

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра на тему:
«Методи та технології аналізу поведінки користувачів на
основі Graylog для виявлення витоків даних та
внутрішніх загроз»

Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Ілля Ковальчук

Керівник доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена Головня

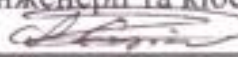
Рецензент проф. кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 А.А. Єфіменко
" 17 " вересня 2024 року

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студента: Ковальчука Іллі Володимировича

Тема проекту: Методи та технології аналізу поведінки користувачів на основі Graylog для виявлення витоків даних та внутрішніх загроз.

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 26 грудня 2024 р.

Вихідні дані до роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес аналізу поведінки користувачів в корпоративних мережах.

У рамках дослідження буде здійснено:

1. аналіз існуючих підходів до моніторингу та аналізу поведінки користувачів;
2. розробка архітектури підсистеми на базі Graylog;
3. налаштування Graylog для збору та обробки логів;
4. створення аналітичних правил та дашбордів для виявлення аномальної активності;
5. тестування та оцінка ефективності розробленої підсистеми.

Консультанти випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються:

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
1	Фальковський І.Г.	05.09.2024	05.09.2024
2	Фальковський І.Г.	17.10.2024	17.10.2024
3	Фальковський І.Г.	25.11.2024	25.11.2024

Студент І.В. Ковальчук

Керівник О.С. Головня

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	07.09.2024 р.	виконано
2	Аналіз літературних джерел	15.09.2024 р.	виконано
3	Аналіз об'єкта дослідження	20.09.2024 р.	виконано
4	Подача чернетки керівнику для перевірки	03.10.2024 р.	виконано
5	Проектування структури системи	19.10.2024 р.	виконано
6	Розробка архітектури системи	26.10.2024 р.	виконано
7	Розробка рішень, моделей та алгоритмів	07.11.2024 р.	виконано
8	Реалізація проекту та його налаштування	14.11.2024 р.	виконано
9	Аналіз ефективності роботи системи	27.11.2024 р.	виконано
10	Тестування працездатності	30.11.2024 р.	виконано
11	Написання пояснювальної записки	10.12.2024 р.	виконано
12	Підготовка додаткових матеріалів	16.12.2024 р.	виконано
13	Отримання відгуку та рецензії на кваліфікаційну роботу	20.12.2024 р.	виконано
14	Захист кваліфікаційної роботи	Згідно з розкладом	виконано

Студент І.В. Ковальчук

Керівник О.С. Головня

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи магістра складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 65 сторінках друкованого тексту. Пояснювальна записка має 5 сторінок додатків. Список використаних джерел містить 21 найменування і займає 2 сторінки. В роботі наведено 39 рисунків. Загальний обсяг роботи – 78 сторінок.

Мета роботи – розробка системи аналізу поведінки користувачів на основі платформи Graylog для виявлення витоків даних і внутрішніх загроз у корпоративних мережах.

У кваліфікаційній роботі проведено аналіз сучасних методів моніторингу поведінки користувачів, розглянуто особливості SIEM-систем та обґрунтовано вибір Graylog як основної платформи для реалізації системи. Спроектовано архітектуру підсистеми безпеки, налаштовано збір і обробку логів, розроблено аналітичні правила та дашборди для виявлення аномальної активності. Виконано інтеграцію з іншими сервісами та технологіями, проведено тестування працездатності та оцінку ефективності запропонованого рішення. Результати роботи підтверджують доцільність використання системи для підвищення рівня інформаційної безпеки та своєчасного виявлення загроз.

Ключові слова: GRAYLOG, SIEM, КІБЕРБЕЗПЕКА, ВИТОКИ ДАНИХ, ВНУТРІШНІ ЗАГРОЗИ, ЛОГУВАННЯ.

ANNOTATION

The explanatory note for the master's qualification thesis consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual portion spans 65 pages of printed text. The explanatory note includes 5 pages of appendices. The list of references contains 21 entries and occupies 2 pages. The thesis contains 39 figures. The total volume of the thesis is 78 pages.

Objective of the thesis: To develop a user behavior analysis system based on the Graylog platform for detecting data leaks and internal threats in corporate networks.

The qualification thesis includes an analysis of modern methods for monitoring user behavior, an examination of the features of SIEM systems, and a justification for selecting Graylog as the primary platform for implementing the system. The security subsystem architecture was designed, log collection and processing were configured, analytical rules and dashboards for detecting anomalous activity were developed. Integration with other services and technologies was performed, and the system's functionality was tested along with an evaluation of the proposed solution's effectiveness. The results confirm the feasibility of using the system to enhance information security and ensure the timely detection of threats.

Keywords: GRAYLOG, SIEM, CYBERSECURITY, DATA LEAKS, INTERNAL THREATS, LOGGING.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ ВИЯВЛЕННЯ ВИТОКІВ ДАНИХ ТА ВНУТРІШНІХ ЗАГРОЗ.....	10
1.1 Аналіз поняття SIEM систем та їх важливості в корпоративних мережах.	10
1.2 Вибір Graylog як платформи для захисту в порівнянні з іншими SIEM.....	18
1.3 Огляд функціональних можливостей Graylog	22
РОЗДІЛ 2 ПРОЕКТУВАННЯ АРХІТЕКТУРИ ПІДСИСТЕМИ НА ОСНОВІ SIEM.....	30
2.1 Топологія мережі та архітектура системи Graylog.....	30
2.2 Інтеграція Graylog з Active Directory та іншими технологіями для безпеки користувачів	34
2.3. Визначення типів подій та логів для моніторингу	38
2.4 Додаткові технології для розширення можливостей системи	41
РОЗДІЛ 3 РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ ТА ДОСЛІДЖЕННЯ ЇЇ РОБОТИ.....	45
3.1. Встановлення Graylog та його компонентів.....	45
3.2 Налаштування індексів, колекторів логів та правил виявлення інцидентів.....	49
3.3 Налаштування інтеграції системи з Active Directory та створення звітів для моніторингу та аналізу подій.....	55
3.4 Аналіз ефективності роботи підсистеми та тестування правил виявлення інцидентів та сповіщень	60
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

AD – Active Directory

SIEM - Security Information & Event Management

SEM - Security event management

SIM - Security information management

UEBA - User and Entity Behavior Analytics

SOAR - Security Orchestration, Automation and Response

SOC - Security Operations Center

MTTR - Mean Time to Repair

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

LDAP - Lightweight Directory Access Protocol

ВСТУП

Захист конфіденційної інформації та запобігання витокам даних стають все більш актуальними завданнями в умовах постійного розвитку інформаційних технологій та зростаючої кількості кіберзагроз. У цьому контексті системи аналізу поведінки користувачів стають надзвичайно важливими інструментами для виявлення витоків даних та внутрішніх загроз.

Ця кваліфікаційна магістерська робота спрямована на вивчення та розробку системи аналізу поведінки користувачів на основі платформи Graylog з метою ефективного виявлення витоків даних та внутрішніх загроз у корпоративних мережах.

Актуальність теми. Сьогодення відзначається зростанням кількості кібератак, спрямованих на підприємства та організації різних галузей. Величезний обсяг конфіденційної інформації, що зберігається в цифровому форматі, робить їх особливо вразливими перед потенційними загрозами. Водночас, існуючі методи та засоби захисту часто виявляються неефективними перед сучасними та ретельно обдуманими кібератаками.

Загострення ситуації вимагає постійного вдосконалення методів та інструментів виявлення та запобігання загрозам кібербезпеки. Серед сучасних методів та технологій важливу роль виконує аналіз поведінки користувачів, який передбачає не лише дослідження технічних параметрів, а й діяльності користувачів у мережі.

Метою даної роботи є розробка системи аналізу поведінки користувачів на базі платформи Graylog для виявлення витоків даних та внутрішніх загроз у корпоративних мережах.

Для досягнення визначеної мети роботи передбачаються наступні завдання:

1. Аналіз сучасних методів та інструментів виявлення витоків даних та внутрішніх загроз.

2. Розробка алгоритмів аналізу поведінки користувачів на основі платформи Graylog.

3. Реалізація системи аналізу поведінки користувачів на основі отриманих алгоритмів.

4. Тестування та оцінка ефективності розробленої системи.

Об'єктом дослідження є процес аналізу поведінки користувачів в корпоративних мережах.

Предметом дослідження є застосування систем аналізу поведінки користувачів для виявлення витоків даних та внутрішніх загроз.

У рамках дослідження буде здійснено аналіз існуючих підходів до моніторингу та аналізу поведінки користувачів, розробка архітектури підсистеми на базі Graylog, налаштування Graylog для збору та обробки логів, створення аналітичних правил та дашбордів для виявлення аномальної активності, тестування та оцінка ефективності розробленої підсистеми.

Реалізація даної підсистеми сприятиме підвищенню рівня інформаційної безпеки організацій, забезпечуючи їх надійний захист від внутрішніх загроз та витоків даних.

РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ ВИЯВЛЕННЯ ВИТОКІВ ДАНИХ ТА ВНУТРІШНІХ ЗАГРОЗ

1.1 Аналіз поняття SIEM систем та їх важливості в корпоративних мережах

SIEM (Security Information & Event Management) - це кібербезпекова платформа, яка централізує інформацію про безпеку з різних кінцевих точок, серверів, додатків та інших джерел, щоб допомогти моніторити IT-інфраструктуру, виявляти аномалії в реальному часі, сповіщати професіоналів з безпеки про будь-які аномальні події та зберігати детальні журнали всіх подій (аномальних, негативних чи звичайних) - часто за допомогою інструментів, таких як бази даних загроз, штучний інтелект, автоматизація та інші.[1]

SIEM - це рішення, яке комбінує два старі інструменти: SIM (управління інформацією про безпеку) та SEM (управління подіями безпеки). Сучасні системи SIEM також містять технології Security Orchestration, Automation and Response (SOAR) та User and Entity Behavior Analytics (UEBA) для автоматизації реакції на загрози та виявлення загроз на основі відхилень від звичайної діяльності, відповідно (рис. 1.1).

Разом вони прискорюють виявлення та вирішення подій та інцидентів з безпеки всередині IT-середовища. Вони пропонують експертам з кібербезпеки повну та консолідовану картину загальної безпеки цифрової інфраструктури та видимість дій всередині їх IT-середовища.

Для захисту від більш складних кібератак у цифровій економіці бізнеси повинні моніторити та захищати свої дані. Сучасні організації, напевно, мають більше інформації для збору та аналізу, ніж будь-коли раніше. Перед SIEM аналітики з безпеки вручну переглядали мільйони фрагментованих та ізольованих даних для кожного додатку та точки безпеки.[2]

Отже, SIEM може прискорити реакцію та виявлення кібератак, зробивши розслідування аналітиків з безпеки більш ефективним та точним.

SIM vs SEM vs SIEM

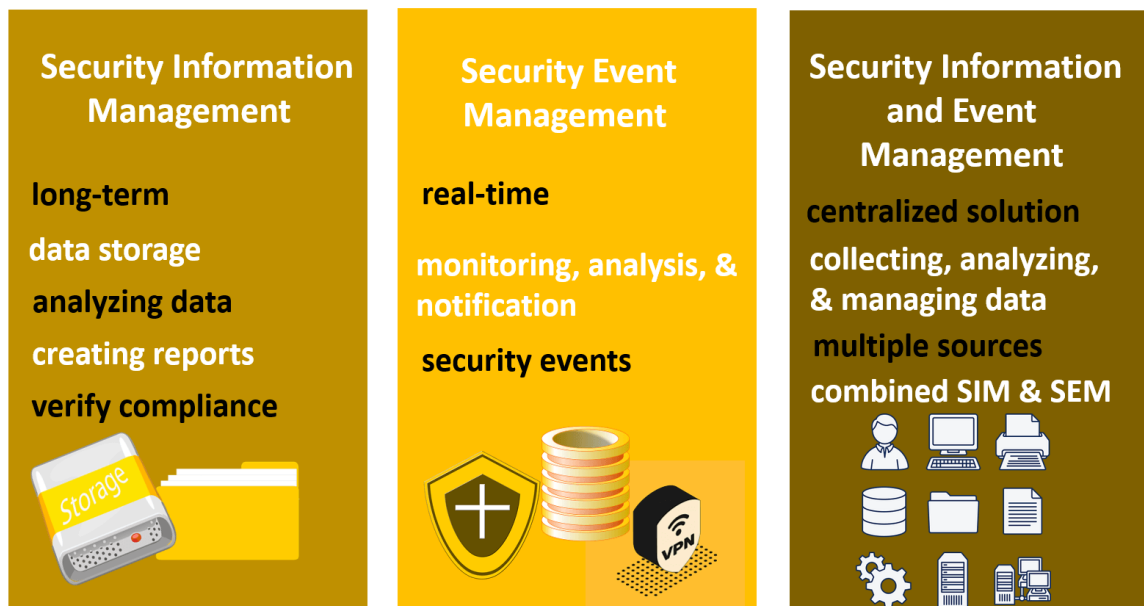


Рисунок 1.1 – Інструменти безпеки інформації у порівнянні

Централізовані збирання, категоризація, моніторинг, синхронізація та аналіз функцій програмного забезпечення SIEM покращують швидкість та точність реакції на події з безпеки. Це сприяє моніторингу в реальному часі та усуненню неполадок в IT-інфраструктурі інформаційно-технологічними командами.

Фреймворки SIEM відрізняються за функціональністю, але часто включають наступні основні функції.

- **Управління журналами:** системи SIEM збирають величезні обсяги даних в центральному місці, організовують їх, а потім вирішують, чи вказує воно на ризики, вторгнення чи проникнення.
- **Кореляція подій:** матеріал аналізується для виявлення зв'язків і тенденцій, щоб можливі небезпеки могли бути виявлені та на них можна було оперативно відреагувати.

- Моніторинг та реакція на інциденти: системи SIEM моніторять проблеми з безпекою в мережі організації і надають попередження та перевірки всіх дій, пов'язаних з інцидентом.
- Збереження даних: SIEM зберігає довгострокові історичні дані для полегшення аналізу відповідності, відстеження та звітування. Особливо важливо в судовому дослідженні, яке може відбутися через роки після події.
- Автоматизація ЦОК: за допомогою інтерфейсів програмування застосунків (API) SIEM може взаємодіяти з іншими системами безпеки та дозволяти співробітникам з безпеки розробляти автоматизовані плейбуки та процеси для реагування на певні події.
- Інформаційні панелі та візуалізація: SIEM генерує візуалізацію, яка дозволяє особам аналізувати дані подій, визначати тенденції та виявляти поведінку, яка відхиляється від звичайних процедур або потоків подій.

Системи SIEM можуть зменшувати кіберризик за допомогою різноманітних варіантів використання, включаючи виявлення аномальної поведінки користувачів, відстеження шаблонів використання, обмеження спроб доступу та створення звітів з відповідності.

Еволюція SIEM

SIEM просунулася від простих систем адміністрування журналів до технологій, що використовують складну UEBA. Тепер це важливий компонент цілісного програмного забезпечення для кібербезпеки, призначений для виконання значної ролі в регуляції та моніторингу відповідності для кількох підприємств.[3]

SIEM пройшов три етапи еволюції: від основного інструменту, який допомагає підприємствам підтримувати та досягати відповідності, до складної системи аналізу загроз, яка дозволяє аналітикам Центру операцій безпеки (SOC) реагувати на події швидше та ефективніше.

Зараз компанії розглядають можливість впровадження цієї базової технології виявлення загроз шляхом побудови узгоджених і послідовних операцій на платформі аналітики та управління безпекою.

Сучасні SIEM повинні включати вбудовані засоби автоматизації та безпеки, оскільки хакери автоматизують усе та використовують інструменти з попередньо налаштованими можливостями.

Майбутня SIEM визначатиметься трьома можливостями: хмарними обчисленнями (розширювані послуги на вимогу), співпрацею (обмін інформацією про загрози та аналітикою) і когнітивними технологіями (штучний інтелект і автоматизація, які допомагають приймати розумніші та швидші рішення).

Як працює SIEM?

Продукти SIEM збирають дані про події та журнали, створені хост-системами, програмами та обладнанням безпеки, як-от антивірусні фільтри та брандмауери, і передають їх на централізовану платформу. Інструменти SIEM виявляють і класифікують інформацію за такими групами, як успішні та невдалі входи, активність зловмисного програмного забезпечення та інша потенційно шкідлива поведінка.

Коли програмне забезпечення SIEM виявляє можливі проблеми з безпекою, воно створює сповіщення безпеки. Підприємства можуть призначити високий або низький пріоритет цим сповіщенням за допомогою набору встановлених критеріїв.

Наприклад, обліковий запис користувача з десятьма невдалими спробами з'єднання протягом 10–15 хвилин може бути позначено як підозрілий, але йому буде присвоєно менший пріоритет, оскільки запити на доступ, ймовірно, були зроблені користувачем, який забув свої облікові дані для входу. Тим не менш, обліковий запис, який створює 500 невдалих спроб входу протягом 10-15 хвилин, буде позначено як інцидент підвищеного рівня, оскільки він, безперечно, піддається атаці грубої сили.

Можна розділити процедуру управління інформацією про безпеку та подіями на такі кроки:

Збір даних: усі джерела інформації про мережеву безпеку, включаючи серверні системи, ОС, брандмауери, програмне забезпечення для захисту від вірусів і механізми запобігання вторгненням, структуровані таким чином, щоб надавати дані про події інструменту SIEM. Більшість сучасних платформ SIEM отримують записи з корпоративних програм через агентів, які згодом аналізуються, фільтруються та передаються в SIEM. Деякі SIEM дозволяють збирати дані без агента.

Створення та застосування політик: адміністратор SIEM створює профіль, який описує поведінку серверів компанії як за звичайних обставин, так і під час попередньо визначених подій безпеки. SIEM за замовчуванням включає правила, сигнали тривоги, звіти та інформаційні панелі, які можна змінювати та налаштовувати відповідно до певних вимог безпеки.

Кореляція даних: системи SIEM агрегують, обробляють і оцінюють файли журналів. Після класифікації подій – з використанням необроблених даних – алгоритми кореляції використовуються для інтеграції конкретних подій даних у відповідні проблеми безпеки.

Активація сповіщень: система інформує працівників служби безпеки щоразу, коли подія або набір випадків запускає правило SIEM (рис. 1.2).



Рисунок 1.2 – Функції SIEM систем

Важливість SIEM

SIEM є важливою складовою стека технологій кібербезпеки будь-якого бізнесу. Значення SIEM можна підсумувати його наступними незаперечними перевагами.

1. Робить операції безпеки та реагування більш ефективними

Завдяки SIEM, що прочісує величезні набори даних, аналітики SOC можуть отримати швидке уявлення про те, що відбувається. Теми аналізу дають змогу швидко перевіряти журнали та інформацію про загрози, що може скоротити як час, необхідний для реагування на загрозу безпеці, так і негативні наслідки кібератаки. Без SIEM експертам із безпеки довелося б вручну аналізувати кілька системних журналів безпеки та джерел даних, зокрема канали

інформації про загрози. Ви також можете налаштувати своє рішення SIEM на реагування на події в режимі реального часу.

2. Нормалізує дані в неоднорідному корпоративному середовищі

Розгляньте різноманітність компонентів, які складають вашу ІТ-екосистему, включаючи кожну програму, точку входу, базу даних і пристрій. Кожен може щомісяця створювати терабайти відкритих текстових даних. Самостійне збирання таких обсягів даних є трудомісткою операцією. Кожен створює, форматує та передає дані по-різному. Спроба вручну зрозуміти все та ідентифікувати пов'язані події безпеки, які вказують на порушення, є величезною справою. Системи SIEM не тільки збирають дані, але й стандартизують їх. Це означає, що вони реструктурують дані відповідно до ваших уподобань, забезпечуючи не лише одноманітність керування журналами, але й пряму кореляцію.

3. Допомогає запобігти внутрішнім загрозам

Окрім зовнішньої вразливості, різноманітні внутрішні ризики, які можуть зробити бізнес уразливим, сприяють зростанню виклику кібербезпеці. Рішення SIEM є особливо важливими, оскільки вони дозволяють організаціям ефективно контролювати діяльність користувачів і відстежувати будь-які аномалії даних. Системи SIEM також забезпечують детальний моніторинг прав доступу. Вони можуть швидко створювати попередження, коли відбувається підозріла діяльність, наприклад, коли користувач запитує інформацію, для якої він не має авторизації, або вимикає необхідне безпекове програмне забезпечення.

4. Спрощує звітування про безпеку та відповідність

Без системи SIEM навряд чи компанія матиме потужні централізовані можливості журналу для надання детальних індивідуальних звітів. У такому випадку може знадобитися створення окремих підсумків для кожного хоста. З іншого боку, потрібно регулярно вручну збирати інформацію з кожного хоста та реконструювати її в централізованому місці для створення єдиного звіту.

Окремий сервер SIEM отримує дані журналу з кількох хостів і може надати єдиний звіт про інцидент, що стосується всіх відповідних подій безпеки, про які повідомляють ці хости. Ще одна причина, чому продукти SIEM такі корисні, полягає в тому, що вони часто забезпечують вбудовану підтримку більшості типових нормативних вимог.

5. Виявляє ранні ознаки кібератаки

Оскільки кібератаки стають все більш складними, їх дедалі складніше вчасно виявляти. Збираючи та стандартизуючи системні журнали з багатьох комп'ютерів, рішення SIEM може ідентифікувати різні компоненти атак на різних хостах у вашій системі. Наприклад, операційна система комп'ютера може виявити частину нападу, тимчасом як система виявлення вторгнення може виявити інший компонент. Порівнюючи системні журнали з кожного хоста, програма може реконструювати послідовність подій, щоб визначити точну природу атаки і чи вона була успішною.

Існує велика різниця між виявленням атаки безпосередньо тоді, коли вона відбувається, і виявленням її після того, як вона вже була здійснена. Розпізнаючи події, які інакше могли б залишатися невиявленими протягом тривалого періоду, процес SIEM може обмежити ступінь будь-якої потенційної шкоди, спричиненої загрозою.

6. Підтримує інтеграцію з ШІ

Сучасні системи SIEM поєднані з надійними функціями оркестрації безпеки, автоматизації та реагування (SOAR), що дозволяє ІТ-командам керувати організаційною безпекою з набагато меншими витратами часу та ресурсів. Використовуючи вдосконалену ML, яка автоматично адаптується до мережевої активності, ці системи можуть обробляти складні протоколи аналізу загроз і керування інцидентами за значно коротші терміни, ніж звичайні команди.

7. Підтримує застосування для великих підприємств

Раніше цілий відділ мав перевіряти, чи всі відділи дотримуються ідентичних найкращих практик безпеки. SIEM може об'єднати всі команди, якщо організація велика. Єдиний звіт на одній робочій станції — це все, що потрібно, щоб швидко стежити за всіма відділами безпеки, інтегруючи все в одну програму. Підприємствам, які мають велику кількість робочої сили та навіть більше пристроїв, іноді важко відстежувати їх усі. У централізованій базі даних системи SIEM дозволяють саме це.

1.2 Вибір Graylog як платформи для захисту в порівнянні з іншими SIEM

Graylog є лідером у сфері керування журналами та управління інформацією про безпеку та подіями (SIEM). Як компанія з інформаційної безпеки, вони також прагнуть зробити світ і його дані більш безпечними та ефективними. Створений практиками для практиків, Graylog надає потужні рішення SIEM тисячам команд IT і безпеки. Ці професіонали вирішують різноманітні проблеми безпеки, відповідності та операцій.

Graylog, заснований Леннартом Купманном (Lennart Koopmann), спочатку розроблявся як проект з відкритим кодом. Купманн керувався бажанням подолати проблеми зручності використання та вартості, пов'язані з багатьма рішеннями централізованого керування журналами. Сьогодні Graylog продовжує розвиватися, задовольняючи різноманітні потреби понад 200 000 фахівців з IT та безпеки.

Відома платформа Graylog, що має понад 50 000 встановлень у всьому світі, вирізняється швидкістю, масштабованістю та аналізом величезних обсягів даних у реальному часі. Це спрощує аналіз даних, пошук загроз, виявлення та розслідування інцидентів завдяки зменшенню нерелевантної інформації. Його адаптивна архітектура оптимізує ці процеси, що покращує взаємодію з користувачем.

Graylog відомий чотирма продуктами: Graylog Security, Graylog Operations, Graylog Open і Graylog Cloud.

Graylog Security — це масштабоване рішення для кібербезпеки, яке надає експертам із безпеки цінну інформацію про стан їх мережі. Він доступний як автономний або хмарний варіант. Поєднуючи SIEM, аналіз загроз і можливості виявлення аномалій, Graylog Security спрощує ідентифікацію загроз. Цей процес робить дослідження та реагування на кіберзагрози легшими, ніж будь-коли.

Graylog Security, створений для задоволення конкретних потреб організацій середнього розміру, є ідеальним вибором для команд з обмеженими ресурсами. Ці команди можуть отримати вигоду від доступного та проактивного виявлення загроз, аналізу інцидентів, реагування та звітування про відповідність. SIEM від Graylog поєднує в собі керування журналами, виявлення загроз, нормалізацію даних, кореляцію та звітування в одній зручній у використанні платформі. Це усуває складність і вартість, які часто зустрічаються в традиційних рішеннях SIEM.

Graylog Security рекламує слоган «SIEM Done Right». Для організацій середнього розміру це означає наступні переваги.

- Надання блискавичних можливостей пошуку, які швидко очищують значні обсяги даних.
- Зосередження на найважливіших аспектах безпеки шляхом фільтрації шуму сповіщень.
- Підвищення продуктивності за рахунок надійної автоматизації повторюваних і вимогливих до безпеки завдань.
- Використання механізму машинного навчання для виявлення аномалій, який постійно вивчає вашу безпекову поведінку.
- Інтуїтивно зрозумілий інтерфейс користувача та робочі процеси користувача з попередньо налаштованими представленнями, шаблонами пошуку та робочими процесами дослідження.

- Повний збір журналів, нормалізацію та представлення з різних джерел у мережі.
- Ефективне визначення пріоритетних подій безпеки серед численних сповіщень.
- Інформування про нормативні вимоги та нормативні вимоги за допомогою збору журналів, інтегрованої інформаційної панелі та автоматизованого звітування.
- Повна інтеграція з існуючими платформами автоматизації безпеки для швидшого вирішення.
- Надання легкого в освоєнні інтерфейсу, який не вимагає вивчення SQL або ексклюзивних мов запитів.

Graylog Security пропонує вбудовані в хмару функції, простий у використанні інтерфейс і готовий вміст. Це робить отримання цінної інформації з журналів ще легшим порівняно з традиційними рішеннями SIEM. Його функції допомагають зменшити витрати, покращити стан безпеки та мінімізувати втому від сповіщень, що зрештою розширює можливості аналітиків безпеки.

Порівняння Graylog та інших інструментів SIEM

Серед найбільш поширених та популярних SIEM систем можна виділити наступні.

1. Splunk - потужна платформа для збору та аналізу великих обсягів даних, яка підтримує інтеграцію з різними джерелами даних та має широкий набір інструментів для аналітики.
2. IBM QRadar - інтегроване рішення для управління безпекою, яке забезпечує збір, нормалізацію, кореляцію та аналіз подій у режимі реального часу.
3. ArcSight - SIEM платформа від Micro Focus, яка спеціалізується на кореляції подій та забезпеченні детального аналізу безпекових інцидентів.[5]

4. Graylog - відкрита система для управління логами та подіями, яка дозволяє збирати, зберігати, аналізувати та візуалізувати дані в режимі реального часу. Детальніше в таблиці 1.1.

Таблиця 1.1 – Порівняння популярних SIEM-систем

Характеристика	Splunk	IBM QRadar	ArcSight	Graylog
Ліцензія	Пропрієтарна	Пропрієтарна	Пропрієтарна	Відкрита (Open-source)
Масштабованість	Висока	Висока	Висока	Висока
Інтеграція	Широкі інтеграції	Глибока інтеграція з IBM	Різноманітні джерела	Гнучка інтеграція
Функціональність	Потужна аналітика, ML, дашборди	Кореляція подій, аналітика реального часу	Аналіз інцидентів, кореляція	Реальний час, пошук, настроювані дашборди
Простота використання	Вимагає часу для освоєння	Складний інтерфейс	Вимагає значних зусиль	Інтуїтивний інтерфейс
Вартість	Висока	Висока	Висока	Низька
Використання API	Підтримує інтеграцію	Обмежена без додаткових модулів	Підтримує інтеграцію	Розширені можливості

Graylog є оптимальним вибором серед розглянутих систем завдяки своїй відкритій ліцензії, що значно знижує вартість впровадження та обслуговування. Його гнучка архітектура дозволяє масштабувати систему відповідно до потреб підприємства, а зручний інтерфейс та детальна документація забезпечують простоту використання навіть для новачків. Graylog підтримує розширену інтеграцію з різноманітними джерелами даних і забезпечує ефективний аналіз логів у реальному часі. Крім того, його потужні API-можливості дозволяють інтегрувати систему з сучасними додатками, що особливо важливо для захисту інфраструктури. Зважаючи на низьку вартість володіння, високу

функціональність і зручність, Graylog є універсальним рішенням для підприємств будь-якого масштабу.[6]

1.3 Огляд функціональних можливостей Graylog

Graylog є потужним інструментом для централізованого збору, обробки та аналізу логів, що забезпечує широкі можливості для моніторингу та виявлення загроз. У цьому розділі розглянемо основні функціональні можливості Graylog, які роблять його ефективним рішенням для забезпечення безпеки мереж.

Основні функції Graylog (рис. 1.3):

- Graylog дозволяє збирати логи з різних джерел, таких як мережеве обладнання, сервери, додатки та інші пристрої, у єдине централізоване сховище.
- Платформа автоматично перетворює зібрані логи у стандартизований формат, що спрощує їх подальший аналіз.
- Graylog забезпечує потужні інструменти для швидкого пошуку та фільтрації даних, що дозволяє ефективно виявляти підозрілі події та аномалії.
- Можливість кореляції подій з різних джерел допомагає виявляти складні загрози та аномальні поведінки користувачів.
- Платформа підтримує налаштування оповіщень для різних типів подій, що дозволяє оперативно реагувати на інциденти безпеки.
- Graylog дозволяє створювати персоналізовані дашборди та звіти для візуалізації даних та моніторингу стану безпеки в режимі реального часу.
- Платформа легко інтегрується з іншими інструментами безпеки та управління ІТ, що забезпечує комплексний підхід до захисту мереж.

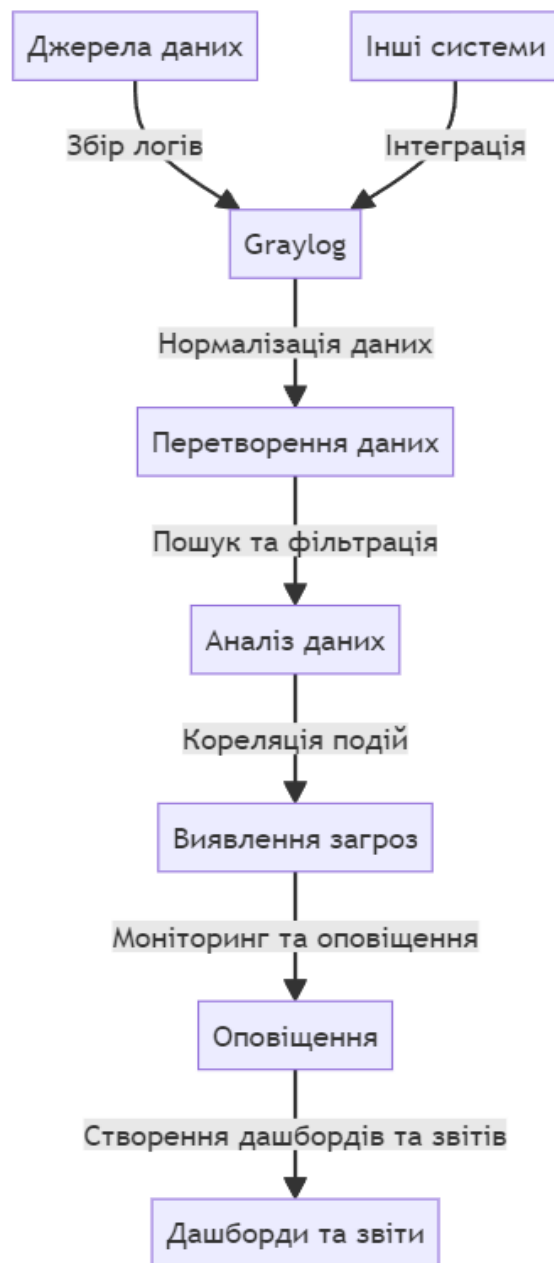


Рисунок 1.3 - Основні функції Graylog

Graylog підтримує збір логів з різних джерел, таких як (рис. 1.4):

- Мережеві пристрої (роутери, комутатори)
- Сервери (Windows, Linux)
- Додатки (веб-сервери, бази даних)
- Безпекові системи (антивіруси, IDS/IPS)

Особливості Graylog Security

Graylog Security — це багатофункціональна платформа, яка пропонує широкий набір можливостей для керування та захисту даних. Зосередимося на основних. [4]

- Виявлення аномалій/UEBA

Дозволяє легко ділитися конфігураціями для екстракторів, входів, конвеєрів, інформаційних панелей тощо, забезпечуючи плавний перехід від тестування до виробництва.

- Звіт про відповідність

Використовує функції інформаційної панелі Graylog, щоб легко створювати та планувати звіти про відповідність вимогам.

- Кореляція та сповіщення

Можливість отримувати сповіщення електронною поштою, текстовими повідомленнями, Slack тощо з можливістю оновлення критеріїв сповіщень на основі динамічних списків у таблицях пошуку.

- Нормалізація та збагачення даних

Дозволяє збільшити швидкість дослідження, додавши WHOIS, геолокацію IP, розвідку про загрози або інші структуровані дані для контексту.

- Журнали користувачів

Відстеження доступу користувачів до даних журналу та дії, які виконуються з ними, забезпечуючи відповідність і безпеку.

- Розслідування інциденту

Створення й об'єднання кількох пошуків для будь-якого аналізу в одну дію та експорт результати на інформаційну панель.

- Конструктор пошукових запитів

Створення й об'єднання кількох пошуків для будь-якого аналізу в одну дію та експортуй результати на інформаційну панель.

- Інформаційні панелі аналізу безпеки

Налаштування відображення даних шляхом комбінування віджетів та автоматизація доставки звітів у папку “Вхідні”.

- Правила SIGMA

Імпорт правил SIGMA для покращення виявлення кіберінцидентів і надання додаткового контексту для заходів середнього часу до вирішення (MTTR).

- Стрічки інформації про загрози

Інтеграція наявних каналів аналізу загроз, щоб додати контекст до даних журналу подій і виявити потенційні проблеми безпеки.

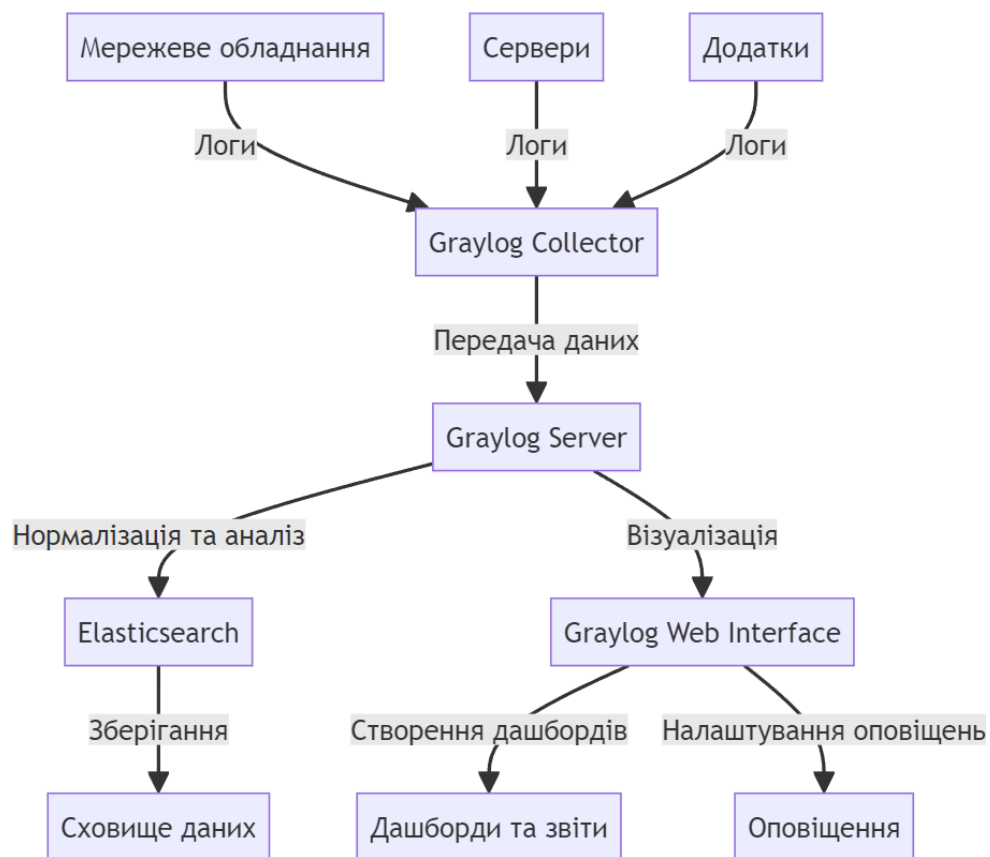


Рисунок 1.4 - Процес інтеграції та обробки даних у Graylog

Graylog автоматично нормалізує зібрані логи, перетворюючи їх у стандартизований формат для спрощення подальшого аналізу. Це включає парсинг даних, виділення ключових полів та перетворення часових міток (рис 1.4).

Платформа забезпечує швидкий та ефективний пошук за логами, використовуючи потужні інструменти фільтрації та запитів. Це дозволяє знаходити конкретні події та аномалії у великих обсягах даних.

Можливість кореляції подій дозволяє виявляти складні загрози, що можуть залишитися непоміченими при аналізі окремих логів. Graylog може поєднувати події з різних джерел для створення більш повної картини загрози.

Graylog підтримує налаштування оповіщень для різних типів подій. Користувачі можуть налаштувати правила оповіщення для отримання миттєвих повідомлень про критичні інциденти .

Платформа дозволяє створювати персоналізовані дашборди для візуалізації даних у реальному часі. Користувачі можуть створювати звіти для регулярного моніторингу стану безпеки та представлення даних керівництву (рис.1.5).

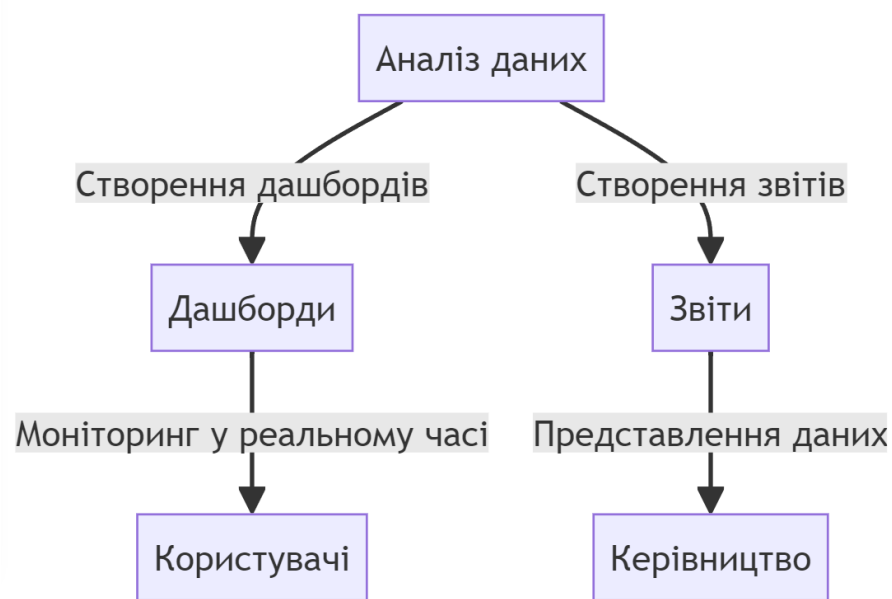


Рисунок 1.5 - Процес створення дашбордів у Graylog

Graylog підтримує інтеграцію з іншими системами безпеки та управління ІТ, такими як SIEM платформи, антивірусні програми, системи управління конфігураціями та інші. Це забезпечує комплексний підхід до захисту мереж.

Розгортання Graylog складається з 3 компонентів (рис 1.6).

1. Сервер Graylog.

Він обслуговує веб-інтерфейс користувача/API і дає змогу взаємодіяти з Graylog. Від налаштування входів, сповіщень, індексів до інформаційних панелей.

2. OpenSearch (раніше Elasticsearch)

OpenSearch — це пошуковий і аналітичний пакет із відкритим кодом, який складається з наступного:

- OpenSearch: сховище даних і пошукова система
- Інформаційні панелі OpenSearch: візуалізація та інтерфейс користувача
- Data Prepper: збирач даних на стороні сервера

OpenSearch базується на Elasticsearch і Kibana, має відкритий код і залишається, технологією, керованою спільнотою, яка дозволяє розробникам створювати продукти за допомогою різних плагінів за такими напрямками, як:

- пошук;
- аналітика;
- спостереження;
- безпека;
- машинне навчання.

За допомогою OpenSearch користувачі можуть використовувати можливості пошуку та візуалізації, щоб отримати більше інформації з даних своїх журналів, уможливорюючи такі випадки використання (use cases):

- швидкий пошук у великих обсягах даних;
- моніторинг додатків;
- моніторинг інфраструктури;
- моніторинг безпеки та криміналістичний аналіз;
- оперативний моніторинг здоров'я.

Як проект із відкритим вихідним кодом OpenSearch має прозорість, забезпечуючи видимість коду та контроль над тим, як розробники можуть його використовувати.

3. MongoDB

Використовується для зберігання метаданих Graylog.

MongoDB - система управління базами даних, яка працює з документоорієнтованою моделлю даних. На відміну від реляційних СУБД, MongoDB не потрібні таблиці, схеми або окрема мова запитів. Інформація зберігається у вигляді документів або колекцій.

Розробники позиціонують продукт як проміжну ланку між класичними СУБД і NoSQL. MongoDB не використовує схеми, як це роблять реляційні бази даних, що підвищує продуктивність усієї системи. Архітектуру Graylog детальніше описано у розділі 2.

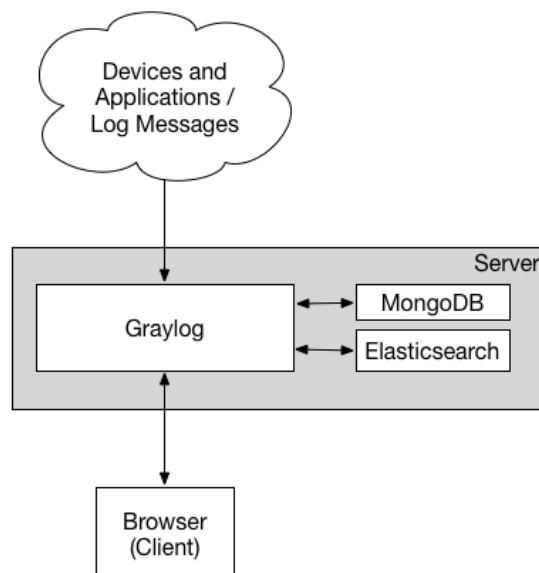


Рисунок 1.6 - Діаграма мінімального налаштування Graylog

Для реалізації у даному проєкті обрано базове одновузлове розгортання Graylog. У майбутньому таке розгортання за потреби можна масштабувати в багатовузлове, натомість саме одновузловий варіант рекомендують для початківців [21].

Висновок до першого розділу

У першому розділі роботи було проведено аналіз сучасних методів та інструментів для виявлення витоків даних і внутрішніх загроз. Особливу увагу приділено поняттю SIEM-систем, їх важливості в корпоративних мережах, а

також перевагам і недолікам найпоширеніших платформ. Здійснено порівняльний аналіз популярних систем SIEM, в результаті якого для реалізації у даному проєкті обрано Graylog. Проаналізовано вибір Graylog як платформи для забезпечення безпеки у порівнянні з іншими SIEM-системами, зокрема його функціональні можливості, які роблять його ефективним рішенням у сфері моніторингу та аналізу поведінки користувачів.

Результати аналізу підтвердили, що Graylog є оптимальним вибором завдяки його широким можливостям для збору, обробки та кореляції даних, налаштування сповіщень і створення дашбордів.

РОЗДІЛ 2 ПРОЕКТУВАННЯ АРХІТЕКТУРИ ПІДСИСТЕМИ НА ОСНОВІ SIEM

2.1 Топологія мережі та архітектура системи Graylog

Схема топології створена для візуалізації взаємозв'язків між компонентами системи Graylog. На схемі відображено, як дані (логи) переміщуються від джерел до центрального сервера обробки, а також роль кожного елемента у забезпеченні інформаційної безпеки.

Це зроблено для полегшення аналізу структури мережі та схематичної візуалізації мережі. Топологія дозволяє забезпечити надійний зв'язок між компонентами та ефективну обробку логів, що є основою для виявлення загроз і аномалій у поведінці користувачів (рис. 2.1).

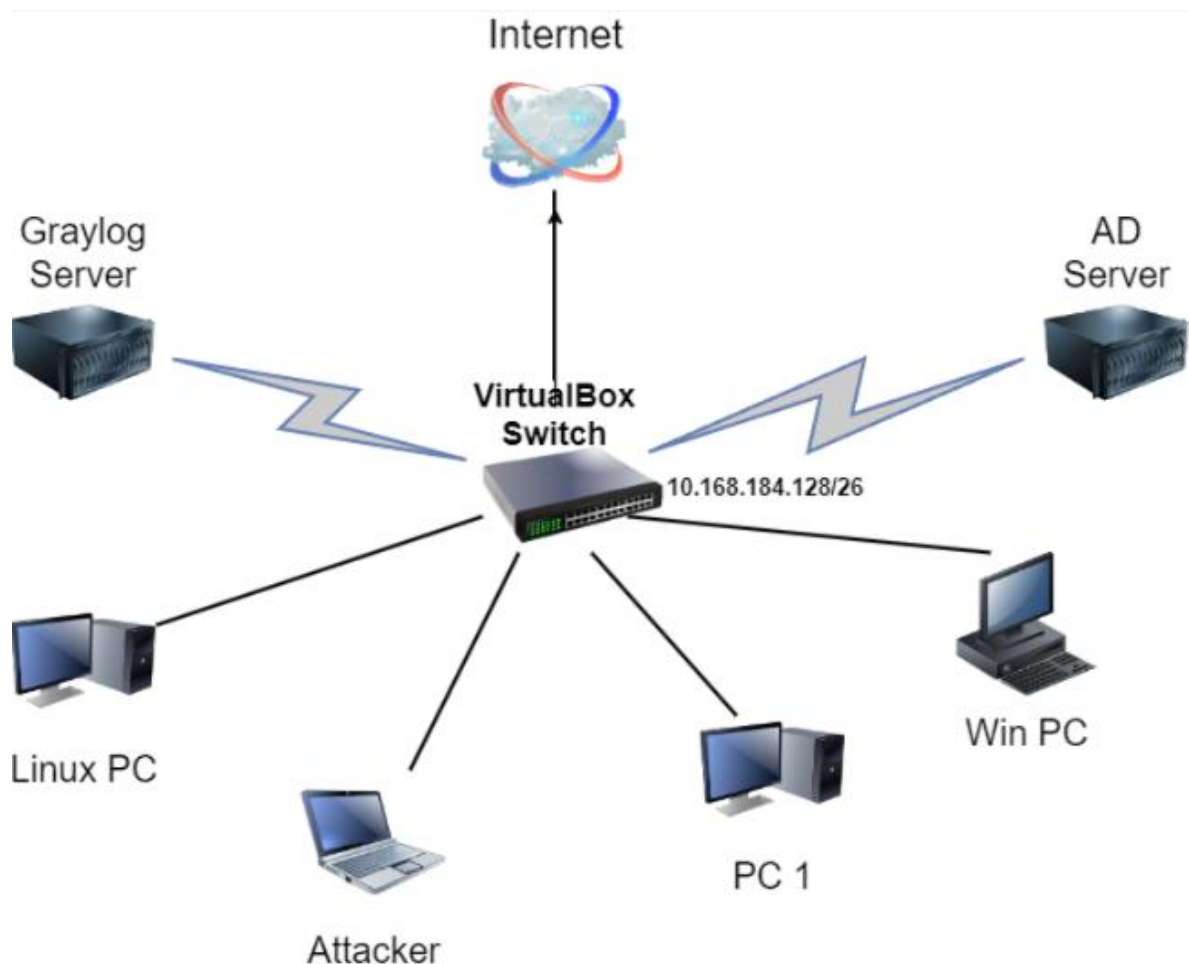


Рисунок 2.1 – Модель мережі для роботи системи Graylog

Схема адресації розроблена для точного визначення мережесих параметрів кожного пристрою в системі. У таблиці наведені IP-адреси, маски підмереж, шлюзи за замовчуванням та інші дані для всіх ключових компонентів мережі, таких як сервер Graylog, сервер Active Directory, робочі станції (таблиця 2.1).

Це зроблено для забезпечення чіткої взаємодії між елементами системи, унеможливлення конфліктів адрес і підтримки належного функціонування системи збору та обробки логів. Завдяки адресації забезпечується зручність налаштування, а також можливість масштабування мережі в майбутньому. Для моделювання мережі було використано середовище VirtualBox, де кінцеві вузли працювали на операційних системах Ubuntu 22.04 та Windows 10.

Таблиця 2.1 – Адресація мережі системи

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
Router	Інтерфейс E1/0 (до Інтернету)	10.168.184.129	255.255.255.192/26	—
Graylog Server	Інтерфейс E0	10.168.184.139	255.255.255.192	10.168.184.129
AD Server	Інтерфейс E0	10.168.184.135	255.255.255.192	10.168.184.129
Linux PC	Інтерфейс E0	10.168.184.136	255.255.255.192	10.168.184.129
Win PC	Інтерфейс E0	10.168.184.137	255.255.255.192	10.168.184.129
PC 1	Інтерфейс E0	10.168.184.138	255.255.255.192	10.168.184.129
Attacker	Інтерфейс E0	10.168.184.130	255.255.255.192	10.168.184.129

Архітектура системи Graylog для аналізу поведінки користувачів та виявлення витоків даних та внутрішніх загроз складається з кількох ключових компонентів, кожен з яких виконує специфічні функції для забезпечення безперебійної роботи та ефективного аналізу даних.

Основні компоненти архітектури Graylog:[8]

- Джерела даних
- Graylog Collectors
- Graylog Server
- Elasticsearch
- Graylog Web Interface
- Користувачі та адміністративний інтерфейс

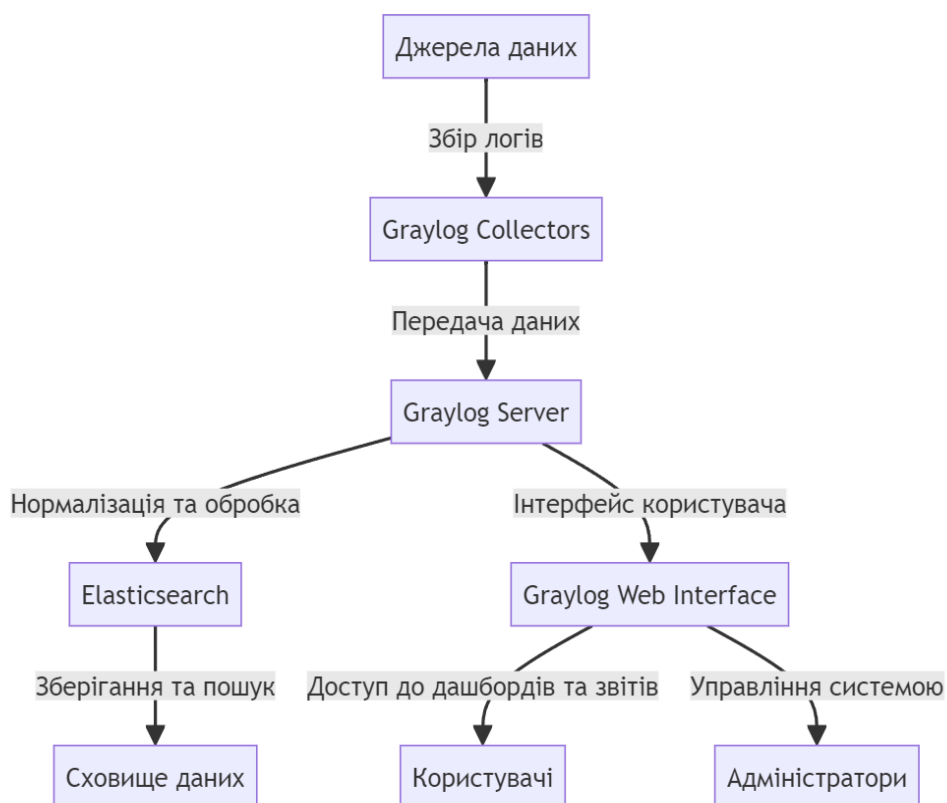


Рисунок 2.2 - Загальна архітектура Graylog[9]

Джерела даних включають різноманітні пристрої та системи, які генерують лог-файли. До них відносяться:

- Мережеве обладнання (маршрутизатори, комутатори, брандмауери)
- Сервери (Windows, Linux)

- Додатки (веб-сервери, бази даних)
- Безпекові системи (антивіруси, IDS/IPS)

Graylog Collectors – це агенти, які встановлюються на джерелах даних для збору логів. Вони забезпечують:

- Збір логів з різних джерел
- Передачу зібраних логів на Graylog Server
- Фільтрацію та попередню обробку даних

Graylog Server є центральним компонентом системи, який відповідає за:

- Прийом логів від колекторів
- Нормалізацію та обробку даних
- Передачу нормалізованих даних до Elasticsearch для зберігання та

пошуку

Elasticsearch є розподіленою пошуковою та аналітичною системою, яка забезпечує:

- Зберігання нормалізованих логів
- Швидкий пошук та аналіз даних
- Масштабованість для обробки великих обсягів даних

Graylog Web Interface – це інтерфейс користувача, який надає можливості для:

- Перегляду та аналізу логів
- Створення та налаштування дашбордів
- Генерації звітів
- Налаштування оповіщень

Налаштування доступу до функціоналу розділені на два основних доступи (таблиця 2.2).

Таблиця 2.2 – Доступи до функціоналу

Аутентифікація	Доступ
Адміністратор	• Управління налаштуваннями системи

Аутентифікація	Доступ
Адміністратор	• Налаштування політик безпеки • Моніторингу стану системи
Користувач	• Перегляду дашбордів та звітів • Аналізу логів та подій

Архітектура Graylog забезпечує надійний та масштабований механізм для збору, обробки та аналізу логів, що дозволяє ефективно виявляти та реагувати на загрози безпеці. Кожен компонент системи виконує свою специфічну функцію, що забезпечує комплексний підхід до забезпечення інформаційної безпеки.[7]

2.2 Інтеграція Graylog з Active Directory та іншими технологіями для безпеки користувачів

Інтеграція Graylog з Active Directory (AD) забезпечує централізоване управління користувачами та їхніми правами доступу. Це дозволяє ефективно контролювати доступ до системи, підвищує рівень безпеки та спрощує адміністрування.

AD забезпечує єдине місце для управління обліковими записами користувачів, що спрощує адміністрування та підвищує безпеку.

Інтеграція дозволяє застосовувати політики безпеки AD для контролю доступу до Graylog, включаючи багаторівневу автентифікацію та управління ролями (рис. 2.3).

Використання єдиних облікових даних для доступу до AD та Graylog спрощує управління паролями та зменшує кількість паролів, які потрібно запам'ятовувати користувачам.

Використання AD дозволяє вести аудит дій користувачів та моніторити доступ до Graylog, забезпечуючи прозорість та контроль.[10]

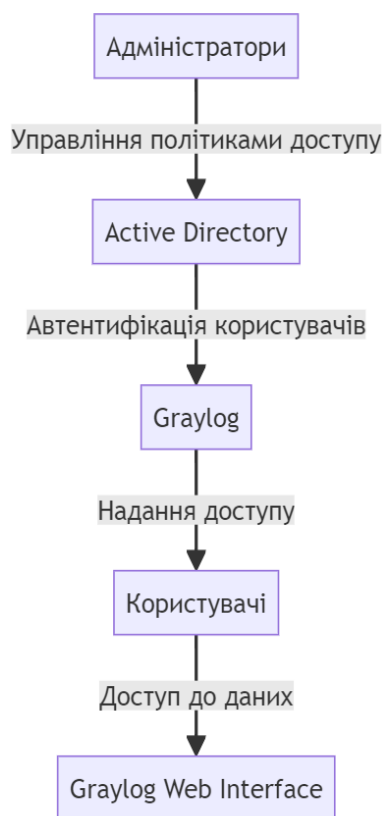


Рисунок 2.3 - Інтеграція Graylog з Active Directory

Для інтеграції Graylog з Active Directory необхідно виконати наступні кроки.

1. Налаштування Active Directory

Створення груп користувачів та ролей в AD, які будуть використовуватись для управління доступом до Graylog.

Налаштування політик безпеки, що застосовуються до цих груп.

2. Налаштування Graylog

Встановлення та конфігурація Graylog для інтеграції з AD.

Налаштування автентифікації через LDAP (Lightweight Directory Access Protocol), який використовується для доступу до інформації в AD.

3. Конфігурація LDAP в Graylog

Введення параметрів підключення до AD, таких як адреса сервера, порт, тип з'єднання (захищене або незахищене), та облікові дані для доступу. Налаштування базового DN (Distinguished Name) для пошуку користувачів та

груп у AD. Налаштування фільтрів для автентифікації користувачів та отримання їхніх груп (рис. 2.4).



Рисунок 2.4 - Конфігурація LDAP в Graylog

4. Управління ролями та дозволами

Призначення ролей та дозволів користувачам в Graylog на основі груп AD.

Налаштування політик доступу до різних розділів та функцій Graylog залежно від ролей користувачів (рис. 2.5).



Рисунок 2.5 - Управління ролями та дозволами

```
ldap:
  enabled: true
  ldap_uri: "ldap://localhost:389"
  system_username: "cn=admin,dc=domain,dc=com"
  system_password: "admin"
  search_base: "dc=domain,dc=com"
  search_pattern: "(&(objectClass=user)(sAMAccountName={0}))"
  display_name_attribute: "cn"
  group_search_base: "dc=domain,dc=com"
  group_id_attribute: "cn"
  default_group: "graylog-users"
  use_start_tls: true
  active_directory: true
```

Рисунок 2.6 – Приклад конфігурації LDAP в системі Graylog[12]

Цей приклад конфігурації LDAP показує основні параметри, необхідні для підключення Graylog до Active Directory (рис. 2.6). Необхідно налаштувати адресу сервера, облікові дані для доступу, пошукові бази та шаблони, що використовуються для пошуку користувачів та груп.[11]

Інтеграція Graylog з Active Directory забезпечує централізоване управління користувачами, підвищуючи рівень безпеки та спрощуючи адміністрування. Завдяки використанню LDAP, Graylog може легко підключатися до AD для автентифікації користувачів, управління ролями та контролю доступу. Це дозволяє забезпечити ефективний моніторинг та аналіз логів з високим рівнем безпеки.

Інтеграція Graylog з додатковими сервісами та технологіями дозволяє розширити можливості системи моніторингу і підвищити її функціональність. Це може включати інтеграцію з аналітичними платформами, системами управління інцидентами, системами попередження загроз і іншими корисними інструментами. В процесі реалізації проєкту я інтегрував Graylog з додатковими

сервісами, що дозволило розширити функціонал та підвищити ефективність системи.

Graylog вже використовує Elasticsearch як основний механізм зберігання і пошуку даних. Проте для розширення можливостей аналітики я налаштував використання наступних розширених функцій Elasticsearch.

1) Використання функцій агрегації та аналізу в Elasticsearch для створення більш складних звітів та дашбордів. Використовував Elasticsearch Query DSL для створення кастомних запитів та агрегатів.

2) Налаштування індексації даних за специфічними критеріями дозволяє зберігати і аналізувати дані з урахуванням специфічних вимог. Також налаштування автоматичного імпорту даних про загрози для використання у фільтрах та правилах Graylog. Використання отриманої інформації може використовуватись для покращення правил виявлення і зменшення кількості хибних спрацьовувань.

3) Інтеграція Graylog з додатковими технологіями дозволила значно розширити можливості системи моніторингу і підвищити її функціональність. Завдяки інтеграції з аналітичними платформами, системами попередження загроз вдалося забезпечити більш ефективний аналіз даних, автоматизувати процеси управління інцидентами та підвищити загальний рівень безпеки. Це сприяло покращенню оперативної готовності системи та швидшій реакції на потенційні загрози.

2.3. Визначення типів подій та логів для моніторингу

Для забезпечення ефективного моніторингу та виявлення загроз необхідно визначити типи подій та логів, які будуть збиратися та аналізуватися за допомогою Graylog. Це дозволяє сфокусуватися на найважливіших подіях, що впливають на безпеку та продуктивність системи.

Основні типи подій та логів для моніторингу (рис. 2.7):

- Системні логи
- Мережеві логи

- Логи додатків
- Безпекові логи
- Аудиторські логи
- Події користувачів

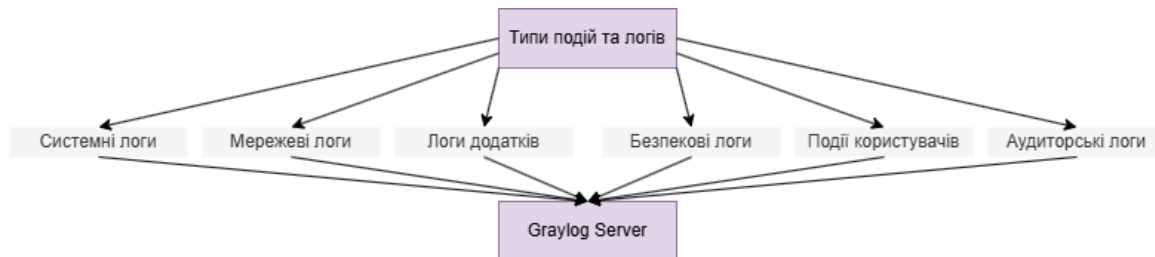


Рисунок 2.7 - Типи подій та логів для моніторингу

Системні логи містять інформацію про роботу операційних систем серверів та робочих станцій. Вони включають:

- логи системних помилок, інформація про збої системи, помилки драйверів та апаратного забезпечення;
- логи системних оновлень, записи про встановлені оновлення та патчі безпеки;
- логи служб, інформація про роботу служб та демони системи.

Мережеві логи містять інформацію про мережевий трафік та активність пристроїв у мережі. Вони включають:

- логи маршрутизаторів та комутаторів, інформація про підключення, маршрутизацію та передачу даних;
- логи брандмауерів, записи про дозволені та заблоковані з'єднання, спроби проникнення;
- логи VPN, інформація про підключення та аутентифікацію користувачів.

Логи додатків містять інформацію про роботу програмного забезпечення, яке використовується у системі. Вони включають:

- логи веб-серверів, записи про запити до серверу, відповіді, помилки;

- логи баз даних, інформація про запити, транзакції, помилки баз даних;
- логи користувацьких додатків, записи про виконання завдань, помилки, активність користувачів.

Безпекові логи містять інформацію про події, що впливають на безпеку системи. Вони включають:

- логи антивірусних програм, записи про виявлені загрози, сканування, оновлення бази вірусів;
- логи IDS/IPS, інформація про виявлені атаки, запобігання проникненням;
- логи системи контролю доступу, записи про успішні та неуспішні спроби автентифікації, зміну прав доступу.

Аудиторські логи містять записи про дії користувачів та адміністраторів, що важливі для забезпечення прозорості та відповідності політикам безпеки. Вони включають:

- логи змін конфігурацій, записи про зміни у конфігурації системи, налаштування мережі;
- логи управління користувачами, інформація про створення, зміну та видалення облікових записів.
- логи доступу до даних, записи про доступ до конфіденційних даних, їхнє редагування та видалення.

Події користувачів містять інформацію про активність користувачів у системі. Вони включають:

- логи входу/виходу, записи про успішні та неуспішні спроби входу у систему;
- логи активності, інформація про виконані дії, використані ресурси;
- логи підозрілої активності, записи про аномальні дії, що можуть вказувати на можливі загрози.

Для ефективного моніторингу та аналізу необхідно обрати відповідні типи логів залежно від специфіки системи та вимог безпеки. Основні критерії вибору включають:

- важливість для безпеки, логи, що містять інформацію про критичні події безпеки;
- частота подій, логи, що містять часті події, які можуть вказувати на аномалії;
- аналіз продуктивності, логи, що допомагають оцінити продуктивність системи та виявити можливі проблеми.

Визначення типів подій та логів для моніторингу є критичним етапом у забезпеченні безпеки системи. Правильний вибір логів дозволяє ефективно виявляти та реагувати на загрози, забезпечуючи надійний захист інформаційних ресурсів. Інтеграція різних типів логів у Graylog дозволяє отримати повну картину про стан системи та своєчасно виявляти можливі проблеми та загрози.

2.4 Додаткові технології для розширення можливостей системи

Інтеграція додаткових технологій та сервісів з Graylog допомагає розширити функціональні можливості системи, забезпечити вищий рівень безпеки, ефективність обробки даних та зручність використання. Нижче наведено список додаткових технологій, які можуть бути інтегровані в систему для покращення її роботи.[19]

Додаткові технології та сервіси:

- Logstash
- Grafana
- Kafka
- Prometheus
- Ansible
- Jenkins
- Suricata
- Wazuh



Рисунок 2.8 – Перелік відомих технологій для інтеграції

Logstash – потужний інструмент для збору, обробки та зберігання даних, який може бути інтегрований з Graylog для проміжної обробки логів, включаючи фільтрацію, нормалізацію та агрегацію, а також підтримку широкого спектру джерел даних, включаючи файли, мережеві пристрої, бази даних.

Grafana – інструмент для візуалізації даних, який може бути інтегрований з Graylog для створення інтерактивних дашбордів, що забезпечують візуалізацію даних та моніторинг у реальному часі.

Kafka – розподілена потокова платформа, яка може бути використана для обробки великих обсягів даних у реальному часі, забезпечуючи потокову обробку та передачу даних між різними компонентами системи, а також підтримку високого навантаження та великих обсягів даних. [16]

Prometheus – система моніторингу та оповіщення з відкритим вихідним кодом, яка може бути інтегрована з Graylog для моніторингу метрик, забезпечуючи збір та зберігання метрик системи для аналізу продуктивності та стану, а також налаштування оповіщень на основі зібраних метрик для оперативного реагування на проблеми.

Ansible – інструмент для оркестрації та управління конфігураціями, який може бути використаний для автоматизації налаштувань Graylog та його компонентів, забезпечуючи автоматичне розгортання та конфігурацію

компонентів системи, а також збереження та застосування конфігураційних змін у системі.

Jenkins – інструмент для безперервної інтеграції та доставки, який може бути використаний для автоматизації процесів тестування та розгортання Graylog, забезпечуючи автоматичне тестування та інтеграцію змін у коді, а також автоматичне розгортання нових версій Graylog та його компонентів.

Suricata – система виявлення вторгнень (IDS), яка може бути інтегрована з Graylog для аналізу мережевого трафіку та виявлення загроз, забезпечуючи аналіз мережевого трафіку для виявлення підозрілих активностей та атак, а також збір та передачу логів про виявлені загрози у Graylog.

Wazuh – платформа для безпеки та моніторингу, яка може бути інтегрована з Graylog для розширеного аналізу безпеки, забезпечуючи аналіз системних логів для виявлення загроз та вразливостей, а також перевірку відповідності політикам безпеки та нормативним вимогам.

Інтеграція додаткових технологій та сервісів з Graylog дозволяє створити комплексну систему для збору, обробки, аналізу та моніторингу даних. Використання Logstash, Grafana, Kafka, Prometheus, Ansible, Jenkins, Suricata та Wazuh дозволяє забезпечити високу ефективність, масштабованість та надійність системи, а також підвищити рівень безпеки та зручність використання.

Висновок до другого розділу

У другому розділі роботи було виконано проектування архітектури підсистеми на основі SIEM-платформи Graylog для аналізу поведінки користувачів і виявлення загроз. Визначено ключові компоненти архітектури, їх функціональні ролі та взаємодію, що дозволяє ефективно збирати, обробляти та аналізувати логи. Особливу увагу приділено інтеграції з Active Directory та іншими технологіями, що забезпечує централізоване управління доступом і покращує можливості моніторингу.

Проектування охоплювало визначення типів подій і логів для моніторингу, а також вибір додаткових технологій для інтеграції, таких як Logstash, MongoDB, Grafana та інші. Це створює комплексну основу для подальшої реалізації системи, спрямованої на підвищення рівня інформаційної безпеки та своєчасне виявлення витоків даних і внутрішніх загроз.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ СИСТЕМИ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ ТА ДОСЛІДЖЕННЯ ЇЇ РОБОТИ

3.1. Встановлення Graylog та його компонентів

Встановлення Graylog складається з кількох кроків, включаючи підготовку середовища, встановлення необхідних компонентів та конфігурацію системи. Нижче опишемо хід встановлення Graylog на операційній системі Ubuntu.

Кроки для встановлення Graylog є наступними:

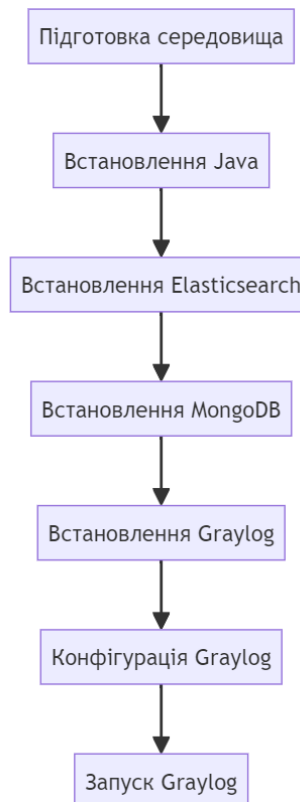


Рисунок 3.1 – Послідовність встановлення Graylog

Перед встановленням Graylog необхідно підготувати середовище на сервері. Переконайтеся, що ваша система оновлена та має всі необхідні залежності.[13]

```
sudo apt update
```

```
sudo apt install curl wget apt-transport-https
```

Graylog вимагає встановлення Java. Використано OpenJDK 17 для забезпечення сумісності.

```
sudo apt install openjdk-17-jre-headless -y
```

Elasticsearch є ядром для зберігання та пошуку логів у Graylog.
Завантаження та встановлення останньої версії Elasticsearch.[14]

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo  
apt-key add -
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main"  
| sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt update
```

```
sudo apt install elasticsearch -y
```

Після встановлення Elasticsearch, відкриваємо файл конфігурації
/etc/elasticsearch/elasticsearch.yml та додаємо або змінюємо наступні рядки:

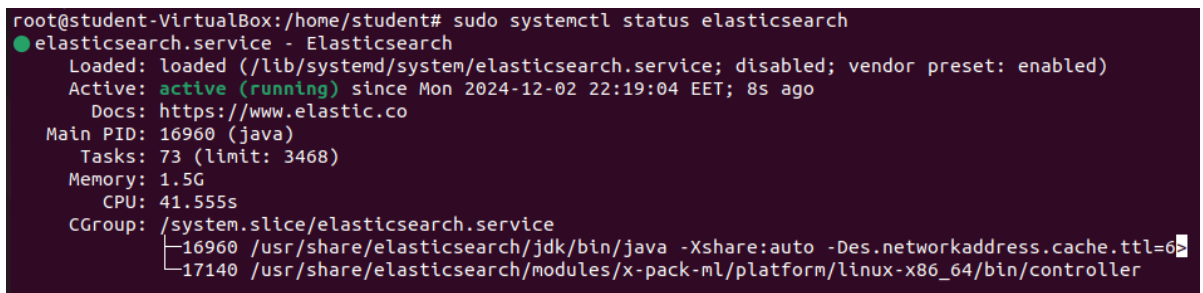
```
cluster.name: graylog
```

```
action.auto_create_index: false
```

Запускаємо та вмикаємо Elasticsearch (рис.3.2):

```
sudo systemctl start elasticsearch
```

```
sudo systemctl enable elasticsearch
```



```
root@student-VirtualBox:/home/student# sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-12-02 22:19:04 EET; 8s ago
     Docs: https://www.elastic.co
   Main PID: 16960 (java)
    Tasks: 73 (limit: 3468)
   Memory: 1.5G
      CPU: 41.555s
   CGroup: /system.slice/elasticsearch.service
           └─16960 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60
           └─17140 /usr/share/elasticsearch/modules/x-pack-nl/platform/linux-x86_64/bin/controller
```

Рисунок 3.2 – Результат встановлення та запуску ElasticSearch

MongoDB використовується для зберігання конфігураційних даних Graylog.

Для встановлення додаємо ключ підпису MongoDB GPG.

```
curl -fsSL https://pgp.mongodb.com/server-6.0.asc | \
```

```
sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/mongodb-server-6.0.gpg
```

Далі додаємо сховище MongoDB до каталогу sources.list.d у системі.

```
echo «deb [ arch=amd64,arm64
```

```
signed=/etc/apt/trusted.gpg.d/keyrings/mongodb-server-6.0.gpg ]
```

```
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 multiverse» |  
sudo tee /etc/apt/sources.list.d/mongodb-org-6.0 list  
sudo apt update
```

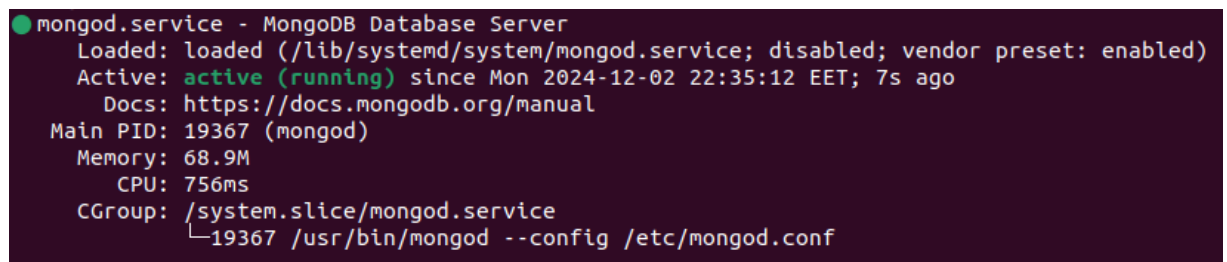
Потім встановлюємо сервер бази даних MongoDB.

```
sudo apt install mongodb-org -y
```

Запустимо та увімкнемо MongoDB (рис.3.3):

```
sudo systemctl start mongod
```

```
sudo systemctl enable mongod
```



```
● mongod.service - MongoDB Database Server  
   Loaded: loaded (/lib/systemd/system/mongod.service; disabled; vendor preset: enabled)  
   Active: active (running) since Mon 2024-12-02 22:35:12 EET; 7s ago  
     Docs: https://docs.mongodb.org/manual  
  Main PID: 19367 (mongod)  
    Memory: 68.9M  
       CPU: 756ms  
    CGroup: /system.slice/mongod.service  
            └─19367 /usr/bin/mongod --config /etc/mongod.conf
```

Рисунок 3.3 – Результат встановлення та запуску MongoDB

Завантажимо та встановимо Graylog за допомогою наступних команд:

```
wget https://packages.graylog2.org/repo/packages/graylog-5.2-  
repository_latest.deb  
sudo dpkg -i graylog-5.2-repository_latest.deb  
sudo apt update  
sudo apt install graylog-server -y
```

Відкриваємо файл конфігурації /etc/graylog/server/server.conf та внесимо необхідні зміни (рис. 3.4):

Встановлюємо секретний пароль (його можна згенерувати за допомогою команди `pwgen -N 1 -s 96`):

```
password_secret = YOUR_SECRET_PASSWORD
```

Встановимо хеш паролю адміністратора (його можна згенерувати за допомогою команди `echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1`):

```
root_password_sha2 = YOUR_HASHED_PASSWORD
```

Встановимо URL для веб-інтерфейсу Graylog:

```
http_bind_address = 0.0.0.0:9000
```

```
# The auto-generated node ID will be stored in this file and read after restarts. It is a good idea
# to use an absolute file path here if you are starting Graylog server from init scripts or similar.
node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid.
password_secret = Gq44st7e0SrUIeL3CuQVIGtxN9kW3hCGsOUarJXILYUCCFoZ0DvEiWdE7rXl7vbc7Zku3Zm9Dm5v3J6M4urbI20L43ta8fBe

# The default root user is named 'admin'
#root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = bcb15f821479b4d5772bd0ca866c00ad5f926e3580720659cc80d39c9d09802a

# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
#http_bind_address = [2001:db8::1]:9000
```

Рисунок 3.4 – Результат налаштованого конфігураційного файлу Graylog[15]

Запустимо та увікнемо Graylog (рис. 3.5):

```
sudo systemctl start graylog-server
```

```
sudo systemctl enable graylog-server
```

```
● graylog-server.service - Graylog server
   Loaded: loaded (/lib/systemd/system/graylog-server.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-12-02 22:53:26 EET; 4s ago
     Docs: http://docs.graylog.org/
    Main PID: 21612 (graylog-server)
      Tasks: 34 (limit: 3468)
     Memory: 296.6M
        CPU: 7.392s
    CGroup: /system.slice/graylog-server.service
            └─21612 /bin/sh /usr/share/graylog-server/bin/graylog-server
              └─21613 /usr/share/graylog-server/jvm/bin/java -Xms1g -Xmx1g -server -XX:+UseG1GC -XX:-Omit
```

Рисунок 3.5 – Результат встановлення та запуску Graylog Server

Перевірка встановлення

Відкриємо веб-браузер та перейдемо за адресою <http://127.0.0.1:9000>. Використовуємо облікові дані адміністратора, які вказали під час конфігурації, щоб увійти в Graylog (рис. 3.6).



Рисунок 3.6 – Перевірка доступності Web-інтерфейсу Graylog

3.2 Налаштування індексів, колекторів логів та правил виявлення інцидентів

Налаштування індексів та колекторів логів в системі Graylog є важливим етапом для забезпечення ефективного збору та зберігання логів. В процесі роботи над проєктом я здійснив декілька ключових кроків, щоб налаштувати індекси та колектори, що дозволило оптимізувати обробку та аналіз даних.

Першим кроком було налаштування індексів. Індекси в Graylog використовуються для організації зберігання логів, що дозволяє спростити їх пошук та управління. Я створив новий індексний набір для логів додатків, що дозволило ефективно розподілити навантаження на систему зберігання даних.

Створив новий індексний набір з назвою "filebeat index" (рис 3.7).

Налаштував політику ротації індексів за часом, щоб індекси оновлювалися кожні 5 секунд. Встановив максимальну кількість індексів для збереження на рівні, що дозволяє зберігати дані за останній рік.

The screenshot displays the configuration page for an index set named "filebeat-index". The interface is divided into several sections:

- General Settings:** Includes fields for Title, Description, Index shards (set to 4), Index replicas (set to 0), Max. number of segments (set to 1), Index optimization after rotation (unchecked), and Field type refresh interval (set to 5).
- Index Rotation Configuration:** Contains a description of the rotation strategy, a dropdown for "Select rotation strategy" (set to "Index Time"), a field for "Rotation period (ISO8601 Duration)" (set to "P1D"), and a checkbox for "Empty index set" (checked).
- Index Retention Configuration:** Includes a description of the retention strategy, a dropdown for "Select retention strategy" (set to "Delete Index"), and a field for "Max number of indices" (set to 5).

At the bottom, there are "Update index set" and "Cancel" buttons.

Рисунок 3.7 – Створення індексу для спрощення пошуку логів

Для збору логів з різних джерел я налаштував колектори логів. Використовуючи Filebeat як колектор, я забезпечив передачу логів з серверів додатків до Graylog. Це дозволило централізувати збір даних та спростити їх подальший аналіз (рис. 3.8).

Встановив Filebeat на серверах додатків, налаштувавши його для збору логів з директорії /var/log.

```
curl -L -O
```

```
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.3.2-  
amd64.deb
```

```
sudo dpkg -i filebeat-6.3.2-amd64.deb
```

Налаштував передачу логів з Filebeat до Graylog через протокол Logstash на порт 5044.

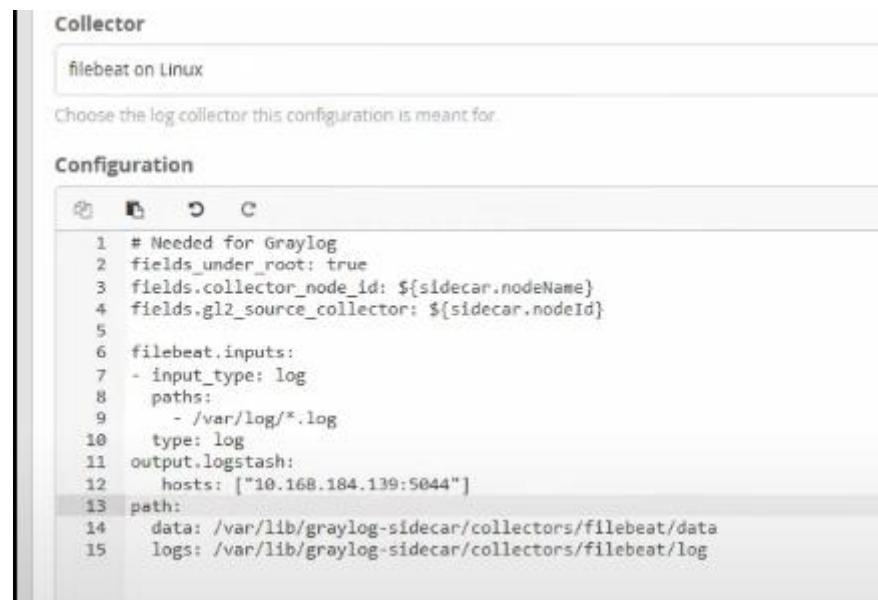


Рисунок 3.8 – Конфігурація плагіну Filebeat для збору логів на Linux
Створив вхідний потік в Graylog для обробки логів від Filebeat.

Після налаштування індексів та колекторів логів я здійснив конфігурацію потоків логів. Потоки логів дозволяють організувати обробку та зберігання логів за визначеними правилами, що підвищує ефективність аналізу даних.

Створив потік логів "Sidecar" для логів додатків, спрямовуючи їх до відповідного індексного набору (рис. 3.9).

Додав правила для фільтрації логів за полем source, що дозволило розділити логи від різних серверів додатків.

Налаштував маркування логів, додаючи відповідні теги для полегшення подальшого пошуку та аналізу.

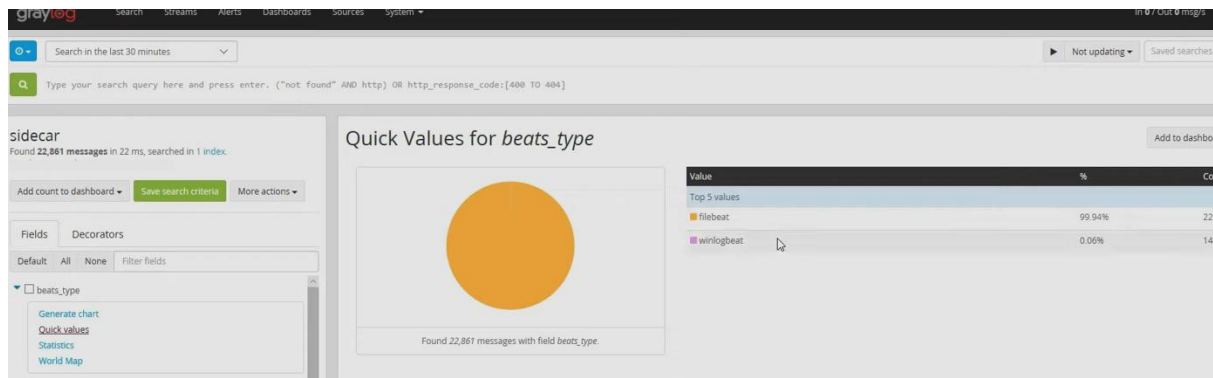


Рисунок 3.9 – Налаштований потік з джерелом логів Filebeat

Налаштування індексів та колекторів логів в Graylog є важливим етапом для організації ефективного збору та зберігання логів. Завдяки налаштуванню індексів, ротації даних та колекторів я зміг централізувати збір логів з різних джерел та спростити їх подальший аналіз. Конфігурація потоків логів дозволила організувати обробку даних за визначеними правилами, що значно підвищило ефективність роботи системи.[18]

Важливою частиною роботи з Graylog є розробка та налаштування правил для виявлення інцидентів безпеки. Ці правила дозволяють автоматизувати процес моніторингу та сповіщення про потенційні загрози або аномальні дії. В процесі реалізації проєкту я створив декілька важливих правил для забезпечення своєчасного реагування на інциденти.

Для розробки правил виявлення інцидентів в Graylog я використовував механізми потоків (streams) та сповіщень (alerts). Це дозволило налаштувати автоматичну обробку логів та відправку сповіщень при виявленні підозрілої активності.

Створивши нові потоки для різних типів логів, таких як системні журнали, журнали додатків та журнали мережевої безпеки. Це дозволило розділити логи за категоріями та спростити їх обробку.

Наприклад, для системних журналів було створено потік з назвою "System Logs Stream", який фільтрував логи за джерелом syslog.

Додав до потоку правила для фільтрації специфічних подій. Наприклад, для виявлення невдалих спроб входу до системи було створено правило, яке фільтрує логи за ключовим словом authentication failure (рис. 3.10).

Для потоку "System Logs Stream" налаштував правило, яке шукає логи з полем message містить authentication failure.

```
rule "Detect Authentication Failures"
when
  contains(to_string($message.message), "authentication failure")
then
  set_field("alert", true);
end
```

Pipeline connections

This pipeline is processing messages from the stream "System Logs Stream".

Edit connections

Pipeline Stages

Stages are groups of conditions and actions which need to run in order, and provide the necessary control flow to decide whether or not to run the rest of a pipeline.

Add new stage

Stage 0

Contains 0 rules

Messages satisfying **at least one rule** in this stage, will continue to the next stage.

Throughput: 0 msg/s

Delete

Edit

This stage has no rules yet. Click on edit to add some.

Stage 1

Contains 1 rule

There are no further stages in this pipeline. Once rules in this stage are applied, the pipeline will have finished processing.

Throughput: 0 msg/s

Delete

Edit

Title	Description	Throughput	Errors
Detect Authentication Failures		0 msg/s	0 errors/s (0 total)

Рисунок 3.10 – Результат налаштування Pipeline з правилом пошуку

Після налаштування правил для потоків, я налаштував сповіщення для автоматичного відправлення повідомлень при виявленні інцидентів. Сповіщення було налаштовано для відправлення на Slack.

Alerts & Events Event Definitions Notifications

Edit "sysadmin_package_installation_or_removal" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Event Details **Filter & Aggregation** Fields

Event Condition
Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.

Condition Type
Filter & Aggregation
Choose the type of Condition for this Event.

Filter
Add information to filter the log messages that are relevant for this Event Definition.

Search Query
auditbeat_event_action: package_installed OR auditbeat_event_action: package_removed
Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

Streams (Optional)
auditbeat x
Select streams the search should include. Searches in all streams if empty.

Search within the last
3 minutes

Execute search every
2 minutes

☒ Enable
Should this event definition be executed automatically?

Create Events for Definition if...
☒ Filter has results
☐ Aggregation of results reaches a threshold

[Previous](#)

Рисунок 3.11 – Створення нового Event Definition

Наприклад, для потоку "auditbeat" налаштував сповіщення, щоб спрацьовувало кожного разу, коли пакет встановлено або видалено (рис. 3.11).

У веб-інтерфейсі Graylog перейшов до меню Alerts > Event Definitions.

Натиснув кнопку Create Event Definition та заповнив форму:

Title: Ввів назву (наприклад, "sysadmin_package_installation_or_removed").

Priority: Вибрав пріоритет (наприклад, Medium).

Condition: Обрав умову Filter & Aggregation

Додав нове сповіщення до створеної події. Вибрав тип сповіщення Slack Notification (рис. 3.13).

Edit "sysadmin_package_installed_or_removed" Notification

Notifications alert you of any configured Event when they occur. Graylog can send Notifications directly to you or to other systems you use for that purpose.

Title
sysadmin_package_installed_or_removed
Title to identify this Notification.

Description (Optional)
pkg installation or removal alert
Longer description for this Notification.

Notification Type
Slack Notification
Choose the type of Notification to create.

Configuration color
Change color
Choose a color to use for this configuration.

Webhook URL
https://hooks.slack.com/services/...
Slack "Incoming Webhook" URL.

Channel
#channel
Name of Slack #channel or @user for a direct message

Custom Message (optional)
[Graylog]
\$(if backlog)
\$(foreach backlog message)
\$(message.message)
source: \$(message.source)
\$(end)
\$(end)
Timestamp: \$(event.timestamp)
Custom message to be appended below the alert title. See [docs](#) for more details.

Time zone for date/time values
New York
Time zone used for timestamps in the notification body.

Message Backlog Limit (optional)
1
Limit the number of backlog messages sent as part of the Slack notification. If set to 0, no limit will be enforced.

User Name (optional)
Graylog
User name of the sender in Slack

Рисунок 3.12 – Налаштування Alert в Graylog для відправки в Slack

Заповнив необхідні поля для налаштування сповіщення:

Webhook URL: Ввів адресу Slack для отримання сповіщень.

Custom Message: Ввів текст повідомлення з інформацією про інцидент (рис. 3.12).

Alerts & Events | Event Definitions | Notifications

Edit "sysadmin_package_installation_or_removal" Event Definition

Event Definitions allow you to create Events from different Conditions and alert on them.

Event Details | Filter & Aggregation

Notifications (optional) [Manage Notifications](#)

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
sysadmin_package_installed_or_removed	Slack Notification	Remove from Event

[Add Notification](#)

Grace Period
5 minutes

Graylog sends Notifications for Alerts every time they occur. Set a Grace Period to control how long Graylog should wait before sending Notifications again. Note that Events with keys will have a Grace Period for each different key value.

Message Backlog
1
Number of messages to be included in Notifications.

[Previous](#)

Рисунок 3.13 – Додавання сповіщення до попереднього кроку

Провів тестування налаштувань сповіщень, створивши декілька тестових інцидентів. Переконався, що сповіщення надходять до Slack (рис. 3.18).

Розробка та налаштування правил виявлення інцидентів в Graylog дозволили автоматизувати процес моніторингу безпеки та оперативно реагувати на потенційні загрози. Завдяки створенню потоків для фільтрації логів, налаштуванню правил для виявлення підозрілої активності та конфігурації сповіщень вдалося значно підвищити ефективність виявлення інцидентів та забезпечити своєчасне інформування про них.

3.3 Налаштування інтеграції системи з Active Directory та створення звітів для моніторингу та аналізу подій

Інтеграція Graylog з Active Directory (AD) дозволяє централізувати управління користувачами та підвищити безпеку за рахунок використання єдиної системи автентифікації. В процесі реалізації проєкту я здійснив інтеграцію Graylog з Active Directory, що дозволило використовувати існуючі облікові записи користувачів AD для доступу до Graylog.

Для інтеграції Graylog з Active Directory спочатку було необхідно зібрати інформацію про конфігурацію AD, зокрема:

- Адресу сервера LDAP.
- Базове DN (Distinguished Name) для пошуку користувачів та груп.
- Облікові дані користувача, що має права на пошук в AD.

Наступним кроком було налаштування підключення до LDAP в веб-інтерфейсі Graylog. Для цього я виконав наступні дії:

Увійшов у веб-інтерфейс Graylog як адміністратор.

Перейшов до меню System > Authentication > AD settings.

Заповнив поля конфігурації LDAP (рис. 3.14):

AD Server: Вказав адресу сервера AD (наприклад, ldap://10.168.184.135:389).

Search Base DN: Вказав базове DN для пошуку користувачів (наприклад, DC=bitsbytehard, DC=local).

Bind DN: Вказав DN облікового запису для підключення до AD (наприклад, CN=admin, OU=Users, DC= bitsbytehard, DC= local).

Bind Password: Вказав пароль для облікового запису.

User Search Pattern: Вказав шаблон для пошуку користувачів (наприклад стандартний шаблон, (&(objectClass=user) (sAMAccountName={0}))).

Натиснув кнопку Save, щоб зберегти налаштування.

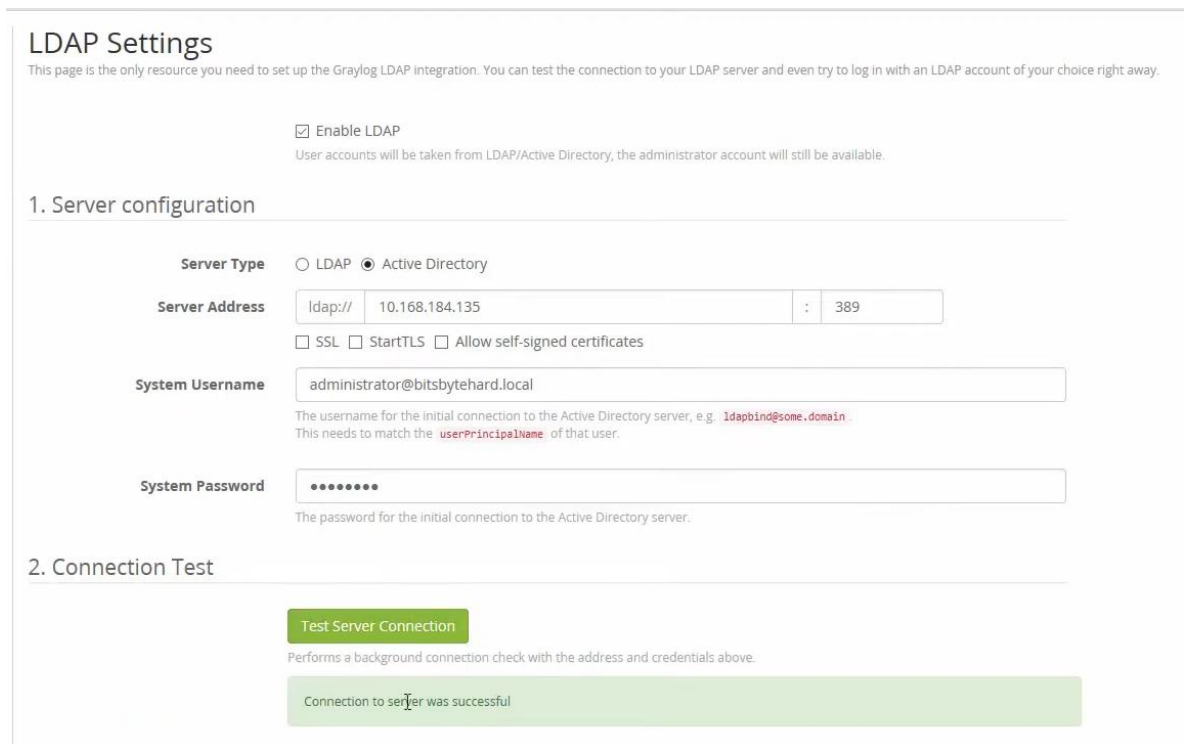


Рисунок 3.14 – Налаштування та результат підключення до домену AD

Після збереження налаштувань я провів тестування підключення до AD:

Натиснув кнопку Test Connection, щоб перевірити підключення до сервера AD. Щоб призначати ролі та права користувачам, що автентифікуються через AD, я налаштував відповідні групи:

У веб-інтерфейсі Graylog перейшов до меню System > Authentication > LDAP settings. В секції Group Mapping додав відповідні групи AD, що визначають права доступу користувачів в Graylog (рис.3.15).

Group Base DN: Вказав базове DN для пошуку груп (наприклад, OU=Groups, DC= bitsbytehard, DC=local).

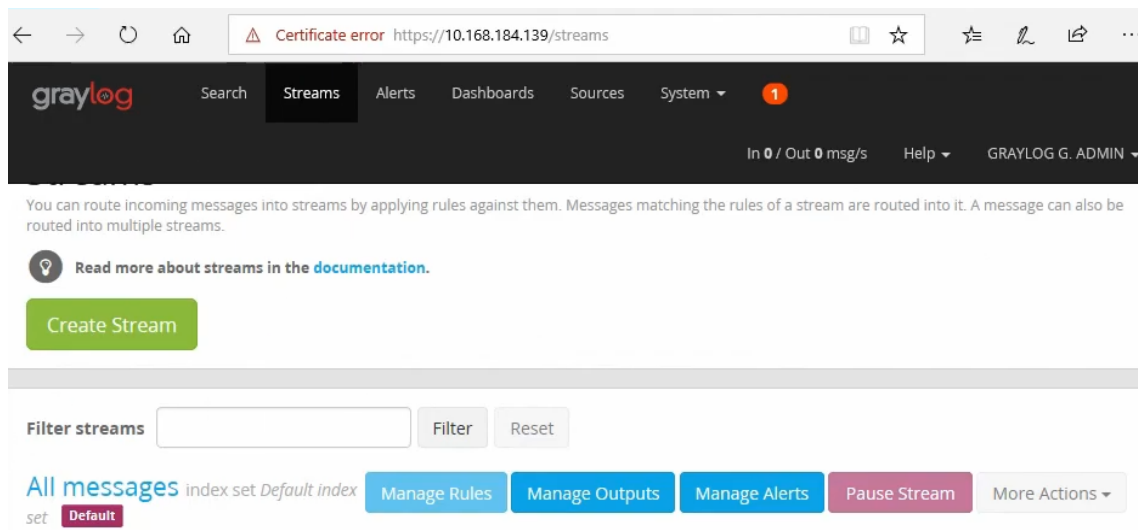
Group Search Pattern: Вказав шаблон для пошуку груп (наприклад, (&(objectClass=group)(cn=graylog-users))).

Відповідно призначив ролі для груп (наприклад, групі graylog-readers призначив роль read everything).

Enterprise Read-only Domain Controllers	None
GRAYLOG_ADMINIS	Admin
GRAYLOG_READERS	Read everything
Group Policy Creator Owners	None
NetworkAdmins	network admins
Protected Users	None
RAS and IAS Servers	None
Read-only Domain Controllers	None

Рисунок 3.15 – Налаштування прав доступу користувачів за допомогою Group Mapping

Після успішного підключення виконав перевірку автентифікації користувачів з AD, їхні права та доступи до системи.



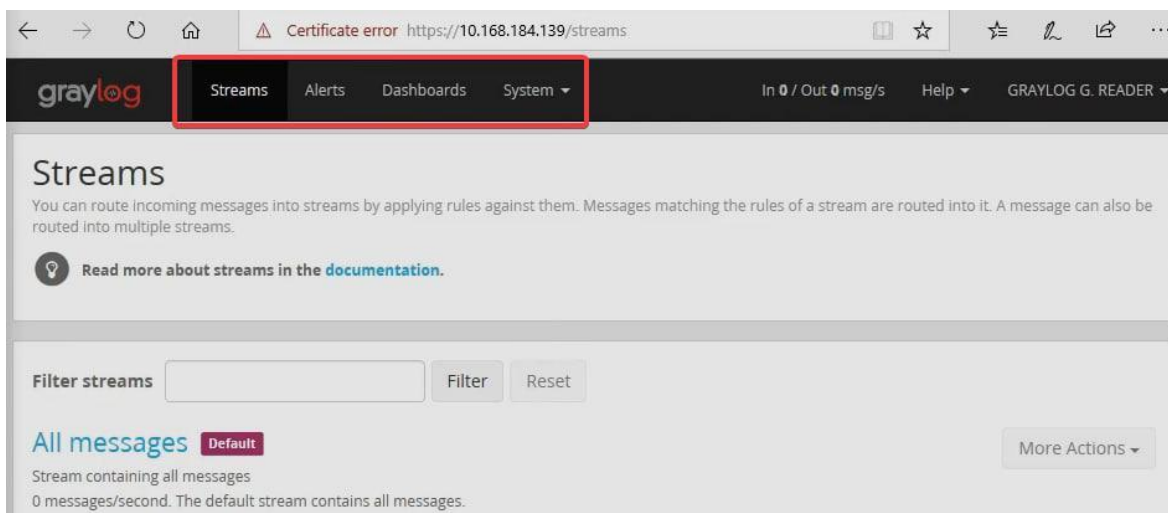


Рисунок 3.16 – Перевірка доступності вкладок під користувачами Graylog.Admin та Reader

Інтеграція Graylog з Active Directory дозволила централізувати управління користувачами та спростити процес аутентифікації, використовуючи існуючу інфраструктуру AD. Це забезпечило більш зручне управління доступом до системи та підвищило загальну безпеку. Завдяки налаштуванню LDAP підключення, тестуванню автентифікації та налаштуванню груп користувачів вдалося успішно інтегрувати Graylog з Active Directory та забезпечити ефективне управління доступом для користувачів.

Створення звітів є ключовим етапом в процесі моніторингу та аналізу безпекових подій у Graylog. Звіти дозволяють узагальнити інформацію про події, виявлені інциденти та загальні тенденції, що дозволяє швидко оцінити стан системи та приймати обґрунтовані рішення. В процесі реалізації проєкту я створив кілька звітів для аналізу подій та спостереження за загальним станом безпеки.

Для створення звітів я використовував панелі (dashboards) в Graylog, які дозволяють візуалізувати дані у вигляді графіків, таблиць та діаграм.

Увійшов у веб-інтерфейс Graylog.

Перейшов до меню Dashboards.

Натиснув кнопку Create Dashboard та ввів назву панелі (наприклад, "SSH Dashboard"). Вибрав необхідний тип панелі (наприклад, Pie Chart, Bar Chart, Table).

Додав віджети до панелі для відображення важливої інформації. Наприклад, для моніторингу невдалих спроб входу створив віджет Bar Chart, що показує кількість спроб входу за останні 24 години (рис.3.17). Налаштував віджет для фільтрації даних за специфічними полями (наприклад, source, event_type).

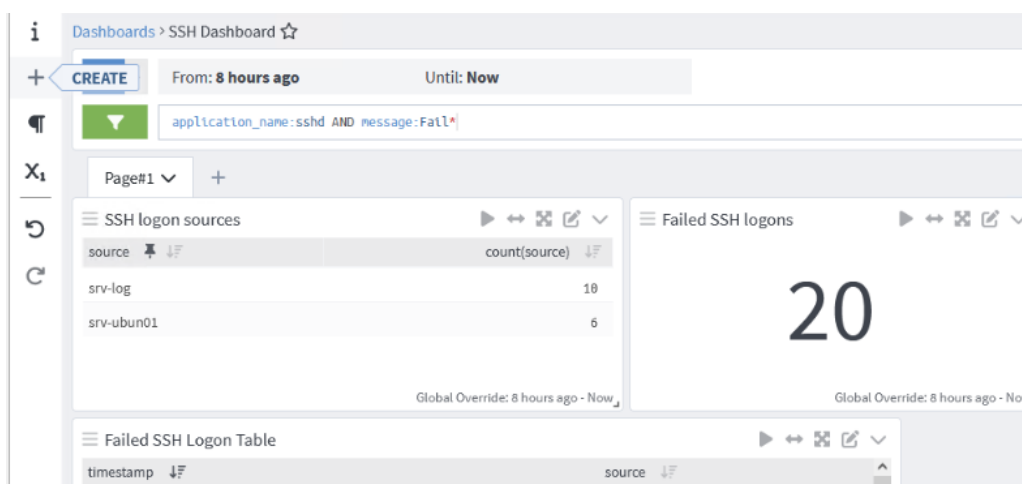


Рисунок 3.17 – Налаштовані віджети невдалих спроб входу по SSH в Дашборді

Використовував створені звіти для оцінки загального стану системи, виявлення аномальних подій та оцінки ефективності виявлення інцидентів. Виявлені проблеми або тренди документував для подальшого аналізу та вдосконалення системи безпеки.

Створення та налаштування звітів у Graylog дозволило систематизувати інформацію про безпекові події, виявлені інциденти та загальні тенденції. Завдяки панелям для візуалізації даних, автоматичній генерації звітів та їхній розсилці вдалося забезпечити регулярний моніторинг безпекового стану системи та своєчасно реагувати на потенційні загрози. Це значно підвищило ефективність управління безпекою та допомогло підтримувати високий рівень захисту інформаційних систем.

3.4 Аналіз ефективності роботи підсистеми та тестування правил виявлення інцидентів та сповіщень

Тестування правил виявлення інцидентів є важливим етапом впровадження системи моніторингу безпеки на основі Graylog. Основною метою цього процесу є перевірка правильності роботи створених правил, визначення їх ефективності та виявлення можливих помилкових спрацювань. Це дозволяє забезпечити коректне функціонування системи в реальних умовах, зводячи до мінімуму кількість помилкових тривог і пропущених подій.

Процес тестування розпочинається з визначення сценаріїв, які покривають як позитивні, так і негативні випадки використання. Важливо охопити різні типи подій, що повинні відстежуватися системою, такі як невдалі спроби входу, підозрілі зміни конфігурації або аномальна мережева активність.[17]

Для створення тестових подій можуть бути використані різні методи. Наприклад, для перевірки реакції системи на невдалу спробу входу на сервер може бути виконано спробу підключення через SSH під неіснуючим користувачем за допомогою наступної команди:

```
ssh invalid_user@localhost
```

Ця команда спробує підключитися до локального сервера, що створить запис у журналах про невдалу спробу входу. Інший приклад — імітація підозрілого мережевого трафіку за допомогою інструмента nmap, що дозволяє просканувати порти на сервері:

```
nmap -sS -p 1-65535 localhost
```

Ця команда ініціює сканування всіх портів на локальному сервері, що також створює відповідні записи у журналах.

Наступним етапом є налаштування правил в Graylog, які повинні реагувати на відповідні події. Наприклад, для виявлення невдалих спроб входу може бути створене наступне правило:

```
{  
  "rule": "when has_field(\"sshd_authentication_failure\") then  
create_alert(\"Authentication Failure\");",
```

```
"title": "SSH Authentication Failure",  
"description": "Виявлення невдалих спроб входу через SSH.",  
"priority": 2  
}
```

Це правило автоматично створює сповіщення при кожному зафіксованому інциденті, що відповідає умовам правила.

Після налаштування правил необхідно провести аналіз їх спрацювання. Для цього перевіряється, чи коректно правила обробляють тестові події, та чи генеруються відповідні сповіщення. Для цього можна використовувати наступний запит до API Graylog:

```
curl -X GET "http://localhost:9000/api/alerts" -H "Content-Type:  
application/json" -u admin:admin_password
```

Ця команда поверне список сповіщень, згенерованих Graylog.

Якщо правила спрацьовують некоректно, їх необхідно відкоригувати. Оптимізація правил може включати додавання додаткових фільтрів, зміни порогів спрацювання або корекцію логіки обробки даних. Наприклад, можна налаштувати правило так, щоб виключити певні IP-адреси, які не повинні викликати тривогу:

```
{  
  "rule": "when has_field(\"sshd_authentication_failure\") and not  
cidr_match(\"10.0.0.0/8\", to_string($message.source)) then  
create_alert(\"Authentication Failure\");",  
  "title": "SSH Authentication Failure - External",  
  "description": "Виявлення невдалих спроб входу через SSH з  
зовнішніх IP.",  
  "priority": 2 }  
}
```

Таким чином, процес тестування правил виявлення інцидентів забезпечує ефективну роботу системи Graylog, що дозволяє своєчасно реагувати на загрози, зменшуючи кількість помилкових спрацювань і пропущених подій.

Перевірка коректності роботи сповіщень є важливою складовою тестування системи моніторингу на основі Graylog. Цей етап має на меті

забезпечити, щоб сповіщення генерувалися своєчасно, містили точну інформацію та надсилалися відповідним каналом до зацікавлених сторін.

Перевірка розпочинається з тестування правил, що визначають умови для генерування сповіщень. Для цього використовуються заздалегідь підготовлені сценарії, які імітують інциденти, що повинні викликати спрацювання правил і, відповідно, генерувати сповіщення. Наприклад, під час перевірки сповіщень про невдалі спроби входу, створюється тестовий інцидент за допомогою спроби входу з неіснуючим користувачем через SSH. У випадку коректної роботи системи, це повинно спричинити негайне створення сповіщення в Graylog.

Одним із ключових аспектів перевірки є тестування каналів доставки сповіщень. Система Graylog підтримує різні методи надсилення сповіщень, включаючи електронну пошту, повідомлення в месенджери або інтеграцію з іншими системами оповіщення. Для перевірки коректності роботи цих каналів створюються тестові повідомлення, які надсилаються через налаштовані канали, після чого перевіряється їхнє отримання на боці користувача.[20]

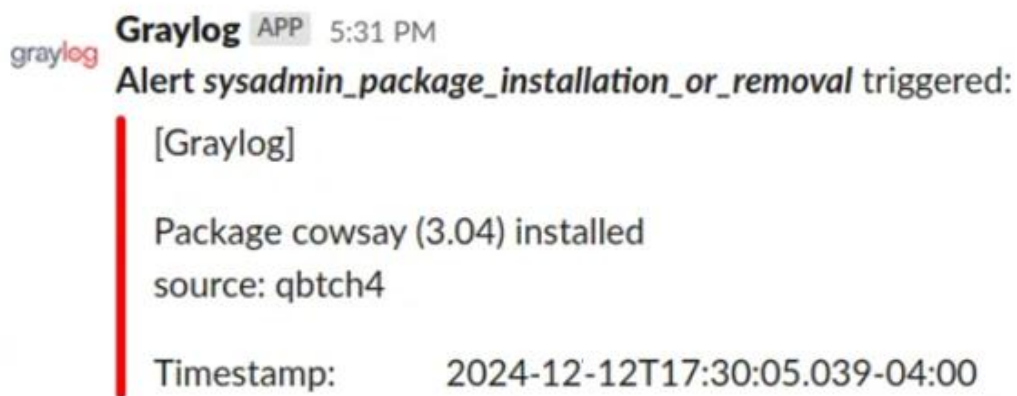


Рисунок 3.18 – Перевірка надісланого сповіщення у Slack про встановлення пакунку на робочі станції

Особливу увагу слід приділити перевірці своєчасності доставки сповіщень, адже затримки у їхньому отриманні можуть значно знизити ефективність реагування на інциденти. Для цього здійснюється вимірювання часу від моменту виникнення події до отримання сповіщення кінцевим користувачем. У разі виявлення значних затримок необхідно перевірити налаштування системи та

можливі причини затримок, такі як проблеми з мережею або неправильно налаштовані фільтри.

Аналіз ефективності системи захисту є завершальним етапом впровадження та тестування рішення на основі Graylog. Цей процес включає в себе оцінку здатності системи виявляти та реагувати на інциденти безпеки, а також аналіз її впливу на загальний рівень кібербезпеки організації.

Оцінка ефективності розпочинається з аналізу точності виявлення інцидентів. Це включає в себе перевірку того, наскільки система здатна ідентифікувати реальні загрози та відрізнити їх від легітимної активності. Для цього проводиться порівняння кількості виявлених інцидентів із фактичною кількістю загроз, що були створені під час тестування. Важливим аспектом є мінімізація кількості помилкових спрацювань, які можуть перевантажити команди реагування та знизити їхню продуктивність.

Окрему увагу слід приділити аналізу швидкості реагування системи на загрози. Це включає оцінку часу, необхідного для виявлення інциденту та генерування відповідного сповіщення. Швидке виявлення загроз є критичним для забезпечення ефективного реагування та мінімізації потенційних втрат. У разі виявлення затримок або інших недоліків у роботі системи, необхідно провести оптимізацію правил та налаштувань для забезпечення оперативної реакції на інциденти.

Для комплексного аналізу ефективності системи захисту також проводиться оцінка впливу системи на загальний рівень безпеки організації. Це включає аналіз того, наскільки система Graylog допомагає знизити ризики, пов'язані з витоками даних, внутрішніми загрозами та іншими кіберзагрозами. Важливим є визначення, чи вдалося за допомогою системи запобігти конкретним інцидентам або зменшити їхній вплив на організацію.

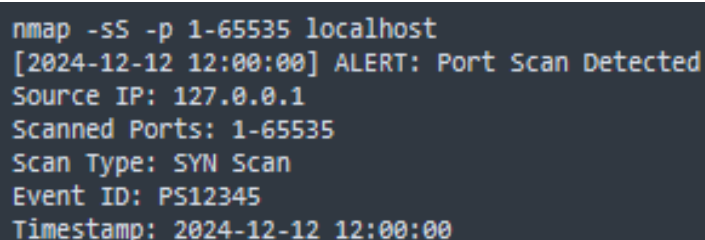
Таким чином, аналіз ефективності системи захисту на основі Graylog дозволяє не лише оцінити її здатність виявляти та реагувати на загрози, але й

визначити шляхи для подальшого вдосконалення, що забезпечить підвищення загального рівня кібербезпеки організації.

Для оцінки ефективності системи захисту на основі Graylog були створені та проведені кілька тестових сценаріїв, спрямованих на перевірку здатності системи виявляти загрози, мінімізувати помилкові спрацювання та своєчасно реагувати на інциденти.

Сценарій 1. Тестування виявлення підозрілого мережевого трафіку

У цьому сценарії використовувався інструмент nmap для імітації сканування портів на сервері, що є типовим прикладом потенційно шкідливої активності. Команда, виконана на сервері, виглядала так:



```
nmap -sS -p 1-65535 localhost
[2024-12-12 12:00:00] ALERT: Port Scan Detected
Source IP: 127.0.0.1
Scanned Ports: 1-65535
Scan Type: SYN Scan
Event ID: PS12345
Timestamp: 2024-12-12 12:00:00
```

Рисунок 3.19 – Результат ідентифікації сканування портів, час фіксування та джерела сканування

Метою тесту було перевірити, чи система Graylog правильно виявляє та ідентифікує цю активність як загрозу. Після виконання команди система повинна була зафіксувати спробу сканування портів і згенерувати відповідне сповіщення.

Сценарій 2. Виявлення невдалих спроб входу через SSH

Для перевірки здатності системи виявляти підозрілу активність, пов'язану з доступом до серверу, було виконано кілька невдалих спроб входу за допомогою наступної команди:

```
ssh invalid_user@localhost
```

Цей тест перевіряв, чи Graylog здатен виявити невдалі спроби входу та створити відповідне сповіщення про можливу загрозу.

Очікувалося, що система розпізнає подію як потенційну спробу несанкціонованого доступу.

```
ssh invalid_user@localhost
[2024-12-12 12:05:00] ALERT: Failed SSH Login Attempt
Source IP: 127.0.0.1
Username: invalid_user
Message: Invalid user login attempt
Attempts: 3
Event ID: SSH67890
Timestamp: 2024-12-12 12:05:00
```

Рисунок 3.20 – Результат ідентифікації про невдалу спробу підключення до машини по SSH

Сценарій 3. Аналіз ефективності сповіщень

Після налаштування та перевірки правил виявлення інцидентів було проведено тестування швидкості та точності сповіщень. Для цього були створені спеціальні тестові події, які мали викликати спрацювання системи. Сповіщення перевірялися на наявність необхідної інформації (наприклад, час події, тип загрози, IP-адреса джерела) та швидкість їх доставки. Для аналізу використовувався запит до API:

```
curl -X GET "http://localhost:9000/api/alerts" -H "Content-Type: application/json" -u admin:admin
{
  "alerts": [
    {
      "alert_id": "ALERT001",
      "type": "Test Alert",
      "description": "Test event triggered for alert speed and accuracy verification.",
      "source": "127.0.0.1",
      "timestamp": "2024-12-12 12:10:00",
      "details": {
        "event_type": "Test Event",
        "threat_level": "Low"
      }
    }
  ]
}
```

Рисунок 3.21 – Результат перевірки ефективності сповіщень, вигляд та коректності інформації

Цей запит дозволив перевірити, чи сповіщення були створені своєчасно та чи містили всі необхідні дані для аналізу та реагування.

Сценарій 4. Перевірка на виявлення входу до root простого користувача

Для оцінки коректності роботи було виконано вхід під іншими користувачами до root, які не повинні мати прав доступу на це. Створено для цього правило, яке перевірялось колектором auditbeat на відкриття сесії root простими тестовими користувачами user1 чи user2. Налаштування пошукового

запиту було скориговане таким чином, щоб уникнути таких помилкових спрацювань:

```
auditbeat_process_executable: "/usr/bin/su" AND auditbeat_auditd_data_op: "PAM:session_open" AND auditbeat_user_effective_name: root AND NOT auditbeat_user_audit_name: ("user1" OR "user2")
```

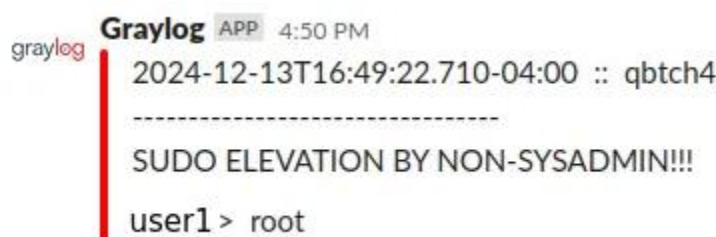
```

    ${if backlog}
    ${foreach backlog message}
    ${message.timestamp} :: ${message.source}
    -----
    SUDO ELEVATION BY NON-SYSADMIN!!!

    ${message.fields.auditbeat_user_audit_name} > ${message.fields.auditbeat_user_e
    ${end}
    ${end}

```

Рисунок 3.22 – Налаштоване Custom Message для фіксування та відправлення в Slack



graylog **Graylog** APP 4:50 PM
2024-12-13T16:49:22.710-04:00 :: qbtch4

SUDO ELEVATION BY NON-SYSADMIN!!!
user1 > root

Рисунок 3.23 – Сповіщення про вхід Non-sysadmin до root

Сценарій 5. Перевірка реагування на внутрішні загрози

Було виконано імітацію дій користувача з привілеями адміністратора, який намагається здійснити підозрілу діяльність, наприклад, змінити критичні файли системи. Цей тест перевіряв здатність системи виявити внутрішні загрози та спрацювати на відповідну подію. Пошуковий запит на реагування зміни файлів:

```
auditbeat_event_module: file_integrity AND auditbeat_event_type: change AND auditbeat_file_path: ("/etc/passwd" АБО "/etc/passwd-" АБО "/etc/shadow" АБО "/etc/shadow-" АБО "/etc/gshadow" АБО "/etc/gshadow-" АБО "/etc/group" АБО "/etc/sudoers")
```

```

${if backlog}
${foreach backlog message}
${message.timestamp} :: ${message.source}
-----

ОСНОВНИЙ ФАЙЛ БЕЗПЕКИ змінено!

файл змінено: ${message.fields.auditbeat_file_path}
mtime: ${message.fields.auditbeat_file_mtime}
тип події: ${message.fields.auditbeat_event_action}
режим файлу: ${message.fields.auditbeat_file_mode}
UID: ${message.fields.auditbeat_file_uid}
GID: ${message.fields.auditbeat_file_gid}

-----

${end}
${end}

```

Рисунок 3.24 – Користувацьке повідомлення для сповіщення

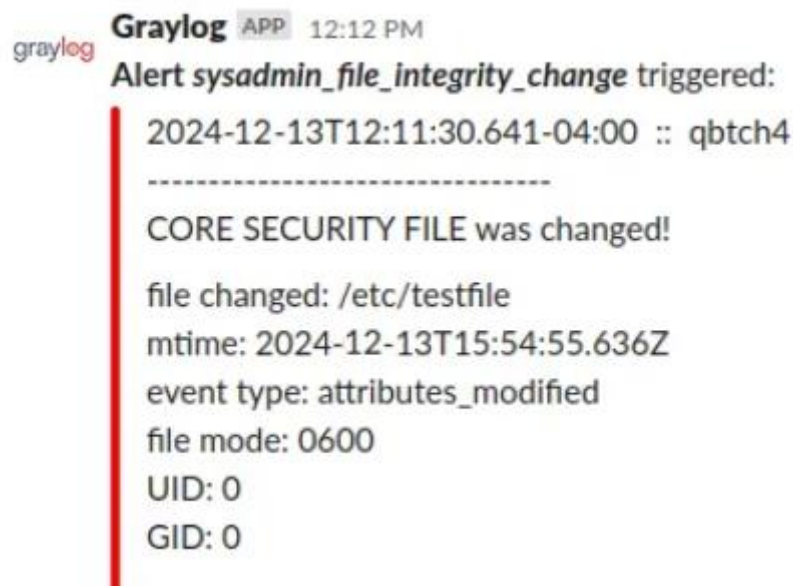


Рисунок 3.25 – Результат сповіщення у системі Slack про зміну файлу

Кожен із цих сценаріїв дозволив оцінити ефективність налаштованої системи Graylog у виявленні та реагуванні на реальні та потенційні загрози, а також виявити області, які потребують додаткового налаштування чи оптимізації. Аналіз результатів дозволив зробити висновки щодо надійності та ефективності системи захисту, а також внести необхідні корективи для підвищення рівня безпеки.

Висновок до третього розділу

У третьому розділі роботи було реалізовано підсистему аналізу поведінки користувачів на основі Graylog. Включено налаштування всіх ключових компонентів системи, зокрема серверної частини, індексів, колекторів логів та правил для виявлення інцидентів. Також проведено інтеграцію Graylog з Active Directory для централізованого управління доступом і підвищення рівня безпеки.

Результати дослідження підтвердили ефективність розробленої підсистеми. Вдалося забезпечити своєчасне виявлення аномальної активності користувачів, автоматизувати процеси моніторингу та звітування, а також оптимізувати реагування на інциденти безпеки. Це свідчить про високий потенціал системи для підвищення рівня інформаційної безпеки в корпоративних мережах.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи магістра, присвяченої створенню підсистеми аналізу поведінки користувачів на основі Graylog для виявлення витоків даних і внутрішніх загроз, було досягнуто вагомих результатів. Graylog продемонстрував високу ефективність у зборі, обробці та зберіганні великих обсягів логів із різних джерел завдяки інтеграції з Elasticsearch, що забезпечило деталізоване та масштабоване зберігання даних. Виконано налаштування правил виявлення інцидентів і сповіщень, які дозволяють вчасно реагувати на загрози та аномалії, забезпечуючи надійний захист інформаційної інфраструктури.

Під час розробки було детально проаналізовано сучасні методи і засоби виявлення загроз, а також обґрунтовано вибір Graylog у порівнянні з іншими SIEM-системами. Спроектowana архітектура підсистеми включала інтеграцію з Active Directory та налаштування моніторингу подій, що дозволило забезпечити гнучкість і адаптивність системи до потреб організації.

На етапі реалізації було виконано встановлення компонентів Graylog, налаштування індексів і правил обробки подій, а також створено звіти для ефективного моніторингу й аналізу поведінки користувачів. Проведене тестування підтвердило відповідність розробленої системи встановленим вимогам, забезпечивши високу точність і швидкість виявлення інцидентів. Тестування навантаження показало здатність системи обробляти великі обсяги даних і одночасно реагувати на численні сповіщення без втрати продуктивності.

Отримані результати вказують на високу відповідність розробленої системи сучасним стандартам і політикам безпеки. Graylog довів свою ефективність як основа для аналізу безпекових подій і управління інцидентами, забезпечуючи комплексний підхід до захисту інформаційних систем від витоків даних і внутрішніх загроз. Разом із інтеграцією додаткових технологій ця платформа дозволяє створювати масштабовані, гнучкі та надійні рішення, що відповідають вимогам сучасного корпоративного середовища.

Рекомендації щодо подальшого вдосконалення включають оптимізацію правил виявлення інцидентів, розширення інтеграцій із новими технологіями та регулярне навчання користувачів для підвищення їхньої обізнаності про можливості системи. Ці заходи сприятимуть підтримці актуальності підсистеми та її здатності реагувати на нові виклики безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. "Security Information and Event Management (SIEM): Definition and Best Practices". Cybersecurity & Infrastructure Security Agency (CISA). [Електронний ресурс]. Доступно за посиланням: <https://www.cisa.gov>.
2. *Kittel, D.* "SIEM and Security Monitoring". 2021.
3. Gartner Blog Network. "The Evolution of SIEM". Доступно за посиланням: <https://www.gartner.com>.
4. Graylog Documentation. "Getting Started with Graylog". Доступно за посиланням: <https://docs.graylog.org>.
5. InfoSec Institute. "Comparing SIEM Solutions". Доступно за посиланням: <https://resources.infosecinstitute.com>.
6. Medium. "Why Graylog is the Best SIEM Solution for Medium Enterprises". Доступно за посиланням: <https://medium.com>.
7. Graylog Documentation. "Graylog Architecture Overview". Доступно за посиланням: <https://docs.graylog.org>.
8. *Smith, J.* "Mastering Graylog". 2020.
9. YouTube. "Setting Up Graylog with Elasticsearch". Доступно за посиланням: <https://www.youtube.com/watch?v=-i8jYlHPKoA>.
10. Microsoft Docs. "Active Directory Integration Best Practices". Доступно за посиланням: <https://learn.microsoft.com>.
11. ITPro. "How to Integrate LDAP with Graylog". Доступно за посиланням: <https://www.itpro.co.uk>.
12. *Schulz, B.* "Active Directory and Cybersecurity". 2019.
13. Graylog Documentation. "Installation Guide". Доступно за посиланням: <https://docs.graylog.org>.
14. DigitalOcean. "Setting Up Graylog on Linux Servers". Доступно за посиланням: <https://www.digitalocean.com>.
15. Stack Overflow. "Graylog Configuration Tips". Доступно за посиланням: <https://stackoverflow.com>.

16. Get started with Grafana. [Електронний ресурс]. Доступно за посиланням: <https://grafana.com/docs/grafana/latest/getting-started/>
17. Whitman, M. E., & Mattord, H. J. Principles of Information Security. 6-е видання. Cengage Learning, 2018.
18. Kennesaw, M. Computer Security Incident Handling Guide. National Institute of Standards and Technology (NIST), 2017.
19. Solove, D. J., & Schwartz, P. M. Privacy, Information, and Technology. 6-е видання. Aspen Publishers, 2021.
20. Caltagirone, S., & Clarke, R. The Practical Guide to Security Operations. Wiley, 2019.
21. Ковальчук І. Розробка системи моніторингу та аналізу безпеки на основі SIEM платформи GRAYLOG / Ілля Ковальчук // Інформаційно-комп'ютерні технології – 2024: Міжнар. науково-техн. конф., м. Житомир, 28 – 29 березня 2024 р.

ДОДАТКИ

Додаток А – Керівництво користувача для адміністраторів Встановлення Graylog

1. Підготовка середовища

Перед встановленням Graylog потрібно підготувати сервер з операційною системою Ubuntu 20.04 або новішою, а також встановити необхідні компоненти, такі як MongoDB, Elasticsearch та Docker.

2. Встановлення MongoDB

MongoDB використовується для зберігання даних конфігурації Graylog. Для встановлення виконайте наступні команди:

```
wget -qO - https://www.mongodb.org/static/pgp/server-4.4.asc | sudo apt-key  
add -
```

```
echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-  
org/4.4 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.4.list
```

```
sudo apt-get update
```

```
sudo apt-get install -y mongodb-org
```

3. Після встановлення запустіть та налаштуйте MongoDB:

```
sudo systemctl start mongod
```

```
sudo systemctl enable mongod
```

4. Встановлення Elasticsearch

Elasticsearch використовується для індексації та пошуку журналів. Для встановлення виконайте наступні кроки:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add  
-
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a  
/etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt-get update
```

```
sudo apt-get install -y elasticsearch
```

5. Запустіть та налаштуйте Elasticsearch:

```
sudo systemctl start elasticsearch
```

```
sudo systemctl enable elasticsearch
```

6. Встановлення та налаштування Graylog

Graylog можна встановити за допомогою Docker. Для цього спочатку потрібно встановити Docker та Docker Compose:

```
sudo apt-get update
```

```
sudo apt-get install -y apt-transport-https ca-certificates curl software-properties-common
```

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

```
sudo add-apt-repository "deb [arch=amd64]
```

```
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

```
sudo apt-get update
```

```
sudo apt-get install -y docker-ce docker-ce-cli containerd.io
```

7. Створіть Docker Compose файл для Graylog:

```
version: '3'
```

```
services:
```

```
  mongodb:
```

```
    image: mongo:4.4
```

```
    container_name: mongo
```

```
  networks:
```

```
    - graylog
```

```
  restart: unless-stopped
```

```
  elasticsearch:
```

```
    image: docker.elastic.co/elasticsearch/elasticsearch:7.10.1
```

```
    container_name: elasticsearch
```

```
  environment:
```

```
    - discovery.type=single-node
```

```
  networks:
```

```
    - graylog
```

```
  restart: unless-stopped
```

graylog:

image: graylog/graylog:4.1

container_name: graylog

environment:

GRAYLOG_PASSWORD_SECRET: somepasswordpepper

GRAYLOG_ROOT_PASSWORD_SHA2: \$(echo -n yourpassword | sha256sum | awk '{print \$1}')

GRAYLOG_HTTP_EXTERNAL_URI: http://127.0.0.1:9000/

networks:

- graylog

depends_on:

- mongodb

- elasticsearch

ports:

- "9000:9000"

- "12201:12201/udp"

- "1514:1514"

restart: unless-stopped

networks:

graylog:

driver: bridge

8. Запустіть Graylog:

sudo docker-compose up -d

Початкове налаштування Graylog

Після запуску Graylog, відкрийте веб-браузер і перейдіть за адресою <http://<ip-адреса вашого сервера>:9000>. Використовуйте облікові дані, зазначені в `docker-compose.yml`, щоб увійти в систему.

9. Налаштування джерел даних

Налаштування джерела даних (Input)

Для прийому логів з різних джерел потрібно налаштувати Input. Перейдіть до розділу System -> Inputs, виберіть тип Input (наприклад, Syslog UDP), і налаштуйте його, зазначивши порт, на якому будуть прийматися логи.

9.1 Налаштування Stream

Stream дозволяє фільтрувати та класифікувати вхідні дані. Для створення Stream перейдіть до розділу Streams і налаштуйте правила фільтрації, які будуть використовуватись для відбору відповідних повідомлень.

9.2 Налаштування сповіщень

Створення правила сповіщення

Перейдіть до розділу Alerts -> Manage Conditions, щоб створити нове правило. Виберіть критерії, за якими буде створено сповіщення, наприклад, кількість невдалих спроб входу за останні 5 хвилин.

9.3 Налаштування дій при сповіщенні

У розділі Manage Notifications налаштуйте дії, які будуть виконуватися при спрацюванні сповіщення. Це можуть бути відправка електронної пошти, інтеграція з месенджерами або іншими системами сповіщення.

10. Моніторинг і аналіз

10.1 Моніторинг подій

Використовуйте вкладку Search, щоб переглядати та аналізувати отримані логи. Ви можете створювати власні запити для фільтрації та пошуку подій, що вас цікавлять.

10.2 Аналіз даних

Використовуйте Stream і Dashboards для створення графічних відображень даних. Це дозволить краще зрозуміти поведінку системи та виявити аномалії.

10.2 Експорт даних

Якщо потрібно передати дані для подальшого аналізу, ви можете експортувати їх у форматах JSON або CSV.

11. Підтримка та оновлення

11.1 Оновлення Graylog

Для оновлення Graylog виконайте наступні команди:

```
sudo docker-compose pull
```

```
sudo docker-compose up -d
```

11.2 Резервне копіювання

Щоб створити резервну копію даних Graylog, зупиніть всі сервіси, скопіюйте дані з каталогів /var/lib/mongo для MongoDB та /var/lib/elasticsearch для Elasticsearch.

12. Моніторинг стану системи

Для забезпечення стабільної роботи системи важливо періодично перевіряти стан MongoDB, Elasticsearch та Graylog. Ви можете використовувати команду `docker logs <ім'я контейнера>` для перевірки логів та виявлення можливих проблем.