Харківський національний університет імені В.Н. Каразіна
Факультет комп’ютерних наук
Безпека інформаційних систем і технологій

«Допущено до захисту»
Зав.кафедрою БІСТ
Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
спеціальність: 125 Кібербезпека

на тему: «Дослідження шляхів та вироблення рекомендацій щодо вибору та застосування SIEM-системи в корпоративній інформаційній системі»

оцінка « » Керівник к.т.н.Сватовський І.І. _____
(прізвище та ініціали/підпис)

Голова ЕК Рецензент к.т.н. Бакуменко Н.С. _____
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студентка групи КБ-41

Шорнікова І.О. _____
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 54 сторінки, 19 рисунків, 5 таблиць, посилання на 16 літературних джерел, та 1 додаток.

Метою дипломної роботи є дослідження та аналіз систем управління інформаційною безпекою та подій інформаційної безпеки, тобто систем SIEM.

Об’єктом дипломної роботи є SIEM - системи управління інформаційною безпекою та події інформаційної безпеки.

Методи дослідження: проведено аналіз методів захисту інформації в компанії з використанням сучасних систем SIEM.

Актуальність роботи полягає в тому, що сучасні механізми збору та аналізу журналів не є повністю ефективними, через що зловмисники можуть тривалий час залишатися непоміченими у внутрішній мережі.

Результатами проведеної роботи є висновок про те, що інформація надходить з різних джерел - таких як системи DLP, IDS, маршрутизатори, брандмауери, сервери і т. д. Крім того, бувають ситуації, коли на перший погляд нешкідливі події, отримані з різних джерел, разом несуть загрозу. Скажімо, коли лист із конфіденційними даними компанії надсилається особі, яка має на це право, але на адресу, що виходить за межі звичного кола адрес, на які він надсилає. Система DLP може не вловити це, але SIEM, використовуючи накопичену статистику, вже зафіксує інцидент на основі цього.

Ключові слова: СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ, SIEM, КІБЕРБЕЗПЕКА, МЕТОДИ КОРЕЛЯЦІЇ, SPLUNK.

ABSTRACT

The explanatory note contains 54 pages, 19 figures, 5 tables, references to 16 literature sources, and 1 appendix.

The purpose of the thesis is to study and analyze information security management systems and information security events, i.e. SIEM systems.

The object of the research of the thesis is SIEM - information security management systems and information security events.

Research methods: an analysis of information security methods in the company using modern SIEM systems.

The relevance of the work lies in the fact that modern mechanisms for collecting and analyzing logs are not fully effective, which is why attackers can go unnoticed in the internal network for a long time.

The results of this work show that information comes from various sources, such as DLP systems, IDS, routers, firewalls, servers, etc. In addition, there are situations where seemingly harmless events from different sources combine to pose a threat. For example, when an email with confidential company data is sent to a person who is authorized to receive it, but to an address that is outside the usual range of addresses to which it is sent. The DLP system may not catch this, but the SIEM, using the accumulated statistics, will already record an incident based on this.

Keywords: SECURITY MANAGEMENT SYSTEMS, SIEM, CYBERSECURITY, CORRELATION METHODS, SPLUNK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

AI – Штучний інтелект
CRE – Custom Rules Engine Механізм користувацьких правил
DLP – Data Leak Prevention Запобігання втраті даних
DS – Сервер розгортання
FIM – дані моніторингу цілісності файлів
GDPR – Загальний регламент захисту даних
HIPAA – Закон про перенесення та захист медичного страхування
HTTPS – Захищений протокол передачі гіпертексту
IDS – система виявлення вторгнень
IPS – Системи запобігання вторгненням
ISO – Міжнародна організація зі стандартизації
LB – Балансувальник навантаження
NTBA – аналітика мережевого трафіку та поведінки
OSSEC – хостова система виявлення вторгнень
PCI – Індустрія платіжних карток
SDEE – обмін подіями пристроїв безпеки
SEM – управління подіями безпеки
SIEM – Security information and event management Інформація про безпеку та управління подіями
SIM – управління інформаційною безпекою
SOC – Операційний центр безпеки
SPAN – Система портфельного аналізу ризиків
SQL – мова структурованих запитів
UAM – моніторинг активності користувачів
UDLA – універсальний адаптер журналу бази даних
UDP – Протокол датаграм користувача
UEBA – аналітика об’єктів і поведінки
XDR – Розширене виявлення й реагування

ВСТУП

Важко уявити сучасний світ без технологій, кожен процес, виробництво і навіть особисте життя пов'язані з ними. У процесі роботи кожен пристрій, починаючи від персонального комп'ютера і закінчуючи складними системами штучного інтелекту, фіксує в журналах реєстру всі події, що відбуваються в його системі. Завдяки даним, що записуються в ці журнали, адміністратор інформаційної безпеки може дати оцінку діяльності системи та сказати, які операції відбувалися в певний момент часу.

На даний момент аналіз записів журналу є провідним методом пошуку потенційно небезпечних і шкідливих дій у системі. Однак кожен пристрій має різну складність інфраструктури, тому кількість журналів реєстрації подій може сягати кількох десятків і аналізувати їх окремо один від одного практично неможливо.

Отже, щоб вирішити цю проблему централізованого збору та аналізу всіх подій, були створені перші системи, пізніше названі SIEM. Ці системи дозволяють обробляти велику кількість даних і відбирати лише ті, які становлять загрозу інформаційній безпеці та компанії в цілому. Програмне забезпечення SIEM діє як керуюча та інтегруюча ланка, яка розташована поверх існуючої системної інфраструктури та програмного забезпечення безпеки. Інструменти SIEM збирають і генерують усі комп’ютерні звіти, зареєстровані кожною окремою програмою, службою чи функцією безпеки в системі, відображаючи отримані дані в зручному для читання форматі. Детальніше про них:

- збір даних. Інструменти SIEM консолідують журнали подій і системні журнали, а також дані безпеки з різних джерел і програм в одному місці.
- збереження даних. Забезпечує можливість обслуговування безпеки для відображення даних у часових діапазонах і розслідування загроз або інцидентів, які спочатку могли залишитися непоміченими.

- аналіз інцидентів. Синтаксичний аналіз, нормалізація і категоризація, журнали — це додаткові функції інструментів SIEM, які роблять звіти зручнішими для пошуку.

Зараз кіберзлочинці постійно вдосконалюють свої методи атак, тому SIEM має бути на крок попереду. Необхідно періодично тестувати систему, імітуючи потенційні атаки та оцінюючи її відповідь. Атаки з уособленням можуть допомогти покращити вашу конфігурацію SIEM, налаштувавши правила кореляції, політики та процедури, щоб випереджати зловмисників.

Інформація надходить з різних джерел - таких як системи DLP, IDS, маршрутизатори, брандмауери, сервери і т. д. Крім того, бувають ситуації, коли на перший погляд нешкідливі події, отримані з різних джерел, разом несуть загрозу. Скажімо, коли лист із конфіденційними даними компанії надсилається особі, яка має на це право, але на адресу, що виходить за межі звичного кола адрес, на які він надсилає. Система DLP може не вловити це, але SIEM, використовуючи накопичену статистику, вже створить інцидент на основі цього.

Метою даної дипломної роботи є дослідження та аналіз систем управління інформаційною безпекою та подій інформаційної безпеки, тобто систем SIEM.

Об'єкт дослідження - SIEM - системи управління інформаційною безпекою та події інформаційної безпеки.

Предмет дослідження - аналіз методів захисту інформації в компанії з використанням сучасних систем SIEM.

Актуальність роботи полягає в тому, що сучасні механізми збору та аналізу журналів не є повністю ефективними, через що зловмисники можуть тривалий час залишатися непоміченими у внутрішній мережі.

Для досягнення поставлених цілей вирішувалися наступні задачі:

1) Аналіз характеристик і особливостей систем SIEM.

2) Дослідження збору даних та обробки подій у сучасних системах SIEM та їх порівняльна характеристика.

3) Опис та аналіз системи Splunk SIEM

1 СТАН ПИТАННЯ

1.1 Основні поняття, характеристики та застосування SIEM-системи

Термін SIEM був вперше введений Gartner у 2005 році. Злиття двох вже існуючих на той момент термінів: SIM (Security Information Management) - управління інформаційною безпекою, SEM (Security Event Management) - управління подіями безпеки. Згідно з цим визначенням, система SIEM повинна мати можливість збирати та аналізувати інформацію з різних мережевих пристроїв і пристроїв захисту інформації, а також містити системи контролю доступу, інструменти управління вразливістю та бази даних. Тобто SIEM - це програмний пристрій для централізованого збору даних журналів подій з різних машин користувачів, мережевих пристроїв і пристроїв захисту інформації для їх подальшої категоризації, класифікації та аналізу.

Як бачите, SIEM - це набір інструментів і технологій для керування інцидентами та подіями безпеки в одному місці. Ось деякі ключові особливості:

- Збір подій з різних джерел/пристроїв;
- Можливість зберігати події протягом необхідного часу;
- Забезпечення швидкого пошуку та можливість відновлення хронології;
- Забезпечення повноти інтерпретацій зібраних подій;
- Забезпечення можливості кореляції між подіями з різного джерела;
- Базова система сповіщень.

Існує багато різних компаній, тому кожна з них встановлює власні системи даних, але в цілому система виконує два основних завдання:

- створення та надання звітів про інциденти інформаційної безпеки, такі як діяльність програмного забезпечення, програмне забезпечення на сервері,

автентифікація користувачів на пристроях інформаційної діяльності

- аналіз інцидентів інформаційної безпеки та своєчасне попередження адміністратора про потенційну небезпеку, якщо діяльність порушує заздалегідь встановлені правила та набори політик безпеки [1].

Для виконання всіх поставлених перед системою завдань робота з подіями проходить у кілька етапів, які наведені в таблиці 1.1.

Таблиця 1.1 Етапи виконання завдання в системах SIEM.

№	Етап	Процес виконання
1)	Збирання даних	Дані в системі збираються з усіх джерел, починаючи від операційної системи, встановленої на робочі машини користувача, закінчуючи пристроями інформаційної безпеки: системи протидії вторгненням, мережеві екрани, антивірусне забезпечення.
2)	Нормалізація даних	Система збирає дані з величезної кількості логів різних систем, що записують дані у різному форматі, тому на даному етапі система приводить до одного структурного формату.
3)	Кореляція даних	На даному етапі система проводить аналіз отриманих даних, аналіз відбувається на основі правил, що надаються розробникам SIEM, або створені та налаштовані адміністратором з інформаційної безпеки. Правила кореляції визначають певну послідовність дій, що допомагає виділити більш важливі події, що відбуваються в системі.
4)	Формування звітів	Можливість візуалізації даних, або надання їх в більш зручній формі для обробки аналітиком.
5)	Сповіщення	Попередження адміністратора з інформаційної безпеки, про потенційно небезпечні дії, що відбуваються у системі.

Звичайно, стіл зі ступенями може бути доповнений іншими функціональними рішеннями, відповідно до цілей і завдань підприємства, на якому він встановлений, але все ж вона базова, і кожна сучасна SIEM

виконує описані вище дії.

Сучасні системи безпеки та управління подіями аналізу даних, отриманих із журналу реєстру, базуються на двох різних принципах, як це добре видно на рис. 1.1 [2].

Рисунок 1.1 – Основні принципи SIEM

Існує багато конкретних випадків використання SIEM, які застосовуються для отримання кращого результату, оскільки автоматизований цілеспрямований підхід необхідний як для загального аналізу загроз, так і для відповідності бізнесу.

Основні сфери використання SIEM:

1) HIPAA: Закон про перенесення та захист медичного страхування (HIPAA) вимагає, щоб дані пацієнтів були захищені фізичними, безпековими й мережевими заходами.

2) GDPR: Загальний регламент захисту даних (GDPR) — це основний європейський закон про конфіденційність даних, який вимагає певним захистом особистих даних європейських громадян. Крім того, організації також зобов’язані вести реєстр порушень персональних даних, а це означає, що потрібен інструмент для повідомлення про будь-які порушення даних.

3) PCI: Індустрія платіжних карток (PCI) — це ще одна ситуація, де можна використовувати інструмент SIEM, оскільки інформація про кредитну картку також підлягає багатьом вимогам безпеки.

4) Внутрішні загрози. Внутрішні загрози є ще одним важливим випадком використання інструментів SIEM. Користувачі, які мають доступ

до конфіденційної та приватної інформації, повинні бути ретельно відібрані та захищені, і жоден користувач не повинен мати більше доступу до даних, ніж йому потрібно для виконання своєї роботи.

5) Зловживання привілейованим доступом. Використання привілейованого доступу є ще однією причиною, чому організації повинні використовувати інструменти SIEM. Моніторинг доступу до системи, привілеїв і поведінки облікового запису є важливим, щоб запобігти зловживанню привілейованим доступом до того, як воно станеться.

6) Полювання на загрози. Інструменти SIEM також можуть допомогти у загальних процесах пошуку та ідентифікації загроз, оскільки вони можуть сповіщати вас про незвичайні події, облікові записи, які поводяться дивно, або велику кількість незвичних журналів. Це може допомогти вказати, коли почалася атака або чи було зламано обліковий запис або програму до злому чи втрати даних.

7) Загальна безпека: для цілей загальної безпеки інструменти SIEM корисні в тандемі з брандмауерам для захисту від зовнішніх загроз і добре працюють із інструментами керування правами доступу для захисту конфіденційних даних від внутрішнього доступу. [3].

1.2 Особливості систем SIEM

SIEM збирає та обробляє дані. Дані базуються на журналах. Журнал, також відомий як файл журналу — це файл даних про роботу машини або програми. Файли журналу включають такі типи: FlatFile, SysLog, журнали подій Microsoft, дані моніторингу цілісності файлів (FIM), UDLA (універсальний адаптер журналу бази даних), SDEE (обмін подіями пристроїв безпеки), дані контрольних точок тощо.

Журнали містять дані про активність пристрою, стан працездатності, взаємодію користувача з пристроєм, а також ефективність і діяльність програми.

SIEM збирає дані журналу з різноманітних джерел, пов’язаних із цими системами, мережами та мережевими пристроями та програмами. Дані

журналу, які збираються, можуть бути пов’язані з безпекою, несанкціонованою діяльністю, зловживанням ресурсами компанії, діяльністю користувачів, цілісністю файлів і багатьма іншими поширеними обчислювальними діями.

Джерело журналів - це тип журналу або унікальний журнал, що походить від певного хоста.

Журнали генеруються в різноманітних форматах і представляють різний ступінь важливості для підтримки та захисту мережі. Журнали зазвичай мають форму журнальних повідомлень.

1.2.1 Що відбувається з даними журналу, коли вони надходять у SIEM

Як правило, на провідних платформах SIEM журнал повідомлень підлягає декільком процесам.

Журнал повідомлень "нормалізовано за часом", щоб гарантувати, що мітки часу відображають той самий часовий пояс. Потім він витягує та позначає метадані, активно аналізує та розбиває журнал повідомлень на основні компоненти.

Потім кожному ідентифікованому повідомленню журналу призначається класифікація та загальна подія, щоб допомогти ідентифікувати тип дії, описаний у повідомленні. Контекст загрози та ризику також можна провести, щоб оцінити кожен журнал і призначити значення пріоритету на основі ризику.

1.2.2 Вилучення метаданих і маркування

Вилучення та позначення метаданих активно аналізує та розбиває журнал повідомлень на основні компоненти, визначаючи, який тип даних містить журнал повідомлень, значення, що стоїть за повідомленням, і відносну важливість дії, описаної в повідомленні.

По суті, платформа SIEM бере необроблене повідомлення журналу та аналізує його, полегшуючи використання даних. Дані, витягнуті з

повідомлення журналу, називаються метаданими.

Метадані зберігаються в базах даних із використанням загальних полів метаданих, тож на них можна швидко посилатися для більш ефективного пошуку, уможливлюючи поглиблені звіти та аналіз.

Метадані класифікуються як:

Контекстні метадані - це поля, які безпосередньо аналізуються з журналів повідомлень. Зазвичай вони мають текстовий і описовий характер відносно повідомлення. Наприклад, вони включають суб'єкт, джерело домену та об'єкт.

Кількісні метадані - це поля, які безпосередньо передаються з повідомлень журналу та можуть використовуватися для числового порівняння. Наприклад, вони включають отримані хостом байти, швидкість і розмір.

Окрім аналізу метаданих безпосередньо з журналів повідомлень SIEM може отримувати деякі журнали. Отримані метадані – це поля, які використовують проаналізовану інформацію в повідомленнях журналу для надання додаткового контексту про повідомлення. Наприклад, вони включають:

- походження предмета;
- з'ясування господаря впливу;
- напрямок.

Провідні платформи SIEM призначають класифікацію та загальну подію кожному визначеному журналу повідомлень.

Класифікації визначають широкий спектр видів діяльності. Існує три основні типи класифікації (з підкласифікаціями нижче):

- аудит;
- операції;
- безпека.

Загальні події не обов’язково повинні бути точними, але вони повинні надавати більш чіткий контекст для дії, описаної в повідомленні журналу.

Перетворюючи багато різних типів повідомлень журналу з багатьох різних систем у загальне подання (або загальні поля метаданих), платформа SIEM порівнює, а потім зіставляє дані, які інакше не могли б бути пов’язаними (і, отже, корисними).

Подія – це журнал, який є більш важливим для операцій, безпеки чи відповідності та зазвичай включає такі класифікації, як: помилки, збої або атаки.

1.2.3 Події (події безпеки)

Події – це лише ті елементи журналу, які є корисними, тобто вони мають більше значення, ніж інші журнали.

Журнали містять такі елементи, як помилки входу, спроби злому та підвищені дозволи. Або елементи, пов’язані з системою, наприклад збої служби чи програмного забезпечення та сповіщення про перезавантаження.

Зазвичай події становлять 5% або менше від загальної кількості зібраних журналів. Після виявлення подій вони використовуються як частина моніторингу в реальному часі, звітування, розслідування та виявлення небезпек.

Відповідний SIEM також допомагає створювати та видавати сповіщення та звіти, часто включаючи систему сигналізації в реальному часі, щоб сповіщати користувачів і системи про виконання певних критеріїв. Крім того, система загроз повинна включати дії для розумної реакції на певні сценарії, які спостерігає платформа SIEM. Звіти потім дозволяють користувачам створювати детальні або зведені звіти на основі даних колоди, зібрані платформою [4].

1.3 SIEM як вдосконалена система виявлення вторгнень

На думку деяких експертів, SIEM є вдосконаленою системою для виявлення шкідливих дій і різних системних аномалій. SIEM дозволяє побачити більш повну картину мережевої активності та подій безпеки. Коли звичайні засоби виявлення не бачать атаку окремо, але її можна виявити шляхом ретельного аналізу та співвіднесення інформації з різних джерел. Так, багато організацій використовують системи SIEM як додатковий і дуже важливий елемент захисту від цілеспрямованих атак. [5].

1.4 Основні функції SIEM

Приклад №1: Атаки SQL ін'єкції.

Атаки SQL-ін’єкції існували завжди. Атаки становлять загрозу веб-сайтам і базам даних. Все, що потрібно, це кілька зловмисних команд, щоб зламати сервер SQL, і їх можна ввести, щоб відкрити конфіденційну інформацію.

Щоб цього не сталося, SIEM надають кілька варіантів. Перший — це система виявлення вторгнень (IDS), яка сканує мережу на наявність шкідливого вмісту, націленого на розгортання SQL.

Якщо систему було зламано, IDS негайно повідомить вас. Це дає змогу встигнути та вжити відповідних заходів до того, як дані будуть видалені. Навіть якщо немає безпосередньої небезпеки, ви завжди повинні перевіряти системи, на яких працює SQL, щоб виявити порушення.

Приклад №2: Напади на водопій.

Важко уявити, але атаки на водопій неймовірно ефективні та їх важко виявити. Принцип роботи цього методу полягає в тому, що один заражений сайт заражає інший. Атака починається, коли для зараження вибрано цільовий веб-сайт. Потім створюються профілі відвідувачів, які часто користуються цільовим веб-сайтом. Коли вони відвідують веб-сайт із уразливими місцями, зловмисники навмисно впроваджують у нього шкідливий код. Під час повторного відвідування код перенаправляє відвідувачів на веб-сайт третьої сторони, де вони заражаються шкідливим програмним забезпеченням.

Коли ці відвідувачі знову відвідають цільовий сайт, зловмисне програмне забезпечення заразить його.

Рисунок 1.2 – Зображення атак водопою

Хоча їх важко виявити, SIEM можуть стримувати атаки Watering Hole на будь-якому етапі. Система IDS постійно шукає зловмисне програмне забезпечення, яке намагається отримати доступ до веб-сайту або скомпрометувати інші життєво важливі системи.

Приклад №3: зараження шкідливими програмами.

Атаки зловмисного програмного забезпечення залишаються популярними, як ніколи. Про це знає навіть пересічний користувач комп'ютера: шпигунське програмне забезпечення, троянські програми та програми-вимагачі. Зловмисники покладаються на неліцензійне програмне забезпечення, намагаючись створити початковий опір. У цих випадках зловмисному програмному забезпеченню надається перевага через легкість, з якою його можна встановити в системі.

Традиційні технології безпеки не встигають за атаками шкідливих програм. Нове зловмисне програмне забезпечення розробляється майже щодня, через що більшість систем недостатньо обладнані для ефективного пошуку потенційних загроз. SIEM дозволяють вам використовувати цілодобові дані, якими керує спільнота OTX, щоб бути в курсі.

Усі вхідні повідомлення від відомих шкідливих хостів перевіряються на наявність загрози встановлення зловмисного програмного забезпечення через електронну пошту або завантаження. OTX Backup — це система IDS,

яка відстежує джерела трафіку, націлені на вразливі системи. Повідомлення буде надіслано, якщо зловмисне програмне забезпечення Seciruty спробує зупинити службу безпеки або змінити файли в системі. Зазвичай це робиться для запобігання виявленню вторгнення.

Приклад №4: відповідність.

Відповідність вимоги і нормативні стандарти є надзвичайно важливими. Будь-яке недотримання таких стандартів, як HIPAA або GDPR, може коштувати компанії мільйони доларів або навіть банкрутства. Існує нагальна потреба знайти способи кращого управління цим процесом.

За допомогою SIEM можна одночасно перевірити стан відповідності процесів безпеки для системи, замість того, щоб вручну обходити кожну систему. Централізована інформаційна панель звітів надає інформацію про місцезнаходження та стан відповідності критичних активів.

Інформаційна панель має сотні вбудованих звітів, що означає, що ви можете запускати їх усі одночасно. Існують звіти, які допомагають відповідати майже всім відповідним стандартам. Кілька прикладів включають PCI-DSS, ISO 27002, HIPAA та GDPR. Якщо існують унікальні вимоги до звітності, ці звіти можна легко налаштувати відповідно до ваших потреб.

Ось короткий підсумок того, як SIEMs можуть отримати переваги всього за кілька кліків:

- Запобігання атакам SQL-ін’єкцій шляхом моніторингу справності систем.
- SIEM дозволяє легко відстежувати підозріле спілкування, яке натякає на будь-яку атаку.
- Відстеження погроз, інфекцій, зловмисного програмного забезпечення.
- Постійний моніторинг [6].

1.5 Джерела інформації систем SIEM

Завдання SIEM полягає в аналізі інформації, що надходить від різних систем, таких як антивірус, DLP, IDS, маршрутизатори та інші, і виявити відхилення від норм за деякими критеріями. Якщо таке відхилення

виявлено, система генерує інцидент. Тобто серед багатьох записів у системних журналах рішення SIEM виявляє сліди деяких підозрілих дій. Важливо, що з його допомогою можна виявити дії, які зовні виглядають абсолютно нешкідливими, але в сукупності становлять загрозу.

Основні джерела інформації:

1) Доступ, контроль, автентифікація.

Управління доступом - термін безпеки, який використовується для позначення набору політик для обмеження доступу до інформації, інструменти та фізичні місця розташування.

Автентифікація - це будь-який процес, за допомогою якого система перевіряє особу користувача, який бажає отримати доступ до системи.

2) DLP-системи.

Запобігання втраті даних (DLP) – це практика виявлення та запобігання витоку даних, викраденню або небажаному знищенню конфіденційних даних.

3) IDS/IPS-системи.

Системи виявлення вторгнень (IDS) - аналізують мережевий трафік на наявність сигнатур, які відповідають відомим кібератакам. Системи запобігання вторгненням (IPS) також аналізують пакети, але також можуть зупиняти доставку пакета на основі виявлених атак, допомагаючи зупинити атаку.

4) Антивірусне програмне забезпечення.

Антивірусне програмне забезпечення - це клас програмного забезпечення, призначеного для запобігання, виявлення та видалення зловмисного програмного забезпечення на окремих комп’ютерних пристроях, мережах та IT-системах.

5) Інтернет-екрани.

Інтернет-екрани - це комплекс програмно-апаратних засобів, призначених для фільтрації вхідного та локального трафіку за деякими заздалегідь заданими критеріями.

6) Мережеве обладнання.

Мережеве обладнання- це обладнання, що містить електронні схеми, які отримують живлення від електричної мережі або інших джерел і виконують функції підсилення, перетворення сигналу та інші.

7) Сканери вразливостей.

Сканери вразливостей - це програмні або апаратні засоби, що використовуються для діагностики та моніторингу мережевих комп'ютерів, які дозволяють сканувати мережі, комп'ютери та програми для виявлення можливих проблем у системі безпеки, оцінки та усунення вразливостей.

8) Системи веб-фільтрації.

Веб-фільтрація- це технологія, яка не дозволяє користувачам переглядати певні URL-адреси чи веб-сайти, не дозволяючи їхнім браузерам завантажувати сторінки з цих сайтів [7].

ВИСНОВКИ ДО РОЗДІЛУ 1

SIEM - це управління існуючими системами та контроль безпеки. Він об'єднує та уніфікує інформацію, що міститься в системах, дозволяючи аналізувати її діяльність за допомогою єдиного інтерфейсу. SIEM є чудовим прикладом принципу «сміття входить, сміття виходить». SIEM корисний лише тоді, коли до нього надсилається інформація. Чим повнішу інформацію про мережі, системи та активи отримує SIEM, тим ефективніше вона допоможе виявляти й аналізувати загрози.

Окрім основних варіантів використання SIEM для керування подіями та журналами, SIEM також використовується для інших цілей. Одним з альтернативних способів використання є допомога в демонстрації відповідності таким нормам, як HIPAA, PCI, SOX і GDPR.

Успішні атаки на комп'ютерні системи рідко схожі на справжні атаки, за винятком найпримітивніших. Зловмисники зазвичай намагаються видалити або виправити записи журналу, щоб замести сліди.

Зрештою, це джерело інформації, якій можна довіряти, і яка є критично важливою для будь-якого розслідування втручання в роботу комп’ютерних систем. SIEM надає більш детальне уявлення про те, що

відбувається в мережі, ніж будь-яка інша система керування безпекою чи джерело інформації:

- система виявлення вторгнень (IDS) розпізнає лише пакети, протоколи та IP-адреси;
- Endpoint Security бачить файли, імена хостів і користувачів;
- журнали обслуговування відображають дані входу користувачів, діяльність служби та зміни конфігурації;
- система управління активів бачить програми, процеси і власників.

З джерел даних для систем SIEM можна виділити:

- Журнали подій, які записуються клієнтами та контролюють права доступу.
- Антивіруси. Цей тип рішення повідомляє про виявлення шкідливого програмного забезпечення або коду.
- DLP (запобігання втраті даних). Такі системи контролюють і запобігають несанкціонованому переміщенню інформації за межі мережі.
- Системи контролю доступу. Служать для отримання доступу до інформаційного потоку.
- IDS / IPS. Такі системи передають інформацію про зміни в правах доступу або мережевих атаках.
- Інтернет-екрани. Такі рішення передають інформацію про наявне шкідливе програмне забезпечення та інциденти безпеки.
- Мережеве обладнання. Контролює доступ користувача до різних інформаційних потоків і зчитує трафік.
- Веб-фільтр. Цей додаток контролює доступ до шкідливих сайтів [9].

2 ПОРІВНЯННЯ СУЧАСНИХ SIEM СИСТЕМ

У цьому розділі розглянуто та проаналізовано роботу трьох інструментів SIEM, наведено порівняльну характеристику. Лідерами ринку були обрані: Splunk, LogRhythm і IBM QRadar.

Splunk — це передова, масштабована та ефективна технологія, яка індексує та шукає журнали, що зберігаються в системі. Він аналізує дані, створені машиною, щоб забезпечити оперативну розвідку. Основна перевага використання Splunk полягає в тому, що для зберігання даних не потрібна база даних, оскільки для зберігання даних широко використовуються її каталоги [10].

Пакет LogRhythm SIEM розроблений для середніх і великих організацій і складається з повнофункціональної платформи, яка використовується для створення загальнокорпоративної системи виявлення загроз і реагування на них. Пакет SIEM від LogRhythm об’єднує все в одній панелі скляного контролера: керування корпоративними журналами, аналітику безпеки, аналітику об’єктів і поведінки (UEBA), аналітику мережевого трафіку та поведінки (NTBA) і автоматизацію безпеки [12].

IBM QRadar — це продукт безпеки та керування подіями або SIEM, розроблений для підприємств. Інструмент збирає дані з організації та мережевих пристроїв. Він також підключається до операційних систем, ресурсів хосту, додатків, вразливостей, дій і поведінки користувачів. IBM QRadar використовується для аналізу даних журналу та мережевих потоків у режимі реального часу, щоб зловмисні дії можна було виявити та зупинити якомога швидше. Таким чином, головна мета IBM QRadar — запобігти або звести до мінімуму шкоду для організації, що приймає [15].

2.1 Обробка подій у сучасних SIEM–рішеннях

2.1.1 Обробка подій у Splunk

Splunk бере дані та індексує їх у об’єкти для пошуку у формі подій. Потік даних показує основні процеси, які діють на дані під час індексування. Ці процеси складають обробку подій.

Обробка подій відбувається в два етапи: аналіз та індексація. Усі дані надходять через конвеєр для аналізу у великих обсягах. Під час аналізу програмне забезпечення Splunk розбиває ці фрагменти на події. Потім він передає події в конвеєр індексації, де відбувається остаточна обробка. Під час аналізу та індексування програмне забезпечення Splunk перетворює дані.

Під час аналізу програмне забезпечення Splunk виконує низку дій, зокрема:

- Витягує набір стандартних сховищ для кожної події, включаючи хост, джерело та тип джерела.
- Параметри кодування набору символів.
- Визначення завершення одного з процесів за допомогою правил.
- Визначення або створення позначок часу.
- Анонімізація даних на основі конфігурації.
- Застосування власних метаданих до вхідних подій на основі конфігурації. [10].

2.1.2 Обробка подій у LogRhythm

Технологія збору LogRhythm спрощує агрегування даних журналу, подій безпеки та інших машинних даних. Збирачі даних можуть працювати локально або віддалено, дані централізовано контролюються та керуються для спрощення розгортання та керування. Масштабованість розгортання додатково покращується завдяки балансуванню навантаження додатків між процесорами даних.

Збирачі даних забезпечують цілісність даних під час збоїв у мережі, інтелектуально розгортаючи незалежний трафік UDP і відстежуючи стан енергонезалежних даних.

Збирач даних - забезпечує дистанційний, високоефективний збір усіх машинних даних, включаючи повідомлення журналу, дані додатків, події безпеки та мережеві потоки.

Програмне забезпечення для збору даних - локальний збір виконується системним монітором, програмним забезпеченням, яке також функціонує як монітор кінцевої точки. Він консолідує та збирає журнали та машинні дані з віддалених середовищ і хмарної інфраструктури [13].

Рисунок 2.1 – Покрокова візуалізація збору даних у LogRhythm

2.1.3 Обробка подій у IBM QRadar

Обробка даних у IBM QRadar полягає в тому, що дані про події та потокові дані запускаються через спеціальну систему керування правилами, яка генерує порушення та сповіщення, а потім дані записуються в сховище.

Дані подій і потокові дані можуть оброблятися моноблоком без необхідності додавати процесори подій або потокові процесори. Якщо потужність обробки багатофункціонального пристрою перевищена, вам може знадобитися додати процесори подій, потокові процесори або будь-який інший пристрій обробки для виконання додаткових вимог. Інші функції, такі як QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM) або QRadar Incident Forensics, збирають різні типи даних і надають більше функціональних можливостей [15].

2.2 Збір інцидентів у сучасних інструментах SIEM

2.2.1 Ризик доступу адміністратора

Інформаційна панель Incident Review відображає важливі події та їх поточний статус. Splunk виявляє шаблони в даних і автоматично сканує події на наявність інцидентів безпеки за допомогою виявлення кореляції. Коли кореляційний пошук виявляє підозрілий шаблон, створюється сповіщення, яке називається важливою подією.

Інформаційна панель Incident Review охоплює всі важливі події та класифікує їх за потенціалом за суворістю, щоб була можливість швидко сортувати, призначати та відстежувати проблеми.

Процес збору інцидентів:

- Адміністративний аналітик. Перегляд інцидентів, ітерація та сортування на високому рівні за новоствореними важливими подіями.
- Коли відомий інцидент вимагає розслідування, адміністративний аналітик призначає завдання аналітику з огляду, щоб розпочати розслідування інциденту.
- Аналітик, який перевіряє, оновлює статус події з «Нове» на «Виконується» та починає досліджувати причину відомої події.
- Аналітик переглядає, досліджує та збирає інформацію про події, використовуючи поля та дії на полі у важливій події. Аналітик записує деталі свого дослідження в поле коментаря відомої події.
- Після перегляду для усунення причини відомої події та вирішення будь-яких завдань відновлення або підвищення рівня аналітик встановлює для важливої події статус «Вирішено».
- Аналітик надає важливу подію кінцевому аналітику для перегляду.
- Остаточний аналітик переглядає та затверджує внесені зміни
- Вирішення проблеми та встановлення статусу «Закрито» [10].

2.2.2 Збір інцидентів у LogRhythm

Компанія LogRhythm розробила три спеціальні сервіси, які швидко розпізнають нові загрози, і потім захищають середовище від майбутніх атак за допомогою спеціальних правил ШІПлагіни Engine і SmartResponse. [13].

2.2.3 Збір інцидентів у IBM

QRadar – може бути використаним для збору даних безпосередньо з мережі, або ви можете використовувати збирачі, такі як збирачі подій. Колектори QRadar або QRadar QFlow для збору даних подій або потоків. Дані аналізуються та нормалізуються перед тим, як надходять на рівень обробки. Коли необроблені дані аналізуються, вони нормалізуються, щоб представити їх у структурованому та зручному для користувача форматі.

Дані про події представляють події, які відбуваються в певний момент часу в середовищі користувача, як вхід користувача, електронна пошта, VPN-з’єднання, заборона брандмауера, проксі-з’єднання та будь-які інші події, що виникають під час входу на пристрій.

Потокові дані — це інформація про мережеву активність або інформація про сеанс між двома хостами в мережі, яку QRadar перетворює на записи протоколу. QRadar перетворює або нормалізує необроблені дані в IP-адреси, порти, кількість байтів і пакетів, а також іншу інформацію в записи потоку, які фактично представляють сеанс між двома хостами. На додаток до збору інформації про потік за допомогою засобу збирання потоків, повне захоплення пакетів доступне за допомогою компонента QRadar Incident Forensics [16].

2.3 Методи кореляції подій у сучасних системах SIEM

2.3.1 Методи кореляції подій у Splunk

Splunk підтримує п'ять типів кореляції:

- За часовими та географічними координатами. На основі часу та географічного розташування ви можете побачити всі або будь-яку

частину подій, що відбуваються протягом певного періоду часу, а також визначити їхнє місцезнаходження.

- На основі транзакцій. Відстежує ряд пов'язаних подій як одну транзакцію. Ці події можуть відбуватися з будь-якої кількості окремих IT-систем і джерел даних.
- Під обшуком. Взяти результати одного пошуку та використати їх в іншому, щоб створити умови if/then. Використання під пошуком дозволяє користувачам бачити результати пошуку лише за певних умов.
- Пошук. Може використовуватися для покращення, збагачення, перевірки або додавання контексту до даних, зібраних у Splunk.
- Приєднання. Як частина рядка пошуку може зв'язувати один набір даних з іншим на основі одного або кількох загальних полів. Два абсолютно різних набори даних можуть бути пов’язані один з одним на основі поля імені користувача або ідентифікатора події, що призведе до єдиного перегляду [11].

2.3.2 Методи кореляції подій у LogRhythm

AI Engine LogRhythm — це повністю інтегрований компонент платформи LogRhythm, який забезпечує автоматизований і безперервний аналіз, кореляцію всіх типів активності, що спостерігається в навколишньому середовищі. Завдяки унікальному гнучкому та комплексному підходу він забезпечує видимість у реальному часі ризиків, загроз і критичних операцій, які інакше неможливо виявити на практиці.

AI Engine дозволяє організаціям передбачати, виявляти та швидко реагувати на:

- Тонкі вторгнення.
- Інсайдерські загрози.
- Шахрайство
- Аномалії поведінки з користувачами та мережами.

- Порушення відповідності.
- Збої в IT-сервісах [12].

2.3.3 Методи кореляції подій у IBM QRadar

Консоль QRadar обробляє дані лише відповідно до правил, указаних у профілі історичної кореляції.

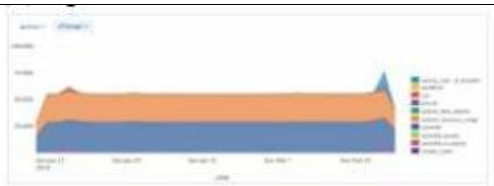
Загальні правила перевіряють дані як за подіями, так і за потоками. Ви повинні мати дозвіл на перегляд подій і потоків, перш ніж ви зможете додати загальні правила до профілю. Коли профіль редагується користувачем, який не має дозволу на перегляд подій і потоків, загальні правила автоматично видаляються з профілю.

Оскільки обробка історичної кореляції відбувається в одному місці, правила, включені в профіль, розглядаються як глобальні правила. Обробка не змінює правило з локального на глобальне, але обробляє правило так, ніби воно було глобальним під час виконання історичної кореляції. Деякі правила, як-от правила стану, можуть не мати такої відповіді, як звичайна кореляція, що виконується на локальному процесорі подій. Наприклад, локальне правило, яке відстежує п’ять невдалих входів протягом 5 хвилин від одного імені користувача, поводиться по-різному в звичайних і історичних кореляціях. При нормальній кореляції це локальне правило підтримує лічильник для кількості невдалих входів, отриманих кожним локальним процесором подій. У історичній кореляції це правило підтримує єдиний лічильник для всієї системи QRadar. У цій ситуації правопорушення можуть відрізнятися від нормального співвідношення [16].

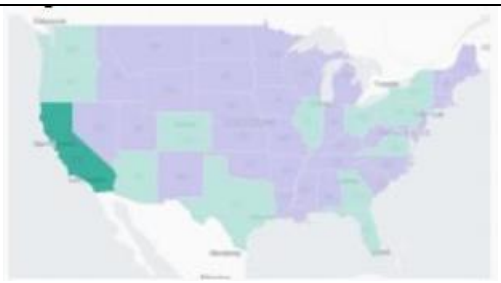
2.4 Візуалізація та інтерфейс сучасних SIEM-рішень

2.4.1 Візуалізація та інтерфейс Splunk

Таблиця 2.1 Візуалізація та інтерфейс Splunk [11].

Ім’я	Візуалізація	Використання
Список подій		1) Показує події без подальшої обробки. 2) Показує витягнуті поля та значення безпосередньо на інформаційній панелі.
Таблиці		1) Виберіть один або кілька конкретних полів з результатів пошуку. 2) Можна додати форматування, щоб підкреслити тенденції чи моделі в певних сферах.
Діаграми		Забезпечує можливість використовувати такі види діаграм: 1) Пиріг; 2) Площа, лінія, стовпець, смуга; 3) Пузир і розлив.
Єдиний		Відстежує останні зміни чи тенденції вартості в режимі реального часу.
Датчики		1) Показує зведений показник даних за діапазоном. 2) Відстежує показник, коли він наближається до певної мети.

Продовження таблиці 2.1 Візуалізація та інтерфейс Splunk [11].

Мапа		Можна скористатися мапою Хороплет, показати і порівнювати регіональні тенденції або концентрації.

2.4.2 Візуалізація та інтерфейс LogRhythm

Ось деякі з основних методів візуалізації, які використовуються в LogRhythm для виділення основних напрямків, включаючи розробку безпеки, операції безпеки та управління.

1) Нові показники перевірки тривоги.

Щоб спростити процес, ми застосовуємо практику переведення нових нагадувань у «бета-статус» і створення чернеток процедур перед виробництвом. Див. рис. 2.2 – знімок цього графіка.

Рисунок 2.2 – Хибнопозитивні показники бета-сигналу за останні 30 днів

2) Візуалізація розгортання LogRhythm.

Візуалізація огляду розгортання LogRhythm, показана на малюнку, забезпечує швидкий і простий спосіб побачити поточний стан розгортання.

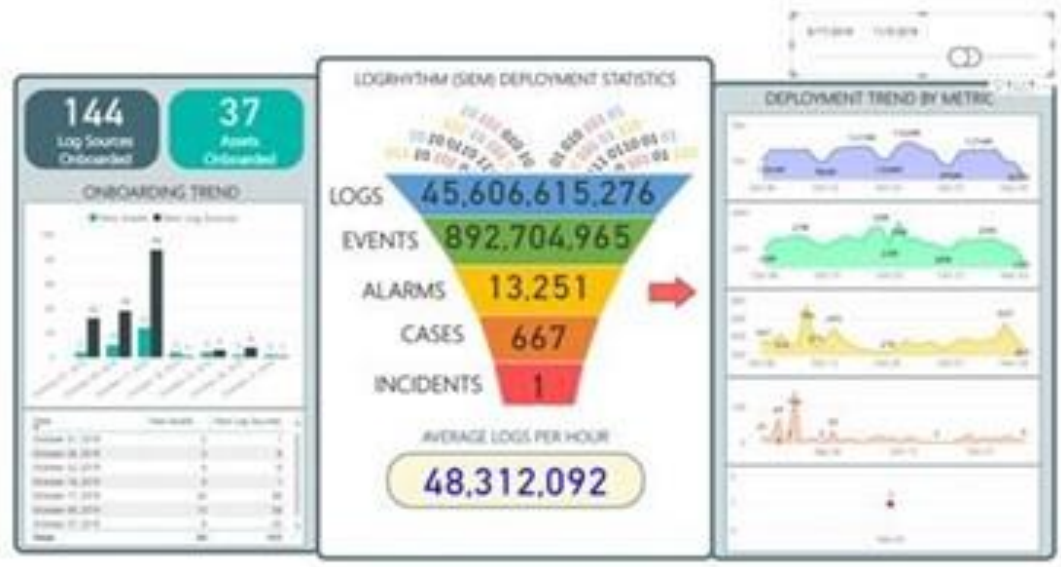


Рисунок 2.3 – Огляд розгортання LogRhythm у Power BI

Візуалізація показників тривожності.

Для оперативних цілей відстежуються загальні індикатори тривоги, які можна переглянути за потрібні періоди за допомогою повзунка календаря [14].

Рисунок 2.4 – Візуалізація метрик тривоги LogRhythm у Power BI

2.4.3 Візуалізація та інтерфейс QRadar

QRadar-панель управління.

Інформаційна панель — це робоче середовище, яке надає звіт і детальну інформацію про події в мережі.

Рисунок 2.5 – Панель керування в консолі QRadar-вкладка правопорушень

Рисунок 2.6 – Вкладка Правопорушення в консолі QRadar-вкладка журналів активності

Використання журналу діяльності для поглибленого дослідження даних про події.

Рисунок 2.7 – Вкладка журналів активності в консолі Qradar−Вкладка активів

QRadar автоматично виявляє активи, сервери та хости, які працюють у вашій мережі.

Рисунок 2.8 – Вкладка «Активи» в консолі QRadar−Вкладка «Звіти» [14]

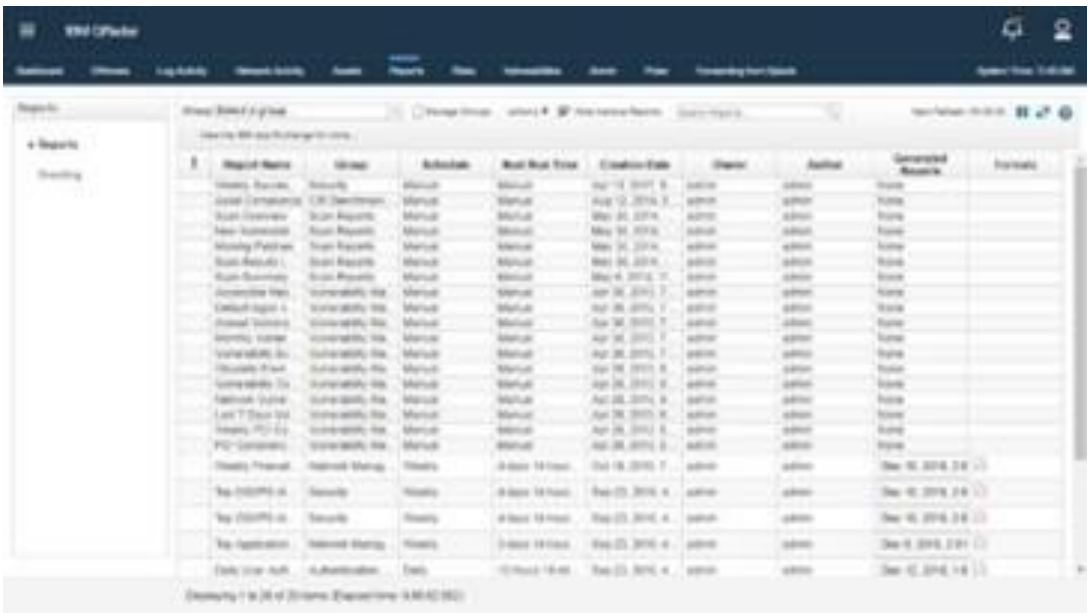


Рисунок 2.9 – Вкладка Звіти в консолі QRadar

2.5 Глобальні параметри і вбудовані функціональні інструменти SIEM

2.5.1 Глобальні параметри та вбудовані функції Splunk

Основні функції та параметри Splunk:

- Універсальне пересилання (UF): основне завдання цього елемента - просто пересилати дані журналу з сервера.
- Балансувальник навантаження (LB): елемент, який розподіляє мережевий трафік або трафік додатків між кластером серверів.
- Heavy forward (HF): цей компонент Splunk дозволяє фільтрувати дані. Наприклад, це допоможе накопичувати лише журнали помилок.
- Індексатор: основним завданням індексатора є зберігання та індексування відфільтрованих даних.
- Пошук голови (SH): це просто зразок splunk, який використовується для досягнення розвідки та виконання звіту.
- Сервер розгортання (DS): допомагає розгортати конфігурацію, наприклад оновлювати файл конфігурації UF (універсальний пересилач) [12].

2.5.2 Глобальні параметри та вбудовані функції LogRhythm

LogRhythm розроблено для роботи в умовах, що постійно змінюються, загроз і викликів із повним набором високоефективних засобів безпеки, відповідності та операційних інструментів. Він забезпечує повне та корисне розуміння того, що насправді відбувається в IT-середовищі підприємства [12].

- AI Engine
- Технологія збирання
- Моніторинг цілісності файлів
- Управління справами
- Геолокація та візуалізація
- Моніторинг кінцевих точок
- Звітність
- SmartResponse.

2.5.3 Глобальні параметри та вбудовані функції IBM QRadar

Розгортання QRadar може містити такі компоненти:

1) Консоль QRadar.

Консоль QRadar надає інтерфейс користувача QRadar і перегляд подій і потоків у реальному часі, звіти, порушення, інформацію про активи та адміністративні функції.

2) Колектор подій QRadar.

Збирач подій пов’язує або з’єднує подібні події, щоб зберегти використання системи, і надсилає дані до процесора подій.

3) Процесор події QRadar.

Процесор подій обробляє події за допомогою Custom Rules Engine (CRE). Якщо події відповідають настроюваним правилам CRE, визначеним на консолі, процесор подій виконує дію, визначену для відповіді на правило.

4) QRadar QFlow Collector.

Колектор потоків збирає потоки, підключаючись до порту SPAN або мережевого TAP.

5) Вузол даних QR.

Вузли даних дозволяють новим і існуючим розгортанням QRadar підвищувати потужність зберігання та обробки за потреби. Вузли даних допомагають збільшити швидкість пошуку у вашому розгортанні, надаючи більше апаратних ресурсів для виконання пошуку.

6) Хост програми QRadar.

Хост програми – це керований хост, призначений для запуску програм. Хости програм надають додаткове сховище, пам’ять і ресурси ЦП для програм, не впливаючи на обчислювальну потужність консолі QRadar [15].

2.6 Особливості сучасних SIEM-рішень

2.6.1 Особливості Splunk

Важливими функціями Splunk є:

- Прискорення розробки та тестування;
- Створення програми даних у реальному часі;
- Гнучка статистика та звітність з архітектурою реального часу;
- Можливості пошуку, аналізу та візуалізації для розширення можливостей користувачів усіх типів [10].

2.6.2 Особливості LogRhythm

Ось основні функції LogRhythm:

- моніторинг в реальному часі;
- автоматичні відповіді;
- управління життєвим циклом загроз;
- управління журналами;
- моніторинг мережі та кінцевих точок;

- виявлення загроз за допомогою аналізу даних [13].

2.6.3 IBM QRadar

IBM QRadar SIEM — один із найкращих продуктів для управління безпекою для організації. Переваги використання цього продукту перераховані нижче.

- Повна видимість хмарних і традиційних середовищ.
- Усунення ручних завдань.
- Виявлення загроз в реальному часі.
- Функції безпеки.
- Можливість звітності.
- Кар'єра в IBM QRadar [15].

При виборі системи SIEM необхідно детально розібрати переваги та недоліки кожної з них. Для цього найкраще буде порівняти основні характеристики обраних інструментів SIEM. Порівняльна характеристика сучасних систем SIEM наведена в додатку А.

ВИСНОВКИ ДО РОЗДІЛУ 2

У цьому розділі були розглянуті три найпопулярніші інструменти SIEM: Splunk, LogRhythm і IBM QRadar.

Інструменти порівнювали за такими характеристиками: стратегія, основні функції, компоненти, обробка подій, збір інцидентів, кореляція, візуалізація, цінова політика та клієнтський досвід.

Кожен продукт має свої плюси і мінуси, кожен має свої сильні сторони. При виборі SIEM-рішення рекомендується поставити завдання і відповідно від нього відштовхуватися. Всі інструменти мають безкоштовну версію на 30 днів, але досить часто для вирішення конкретного завдання потрібні додаткові програми. Тому потрібно купувати ліцензії, а вони досить дорого коштують. Однак втрати компанії без моніторингу подій і виявлення загроз будуть значно більшими.

Наприклад, LogRhythm XDR Stack забезпечує інтегрований набір можливостей, які підтримують основну місію SOC – моніторинг, пошук і дослідження загроз. Ви також можете покластися на дизайн і візуалізацію, які вам більше подобаються.

З розвитком технологій рішення SIEM також розвиваються і вдосконалюються, є багато аналогів, таких як OSSEC, ManageEngine EventLog Analyzer, SolarWinds Security Event Manager та багато інших. Рекомендується визначити пріоритет захисту інформаційної безпеки та відповідно вибрати бажану систему SIEM.

3 ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМ SPLUNK SIEM

Splunk був обраний як наочний приклад того, як працює сучасна система SIEM. Він досить простий в установці, а також має безкоштовну версію на 60 днів. Легкий і зручний інтерфейс. Це одне з найкращих рішень SIEM для перших спроб збору та аналізу подій.

Перше, що вам потрібно зробити, це створити профіль на офіційному сайті і завантажити дистрибутив. На сайті є інструкція з установки. Після установки програма відкривається в браузері і вам потрібно авторизуватися в профілі.

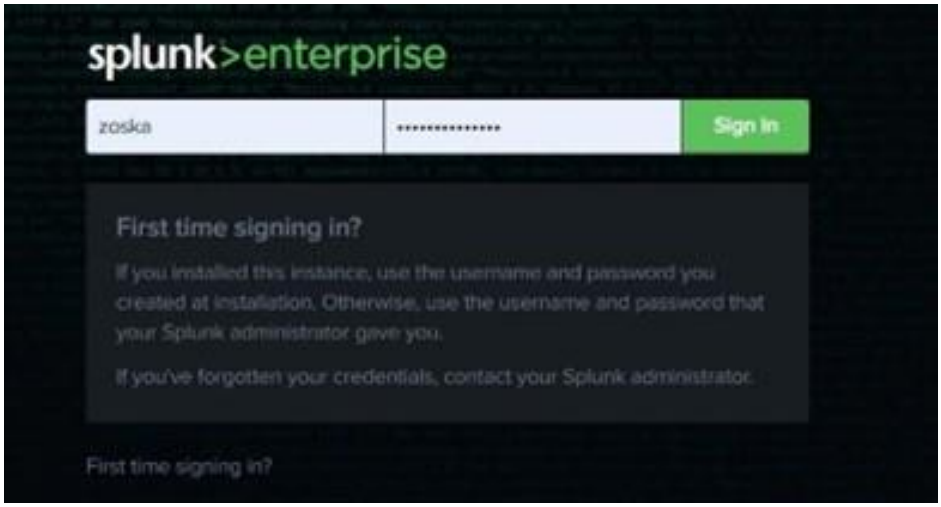


Рисунок 3.1 – Вхід у програму Splunk

Інтерфейс Splunk показаний на рис. 3.2. Як бачите, він досить простий і зрозумілий для простого користувача.

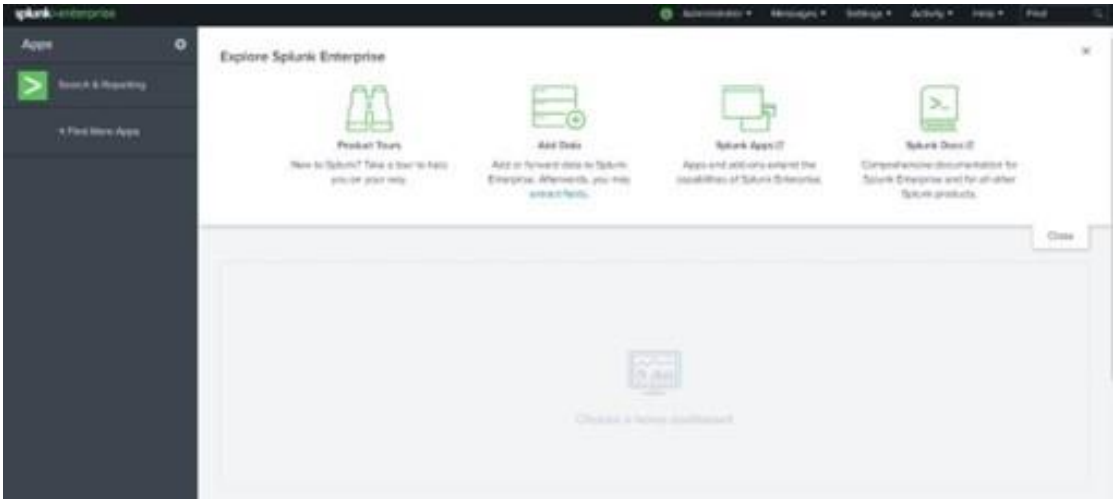


Рисунок 3.2 – Домашня сторінка Splunk

3.1 Збір інформації в Splunk

Коли дані додаються до розгортання Splunk, вони обробляються та перетворюються на серію окремих подій, які можна переглядати, шукати та аналізувати.

Платформа Splunk приймає будь-які типи даних. Зокрема, він працює з усіма інформаційними потоками та історичними даними. Джерелом даних можуть бути журнали подій, веб-журнали, мережеві канали, системні показники, моніторинг змін, черги повідомлень, архівні файли тощо. Загалом джерела даних згруповані в такі категорії, див. таблицю 3.1.

Таблиця 3.1 Категорії джерел даних, з яких Splunk збирає інформацію

Джерело даних	Опис
Файли та каталоги	Більшість даних находить безпосередньо з файлів і каталогів.
Мережеві події	Програмне забезпечення Splunk може індексувати віддалені дані з будь-якого мережевого порту та події SNMP від віддалених пристроїв.
IT-оператор	Дані з IT-операцій, таких як Nagios, NetApp і Cisco.
Хмарні сервіси	Дані з хмари сервісів, таких як AWS і Kinesis.
Сервіси баз даних	Дані з баз даних, таких як Oracle, MySQL і Microsoft SQL Server,
Служби безпеки	Дані служб безпеки, наприклад McAfee, Microsoft Active Directory і Symantec Endpoint Protection.
Послуги віртуалізації	Дані служб віртуалізації, наприклад VMWare і XenApp.
Сервери додатків програми	Дані з серверів додатків, таких як JMX і JMS,програми WebLogic і WebSphere.

Продовження таблиці 3.1 Категорії джерел даних, з яких Splunk збирає інформацію

Вихідні коди Windows	Windows приймає широкий спектр специфічних для Журналів Windows, включаючи журнали подій Windows, реєстр вікна, WMI, активний довідник і моніторинг ефективності.
Інші джерела	Підтримуються інші джерела вхідного сигналу. Черги FIFO та вхідні скрипти для отримання даних від API та інших віддалених інтерфейсів даних.

Процес перетворення даних називається індексуванням. Протягом індексації вхідні дані обробляються для забезпечення швидкого пошуку та аналізу. Оброблені результати зберігаються в індексі як події. Індекс — це сховище файлів для даних.

Події зберігаються в індексі як група файлів, які розділені на дві категорії:

- Необроблені дані – це дані, які додаються до розгортання Splunk. Необроблені дані зберігаються в стислому форматі.
- Індексні файли, які містять деякі файли метаданих, які вказують на необроблені дані.

Як приклад, збір інформації про помилки автентифікації буде використовуватися для виявлення потенційно зловмисників, які намагаються отримати доступ. У пошуку введіть fail* password, щоб зібрати всі неправильні записи пароля, див. рис. 3.3. На малюнку також показаний результат пошуку, який показує, що при введенні пароля було 2550 помилок.

Результати пошуку показують наступне:

- Часова шкала: показує розподіл відповідних подій у часі у формі гістограми подій. Часові рамки можна збільшувати та зменшувати, щоб зрозуміти розподіл подій у часі.

- Бічна панель полів: показує поля, отримані з подій автентифікації в результатах пошуку.
- Перегляд подій: відображає необроблені події з виділенням відповідних пошукових систем, за замовчуванням спочатку відображається остання подія.

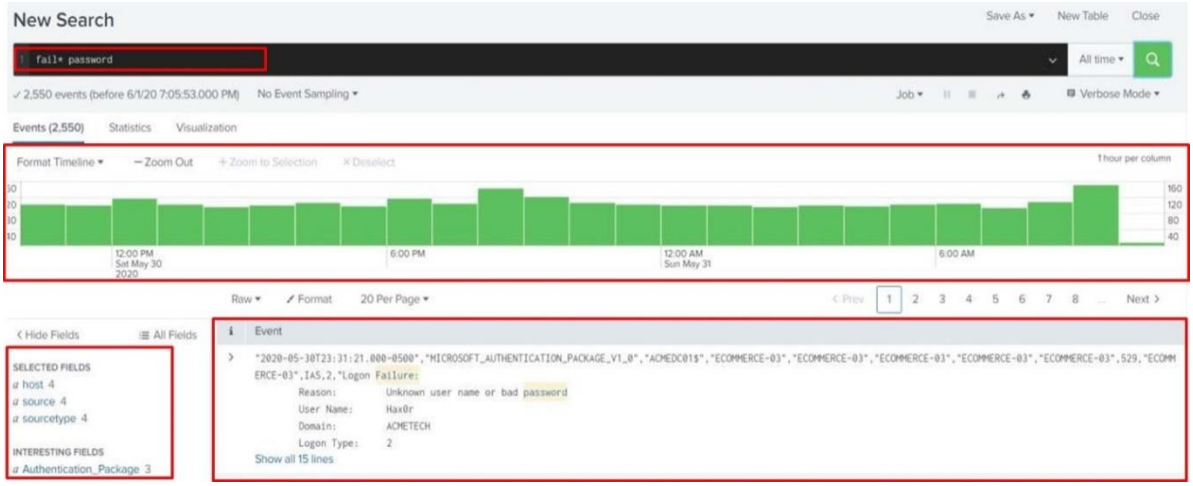


Рисунок 3.3 – Результат пошуку «fail* password»

3.2 Зберігання інформації в Splunk

Під час створення пошуку є кілька варіантів збереження пошуку, див. таблицю 3.2.

Таблиця 3.2 Параметри збереження пошуку в Splunk

параметр	опис
Зберегти як звіт	Створюється пошук, який буде запущено з самого початку, і можливість зберегти його як звіт.
Інформаційна панель	Також можна зберегти пошук як інформаційну панель. В інформаційних панелях можливі одна або декілька панелей, які можуть відображати результати пошуку в таблицях або графічних візуалізаціях.
Сповіщення	Є можливість зберегти пошук як сповіщення. Сповіщення – це дія, яку ініціює збережений пошук на основі результатів пошуку. Дією може бути надсилання електронного листа або виконання сценарію.

Продовження таблиці 3.2 Параметри збереження пошуку в Splunk

Тип події	Ви можете зберегти пошук як тип події. Типи подій – це система категоризації, яка допомагає зрозуміти дані. Типи подій дозволяють переглядати величезні масиви даних, знаходити схожі шаблони та створювати сповіщення та звіти.

Далі отримані дані зберігаються у звіті, щоб їх було зручніше переглядати та завжди мати під рукою.

Рисунок 3.4 – Збереження звіту даних пошуку

3.3 Аналіз отриманих даних та особливості реагування на події

Після пошуку помилок автентифікації, перегляду джерела (src), призначення (dest) і залучених користувачів (users) наступним кроком є аналіз даних. Щоб визначити, які користувачі намагалися увійти на які хости. Помилки автентифікації аналізуються за допомогою простої статистики, тобто кількість помилок автентифікації агрегується за джерелом (src), одержувачем (dest), користувачем, який намагається ввійти в цільову систему (user) і типом джерела (sourcetype) для фільтрації та перегляду статистики , див. рис. 3.5

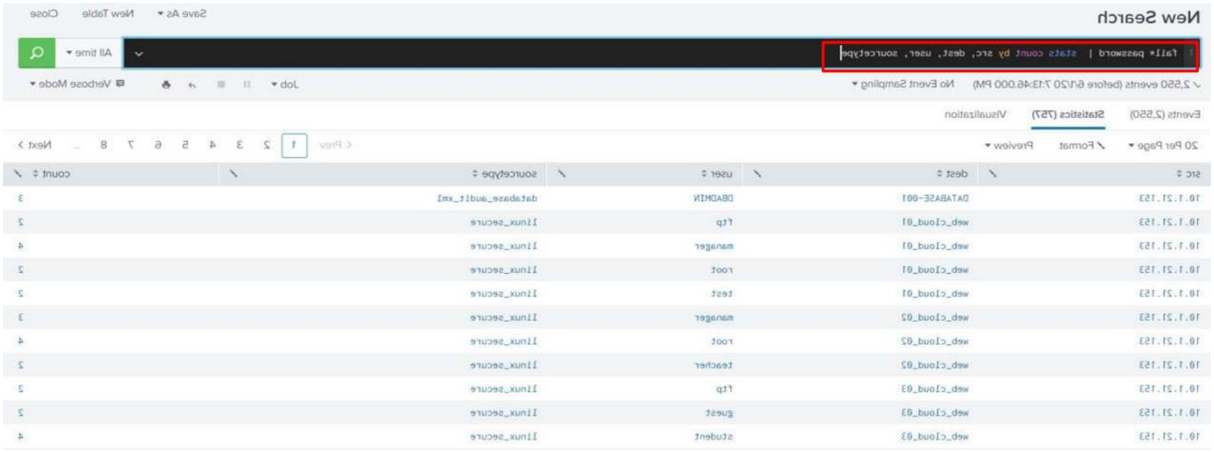


Рисунок 3.5 – Відфільтрована статистика помилок

Численні невдалі спроби автентифікації — це більше ніж просто загроза. Належне візуальне застосування полегшує представлення результатів аналізу. Вибирається «Візуалізація», а потім вибирається тип діаграми, яка може відображати зв’язки сутностей між вузлом джерела, хостом призначення, користувачами та кількістю їхніх дій, дивіться рис. 3.6. На зображенні видно, що найчастіші спроби були з хоста 10.1.21.153.

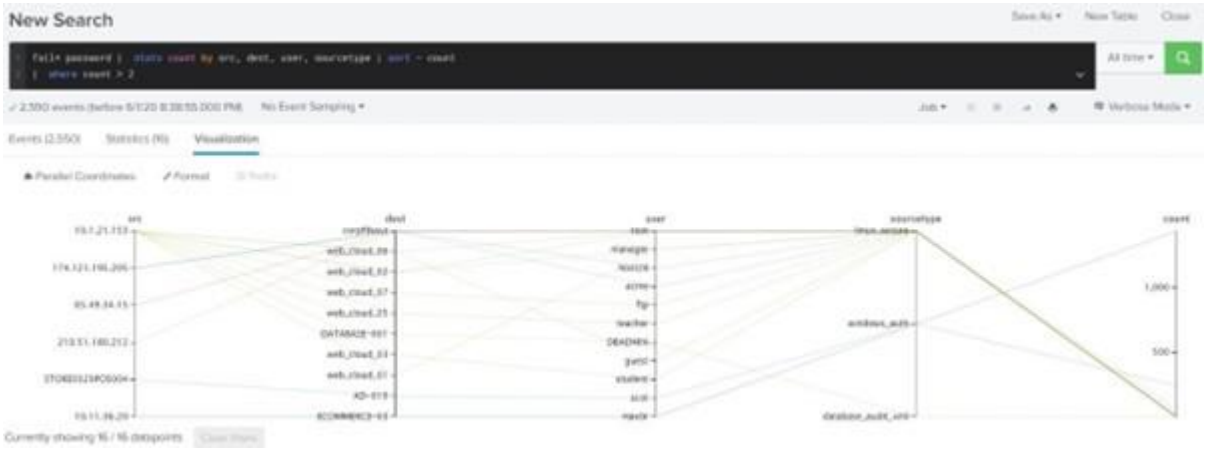


Рисунок 3.6 – Візуалізація найбільших спроб автентифікації

Ми продовжили досліджувати хост 10.1.21.153, який намагався отримати доступ до кількох веб-серверів і критичного сервера бази даних. Переглянута візуалізація невдалих спроб вихідного хоста отримати доступ до різних напрямків у часі, див. рис. 3.7. На зображенні показано найбільшу кількість спроб 30 травня 2020 року о 20:00 та 21:00.

Рисунок 3.7 – Візуалізація спроб хоста 10.1.21.153 отримати доступ

Графічний дисплей дозволяє легко розрізнити кількість невдалих спроб автентифікації за призначенням, див. рис. 3.8.

Рисунок 3.8 – Смуга візуалізації для кращого розуміння кількості відмов спроби

Ця візуалізація дає змогу швидко візуалізувати кількість атак із хоста 10.1.21.153, упорядкованих за призначенням протягом певного часу. За допомогою цієї візуалізації можна визначити такі аспекти атаки:

- Послідовність спроб автентифікації, зроблених зловмисником протягом певного часу проти різних активів.
- Інтервал і тривалість активності, що показує повторюваний шаблон спроб зловмисника, який використовує той самий хост протягом певного часу.

ВИСНОВКИ ДО РОЗДІЛУ 3

Коротке дослідження показало, що Splunk може ефективно та легко знаходити події, створювати звіти та фільтрувати інформацію. Як приклад наведено приклад виявлення загрози у вигляді некоректної автентифікації. Як видно з результатів, використовуючи правила кореляції, непотрібні дані сортуються і залишаються лише найважливіші.

За допомогою візуалізації узагальненої статистики в інтерактивних діаграмах, які дозволяють проводити більш детальний аналіз у часі та перевіряти конкретні підозрілі дії. Розуміючи попередні спроби автентифікації, можна визначити, що невдалі спроби автентифікації, ймовірно, були ініційовані зараженим зловмисним програмним забезпеченням хостом (10.1.21.153), який досліджував внутрішню мережу.

Крім того, Splunk має багато інших можливостей, таких як: збирати дані з машини, з інших осей, з веб-сайтів, а також ви можете імпортувати вже зібрані дані та аналізувати їх. Дані можна завантажувати на сервер. Потім у пошуку сортуйте та вибирайте дані, створюйте звіти та графіки. За допомогою часового діапазону легко зрозуміти, коли відбулася та чи інша подія. Крім того, однією з корисних функцій Splunk є те, що ви можете надавати та скасовувати права доступу іншим користувачам. Це дозволяє розповсюджуватись у внутрішньому середовищі компанії.

ВИСНОВКИ

У роботі проаналізовано характеристики та особливості роботи та джерела інформації, з якими працює система SIEM. Системи SIEM досліджувалися як додатковий і дуже важливий елемент захисту від цілеспрямованих атак, у яких система виявляє вторгнення.

Сучасні системи безпеки та управління подіями аналізують дані, отримані з журналу реєстру, на основі двох різних принципів: використання правил кореляції та побудова моделей користувачів і активів.

Перетворюючи багато різних типів повідомлень журналу з багатьох різнорідних систем на спільну мову, платформа SIEM може порівнювати схожі, а потім співвідносити дані, які інакше не були б відносними.

SIEM в основному використовується в HIPAA, PCI, GDPR, інсайдерських загрозах, зловживанні привілейованим доступом, пошуку загроз і для загальної безпеки.

Збір даних та обробка подій у сучасних системах SIEM та їх порівняльні характеристики також досліджувалися за такими критеріями: кореляція подій, візуалізація, глобальні параметри, функціональність та особливості.

Вибір правильного інструменту SIEM залежить від ряду факторів, зокрема бюджету організації та стану безпеки.

Однак компаніям слід шукати інструменти SIEM, які пропонують такі можливості:

- звітність про відповідність;
- реагування на інциденти та криміналістика;
- моніторинг доступу до бази даних і серверів;
- виявлення внутрішніх і зовнішніх загроз;
- моніторинг, кореляція та аналіз загроз у реальному часі для різних програм і систем;

- система виявлення вторгнень (IDS), IPS, брандмауер, журнал подій програми та інші інтеграції програм і системи;
- розвідка загроз;
- моніторинг активності користувачів (UAM).

На прикладі сучасної системи Splunk SIEM досліджено спроби несанкціонованого доступу до інформації. Показувалися звіти та статистика всіх подій, що відбувалися в системі. Далі за допомогою кореляції залишаються тільки найнебезпечніші журнали.

Це дало чітке розуміння роботи та чого призначений SIEM для організацій. Варто пам'ятати, що з розвитком технологій розвивається і кіберзлочинність. Кожен день зловмисники намагаються підкорити новітні системи. Вони намагаються запустити шкідливе програмне забезпечення, віруси або отримати несанкціонований доступ до інформації. Для будь-якої компанії це принесе великі збитки, і навіть може призвести до закриття. У компанії повинен бути окремий відділ із захисту інформації та працююча система SIEM.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Іванов О. Що таке системи SIEM і навіщо вони потрібні? URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases (дата звернення: 23.04.2023).
2. Мелоун М., Зінк Д. Думай як хакер: Посібник системного адміністратора з кібербезпеки. 2017. 85 с.
3. Найпопулярніші приклади використання SIEM для кореляції та найкращих практик сповіщень SIEM // DNSstuff. 2020. URL: 7 Top SIEM Use Cases and SIEM Alerts Best Practices - DNSstuff (дата звернення: 03.05.2023).
4. ЩО ТАКЕ SIEM? (ЧАСТИНА 3): ЯК ПРАЦЮЄ SIEM?/Compact SOC, Cyber Security. 2018. URL: What is SIEM? (Part 3): How does SIEM work? - CyberOne (дата звернення: 17.05.2023).
5. ПЕТТЕРС Дж. Що таке SIEM? Посібник для початківців. Вароніс, 2020. URL: What is SIEM? A Beginner’s Guide (varonis.com) (дата звернення: 17.05.2023).
6. Vault A. 4 варіанти використання SIEM, які значно покращать безпеку вашого підприємства / Infocorp Security&Networking. URL: Página no encontrada – Infocorp (дата звернення: 17.05.2023).
7. Сандерс К. Прикладний моніторинг безпеки мережі: збір, виявлення та аналіз. 225 Wyman Street, Waltham, MA 02451, США, 2014. 467 с.
8. Захарова М. Синтез механізмів захисту інформаційних ресурсів від кібератак. Автореф. канд. техн. наук ДСК.
9. SIEM – Security Information and Event Management. Интегратор Amica. URL: SIEM – Security Information and Event Management (дата звернення: 17.05.2023).
10. Карассо Д. Досліджуючи Splunk. Нью-Йорк, 2012. 156 с.
11. Бамгарнер В. Впровадження Splunk: звітування та розробка великих даних для оперативної розвідки. Бірмінгем, 2013. 417 с.
12. Preimesberger C. Splunk vs. LogRhythm: SIEM Head-to-Head. eWEEK, 2019. URL: Splunk vs. LogRhythm: SIEM Head-to-Head - eWEEK (дата звернення:

17.05.2023).

13. Lentz R. Definitive Guide to Security Intelligence and Analytics. Аннаполіс, 2019. 61 с.
14. Jacobs J. Безпека, керована атакою: аналіз, візуалізація та панелі інструментів. Канада, 2014. 321 с.
15. Savaram R. IBM QRadar Tutorial. MindMajix, 2019. URL: IBM QRadar Tutorial | What Is IBM QRadar - Updated 2023 (mindmajix.com) (дата звернення: 23.03.2023).
16. IBM QRadar: Посібник з архітектури та розгортання. // International Business Machines Corporation, 2019. – С. 56

ДОДАТОК А

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СУЧАСНИХ SIEM СИСТЕМ

Таблиця А.1 Порівняльна характеристика таких систем як IBM QRadar, LogRhythm та Splunk

Характеристика	IBM QRadar	LogRhythm	Splunk
Стратегія	QRadarIBM має великі внутрішні ресурси та партнерські відносини для підтримки продажів і розгортання та оперативного забезпечення, в тому числі керованого. Послуги для QRadar, у різних географічних регіонах.	LogRhythm пропонує екосистемний підхід від одного постачальника для покупців, які хочуть уніфіковане рішення, що включає ядро SIEM, моніторинг мережі, моніторинг кінцевої точки та UEBA.	Підхід Splunk до централізованого збору та аналізу даних з рішеннями преміум-класу, заснованими на основному продукті,
Основні функції	IBM QRadar використовується для аналізу даних журналу та мережевих потоків у режимі реального часу, щоб зловмисну активність можна було виявити та зупинити якомога швидше.	Використовується для створення загальнокорпоративної системи виявлення загроз і реагування на них.	Аналізує дані, створені машиною, щоб забезпечити оперативну розвідку.

Продовження таблиці А.1 Порівняльна характеристика таких систем як IBM QRadar, LogRhythm та Splunk

Компоненти	QRadar пропонує користувачам широкий вибір архітектури розгортання з вибором факторів, які можна використовувати в різних комбінаціях. Це включає фізичні та віртуальні пристрої, які можуть бути все-в-одному, а також окремі компоненти, мати власну ліцензію на розгортання хмари.	LogRhythm має широкий вибір опцій для запуску основного рішення SIEM, включаючи фізичне обладнання, програмне забезпечення (вIaaS, AWS, Azure і Google Cloud, SaaS.)	Кілька варіантів реалізації для Splunk Enterprise і Enterprise Security включають програмне забезпечення, хмарний хостинг і допоміжні пристрої.
Обробка подій	Дані про події та дані про потік обробляються пристроєм все-в-одному без необхідності додавати процесори подій або потокові процесори	Для обробки подій використовує пристрій збору даних і програмне забезпечення.	Splunk використовує дані та індекси, перетворюючи їх на об’єкти пошуку у вигляді подій.
Збір інцидентів	QRadar перекладає або нормалізує необроблені дані в IP-адреси, порти, кількість байтів і пакети та інша інформація в записі потоку, яка фактично представляє сеанс між ним та господарем.	Збір відбувається за допомогою розгортання LogRhythm, який об'єднує всю історію подій безпеки, визначаються послідовності атак.	Огляд збирає всі інциденти а потім відображаються важливі події та їх поточний статус.

Продовження таблиці А.1 Порівняльна характеристика таких систем як IBM QRadar, LogRhythm та Splunk

Кореляція	QRadar обробляє дані лише за правилами, визначеними в історичній кореляції.	LogRhythm корелює всі дії.	Splunk підтримує п'ять типів кореляції: часові і географічні координати, засновані на транзакціях, пошук, приєднання.
Візуалізація	Таблична візуалізація з великою кількістю вкладок, зручно розділених на окремі поля.	Зручна візуалізація кольору у формі діаграми, графіка, таблиці.	Гарна передача кольору, позаду багато додаткових датчиків, вікна і статистика.
Цінова політика	IBM демонструє зростаючу залежність від своїх додаткових продуктів, доступних за додаткову плату, наприклад Resilient і QRadar Advisor для можливостей реагування на інциденти.	З LogRhythm все дорого, і нічого не отримується безкоштовно. LogRhythm продає вікно, яке має певну ємність для вхідних повідомлень журналу. Після перевищення цієї потужності вам доведеться придбати іншу коробку.	Ціна доступна як безстрокова або річна ліцензія на основі максимального щоденного використання даних і починається від 2000 доларів США на рік за 1 ГБ/день. Ціни Splunk ES розроблено для необмеженої кількості користувачів, які можуть використовувати всі пов’язані з безпекою дані для вирішення всіх випадків використання безпеки.

Продовження таблиці А.1 Порівняльна характеристика таких систем як IBM QRadar, LogRhythm та Splunk

Клієнтський досвід	Аналітика, поведінка, процеси продажу/укладання контрактів постачальника все ще потребують вдосконалення.	Загалом клієнти LogRhythm залишають позитивні відгуки про можливості продукту.	Splunk клієнти дають високі оцінки за простоту інтеграції, якість і доступність для навчання кінцевих користувачів.