УДК 004.056
DOI: 10.31673/2409-7292.2022.020614

Гундер А.М., Мужанова Т.М.

МОНІТОРИНГ І УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ ВИКОРИСТАННЯ SIEM СИСТЕМИ IBM QRADAR

У статті з'ясовані загальні відомості про системи моніторингу й управління безпекою (SIEM); досліджені SIEM як інструмент досягнення відповідності нормативним вимогам безпеки; вивчені функціональні можливості IBM QRadar як типового зразка SIEM.

Ключові слова: забезпечення інформаційної безпеки підприємства, системи моніторингу й управління безпекою (SIEM), IBM QRadar.

Вступ

У наш час постає гостра проблема постійного зростання кількості та складності різноманітних загроз інформаційній безпеці підприємства. Використання сучасних систем моніторингу й управління безпекою (SIEM) створює додаткові можливості для надійного захисту інформаційних активів підприємства, зокрема удосконалення підходів до моніторингу й аналізу подій, виявлення загроз, управління інцидентами та записами, аналізу поведінки користувачів та захисту даних. З огляду на зазначене дослідження систем моніторингу й управління безпекою є актуальним науковим завданням і сприятиме більш ефективному застосуванню перевірених на практиці SIEM-рішень для забезпечення інформаційної безпеки підприємства.

Мета статті полягає у дослідженні засобів моніторингу та управління безпекою у забезпеченні інформаційної безпеки підприємства на прикладі IBM QRADAR як типового зразка SIEM.

Загальна інформація про IBM Qradar

Для вивчення сучасних SIEM-систем у якості прикладу обрано IBM Qradar. Саме це SIEM-рішення використовується у багатьох провідних світових компаніях. Ця SIEM відповідає усім вимогам міжнародних стандартів та є одним із лідерів на світовому ринку відповідно до рейтингу Gartner за 2021 рік [1]. Згідно з інформацією із офіційного веб-сайту IBM Qradar допомагає спеціалістам з інформаційної безпеки виявляти, розставляти пріоритети та реагувати на загрози по всьому підприємству. Як невід'ємна частина вашої інфраструктури захисту інформації, він автоматично об'єднує та аналізує дані журналів і потоків із тисяч пристроїв, кінцевих точок і програм у вашій мережі, надаючи єдині пріоритетні сповіщення для прискорення аналізу і усунення інцидентів. QRadar SIEM доступний для локальних і хмарних середовищ [2].

Серед основних переваг використання даної SIEM розробники виділяють наступні:

Визначення внутрішніх загроз. Виявлення підозрілої активності користувачів, яка може свідчити про зламані облікові дані або інсайдерську загрозу.

Виявлення розширення загрози. Отримання точного виявлення загроз у реальному часі, щоб об'єднати кілька подій, які, здавалося б, з низьким ризиком, щоб виявити кібератаку високого ризику.

Захист хмарного середовища. Виявлення прихованих ризиків у гібридних мультихмарних середовищах і контейнерних робочих навантаженнях.

Розкриття вилучення даних. Співвідношення подій ексфільтрації, таких як вставка USB, використання персональних служб електронної пошти, несанкціоноване хмарне сховище або надмірний друк.

Керування відповідністю. Керування регуляторними ризиками для різних вимог щодо відповідності, таких як GDPR, PCI, SOX, HIPAA тощо.

Контроль OT та IoT безпеки. Централізований моніторинг рішень OT та IoT для виявлення ненормальної активності та потенційних загроз.

Інтерфейс користувача (консоль) QRadar надає повне управління системою та аналіз подій безпеки через Web за безпечним протоколом (HTTPS).

Консоль QRadar включає наступні елементи:

Dashboard – набір панелей з оглядовою інформацією про події, мережеві потоки, зареєстрованих порушеннях, функціонуванні продукту та ін.

Offences – порушення, зареєстровані у системі; налаштування правил кореляції

Log Activity – огляд та аналіз подій безпеки, зареєстрованих та нормалізованих системою

Network Activity – огляд та аналіз мережевих потоків, зареєстрованих та нормалізованих системою

Assets – огляд та налаштування профілів пристроїв; виявлення серверів та управління сканерами вразливостей

Reports – управління звітами

Vulnerabilities – керування сканером уразливостей (опційний компонент).

Admin – керування налаштуваннями системи, користувачами, джерелами подій та ін.

Панелі оглядової інформації та порушень

Панель «Dashboard»

Вкладка «Dashboard» або Інформаційна панель - це робоче середовище, яке надає підсумкову та детальну інформацію про події, що відбуваються у мережі. Вкладка «Dashboard» підтримує кілька інформаційних панелей, де можна відображати певні погляди на безпеку мережі, діяльність або дані, які збирає QRadar. Доступно п’ять інформаційних панелей за замовчуванням. Кожна приладова панель містить елементи, які надають зведену та детальну інформацію про правопорушення, які відбуваються у визначеній мережі. Також можна створити окрему спеціальну інформаційну панель, щоб зосередитися на певних обов'язках щодо безпеки або роботи в мережі. За замовчуванням система надає кілька варіантів відображення інформаційних панелей (залежно від підключених компонентів) для огляду різних аспектів функціонування продукту, які надають різну інформацію:

Application Overview – огляд програм, зареєстрованих під час аналізу мережевих потоків, розподіл трафіку та ін.

Compliance Overview – огляд різних аспектів політик відповідності стандартам.

Network Overview – огляд різних аспектів активності мережі.

System Monitoring – огляд системних повідомлень, статистики за джерелами подій та ін.

Threat and Security Monitoring – огляд зареєстрованих інцидентів, порушень, статистика про роботу системи, інформація про атаки.

Virtual Cloud Infrastructure – огляд даних, отриманих із підключених гіпервізорів.

На рис. 1 показана вкладка Dashboard з відображенням моніторингу загроз Threat and Security Monitoring.

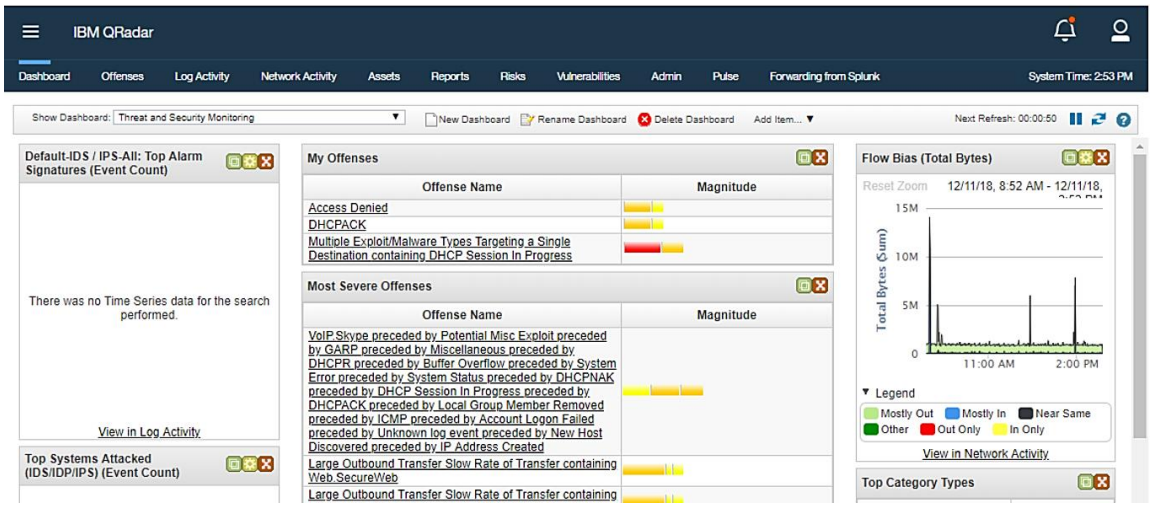

Рис. 1. Вкладка Dashboard

Користувач має можливість відредагувати існуючі або створити нові види інформаційних панелей, а також перевизначити види відображення інформації (графік, кругова діаграма, таблиця і т.д.). Дані для відображення на панелі генеруються за допомогою пошукових шаблонів, що налаштовуються за подіями або потоками з бази даних QRadar.

Панель «Offences»

У даній панелі «Інциденти» відображаються порушення, що автоматично зареєстровані системою на основі опрацьовування одного (або декількох) відповідних кореляційних правил, і можуть ґрунтуватися як на окремих подіях, агрегації та зіставленні різнорідних подій та мережевих потоків. Зручне переглядання порушень, які відбуваються у внутрішній мережі, які можна знайти, використовуючи різні параметри навігації або через розвинуту систему пошуку. На вкладці «Порушення» досліджують правопорушення, щоб визначити основну причину проблеми, а потім працювати над її вирішенням.

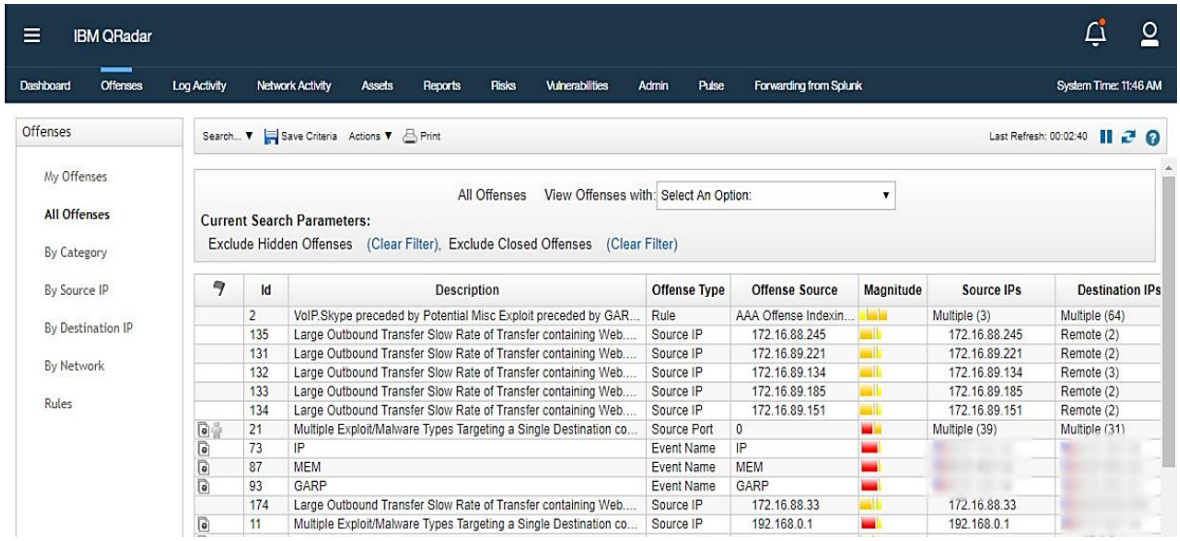

Рис. 2. Панель управління усіма порушеннями

Одне порушення може складатися з десятків тисяч проаналізованих та кореляційних подій та/або потоків. Кожне порушення містить вичерпну інформацію про інцидент, що відбувся, як то IP-адреси джерел і цілей, номери портів, MAC-адреси, ім'я та групу користувача тощо. Також у деталях порушення можна виявити інформацію про основні джерела подій, що брали участь у створенні порушення, основні категорії подій, а також найважливіші події та потоки.

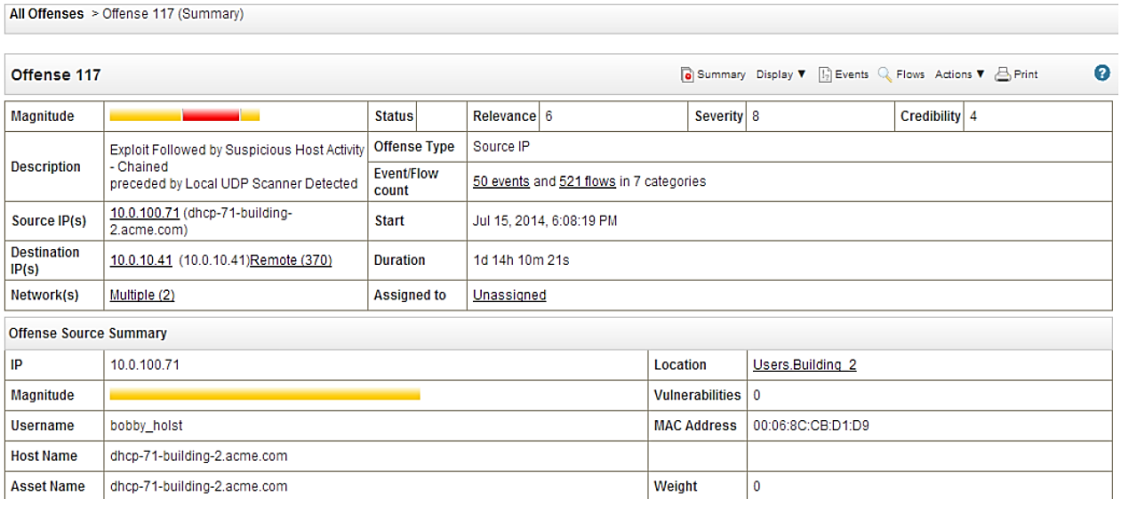

Рис. 3. Детальне відображення одного з інцидентів

Використовуючи детальне відображення порушення, адміністратор ІБ або відповідний відділ може отримати вичерпний опис будь-якої з подій чи потоків, що брали участь у створенні інциденту.

Налаштування правил кореляції для успішного відображення інцидентів

Рішення QRadar надається з великою кількістю встановлених правил, що дозволяють відстежити аномальну активність користувачів, програм, мережевих пристроїв та IT інфраструктури загалом. Правила виконують різні тести відповідності над подіями, потоками чи вже зареєстрованими інцидентами, і при виконанні всіх умов правило виконує у відповідь певну дію.

Приклади таких подій показано на рисунку 4.

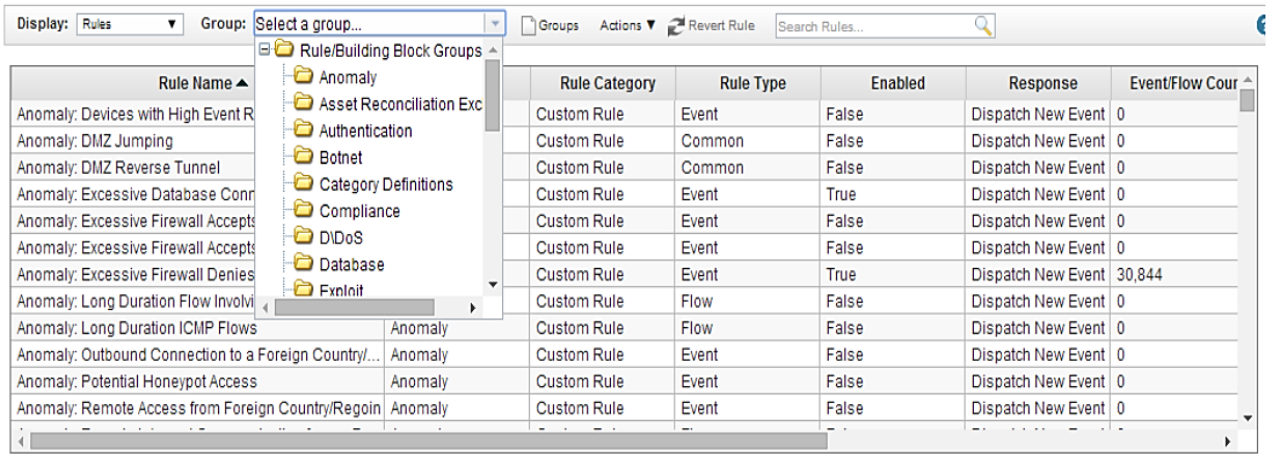

Рис. 4. Приклади правил кореляції за замовчуванням

Щоб краще пристосувати систему до специфіки IT-інфраструктури підприємства у рамках системи можливе створення власних (кастомних) правил кореляції з використанням помічника (Wizard) та інтуїтивно-зрозумілої мови.

Існують такі типи правил, які може застосувати адміністратор ІБ або відповідний відділ безпеки:

Event Rule – перевірка збігів серед подій безпеки в режимі реального часу. Подібні правила можуть створюватися користувачем для виявлення однієї конкретної події (за певним атрибутом нормалізованої події) або послідовності подій. Наприклад, за допомогою Event Rule можна контролювати мережу на наявність невдалих спроб входу до системи, дозволу віддаленого доступу докільком хостам або на наявність подій сканування мережі після настання події виявлення активної вразливості. Поширеною практикою дії у відповідь при спрацьовуванні таких правил є створення інциденту (порушення).

Flow Rule – перевірка збігів серед мережних потоків у режимі реального часу. Подібні правила можуть створюватися користувачем для виявлення одного потоку (за певними властивостями потоку) чи послідовностей потоків. Поширеною практикою дії у відповідь при спрацьовуванні подібних правил є створення інциденту.

Common Rule – перевірка збігів серед атрибутів, спільних для подій безпеки та мережевих потоків. Наприклад, можливе створення загального правила для виявлення подій та потоків, які мають конкретні IP-адреси джерела. Поширеною практикою дії у відповідь при спрацьовуванні подібних правил є створення інциденту.

Offence Rule – спрацьовує лише при внесенні змін до відкритих інцидентів, таких, як додавання нових подій/потоків у інцидент або при запланованій переоцінці інциденту. Поширеною практикою дії у відповідь при спрацьовуванні подібних правил є повідомлення

електронною поштою. На рисунку 5 показаний інструмент-помічник для створення власних кореляційних правил «Rule Wizard».

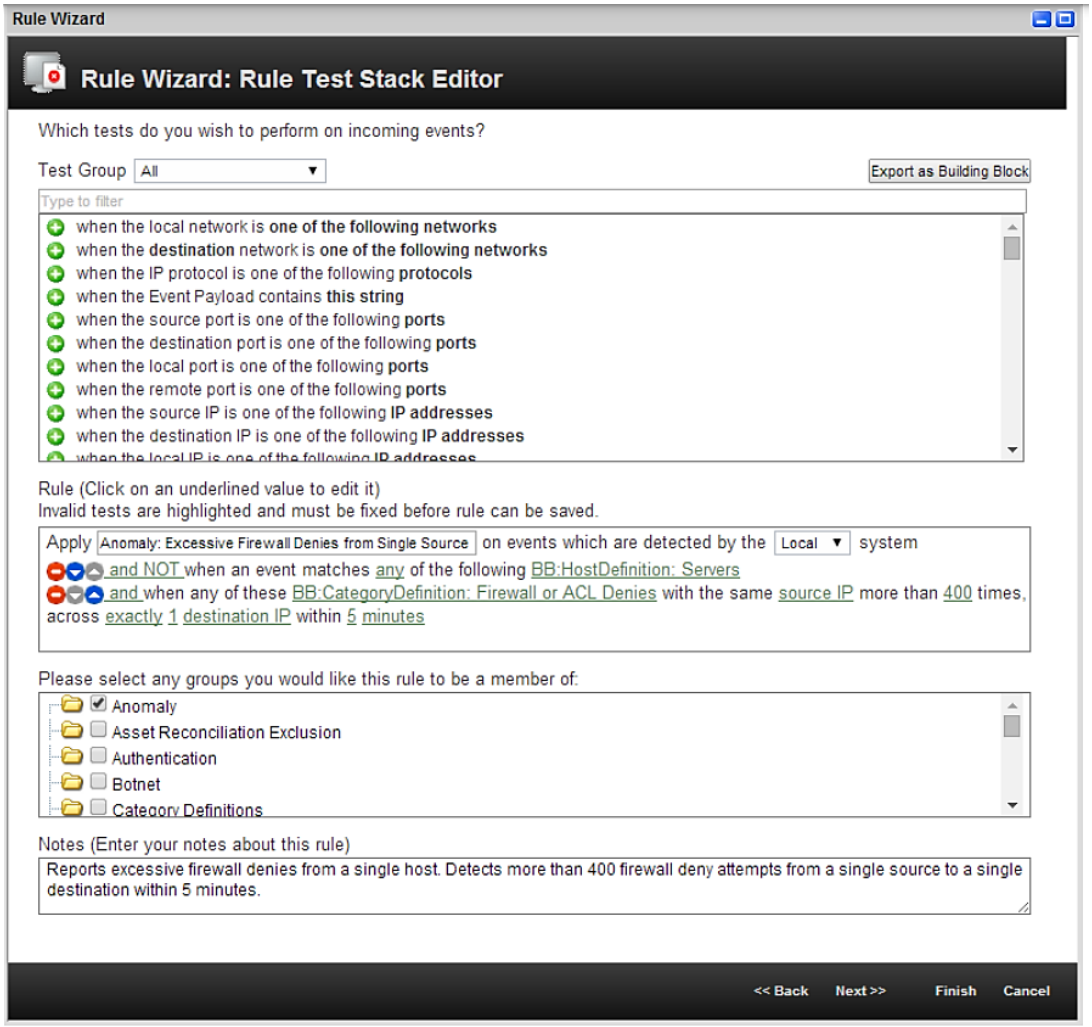

Рис. 5. Інструмент для створення власних кореляційних правил

Функції реєстрації подій та мережевої активності

Панель «Log Activity»

Подія безпеки в рамках системи QRadar є нормалізованим записом з журналу джерела подій (брандмауер або маршрутизатор, операційна система, база даних, додаток та ін.), яка описує деяку активність пристрою або програми. Нормалізація включає аналіз вихідної події та підготовку даних для відображення інформації у вигляді, що легко читається. При нормалізації система привласнює певній події внутрішнє ім'я, через що ім'я, що відображається для нормалізованої події, може не співпадати з іменем оригінальної події. Використовуючи закладку «Log Activity» у консолі QRadar, можна контролювати та розслідувати події інформаційної безпеки в режимі реального часу або виконувати складні пошукові запити на розширений аналіз. Особливо позначаються події, що входять до складу будь-якого інциденту. Перелік подій показаний на рисунку 6:

Типові завдання, що виконуються за допомогою Log Activity у консолі QRadar:

- Пошук певної події
- Пошук підмножини подій
- Збереження й управління критеріями та результатами пошуку
- Перегляд подій у реальному часі
- Перегляд подій, згрупованих за різними критеріями

- Створення, перегляд і дослідження графіків часових рядів (time series charts)
- Перегляд та керування даними захоплення пакетів
- Асоціювання невідомої події з категоріями високого та низького рівня
- Налаштування помилкових спрацьовувань для запобігання появі інцидентів
- Експорт подій

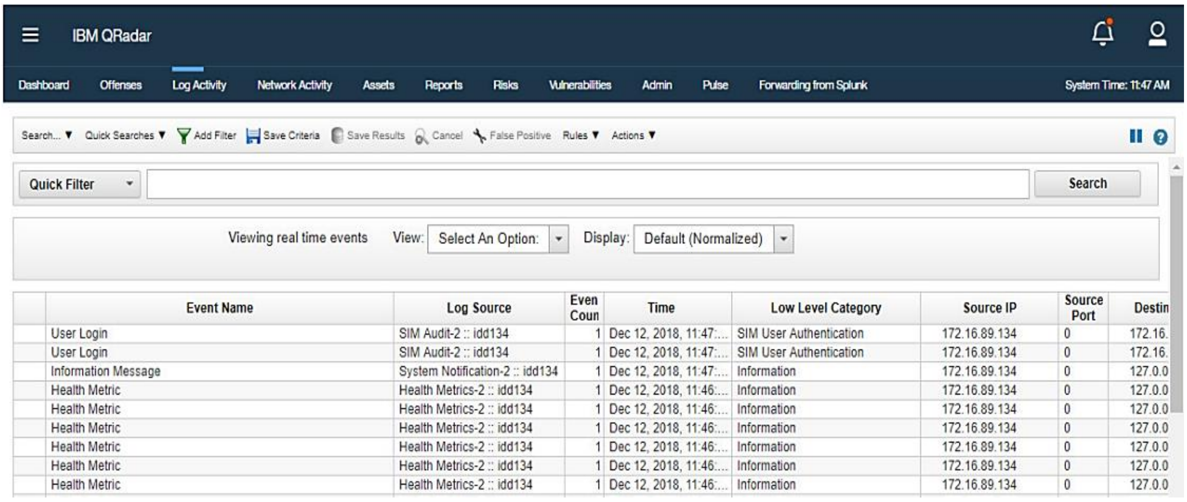

Рис. 6. Перегляд подій безпеки в режимі реального часу

Рішення QRadar надає можливість розширеного пошуку за допомогою набору попередньо встановлених пошукових фільтрів, які дозволяють швидко отримати оглядову інформацію щодо подій, зареєстрованих у системі. Користувач також має можливість змінити існуючі пошукові фільтри або створити нові (рис. 7)

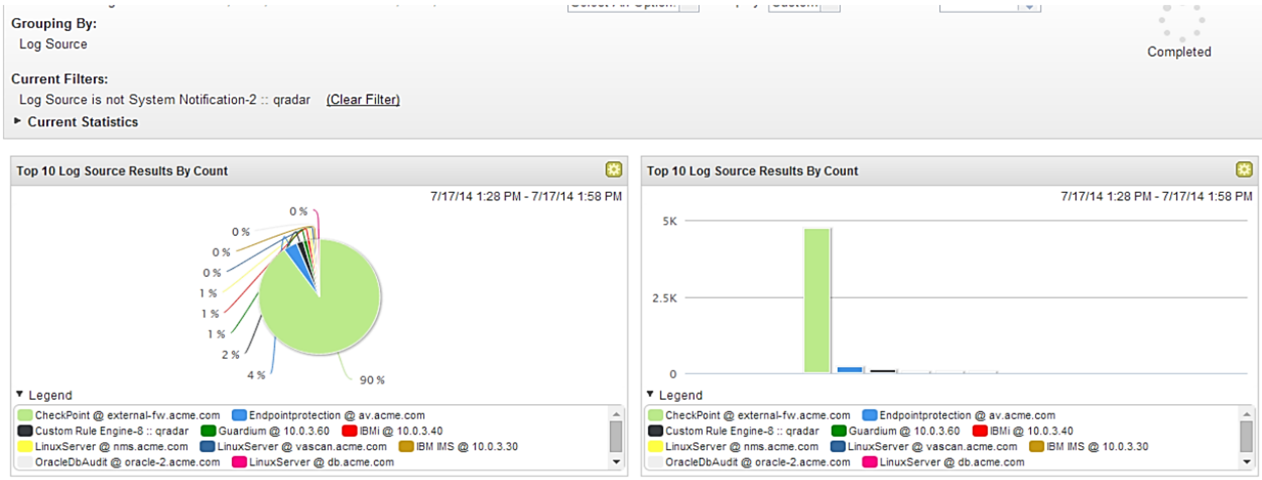

Рис. 7. Використання пошукового фільтру для аналізу подій безпеки
(де джерело події не є системним сповіщенням)

Панель «Network Activity»

Потік - це сеанс зв'язку між двома хостами. Рішення QRadar включає в себе програмний модуль QFlow, який дозволяє аналізувати мережеві потоки у режимі реального часу. Дані процесора QFlow нарівні з даними безпеки беруть участь у генерації інцидентів та створення звітів відповідності. Вкладка «Мережева активність» у консолі QRadar дозволяє візуально відслідковувати та розслідувати мережеві потоки даних у режимі реального часу або виконувати складні запити для фільтрації показаних потоків. Мережевий потік може бути

проаналізований для визначення типу передачі трафіку та типу повідомлення (при включеній опції захоплення змісту потоку).

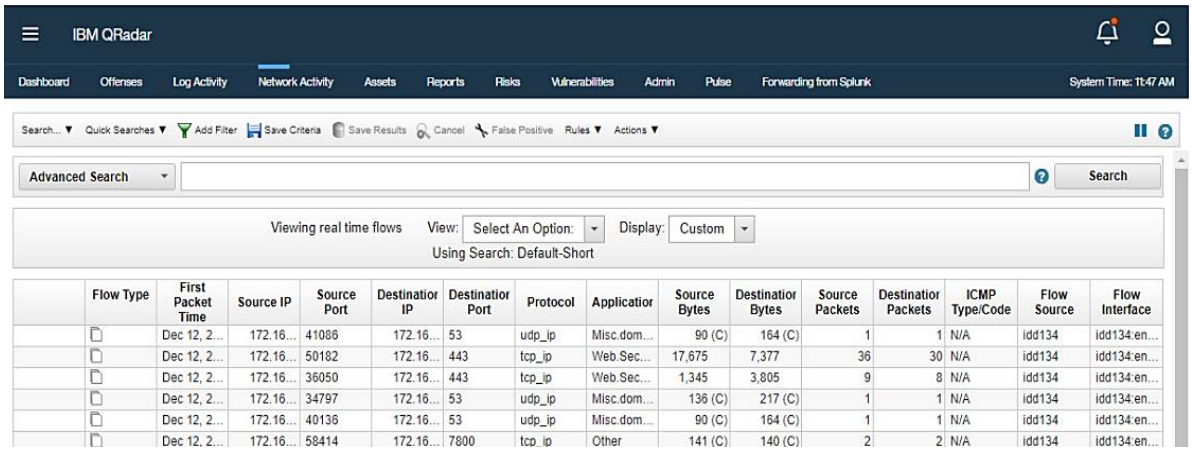

Рис. 8. Перегляд мережевих потоків у режимі реального часу

Однією з основних особливостей процесора мережної активності QRadar є глибокий аналіз мережевих пакетів, що дозволяє надати користувачеві вичерпну інформацію про переданих даних, аж до Application Level моделі TCP/IP, визначаючи додаток, що генерує трафік даних аналізу вмісту TCP пакета (при використанні QFlow як джерело інформації про мережевий трафік). За необхідності будь-який з потоків може бути детально досліджений користувачем.

Облік активів, звітування й адміністрування

Панель «Assets»

QRadar автоматично виявляє активи, сервери та хости, які працюють у даній мережі. Автоматичне виявлення базується на даних пасивного потоку та даних про вразливості, що дозволяє QRadar створити профіль активу. Профілі активів надають інформацію про кожен відомий актив у мережі, включно з ідентифікатором інформації за наявності й усі служби, які працюють на кожному активі. Ці дані профілю використовуються для кореляційних цілей, щоб сприяти зменшенню кількості хибнопозитивних результатів. Наприклад, атака намагається використати певну службу, яка працює на одному з активів. У цій ситуації QRadar може визначити, чи є актив уразливим до цієї атаки, співвідносячи атаку з профілем активу. Використовуючи вкладку «Активи», можна переглядати вивчені активи або шукати певні активи, щоб переглянути їх профілі. Відображення списку таких профілів показано на рисунку 9.

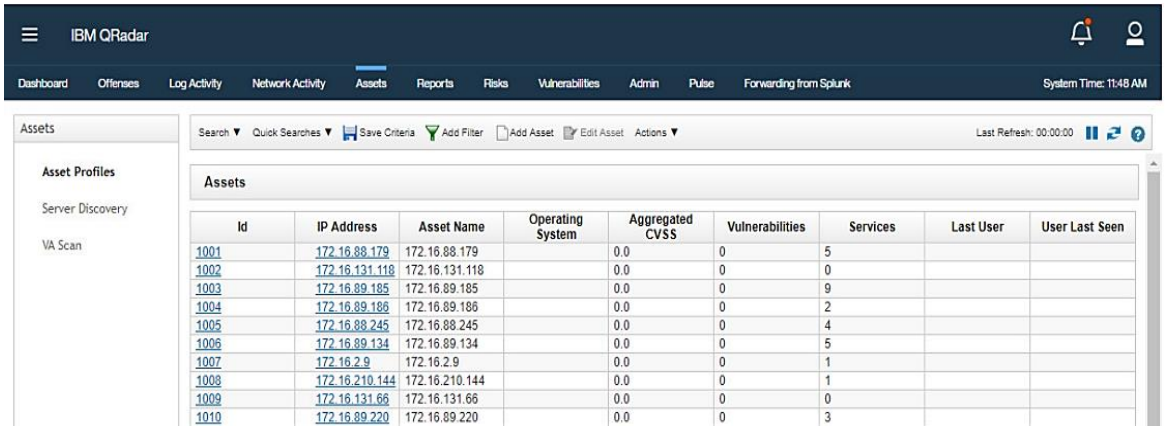

Рис. 9. Список профілів активів

Типові завдання, які виконуються за допомогою «Assets» у консолі QRadar:

- Пошук конкретних профілів активів
- Перегляд усіх профілів
- Перегляд ідентифікаційної інформації для відомих профілів
- Ручне додавання профілів
- Редагування заданих вручну та автоматично виявлених профілів
- Налаштування помилкових спрацьовувань для вразливостей
- Друк та експорт профілів активів

За наявності у мережевій інфраструктурі сканера вразливостей (у випадку з IBM Qradar сканер є вбудованим), у профіль пристрою автоматично додається інформація про можливі вразливості.

Панель «Reports»

Вкладка «Звітування» може бути використана для створення, редагування, розповсюдження та управління звітами. QRadar включає велику кількість попередньо встановлених звітів, розбитих на 8 основних груп. Звіти за основними міжнародними нормами відповідності доступні для завантаження як додаткових модулів з IBM та за необхідності можуть бути переналаштовані у відповідності до внутрішніх стандартів компанії. Відображення звітів показано на рисунку 10.

Користувач також має можливість створювати власні звіти, засновані на встановлених або користувацьких фільтрах пошуку за подіями та потоками. Користувачі з правами Адміністратора можуть переглядати всі звіти, створені іншими користувачами QRadar. Користувачі без прав адміністратора можуть переглядати звіти, які вони самі створили, або звіти, які є спільними для всіх користувачів.

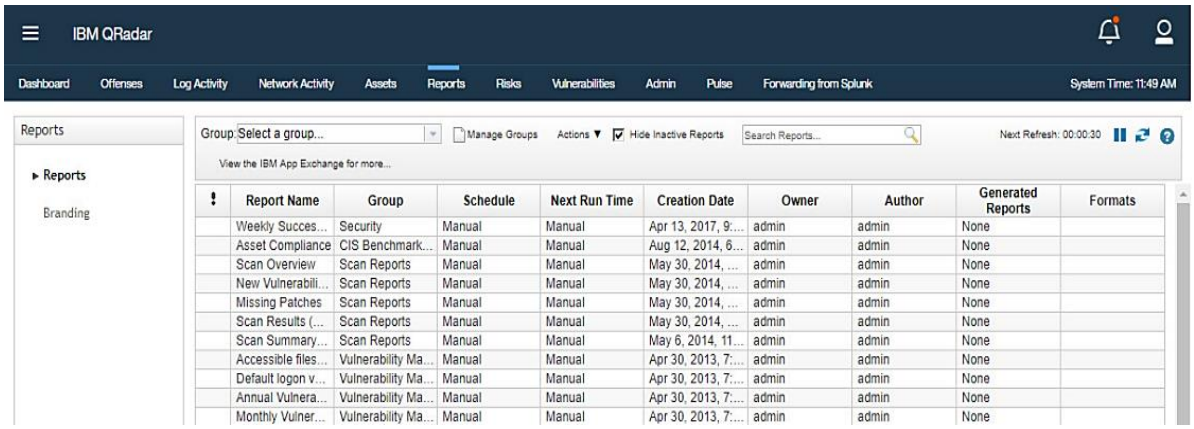

Рис. 10. Відображення звітів

Вкладка «Admin»

Дана адміністративна панель налаштувань дозволяє регулювати глобальні налаштування системи та консолі управління, запланувати автоматичне оновлення системи та модулів підтримки пристроїв, резервне копіювання та відновлення, вибудувати ієрархію мережевих сегментів та ін. Керування користувачами та ролями дозволяє гнучко налаштувати права доступу кожного користувача системи до конкретних об'єктів чи звітів. Вигляд даної панелі представлений на рисунку 11.

Управління консолю QRadar здійснюється за допомогою таких функціональних елементів, згрупованих за трьома категоріями:

- System Configuration - категорія, що об'єднує системні установки, облік встановлених ліцензій, авто-оновлення, відновлення та резервне копіювання, систему глобального оповіщення, керування користувачами, їх ролями та автентифікацією.

- Data Sources - категорія, що поєднує налаштування джерел подій, їх розширень, групування джерел подій, конфігуровані властивості подій, налаштування зберігання подій та різні правила переадресації. Також тут знаходяться налаштування джерел потоків даних, конфігуровані властивості потоків, налаштування зберігання потоків.
- Plug-ins - категорія, що містить дані щодо встановлених розширень (plug-in) QRadar та їх відповідним налаштуванням.

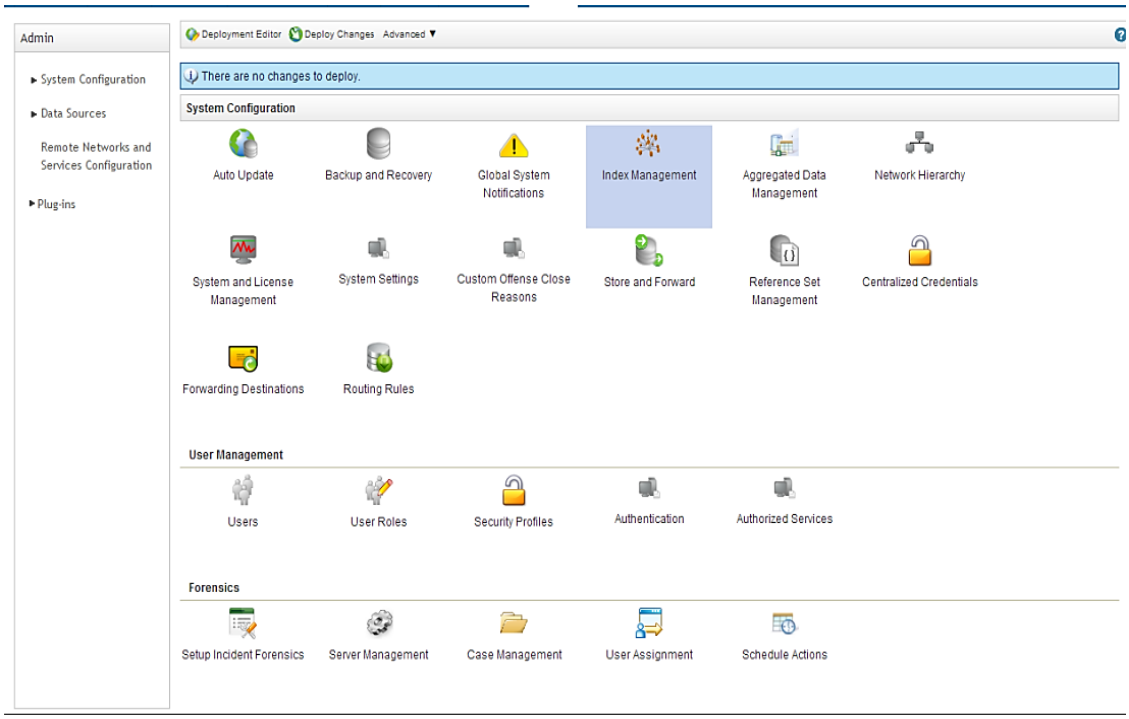

Рис. 11. Вкладка Admin

Висновки

SIEM-система IBM Qradar перевірена часом і багатьма великими світовими й українськими компаніями. Досліджено функціонал, можливості й переваги використання даного SIEM-рішення. Встановлено, що консоль QRadar включає низку елементів, які відповідають за різні аспекти управління інформацією та подіями, зокрема надання й аналіз інформації про події та порушення, зареєстровані в системі, огляд і аналіз подій безпеки, мережевої активності, а також управління активами, звітування та адміністрування.

На прикладі популярного рішення Qradar від IBM досліджено типові характеристики SIEM. Qradar, який є одним із лідерів на світовому ринку сучасних SIEM-продуктів, пропонує обширні можливості для контролю, моніторингу мережі активності, має добре налаштовані алгоритми й велику кількість попередньо встановлених шаблонів та правил кореляції. У статті проілюстровано зручність використання системи, розглянуто її інтерфейс, можливості розширеного пошуку, сортування та налаштування системи.

Перелік посилань

1. LogRhythm – Gartner Magic Quadrant SIEM Report. URL: https://logrhythm.com/gartner-magic-quadrant-siem-report-2021/ (дата звернення: 15.05.2022)
2. IBM – IBM Qradar. URL: https://www.ibm.com/qradar/security-qradar-siem (дата звернення: 15.05.2022)
3. IBM Qradar Documentation. URL: https://www.ibm.com/docs/en/qsip/7.3.2 (дата звернення: 15.05.2022)

Надійшла: 16.05.2022 Рецензент: к.т.н., доцент Дзюба Т.М.