ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ IBM QRADAR SIEM»

Виконала студентка 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Букет Д.А.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Букет Дар'ї Анатоліївні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія управління безпекою інформаційних систем на базі IBM QRadar SIEM»

керівник магістерської роботи Гайдур Галина Іванівна, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси управління захистом кінцевих точок;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту інформаційних систем.
2. Аналіз методів та засобів для вирішення задачі з проектування системи захисту.
3. Дослідити алгоритм створення системи на прикладі IBM QRadar SIEM.
4. Розроблення розгортання в інформаційній системі з використанням IBM QRadar SIEM.
5. Перелік графічного матеріалу

1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Аналіз платформи IBM QRadar SIEM та її переваги.
4. Призначення, можливості та функції IBM QRadar SIEM.
5. Компоненти та архітектура рішення IBM QRadar SIEM.
6. Розробленя варіанта розгортання QRadar та рекомендації щодо впровадження.
7. Розгортання IBM QRadar All-in-one.
8. Розширення розгортання IBM QRadar та територіально розподілене розгортання.
9. Рекомендації щодо управління коритувачами корпоративної інформаційної системи.
10. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок корпоративних інформаційних систем.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	01.10.2022 р.	
3.	Аналіз проблеми управління безпекою інформаційних систем.	30.10.2022 р.	
4.	Розроблення варіантів розгортання QRadar.	10.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування технології управління безпекою інформаційних систем.	30.11.2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	13.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Букет Д.А
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Букет Д.А. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія управління безпекою інформаційних систем на базі IBM QRadar SIEM».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Букет Д.А. за період навчання в інституті
(прізвище та ініціали студента)

ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка ***Букет Д.А.*** обрала тему роботи, метою якої було дослідити зміст технології управління безпекою інформаційних систем на базі IBM QRadar SIEM та проаналізувати особливості розробки та практичної реалізації комплексної системи захисту інформації. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Букет Д.А. показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студентки Букет Дар'ї Анатоліївни на оцінку **«відмінно»** та присвоїти їй кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
"____" _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Букет Д.А.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 82 сторінки, 20 рисунків, 32 джерел.

Об'єкт дослідження – проектування програми інформаційного захисту в інформаційно-телекомунікаційній системі підприємства.

Предмет дослідження – особливості застосування засобів математичного моделювання для реалізації програмного модулю захисту інформації від несанкціонованого впливу в ІТС на підприємстві.

Мета дослідження – аналіз особливостей розробки та практичної реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом кінцевих точок корпоративної інформаційної системи.

Дипломний проект на тему «Технологія управління безпекою інформаційних систем на базі IBM QRadar SIEM» складається зі вступу, трьох розділів, висновків, переліку джерел посилання, додатків.

В роботі проведено аналіз застосування технології управління безпекою інформаційних систем. Досліджено методи та засоби комплексної системи захисту інформації для підприємства.

На основі досліджень проведених в роботі було розроблено варіант реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM в ІТС підприємства.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, АВТОМАТИЗОВАНА МОДЕЛЬ, ШТУЧНИЙ ІНТЕЛЕКТ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.

ABSTRACT

Master’s thesis: 82 pages, 20 figures, 32 sources.

Object of research – the design of the information protection program in the information and telecommunication system of the enterprise.

Subject of research – the peculiarities of the use of mathematical modeling tools for the implementation of the software module for protecting information from unauthorized access in IT at the enterprise.

The aim of research – to analyze the features of the development and practical implementation of a comprehensive information protection system based on IBM QRadar SIEM.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison, modeling of the process of managing the protection of the endpoints of the corporate information system.

The diploma project on the topic "Security management technology of information systems based on IBM QRadar SIEM" consists of an introduction, three sections, conclusions, a list of reference sources, appendices.

In this work, an analysis of the application of information system security management technology was carried out. The methods and means of a comprehensive system of information protection for the enterprise have been studied.

On the basis of the research carried out in the work, an option to implement a comprehensive information protection system based on IBM QRadar SIEM in the enterprise's ITS was developed.

Field of use – cybersecurity of corporate information system.

COMPLEX INFORMATION PROTECTION SYSTEM, CYBER SECURITY, AUTOMATED MODEL, ARTIFICIAL INTELLIGENCE, SOFTWARE, INTELLIGENT INFORMATION TECHNOLOGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСК - автоматизована система керування;

БД – база даних;

ІІТ – інтелектуальні інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

ЕОМ – електронно-обчислювальна машина;

ЕОД – електронний обмін даними;

НМ – нейронна мережа;

ПК – персональний комп’ютер;

СІМ – система інтернет-моніторингу;

СУБД – система управління базою даних;

SEIM (Security Information and Event Management) - управління інформацією та подіями безпеки

ВСТУП

У сучасних умовах розвитку інформаційних процесів майже щодня створюються нові компанії. Для забезпечення роботи вони використовують сучасні інтелектуальні інформаційні технології (ІІТ), які є основою функціонування інформаційно-телекомунікаційної системи (ІТС) компанії. З метою оптимізації виробничих процесів ці структури намагаються підвищити ефективність своєї комплексної системи захисту інформації (КСЗІ), також шляхом моніторингу Інтернет-середовища. Результатом таких процесів буде покращення роботи компанії в цілому, а також допоможе знизити ризик проникнення в чужі дані та витоку конфіденційної інформації, на захист якої витрачається чимало ресурсів компанії.

З іншого боку, можливість отримати достовірні дані про працездатність програмного забезпечення та технічний стан апаратного забезпечення, яке підтримується програмним забезпеченням, дуже важлива для управління корпоративною мережею передачі даних. Загалом, майже будь-який бізнес будь-якого профілю вже має комп’ютери та оргтехніку, але якщо процес їх придбання та встановлення був необдуманим, їх використання зазвичай може бути неефективним та неповним.

Крім того, мало уваги приділяється інформаційній безпеці в існуючих мережах. Кожна організація являє собою сукупність взаємодіючих структурних елементів, кожен з яких може мати свою специфіку. Елементи пов’язані функціонально та інформаційно, тобто виконують певні види роботи в рамках одного бізнес-процесу. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія може бути як інформаційною, так і функціональною. У міру зростання і розвитку організації у її керівництва неминуче виникає бажання створити найбільш гнучку і ефективну систему управління мережею компанії в цілому і її структурних підрозділів.

Слід зазначити, що важливість своєчасного отримання точних даних при управлінні безпекою комп’ютерної мережі неможливо переоцінити. Швидкість

виявлення загроз – одна з актуальних проблем. Наприклад, один із серверів компанії заражений вірусом і співробітники намагаються переглянути веб-сайт зі шкідливим вмістом - час обчислюється в секундах. У таких випадках слід використовувати сучасні інтелектуальні програмні засоби категорії SIEM, які забезпечують можливість швидкого отримання та аналізу даних, щоб мати можливість негайно реагувати в небезпечних ситуаціях. Основними завданнями систем SIEM є збір, зберігання та об'єднання інформації про події безпеки з різних джерел комп'ютерної мережі, їх нормалізація та кореляція, ідентифікація загроз і порушень політик безпеки та звітність.

Виходячи з вищеокресленого, аналіз особливостей проектування і реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM в ІТС підприємства є актуальним.

Мета дослідження – аналіз особливостей розробки та практичної реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM.

Завдання дослідження:

1. проаналізувати теоретичні засади системи захисту інформації та визначити її складові;

2. охарактеризувати принципи роботи SIEM систем;

3. розглянути існуючі моделі захисту ІТС;

4. проаналізувати методи та засоби управління безпекою інформаційних систем на базі IBM QRadar SIEM;

5. розроблення варіантів розгортання QRadar;

6. розроблення рекомендацій щодо застосування технології управління безпекою інформаційних систем.

Об’єкт дослідження – управління безпекою інформаційно-телекомунікаційній системі підприємства.

Предмет дослідження – особливості застосування засобів математичного моделювання для реалізації програмного модулю захисту інформації від несанкціонованого впливу в ІТС на підприємстві.

Методи дослідження: метод системного аналізу; метод аналізу наукової літератури; метод спостереження; метод абстрагування; метод узагальнення.

Теоретично - інформаційна база дослідження складається з робіт таких науковців, як В. Антонюк, В. Бабак, В. Бурячок, В. Бугаш, Е. Вентцель, В. Глушков, Г. Конохович, В. Комашинський, Ю. Ліпунцов, О. Лотов, О. Малюк, Г. Поспєлов, Л. Растригін, Д. Рутковська, Б. Совєтов, В. Шаньгін, Л. Ясницький та інших.

Наукова новизна одержаних результатів. Результати дипломного проекту пропонують варіативний спосіб застосування інструментів програмування під час проектування комплексної системи захисту інформації на базі IBM QRadar SIEM.

Практичне значення одержаних результатів. Робота заснована на результатах поглибленого аналізу специфіки застосування технології управління безпекою інформаційних систем.

Апробація результатів дослідження. Результати роботи були представлені на кафедрі інформаційної та кібернетичної безпеки ННІ Захисту інформації Державного університету телекомунікацій.

Публікації. За результатами наукового дослідження опубліковано наукову статтю «Управління інформаційною безпекою за допомогою комплексної системи захисту».

1 АНАЛІЗ ТА ТЕОРЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОГО ЗАХИСТУ

1.1. Поняття системи захисту інформації, її складові та принципи

Інформаційна безпека – це практичний захист інформації шляхом зниження інформаційного ризику. Інформаційна безпека також є частиною управління інформаційними ризиками. Загалом це включає запобігання або зменшення ймовірності неавторизованого отримання інформації чи її незаконного розголошення, або пошкодження, зміни чи спотворення фактів. Це включає заходи, спрямовані на суттєве зменшення негативних наслідків таких заходів. Захищені дані можуть мати будь-яку форму (електронну чи фізичну), матеріальну (на папері) або нематеріальну (у формі знань). Основна мета інформаційної безпеки полягає в захисті конфіденційності та цілісності інформації шляхом наголошення на ефективній реалізації стратегії. Ці процеси мають відбуватися без впливу на продуктивність компанії. Цього можна досягти за допомогою структурованого процесу управління ризиками, який включає такі елементи [11]:

- виявлення даних та пов’язаних з ними активів та можливих загроз, уразливостей та впливів;

- оцінка ризиків;

- прийняття рішень про усунення та запобігання ризикам, тобто можливість їх уникнення, пом'якшення та розподілу;

- зменшення ризиків, при необхідності вибір або проектування певних заходів безпеки та їх впровадження;

Щоб стандартизувати цю дисципліну, вчені та практики працюють разом, щоб розробити політику, рекомендації та галузеві стандарти для паролів, антивірусного програмного забезпечення, брандмауерів, шифрування, юридичної відповідальності, безпеки та освіти. Цю стандартизацію можна забезпечити за допомогою різноманітних законів і нормативних актів, які впливають на доступ, обробку, зберігання, передачу та знищення даних. Однак впровадження стандартів

і політики в організації може мати лише обмежений вплив, якщо не прийнято культуру постійного вдосконалення [24].

Слід зазначити, що безпека інформації та інформаційних ресурсів з використанням телекомунікаційної системи або пристроїв означає захист інформації, інформаційних систем або книг від несанкціонованого доступу, пошкодження, крадіжки або знищення. При цьому комп'ютерна безпека, кібербезпека або безпека ІІТ (ІТ-безпека) - це захист комп'ютерних систем і мереж від крадіжки або пошкодження їх обладнання, програмного забезпечення або електронних даних, а також від порушення або неправильного напряму послуг, які вони надають.

Отже, сфера інформаційної безпеки стає все більш важливою через все більшу залежність від комп'ютерних систем, Інтернету і стандартів бездротової мережі, такої як блютуз та вай-фай, а також через зростання «розумних» пристроїв, включаючи смартфони, телевізори та інші пристрою, що становлять «Інтернет речей». Через свою складність, як з політичної, так і з технологічної точки зору, кібербезпека є однією з основних проблем в сучасному світі.

Слід зазначити, що безпека інформації та інформаційних ресурсів за допомогою телекомунікаційної системи чи пристроїв означає захист інформації, інформаційних систем чи книг від несанкціонованого доступу, пошкодження, викрадення чи знищення. У той же час кібербезпека або ІІТ-безпека (комп'ютерна безпека) — це захист комп'ютерних систем і мереж від крадіжки або пошкодження їх апаратного, програмного забезпечення чи електронних даних, а також від переривання або зриву послуг, які вони надають.

Таким чином, сфера інформаційної безпеки стає все більш важливою через зростаючу залежність від комп'ютерних систем, Інтернету та стандартів бездротових мереж, таких як Bluetooth і Wi-Fi, а також зростання «розумних» пристроїв, включаючи смартфони, телевізори та інші пристрої, які складають «Інтернет речей». Кібербезпека є однією з головних проблем сучасного світу як через політичну, так і технологічну складову.

Розглянемо принципи інформаційної безпеки. Серед них такі [29]:

1. Конфіденційність.

Конфіденційність — це керівний принцип, який забезпечує приватність, секретність та безпеку даних. Теоретично без конфіденційності всі дані були б доступні будь-кому й будь-де — працівникам чи громадськості — що може бути катастрофічним.

Цей принцип гарантує, що доступ до даних можуть мати лише призначені ролі або конкретні особи, а не будь-хто в компанії. Цей принцип також допомагає захистити зовнішні дані та дані клієнтів шляхом впровадження дозволів, автентифікації та контролю авторизації для запобігання несанкціонованому доступу.

2. Цілісність.

Цілісність встановлює базовий рівень для активів і вимагає від організацій забезпечення послідовних, точних, надійних і безпечних даних. Якщо інформація неточна або змінена, це може означати кібератаку, вразливість або інцидент із безпекою. Дотримання цього принципу вимагає шифрування даних під час передачі, хешування паролів, впровадження контролю версій і використання систем виявлення вторгнень для підтримки цілісності даних.

3. Доступність.

Системи, додатки та дані повинні постійно бути в стані доступності; якщо програми недоступні, це може означати, що їх виведено з ладу через атаку. Відсутність доступності може призвести до уповільнення або зупинки бізнес-процесів або призвести до неможливості клієнтам отримати доступ до своєї інформації чи пов’язаного програмного забезпечення.

Нижче наведемо приклади статистичних даних відносно загроз з боку несанкціонованого доступу до корпоративних мереж та ПК (рис. 1.1 – 1.3).

На рисунках 1.1 – 1.3 представимо статистику атак за допомогою мережі Інтернет на ПК, джерела атак та кількість реалізованих атак.

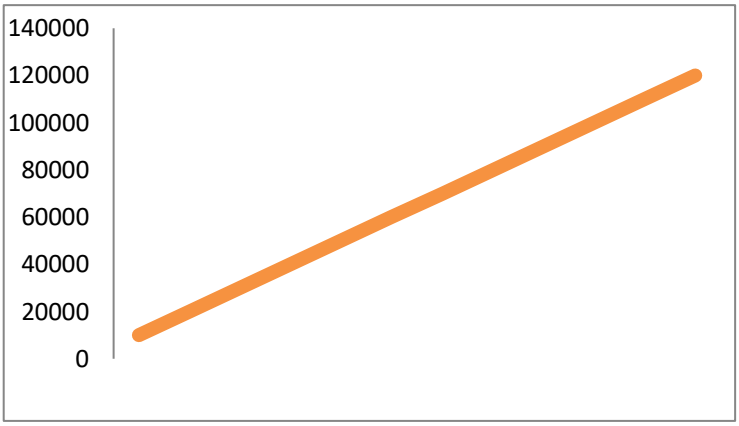


Рис. 1.1. Статистика атак в мережі Інтернет протягом 2018 -2021 років

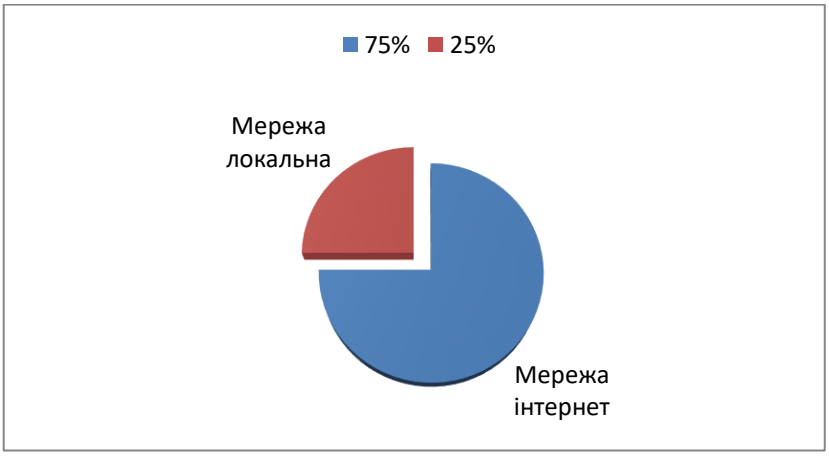


Рис. 1.2. Джерела атак на ПК

Рис. 1.3. Впроваджені системні атаки в мережі OSI

1.2. Характеристика SIEM систем

Security information and event management (SIEM) — це підхід до керування безпекою, який об’єднує у собі функції управління інформаційною безпекою (SIM

- *Security information management*) і управління подіями безпеки (SEM - *Security event management*) в одну систему керування безпекою [32].

Основними принципами кожної системи SIEM є агрегування відповідних даних із багатьох джерел, виявлення відхилень від норми та вживання відповідних заходів. Наприклад, коли виявляється потенційна проблема, система SIEM може реєструвати додаткову інформацію, генерувати сповіщення та вказувати іншим елементам керування безпекою зупинити виконання дії.

На самому базовому рівні система SIEM може базуватися на правилах або використовувати механізм статистичної кореляції для встановлення зв'язків між записами журналу подій. Розширені системи SIEM розвинулися, щоб включити аналітику поведінки користувачів і об'єктів, а також оркестрування безпеки, автоматизацію та реагування (SOAR - *security orchestration, automation and response*).

Системи SIEM працюють шляхом розгортання кількох агентів збору в ієрархічній манері для збору пов'язаних із безпекою подій від пристроїв кінцевих користувачів, серверів і мережевого обладнання, а також спеціалізованого обладнання безпеки, такого як брандмауери , антивірусні програми або системи запобігання вторгненням (IPS - *intrusion prevention systems*). Колектори пересилають події на централізовану консоль керування, де аналітики безпеки відсіюють шум, з'єднуючи точки та визначаючи пріоритетність інцидентів безпеки.

У деяких системах попередня обробка може відбуватися на граничних колекторах, лише певні події передаються до централізованого вузла керування. Таким чином можна зменшити обсяг інформації, що передається та зберігається. Незважаючи на те, що прогрес у машинному навчанні допомагає системам точніше позначати аномалії, аналітики все одно повинні надавати зворотний зв'язок, постійно навчаючи систему про середовище.

Розглянемо, як працюють SIEM системи (див. рис. 1.4). Інструменти SIEM збирають дані про події та журнали, створені хост-системами по всій інфраструктурі компанії, і об'єднують ці дані на централізованій платформі. Хост-

системи включають програми, пристрої безпеки, антивірусні фільтри та брандмауери. Інструменти SIEM ідентифікують і сортують дані за такими категоріями, як успішні та невдалі входи, активність зловмисного програмного забезпечення та інша ймовірна шкідлива діяльність.

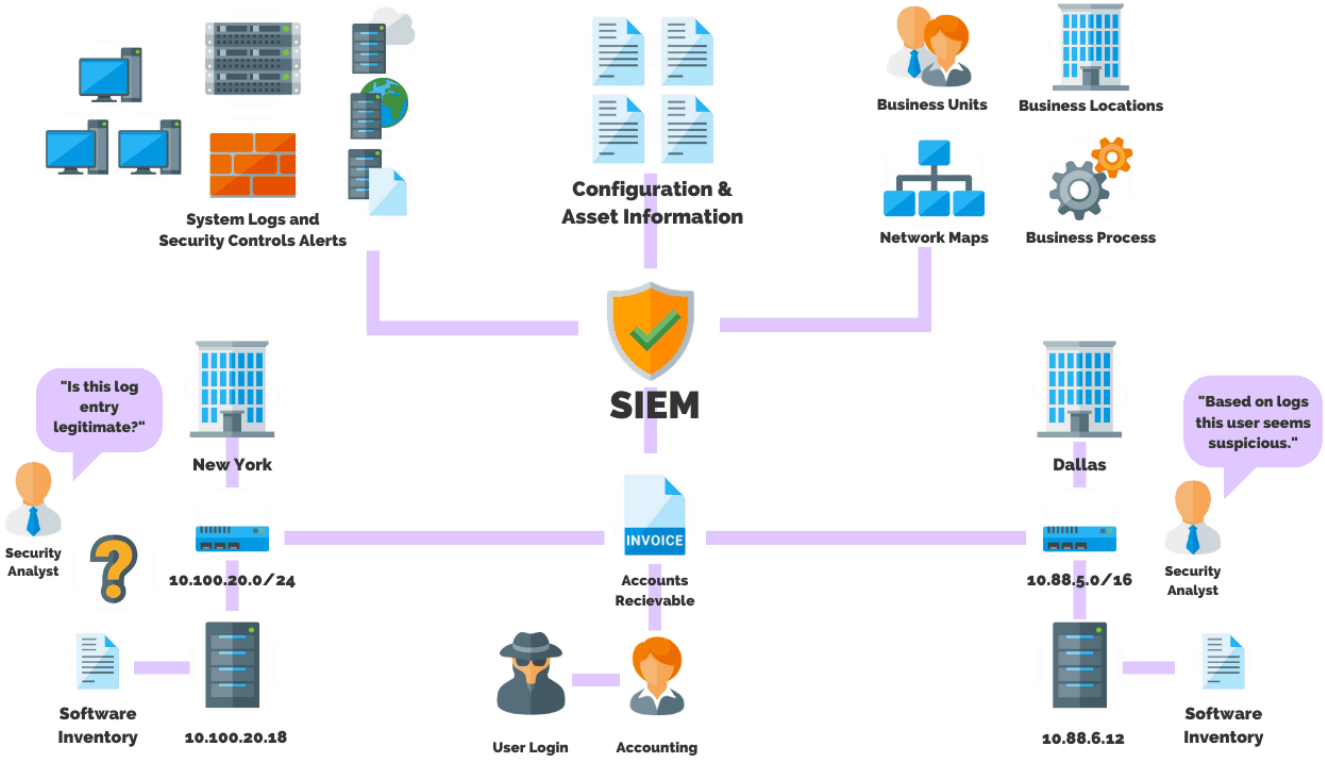


Рис. 1.4. Як працює SIEM система

Програмне забезпечення SIEM генерує сповіщення безпеки, коли виявляє потенційні проблеми безпеки. Використовуючи набір попередньо визначених правил, організації можуть встановити ці сповіщення як низький або високий пріоритет.

Наприклад, обліковий запис користувача, який генерує 25 невдалих спроб входу протягом 25 хвилин, може бути позначений як підозрілий, але йому все одно буде встановлено нижчий пріоритет, оскільки спроби входу були зроблені користувачем, який забув свою інформацію для входу.

Однак обліковий запис користувача, який генерує 130 невдалих спроб входу протягом п’яти хвилин, буде позначено як подія з високим пріоритетом, оскільки, швидше за все, це атака повного перебору.

SIEM система спрощує для підприємств керування безпекою, фільтруючи величезні обсяги даних безпеки та визначаючи пріоритетність сповіщень безпеки, які генерує програмне забезпечення.

Програмне забезпечення SIEM дозволяє організаціям виявляти інциденти, які інакше могли б залишитися непоміченими. Програмне забезпечення аналізує записи журналу, щоб виявити ознаки зловмисної діяльності. Крім того, оскільки система збирає події з різних джерел у мережі, вона може відтворити хронологію атаки, дозволяючи організації визначити характер атаки та її вплив на бізнес.

Система SIEM також може допомогти організації виконати вимоги відповідності шляхом автоматичного створення звітів, які містять усі зареєстровані події безпеки серед цих джерел. Без програмного забезпечення SIEM компанії довелося б збирати дані журналів і складати звіти вручну.

Система SIEM також покращує керування інцидентами , допомагаючи групі безпеки компанії розкривати маршрут атаки в мережі, визначати джерела, які були скомпрометовані, і надавати автоматизовані інструменти для запобігання атакам, що відбуваються.

Переваги SIEM включають наступне:

1. Це значно скорочує час, необхідний для виявлення загроз, мінімізуючи шкоду від цих загроз.
2. SIEM пропонує цілісне уявлення про середовище інформаційної безпеки організації, полегшуючи збір і аналіз інформації про безпеку для забезпечення безпеки систем. Усі дані організації надходять у централізоване сховище, де вони зберігаються та легко доступні.
3. Компанії можуть використовувати SIEM для різноманітних випадків використання даних або журналів, включаючи програми безпеки, звіти про аудит і відповідність, службу підтримки та усунення несправностей мережі.
4. SIEM підтримує великі обсяги даних, тому організації можуть продовжувати масштабувати та додавати більше даних.
5. SIEM забезпечує виявлення загроз і сповіщення безпеки.

6. Він може виконувати детальний криміналістичний аналіз у разі серйозних порушень безпеки.

Незважаючи на свої переваги, ***SIEM також має такі обмеження***:

1. Впровадження SIEM може зайняти багато часу, оскільки для забезпечення успішної інтеграції з засобами безпеки організації та багатьма хостами в її інфраструктурі потрібна підтримка. Зазвичай для встановлення SIEM потрібно 90 днів або більше, перш ніж він почне працювати.
2. Висока вартість. Початкові інвестиції в SIEM можуть обчислюватися сотнями тисяч доларів. Супутні витрати можуть збільшитися, включаючи витрати на персонал для керування та моніторингу впровадження SIEM, щорічну підтримку та програмне забезпечення або агентів для збору даних.
3. Аналіз, налаштування та інтеграція звітів вимагають таланту експертів. Ось чому деякими системами SIEM керують безпосередньо в центрі безпеки , централізованому підрозділі, укомплектованому командою інформаційної безпеки, яка займається питаннями безпеки організації.
4. Інструменти SIEM зазвичай залежать від правил для аналізу всіх записаних даних. Проблема полягає в тому, що мережа компанії може генерувати тисячі сповіщень на день. Важко визначити потенційні атаки через кількість нерелевантних журналів.
5. Неправильно налаштований інструмент SIEM може пропустити важливі події безпеки, що зменшить ефективність керування інформаційними ризиками .

Важливі характеристики, які слід враховувати при оцінці продуктів SIEM, включають наступне.

Агрегація даних. Дані збираються та контролюються з програм, мереж, серверів і баз даних.

Кореляція. Як правило, кореляція є частиною SEM в інструменті SIEM. Це означає, що інструмент знаходить подібні атрибути між різними подіями.

Приладові панелі. Дані збираються та агрегуються з програм, баз даних, мереж і серверів і відображаються на діаграмах, щоб допомогти знайти закономірності та уникнути пропуску критичних подій.

Оповіщення. У разі виявлення інциденту безпеки інструменти SIEM можуть повідомити користувачів.

Автоматизація. Деяке програмне забезпечення SIEM також може містити автоматизовані функції, наприклад автоматичний аналіз інцидентів безпеки та автоматичні відповіді на інциденти .

На ринку існує велика різноманітність інструментів SIEM, нижче наведено деякі з них:

Splunk — це локальна система SIEM, яка підтримує моніторинг безпеки та пропонує постійний моніторинг безпеки, розширене виявлення загроз, розслідування інцидентів і реагування на інциденти.

Платформа ***IBM QRadar SIEM*** забезпечує моніторинг безпеки IT-інфраструктур. Він включає збір даних журналу, виявлення загроз і кореляцію подій.

LogRhythm - це система SIEM для невеликих організацій. Він об’єднує керування журналами , мережевий моніторинг і моніторинг кінцевих точок, а також криміналістику й аналітику безпеки.

Exabeam. Портфоліо SIEM від Exabeam Inc. пропонує озеро даних, розширену аналітику та засіб пошуку загроз .

Платформа RSA ***NetWitness*** — це інструмент виявлення загроз і реагування на них, який включає збір, пересилання, зберігання та аналіз даних.

Datadog Cloud SIEM від Datadog Security — це хмарна мережа та система керування. Інструмент включає як моніторинг безпеки в реальному часі, так і керування журналами.

Інструмент ***Log360 SIEM*** пропонує аналіз загроз, керування інцидентами та функції SOAR. Збір журналів, аналіз, кореляція, попередження та архівування доступні в режимі реального часу.

Інструмент ***SolarWinds Security Event Manager SIEM*** автоматично виявляє загрози, відстежує політику безпеки та захищає мережі. Інструмент пропонує такі функції, як моніторинг цілісності, звітування про відповідність і централізований збір журналів.

Ключ до вибору правильного інструменту SIEM залежить від ряду факторів, включаючи бюджет організації та стан 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 загроз у реальному часі, кореляція та аналіз у різноманітних програмах і системах;
- система виявлення вторгнень, IPS, брандмауер, журнал подій, а також інші прикладні та системні інтеграції;
- розвідка загроз;
- моніторинг активності користувачів.

Майбутні тенденції SIEM включають наступне:

Покращене оркестрування. Наразі SIEM надає компаніям лише базову автоматизацію робочого процесу. Однак, оскільки ці організації продовжують розвиватися, SIEM має запропонувати додаткові можливості. Наприклад, завдяки штучному інтелекту та машинному навчанню інструменти SIEM повинні пропонувати швидшу оркестровку, щоб забезпечити однаковий рівень захисту для різних відділів компанії. Крім того, протоколи безпеки та виконання цих протоколів будуть швидшими, ефективнішими та ефективнішими.

Краща співпраця з інструментами керованого виявлення та реагування (MDR). Оскільки загрози злому та несанкціонованого доступу продовжують зростати, важливо, щоб організації застосовували дворівневий підхід для виявлення та аналізу загроз безпеці. IT-команда компанії може впровадити SIEM

власними силами, а керований постачальник послуг може впровадити інструмент MDR.

Покращене керування хмарою та моніторинг. Постачальники SIEM вдосконалять можливості керування хмарою та моніторингу своїх інструментів, щоб краще задовольнити потреби безпеки організацій, які використовують хмару.

SIEM і SOAR стануть одним інструментом. Шукайте традиційні продукти SIEM, щоб скористатися перевагами SOAR; однак постачальники SOAR, швидше за все, відреагують розширенням можливостей своїх продуктів.

1.3. Огляд та оцінка існуючих моделей захисту інформаційних систем

Комплексна система захисту інформації – сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу [3].

Основними цілями КСЗІ є:

– захист законних інтересів підприємства від протиправних дій;

– не допустити розкрадання фінансових та матеріально-технічних засобів;

– захистити від розголошення, витоку та несанкціонованого доступу до службової інформації;

– не допустити порушення роботи технічних засобів забезпечення виробничої діяльності,

– включаючи інформаційні технології.

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства загалом. КСЗІ є універсальним підходом щодо встановлення безпеки та основною концепцією для безпеки інфраструктури підприємства загалом. Необхідність побудови КСІ визначається вимогами нормативних документів у сфері технічного та криптографічного захисту інформації або бажанням власника інформаційних ресурсів.

Організаційні методи захисту. Організаційні засоби захисту є обов’язковою частиною будь-якої КСЗІ, а програмно-технічні заходи впроваджуються в міру

необхідності, виходячи з потреб, можливостей та стану захищеності інформації підприємства.

Організаційні міри захисту передбачають:

– створення посадових інструкцій для працівників підприємства (користувачів системи) та обслуговуючого персоналу;

– встановлення правил адміністрування інформаційної системи, обліку, зберігання,

– розповсюдження, знищення носіїв інформації, ідентифікації користувачів;

– розробка плану дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

– навчання правилам інформаційної безпеки користувачів.

Програмно-технічні засоби захисту. Програмно-технічні міри захисту, що проводяться для захисту інформаційної інфраструктури підприємства, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу. Також ефективним є застосування наступних систем: система виявлення вторгнень (IDS), система запобігання вторгнень (IPS), також UTM-системи.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Комплексна система захисту інформації на підприємстві передбачає два види функцій [3]:

- функції, основною метою яких є створення механізмів захисту;
- функції, що здійснюються з метою безперервного та оптимального керування механізмами захисту.

Створення концепції системи захисту інформації.

Основною метою управління системою захисту на підприємстві є забезпечення максимально можливої ефективності використання ресурсів. Технологія управління має бути побудована так, щоб забезпечувати ефективну обробку інформації для всіх функціональних підрозділів під час раціонального використання ресурсів сучасних засобів обчислювальної техніки та інформаційних технологій.

Особливе місце в сучасній системі захисту інформації на підприємстві мають інформаційні ресурси. Під інформаційними ресурсами розуміються документи та масиви документів в інформаційних системах підприємства. Інформаційні ресурси підприємства схильні до різноманітних загроз. Для зниження загроз, вразливостей, ризиків для підприємства необхідний контроль та ефективне управління інформаційними ресурсами. Питання розподілу, використання та захисту інформаційних ресурсів підприємства покладено на службу КСЗІ, яка формує стратегію потреб в інформаційних ресурсах, що оцінює поточний стан системи захисту інформації та ефективність використання інформаційних ресурсів.

На підприємстві захист інформаційних ресурсів зводиться до оптимізації методів захисту інформації, технічних засобів та її складу. Управління інформаційними ресурсами пов'язані з потужністю підприємства.

Інформаційна потужність підприємства – синергетична характеристика, що описує рівень ефективності використання існуючих інформаційних активів для збільшення конкурентоспроможності підприємства з досягненням максимуму при [18]:

- повному використанні функціоналу та можливостей інформаційних систем,
- організації інформаційних бізнес-рішень, адекватних завдань, що вирішуються підприємством.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [26]:

- інформація, що є власністю держави, або інформація з обмеженим доступом має бути

- захищена шляхом побудови КСЗІ, та подальшим отриманням «Атестату відповідності», який видається Адміністрацією державної служби спеціального зв'язку та захисту інформації України за результатами проведення державної експертизи КСЗІ;
- інша інформація може бути захищена за допомогою КСЗІ за бажанням її власника.

Загалом можна виділити дві основні категорії вразливостей інформаційної системи: людський фактор користувача цієї системи та незахищеність чи несправність роботи програмного та системного забезпечення.

Тому при проектуванні системи захисту потрібно обов’язково враховувати це, будуючи її за двома напрямками.

Варто зазначити, що автоматизовані системи на сучасних підприємствах наразі демонструють потенційно смертельні уразливості. Є багато повідомлень про зломи різноманітних організацій, включаючи атаки шкідливих програм, експлойтів Windows XP, вірусів і витоку конфіденційних даних, що зберігаються на серверах підприємств. Враховуючи вищевикладені обставини, розглянемо детальніше існуючі моделі захисту інформації в установах з метою проектування та реалізації КСЗІ в ІТС підприємства. Для розробки прототипу пропонується застосовувати програму моніторингу веб-середовища в ІТС комерційної структури.

Отже, моніторинг - це набір НТ, технологічних та інших інструментів, які сприяють реалізації систематичного моніторингу за станом різних явищ та процесів.

Більшість платних програм інтернет-моніторингу веб-ресурсів також пропонують функції забезпечення безпеки на кшталт сканування і наявність вірусів та шкідливого ПЗ, що набуває актуальності наразі, адже веб-сайти стають все більш складнішими та потрібнішими для ведення бізнесу.

Системи захисту може працювати як всередині, так і зовні корпоративного брандмауера. Класичні рішення з керування мережею зосереджуються на питаннях моніторингу брандмауера, тоді як зовнішній контролінг ефективності буде

тестувати та стежити за проблемами продуктивності через магістраль мережі інтернету, а подекуди аж до рівня кінцевого юзера.

Сторонні рішення для контролінгу продуктивності ресурсів здатні відстежити внутрішні (за брандмауером) та зовнішні (орієнтовані на користувача) чи хмарні веб-застосування [24].

Внутрішній моніторинг брандмауера використовується через спеціальні апаратні засоби, що здатні допомагати у визначенні, чим саме викликана повільна продуктивність внутрішніх додатків: моделюванням додатків, внутрішньою інфраструктурою чи внутрішніми системами, або навіть підключенням до глобального павутиння.

Зовнішній моніторинг продуктивності ще називають моніторингом кінцевого користувача чи наскрізним моніторингом продуктивності.

Моніторинг реального користувача вимірює продуктивність та доступність, з якими мають справу реальні клієнти, виявляє окремі інциденти та контролює вплив трансформацій.

Отже, вирішенням проблеми забезпечення інформаційної безпеки установи може стати впровадження автоматизованої стратегії інтернет-моніторингу.

Розглянемо ПЗ з відкритимм вихідними кодами, що кожного дня доводять власну цінність в мережі будь-якого складу та змісту.

Від виявлення обладнання, управління мережевими пристроями та серверами до з’ясування тенденцій відносно функціонування мереж, графічного показу результату моніторингу та навіть розробки резервних копій конфігурацій комутатору та маршрутизатору. Ними є безкоштовні утиліти, які допомагають відбутися моніторингу мережі і серверів.

1. Cacti.

Відразу це була програма MRTG - система для організаційного вирішення питань сервісів моніторингу мереж, а також вимірювання інформації через деякий час. Наразі програма Cacti являє собою сучасне рішення серед ПЗ з відкритим вихідним кодом в галузі графічного представлення мереж. Дана система виводить принцип MRTG на принципово новий щабель розвитку [23, с. 1].

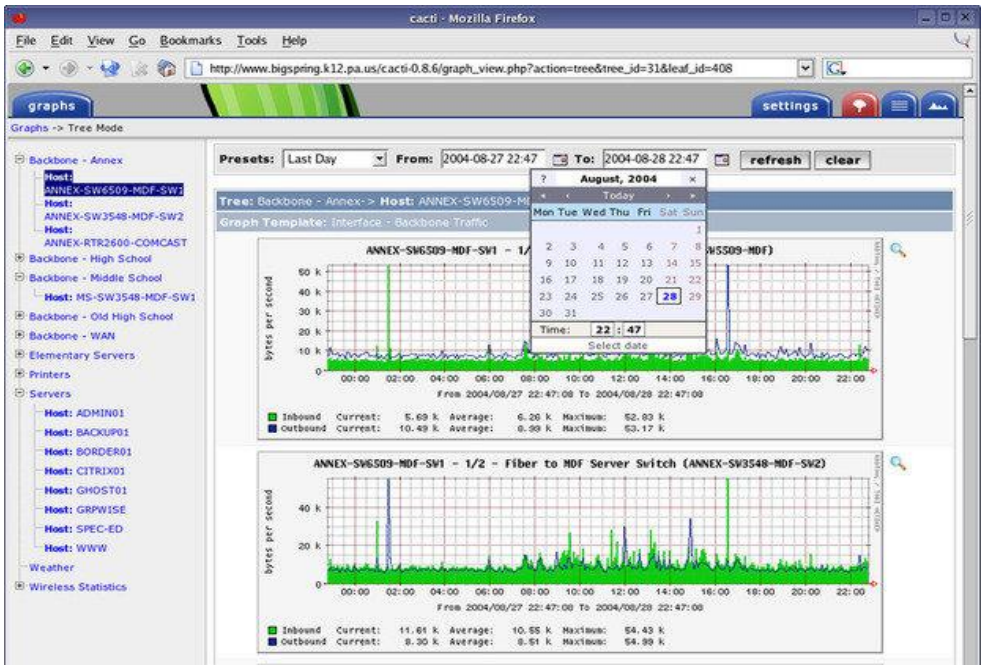


Рис. 1.5. Приклад інтерфейсу Cacti

Cacti є програмою, що надає класичну програмну платформу для розробки графіку на базі практично будь-якої статистичної інформації. В разі коли будь-яке обладнання чи сервіс повертає кількісні показники, то вони, передусім, можуть сполучатися з Cacti.

Фреймворки ПЗ вдало розділяють на дискретні екземпляри збору інформації та на їхнє графічне відображення, яке допомагає легко повторно оброблювати та реорганізувати існуючу інформацію для різноманітних візуальних представлень [25].

Одночасно можна обрати певні часові рамки та відповідні елементи графіків. Так, наприклад, можна оперативно переглядати дані за кілька років навіть, аби зрозуміти, чи є сучасна поведінка мережевого пристрою чи серверу є аномальною, чи подібні властивості є регулярними. Застосування програм NetworkWeathermap, PHP-плагіну для Cacti, допоможе без особливих зусиль проектувати карти власних мереж в реальному часі, які демонструватимуть завантаженість каналів зв'язків між мережевим обладнанням, яке реалізовується за рахунок графіків, що виникають при наведенні покажчиків миші на картинку мережі.

2. Nagios.

Nagios - це програма для моніторингу мереж, що вже довгий час знаходиться на стадії проектування. Вона написана на мові С та допомагає робити майже все, що може бути потрібним в роботі системних та мережевих адміністраторів, починаючи від пакета прикладного ПЗ для моніторингу. Веб-інтерфейс даного ПЗ є швидким та простим для розуміння, в той час як його серверна частина є досить надійною [1].

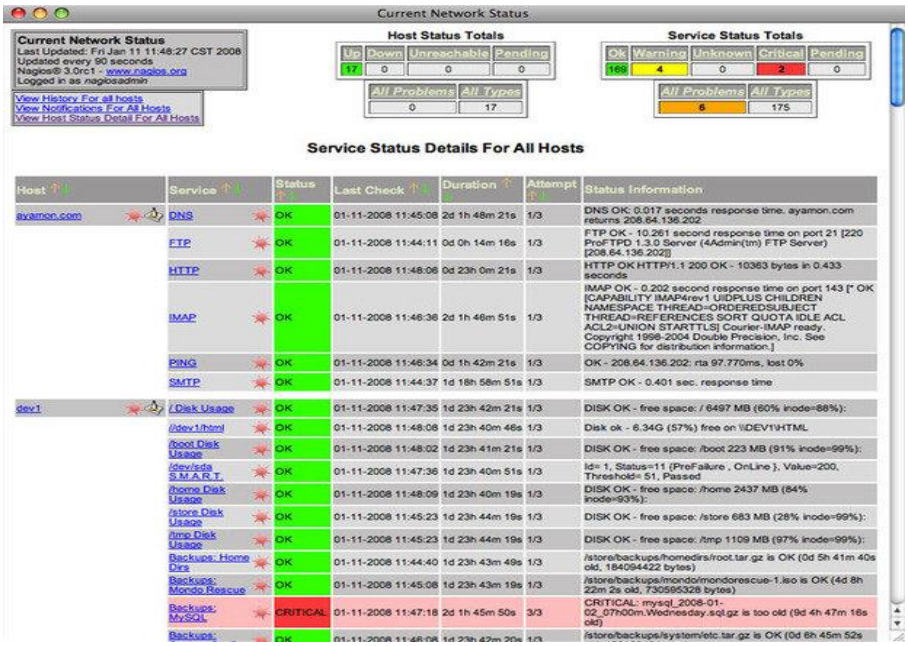


Рис. 1.6. Інтерфейс програми Nagios

Nagios допомагає виконувати функцію постійного моніторингу стану серверу, сервісів, мережевого каналу і всього іншого, що буде зрозумілим для мережевого протокола типу IP. Є можливість виконувати контроль застосування дискового простору на серверах, завантаженість центрального процесору, використання ліцензій типу FLEXlm, температурний режим повітря серверу, затримку у роботі вай-фаю та інтеренет-мережі.

Недоліком Nagios можна вважати конфігурацію, оскільки її найкраще виконувати за рахунок командного рядка, яке значно утруднює навчання користувачів з нуля. Однак люди, які знаються на роботі зі стандартними файлами конфігурації Linux / Unix, особливих проблем не відчують [22].

3. Icinga.

Icinga виникла вякості відгалуження від системи моніторингу Nagios, проте нещодавно була переписаною в самостійну програму, відому під назвою Icinga2.

Наразі дві версії даного ПЗ знаходяться на стадії проектування та є доступними для застосування, при цьому Icinga1 є сумісною з великим числом плагінів та конфігурацією Icinga2. Вона проектувалася менш громіздкою, з направленістю на продуктивність. Програма має модульну архітектуру та широкий функціонал дизайну, що не має ані Nagios, ані Icinga1.

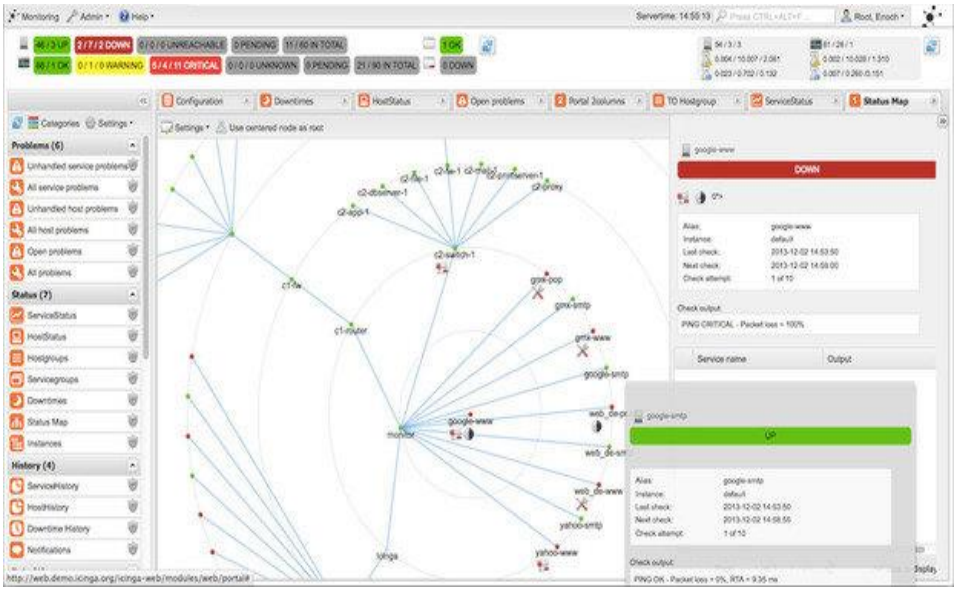


Рис. 1.7. Приклад інтерфейсу Icinga

Як і Nagios, Icinga може використовуватися для моніторингу скрізь, де присутня мова типу IP, настільки вдало, наскільки можна застосовувати SNMP. Крім того, можна налаштувати плагіни та додатковий функціонал.

Існують варіанти веб-інтерфейсу для ПЗ Icinga, проте особливою відмінністю цього ПЗ для моніторингу від Nagios є саме конфігураційне виконання, що може виконуватися за допомогою веб-інтерфейсу, а не за допомогою файлів конфігураційного рішення.

Icinga здатна інтегруватися з великою кількістю програм для моніторингу та графічного представлення на кшталт PNP4Nagios, inGraph та Graphite, що забезпечує чітку візуалізацію мереж.

4. Ntop.

Програма Ntop більш відома як Ntopng наразі є першокласним інструментом для моніторингу мережевого трафіку в купі зі швидким та простим веб-

інтерфейсом. Ntop являє собою засіб для дослідження пакетів з легким веб-інтерфейсом, що демонструє дані в режимі онлайн відносно трафіку мережі.

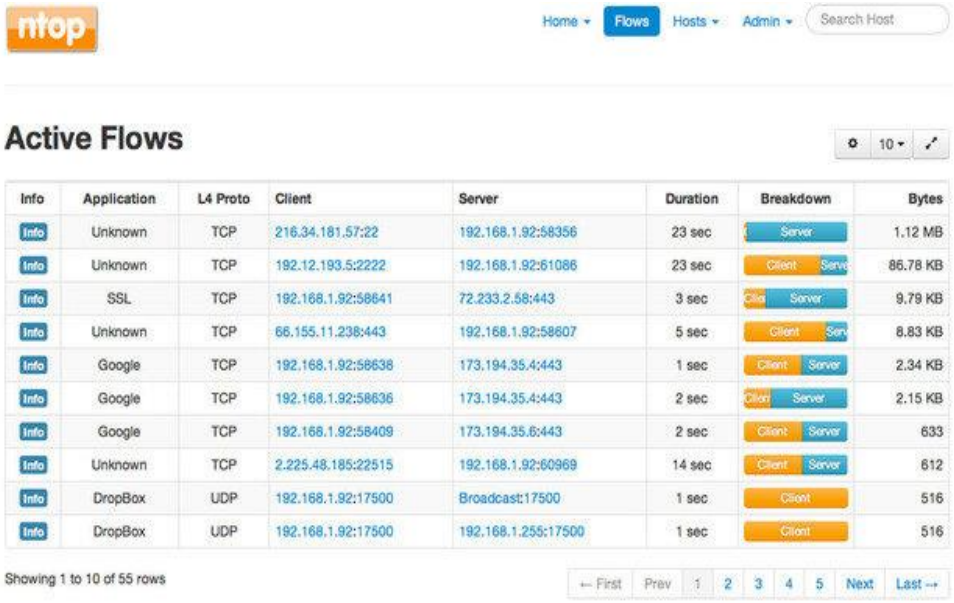


Рис. 1.8. Інтерфейс Ntop

Ntop надає можливість з легкістю отримувати графіки та таблиці, які демонструють реальні та минулі мережеві трафіки, враховуючи протоколи, джерела, призначення і історію відповідних операцій, крім того хости з обох кінців. Водночас у функціоналі представлено вражаючу кількість графіків, діаграм та карт застосування мереж в режимі он-лайн, а також модульну архітектуру для великого числа надбудов на кшталт добавки моніторів NetFlow та sFlow. Тут навіть можна знайти Nbox - апаратний монітор, який вбудовує в Ntop.

Водночас програма Ntop має API-інтерфейс задля скриптової мови програмування Lua, що здатний застосовуватися під час підтримки відповідного розширення. Ntop здатна зберегти дані хоста у вигляді файлів RRD для того, аби здійснити постійний збір даних. Одним з найбільш корисних програмних додатків Ntopng є контролінг трафіку в певному місці.

5. Observium.

Observium - це система для моніторингу мережевих пристоїв та серверів, що має великий набір підтримуваного обладнання, яке використовує протоколи типу SNMP. В якості ПЗ, яке відноситься до LAMP, програма Observium достатньо не

вимагає складних установок, а лише налаштування Apache, PHP та MySQL, проектування БД, конфігураційних рішень Apache [38].

Програма встановлюється як самостійний сервер з виділеною URL-адресою. Observium об’єднує в собі моніторинг системи та мережі із дослідженням тенденцій продуктивності функціонування. Можна легко входити до графічного інтерфейсу програми та додавати нові хости та мережі, а також задавати діапазон для автоматичного контролю та даних SNMP, для того, щоб програма могла надалі аналізувати навколишні мережі і збирати дані відносно кожної виявленої системи. ПЗ типу Observium здатне знаходити мережеве обладнання за допомогою протоколів типу CDP, типу LLDP чи типу FDP, а віддалені агенти хоста здатні розгортатися на Linux-програмах для того, аби допомогти під час збору даних.

Всі ці зібрані дані доступні через легкий у застосування призначений для користувача інтерфейс, що надає функціонал для статистичного показу даних, а також у виді діаграми та графіку. Можна також отримувати будь-що, наприклад, часу відгуку ping та SNMP, чи графіки пропускної спроможності, фрагментації, число IP-пакетів [37].

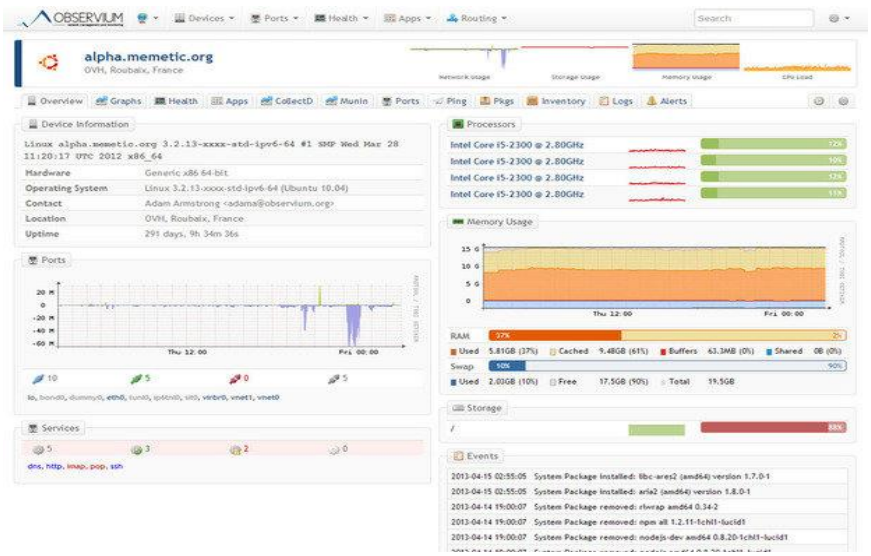


Рис. 1.9. Інтерфейс програми Observium

Отож, наразі є безліч рішень відносно програм CIM, однак багато з них мають складнощі в площині програмного впровадження та досить обмежений функціонал.

1.4. Обгрунтування вибору платформи IBM QRadar SIEM та її переваги

Компанія IBM Security пропонує одні із найдосконаліших інтегрованих портфелів продуктів корпоративної безпеки та послуг. Портфоліо, підтримане всесвітньо відомими Дослідження IBM X-Force надають рішення безпеки для допомоги організаціям для впровадження безпеки в структуру діяльності свого бізнесу, щоб вони могли процвітати в умовах невизначеності. IBM керує однією з найширших і найглибших систем безпеки науково-дослідних та дослідницьких організацій. Моніторинг понад одного трильйона подій на місяць у більш ніж у 130 країнах, IBM володіє понад 3000 патентами безпеки.

Компанія IBM пропонує сучасний інтелектуальний комплекс моніторингу інформаційної безпеки підприємства – IBM QRadar. Цей комплекс надає можливість кореляційного аналізу даних у реальному часі для отримання актуальних знань про загрози безпеці. Комплекс QRadar забезпечує високий рівень масштабування та продуктивності, централізоване управління, можливість конфігурації та адаптації до специфічних вимог на основі сервісних майстрів та інші переваги. Продукт QRadar належав компанії Q1Labs, яка увійшла до корпорації IBM в 2011 році.

Переваги вибору платформи IBM QRadar SIEM [43]:

– Проста конфігурація і розвертання на локальних ресурсах і в хмарному середовищі.

– Відображення подій в реальному часі або за результатами минулих періодів.

– Комплексне виявлення інцидентів і управління уразливістю.

– Сильні аналітичні можливості завдяки QRadar використовує контекст для підозрювальних інцидентів, що призводить до масового скорочення даних і більшої швидкості виявлення інцидентів.

– Можливість надати аналіз поведень і відхилень даних мережевого потоку і журналів.

– Дані потоки (сетевого трафіку) і дані подій об'єднані в єдину панель, що дозволяє користувачам точно визначати пріоритети даних об інцидентах, зменшуючи кількість ложних обробок.

– IBM Security App Exchange дозволяє клієнтам, робочим партнерам та іншим розробникам створювати додатки, що розширюють можливості QRadar.

– Інтегрується з усіма відповідними продуктами IBM і багатьма сторонніми постачальниками.

Отже, використання платформи QRadar адміністраторами підвищує ефективність обслуговування комп’ютерної мережі у декілька разів завдяки застосуванню функцій автоматичного пошуку й аналізу виникнення загроз, попередження їх виникнення, а також надання повної інформації про вузли, виконання процесів та передавання пакетів у мережі. Завдяки QRadar розширюються можливості відділів підприємства, які зможуть швидше і ефективніше реагувати на зміни і вирішувати оперативні завдання.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ IBM QRADAR SIEM

2.1. Призначення, можливості та функції IBM QRadar SIEM

Не бракує проблем, з якими стикаються команди безпеки: збільшення обсягу та складності кібератак, витік даних, розширення поверхні атаки, розрізнені інструменти безпеки та брак кваліфікованого персоналу служби безпеки. Насправді організації витрачають сотні годин на тиждень на розслідування підозрілих сповіщень, але, незважаючи на цей витрачений час, близько 17% сповіщень не розслідуються [29]. Організації, які прагнуть забезпечити конфіденційність своїм клієнтам, захистити їхню інтелектуальну власність і уникнути ризиків щодо бізнесу, повинні проактивно контролювати своє середовище, щоб вони могли швидко виявляти загрози та точно реагувати до того, як зловмисники зможуть завдати фінансової та репутаційної шкоди.

IBM Security QRadar, провідне на ринку рішення SIEM, допомагає захиститися від зростаючих загроз, модернізуючи та масштабуючи операції безпеки за допомогою інтегрованої видимості, виявлення, дослідження та реагування. QRadar надає командам із безпеки централізовану видимість даних про безпеку в масштабах підприємства та практичну інформацію щодо найпріоритетніших загроз. Аналітики безпеки можуть працювати з однієї панелі, щоб швидко зрозуміти механізми своєї безпеки, виявити найбільш критичні загрози та детальніше розібратися, щоб спростити робочі процеси та позбутися необхідності переходити між інструментами.

Завдяки можливостям виявлення аномалій QRadar служби безпеки можуть швидко ідентифікувати зміни в поведінці користувачів, які можуть вказувати на невідому загрозу.

Рішення отримує величезну кількість даних у всьому підприємстві, щоб забезпечити повне уявлення про діяльність у локальному та хмарному середовищах. У міру надходження даних QRadar застосовує автоматизовану

інформацію про безпеку в реальному часі, щоб швидко й точно виявляти загрози та визначати пріоритети. Дійсні сповіщення надають широкий контекст потенційних інцидентів, дозволяючи аналітикам безпеки швидко реагувати, щоб обмежити вплив зловмисників. QRadar розроблено спеціально для широкого спектру випадків використання безпеки та легко масштабується з обмеженими зусиллями щодо налаштування.

Корпоративні мережі можуть охоплювати традиційні локальні IT-середовища, хмарні середовища та операційні технології (OT), усі з яких вимагають певного рівня нагляду для ефективного захисту активів, точного виявлення загроз і підтримки відповідності. Перш ніж служби безпеки зможуть почати аналізувати дані для виявлення загроз і керування ними, вони повинні мати централізований доступ до розрізнених даних безпеки.

QRadar дає змогу організаціям отримати *централізовану повну видимість* ізольованих середовищ шляхом збору, аналізу та нормалізації даних журналів і потоків. З однієї панелі аналітики безпеки можуть контролювати локальні, хмарні та гібридні середовища. Рішення включає понад 450 попередньо створених *модулів підтримки пристроїв* (DSM - Device Support Modules), які забезпечують інтеграцію налаштувань за замовчуванням з іншими інвестиціями в безпеку. Клієнти можуть просто направляти журнали на QRadar, і рішення може автоматично визначати тип джерела журналу та застосовувати правильний DSM для аналізу та нормалізації даних журналу. У результаті клієнти QRadar можуть налагодити роботу набагато швидше, ніж клієнти альтернативних рішень. Додаткові інтеграції можна легко додати через програми в IBM Security App Exchange.

QRadar також пропонує *простий редактор DSM* з інтуїтивно зрозумілим графічним інтерфейсом користувача (GUI), який дозволяє командам безпеки легко визначати, як аналізувати журнали з користувацьких програм.

Щоб легко створити базу даних активів, що дозволяє організаціям визначати критичні активи або сегменти мережі, QRadar може перевіряти дані мережевого потоку, щоб *автоматично ідентифікувати та класифікувати* дійсні активи в мережі на основі програм, протоколів, служб і портів, які вони використовують.

QRadar підтримує широкий спектр технологій, додатків і хмарних служб, щоб допомогти клієнтам отримати повну видимість діяльності в масштабах підприємства. Після централізації цих даних їх можна автоматично аналізувати, щоб виявити відомі загрози, аномалії, які можуть вказувати на невідомі загрози, і критичні ризики, через які конфіденційні дані можуть стати відкритими.

QRadar *розроблений для автоматичного аналізу та кореляції активності* в багатьох джерелах даних, включаючи журнали, події, мережеві потоки, активність користувачів, інформацію про вразливості та розвідку про загрози, щоб ідентифікувати відомі та невідомі загрози.

QRadar збирає, аналізує та співвідносить дані з різноманітних джерел, щоб виявляти та визначати пріоритетність найбільш критичних загроз, які потребують дослідження (див. рис. 2.1).

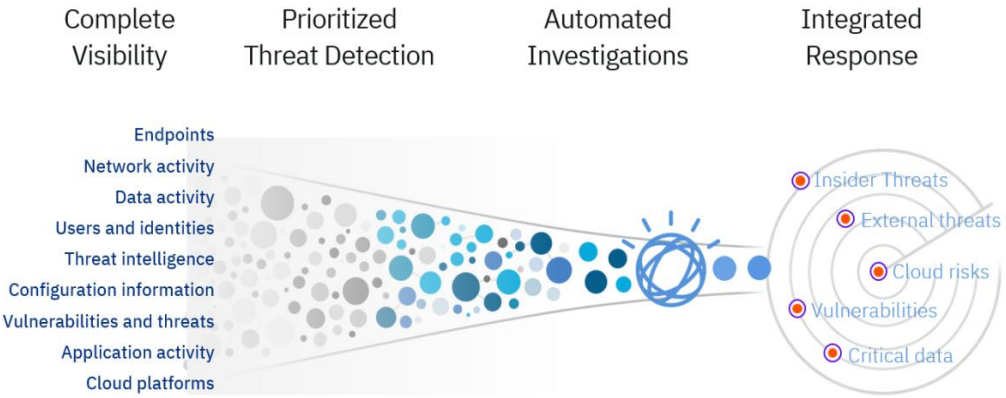


Рис. 2.1. Автоматичний аналіз та визначення пріорітетних загроз у QRadar

QRadar співвідносить та аналізує безліч типів даних із різноманітних джерел, зокрема:

1. *Дані кінцевої точки*: із журналу подій Windows, Sysmon, рішень EDR тощо.
2. *Дані про мережеву активність*: від брандмауерів, шлюзів, маршрутизаторів або датчиків.
3. *Дані про вразливості*: з антивірусних інструментів, сканерів уразливостей, систем виявлення вторгнень, систем запобігання вторгненням, систем запобігання втраті даних тощо.

4. *Хмарна діяльність*: із середовищ SaaS та IaaS, таких як Office365, SalesForce.com, Amazon Web Services (AWS), Microsoft Azure та Google Cloud.
5. *Дані користувача та ідентифікаційні дані*: отримані з Active Directory, LDAP або інших рішень для керування ідентифікацією та доступом.
6. *Дані додатків*: із рішень планування ресурсів підприємства (ERP), баз даних додатків, додатків SaaS тощо.
7. *Інтелектуальні дані про загрози*: з таких джерел, як IBM X-Force, і сторонніх каналів аналізу загроз.
8. *Дані про діяльність контейнера*: програмне забезпечення технологій управління та оркестровки контейнерів, наприклад Kubernetes QRadar, включає сотні попередньо створених варіантів використання безпеки, алгоритми виявлення аномалій, правила та політики кореляції в реальному часі для виявлення відомих і невідомих загроз. Коли загрози виявляються, рішення об'єднує пов'язані події безпеки в єдині пріоритетні сповіщення, відомі як «првопорушення». Пріоритети правопорушень автоматично встановлюються на основі серйозності загрози та критичності залучених активів (див. рис.2.2) [29].

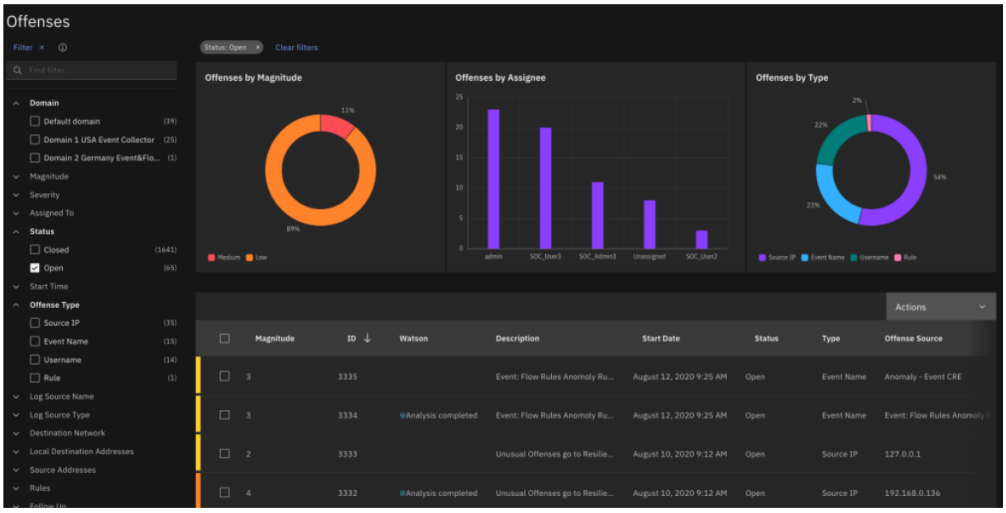


Рис. 2.2. Перегляд правопорушень у QRadar надає пріоритетний список загроз

У межах кожного правопорушення аналітики безпеки можуть бачити повний ланцюжок загроз на одному екрані. Звідси аналітики можуть легко детально

ознайомитися з конкретними подіями чи мережевими потоками, щоб почати розслідування, призначити вирішення правопорушення конкретному аналітику або закрити його. *Порушення автоматично оновлюються*, коли відбувається нова пов'язана діяльність, щоб аналітики могли бачити найновішу інформацію в будь-який момент часу. Цей унікальний підхід допомагає аналітикам безпеки легко зрозуміти найбільш критичні загрози в середовищі, надаючи наскрізне розуміння кожного потенційного інциденту, одночасно зменшуючи загальний обсяг попереджень.

Оскільки зловмисники стають більш досконалими у своїх методах, виявлення відомих загроз вже недостатньо. Натомість організації також повинні мати можливість виявляти незначні зміни в поведінці мережі, користувачів або системи, які можуть вказувати на невідомі загрози, такі як зловмисники, скомпрометовані облікові дані або зловмисне програмне забезпечення без файлів.

QRadar *містить різноманітні можливості виявлення аномалій* для ідентифікації змін в поведінці, які можуть бути індикаторами невідомої загрози.

QRadar User Behavior Analytics аналізує активність користувачів, щоб виявити зловмисників і визначити, чи були скомпрометовані облікові дані користувача. Аналітики безпеки можуть легко бачити користувачів, які піддаються ризику, переглядати їхні аномальні дії та детально вивчати базові дані журналу та потоків, які внесли свій внесок у оцінку ризику користувача.

Додатково використовуючи QRadar Network Insights як частину розгортання SIEM, організації можуть отримати уявлення про те, які системи обмінювались інформацією одна з одною, які програми були задіяні та які дані передавалися в пакетах. Співвідносячи цю інформацію з іншою мережею, журналом і діяльністю користувачів, аналітики безпеки можуть виявити аномальну мережеву активність, яка може вказувати на скомпрометовані хости, або ж користувачів чи спроби викрадання даних.

Хоча QRadar постачається з численними правилами виявлення аномалій і поведінки в якості налаштувань за замовчуванням, групи безпеки також можуть створювати власні правила, адаптувати параметри виявлення аномалій і

завантажувати понад *265 готових додатків із IBM Security App Exchange*, щоб покращити своє розгортання.

Групи безпеки обтяжені великою кількістю попереджень, ручними завданнями та обмеженим персоналом, що часто призводить до виснаження та послаблення системи безпеки організації. QRadar Advisor with Watson використовує штучний інтелект і автоматизацію, щоб значно скоротити час, витрачений на дослідження сповіщень про загрози, від днів і тижнів до хвилин або годин. Advisor надає пріоритетні дослідження попереджень і корельовані дані, щоб допомогти аналітикам зосередитися на ефективнішому стратегічному аналізі та пошуку загроз, використовуючи стандартне відображення MITER ATT&CK для покращення аналізу першопричин.

Це забезпечує швидше виправлення, коротший час очікування, менше пропущених критичних інцидентів, меншу втому аналітиків і покращену ефективність SOC/аналітиків.

QRadar групує та визначає пріоритети всіх пов’язаних подій під одним злочином, надаючи аналітикам безпеки повне уявлення про потенційно розвивається сценарій атаки. Аналіз перехресних розслідувань забезпечує багатий контекст попереджень шляхом автоматичного зв’язування розслідувань через пов’язані інциденти, що зменшує дублювання зусиль і розширює розслідування за межі поточного ймовірного інциденту та попередження.

Крім того, Advisor з Watson забезпечує поєднання когнітивних ідей і локального аналізу даних, призначених для виявлення пов’язаних індикаторів компромісу (IOC – indicators of compromise). QRadar може будувати графік взаємозв’язків у розслідуванні, щоб візуалізувати збагачені дані розслідування та досліджувати зв’язки з іншими IOC, активами, користувачами чи дослідженнями.

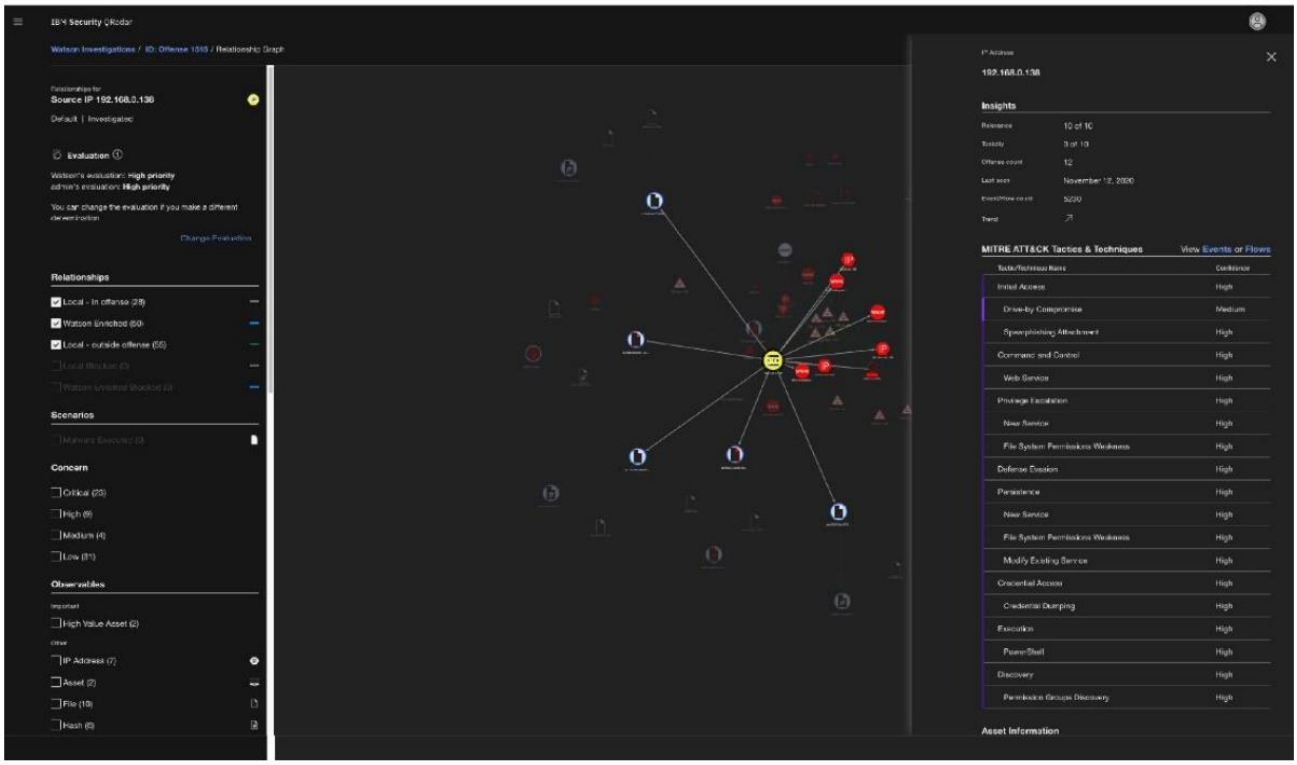


Рис. 2.3. Графік зв’язків між IOC, активами, користувачами чи іншими дослідженнями

Advisor також прив’язує розслідування до структури MITER ATT&CK, щоб групи безпеки могли візуалізувати тактику та прийоми зловмисників, детально вивчати події та потоки на стадії ATT&CK і приймати більш впевнені рішення.

Інтеграція IBM Security QRadar із IBM Security SOAR дозволяє командам безпеки пришвидшувати час реагування на інциденти за допомогою покрокових посібників, автоматизації ручних завдань, а також послідовної співпраці та координації з керуванням справами. Аналітики безпеки можуть швидко й ефективно передавати підозрілі події з QRadar до IBM Security SOAR, ініціювати додаткові автоматизовані збагачення та керувати повним процесом розслідування. У міру розвитку інциденту вся інформація синхронізується між QRadar і IBM Security SOAR, забезпечуючи повну цілісність даних. Будь-яка нова інформація, виявлена IBM Security SOAR, повертається в QRadar для покращення процесу виявлення.

QRadar *забезпечує прозорість, підзвітність і можливість вимірювання*, які є критично важливими для успішного виконання організацією нормативних вимог і звітності про відповідність. Здатність рішення співвідносити та інтегрувати канали аналізу загроз дає повніші показники для звітності про IT-ризики для аудиторів. Сотні готових звітів і шаблонів правил можуть допомогти організаціям легше відповідати галузевим вимогам відповідності.

Гнучка, масштабована архітектура QRadar розроблена для підтримки як великих, так і малих організацій із різними потребами. Менші організації можуть почати з єдиного комплексного рішення, яке можна легко оновити до розподіленого розгортання в міру розвитку потреб.

Більші корпоративні організації можуть розгортати спеціальні компоненти для підтримки глобальних розподілених мереж із великими обсягами даних.

IBM Security QRadar включає такі *компоненти:* збирачі подій, процесори подій, збирачі потоків, процесори потоків, вузли даних (для менш вартісного зберігання та підвищення продуктивності) і центральну консоль. Усі компоненти доступні як обладнання, програмне забезпечення або віртуальні пристрої. Варіанти програмного забезпечення та віртуальних пристроїв можна розгортати локально, у середовищах IaaS або розподіляти між гібридними середовищами.

Незалежно від моделі розгортання, організації можуть додатково додати *захист високої доступності та аварійного відновлення*, де і коли це необхідно, щоб забезпечити безперервну роботу. Для організацій, яким потрібна відмовостійкість бізнесу, QRadar забезпечує інтегроване автоматичне перемикання після відмови та повну синхронізацію дисків між системами без необхідності використання додаткових продуктів сторонніх виробників для керування несправностями. Для організацій, які потребують захисту та відновлення даних, можливості аварійного відновлення QRadar можуть пересилати поточні дані, такі як потоки та події, з основної системи QRadar до вторинної паралельної системи, розташованої на окремому об’єкті.

Можна зробити висновок, що IBM Security QRadar — це провідне рішення на ринку SIEM, яке застосовує автоматизовану інтелектуальну аналітику до великої

кількості даних безпеки, щоб надати аналітикам безпеки ефективне розуміння найбільш критичних загроз, дозволяючи їм приймати кращі та швидші рішення щодо сортування та реагування.

Це комплексне рішення поєднує керування журналами, аналіз мережі, аналітику поведінки користувачів, розвідку про загрози та розслідування на основі штучного інтелекту в одному рішенні – інтегрованому з IBM Security SOAR для реагування на інциденти – усе з комплексною видимістю в локальних, хмарних і гібридних середовищах.

2.2. Компоненти та архітектура рішення IBM QRadar SIEM

Задля розгортання IBM QRadar, необхідно добре знати архітектуру QRadar, щоб оцінити, як компоненти QRadar можуть функціонувати в обраній мережі [29].

IBM QRadar збирає, обробляє, агрегує та зберігає мережеві дані в реальному часі. QRadar використовує ці дані для керування мережевою безпекою, надаючи інформацію в реальному часі та моніторинг, попередження та порушення, а також відповіді на мережеві загрози.

IBM QRadar SIEM — це модульна архітектура, яка забезпечує видимість IT-інфраструктури в режимі реального часу, яку можна використовувати для виявлення загроз і встановлення пріоритетів. Систему QRadar можна масштабувати для задоволення потреби в зборі журналів і потоків і аналізі. Є можливість додати інтегровані модулі до платформи QRadar, наприклад QRadar Risk Manager, QRadar Vulnerability Manager і QRadar Incident Forensics.

Робота платформи безпеки QRadar складається з трьох рівнів і застосовується до будь-якої структури розгортання QRadar, незалежно від її розміру та складності. На наступній діаграмі показано рівні, які складають архітектуру QRadar (див. рис. 2.4).

Архітектура QRadar функціонує однаково незалежно від розміру чи кількості компонентів у розгортанні. Наступні три рівні, представлені на схемі, представляють основні функції будь-якої системи QRadar.

Збір даних

Збір даних – це ***перший рівень***, на якому збираються такі дані, як події або потоки, з поточної мережі. Пристрій All-in-One можна використовувати для збору даних безпосередньо з мережі або використовуються збирачі даних, такі як QRadar Event Collectors або QRadar Flow Collectors, щоб збирати дані про події чи потоки. Дані аналізуються та нормалізуються перед тим, як вони передаються на рівень обробки. Коли необроблені дані аналізуються, вони нормалізуються, щоб представити їх у структурованому та зручному форматі.

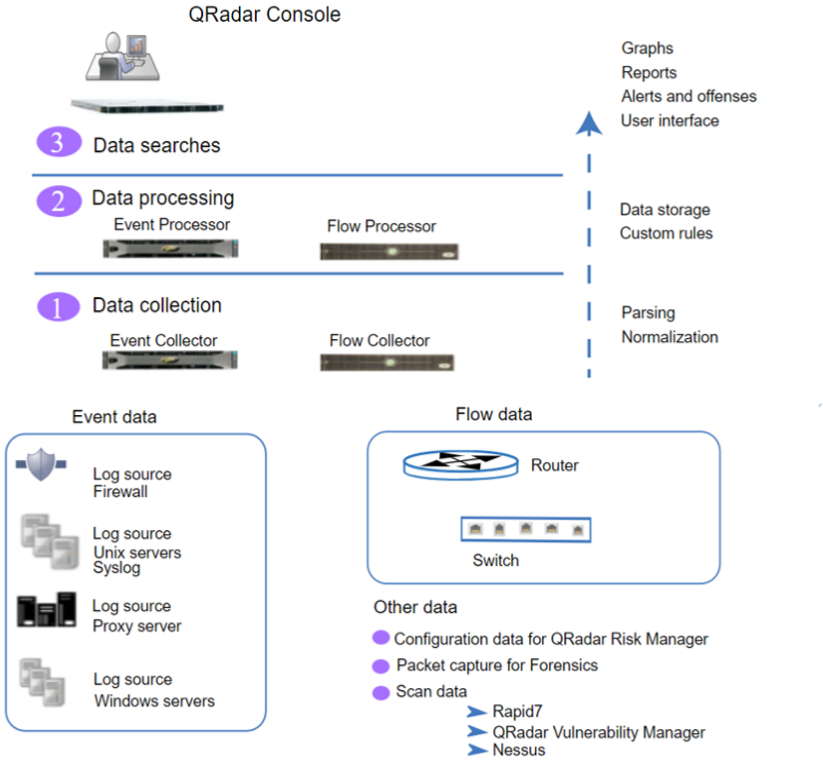


Рис. 2.4. Архітектура QRadar

Основні функції QRadar SIEM зосереджені на зборі даних про події та потоках.

Дані про події представляють події, які відбуваються в певний момент часу в середовищі користувача, як-от входи користувачів, електронна пошта, VPN-з'єднання, заборони брандмауера, проксі-з'єднання та будь-які інші події, які можна реєструвати в журналах пристрою.

Дані потоку — це інформація про мережеву активність або інформація про сеанс між двома хостами в мережі, яку QRadar перетворює на записи потоку. QRadar перетворює або нормалізує необроблені дані в IP-адреси, порти, кількість байтів і пакетів, а також іншу інформацію в записи потоку, що фактично представляє сеанс між двома хостами. На додаток до збору інформації про потік за допомогою Flow Collector, повне захоплення пакетів доступне за допомогою компонента QRadar Incident Forensics.

Обробка даних

Після збору даних йде ***другий рівень*** — це місце, на якому дані про події та дані потоку запускаються через механізм спеціальних правил (CRE), який генерує порушення та сповіщення, а потім дані записуються в сховище.

Дані подій і дані потоку можуть оброблятися за допомогою пристрою All-in-One без необхідності додавання процесорів подій або процесорів потоку. Якщо потужність обробки багатофункціонального пристрою перевищена, може знадобитися додати процесори подій, процесори потоку або будь-який інший пристрій обробки, щоб виконати додаткові вимоги. Також може знадобитися більший обсяг пам’яті, який можна отримати, додавши вузли даних.

Інші функції, такі як QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM) або QRadar Incident Forensics, збирають різні типи даних і надають більше функцій.

QRadar Risk Manager збирає конфігурацію мережевої інфраструктури та надає карту топології мережі. Ви можете використовувати дані для управління ризиками, імітуючи різні мережеві сценарії шляхом зміни конфігурацій і впровадження правил у вашій мережі.

QRadar Vulnerability Manager використовується для сканування мережі та обробки даних про вразливості або керування даними про вразливості, зібраними з інших сканерів, таких як Nessus і Rapid7. Зібрані дані про вразливості використовуються для виявлення різних ризиків безпеки у вашій мережі.

QRadar Incident Forensics використовується для проведення поглиблених криміналістичних розслідувань і відтворення повних сеансів мережі.

Пошук даних

На ***третьому або верхньому рівні*** знаходяться дані, які збирає та обробляє QRadar, доступні користувачам для пошуку, аналізу, звітування та сповіщень або розслідування правопорушень. Користувачі можуть здійснювати пошук і керувати завданнями адміністратора безпеки для своєї мережі з інтерфейсу користувача на консолі QRadar.

У системі All-in-One усі дані збираються, обробляються та зберігаються на пристрої All-in-One.

У розподілених середовищах QRadar Console не виконує обробку подій і потоків або зберігання. Натомість консоль QRadar використовується переважно як інтерфейс користувача, де користувачі можуть використовувати її для пошуку, звітів, сповіщень і досліджень.

Компоненти QRadar

Компоненти IBM QRadar застосовуються для масштабування розгортання QRadar, а також для керування збором і обробкою даних у розподілених мережах.

Важливо: версії програмного забезпечення для всіх пристроїв IBM QRadar у розгортанні повинні мати однакову версію та рівень пакета виправлень. Розгортання, які використовують різні версії програмного забезпечення, не підтримуються, оскільки середовища, які використовують змішані версії, можуть призвести до того, що правила не запускаються, порушення не створюються чи оновлюються, а також помилки в результатах пошуку.

Розгортання QRadar може включати наступні компоненти, що описані нижче.

Консоль QRadar

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

У розподілених розгортаннях QRadar використовується консоль QRadar для керування хостами, які включають інші компоненти.

Збирач подій QRadar

Збирач подій колекціонує події з локальних і віддалених джерел журналу та нормалізує вихідні події необробленого журналу, щоб відформатувати їх для використання QRadar. Збирач подій групує або об'єднує ідентичні події для економії використання системи та надсилає дані до процесора подій.

QRadar Event Collector Virtual 1599 можна застосовувати у віддалених місцях із повільними WAN-з'єднаннями. Пристрої Event Collector не зберігають події локально. Замість цього пристрої збирають і аналізують події перед тим, як надсилати події на пристрій процесора подій для зберігання.

Збирач подій може використовувати обмежувачі пропускної здатності та розклади для надсилання подій до процесора подій, щоб подолати обмеження WAN, такі як переривчасте підключення.

Збирач подій призначається ліцензії EPS, яка відповідає процесору подій, до якого він підключений.

Процесор подій QRadar

Процесор подій обробляє події, зібрані з одного або кількох компонентів збирача подій. Процесор подій обробляє події за допомогою механізму спеціальних правил (CRE). Якщо події зіставляються з настроюваними правилами CRE, попередньо визначеними на консолі, процесор подій виконує дію, визначену для відповіді правила.

Кожен процесор подій має локальне сховище, а дані подій зберігаються в процесорі або можуть зберігатися у вузлі даних.

Швидкість обробки подій визначається ліцензією подій за секунду (EPS). Якщо перевищується показник прибутку на акцію, події буферизуються та залишаються в чергах джерела збирача подій, доки показник не знизиться. Однак якщо перевищення ліцензійної ставки EPS перевищується і черга заповнюється, система пропускає події, і QRadar видає попередження про перевищення ліцензованої ставки EPS.

Додаючи процесор подій до пристрою All-in-One, функція обробки подій переміщується від All-in-One до Event Processor.

QRadar Flow Collector

Flow Collector збирає потоки, підключаючись до порту SPAN або мережевого TAP. IBM QRadar Flow Collector також підтримує збір зовнішніх потокових джерел даних, таких як NetFlow з маршрутизаторів.

QRadar Flow Collectors не розроблені як системи повного захоплення пакетів. Для повного захоплення пакетів розглядається опція QRadar Incident Forensics. Зокрема, пристрій QRadar Flow Collector 1310 може пересилати пакети на пристрій QRadar Packet Capture, що дозволяє збирати потік і збирати пакети з одного джерела пакетів.

Процесор потоку QRadar

Flow Processor обробляє потоки з одного або кількох пристроїв QRadar Flow Collector. Пристрій Flow Processor також може збирати зовнішні мережеві потоки, такі як NetFlow, J-Flow і sFlow, безпосередньо з маршрутизаторів у мережі. Щоб масштабувати розгортання QRadar для керування вищими показниками потоків за хвилину (FPM), застосовується пристрій Flow Processor. Процесори потоку включають вбудований процесор потоку та внутрішню пам’ять для даних потоку. Додаючи Flow Processor до пристрою All-in-One, функція обробки переміщується з пристрою All-in-One до Flow Processor.

Вузол даних QRadar

Вузли даних дозволяють розгортати нові та існуючі QRadar , щоб за потреби додавати обсяги зберігання та обробки. Вузли даних допомагають збільшити швидкість пошуку у вашому розгортанні, надаючи більше апаратних ресурсів для виконання пошукових запитів.

Хост програми QRadar

Хост додатків — це керований хост, призначений для запуску програм. Хости додатків надають додаткові ресурси пам’яті, пам’яті та ЦП для ваших додатків, не впливаючи на обробну здатність консолі QRadar. Такі додатки, як User Behavior Analytics з Machine Learning Analytics, вимагають більше ресурсів, ніж зараз доступно на Консолі.

Методологія сертифікації максимального EPS QRadar

Пристрої IBM QRadar сертифіковано для підтримки певної максимальної швидкості подій за секунду (EPS). Максимальний EPS залежить від типу даних, що обробляються, конфігурації системи та завантаження системи.

Розгортання, які значно відрізняються від параметрів тестування, описаних у цьому документі, можуть не підтримувати сертифіковані показники. Максимальна сертифікована норма EPS є абсолютною. Якщо навантаження на систему менше, ніж максимальне навантаження сертифікації EPS QRadar, максимальна швидкість EPS для розгортання не збільшиться.

Події та потоки QRadar

Основними функціями IBM QRadar SIEM є керування безпекою мережі шляхом моніторингу потоків і подій.

Суттєва різниця між даними про подію та потоком полягає в тому, що подія, яка зазвичай є журналом певної дії, як-от вхід користувача або з'єднання VPN, відбувається в певний час, і в цей час подія реєструється. Потік — це запис мережевої активності, який може тривати секунди, хвилини, години або дні, залежно від активності протягом сеансу. Наприклад, веб-запит може завантажувати кілька файлів, таких як зображення, оголошення, відео, і триватиме від 5 до 10 секунд, або користувач, який дивиться фільм Netflix, може перебувати в мережевому сеансі, який триває до кількох годин. Потік — це запис мережевої активності між двома хостами.

Події

QRadar приймає журнали подій із джерел журналів у мережі. Джерело журналу — це джерело даних, наприклад брандмауер або система захисту від вторгнень (IPS), яка створює журнал подій. QRadar приймає події з джерел журналу за допомогою таких протоколів, як syslog, syslog-tcp і SNMP. QRadar також може налаштувати вихідні з'єднання для отримання подій за допомогою таких протоколів, як SCP, SFTP, FTP, JDBC, Check Point OPSEC і SMB/CIFS.

Конвеєр подій

Перш ніж ви зможете переглядати та використовувати дані подій на консолі QRadar, події збираються з джерел журналів, а потім обробляються процесором подій. Пристрій QRadar All-in-One функціонує як збирач подій і процесор подій на додаток до виконання ролі консолі QRadar.

QRadar може збирати події за допомогою спеціального пристрою Event Collector або за допомогою пристрою All-in-One, де служба збору подій і служба обробки подій працює на пристрої All-in-One. На наступній діаграмі показано рівні конвеєра подій.

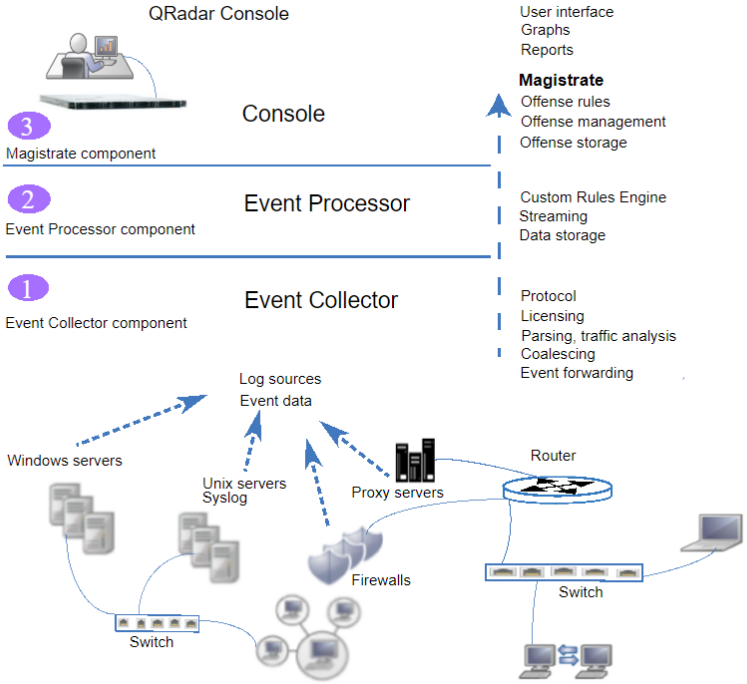


Рис. 2.5. Конвеєр подій

Колекція подій

Компонент *Event Collector* виконує такі функції:

1. *Протокол* - збирає дані з протоколів джерел журналу, таких як Syslog, JDBC, OPSEC, Log File і SNMP.
2. *Обмеження ліцензії*. Відстежує кількість вхідних подій до системи для керування чергами введення та ліцензуванням EPS.
3. *Розбір*. Бере необроблені події з вихідного пристрою та аналізує поля у форматі, придатному для використання QRadar .

4. *Журнал аналізу трафіку джерела та автоматичне виявлення*. Застосовує аналізовані та нормалізовані дані подій до можливих DSM, які підтримують автоматичне виявлення.
5. *Об'єднання.* Події аналізуються, а потім об'єднуються на основі спільних атрибутів подій.
6. *Пересилання подій*. Застосовує правила маршрутизації для системи для пересилання даних до зовнішніх цілей, зовнішніх систем Syslog, систем JSON та інших SIEM.

Коли збирач подій отримує події з джерел журналу, таких як брандмауери, події розміщуються у вхідних чергах для обробки.

Розміри черги залежать від протоколу або методу, який використовується, і з цих черг події аналізуються та нормалізуються. Процес нормалізації передбачає перетворення необроблених даних у формат із такими полями, як IP-адреса, які може використовувати QRadar.

QRadar розпізнає відомі джерела журналів за IP-адресою джерела або іменем хоста, які містяться в заголовку.

QRadar аналізує та об'єднує події з відомих джерел журналу в записи. Події з нових або невідомих джерел журналу, які не були виявлені в минулому, перенаправляються до механізму аналізу трафіку (автоматичне визначення).

Коли виявляються нові джерела журналу, на консоль QRadar надсилається повідомлення із запитом конфігурації для додавання джерела журналу. Якщо автоматичне виявлення вимкнено або перевищено ліцензійний ліміт джерела журналу, нові джерела журналу не додаються.

Обробка подій

Компонент процесора подій виконує такі функції:

1. *Механізм спеціальних правил (CRE)* відповідає за обробку подій, отриманих QRadar, і порівняння їх із визначеними правилами, відстеження систем, залучених до інцидентів протягом певного часу, створення сповіщень для користувачів. Коли події збігаються з правилом, сповіщення з процесора подій надсилається судді на консолі QRadar про те, що певна подія

ініціювала правило. Компонент Magistrate на консолі QRadar створює правопорушення та керує ними. Коли правила запускаються, генеруються відповіді або дії, такі як сповіщення, системний журнал, SNMP, повідомлення електронної пошти, нові події та порушення.

2. *Потокове передавання* надсилає дані подій у реальному часі на консоль QRadar, коли користувач переглядає події на вкладці Журнал активності в реальному часі (потокове передавання). Потокові події не надаються з бази даних.
3. *Зберігання подій (Ariel)*. База даних часових рядів для подій, де дані зберігаються щохвилини. Дані зберігаються там, де обробляється подія.

Колекціонер подій надсилає нормалізовані дані подій до процесора подій, де події обробляються механізмом спеціальних правил (CRE). Якщо події зіставляються з настроюваними правилами CRE, попередньо визначеними на консолі QRadar, процесор подій виконує дію, визначену для відповіді правила.

Магістрат на консолі QRadar

Компонент Magistrate виконує такі функції:

1. Правила правопорушень. Відстежує правопорушення та реагує на них, наприклад, створює сповіщення електронною поштою.
2. Управління правопорушеннями. Оновлює активні правопорушення, змінює статуси правопорушень і надає користувачам доступ до інформації про правопорушення на вкладці «Порушення».
3. Зберігання злочинів. Записує дані про порушення в базу даних Postgres.

Ядро обробки суддів (MPC) відповідає за співвіднесення правопорушень із сповіщеннями про події від кількох компонентів процесора подій. Лише QRadar Console або All-in-One appliance мають компонент Magistrate.

Потоки

Потоки QRadar представляють мережеву активність шляхом нормалізації IP-адрес, портів, кількості байтів і пакетів, а також інших даних у записи потоку, які фактично є записами мережевих сеансів між двома хостами. Компонент у QRadar, який збирає та створює інформацію про потік, відомий як QFlow.

Збір QRadar Flow не є повним захопленням пакетів. Для мережевих сеансів, які охоплюють кілька часових інтервалів (хвилин), конвеєр потоку повідомляє про запис у кінці кожної хвилини з поточними даними для таких показників, як байти та пакети. Ви можете бачити кілька записів (за хвилину) у QRadar з тим самим «Часом першого пакета», але значення «Часу останнього пакета» збільшуються з часом.

Потік починається, коли Flow Collector виявляє перший пакет, який має унікальну IP-адресу джерела, IP-адресу призначення, порт джерела, порт призначення та інші параметри конкретного протоколу, включаючи поля 802.1q VLAN.

Кожен новий пакет оцінюється. Кількість байтів і пакетів додається до статистичних лічильників у записі потоку. У кінці інтервалу запис про стан потоку надсилається до процесора потоку , а статистичні лічильники потоку скидаються. Потік завершується, якщо протягом налаштованого часу не виявлено активності для потоку.

QFlow може обробляти потоки з таких внутрішніх або зовнішніх джерел:

- *Зовнішні джерела* - це джерела потоку, такі як netflow, sflow, jflow. Зовнішні джерела можна надсилати до спеціального збирача потоку або до процесора потоку, наприклад QRadar Flow Processor 1705. Зовнішні джерела не вимагають стільки обробки ЦП, оскільки кожен пакет не обробляється для створення потоків. У цій конфігурації ви можете мати спеціалізований збирач потоку та процесор потоку, які отримують і створюють дані потоку. У менших середовищах (менше 50 Мбіт/с) пристрій All-in-One може виконувати всю обробку даних.
- Flow Collector збирає *внутрішні потоки*, підключаючись до порту SPAN або мережевого TAP. QRadar Flow Collector 1310 може пересилати повні пакети зі своєї карти захоплення на пристрій захоплення пакетів, але сам не захоплює повні пакети.

На наступній діаграмі показано варіанти збирання потоків у мережі.

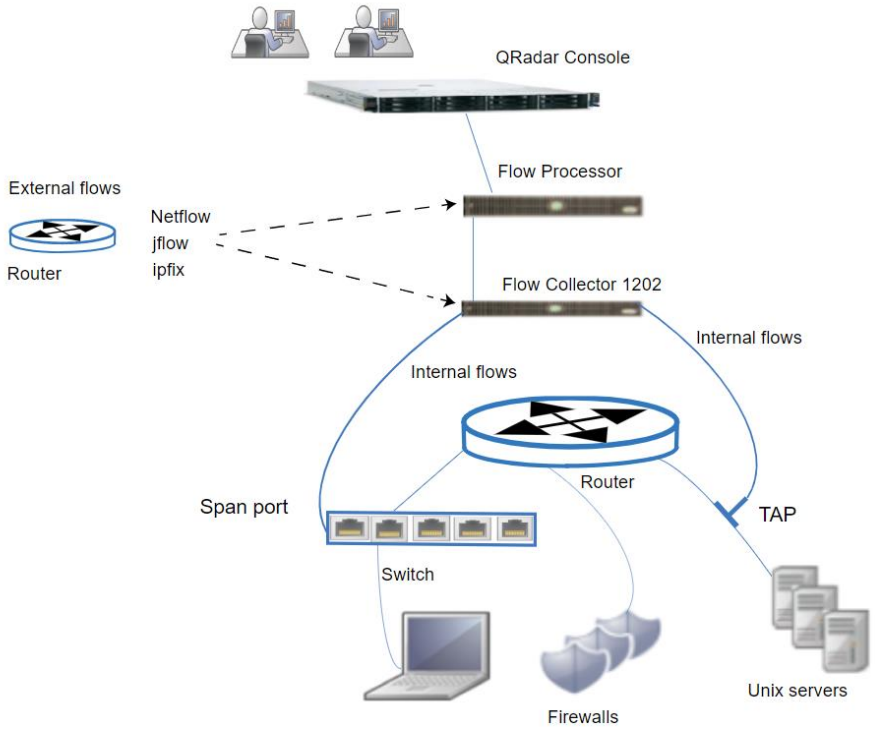


Рис. 2.6. Потоки QRadar

Потокова магістраль

Flow Collector генерує дані потоку з необроблених пакетів, які збираються з портів моніторингу, таких як SPAN, TAP і сеанси моніторингу, або із зовнішніх джерел потоку, таких як netflow, sflow, jflow. Потім ці дані перетворюються у формат потоку QRadar і надсилаються по конвеєру для обробки.

Процесор потоку виконує такі функції:

1. Дедуплікація потоку – це процес, який видаляє повторювані потоки, коли кілька збирачів потоків надають дані пристроям Flow Processors.
2. Асиметрична рекомбінація. Відповідає за поєднання двох сторін кожного потоку, коли дані надаються асиметрично. Цей процес може розпізнавати потоки з кожного боку та об’єднувати їх в один запис. Однак іноді існує лише одна сторона потоку.
3. Обмеження ліцензії. Відстежує кількість вхідних потоків до системи для керування чергами введення та ліцензуванням.
4. Пересилання. Застосовує правила маршрутизації для системи, наприклад надсилання даних потоку до зовнішніх цілей, зовнішніх систем Syslog, систем JSON та інших SIEM.

Дані потоку проходять через механізм користувацьких правил (CRE), і вони співвідносяться з налаштованими правилами, і на основі цієї кореляції може бути створено порушення.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ IBM QRADAR SIEM

3.1. Розробленя варіанта розгортання QRadar та рекомендації щодо впровадження

Основна мета першого прикладу розгортання полягає в тому, щоб описати розгортання одного пристрою All-in-One для компанії середнього розміру. Наступні приклади описують варіанти розгортання в міру розширення компанії. Приклади описують, коли додавати QRadar компоненти, такі як процесори потоку, збирачі подій iData Nodes, а також коли може знадобитися спільне розміщення певних компонентів.

Вимоги до розгортання QRadar залежать від потужності вибраного розгортання для обробки та зберігання всіх даних, які необхідно проаналізувати у вибраній мережі.

Наступна діаграма (див. рис. 3.1) показує компоненти QRadar, які можна використовувати для збору, обробки та зберігання даних подій і потоків у розгортанні. Пристрій All-in-One включає збір, обробку, зберігання, моніторинг, пошук, звітування та можливості керування правопорушеннями.

Збирач подій збирає дані про події з джерел журналів у мережі, а потім надсилає огшлдані подій до процесора подій. Flow Collector збирає дані потоку з мережевих пристроїв, таких як SPAN-порт комутатора, а потім надсилає дані до процесора потоку. Обидва процесори обробляють дані від збирачів і надають дані QRadar Console. Пристрої процесора можуть зберігати дані, але вони також можуть використовувати Data Nodes для зберігання даних. Пристрій The QRadar Console використовується для моніторингу, пошуку даних, звітності, керування правопорушеннями та адміністрування розгортання QRadar.

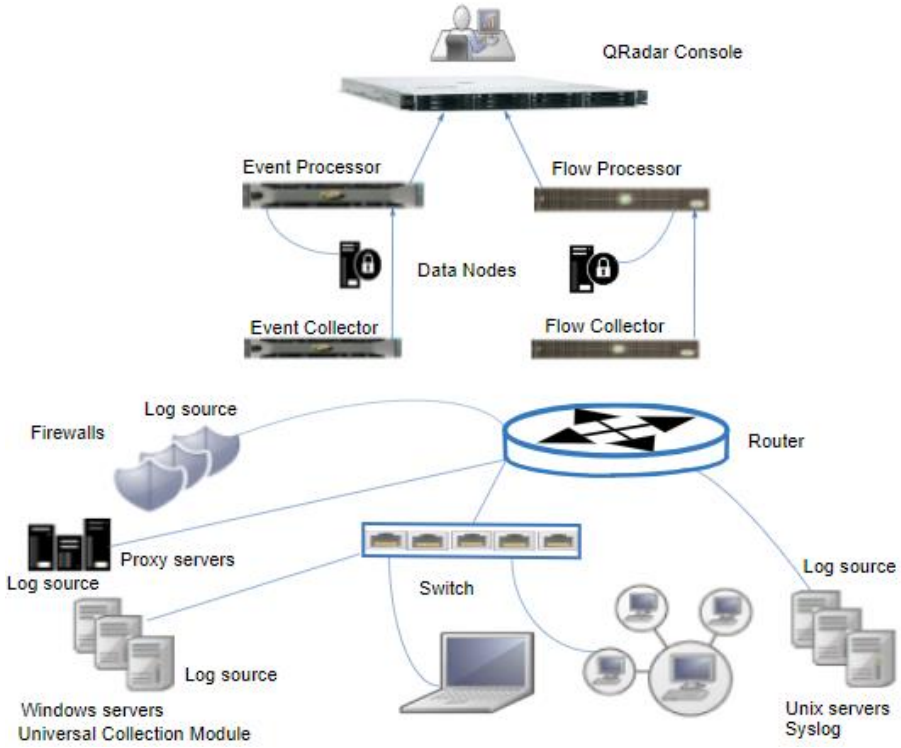


Рис.3.1. QRadar компоненти події та потоку

Розгортання All-in-one

У розгортанні QRadar на одному хості є універсальний пристрій QRadar, який є єдиним сервером, який збирає дані, наприклад журнали даних подій системного журналу та події Windows, а також дані потоку з вашої мережі.

Розширення розгортання для збільшення потужності

Компанія може створити або розширити розгортання за межі пристрою IBM QRadar All-in-One через брак можливостей обробки чи зберігання даних або якщо є особливі вимоги щодо збору даних.

Територіально розподілене розгортання

У територіально розподілених розгортаннях на розгортання IBM QRadar може вплинути переривчасте або погане підключення до віддалених центрів обробки даних. Також можуть вплинути місцеві нормативні акти, як-от дотримання певних нормативних актів країни щодо зберігання даних у місці походження. Обидві ці ситуації вимагають тримати збирачі даних на місці. Якщо необхідно зберігати дані в місці походження, то процесор повиен зберігатись на місці.

Розгортання QRadar Vulnerability Manager

Знаходити і керувати вразливими місцями у мережі можна розгорнувши IBM QRadar Vulnerability Manager. Підвищення безпеки мережі досягається за допомогою інтегрування додаткових функцій, таких як HCL BigFix і IBM Security SiteProtector.

Криміналістика та повний збір пакетів

Використання IBM QRadar Incident Forensics у розгортанні надасть змогу відстежити крок за кроком дії потенційного зловмисника та провести поглиблене криміналістичне розслідування ймовірних зловмисних інцидентів безпеки мережі.

Розгортання All-in-one

При розгортанні QRadar в єдиному хості є універсальний пристрій QRadar, який являється єдиним сервером, що збирає дані, такі як журнали даних подій системного журналу та події Windows, а також дані потоку з обраної мережі [29].

All-in-one пристрій підходить для компаній середнього розміру, які мають низький доступ до Інтернету, або для цілей тестування та оцінки. Розгортання з одним сервером підходить для компаній, які відстежують мережеву активність і події, такі як служби автентифікації та активність брандмауера.

All-in-one пристрій надає необхідні можливості, аж до певної ємності, яка визначається ліцензією та апаратними характеристиками системи. Наприклад, QRadar3105 (All-in-one) зазвичай обробляє до 5000 EPS (подій за секунду) і 200 000 FPM (потоків за хвилину), тоді як QRadar3128 (All-in-one) зазвичай обробляє до 15 000 EPS і 300 000 FPM.

До прикладу, розглянемо компанію, яка розгортає єдиний сервер QRadar. Візьмемо виробничу компанію середнього розміру з менш ніж 1000 співробітниками. Можна розгорнути QRadar3105 All-in-one пристрій для збору, обробки та моніторингу даних про події та потоки. З таким розгортанням є можливість збирати до 5000 подій на секунду (EPS) і 200 000 потоків на хвилину (FPM).

На наступній діаграмі показано All-in-one пристрій, який збирає дані з джерел подій і потоків, обробляє дані та надає веб-програму, де можна шукати, контролювати та реагувати на загрози безпеці.

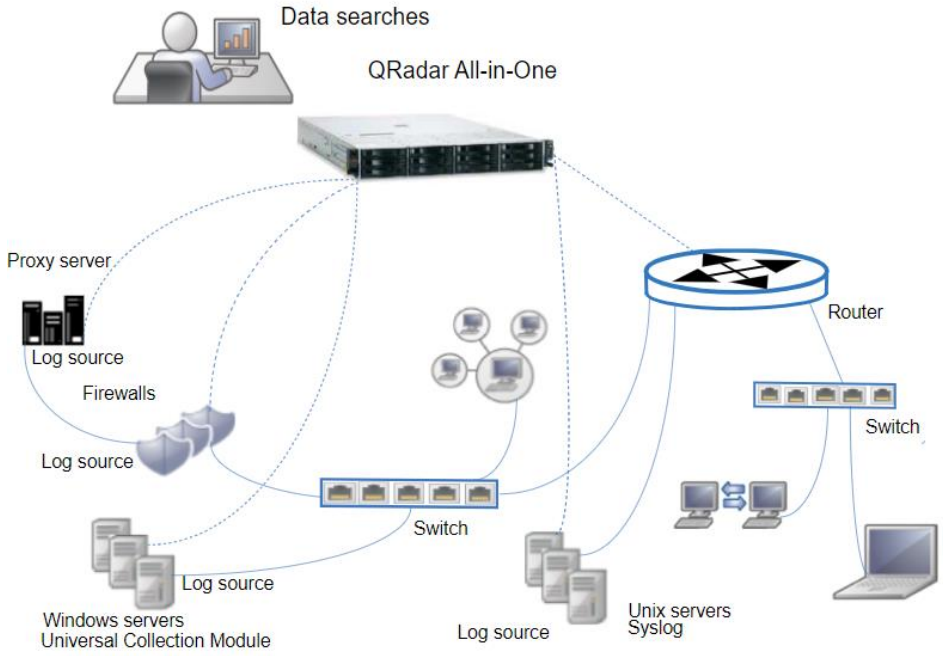


Рис. 3.2. Розгортання «All-in-one»

Пристрій The QRadar All-in-One виконує наступні завдання:

- Збирає дані про події та мережевий потік, а потім нормалізує дані у формат даних, який QRadar може використовувати.
- Аналізує та зберігає дані, а також визначає загрози безпеці компанії.
- Надає доступ до веб-додатку QRadar.

У міру того, як джерела даних компанії або потреби в обробці чи сховищі збільшаться, є можливість додавати пристрої для розширення розгортання.

Розширення розгортання для збільшення потужності

Якщо компанії недостатньо використання розгортання IBM QRadar All-in-one, є можливість створити або розширити розгортання за межами All-in-one пристрою. Розширення розгортання варто застосовувати через недостатню ємність для обробки чи зберігання даних або коли у компаніїї є особливі вимоги щодо збору даних.

Топологія і склад обраного розгортання QRadar впливають на здатність і спроможність цього розгортання збирати, обробляти та зберігати всі дані, які необхідно проаналізувати в обраній мережі.

Якщо потреби в обробці або сховищі виходять за межі можливостей обраного багатофункціонального пристрою, необхідно переналаштувати середовище QRadar для розподіленого розгортання.

Щоб отримати приблизну оцінку кількості подій за секунду (EPS) або потоків за хвилину (FPM), які потрібно обробити в обраному розгортанні, слід використовувати розмір журналів, зібраних із брандмауерів, проксі-серверів і систем Windows.

Причини додавання збирачів подій або потоків до розгортання All-in-One

Додавання збирачів потоків або подій до розгортання може знадобитись за таких умов:

- Ваші вимоги до збору даних перевищують можливості збору даних пристрою All-in-One.
- Ви повинні збирати події та потоки не в тому місці, де встановлено пристрій All-in-One.
- Ви відстежуєте більші або високошвидкісні пакетні джерела потоку, які є швидшими за з'єднання зі швидкістю 50 Мбіт/с на багатофункціональному пристрої.

Пристрій 3128 All-in-One може збирати до 15 000 подій за секунду (EPS) і 300 000 потоків за хвилину (FPM). Якщо вимоги до збирання є більшими, можна додати збирачі подій і збирачі потоків до свого розгортання. Наприклад, можна додати QRadar Flow Collector 1202, який збирає до 3 Гбіт/с.

Пристрій All-in-One обробляє зібрані події та потоки. Додавши збирачі подій і збирачі потоків, можна використовувати обробку, яку зазвичай виконує пристрій All-in-One для пошуку та інших завдань безпеки.

Джерела потоку на основі пакетів вимагають збирача потоку, підключеного або до процесора потоку, або до пристрою All-in-One в розгортаннях, де немає пристрою процесора потоку. Збирати зовнішні джерела потоку, такі як NetFlow або IPFIX, можна безпосередньо на пристрої Flow Processor або All-in-One.

Додавання віддалених колекторів до розгортання

Додавання елементів QRadar Event Collectors або QRadar Flow Collectors для розширення розгортання необхідно тоді, коли потрібно збирати більше подій локально, а також при потребі збирати події та потоки з віддаленого розташування.

Наприклад, є виробнича компанія, яка має QRadar Розгортання All-in-One, та потребує додавання електронної комерції та віддаленого офісу продажів. Тепер компанія повинна стежити за загрозами безпеки в цих зонах також.

Коли у компанії збільшується кількість співробітників, то і використання Інтернету змінюється з переважного завантаження на двосторонній трафік між співробітниками та Інтернетом. Візьмемо компанію з таким набором характеристик:

- Ліцензія на поточні події в секунду (EPS) становить 1000 EPS.
- Ви хочете збирати події та потоки в офісі продажів і події з платформи електронної комерції.
- Для збирання подій із платформи електронної комерції потрібно до 2000 подій за секунду (EPS).
- Для збирання подій із віддаленого офісу продажів потрібно до 2000 подій за секунду (EPS).
- Ліцензії на потоки за хвилину (FPM) достатньо для збору потоків у віддаленому офісі.

Тоді необхідно виконати наступні дії:

1. Додати платформу електронної комерції у головному офісі, а потім відкрити віддалений офіс продажів.
2. Встановити Event Collector і Flow Collector у віддаленому офісі продажів, який надсилає дані через Інтернет до пристрою All-in-One у головному офісі.
3. Оновити ліцензію EPS з 1000 EPS до 5000 EPS, щоб відповідати вимогам щодо додаткових подій, які збираються у віддаленому офісі.

На наступній діаграмі показано приклад розгортання, коли збирач подій і збирач потоків додаються у віддалений офіс.

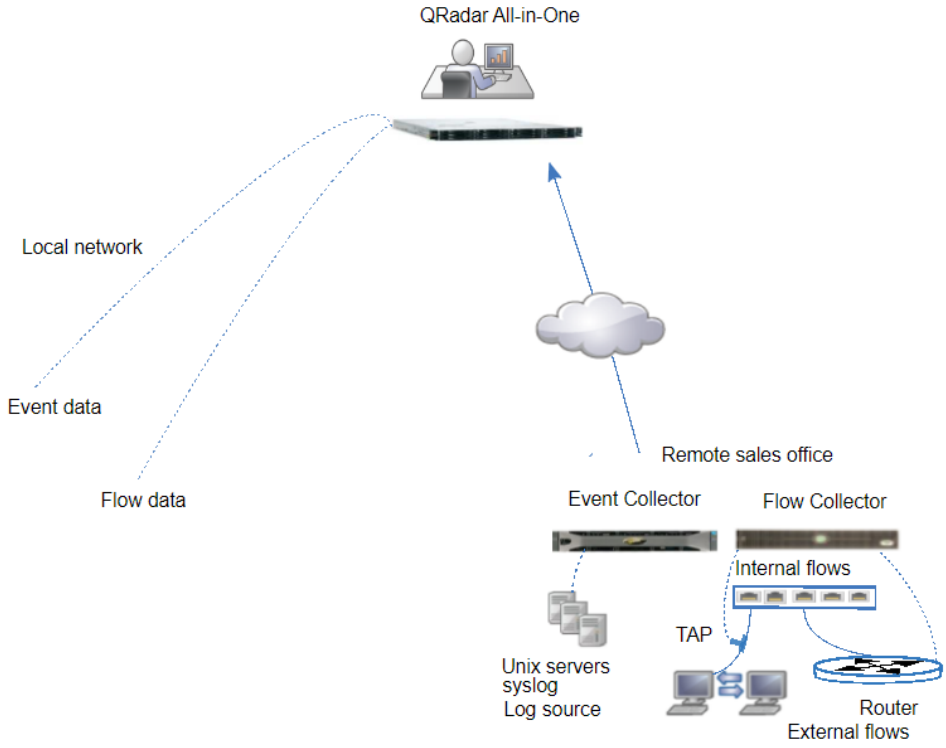


Рис. 3.3. Event Collector і Flow Collector у віддаленому офісі

У цьому розгортанні відбуваються такі процеси:

1. У віддаленому офісі Event Collector збирає дані з джерел журналів, а Flow Collector збирає дані з маршрутизаторів і комутаторів. Збирачі об’єднують і нормалізують дані.
2. Збирачі стискають і надсилають дані на пристрій All-in-One через глобальну мережу.
3. Пристрій All-in-One обробляє та зберігає дані.
4. Компанія відстежує мережеву активність за допомогою веб-додатку QRadar для пошуку, аналізу, звітування, а також для керування сповіщеннями та правопорушеннями.
5. All-in-one збирає та обробляє події з локальної мережі.

Додавання потужності обробки до розгортання All-in-One

Також можна додати Event Processors і Flow Processors до розгортання QRadar, щоб збільшити потужність обробки та збільшити обсяг пам’яті. Додавання

процесорів звільняє ресурси QRadar Console перемістивши навантаження обробки та зберігання на виділені сервери.

Якщо додати процесори подій або процесори потоку до пристрою All-in-One, то даний пристрій діє як QRadar Console. Потужність обробки на пристрої All-in-One призначена для керування та пошуку даних, які надсилають процесори, і дані тепер зберігаються на процесорах подій та інших пристроях зберігання даних, а не на консолі.

Зазвичай додавати процесори подій і процесори потоків до QRadar розгортання необхідно з таких причин:

- У міру того, як розгортання зростає, робоче навантаження перевищує потужність обробки багатофункціонального пристрою.
- У центрі безпеки працює більше аналітиків, які виконують більше одночасних пошуків.
- Типи відстежуваних даних і період зберігання цих даних збільшуються, що збільшує вимоги до обробки та зберігання.
- Оскільки команда аналітиків безпеки зростає, то потрібна краща продуктивність пошуку.

При масштабуванні QRadar розгортання понад 15 000 EPS і 300 000 FPM на найпотужнішому пристрої All-in-One, необхіднододати процесорні пристрої для обробки цих даних.

На наведеній нижче діаграмі потужність обробки додається, коли процесор подій і процесор потоку додаються до QRadar 3128 (All-in-One) і відбуваються такі зміни:

- Обробку подій і потоків перенесено з пристрою All-in-One до процесорів подій і потоків.
- Потужність обробки подій збільшується до 40 000 EPS, включаючи 15 000 EPS, які були на моноблоці.
- Потужність обробки потоку збільшується до 1 200 000 футів за хвилину, включаючи 300 000 футів за хвилину, які були на багатофункціональному пристрої.

- Дані, які надсилаються збирачами подій і потоків, обробляються та зберігаються в процесорах подій і потоків.

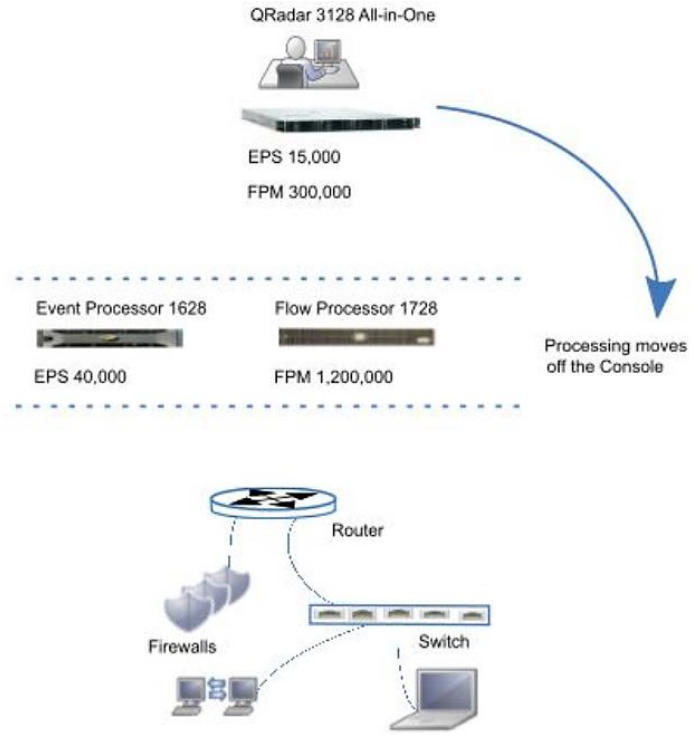


Рис. 3.4. Додавання потужності обробки даних

У територіально розподілених розгортаннях IBM QRadar на розгортання може вплинути переривчасте або погане підключення до віддалених центрів обробки даних. Також можуть вплинути місцеві нормативні акти, як-от дотримання певних нормативних актів країни щодо зберігання даних у місці походження. Обидві ці ситуації вимагають, щоб збирачі зберігались на місці. Якщо необхідно зберігати дані в місці походження, то треба зберігати процесор на тому ж місці.

Наприклад, компанія розвивається, і це зростання не тільки збільшує активність у мережі, але також вимагає розширення QRadar розгортання в інших країнах. Закони про збереження даних відрізняються у рвзних країнах, тому QRadar розгортання необхідно планувати з урахуванням цих правил. Тож, якщо компанія повинна збирати дані про події в одному з офісів, де є переривчасте з’єднання, то необхідно дотримуватися правил зберігання даних у країнах, де дані

збираються. Наприклад, якщо Німеччина вимагає, щоб дані залишалися в країні, то ці дані не повинні зберігатися за межами цієї країни.

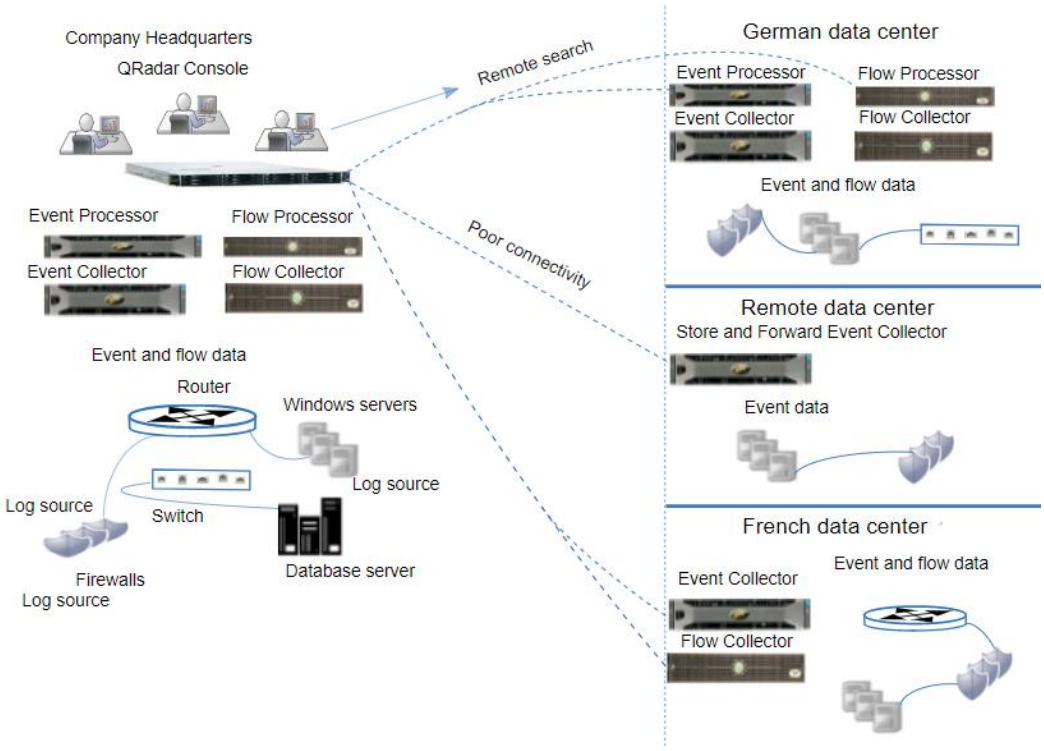


Рис. 3.5. Територіально розподілене розгортання

Розглянемо, які процеси відбуваються в територіально розподіленому розгортанні. Наприклад, компанія встановлює збирачі та процесори в німецькому центрі обробки даних, щоб відповідати місцевому законодавству щодо даних. Тоді у французькому дата-центрі ця ж компанія встановлює збирачі, щоб дані надсилалися збирачам до головного офісу, котрі б оброблялися та зберігалися в головному офісі. Швидкість пошуку збільшується завдяки тому, що процесорні пристрої знаходяться в тому самому високошвидкісному сегменті мережі, що й QRadar Console. Компанія додає збирач подій для зберігання та пересилання, який має заплановані та обмежені за швидкістю підключення до віддаленого центру обробки даних. З'єднання за розкладом і з обмеженою швидкістю компенсують переривчасте з'єднання з мережею та гарантують уникнення потреби у більшій пропускній здатності протягом звичайних робочих годин.

За допомогою розгортання IBM QRadar Vulnerability Manager можна знайти уразливі місця у мережі й усунути їх. Підвищення безпеки мережі можливе за

рахунок інтегрування таких додаткових функцій, як HCL BigFix iIBM Security Site Protector.

IBM QRadar Vulnerability Manager виявляє вразливості на мережевих пристроях, програмах і програмному забезпеченні, додає контекст до вразливостей, визначає пріоритет ризику активів у мережі та підтримує виправлення виявлених уразливостей.

3.2. Розроблення рекомендацій щодо застосування технології управління безпекою інформаційних систем

Політика безпеки для працівників компанії

При роботі з інформаційними ресурсами компанії кожен ***співробітник повинен***:

- за своїми навичками та спеціальними завданнями забезпечувати інформаційну безпеку ІТС підприємства, забезпечувати захист від несанкціонованого доступу до інформації системи, до якої надано доступ за виконанням службових обов'язків;
- жодним чином не брати участь у процесах несанкціонованого доступу до інформації інших співробітників та підрозділів;
- не використовувати в будь-якій формі дані, які стали йому відомі в результаті виконання своїх функціональних обов'язків, інформацію не за призначенням;
- у разі порушення встановлених правил доступу іншими працівниками повідомляти про це безпосереднього керівника, відповідальних за ІТС підприємства адміністраторів або службу безпеки установи.

Ремонтні та профілактичні роботи повинні проводитися тільки уповноваженими особами експлуатаційної служби за погодженням з керівником підприємства, де встановлено комп'ютерну техніку. Порядок зняття, перенесення та зміни конфігурації апаратури визначено регламентом проведення таких робіт та виконується лише уповноваженими особами експлуатаційної служби.

Під час роботи в автоматизованій інформаційній системі підприємства працівники повинні:

1. Тримати в таємниці паролі доступу до компанії.

2. Безпечно зберігати фізичні ключі доступу (ідентифікатори).

3. Час від часу змінювати персональні паролі, якщо це передбачено законодавством для управління доступом до корпоративних ІТС.

4. У разі випадкового доступу (відсутність механізмів захисту, нещасні випадки, недбалість персоналу) до конфіденційної інформації інших осіб припинити всі дії в системі та негайно повідомити службу безпеки та системного адміністратора ІТС підприємства.

5. Повідомити службу безпеки підприємства та системного адміністратора про відомі канали виходу, способи та засоби обходу або знищення механізмів захисту.

Під час роботи в автоматизованій інформаційній системі підприємства ***працівникам забороняється*** (крім спеціально передбачених випадків):

- записувати або вимовляти вголос відомі користувачеві паролі в будь-якій доступній формі;
- реєстрація та робота в системі з чужим ID та паролем;
- надавати ідентифікатори та паролі третім особам;
- залишати робоче місце без нагляду під час роботи;
- дозволяти іншим людям виконувати будь-які дії з будь-якими програмними та апаратними засобами, не призначеними для них;
- несанкціонована зміна або знищення даних або програм в мережі або на зовнішніх носіях (відчужених);
- залишати носії критичної інформації ІТС підприємства немаркованими;
- використовувати ІТ-системи в неробочий час не за призначенням;
- проводити дослідження в комп'ютерних мережах;
- ігнорувати системні повідомлення та повідомлення про помилки;

- несанкціоноване встановлення на автоматизованих робочих місцях додаткових програмно-технічних компонентів і пристроїв;
- копіювати програмне забезпечення та файли даних на знімні носії;
- використовувати не передбачені засоби та канали зв'язку для передачі інформації з обмеженим доступом.

Політика безпеки для підприємства

Реалізація організаційних заходів на підприємстві не вимагає великих фінансових витрат, але їх ефективність підтверджена життям і часто недооцінена потенційними жертвами. Відзначимо одну їхню особливість щодо технічних засобів: організаційні заходи ніколи не стають провокуючим фактором агресії.

Вони застосовуються для протистояння зі зловмисником. Виходячи з досвіду багатьох організацій у сфері проектування СЗІ, зазначимо, що організаційні дії включають створення концепції інформаційної безпеки як складової частини функціонування автоматизованої системи комплексного захисту інформації підприємства, а також наступні:

1. Створення робочих інструкцій для користувачів і персоналу.
2. Створення правил управління компонентами інформаційної системи, обліку, архівування, тиражування, знищення носіїв інформації, ідентифікації користувачів.
3. Розроблення планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи підприємства, виходу з ладу засобів захисту, виникнення аварійної ситуації.
4. Навчання користувачам правилам комп'ютерної безпеки.

Дотримання основних принципів і простих правил дозволить уникнути втрати інформації, а також можливих матеріальних, моральних і фінансових втрат.

При необхідності в рамках організаційних заходів можуть бути створені служба інформаційної безпеки підприємства, режимно-пропускний відділ, реорганізація системи обліку та зберігання документів.

Під час впровадження SIEM необхідно дотримуватись наступних передових практик.

Ставити зрозумілі цілі. Інструмент SIEM слід вибирати та впроваджувати на основі цілей безпеки, відповідності та потенційних загроз організації.

Застосовувати правила кореляції даних. Правила кореляції даних повинні бути реалізовані в усіх системах, мережах і хмарних розгортаннях, щоб дані з помилками можна було легше знайти.

Визначати вимоги відповідності. Це допомагає переконатися, що вибране програмне забезпечення SIEM налаштовано на перевірку та звітування щодо правильних стандартів відповідності.

Список цифрових активів. Перелік усіх цифрових даних, що зберігаються в IT-інфраструктурі, допомагає керувати даними журналу та відстежувати мережеву активність.

Записувати плани реагування на інциденти та робочі процеси. Це допомагає командам швидко реагувати на інциденти безпеки.

Призначити адміністратора SIEM. Адміністратор SIEM забезпечує належне обслуговування реалізації SIEM.

ВИСНОВКИ

Підсумовуючи загальний зміст роботи, можемо зробити наступні висновки:

1. Для оптимізації процесів виробничої діяльності такі структури намагаються підвищувати ефективність власної КСЗІ, в тому числі за допомогою різноманітних платформ інтернет-моніторингу вразливостей та сторонніх загроз. Результатом таких процесів стане покращення продуктивності діяльності підприємства в цілому, а також сприятиме зменшенню ризиків проникнення сторонніх даних і витоків конфіденційної інформації, на захист якої йде багато часу і грошей. З іншої сторони, для керування корпоративною мережею передачі даних конче важливим є здатність отримати достовірні дані відносно стану ПЗ та технічного стану обладнання, що підтримується софтом. Саме ці вище окреслені питання вирішуються за допомогою реалізації електронної системи інтернет-моніторингуна підприємстві

2. Інформаційна безпека являє собою практичний захист інформації за рахунок зниження інформаційних ризиків. Інформаційна безпека також є частиною керування інформаційними ризиками. Як правило, це вбирає в себе запобігання або зменшення ймовірності несанкціонованого отримання інформації чи незаконного її розповсюдження чи пошкодження, зміни, перекручування фактів. Сюди також можна віднести дії, які направлені на суттєве зниження негативних наслідків від даних дій. Захищені дані можуть сприймати будь-яку форму (електронну чи фізичну), також матеріальну (на папері) чи нематеріальну (у вигляді знань).

3. Безпека інформації та інформаційних ресурсів з використанням телекомунікаційної системи або пристроїв означає захист інформації, інформаційних систем або книг від несанкціонованого доступу, пошкодження, крадіжки або знищення. При цьому комп’ютерна безпека, кібербезпека або безпека ІІТ (ІТ-безпека) - це захист комп’ютерних систем і мереж від крадіжки або пошкодження їх обладнання, програмного забезпечення або електронних даних, а також від порушення або неправильного напряму послуг, які вони надають. Сфера інформаційної безпеки стає все більш важливою через все більшу залежність від

комп’ютерних систем, Інтернету і стандартів бездротової мережі, такої як блютуз та вай-фай, а також через зростання «розумних» пристроїв, включаючи смартфони, телевізори та інші пристрою, що становлять «Інтернет речей». Через свою складність, як з політичної, так і з технологічної точки зору, кібербезпека є однією з основних проблем в сучасному світі.

4. Наразі захист інформації та поняття кібербезпеки трансформувалося на одне із засадничих задач високотехнологічного соціуму. Через широке впровадження ШІ в усіх сферах своєї життєдіяльності суспільство стало вкрай вразливим відносно різних кібератак, які все активніше стають ефективним інструментом несилових способів контролінгу та управління як відносно об’єктів критичної інфраструктури держави, закладу, так і індивідумами. З однієї сторони, кібербезпека –це питання захисту від наявних та потенційних уразливостей інформаційного впливу, яке проектує небезпечні явища для різних інфоструктур, програмних і апаратних механізмів, а також моральних засад соціуму. З іншої сторони, кібербезпека –це систему механізмів, що спрямовуються на захист комп’ютерів, цифрових ресурсів та мережі їх передачі від несанкціонованого проникнення та інших дій, які зв’язан безпосередньо з маніпуляцій ними механізмами чи крадіжкою, блокуванням чи поломкою, знищенням інформації або ж певних даних.

5. Основними цілями КСЗІ є:

– захист законних інтересів підприємства від протиправних дій;

– не допустити розкрадання фінансових та матеріально-технічних засобів;

– захистити від розголошення, витоку та несанкціонованого доступу до службової інформації;

– не допустити порушення роботи технічних засобів забезпечення виробничої діяльності, включаючи інформаційні технології.

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства загалом. КСЗІ є універсальним підходом щодо встановлення безпеки та основною концепцією для безпеки інфраструктури підприємства загалом. Необхідність побудови КСІ визначається вимогами

нормативних документів у сфері технічного та криптографічного захисту інформації або бажанням власника інформаційних ресурсів.

Автоматизовані системи на підприємстві наразі демонструють потенційно смертельні уразливості. Є багато повідомлень про зломи організацій, включаючи атаки шкідливих програм, експлойтів WindowsXP, вірусів і витоку конфіденційних даних, що зберігаються на серверах компаній.

Використання розглянутого комплексного програмного рішення IBM QRadar забезпечить комплексний захист у комп'ютерних мережах будь-якої складності. Програмне рішення дає змогу відслідковувати та аналізувати виникнення загроз, попереджувати їх виникнення, а також надавати адміністраторам повну інформацію про вузли, виконання процесів та передавання пакетів у мережі.

Комплексне програмне рішення IBM QRadar повністю інтегрується в інфраструктуру підприємства, що забезпечує швидкий та надійний моніторинг корпоративної безпеки, а також масштабується з її розвитком, застосовуючи досвід взаємодії з конкретними користувачами до груп користувачів усієї організації. Можливість всебічного перегляду та аналізу інформації підвищує ефективність обслуговування комп'ютерної мережі в декілька разів.

Основними перевагами застосування IBM QRadar є: підвищення рівня захищеності інформаційної інфраструктури внаслідок оперативного реагування на інциденти інформаційної безпеки; прискорення і автоматизація процесу ідентифікації, а також подальше дослідження інцидентів; централізований підхід до задач обробки та зберігання подій інформаційної безпеки.

Отож, проблема інформаційної безпеки є дійсно важливою та потребує постійного пошуку нових рішень захисту, адже світ змінюється, і кіберзлочинці відповідно вдосконалюють способи вчинення атак. Оскільки вірогідність того, що загрози у кіберпросторі можуть повністю припинитись, є мінімальною, то основна задача – вміти приймати запобіжні заходи: правильно створювати, впроваджувати та контролювати систему, яка допомагає керувати інформаційною безпекою.

Проаналізувавши ситуацію в інформаційному просторі, яка склалась на даний час, можна зробити висновки, що забезпечення захисту інформації на

сучасних підприємствах є однією з ключових тенденцій, яка потребує постійне проведення нових досліджень та знаходження дієвих та ефективних засобів та мір захисту, та вдосконалення тих методів, що вже використовуються.

Розроблено варінати впровадження комплексної системи захисту інформації на базі IBM QRadar SIEM та розроблено методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних програм.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Антонюк В. С. Методологія наукових досліджень: [Текст]: навч. пос./ В.С. Антонюк, Л. Г. Полонський, В. І. Аверченков, Ю. О. Малахов. – К.: НТУУ «КПІ», 2015. – 286 с.

2. Бабак В. П. Інформаційна безпека і сучасні мережеві технології: Англо-українсько-рос. словник термінів / В. П. Бабак, О. Г. Корченко. – Київ: Вид.-во НАУ, 2003. – С. 230-255.

3. Букет Д. А. Управління інформаційною безпекою за допомогою комплексної системи захисту / Державний ун-т телекомунікацій / Сучасний захист інформації №1 (49), Київ. – 2022р. – 5с.

4. Бурячок В. Л., Толюпа С. В., Аносов О. О., Козачок В. О., Лукова-Чуйко Н.В. Системний аналіз і прийняття рішень в інформаційній безпеці: підручник. / В. Л. Бурячок,С. В. Толюпа, О. О. Аносов, В. А. Козачок, Н. В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

5. Бурячок В. Л. Інформаційний і кіберпростір: проблеми безпеки, методи і способи боротьби. [Учебник]. / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ООО «СІК ГРУПУКРАЇНА», 2015. – 449 с.

6. Богуш В. М., Кудін А. М. Інформаційна безпека від А до Я: 3000 термінів і визначень. - К.: МОУ, 1999. - 456 с.

7. Бугайський К. Проблеми побудови систем інформаційної безпеки. – 2008. – №2. – С. 5-9.

8. Глушков В. М., Амосов М. М., Артеменко І. А. Енциклопедія кібернетики. Том 2. Київ, - 1974. – С. 33-54.

9. Зегжда Д. П., Ивашко А. М. Основи безпеки інформаційних систем. - М.: Гаряча лінія - Телеком, 2000. - С.26-120.

10. Ізмалкова С. А., Тарасов А. В. Принципи побудови ефективної системи інформаційної безпеки // Управління суспільними та економічними системами. – 2006. – № 2. – С. 3-12.

11. Інтернет-ресурс. – Режим доступу: -https://www.cisco.com/c/ru_ua/ products/cloud-systems-management/dnacenter/index. html.

12. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.

13. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К.: ДУТ, 2015. - 288 с.

14. Конохович Г.Ф. Захист інформації в телекомунікаційних системах. – МК Прес Київ 2005. – 288 с.

15. Комашинський В. І. Смирнов Д. А. Введення до нейро-информаційних технологій. / В. І. Комашинський, Д. А. Смирнов - СПб, 1999. – С. 33-48.

16. Липунцов Ю. П. Управління процесами. М: Компанія АйТі, 2003. – С. 33-42.

17. Лотов О. В., Поспелова І. І. Багатокритеріальні задачі прийняття рішень: навч. посібник. М.: МАКС Прес, 2008. – С. 77 - 89.

18. Малюк О. А., Пазізін С. В., Погожин М. С. Введення в захист інформації в автоматизованих системах. – М.: Гаряча лінія-Телеком, 2001. – 148 с.

19. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія / А. Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

20. Нечаєв М. Правові та организаційні основи комплексних систем захисту інформації // Корпоративні системи. – 2008. – №2. – С.54-57.

21. Скулиш Є. Д. Засоби аналізу та оцінка ризиків інформаційної безпеки / Є. Д. Скулиш, О. Г. Корченко, Ю. І. Горбенко, С. В. Казмирчук // Інформаційна безпека. Людина, суспільство, держава – 2011. – №3 (7). – С. 31-48.

22. Типове положення про службу захисту інформації в автоматизованій системі [Текст]: НД ТЗІ 1.4-001. - 2000. - Чин. 2000.12.04. - К.: ДСТСЗІ СБ України, 2000. - С. 4-30.

23. Уосермен Ф. Нейрокомп'ютерна техніка: Теорія і практика. Переклад І. Ю. Юрчак, 2001. – С. 88-94.

24. Уфімцев Ю. С. Методика інформаційної безпеки / Уфімцев Ю. С., Буянов В. П., Ерофеев Е. А. та ін. – М.: Вид-во «Екзамен», 2004. – 544с.

25. Чипига, О. Ф. Інформаційна безпека автоматизованих систем / О. Ф. Чипига. - М.: Геліос АРВ, 2017. - С. 144-167.

26. Черноруцький І. Г. Методи прийняття рішень [Текст] / І. Г. Черноруцький. – СПб.: БХВ-Спб, 2005. – С. 388-395.

27. Шаньгін В. Ф. Інформаційна безпека комп’ютерних систем і мереж: Навч. посіб. / В.Ф. Шаньгін. – М.: Форум, 2018. – С. 67-88.

28. Фаро С., Лермі П. Рефакторвнг SQLite-застосунків/ С. Фаро, П. Лермі – Символ-Плюс, 2006. – 180 с.

29. IBM QRadar SIEM. [Електронний ресурс] – Режим доступа: https: // www.ibm.com/products/qradar-siem

30. ER: діаграми сутність – зв'язок. // [Електронний ресурс]. - Режим доступу: http: // dl.sumdu.edu.ua/e-pub/db/278409/ER_Modeling.pdf.

31. Moghaddam B. and Pentland A. «Probabilistic Visual Reconition for Object Recognition», Trans. IEEE Pattern Analysis and Machine Intelligence, July 1997. – P. 696–710.

32. Carson Zimmerman. «Ten Strategies of a World-Class Cybersecurity Operations Center», January, 2014.

ДОДАТКИ

2

Об'єкт дослідження – управління безпекою інформаційно-телекомунікаційній системі підприємства.

Предмет дослідження – технологія управління безпекою організації та їх захисту на прикладі IBM QRadar SIEM

Мета роботи – аналіз особливостей розробки та практичної реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM.

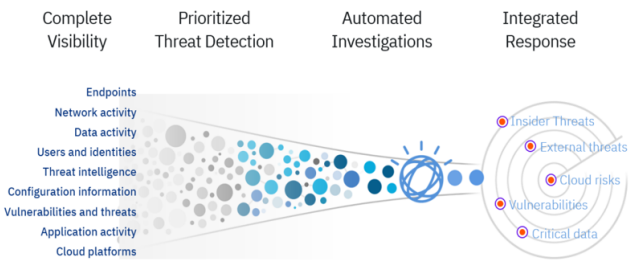
Наукові завдання:

- проаналізувати теоретичні засади системи захисту інформації та визначити її складові;
- охарактеризувати принципи роботи SIEM систем;
- розглянути існуючі моделі захисту ІТС;
- проаналізувати методи та засоби управління безпекою інформаційних систем на базі IBM QRadar SIEM;
- розроблення варіантів розгортання QRadar;
- розроблення рекомендацій щодо застосування технології управління безпекою інформаційних систем.

Призначення, можливості та функції IBM QRadar SIEM

3

IBM Security QRadar, провідне на ринку рішення SIEM, допомагає захиститися від зростаючих загроз, модернізуючи та масштабуючи операції безпеки за допомогою інтегрованої видимості, виявлення, дослідження та реагування. QRadar надає командам із безпеки централізовану видимість даних про безпеку в масштабах підприємства та практичну інформацію щодо найпріоритетніших загроз. Аналітики безпеки можуть працювати з однієї панелі, щоб швидко зрозуміти механізми своєї безпеки, виявити найбільш критичні загрози та детальніше розібратися, щоб спростити робочі процеси та позбутися необхідності переходити між інструментами.



Завдяки можливостям виявлення аномалій QRadar служби безпеки можуть швидко ідентифікувати зміни в поведінці користувачів, які можуть вказувати на невідому загрозу.

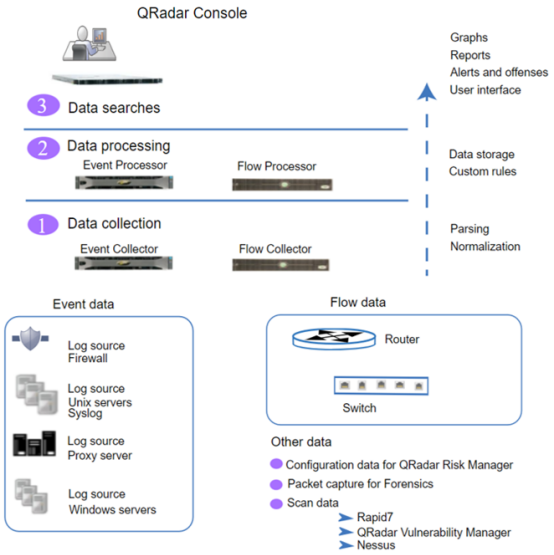
QRadar дає змогу організаціям отримати централізовану повну видимість ізольованих середовищ шляхом збору, аналізу та нормалізації даних журналів і потоків. З однієї панелі аналітики безпеки можуть контролювати локальні, хмарні та гібридні середовища. Клієнти можуть просто направляти журнали на QRadar, і рішення може автоматично визначати тип джерела журналу та застосовувати правильний DSM для аналізу та нормалізації даних журналу. У результаті клієнти QRadar можуть налагодити роботу набагато швидше, ніж клієнти альтернативних рішень. Додаткові інтеграції можна легко додати через програми в IBM Security App Exchange.

Компоненти та архітектура рішення IBM QRadar SIEM

4

IBM QRadar SIEM — це модульна архітектура, яка забезпечує видимість IT-інфраструктури в режимі реального часу, яку можна використовувати для виявлення загроз і встановлення пріоритетів. Систему QRadar можна масштабувати для задоволення потреби в зборі журналів і потоків і аналізі. Є можливість додати інтегровані модулі до платформи QRadar, наприклад QRadar Risk Manager, QRadar Vulnerability Manager і QRadar Incident Forensics.

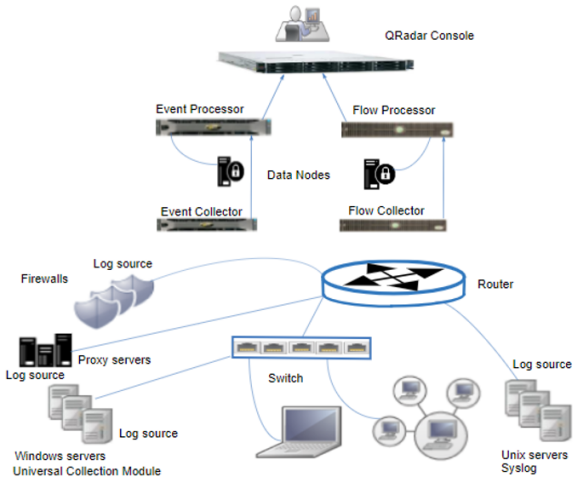
Робота платформи безпеки QRadar складається з трьох рівнів і застосовується до будь-якої структури розгортання QRadar, незалежно від її розміру та складності. На наступній діаграмі показано рівні, які складають архітектуру Qradar.
Архітектура QRadar функціонує однаково незалежно від розміру чи кількості компонентів у розгортанні. Наступні три рівні, представлені на схемі, представляють основні функції будь-якої системи QRadar.



Розробленя варіанта розгортання QRadar та рекомендації щодо впровадження

5

Архітектура IBM QRadar підтримує розгортання різних розмірів і топологій, від розгортання на одному хості, де всі програмні компоненти працюють в одній системі, до кількох хостів, де такі пристрої, як збирачі подій і збирачі потоків, Data Nodes, хост додатків, процесори подій і процесори потоків мають певні ролі

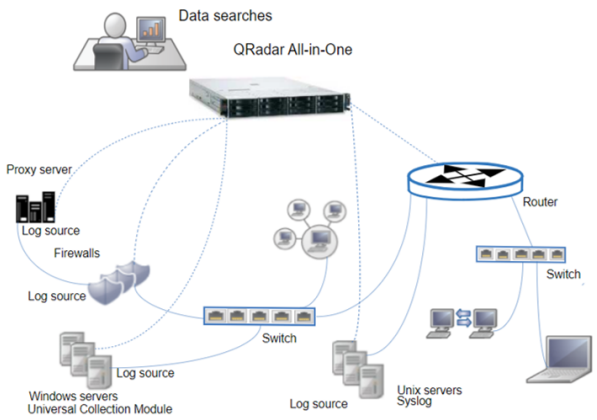


Microsoft Endpoint Manager допомагає організаціям використовувати переваги хмарних засобів, зокрема розгортати всі програми, захищати й контролювати їх, а також кінцеві пристрої та користувачів і забезпечувати безперебійну реалізацію поточних процесів.
Забезпечує безпеку в хмарі на кінцевих точках. Захист пристроїв користувачів від загроз здійснюється завдяки унікальним можливостям моделі нульової довіри Microsoft.

Розгортання IBM QRadar All-in-one

6

При розгортанні QRadar в єдиному хості є універсальний пристрій QRadar, який являється єдиним сервером, що збирає дані, такі як журнали даних подій системного журналу та події Windows, а також дані потоку з обраної мережі.

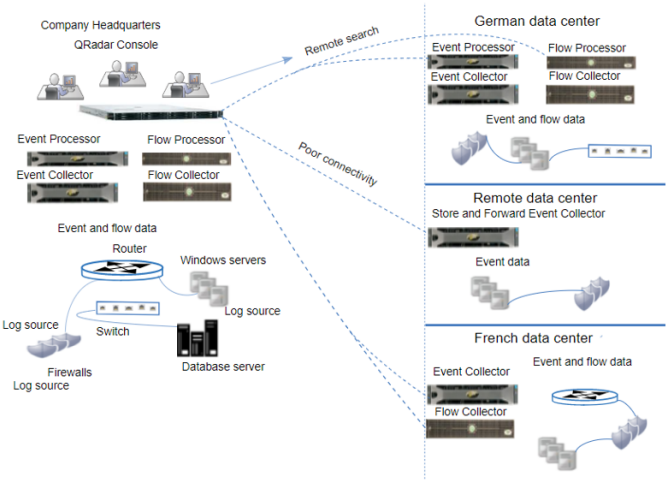


All-in-one пристрій підходить для компаній середнього розміру, які мають низький доступ до Інтернету, або для цілей тестування та оцінки. Розгортання з одним сервером підходить для компаній, які відстежують мережеву активність і події, такі як служби автентифікації та активність брандмауера. All-in-one пристрій надає необхідні можливості, аж до певної ємності, яка визначається ліцензією та апаратними характеристиками системи. Наприклад, QRadar3105 (All-in-one) зазвичай обробляє до 5000 EPS (подій за секунду) і 200 000 FPM (потоків за хвилину), тоді як QRadar3128 (All-in-one) зазвичай обробляє до 15 000 EPS і 300 000 FPM.

Розширення розгортання IBM QRadar та територіально розподілене розгортання

7

У територіально розподілених розгортаннях IBM QRadar на розгортання може вплинути переривчасте або погане підключення до віддалених центрів обробки даних. Також можуть вплинути місцеві нормативні акти, як-от дотримання певних нормативних актів країни щодо зберігання даних у місці походження. Обидві ці ситуації вимагають, щоб збирачі зберігались на місці. Якщо необхідно зберігати дані в місці походження, то треба зберігати процесор на тому ж місці.



Наприклад, компанія розвивається, і це зростання не тільки збільшує активність у мережі, але також вимагає розширення QRadar розгортання в інших країнах. Закони про збереження даних відрізняються у рвзних країнах, тому QRadar розгортання необхідно планувати з урахуванням цих правил. Тож, якщо компанія повинна збирати дані про події в одному з офісів, де є переривчасте з'єднання, то необхідно дотримуватися правил зберігання даних у країнах, де дані збираються.

Рекомендації щодо управління коритувачами корпоративної інформаційної системи

8

Політика безпеки для працівників компанії

При роботі з інформаційними ресурсами компанії кожен ***співробітник повинен***:

- за своїми навичками та спеціальними завданнями забезпечувати інформаційну безпеку ІТС підприємства, забезпечувати захист від несанкціонованого доступу до інформації системи, до якої надано доступ за виконанням службових обов'язків;
- жодним чином не брати участь у процесах несанкціонованого доступу до інформації інших співробітників та підрозділів;
- не використовувати в будь-якій формі дані, які стали йому відомі в результаті виконання своїх функціональних обов'язків, інформацію не за призначенням;
- у разі порушення встановлених правил доступу іншими працівниками повідомляти про це безпосереднього керівника, відповідальних за ІТС підприємства адміністраторів або службу безпеки установи.

Ремонтні та профілактичні роботи повинні проводитися тільки уповноваженими особами експлуатаційної служби за погодженням з керівником підприємства, де встановлено комп'ютерну техніку. Порядок зняття, перенесення та зміни конфігурації апаратури визначено регламентом проведення таких робіт та виконується лише уповноваженими особами експлуатаційної служби.

Під час роботи в автоматизованій інформаційній системі підприємства працівники повинні:

1. Тримати в таємниці паролі доступу до компанії.
2. Безпечно зберігати фізичні ключі доступу (ідентифікатори).
3. Час від часу змінювати персональні паролі, якщо це передбачено законодавством для управління доступом до корпоративних ІТС.
4. У разі випадкового доступу (відсутність механізмів захисту, нещасні випадки, недбалість персоналу) до конфіденційної інформації інших осіб припинити всі дії в системі та негайно повідомити службу безпеки та системного адміністратора ІТС підприємства.
5. Повідомити службу безпеки підприємства та системного адміністратора про відомі канали виходу, способи та засоби обходу або знищення механізмів захисту.

Рекомендації щодо управління коритувачами корпоративної інформаційної системи

9

Під час роботи в автоматизованій інформаційній системі підприємства ***працівникам забороняється*** (крім спеціально передбачених випадків):

- записувати або вимовляти вголос відомі користувачеві паролі в будь-якій доступній формі;
- реєстрація та робота в системі з чужим ID та паролем;
- надавати ідентифікатори та паролі третім особам;
- залишати робоче місце без нагляду під час роботи;
- дозволяти іншим людям виконувати будь-які дії з будь-якими програмними та апаратними засобами, не призначеними для них;
- несанкціонована зміна або знищення даних або програм в мережі або на зовнішніх носіях (відчужених);
- залишати носії критичної інформації ІТС підприємства немаркованими;
- використовувати ІТ-системи в неробочий час не за призначенням;
- проводити дослідження в комп'ютерних мережах;
- ігнорувати системні повідомлення та повідомлення про помилки;
- несанкціоноване встановлення на автоматизованих робочих місцях додаткових програмно-технічних компонентів і пристроїв;
- копіювати програмне забезпечення та файли даних на знімні носії;
- використовувати не передбачені засоби та канали зв'язку для передачі інформації з обмеженим доступом.

Рекомендації щодо управління коритувачами корпоративної інформаційної системи

10

Політика безпеки для підприємства

Реалізація організаційних заходів на підприємстві не вимагає великих фінансових витрат, але їх ефективність підтверджена життям і часто недооцінена потенційними жертвами. Відзначимо одну їхню особливість щодо технічних засобів: організаційні заходи ніколи не стають провокуючим фактором агресії.

Вони застосовуються для протистояння зі зловмисником. Виходячи з досвіду багатьох організацій у сфері проектування СЗІ, зазначимо, що організаційні дії включають створення концепції інформаційної безпеки як складової частини функціонування автоматизованої системи комплексного захисту інформації підприємства, а також наступні:

1. Створення робочих інструкцій для користувачів і персоналу.
2. Створення правил управління компонентами інформаційної системи, обліку, архівування, тиражування, знищення носіїв інформації, ідентифікації користувачів.
3. Розроблення планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи підприємства, виходу з ладу засобів захисту, виникнення аварійної ситуації.
4. Навчання користувачам правилам комп'ютерної безпеки.

Дотримання основних принципів і простих правил дозволить уникнути втрати інформації, а також можливих матеріальних, моральних і фінансових втрат.

При необхідності в рамках організаційних заходів можуть бути створені служба інформаційної безпеки підприємства, режимно-пропускний відділ, реорганізація системи обліку та зберігання документів.

Рекомендації щодо управління коритувачами корпоративної інформаційної системи

11

Під час впровадження SIEM необхідно дотримуватись наступних передових практик.

Ставити зрозумілі цілі. Інструмент SIEM слід вибирати та впроваджувати на основі цілей безпеки, відповідності та потенційних загроз організації.

Застосовувати правила кореляції даних. Правила кореляції даних повинні бути реалізовані в усіх системах, мережах і хмарних розгортаннях, щоб дані з помилками можна було легше знайти.

Визначати вимоги відповідності. Це допомагає переконатися, що вибране програмне забезпечення SIEM налаштовано на перевірку та звітування щодо правильних стандартів відповідності.

Список цифрових активів. Перелік усіх цифрових даних, що зберігаються в IT-інфраструктурі, допомагає керувати даними журналу та відстежувати мережеву активність.

Записувати плани реагування на інциденти та робочі процеси. Це допомагає командам швидко реагувати на інциденти безпеки.

Призначити адміністратора SIEM. Адміністратор SIEM забезпечує належне обслуговування реалізації SIEM.

ВИСНОВКИ

12

Підсумовуючи загальний зміст роботи, можемо зробити наступні висновки:

1. Для оптимізації процесів виробничої діяльності такі структури намагаються підвищувати ефективність власної КСЗІ, в тому числі за допомогою різноманітних платформ інтернет-моніторингу вразливостей та сторонніх загроз.
2. Інформаційна безпека являє собою практичний захист інформації за рахунок зниження інформаційних ризиків. Інформаційна безпека також є частиною керування інформаційними ризиками.
3. Безпека інформації та інформаційних ресурсів з використанням телекомунікаційної системи або пристроїв означає захист інформації, інформаційних систем або книг від несанкціонованого доступу, пошкодження, крадіжки або знищення.
4. Основними цілями КСЗІ є:
   - захист законних інтересів підприємства від протиправних дій;
   - не допустити розкрадання фінансових та матеріально-технічних засобів;
   - захистити від розголошення, витоку та несанкціонованого доступу до службової інформації;
   - не допустити порушення роботи технічних засобів забезпечення виробничої діяльності, включаючи інформаційні технології.

ВИСНОВКИ

13

Використання розглянутого комплексного програмного рішення IBM QRadar забезпечить комплексний захист у комп'ютерних мережах будь-якої складності. Програмне рішення дає змогу відслідковувати та аналізувати виникнення загроз, попереджувати їх виникнення, а також надавати адміністраторам повну інформацію про вузли, виконання процесів та передавання пакетів у мережі.

Комплексне програмне рішення IBM QRadar повністю інтегрується в інфраструктуру підприємства, що забезпечує швидкий та надійний моніторинг корпоративної безпеки, а також масштабується з її розвитком, застосовуючи досвід взаємодії з конкретними користувачами до груп користувачів усієї організації. Можливість всебічного перегляду та аналізу інформації підвищує ефективність обслуговування комп'ютерної мережі в декілька разів.

Основними перевагами застосування IBM QRadar є: підвищення рівня захищеності інформаційної інфраструктури внаслідок оперативного реагування на інциденти інформаційної безпеки; прискорення і автоматизація процесу ідентифікації, а також подальше дослідження інцидентів; централізований підхід до задач обробки та зберігання подій інформаційної безпеки.

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студентки Букет Дар'ї Анатоліївни
на тему: «Технологія управління безпекою інформаційних систем на базі IBM QRadar SIEM»

Актуальність:
У сучасних умовах розвитку інформаційних процесів майже щодня створюються нові компанії. Для забезпечення роботи вони використовують сучасні інтелектуальні інформаційні технології, які є основою функціонування інформаційно-телекомунікаційної системи компанії. З метою оптимізації виробничих процесів ці структури намагаються підвищити ефективність своєї комплексної системи захисту інформації, також шляхом моніторингу. Тому аналіз особливостей проектування і реалізації комплексної системи захисту інформації на базі IBM QRadar SIEM в ІТС підприємства є актуальним.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі встановлено зміст проблеми управління інформаційною системою безпеки, визначено мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи.
2. Досліджено методи та засоби управління безпекою інформаційної системи на базі рішення IBM QRadar SIEM.
3. Запропоновано варіант технології застосування системи управління захистом кінцевих точок корпоративної інформаційної системи на базі рішення IBM QRadar SIEM та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:
1. У магістерській роботі бажано було б провести саме порівняльний аналіз рішень з управління безпекою інформаційних систем різних виробників.
2. Запропонований варіант розгортання системи управління безпекою інформаційної системи на базі рішення IBM QRadar SIEM доцільно було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Букет Дар'я Анатоліївна** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека..

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

_____