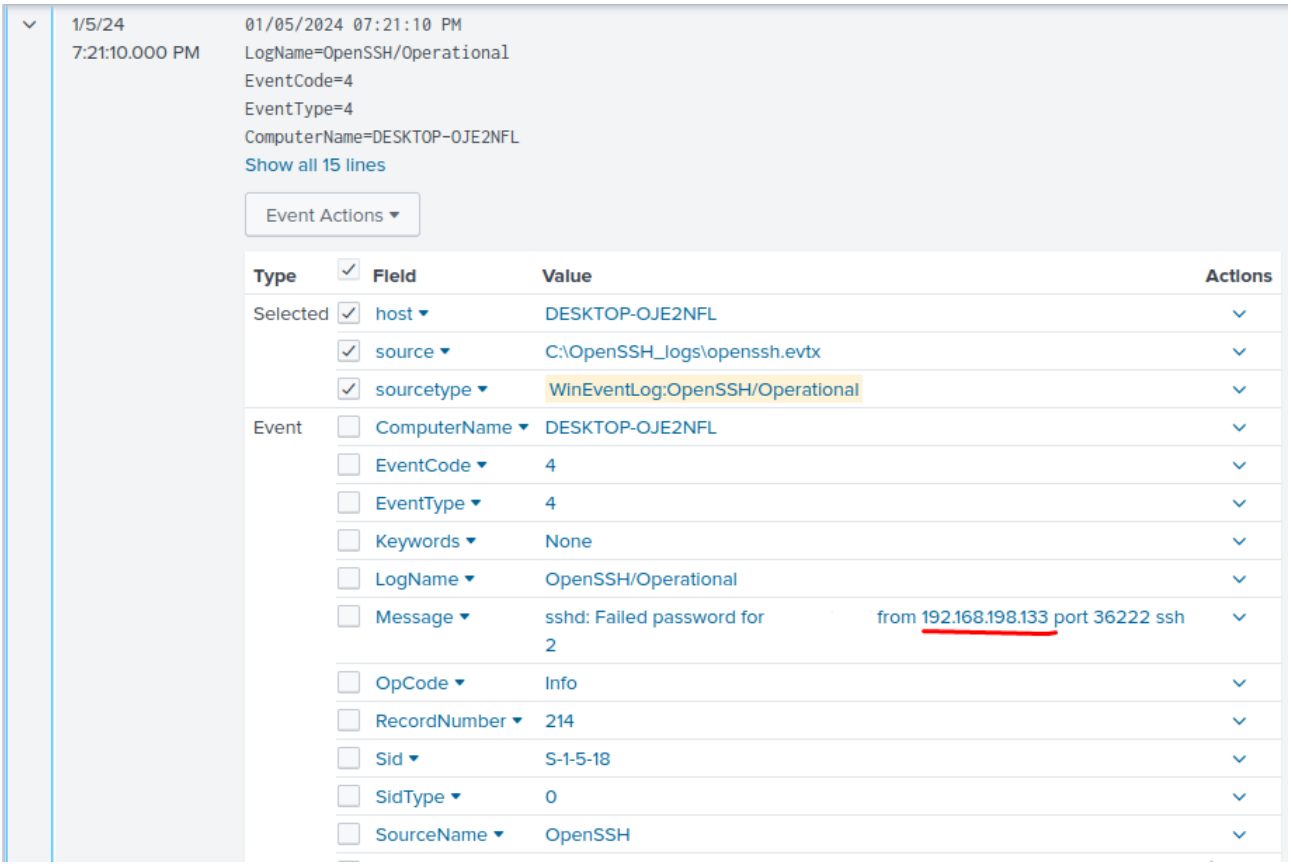


Рисунок 3.16 – Вигляд логів після неуспішного SSH доступу до Windows WS

У Splunk вбудовано потужний пошуковий двигун, що дозволяє по суті усі раніше описані для Wazuh маніпуляції здійснити у пошуковій строчці, проте звісно синтаксис буде залежати від ключових подій, тому є різних для Windows та Linux, приклад можна побачити на Рисунку 3.17. Для ілюстрації було обрано аналогічно назване до тих, що були у частині з Wazuh, правило ssh_failed_{windows\linux}_anomaly_hours_and_ip, адже воно містить у собі усі інші.

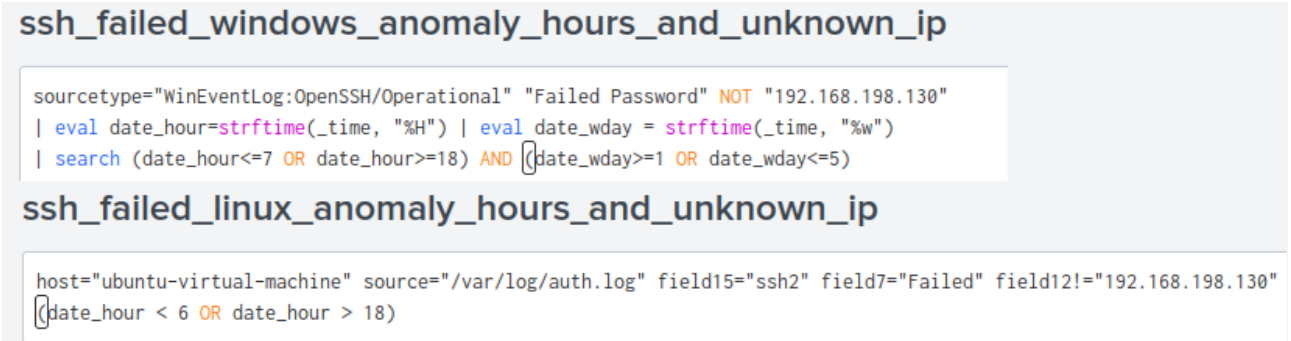
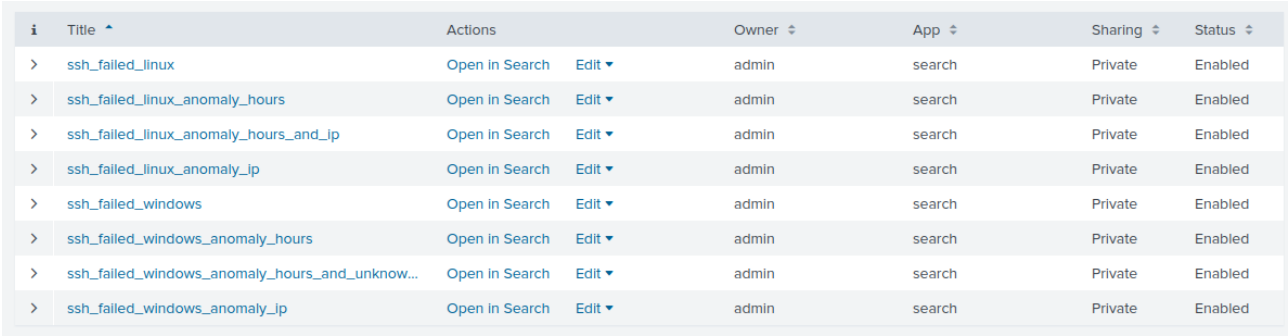


Рисунок 3.17 – Різниця у синтаксисі запитів для Windows та Linux

Після введення пошукового запиту потрібно впевнитись, що отримано саме бажаний результат і далі його можна зберегти у вигляді постійно діючого правила, що генерує спрацювання. Присутні також можливості агрегування за кількістю спрацювань, проте правила дійсно хоча і простіше створювати, вони не є такими гнучкими як у Wazuh, ще й додатковий контекст побачити у меню всіх спрацювань неможливо, що не є зручним для швидкого аналізу. На Рисунку 3.18 наведено вже знайомий набір правил, проте створених для Splunk:



Title	Actions		Owner	App	Sharing	Status
ssh_failed_linux	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_linux_anomaly_hours	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_linux_anomaly_hours_and_ip	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_linux_anomaly_ip	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_windows	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_windows_anomaly_hours	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_windows_anomaly_hours_and_unknow...	Open in Search	Edit	admin	search	Private	Enabled
ssh_failed_windows_anomaly_ip	Open in Search	Edit	admin	search	Private	Enabled

Рисунок 3.18 – Створені у Splunk правила

Натиснувши на правило або ж на спрацювання, можна перейти знову до сторінки пошуку, де й побачити результат виявлення і дослідити всі цікаві поля, як продемонстровано на Рисунку 3.19:

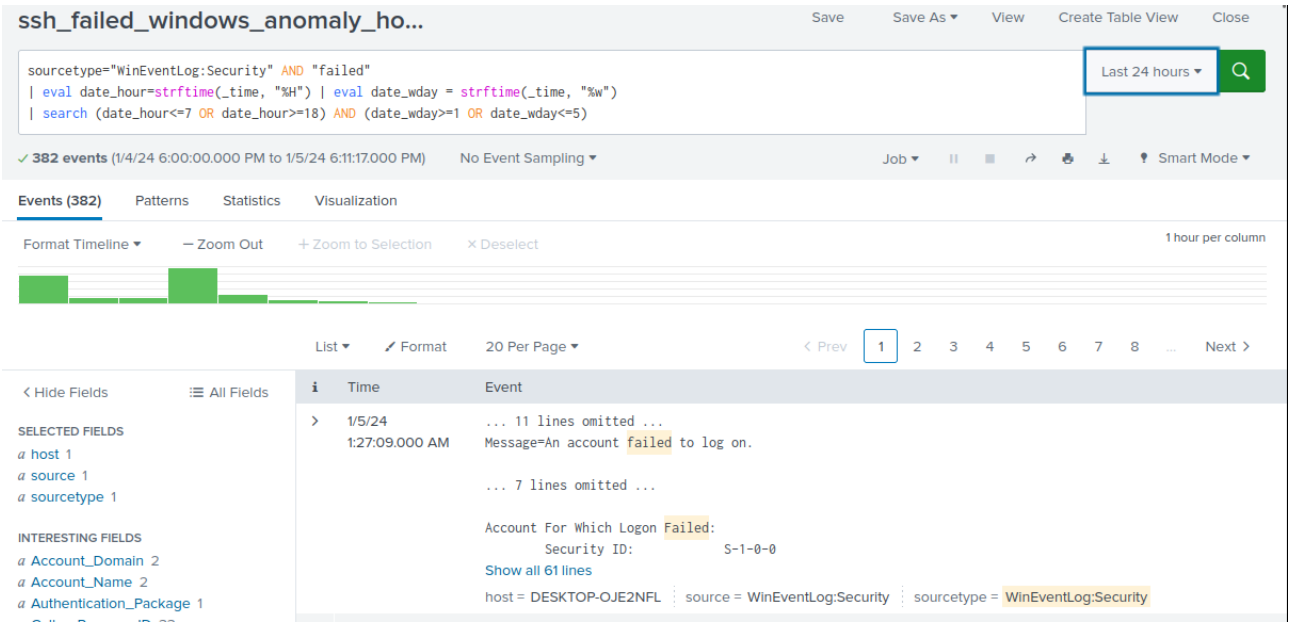


Рисунок 3.19 – Приклад аналізу спрацювань за правилом у Splunk

Спрацюванням за відповідними правилами було надано аналогічну критичність, про яку згадувалось у пункті 3.3.2, вони знаходяться у Splunk на панелі Triggered Alrts, містять лише назву правила, приклад – на Рисунку 3.20:

Time	Fired Alerts	App	Type	Severity	Mode	Actions
2024-01-05 20:20:14 EET	ssh_failed_linux_anomaly_hours	search	Real-time	Medium	Digest	View Results | Edit Search | Delete
2024-01-05 20:20:14 EET	ssh_failed_linux_anomaly_ip	search	Real-time	Medium	Digest	View Results | Edit Search | Delete
2024-01-05 20:20:14 EET	ssh_failed_linux_anomaly_hours_and_ip	search	Real-time	High	Digest	View Results | Edit Search | Delete
2024-01-05 20:19:47 EET	ssh_failed_windows_anomaly_hours_and_unknown_ip	search	Real-time	High	Digest	View Results | Edit Search | Delete
2024-01-05 20:19:47 EET	ssh_failed_windows_anomaly_ip	search	Real-time	Medium	Digest	View Results | Edit Search | Delete
2024-01-05 20:18:42 EET	ssh_failed_windows_anomaly_hours_and_unknown_ip	search	Real-time	High	Digest	View Results | Edit Search | Delete
2024-01-05 20:18:42 EET	ssh_failed_windows_anomaly_ip	search	Real-time	Medium	Digest	View Results | Edit Search | Delete
2024-01-05 20:15:47 EET	ssh_failed_windows	search	Real-time	Low	Digest	View Results | Edit Search | Delete

Рисунок 3.20 – Спрацювання за створеними правилами

Задачу експерименту засобами Splunk було виконано на такому самому рівні, як з Wazuh, проте після використання Splunk можна зробити висновок, що для складних операцій, які потребують ще більш комплексний аналіз, він може не підійти, проте його пошуковий двигун дійсно доволі хороший, особливо для швидкої візуалізації результату.

3.4 Зведені рекомендації щодо дій для оптимізації кількості FP

Врахувавши всі наведені у роботі теоретичні та практичні напрацювання, можна виділити такі рекомендації щодо можливих дій у питанні зменшення кількості FP спрацювань:

1. Виправити або впевнитись у відсутності помилок у організаційному процесі створення правил виявлення
2. Визначити чітку політику доступу та логічно відобразити її у правил виявлення та виключеннях до них
3. Провести аналіз існуючих FP спрацювань за допомогою методів кластеризації аби розбити їх на типові групи
4. Виділити часті епізоди та з них побудувати ланцюжки подій, що призводять до появи однакових сповіщень, внести винятки, змінити правила

5. Знайти за допомогою майнінгу логів всі можливі першопричини FP, за можливості усунути
6. Збільшити комплексність показників, що збираються, за рахунок використання більш повних та універсальних метрик, а також відмови від марних
7. Розробити та протестувати правила виявлення вторгнень, що враховують комплексні показники, для потрібного типу атак
8. Проводити регулярну роботу з перегляду та модифікації існуючих правил аби вони відповідали актуальному стану системи та загрозам

Висновки до розділу 3

У даному розділі роботи було показано яким чином може відбуватись процес оптимізації FPR на прикладі використання SIEM Wazuh та Splunk. Було виконано симуляцію атаки на Ubuntu та Windows WS з неуспішними входами до облікового запису засобами віддаленого доступу SSH. На базі згаданого експерименту було розроблено правила виявлення, які окрім загальноприйнятих даних про події у системі враховують їх комплексним чином, що дозволяє розбивати загальну масу спрацювань за рівнем критичності, адже вірогідність реальності виявленого вторгнення зростає за використанні декількох індикаторів його присутності, як було описаного у пункті 2.3.

Для досягнення мети даного дослідження отримані у Розділі 1 та 2 теоретичні знання, а також практичний досвід з Розділу 3 було врешті-решт об’єднано у пункті 3.4 до універсального алгоритму дій, що призведуть до підвищення ефективності виявлення вторгнень у системі та підвищать рівень обізнаності щодо її стану для фахівців з безпеки, що неодмінно допоможе у процесі боротьби з вторгненнями.

ВИСНОВКИ

Дана робота присвячена дослідженню за актуальною та важливою темою оптимізація ефективності роботи систем виявлення вторгнень. Актуальність задачі пояснюється майже загальноприйнятою практикою використання SIEM систем для вирішення задач інформаційної безпеки, у тому числі і згаданому питанню виявлення вторгнень, а отже постійною потребою у вдосконаленні роботи системи захисту, зменшення шуму у спрацюваннях, збільшенню покриття правилами виявлення різноманітних сучасних атак. В ході розв’язання головної задачі – пошуку універсального ефективного методу виявлення вторгнень – було також проаналізовано існуючі теоретичні та практичні здобутки науковців та фахівців за темою, здійснено критичний аналіз переваг і недоліків їх застосування, розгорнуто SIEM Wazuh та Splunk, проведено практичні експерименти з написання правил виявлення, тощо. Також у ході роботи було зроблено такі висновки:

- Сигнатурні методи виявлення вторгнень є класичним, проте застарілим підходом, що не може бути застосованим до сучасних інформаційних систем через свою надзвичайну об’ємність, неповноту та безпорадність перед новими чи складними атаками;
- Методи, засновані на машинному навчанні потребують великої бази подій для навчання та схильні до хибнихспрацювань через нетипову легітимну поведінку користувачів;
- Статистичні методи, засновані на ймовірностях, за різних статистичних моделей та середовищ можуть давати недостатньо гарантований рівень ефективності;
- Сучасні тенденції розвитку хмарних технологій прогнозують збільшення кількості хибних спрацювань та потребу у комплексному аналізі поведінки користувачів;

- Наявні методи оптимізації FPR включають в себе: організаційні, конфігураційні, методи пошуку ланцюжків подій, методи збільшення даних та пошук першопричин-джерел хибних подій.

Серед практичних досягнень цієї роботи потрібно виділити:

- Розгортання лабораторного середовища для тестування власних правил виявлення та проведення симуляції атаки у нього через відсутність у вільному доступі прийнятних наборів даних;
- Вивчення функціоналу SIEM Wazuh та Splunk з акцентом на побудову складних правил виявлення, що використовують комплексну інформацію про інформаційну систему;
- Створення правил та тестування їх ефективності;
- Формалізація потрібних для оптимізації FPR дій в універсальний алгоритм.

Загальноприйняті методи виявлення вторгнень як от згадані у Розділі 1 сигнатурні, здатні виявити певні типи атак та навіть досить непогано впоратись з типи випадками, коли точно відомо яким чином буде виконана атака чи буде використано відоме шкідливе програмне забезпечення, і якщо наявні ресурси дозволяють, то комбінування складних поведінкових методів виявлення на основі машинного навчання разом з сигнатурними, дасть більш повний захист з різних боків. Комплексні рішення майже завжди дають кращий результат, ніж ті, що базуються лише на одному підході, особливо коли мова йде про захист від складних вторгнень. Проте за умов, коли ресурси не є нескінченними, доводиться шукати компроміс між захищеністю системи та складністю реалізації цього захисту. На нагоді може стати описаний у роботі підхід з комплексним використанням інформації про систему, який потребує не стільки ресурсів, як гарної обізнаності зі станом системи, процесами, що у ній відбуваються та першопричинами великої кількості FP.

Зведений універсальний алгоритм для оптимізації FPR, наведений у пункті 3.4, як не важко помітити, окрім комплексного використання даних про події, рекомендує також у певному вигляді застосувати усі згадані у Розділі 2 методи,

адже вони також є корисними. Перспектива майбутніх досліджень випливає з актуальності теми та може включати у себе автоматизацію вивчення стану системи для пришвидшення процесу оптимізації, а також звісно автоматизацію написання правил виявлення з комплексною інформацією про систему.

Загалом, у роботі наведено ґрунтовні теоретичні дані за темою, здійснено оцінку сучасних тенденцій в інформаційній безпеці з боку SIEM та було визначено універсальний алгоритм, який пришвидшить процес змін у системі, які потрібні для підвищення ефективності виявлення вторгнень. Усі напрацювання можуть бути плідно використані майбутніми дослідниками чи фахівцями, що бажають покращити свою систему захисту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Intrusion Detection System (IDS) [Електронний ресурс] // GeeksForGeeks – Режим доступу до ресурсу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/ (дата звернення: 18.12.2023).
2. A Survey on Secure Network: Intrusion Detection & Prevention Approaches [Текст] / A. Choubey, N. Thakur – International Journal of Engineering & Scientific Research Volume 4, Issue 8. – August 2016. – P. 74-88.
3. What is the difference between signature-based and behavior-based intrusion detection systems? [Електронний ресурс] // Accedian – Режим доступу до ресурсу: https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/ (дата звернення: 29.10.2023).
4. Класифікація методів виявлення аномалій в інформаційних системах [Текст] / І.В. Рубан, В.О. Мартовицький, С.О. Партика – Системи озброєння і військова техніка, 2016, № 3(47) ISSN 1997-9568 – 102с.
5. Survey of intrusion detection systems: techniques, datasets and challenges [Текст] / A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman – SpringerOpenCybersecurity (2019) 2:20 – 22 с.
6. How do antimalwares work and why they are not sufficient anymore [Електронний ресурс] // FlashStart – Режим доступу до ресурсу: https://flashstart.com/the-limits-of-traditional-antivirus-systems-why-they-are-not-sufficient-anymore/ (дата звернення: 29.10.2023).
7. MITRE ATT&CK Matrix for Enterprise [Електронний ресурс] // MITRE – Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 29.10.2023).
8. A survey on anomaly and signature based intrusion detection system (IDS) [Текст] / A. Gangwar, S. Sahu – Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 4(Version 1), April 2014, pp.67–72 – 6 с.

9. Signatureless Anomalous Behavior Detection in Information Systems [Текст] / V. Tkach, A. Kudin, V. Zadiraka & I. Shvidchenko – ISSN 1019-5262. Кібернетика та системний аналіз, 2023, том 59, №5 – ст.100–112 –12 с.
10. Метод Виявлення Аномальної Поведінки в Локальній Мережі [Текст] / В. І. Батинчук, О. М. Барановський – XIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 2018, 112-113с.
11. Виявлення Аномалій в Телекомунікаційному Трафіку Статистичними Методами [Текст] / Т. Радівілова, Л. Кіріченко, М. Тавалбех, А. Ільков – Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 2021, ст. 183–194.
12. Machine Learning for Anomaly Detection: A Systematic Review A. B. Nassif, M. A. Talib, Q. Nasir, F. M. Dakalbab [Текст] / IEEEXPLORE – Digital Object Identifier 10.1109/ACCESS.2021.3083060 – 43с.
13. Top 8 Most Useful Anomaly Detection Algorithms For Time Series And Common Libraries For Implementation [Електронний ресурс] // SpotIntelligence – Режим доступу до ресурсу: https://spotintelligence.com/2023/03/18/anomaly-detection-for-time-series (дата звернення: 18.12.2023).
14. Система виявлення аномалій методами інтелектуального аналізу даних [Текст] / О. Хомич – Магістерська дисертація 2022 – 91с.
15. Survey Threat Hunting: Focusing on the Hunters and How Best to Support Them [Текст] / M. Fuchs, J. Lemon – SANS Whitepaper, April 2023
16. Top 10 Cloud Security Risks & Solution in 2023 & How to Tackle Them [Електронний ресурс] // Appinventiv – Режим доступу до ресурсу: https://appinventiv.com/blog/cloud-security-risks-and-solutions/ (дата звернення: 29.10.2023).
17. Handle a false positive [Електронний ресурс] // CloudFare – Режим доступу до ресурсу: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adjust-rules/false-positive/ (дата звернення: 29.10.2023).

18. Indicators of Compromise Confidence Scoring Method [Текст] / V. Tkach, O. Baranovskyi, A. Kudin, N. Godavarti, O. Kliok, S. Modali – The 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 7-9 September, 2023, Dortmund, Germany – 9c.
19. How to Defend With the Courses of Action Matrix and Indicator Lifecycle Management [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/how-to-defend-with-the-courses-of-action-matrix-and-indicator-lifecycle-management/ (дата звернення: 29.10.2023).
20. “Authorized” to break in: Adversaries use valid credentials to compromise cloud environments [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/posts/adversaries-use-valid-credentials-compromise-cloud-environments/ (дата звернення: 29.10.2023).
21. Avoiding the Storm | How to Protect Cloud Infrastructure from Insider Threats [Електронний ресурс] // SentinelOne – Режим доступу до ресурсу: https://www.sentinelone.com/blog/avoiding-the-storm-how-to-protect-cloud-infrastructure-from-insider-threats/ (дата звернення: 29.10.2023).
22. The Importance of User Behavior Analytics for Cloud Service Security [Електронний ресурс] // Oracle – Режим доступу до ресурсу: https://www.oracle.com/assets/user-behavior-analytics-3497541.pdf (дата звернення: 29.10.2023).
23. QRadar User Behavior Analytics [Електронний ресурс] // IBM – Режим доступу до ресурсу: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-user-behavior-analytics (дата звернення: 29.10.2023).
24. How to Maximize Telemetry Data Value With Observability Pipelines [Електронний ресурс] // DevOps IBM – Режим доступу до ресурсу:

https://devops.com/how-to-maximize-telemetry-data-value-with-observability-pipelines/ (дата звернення: 29.10.2023).

25. Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems [Текст] / Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai – IEEE Communications Magazine March 2012 – 146-154с.

26. Reducing false positives in intrusion detection by means of frequent episodes [Текст] / L.O. Gigstad - Master's Thesis Department of Computer Science and Media Technology Gjøvik University College, 2008 – 95с.

27. Discovery of Frequent Episodes in Event Logs [Текст] / M. Leemans, W. M.P. van der Aalst – International Symposium on Data-Driven Process Discovery and Analysis – November 2014 – 15с.

28. Павловский З. Введение в математическую статистику / [Текст] Пер. с польского. – М.: Статистика, 1967. – 285 с.

29. Тюрин Ю.Н., Макаров А.А. Анализ данных на компьютере / [Текст] М.: Финансы и статистика, 1995. – 384 с.

30. Emphasis on the Minimization of False Negatives or False Positives in Binary Classification – Sanskriti Singh [Електронний ресурс] // Arvix – Режим доступу до ресурсу: https://arxiv.org/pdf/2204.02526.pdf (дата звернення: 18.12.2023).

31. Using Root Cause Analysis to Handle Intrusion Detection Alarms [Текст] / Klaus Julisch – IBM Zurich Research Laboratory, 2003 – 148с.

32. Reduction of False Positives in Intrusion Detection Based on Extreme Learning Machine with Situation Awareness [Текст] / Donald A. Burgio - Doctoral dissertation, 2019 – 139с.

33. Wazuh About us [Електронний ресурс] // Wazuh – Режим доступу до ресурсу: https://wazuh.com/about-us/ (дата звернення: 18.12.2023)

Додаток А

UDC 004.7.056.5

The methods of decreasing FP in Anomaly based Intrusion Prevent System by using of complex information about information system

Anton Kudin[1], Olga Grigorieva[2] and Svetlana Nosok[3]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"; National Bank of Ukraine, Kyiv, Ukraine, e-mail: pplayshner@gmail.com.*
[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv, Ukraine, e-mail: olga.grygorieva.fb83@gmail.com*
[3] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv, Ukraine, e-mail: nos.sv.ol@gmail.com*

Abstract
The main aim of this work is to optimize the efficiency of intrusion detection using complex analysis of indicators in information system by reducing the number of false positives, as well as the development of a universal technique for such optimization. Using laboratory environment with installed SIEMs Wazuh and Splunk we test the proposed optimization methods and proposed newly methodic for decreasing rating false/positive for some intrusion detecting systems.

Keywords: False Positives Optimization; Intrusion Detection Systems (IDS); Anomalies Detection; Comprehensive Behavioral Analysis; Security Information And Event Management (SIEM); Signatureless Intrusion Detection Methods

Introduction

Early intrusion detection is the main task of anything cybersecurity system. One problem of their building is decreasing ratio false/positive. This connected with some theoretical and practical problems. Such problems are:

1. Theoretical:
- indistinguishability of anomalies caused by different types of events (which anomalies are attributed to attacks);
- existing models do not clearly answer and give no recommendations on the choice of parameters, the limits of the scales for measuring parameters, etc.;
- existing models do not fully consider the problem of working with primary / processed data (including the choice of the optimal solution for speed / accuracy);
- inconsistency of these observations from sensors with different metrics thus, not the creation of a single metric, but optimal solutions in space without any metric (general theory of optimal algorithms);
- trust and credibility of the data sensors.

2. Practical:
.
- practical absence of introduction of modern models in commercial systems, predominant use of signature systems, complexity of introduction of the systems based on detection of anomalies

While the rising popularity of cloud data centers is understandable and leaves no arguments against them except for maybe privacy issues, the outsourced SOC matter is questionable. The period of pandemic caused a rapid increase in demand for third-party security services, but as some surveys show, compared to 37% of companies that used outsourced services in 2021, current 22% look less appealing [1]. Whatever statistics may be, it is also undoubtful that both small and unspecialized companies will continue to use such SOC`s help for managing their security due to cost and staff saves.

It is often easier to use the already set-up mechanism than to build one from scratch, and though the third-party specialists may need more time to get familiar with a new infrastructure and will deal with all the sensitive data in the company, the outsourced SOC benefits can make up for it. The process of configuring security systems to effectively detect anomalies and threats may be trickier with the outsourced SOC than with its in-house version, but it will either way obviously create a huge number of false positives. Although, skilled in-house experts are more likely to overcome this problem by thorough tuning, this is not always an option.

Trends in Cloud Data Centers and outsourced SOCs: Impact on Intrusion Detection Quality

Unsurprisingly, the key goal of each security system which relies on SIEM in the matter of finding anomalies, is to reduce the noise or false positive level. Thus, when speaking about efficiency of any detection set-up, we mean the level of false positive alerts it creates. The fewer false positives, the better the system.

To explore the problem, some fresh tendencies are worth mentioning:

1. Rising importance of communication channels in cloud

When relying mainly on cloud services for security or other issues, one must understand that if due to any reason a cloud is unreachable, the whole work stops inevitably. Among such reasons are of course the dreadful DDoS attacks that harm the availability of company`s resources, bringing up not only financial but also reputational damage. According to [2], DDoS attacks remain in the top10 of cloud security risks, hence, protection of communication channels between cloud and its clients are of a great importance. To mitigate them IDS usage and Firewall Traffic Inspection can be offered, as well as anomaly search and IP blocking, all of which will bring more false positive alerts. Unfortunately, even respectable companies like Cloudflare cannot propose more than manually adding exceptions or changing the sensitive level of the detection rule for cases, when legitimate traffic is classified as malicious [3].

2. Increasing IOC`s source authenticity requirements

By trusting immense lists of IOCs of arguable origin, a company decreases its detection efficiency and leaves both experts and system resources overwhelmed. IOC data bases should be not only updated frequently, but also validated for their confidence score and authoritative origin. Different methodologies can be used to evaluate IOC`s confidence score, for example as described in [4] or other ML based decisions. Another option is to analyze the cyber kill chain [5], which in fact can also be automated via ML. Although, a lot of companies are jealous when it comes to sharing a rather valuable experience of fighting against cyber threats, some open-source platforms for accounting IOC exist. Several examples include OpenIOC Framework, MISP, IBM X-FORCE, SANS Internet Storm Center, numerous open Github solutions etc.

3. Trusted attacker

As cloud services gained their popularity, they became of a great use not only to regular users, but also to hackers, which lead to an issue of a malicious user enjoying the same privileges inside the cloud service as a legitimate user. Moreover, a system is unlikely to check in-depth for example the internal traffic, than the one, coming from

outside. As [6] states, “over 35% of cloud security incidents occurred from attackers’ use of valid, compromised credentials”. These statistics reveal a significant problem of mitigating such insider-like attacks, especially taking in consideration the fact that such actions may not be as obviously evil as other incidents. The question arises: How to distinguish such a user's activity from normal? Best practices include giving the least needed privileges to users, implementing some behavioural detection algorithms, and using the DSPM (Data Security Posture Management) approach that can prevent sensitive data breaches [7]. Just as finding anomalies can be the key, it will also create more detection noise.

4. Comprehensive analysis of user behavior

Owing to the advanced nature of modern cyber-attacks, a traditional signature-based attitude towards detection of deviations from normal user behaviour needs more comprehensive treatment. Hackers no longer threaten only high privileged accounts, they prefer to play safe and gradually gain more and more access to the system by starting with lower profile users that often don't get the security attention they need. Hopefully, protection measures are aware of the described risks and some solutions are already presented. Oracle`s CASB (Cloud Access Security Broker) Cloud Service for example has User Behavior Analytics (UBA) module that is able to perform “dynamic, user-risk scoring based on continual assessment of user behavior”, create access patterns and control users` usage of applications [8]. Other changes, including any privileges or security configuration, are also crucial to monitor and validate. IBM QRadar too offers similar UBA service [9] that utilises ML abilities to extract a behavior model from historical data of user activities. Another great instance of UBA implementation is Exabeam, which also by means of ML can detect deviations from established baselines.

5. Increasing volumes of telemetry data

In response to new attacks, specialists are forced to add more detection rules, log sources, checks, all of which multiples telemetry data annually. At some point the company's resources are exhausted, and it no longer has full control over the situation. “38% of companies operate with limited awareness of what’s happening in their software”, states [10]. Excessive log gathering otherwise means not all of them are actually used or useful in investigations. Among already mentioned problems [10] also remarks that “telemetry data is unstructured; varying formats make it hard to use; data preparation is time-consuming and sensitive data in logs may lead to compliance violations”.

6. Not only IOC, but also other telemetry data should be considered comprehensively

It follows from the previous paragraph that all data can be gathered in vain when used without thought. For achieving early anomaly detection, it's never enough to conduct just IOC monitoring or other signature-based detection, as the whole landscape should be taken into account. Security specialists must observe not merely one alert, but rather the sequence of seemingly legitimate actions that result in some attack. This can be done by means of complex detection rules, based on the knowledge of previous attack schemes, for example such as MITRE propose. Alternatively, ML algorithms or neural networks can be fed with

normal system activities and therefore learn to detect such suspicious patterns. Considering current tendencies in cloud services, we can only conclude that all of them demand a more comprehensive approach to detecting anomalies and broadening information we gather from systems, which in turn creates more false positive alerts unless we have the wisdom to tune the detection systems even more carefully or use advanced automated detection algorithms.

Limitations of statistical methods decreasing

The need to increase the size of the sample (the analyzed data) in order to reduce the error of the first kind follows directly from the Chebyshov theorem (or the law of large numbers) [28, 29], namely, with an increase in the number of observations, various random deviations of random values are equalized, therefore, with the probability that the arithmetic mean of the observation results tends to 1 will be arbitrarily little different from the arithmetic mean of the characteristic under investigation in the entire statistical general population.

We have the next one. Let $X_1, \dots X_n$ – independent equally distributed random variables with mathematical expectation M and variance. Then for each $\varepsilon > 0$ if $n \to \infty$ likelihood

$$P\left(\left|\frac{X_1+\dots+X_n}{n} - M\right| < \varepsilon\right) \to 1 \qquad (1)$$

Even more, we can estimate the sample size n from the central limit theorem, which states that the distribution of a random variable $\sqrt{n}(\theta_n - \theta)$ (де θ_n – some statistic of random value, received with sample size of n, a θ – its theoretical analog) have asymptotic normal distribution with (a, σ^2) parameters. Then we have a clear statement of the optimization problem to determine the required amount of experimental data with some rate false/positive. The effect of increasing the number of different types of observed data on reducing the false/positive rate requires further explanation. First, such an increase makes it possible to more clearly define the theoretical distribution of experimental data. Secondly, as a rule, it allows in certain cases to move from statistical intrusion detection methods to deterministic ones, which in turn sharply reduces the false/positive rate. A simple example can be an additional analysis of the location of the analysis subjects (IP addresses) at the statistical limit of the number of false authorization attempts.

Experimental results discussion

Now we have a great problem with good dataset for experimental expectation new methods of intrusion detection. Datasets available to a wide range of researchers, such as KDD98, KDDCUP99, DARPA 1999, NSLKDD and others, just do not meet the above requirements. They are outdated, and therefore do not show modern examples of events, let alone attacks; their size may be insufficient; the number of types of attacks and their balance leaves much to be desired; the information may not be sufficient or it may not be suitable for processing in the necessary ways. So we created own laboratory stand for giving our dataset. Then as part of the detection of unsuccessful remote login via SSH in Windows 11, 4 rules were created that, when triggered, create events:

- ssh_failed_WIN: fires if there were at least 5 failed logins in 5 minutes, critical Low
- ssh_failed_WIN_anomaly_hours: fires if there were at least 3 failed logins in 5 minutes,

and during non-working hours, criticize Medium

- ssh_failed_WIN_anomaly_ip: triggers if there were at least 3 failed logins in 5 minutes, and from an unknown address, criticizes Medium
- ssh_failed_WIN_anomaly_hours_and_ip: triggers if there were at least 2 failed logins in 5 minutes, and during non-working hours, critical High

As result of experiment the following rules was created (see fig. 1).

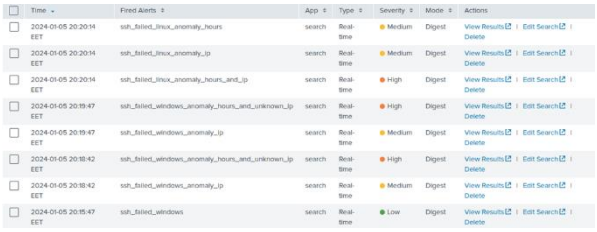


Figure 1: Examples of triggering by created rules

Acknowledgements

We express our gratitude to the entire team of Institute of Physics and Technology Institute and team of CRDF grant G -202102-67499.

Conclusions

We consider one problem decreasing false/positive rate in modern IDS based on fully using monitoring data on the functioning of the information system. The main idea is complex application of statistical and deterministic intrusion detection methods, which is clearly demonstrated by the example of the analysis of statistics of failed user authentication attempts. Another interesting approach is used of universal for all information systems indicators: the time of the event and the location (geography, IP address) of the event taking place. It is the complex application of these two indicators that significantly improves the effectiveness of intrusion detection. We also payed attention to the practical side of the work: a test bench was deployed based on two different types of protection systems - SIEM Splunk and Wazuh, and simulations of various attack scenarios, practical application of the proposed methods were carried out, and a methodology was developed that practically proves the effectiveness of the developed rules/methods of intrusion detection.

References

[1] Intrusion Detection System (IDS) [Електронний ресурс] // GeeksForGeeks – Режим доступу до ресурсу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/ (дата звернення: 18.12.2023).

[2] A Survey on Secure Network: Intrusion Detection & Prevention Approaches [Текст] / A. Choubey, N. Thakur – International Journal of Engineering & Scientific Research Volume 4, Issue 8. – August 2016. – P. 74-88.

[3] What is the difference between signature-based and behavior-based intrusion detection systems? [Електронний ресурс] // Accedian – Режим доступу до ресурсу: https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/ (дата звернення: 29.10.2023).

[4] Класифікація методів виявлення аномалій в інформаційних системах [Текст] / І.В. Рубан, В.О. Мартовицький, С.О. Партика – Системи озброєння і військова техніка, 2016, № 3(47) ISSN 1997-9568 – 102с.

[5] Survey of intrusion detection systems: techniques, datasets and challenges [Текст] / A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman – Springer Open Cybersecurity (2019) 2:20 – 22 с.

[6] How do antimalwares work and why they are not sufficient anymore [Електронний ресурс] // FlashStart – Режим доступу до ресурсу: https://flashstart.com/the-limits-of-traditional-antivirus-systems-why-they-are-not-sufficient-anymore/ (дата звернення: 29.10.2023).

[7] MITRE ATT&CK Matrix for Enterprise [Електронний ресурс] // MITRE – Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 29.10.2023).

[8] A survey on anomaly and signature based intrusion detection system (IDS) [Текст] / A. Gangwar, S. Sahu – Int. Journal of Engineering Research and Applications ISSN

: 2248-9622, Vol. 4, Issue 4(Version 1), April 2014, pp.67–72 – 6 с.
[9] Signatureless Anomalous Behavior Detection in Information Systems [Текст] / V. Tkach, A. Kudin, V. Zadiraka & I. Shvidchenko – ISSN 1019-5262. Кібернетика та системний аналіз, 2023, том 59, №5 – ст.100–112 –12 с.
[10] Метод Виявлення Аномальної Поведінки в Локальній Мережі [Текст] / В. І. Батинчук, О. М. Барановський – XIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 2018, 112-113с.
[11] Виявлення Аномалій в Телекомунікаційному Трафіку Статистичними Методами [Текст] / Т. Радівілова, Л. Кіріченко, М. Тавалбех, А. Ільков – Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 2021, ст. 183–194.
[12] Machine Learning for Anomaly Detection: A Systematic Review A. B. Nassif, M. A. Talib, Q. Nasir, F. M. Dakalbab [Текст] / IEEEXPLORE – Digital Object Identifier 10.1109/ACCESS.2021.3083060 – 43с.
[13] Top 8 Most Useful Anomaly Detection Algorithms For Time Series And Common Libraries For Implementation [Електронний ресурс] // SpotIntelligence – Режим доступу до ресурсу: https://spotintelligence.com/2023/03/18/anomaly-detection-for-time-series (дата звернення: 18.12.2023).
[14] Система виявлення аномалій методами інтелектуального аналізу даних [Текст] / О. Хомич – Магістерська дисертація 2022 – 91с.
[15] Survey Threat Hunting: Focusing on the Hunters and How Best to Support Them [Текст] / M. Fuchs, J. Lemon – SANS Whitepaper, April 2023
[16] Top 10 Cloud Security Risks & Solution in 2023 & How to Tackle Them [Електронний ресурс] // Appinventiv – Режим доступу до ресурсу: https://appinventiv.com/blog/cloud-security-risks-and-solutions/ (дата звернення: 29.10.2023).
[17] Handle a false positive [Електронний ресурс] // CloudFare – Режим доступу до ресурсу: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adjust-rules/false-positive/ (дата звернення: 29.10.2023).
[18] Indicators of Compromise Confidence Scoring Method [Текст] / V. Tkach, O. Baranovskyi, A. Kudin, N. Godavarti, O. Kliok, S. Modali – The 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 7-9 September, 2023, Dortmund, Germany – 9с.
[19] How to Defend With the Courses of Action Matrix and Indicator Lifecycle Management [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/how-to-defend-with-the-courses-of-action-matrix-and-indicator-lifecycle-management/ (дата звернення: 29.10.2023).
[20] “Authorized” to break in: Adversaries use valid credentials to compromise cloud environments [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/posts/adversaries-use-valid-credentials-compromise-cloud-environments/ (дата звернення: 29.10.2023).
[21] Avoiding the Storm | How to Protect Cloud Infrastructure from Insider Threats [Електронний ресурс] // SentinelOne – Режим доступу до ресурсу: https://www.sentinelone.com/blog/avoiding-the-storm-how-to-protect-cloud-infrastructure-from-insider-threats/ (дата звернення: 29.10.2023).
[22] The Importance of User Behavior Analytics for Cloud Service Security [Електронний ресурс] // Oracle – Режим доступу до ресурсу: https://www.oracle.com/assets/user-behavior-analytics-3497541.pdf (дата звернення: 29.10.2023).
[23] QRadar User Behavior Analytics [Електронний ресурс] // IBM – Режим доступу до ресурсу: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-user-behavior-analytics (дата звернення: 29.10.2023).
[24] How to Maximize Telemetry Data Value With Observability Pipelines [Електронний ресурс] // DevOps IBM – Режим доступу до ресурсу: https://devops.com/how-to-maximize-telemetry-data-value-with-observability-pipelines/ (дата звернення: 29.10.2023).
[25] Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems [Текст] / Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai – IEEE Communications Magazine March 2012 – 146-154с.
[26] Reducing false positives in intrusion detection by means of frequent episodes [Текст] / L.O.

Gigstad - Master's Thesis Department of Computer Science and Media Technology Gjøvik University College, 2008 – 95c.
[27] Discovery of Frequent Episodes in Event Logs [Текст] / M. Leemans, W. M.P. van der Aalst – International Symposium on Data-Driven Process Discovery and Analysis – November 2014 – 15c.
[28] Павловский З. Введение в математическую статистику / [Текст] Пер. с польского. – М.: Статистика, 1967. – 285 с.
[29] Тюрин Ю.Н., Макаров А.А. Анализ данных на компьютере / [Текст] М.: Финансы и статистика, 1995. – 384 с.
[30] Emphasis on the Minimization of False Negatives or False Positives in Binary Classification – Sanskriti Singh [Електронний ресурс] // Arvix – Режим доступу до ресурсу: https://arxiv.org/pdf/2204.02526.pdf (дата звернення: 18.12.2023).
[31] Using Root Cause Analysis to Handle Intrusion Detection Alarms [Текст] / Klaus Julisch – IBM Zurich Research Laboratory, 2003 – 148c.
[32] Reduction of False Positives in Intrusion Detection Based on Extreme Learning Machine with Situation Awareness [Текст] / Donald A. Burgio - Doctoral dissertation, 2019 – 139c.
[33] Wazuh About us [Електронний ресурс] // Wazuh – Режим доступу до ресурсу: https://wazuh.com/about-us/ (дата звернення: 18.12.2023).