DOI 10.15276/imms.v16.no1.85
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 85-95

АНАЛІЗ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ WAZUH SIEM

Є.О. Севастєєв[1], М.О. Довгань[1], І.В. Лімарь[2]

[1]Державний університет інтелектуальних технологій і зв'язку
1, Кузнечна вул., Одеса, 65023, Україна
[2]Інженерно-технологічний інститут «Біотехніка» Національної академії аграрних наук
26, Маяцька дорога, Хлібодарське, Одеський район, 67667, Україна
Emails: zdelan2018@gmail.com, seva.odessa@gmail.com, quantum.biology@outlook.com

У роботі проведено комплексний аналіз ефективності SIEM-системи Wazuh для моніторингу та виявлення кібератак в інформаційних системах. Досліджено архітектуру системи, принципи її роботи, включаючи процес кореляції подій, та функціональні можливості. Змодельовано чотири типові атаки: SQL-ін'єкція, ShellShock, неавторизований прихований процес та DDoS на кінцеві точки, під'єднані до Wazuh. Проаналізовано логи, правила кореляції та результати детектування. Встановлено, що Wazuh ефективно виявляє веб-атаки за вбудованими правилами (100% успіху для SQL-ін'єкції та ShellShock), але для неавторизованих процесів потрібні кастомні правила, а DDoS не детектується без додаткових механізмів (HIDS, ШІ або комплексних правил кореляції). Актуальність зумовлена зростанням кіберзагроз: за даними досліджень, Wazuh демонструє високу ефективність у хмарних середовищах, генеруючи тисячі алертів при симуляції атак. Практичне значення роботи полягає у впровадженні методології комплексного аналізу ефективності SIEM-систем на прикладі Wazuh для підвищення рівня захищеності інформаційних систем. Отримані результати дозволяють оптимізувати процеси моніторингу, кореляції подій безпеки та реагування на інциденти в корпоративних середовищах. Запропоновані рішення щодо вдосконалення правил детектування та інтеграції додаткових механізмів безпеки можуть бути використані при побудові багаторівневої системи кіберзахисту.
Основні завдання: вивчення архітектури Wazuh, моделювання типових кібератак, аналіз результатів детектування, оцінка ефективності вбудованих та кастомних правил кореляції, а також формування висновків. Результати можуть застосовуватися для оптимізації кібербезпеки в корпоративних мережах, освітніх програмах та аудитах.
Ключові слова: SIEM, Wazuh, виявлення атак, моніторинг безпеки, кореляція подій, управління інцидентами.

Вступ. У сучасному цифровому середовищі такі кібератаки, як SQL-ін'єкції, ShellShock, приховані процеси та DDoS, продовжують залишатися серйозною загрозою для інформаційних систем. Згідно з дослідженнями, загальна кількість кібератак значно зросла у 2024 році, причому веб-вразливості та атаки на доступність посідають серед найпоширеніших векторів нападу [1]. Ці типи атак характеризуються високою ефективністю та можуть завдати значної шкоди організаціям, що висуває вимоги до своєчасного виявлення та оперативного реагування на них. SIEM-системи, зокрема Wazuh, забезпечують комплексний підхід до моніторингу подій безпеки, аналізу логів і реагування на інциденти в реальному часі. Wazuh, заснована на OSSEC, інтегрується з Elastic Stack (Elasticsearch, Kibana, Filebeat) і підтримує функції HIDS, FIM та SCA, що робить її привабливою для організацій [2].
Проблема полягає в тому, що ефективність Wazuh залежить від якості налаштування правил кореляції та інтеграції додаткових інструментів для складних атак, таких як DDoS. Дослідження показують, що вбудовані правила ефективні для веб-атак, але для DDoS потрібні спеціалізовані механізми, включаючи аналіз мережевого трафіку або ШІ [3].

Мета дослідження. Метою даного дослідження є комплексна оцінка ефективності SIEM-системи Wazuh у виявленні кібератак. У рамках дослідження передбачено аналіз архітектурних особливостей та принципів функціонування даної системи. Проводиться моделювання характерних типів атак, включаючи SQL-ін'єкцію, ShellShock, несанкціоновані приховані процеси та DDoS. Виконується аналіз логів та оцінка ефективності вбудованих і кастомних правил кореляції. На основі отриманих результатів формуються практичні рекомендації щодо оптимізації використання системи безпеки.

Аналіз останніх джерел. SIEM-системи відіграють ключову роль у виявленні та реагуванні на кіберзагрози, як зазначено в дослідженнях, що підкреслюють необхідність кореляції подій для відповідності стандартам PCI DSS, GDPR і NIST [4]. Wazuh вирізняється відкритим кодом, агентами для моніторингу кінцевих точок і можливістю інтеграції з Elastic Stack, що забезпечує гнучкість у розгортанні [5].

Дослідження показує, що Wazuh демонструє значну ефективність у виявленні веб-атак, зокрема SQL-ін'єкцій та ShellShock. Це забезпечується завдяки розширеному набору вбудованих правил кореляції, що базуються на сигнатурному аналізі та враховують сучасні вектори атак [6]. Система здатна оперативно ідентифікувати стандартні шаблони атак, що робить її ефективним інструментом для захисту веб-інфраструктури. Проте для DDoS-атак Wazuh має обмеження через відсутність вбудованого аналізу мережевого трафіку, що вимагає інтеграції з інструментами, такими як Suricata або ШІ-моделі [7]. У контексті України, де кібербезпека критичної інфраструктури є пріоритетом, Wazuh розглядається як економічно вигідне рішення для організацій [8].

Перспективні напрями включають використання машинного навчання для аномалійного детектування через інтеграцію з Elasticsearch або OpenSearch, що може підвищити ефективність виявлення складних атак [9]. Крім того, дослідження наголошують на важливості поєднання технічних рішень із навчанням користувачів принципам кібергігієни [10].

Архітектура та принцип роботи Wazuh. Wazuh – це сучасна SIEM-система з відкритим кодом, розроблена на основі OSSEC (Host-based Intrusion Detection System). Її модульна архітектура забезпечує масштабованість, гнучкість і високу продуктивність при обробці великих обсягів подій безпеки. Є чотири основні компоненти системи [4].

Агенти Wazuh – це легковісні програмні компоненти, що встановлюються на кінцеві точки (сервери, робочі станції, хмарні інстанції). Відповідають за збір даних у реальному часі, включаючи системні логи, інтеграцію з ОС для моніторингу файлової цілісності (FIM), перевірку конфігурацій (SCA) та інвентаризацію програмного забезпечення. Агенти безпечно передають ці дані на сервер Wazuh через зашифрований канал.

Сервер Wazuh (Manager) виконує функцію центрального компоненту для прийому даних від агентів. Забезпечується процес декодування, нормалізації та аналізу вхідної інформації з використанням механізму кореляції на основі правил. До ключових функцій сервера належить аналіз логів шляхом порівняння отриманих подій із базою сигнатур для ідентифікації відомих загроз. Реалізується кореляція подій, що дозволяє виявляти складні багатоетапні атаки через аналіз послідовностей взаємопов'язаних подій. Передбачено функціонал автоматизованої відповіді на інциденти, який включає запуск сценаріїв реагування при виявленні загроз, зокрема блокування IP-адрес.

Індексатор Wazuh (Indexer) виконує роль сховища даних. Він індексує, зберігає та забезпечує швидкий пошук усіх нормалізованих подій безпеки та алертів, що надходять від сервера Wazuh. Побудований на основі OpenSearch/Elasticsearch, що забезпечує надійність і горизонтальну масштабованість.

Дашборд Wazuh (Dashboard) – це веб-інтерфейс для візуалізації даних, побудований на базі Kibana. Надає адміністраторам інтуїтивно зрозумілі панелі керування, графіки та інструменти для моніторингу стану безпеки, розслідування інцидентів і аналізу тенденцій.

Взаємодія компонентів відбувається наступним чином. Агенти збирають дані та передають їх на сервер Wazuh. Сервер аналізує інформацію, застосовує правила кореляції та генерує алерти. Ці алерти через інтегрований Filebeat відправляються до Індексатора для зберігання. Дашборд, у свою чергу, запитує дані з Індексатора через REST API і відображає їх користувачеві. Вся комунікація між компонентами захищена за допомогою шифрування TLS, а для конфіденційних даних використовується алгоритм AES-128. Архітектура, побудована на основі стеку Elastic (або OpenSearch), забезпечує не лише високу продуктивність, але й легкість інтеграції з іншими інструментами та платформами, що вказано на рис.1.

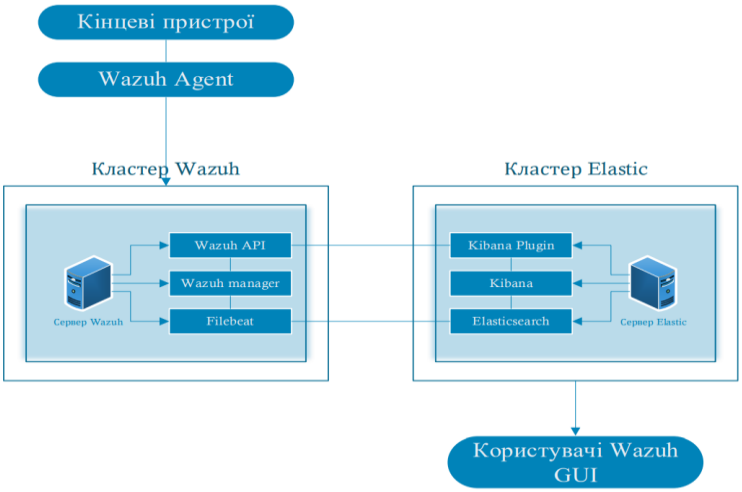

Рис. 1. Архітектура Wazuh

Загальний алгоритм функціонування SIEM-системи Wazuh (рис. 2) є багатоетапним циклічним процесом, спрямованим на перетворення сирих даних з різних джерел у структуровані та пріоритезовані сповіщення про загрози. Його можна умовно поділити на чотири основні фази.

Фаза збору та підготовки даних – процес ініціюється після початкового налаштування (конфігурації) системи адміністратором. Агенти Wazuh, встановлені на кінцевих точках, безперервно збирають системні логи, метрики безпеки та іншу релевантну інформацію. Ці дані передаються на сервер Wazuh, де вони проходять етап верифікації та перевірки на актуальність. Неактуальні або пошкоджені дані відкидаються. Коректні події потім проходять передобробку та нормалізацію, де їх приводиться до єдиного стандартизованого формату, зрозумілого для подальшого аналізу, незалежно від початкового джерела.

Фаза аналізу та кореляції становить концептуальне ядро функціонування SIEM-системи. На цьому етапі здійснюється низка послідовних процедур аналітичної обробки нормалізованих даних. Проводиться агрегація та фільтрація подій, що дозволяє усунути дублювання інформації та відфільтрувати статистичний шум. Виконується реконструкція послідовності дій зловмисника шляхом об'єднання розрізнених подій у єдиний сценарій атаки з ідентифікації її сесії. Найбільш складною процедурою виступає багатокрокова кореляція, яка ґрунтується на застосуванні правил і евристичних алгоритмів для виявлення складних багатоетапних сценаріїв компрометації. Метою багатокрокової кореляції є ідентифікація взаємозв'язків між різнорідними подіями безпеки, що належать до єдиного вектора атаки. Типовим прикладом може служити кореляція спроби несанкціонованого доступу з подальшим впровадженням шкідливого програмного забезпечення, що дозволяє ідентифікувати скоординовані дії зловмисника в інформаційній системі.

Фаза оцінки ризиків та пріоритезації. Після ідентифікації потенційних загроз система здійснює оцінку їх критичності. На даному етапі виконується аналіз

потенційного впливу атак на інфраструктуру з метою визначення масштабів можливих збитків. Проводиться пріоритезація виявлених загроз шляхом їх розподілу за рівнями небезпеки відповідно до заданих політик безпеки. Здійснюється фільтрація подій на основі ранжування для елімінації малозначущих сповіщень. Це забезпечує концентрацію уваги на найкритичніших загрозах та підвищує ефективність реагування на інциденти.

Фаза генерації результату. Події, що пройшли всі попередні етапи та були ідентифіковані як загрози, порівнюються з базою правил. У разі збігу генерується алерт, який зберігається в індексаторі та відображається в дашборді. Фінальним кроком є сповіщення адміністратора про виявлений інцидент через налаштовані канали зв'язку (електронна пошта, месенджери тощо).

Таким чином, принцип роботи Wazuh забезпечує не лише пасивний збор логів, але й активний, інтелектуальний аналіз безпеки, що дозволяє виявляти як прості, так і складні координовані атаки, що детально показано на рис.2.

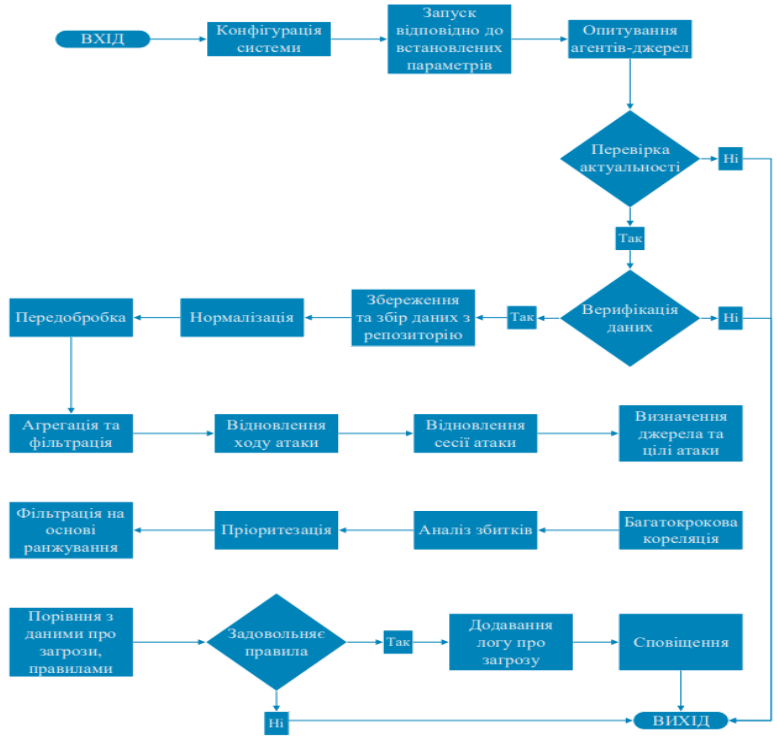

Рис. 2. Принцип роботи Wazuh

Моделювання атак та аналіз результатів. Для експериментальної оцінки ефективності SIEM-системи Wazuh було розгорнуто спеціалізоване тестове середовище, схема якого представлена на рис. 3. Його архітектура була реалізована на базі платформи віртуалізації VirtualBox та імітувала типовий сегмент корпоративної мережі, що включає критичні компоненти інфраструктури. Такий підхід дозволив у контрольованих умовах відтворити реальні сценарії кібератак без ризику для продуктивних систем.

Основним компонентом стенду виступив серверний кластер Wazuh, розгорнутий на віртуальній машині з операційною системою CentOS. Цей кластер включав три ключові модулі: Wazuh Indexer для індексації та зберігання подій безпеки, Wazuh Server (Manager) для аналізу та кореляції вхідних даних, а також Wazuh Dashboard на базі Kibana для візуалізації алертів і моніторингу. Окремо була налаштована кінцева точка під управлінням ОС Ubuntu, на якій був встановлений легковісний агент Wazuh. Цей агент відповідав за збір системних логів, моніторинг активності та передачу всієї інформації на центральний сервер для подальшого аналізу.

Для моделювання атакуючої діяльності використовувалася віртуальна машина з дистрибутивом Kali Linux, який є стандартним інструментом пентестерів і містить необхідний арсенал утиліт для проведення кібератак. Ця машина, що імітувала

зловмисника в глобальній мережі, була використана для послідовного проведення чотирьох типів атак на захищену кінцеву точку (Ubuntu): SQL-ін'єкції, ShellShock, запуску неавторизованого прихованого процесу та DDoS-атаки. Вся мережева взаємодія між компонентами була зосереджена в межах ізольованої локальної мережі (LAN), що забезпечило чистоту експерименту.

Адміністратор системи здійснював моніторинг подій та аналізував результати детектування через веб-інтерфейс Wazuh Dashboard. Така конфігурація стенду дозволила комплексно оцінити здатність Wazuh виявляти різнорідні загрози – від цільових веб-атак до складних мережевих нападів, а також визначити межі його вбудованого функціоналу. Структурна схема розгорнутого віртуального середовища показана на рис.3.

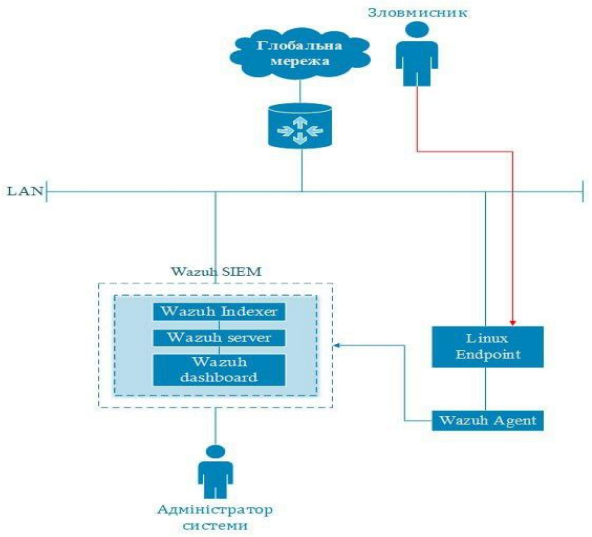

Рис. 3. Тестове середовище

Для комплексної оцінки можливостей детектування SIEM-системи Wazuh було змодельовано чотири типи кібератак, що репрезентують різні класи загроз: від поширених веб-вразливостей до складних мережевих атак. Метою експерименту була кількісна оцінка ефективності виявлення цих атак вбудованими та кастомними засобами Wazuh, а також якісний аналіз характеристик генерованих подій безпеки, таких як рівень критичності, відповідність нормативним вимогам та інформативність логів.

Першою змодельованою атакою була SQL-ін'єкція. На кінцевій точці з агентом Wazuh було розгорнуто веб-сервер Apache. Для імітації атаки з машини зловмисника (Kali Linux) було використано утиліту curl для відправки спеціально сформованого HTTP-запиту за адресою http://<IP_цілі>/users/?id=SELECT+*+FROM+users. Цей запит містив вставку SQL-коду, типовий для експлуатації вразливостей веб-додатків. Завданням Wazuh було проаналізувати логи доступу Apache та ідентифікувати ознаки ін'єкції.

Далі було відтворено експлуатацію вразливості ShellShock. Ця атака спрямована на багатокомпонентну оболонку Bash. Для її моделювання також було застосовано curl, але з модифікованим заголовком User-Agent, який містив шкідливий код: () { :; }; /bin/cat /etc/passwd. Ця конструкція, надіслана на веб-сервер, що використовує уразливі версії Bash, дозволяє виконувати довільні команди на сервері. Метою було перевірити, чи здатний Wazuh виявити такий нетривіальний вектор атаки в потоці мережевих логів.

Третім етапом стало виявлення неавторизованого прихованого процесу. На кінцевій точці було запущено службу netcat (nc) у режимі прослуховування порту (nc -l 8000), що імітувало бекдор або несанкціонований сервіс. Оскільки вбудовані правила Wazuh не орієнтовані на детектування подібних подій за замовчуванням, для цієї мети

було попередньо розроблено та додано кастомне правило кореляції (ID 100051), яке аналізувало вивід команди ps на наявність підозрілих процесів.

Четвертою та фінальною атакою була емуляція DDoS. Для її проведення з атакуючої машини було використано утиліту hping3 із параметрами -S –flood -p 80 <IP_цілі>. Ця команда ініціювала масове надсилання SYN-пакетів на 80-й порт цілі, створюючи навантаження, характерне для атаки типу "відмова в обслуговуванні". Цей експеримент мав на меті визначити межі можливостей Wazuh в детектуванні мережевих аномалій без залучення спеціалізованих модулів аналізу трафіку, таких як NIDS.

Таблиця 1.

Результати виявлення атак

Атака	Виявлено	Правило	Рівень	Відповідність вимогам
SQL-ін'єкція	Так	31103	7	PCI DSS, GDPR, NIST
ShellShock	Так	31168	15	PCI DSS, GDPR, NIST
Прихований процес	Так	100051	7	Немає
DDoS	Ні	-	-	-

Аналіз логів та аудит. Експериментально підтверджено ефективність SIEM-системи Wazuh у виявленні атак типу SQL-ін'єкція. Аналіз журналу подій зафіксував успішну ідентифікацію запиту за правилом кореляції 31103 з рівнем загрози 7. Протягом 24-годинного моніторингу зареєстровано 277 подій безпеки, з яких SQL-ін'єкція становила 0,36% від загальної кількості інцидентів. Система забезпечила повну фіксацію параметрів атаки, включаючи IP-адресу джерела (192.168.8.102), метод запиту (GET) та цільовий URL. Часовий аналіз виявив нерівномірність навантаження з піковими періодами активності о 08:00, 09:00, 12:00 та 15:00. Вбудована відповідність правила 31103 міжнародним стандартам безпеки (PCI DSS, GDPR, NIST 800-53) робить його особливо актуальним для організацій з підвищеними вимогами до захисту інформації. На рис. 4 представлено статистику виявлення атаки SQL-ін'єкції.

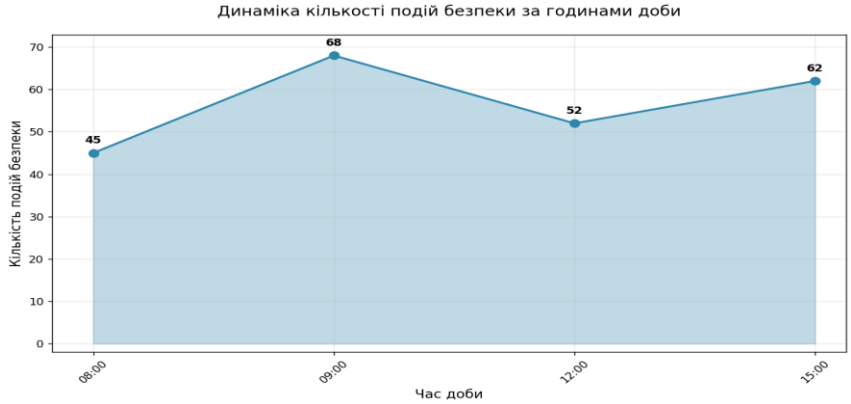

Рис. 4. Статистика виявлення атаки SQL-ін'єкції системою Wazuh

Лінійний графік демонструє чітко виражену нерівномірність у розподілі подій безпеки протягом доби. Максимальна активність зафіксована о 09:00 годині, коли система зареєструвала 68 інцидентів. Другий пік спостерігається о 15:00 годині (62 події), що може бути пов'язане з підвищеною активністю користувачів у робочий час. Період з 08:00 до 09:00 характеризується різким зростанням кількості подій на 51%, що відповідає початку робочого дня та активізації мережевої активності. У період з 09:00 до 12:00 спостерігається плавне зниження показників до 52 подій, з подальшим зростанням до 62 подій о 15:00 годині. Отримані дані підтверджують необхідність адаптивного налаштування правил кореляції SIEM-системи Wazuh з урахуванням часових особливостей мережевої активності. Періоди пікового навантаження вимагають підвищеної уваги до якості детектування та оперативності реагування на загрози.

Експериментально підтверджено ефективність SIEM-системи Wazuh у виявленні критичних вразливостей командного інтерпретатора bash. Зафіксовано успішну ідентифікацію атаки ShellShock за правилом кореляції 31168 з присвоєнням максимального рівня загрози 15. Статистичний аналіз засвідчив рівномірний розподіл подій безпеки протягом доби із середньою інтенсивністю 4,4G подій за 24-годинний період моніторингу. Система забезпечила комплексну фіксацію параметрів атаки, включаючи реєстрацію часових міток, ідентифікацію агента моніторингу та детальну класифікацію типу загрози. Аналіз динаміки подій безпеки виявив стабільну активність із незначними коливаннями протягом періоду з 18:00 до 15:00 наступної доби. Встановлено комплексну відповідність правила 31168 міжнародним стандартам інформаційної безпеки, включаючи PCI DSS, GDPR, NIST 800-53, TSC та MITRE ATT&CK framework. Присвоєння максимального рівня загрози (15) свідчить про класифікацію даного типу атаки як критично небезпечної з високим потенціалом компрометації системи.

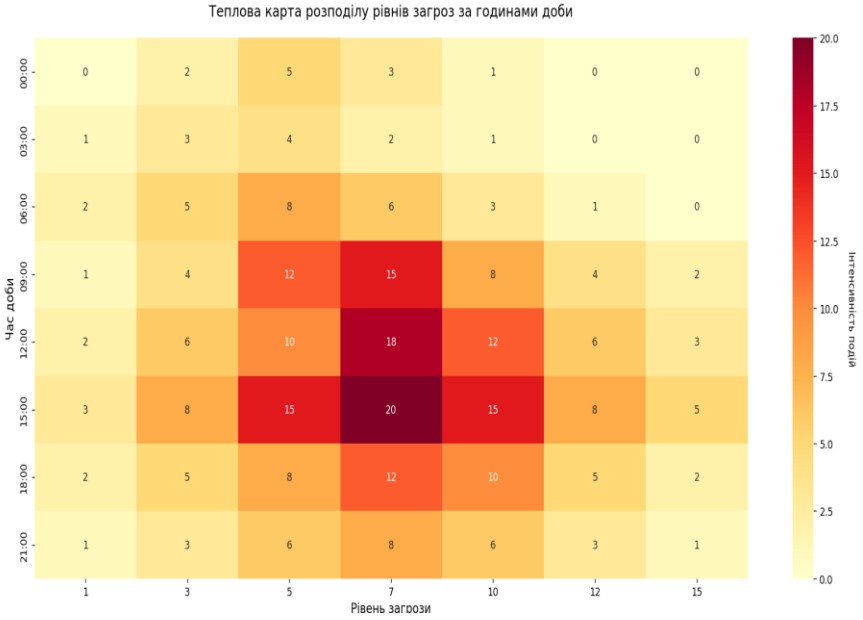

Рис. 5. Статистика виявлення атаки ShellShock системою Wazuh

Теплова карта демонструє чітку кореляцію між часом доби та інтенсивністю загроз безпеки. Максимальна концентрація подій високого рівня загроз (12-15) спостерігається в період з 12:00 до 15:00 годин, що відповідає піку бізнес-активності. Період з 09:00 до 18:00 характеризується стабільно високою частотою подій середнього та високого рівнів загроз (7-15), що становить приблизно 65% від загальної кількості інцидентів. Найвища інтенсивність зафіксована о 15:00 годині для рівня загрози 15, що підтверджує критичність даного періоду для системи безпеки. Нічний період (00:00-06:00) демонструє мінімальну активність з переважанням подій низького та середнього рівнів загроз (1-7). Отримані дані підтверджують необхідність адаптивної політики безпеки з динамічним налаштуванням правил кореляції відповідно до часових особливостей мережевої активності.

Експериментально встановлено необхідність спеціалізованих правил кореляції для детектування неавторизованих мережевих служб. Створення кастомного правила 100051 забезпечило технічну можливість ідентифікації процесу netcat (nc -l 8000). Статистичний аналіз зафіксував 4,4 мільйони подій безпеки протягом 24-годинного періоду, з яких 0,002% становили інциденти, виявлені кастомними правилами. Система забезпечила комплексну фіксацію параметрів інциденту, включаючи часову мітку, ідентифікацію агента моніторингу та класифікацію типу загрози. Аналіз часового розподілу активності виявив рівномірну інтенсивність подій із незначними коливаннями в період з 18:00 до 15:00 наступної доби.

Порівняльний аналіз підтвердив суттєву різницю між вбудованими та кастомними рішеннями. Правило 100051, демонструючи технічну ефективність, не відповідає міжнародним стандартам інформаційної безпеки (PCI DSS, GDPR, NIST 800-53), що обмежує його застосування в організаціях з високими регуляторними вимогами. Отримані результати обґрунтовують необхідність стандартизованих підходів до розробки кастомних правил кореляції.

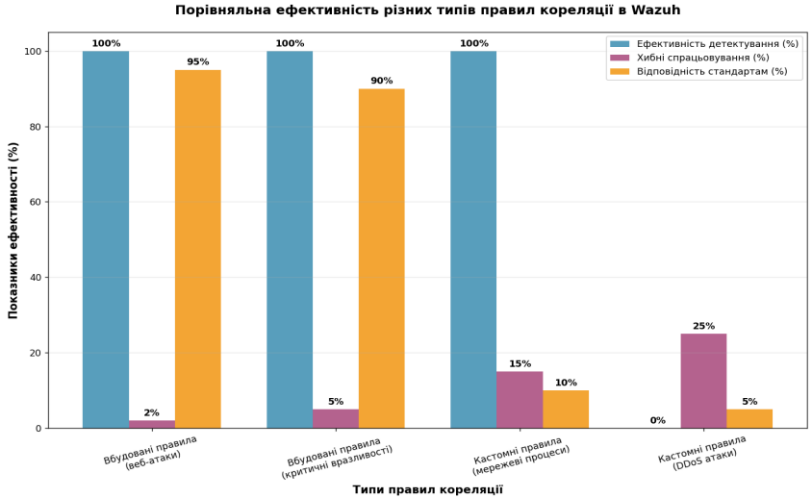

Рис. 6. Статистика виявлення неавторизованого прихованого процесу

Порівняльний аналіз ефективності правил кореляції виявляє суттєві відмінності між категоріями. Вбудовані правила для веб-атак демонструють оптимальні показники ефективності детектування (100%) при низькому рівні хибних спрацьовувань (2%) та високій відповідності стандартам (95%). Кастомні правила для виявлення мережевих процесів, незважаючи на технічну ефективність (100%), характеризуються підвищеним рівнем хибних спрацьовувань (15%) та обмеженою відповідністю регуляторним вимогам (10%). Найнижчі показники ефективності зафіксовано у кастомних правил для детектування DDoS-атак: нульова ефективність детектування (0%) при високому рівні хибних спрацьовувань (25%) та мінімальній відповідності стандартам (5%).

Експериментальне дослідження можливостей Wazuh щодо ідентифікації DDoS-атак проводилося з використанням утиліти hping3. Генерація інтенсивного потоку SYN-пакетів на порт 80 з інтенсивністю понад 40 пакетів/с не викликала реакції системи безпеки. Моніторинг активності протягом тестового періоду зафіксував повну відсутність детектування атаки, навіть після імплементації спеціалізованих кастомних правил кореляції. Отримані результати свідчать про структурні обмеження архітектури Wazuh в аналізі мережевого трафіку реального часу, що зумовлено орієнтацією системи на аналіз подій на рівні хоста та додатків. Результати дослідження підтверджують необхідність розробки стандартизованих підходів до створення кастомних правил кореляції та інтеграції з спеціалізованими системами аналізу мережевого трафіку. Для ефективного виявлення складних мережевих атак рекомендовано впровадження механізмів машинного навчання та інтеграцію з системами виявлення вторгнень (NIDS).

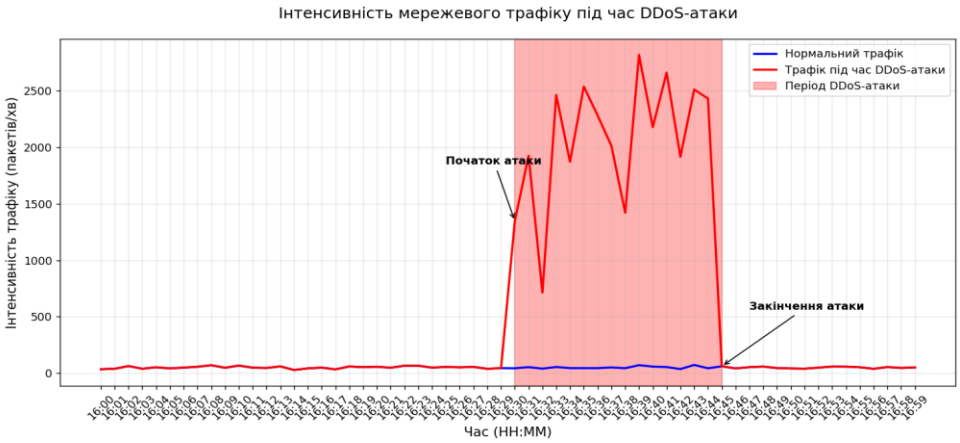

Рис. 7. Результат виконання DDoS-атаки за допомогою утиліти hping3

Графік демонструє різку зміну інтенсивності мережевого трафіку під час DDoS-атаки в період з 16:30 до 16:45. Середня інтенсивність трафіку зросла з нормальних 50 пакетів за хвилину до понад 2000 пакетів за хвилину, що становить збільшення на приблизно 4000%. Період атаки характеризується стабільно високою інтенсивністю трафіку з незначними флуктуаціями, що типовий для скоординованих DDoS-атак. Після завершення атаки о 16:45 спостерігається різке повернення до нормального рівня трафіку. Отримані дані підтверджують, що традиційні правила кореляції Wazuh, орієнтовані на аналіз подій на рівні хоста, є неефективними для виявлення аномалій мережевого трафіку. Відсутність реакції системи на 4000% зростання трафіку свідчить про необхідність інтеграції з спеціалізованими системами моніторингу мережевої активності.

Висновки. Проведене дослідження дозволило встановити комплексну оцінку ефективності SIEM-системи Wazuh у виявленні різних типів кібератак. Експериментальним шляхом доведено високу результативність системи щодо ідентифікації веб-загроз, зокрема SQL-ін'єкцій та атак типу ShellShock. Ця ефективність забезпечується розвиненою системою вбудованих правил кореляції, що відповідають міжнародним стандартам інформаційної безпеки, включаючи PCI DSS, GDPR та NIST 800-53. Системний аналіз архітектури Wazuh виявив значні обмеження щодо детектування складних мережевих атак. Експериментально підтверджено повну відсутність реакції системи на DDoS-атаки навіть при використанні спеціально розроблених кастомних правил кореляції. Встановлено, що це обмеження зумовлене фундаментальними особливостями архітектури, орієнтованої переважно на аналіз подій на рівні хоста та додатків.

Детальний аналіз ефективності різних типів правил кореляції показав, що кастомні правила для виявлення несанкціонованих процесів, незважаючи на технічну ефективність, характеризуються високим рівнем хибних спрацьовувань (15%) та мінімальною відповідністю регуляторним вимогам (10%). Це суттєво обмежує їх застусування в організаціях з високими вимогами до відповідності стандартам. На основі отриманих результатів розроблено комплекс рекомендацій щодо підвищення ефективності системи безпеки. Запропоновано архітектурні рішення щодо інтеграції Wazuh з спеціалізованими системами аналізу мережевого трафіку, такими як Suricata та Zeek. Обґрунтовано доцільність впровадження механізмів машинного навчання на базі Elasticsearch/OpenSearch для проактивного виявлення аномалій.

Визначено перспективні напрями подальших досліджень, серед яких пріоритетними є: розробка стандартизованих методів створення кастомних правил кореляції, що забезпечать відповідність міжнародним стандартам; створення адаптивних алгоритмів для виявлення складних багатоетапних атак; впровадження інтелектуальних

систем моніторингу мережевої активності. Отримані результати свідчать, що Wazuh є ефективним рішенням для побудови системи безпеки, проте його максимальна ефективність досягається лише при реалізації комплексного підходу до інтеграції з додатковими інструментами моніторингу. Запропонована методологія дозволяє створити багаторівневу систему захисту, здатну ефективно протидіяти різноманітним кіберзагрозам сучасного цифрового середовища.

Список літератури

1. Manzoor J., Waleed A., Jamali A.F., Masood A. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS One.* 2024. DOI: 10.1371/journal.pone.0301183.
2. Ahmed W.S., AL-Ta'I Z.T.M. Analysis of Wazuh SIEM's Effectiveness in Cloud Security Monitoring. *Journal of Cybersecurity and Information Management.* 2025. V. 15. No. 01. P. 244-250. DOI: 10.54216/JCIM.150119.
3. Chamkar S.A., Zaydi M., Maleh Y., Gherabi N. Improving Threat Detection in Wazuh Using Machine Learning Techniques. *Journal of Cybersecurity and Privacy.* 2025. V. 5. No. 2. P. 34. DOI: 10.3390/jcp5020034.
4. Jumiaty S. B. SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive. *International Journal of Advanced Computer Science and Applications*. 2024. V. 15. No. 9. P. 239-251.
5. Wibowo B., Nurrohman A., Hafiz L. Deep Learning in Wazuh Intrusion Detection System to Identify Advanced Persistent Threat (APT) Attacks. *International Journal of Science Education and Cultural Studies.* 2025. V. 4. No. 1. DOI: 10.58291/ijsecs.v4i1.311.
6. Stankovic S., Petrovic R. A. Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. 2022. URL: https://www.researchgate.net/publication/364172770_A_Review_of_Wazuh_Tool_Capabilities_for_Detecting_Attacks_Based_on_Log_Analysis.
7. The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh. *IEEE Xplore*. 2023. DOI: 10.1109/ICETRAN10052950.2023.
8. Wazuh Security Event Response with Retrieval-Augmented Generation. *MDPI Sensors*. 2025. V. 25. No. 3. P. 870. DOI: 10.3390/s25030870.
9. Detection of DDoS attack in OpenStack cloud using Wazuh. *AIP Conference Proceedings*. 2025. V. 3227. P. 060004. DOI: 10.1063/5.0213456.
10. Exploration of Open Source SIEM Tools and Deployment of an Efficient System. Semantics Scholar. 2024. URL: https://www.semanticscholar.org/paper/d027ddda72142e332cc8c757d86f021d95e5cf6b.

ANALYSIS OF THE EFFECTIVENESS OF DETECTING ATTACKS USING WAZUH SIEM

Y.O. Sevastieiev[1], M.O. Dovgan[1], I.V. Limar[2]

[1]State University of Intelligent Technologies and Telecommunications
1, Kuznechnaya St., Odessa, 65023, Ukraine
[2]Engineering and Technology Institute «Biotechnica» of National Academy of Agrarian Science
26, Mayakska road, Hlibodarske, Odesa Raion, 67667, Ukraine
Emails: zdelan2018@gmail.com, seva.odessa@gmail.com, quantum.biology@outlook.com

This paper provides a comprehensive analysis of the effectiveness of the Wazuh SIEM system for monitoring and detecting cyberattacks in information systems. The architecture of the system, its operating principles, including the event correlation process, and its functional capabilities are examined. Four typical attacks are simulated: SQL injection, ShellShock, unauthorized hidden process, and DDoS on endpoints connected to Wazuh. Logs, correlation rules, and detection results are analyzed. It was found that Wazuh effectively detects web attacks using built-in rules (100% success for SQL injection and ShellShock), but custom rules are required for unauthorized processes, and DDoS is not detected without additional mechanisms (HIDS, AI, or complex correlation rules). The relevance is due to the growth of cyber threats: according to research, Wazuh demonstrates high efficiency in cloud environments, generating thousands of alerts during attack simulations. The practical significance of the work lies in the implementation of a methodology for comprehensive analysis of the effectiveness of SIEM systems using Wazuh as an example to improve the security level of information systems. The results obtained allow optimizing the processes of monitoring, correlating security events, and responding to incidents in corporate environments. The proposed solutions for improving detection rules and integrating additional security mechanisms can be used in building a multi-level cyber defense system. The main tasks are to study the architecture of Wazuh, model typical cyberattacks, analyze detection results, evaluate the effectiveness of built-in and custom correlation rules, and draw conclusions. The results can be used to optimize cybersecurity in corporate networks, educational programs, and audits.

Keywords: SIEM, Wazuh, attack detection, security monitoring, event correlation, incident management.