ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ВИДИМОСТІ СТАНУ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ QRADAR PULSE»

Виконав студент 4 курсу, групи БСД-44
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гаркуша Д.С.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 8

ВСТУП ……..…… 9

1 **АНАЛІЗ СУТНОСТІ ТА ЗМІСТУ МОНІТОРИНГУ СТАНУ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ** ……. 11

1.1 Призначення, структура, функції та умови функціонування центру управління кібербезпекою …….. 11
1.2 Мета та завдання моніторингу стану кібербезпеки корпоративної інформаційної системи 17
1.3 Аналіз змісту управління кібербезпекою корпоративної інформаційної системи ……..… 23

2 **ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВІЗУАЛІЗАЦІЇ СТАНУ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПРИКЛАДІ IBM QRADAR PULSE** …….. 30

2.1 Можливості щодо розширення функціональності IBM QRadar SIEM …… 30
2.2 Визначення можливостей щодо візуалізації стану безпеки корпоративної інформаційної системи на прикладі IBM QRadar Pulse ….....……. 37
2.3 Аналіз можливостей візуалізації кіберінцидентів в середовищі IBM QRadar Pulse ……..……..……. 44

3 **РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ВИДИМОСТІ СТАНУ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ...…...……..…. 48

3.1 Варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи на прикладі IBM QRadar Pulse 48
3.2 Рекомендації щодо застосування методів та засобів візуалізації стану кібербезпеки корпоративної інформаційної системи …… 50

ВИСНОВКИ …….. 56

ПЕРЕЛІК ПОСИЛАНЬ 58

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

API – Application Programming Interface

APT – Advanced Persistent Threat

AQL – Ariel Query Language

CND – Computer Network Defense

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

SIEM – Security Information and Event Management

SOC – Security Operations Center

ВСТУП

Актуальність дослідження. Для сучасних підприємств, установ та організацій, які мають та застосовують інформаційні системи, центру управління кібербезпекою (Security Operations Center, SOC) є центром компетенцій і оперативного прийняття рішень із усіх питань кібербезпеки. Функціонування центру управління кібербезпекою у десятки разів прискорює роботу фахівців з кібербезпеки та IT при реагуванні на інциденти безпеки та робить її більш узгодженою й ефективною.

Завдяки інтеграції всієї інфраструктури в рамках однієї платформи управління подіями, вразливостями, знаннями й інцидентами кібербезпеки, центр управління кібербезпекою стає постачальником цінної інформації про інформаційні системи та всю інфраструктуру, яка використовується IT та бізнес-підрозділами для кращого розуміння того, що відбувається.

У той же час, центр управління кібербезпекою є споживачем великого об’єму даних з різних джерел корпоративної інформаційної системи для моніторингу її стану та реагування на виникаючі інциденти безпеки.

Величезну роль відіграє забезпечення видимості стану безпеки корпоративної інформаційної системи. Від правильного визначення умов функціонування корпоративної інформаційної системи, вибору та обґрунтування складу методів та засобів моніторингу її стану кібербезпеки та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Вищесказане визначає актуальність теми даної бакалаврської роботи, основний зміст якої становлять дослідження методів та засобів забезпечення видимості стану безпеки корпоративної інформаційної системи.

Об’єкт дослідження – моніторинг стану кібербезпеки корпоративної інформаційної системи.

Предмет дослідження – методи та засоби забезпечення видимості стану

безпеки корпоративної інформаційної системи.

Мета роботи – розробити рекомендації щодо застосування методів та засобів забезпечення видимості стану безпеки корпоративної інформаційної системи.

Наукові завдання:

проаналізувати призначення та умови функціонування центру управління кібербезпекою;

визначити зміст проблеми моніторингу стану кібербезпеки інформаційної системи;

дослідити існуючі методи та засоби забезпечення видимості стану безпеки корпоративної інформаційної системи;

запропонувати варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи;

розробити рекомендації щодо забезпечення видимості стану безпеки корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів забезпечення видимості стану безпеки корпоративної інформаційної системи.

1 АНАЛІЗ СУТНОСТІ ТА ЗМІСТУ МОНІТОРИНГУ СТАНУ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування центру управління кібербезпекою

Під час дослідження Інституту SANS [1] щодо стратегічного бачення перспектив Security Operations Center (SOC) респонденти дали відповідь на питання що є найбільшим викликом (бар'єром) у повному використанні можливостей SOC всією організацією? (рис. 1.1). Однією з найбільших проблем респонденти визначили *відсутність видимості* для всього підприємства.

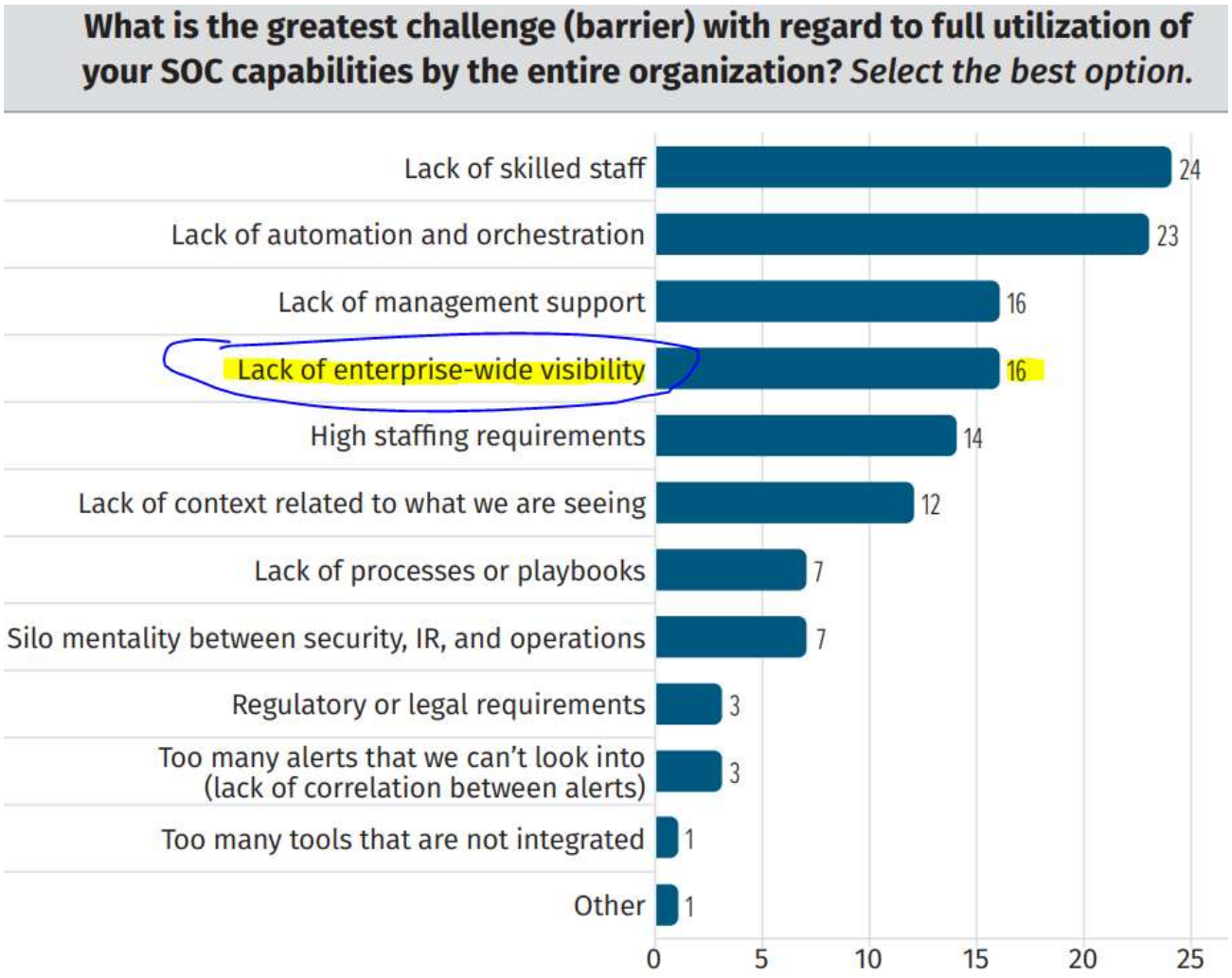

Рис. 1.1. Greatest Challenge to Full Use of SOC Capabilities (Q55 n=127) [1]

Побудова SOC вимагає співпраці та спілкування між кількома функціями (людьми), розрізненими продуктами безпеки (технологіями) та різними процесами та процедурами (процесами), як показано на рис. 1.2. [2].

Рис. 1.2. Тріада операцій безпеки: люди, процеси і технології [2]

Фахівці SOC. Потрібні співробітники, готові виконувати роль реагування на інциденти та аналітиків SOC, або обираються інші варіанти, такі як аутсорсинг (через постачальників керованих послуг безпеки або MSSP) або спеціалістів з підряду, щоб забезпечити швидке реагування на інциденти (IR) та підтримку. Для деяких команд безпеки добре працює гібридна комбінація цих параметрів.

Співробітники SOC повинні мати необхідну підготовку для роботи з постійно мінливою і часто досить складною роботою аналітика з безпеки, розслідувача інцидентів, експерта або менеджера SOC (таблиця 1.1).

Таблиця 1.1

Обов'язки фахівців SOC та потреби в їх навчанні

Посада	Обов'язки	Необхідна підготовка
Рівень 1 Аналітик попередження	Постійно відстежує чергу сповіщень; сортування попереджень безпеки; контролює стан датчиків безпеки та кінцевих точок; збирає дані та контекст, необхідні для початку роботи рівня 2.	Процедури сортування попереджень; виявлення вторгнення; управління мережею, інформацією про безпеку та подіями (SIEM) і розслідувальне навчання на базі хостів; та інше навчання з використанням інструментів.
Рівень 2 Адміністратор реагування на інциденти	Виконує аналіз інцидентів глибокого занурення шляхом співвіднесення даних з різних джерел; визначає, чи зазнали впливу на критичну систему або набір даних; консультує щодо відновлення; забезпечує підтримку нових аналітичних методів виявлення загроз.	Розширена мережева експертиза, криміналістична експертиза на основі хостів, процедури реагування на інциденти, огляди журналів, базова оцінка шкідливого програмного забезпечення, мережева криміналістична експертиза та аналіз загроз.
Рівень 3 Експерт/ Мисливець	Володіє глибокими знаннями про мережу, кінцеву точку, розвідку загроз, криміналістичну експертизу та реверс-інжиніринг зловмисного програмного забезпечення, а також функціонування конкретних програм або базової IT-інфраструктури; діє як «мисливець» за інцидентами, не чекаючи ескалації інцидентів; тісно залучений до розробки, налаштування та впровадження аналітики виявлення загроз.	Підвищення кваліфікації з виявлення аномалій; спеціальне навчання для агрегації та аналізу даних та аналізу загроз.
Менеджер SOC	Керує ресурсами, включаючи персонал, бюджет, планування змін і технологічну стратегію для виконання угод про рівень обслуговування; спілкується з керівництвом; виступає в якості організаційної особи для критичних для бізнесу інцидентів; забезпечує загальне керівництво для SOC та внесок у загальну стратегію безпеки.	Управління проектами, навчання з реагування на інциденти, загальні навички управління людьми.

На додаток до аналітиків SOC, центру безпеки потрібен керівник. Менеджер SOC часто бореться з «пожежами» всередині та поза межами SOC. Менеджер SOC відповідає за визначення пріоритетів роботи та організацію ресурсів з кінцевою метою виявлення, розслідування та пом’якшення інцидентів, які можуть

вплинути на бізнес. Типова організація SOC показана на рис. 1.3.

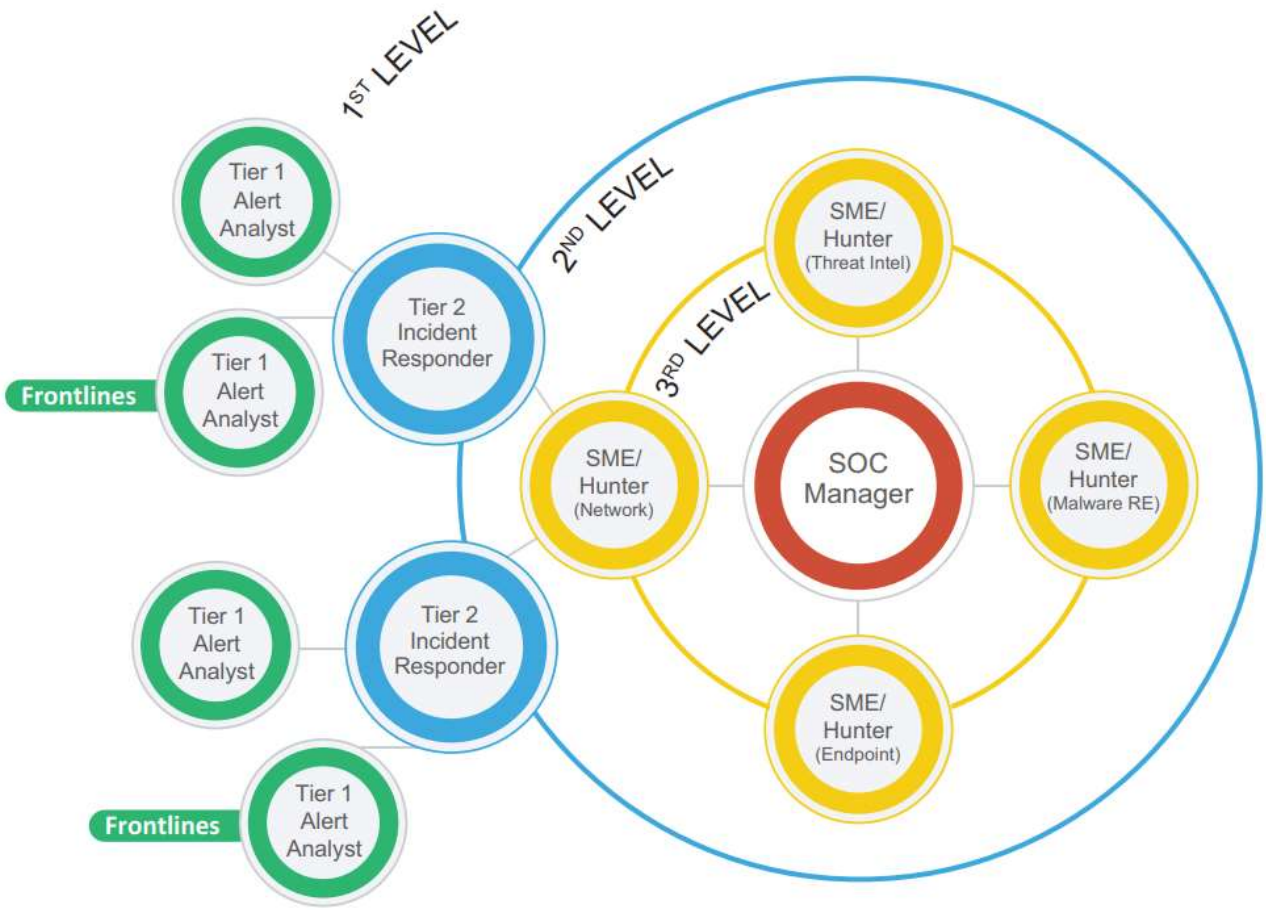

Рис. 1.3. Організація SOC [2]

Менеджер SOC повинен розробити модель робочого процесу та впровадити стандартизовані операційні процедури (SOP) для процесу обробки інцидентів, який спрямовує аналітиків через процедури сортування та реагування.

Процеси. Визначення повторюваних процесів сортування і розслідування інцидентів стандартизує дії, які вживає аналітик SOC, і гарантує, що жодні важливі завдання не пропадуть. Створюючи повторюваний робочий процес управління інцидентами, визначаються обов'язки та дії членів команди від створення сповіщення та початкової оцінки рівня 1 до ескалації, до персоналу рівня 2 або рівня 3.

На основі робочого процесу можна ефективно розподілити ресурси. Однією з найбільш часто використовуваних моделей процесу реагування на інцидент є

модель DOE/CIAC, яка складається з шести етапів: підготовка, ідентифікація, стримування, ліквідація, відновлення та отримані висновки. Крім того, NIST SP800-61 Rev. 2 “Computer Security Incident Handling Guide” [3] забезпечує рекомендації щодо розробки процедур реагування на інциденти.

Технологія. Рішення для збору, агрегації, виявлення, аналітики та управління для всього підприємства є основною технологією успішного SOC. Ефективна система моніторингу безпеки включає дані, зібрані з безперервного моніторингу кінцевих точок (ПК, ноутбуки, мобільні пристрої та сервери), а також мереж, журналів і джерел подій.

Завдяки даним мережі, журналу та кінцевих точок, зібраних до та під час інциденту, аналітики SOC можуть негайно перейти від використання системи моніторингу безпеки як інструменту виявлення до використання її як інструменту розслідування, перевіряючи підозрілі дії, які є причиною цього інциденту. Також як інструмент для управління реакцією на інцидент або порушення.

Сумісність технологій є обов’язковою, особливо якщо організація має існуюче рішення для моніторингу безпеки (SIEM, кінцева точка, мережа чи інше) і хоче включити звіти цього інструменту в рішення для управління інцидентами (рис. 1.4) [2].

Включення інформації про загрози, активів, ідентифікаційної та іншої інформації про контекст – це ще один спосіб, завдяки якому ефективне рішення для моніторингу безпеки підприємства може допомогти аналітику SOC у процесі розслідування. Часто сповіщення пов’язане з діяльністю на основі мережі або хоста і спочатку може містити лише IP-адресу підозрілої кінцевої точки. Щоб аналітик SOC дослідив систему, про яку йде мова, аналітику зазвичай потрібна інша інформація, така як власник і ім’я хоста машини або записи з джерела DHCP для зіставлення IP-адреси та інформації про хост на момент сповіщення.

Якщо система моніторингу безпеки містить інформацію про активи та ідентифікаційну інформацію, це дає величезну перевагу в часі та зусиллях аналітика, не кажучи вже про ключові фактори, які аналітик може використати для визначення пріоритету інциденту безпеки – загалом, більш цінні бізнес-

активи повинні мати пріоритет перед менш цінними.

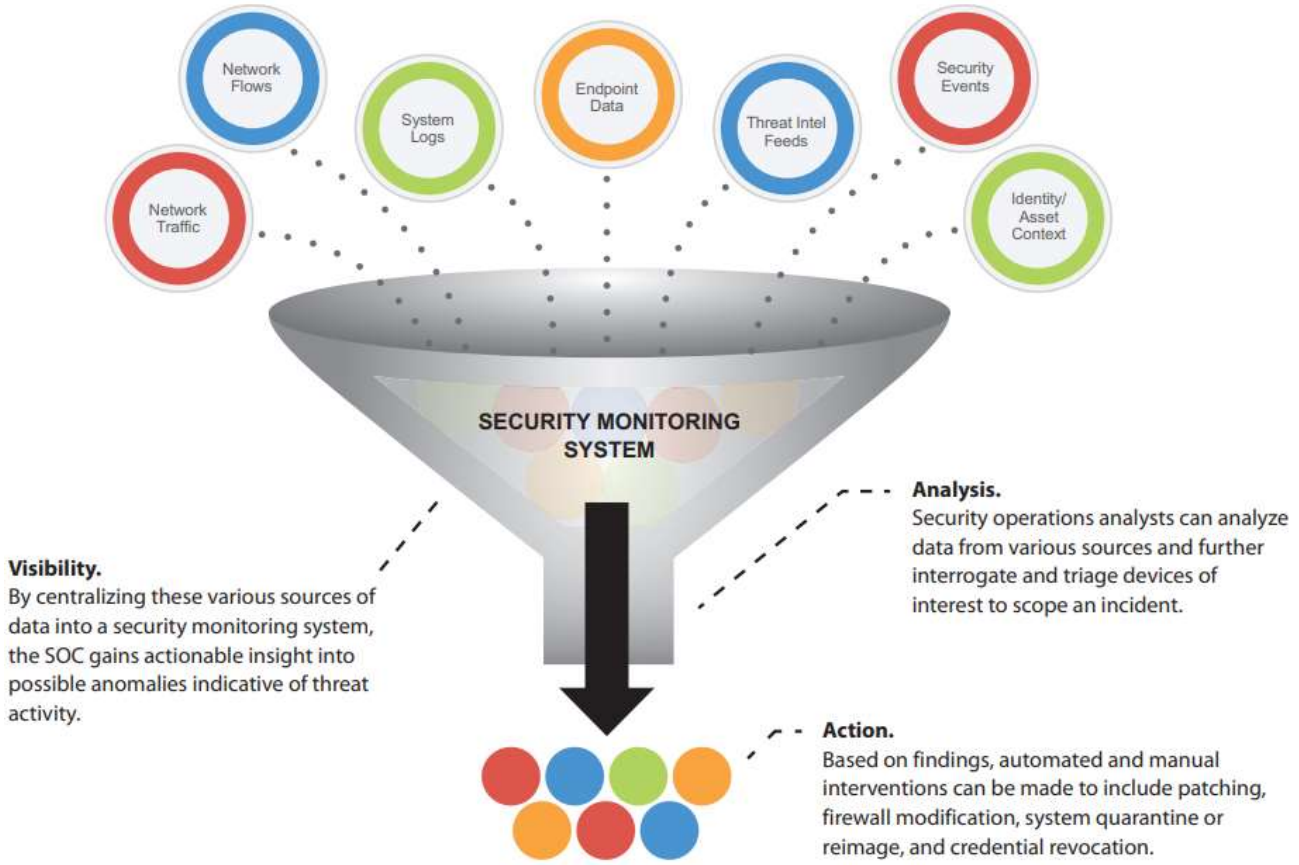

Рис. 1.4. Сумісні технології, які допомагають виявити інциденти [2]

Визначення нормального стану за допомогою базового аналізу. Можливість створити базовий план діяльності для користувачів, додатків, інфраструктури, мережі та інших систем, встановити, як виглядає нормальний вигляд, є однією з переваг агрегованих даних, зібраних з різних джерел підприємства.

Маючи визначення «нормального» стає легше виявляти підозрілу поведінку. Правильно зконфігурована і налаштована система моніторингу безпеки надсилає дійові попередження, яким можна довіряти, і яким часто можна довіряти, і які часто автоматично визначають пріоритет перед тим, як потрапити до аналітика рівня 1.

Однак, згідно з опитуванням SANS 2014 Log Management Survey, одна з найголовніших проблем у використанні даних журналу респондентами було названо нездатність відрізнити нормальне від підозрілої діяльності. Відсутність

такої базової лінії є загальною перешкодою, з якою організації стикаються під час впровадження системи моніторингу безпеки підприємства [2].

Найкращою практикою є використання платформ, які можуть створювати базові лінії шляхом моніторингу активності мережі та кінцевої точки протягом певного періоду часу, щоб допомогти визначити, чи виглядає «нормально», а потім надати можливість встановлювати пороги подій як ключові драйвери попереджень. Коли виявляється несподівана поведінка або відхилення від нормальної діяльності, платформа створює сповіщення, що вказує на необхідність подальшого розслідування.

Зрілі SOC з розвідки загроз постійно розвивають здатність використовувати розвідку про загрози зі своїх минулих інцидентів та з джерел обміну інформацією, таких як спеціалізований постачальник розвідки загроз, партнери в галузі, відділ правоохоронних органів з кіберзлочинів, організації, що обмінюються інформацією або їх постачальників технологій моніторингу безпеки.

Здатність системи моніторингу безпеки впроваджувати розвідку про загрози та використовувати її, щоб допомогти виявити закономірності в кінцевих точках, журналах і мережевих даних, а також пов’язувати аномалії з минулими попередженнями, інцидентами або атаками, може покращити здатність організації виявляти зламану систему або користувача до того, як він має ознаки порушення.

Щоб досягти ефективної обробки інцидентів, SOC повинен уникати вузьких місць у процесі IR, який переміщує інциденти через рівень 1, на рівень 2 і, нарешті, через рівень 3. Вузькі місця можуть виникати через занадто багато «білого шуму». сповіщення, які мають незначні наслідки або хибнопозитивні, що призводять до «втоми попередження».

Незважаючи на те, що кожна організація є унікальною за своєю поточною позицією безпеки, толерантністю до ризиків, знанням і бюджетом, усі мають спільні цілі: намагатися мінімізувати свою поверхню атак, а також швидко виявляти, розставляти пріоритети та розслідувати інциденти безпеки, коли вони трапляються.

1.2. Мета та завдання моніторингу стану кібербезпеки корпоративної інформаційної системи

SOC – це команда, що складається в основному з аналітиків з безпеки, організованих для виявлення, аналізу, реагування на інциденти кібербезпеки, звітування про них та запобігання [4].

SOC визначається насамперед тим, що він здійснює *computer network defense* (CND). CND характеризується як практика захисту від несанкціонованої діяльності в комп'ютерних мережах, включаючи моніторинг, виявлення, аналіз (наприклад, аналіз тенденцій і шаблонів), а також дії з реагування на інциденти та відновлення після них [4].

Розміри SOC можуть варіюватися від невеликих операцій з п'ятьма особами до великих національних координаційних центрів. Типові завдання SOC середнього розміру зазвичай включає такі елементи [4]:

запобігання інцидентам кібербезпеки проактивним шляхом:

постійний аналіз загроз;

сканування мережі та хостів на наявність вразливостей;

координація розгортання контрзаходів;

консалтинг щодо політики безпеки та архітектури;

моніторинг, виявлення та аналіз потенційних вторгнень у реальному часі та за допомогою історичних тенденцій у джерелах даних, що стосуються безпеки;

реагування на підтверджені інциденти шляхом координації ресурсів та керівництва використанням своєчасних і відповідних контрзаходів;

надання ситуаційної обізнаності та звітування про стан кібербезпеки, інциденти та тенденції поведінки противника відповідним організаціям;

розробка та експлуатація технологій CND, таких як IDS та системи збору/аналізу даних.

З цих завдань, мабуть, найбільш трудомісткими є використання та аналіз великої кількості даних, що стосуються безпеки. Серед багатьох релевантних для безпеки каналів даних, які SOC, ймовірно, оброблює, найпомітнішими часто є

IDS. IDS – це системи, розміщені або на хості, або в мережі для виявлення потенційно зловмисної або небажаної діяльності, що вимагає додаткової уваги аналітика SOC. У поєднанні з журналами аудиту безпеки та іншими каналами даних типовий SOC збирає, аналізує та зберігає десятки чи сотні мільйонів подій безпеки щодня.

Необхідно підкреслити, що використання та аналіз великої кількості даних, що стосуються безпеки, вимагає візуалізації стану безпеки корпоративної інформаційної системи як шляху забезпечення її високої видимості.

Іноді події вказують на те, що інцидент стався (наприклад, сповіщення, створене IDS або службою аудиту безпеки). Подія – це не що інше, як необроблені дані. Щоб визначити, чи виправдані подальші дії, потрібен *людський аналіз – процес оцінки значення набору даних, що стосуються безпеки, як правило, за допомогою спеціалізованих інструментів* [4].

SOC зазвичай призначає групу осіб, які займаються сортуванням попереджень у реальному часі, а також телефонними дзвінками від користувачів та іншими рутинними завданнями. Цю групу часто називають Рівнем 1. Якщо Рівень 1 визначає, що сповіщення досягає певного попередньо визначеного порогу, створюється випадок і передається до Рівня 2. Цей поріг можна визначити відповідно до різних типів потенційного «поганого» (типу інциденту, цільовий актив або інформація, задіяна місія тощо).

Зазвичай проміжок часу Рівня 1 для вивчення кожної цікавої події становить від однієї до 15 хвилин. Це залежить від політики ескалації SOC, концепції операцій (CONOPS), кількості аналітиків, розміру вибірки та обсягу заходів. Учасникам Рівня 1 не рекомендується проводити поглиблений аналіз, оскільки вони не повинні пропускати події, які трапляються на їхніх консолях у реальному часі. Якщо для оцінки події потрібно більше часу, вона переходить до Рівня 2.

Рівень 2 приймає випадки з Рівня 1 і виконує поглиблений аналіз, щоб визначити, що насправді сталося наскільки це можливо, з огляду на доступний час і дані і чи потрібні додаткові дії. Перш ніж буде прийнято це рішення, може

знадобитися кілька тижнів, щоб зібрати та перевірити всі необхідні дані, щоб визначити масштаб і серйозність події. Оскільки Рівень 2 не відповідає за моніторинг у режимі реального часу та укомплектований більш досвідченими аналітиками, він може витратити час на повний аналіз кожного набору заходів, збір додаткової інформації та координацію з вибірками.

Як правило, відповідальність рівня 2 (або вище) полягає у визначенні, чи відбувся потенційний інцидент. Відповідно до [4] *інцидентом* є оцінена подія, яка фактично або потенційно ставить під загрозу конфіденційність, цілісність та доступність інформаційної системи або інформації, яку система обробляє, зберігає або передає; або *що* становить порушення чи неминучу загрозу порушення політики безпеки, процедур безпеки чи політики прийнятного використання. Одна подія може породити інцидент, але на кожен інцидент, ймовірно, є тисячі або мільйони подій, які є просто доброякісними.

SOC зазвичай використовує внутрішні та зовнішні ресурси для реагування на інцидент і відновлення після нього. Важливо визнати, що SOC не завжди може застосовувати контрзаходи при перших ознаках вторгнення. Для цього є три причини [4]:

1. SOC хоче бути впевненим, що він не блокує доброякісну діяльність.

2. Дія реагування може вплинути на служби інформаційної системи більше, ніж сам інцидент.

3. Розуміння масштабів і серйозності вторгнення шляхом спостереження за противником іноді є ефективнішим, ніж виконання статичного криміналістичного аналізу скомпрометованих систем, коли противник більше не присутній.

Щоб визначити характер атаки, SOC часто доводиться виконувати розширений криміналістичний аналіз артефактів, таких як зображення жорсткого диска або захоплення пакетів повного сеансу (PCAP), або зворотний інжиніринг шкідливого програмного забезпечення на зразках шкідливих програм, зібраних для підтвердження інциденту.

Коли ознаки атаки зрозумілі достатньо добре, щоб закодувати сигнатуру IDS, яка зчитується комп’ютером, атаку можна запобігти в мережі, як із системою

запобігання вторгненню хоста (HIPS) або системою запобігання вторгненню в мережу (NIPS). Хоча такі системи, як правило, використовуються для запобігання найпростіших атак, міра, до якої вони можуть автоматизувати аналіз, обмежена.

Людський аналіз завжди потрібен, щоб виявити серйозний інцидент. Низка технологій дозволяє SOC щодня прочісувати мільйони подій, підтримуючи життєвий цикл інциденту. Інструменти SIEM збирають, зберігають, співвідносять і відображають безліч каналів даних, що стосуються безпеки, підтримуючи сортування, аналіз, ескалацію та реагування. IDS і системи запобігання вторгненням (IPS) є двома з багатьох систем, які є джерелом даних для SIEM. Нинішній погляд на технології IDS/IPS припускає, що вони можуть бути необхідними, але їх, безумовно, недостатньо для виявлення інцидентів.

SOC не просто використовує дані зі своїх інформаційних систем. Він також збирає чи отримує інформацію з різних зовнішніх джерел, що дає уявлення про загрози, вразливості та TTP противника. Ця інформація називається кіберрозвідкою, і вона включає стрічки кібер-новин, оновлення сигнатур, звіти про інциденти, відомості про загрози та сповіщення про вразливості.

Описуючи всі ролі, які виконують різні частини SOC, треба визнати, що кожен SOC буде розподіляти ролі по-різному і що між функціями може існувати накладення. Деякі SOC здійснюють поглиблений аналіз та реагування в одному розділі Рівня 2. Інші розділять деякі з цих функцій на Рівень 3. Загальний шлях ескалації та ролі реагування на інцидент SOC проілюстровано на рис 1.5.

Щоб SOC ефективно надавав набір можливостей компонентам, він повинен розуміти середовище, в якому він виконує завдання CND, як на макроскопічному, так і на мікроскопічному рівні. Значна частина роботи SOC, навмисно чи випадково, полягає в тому, щоб підтримувати та надавати це розуміння стану безпеки інформаційної системи. Це розуміння називається *ситуаційною обізнаністю (Situational Awareness, SA)* [4].

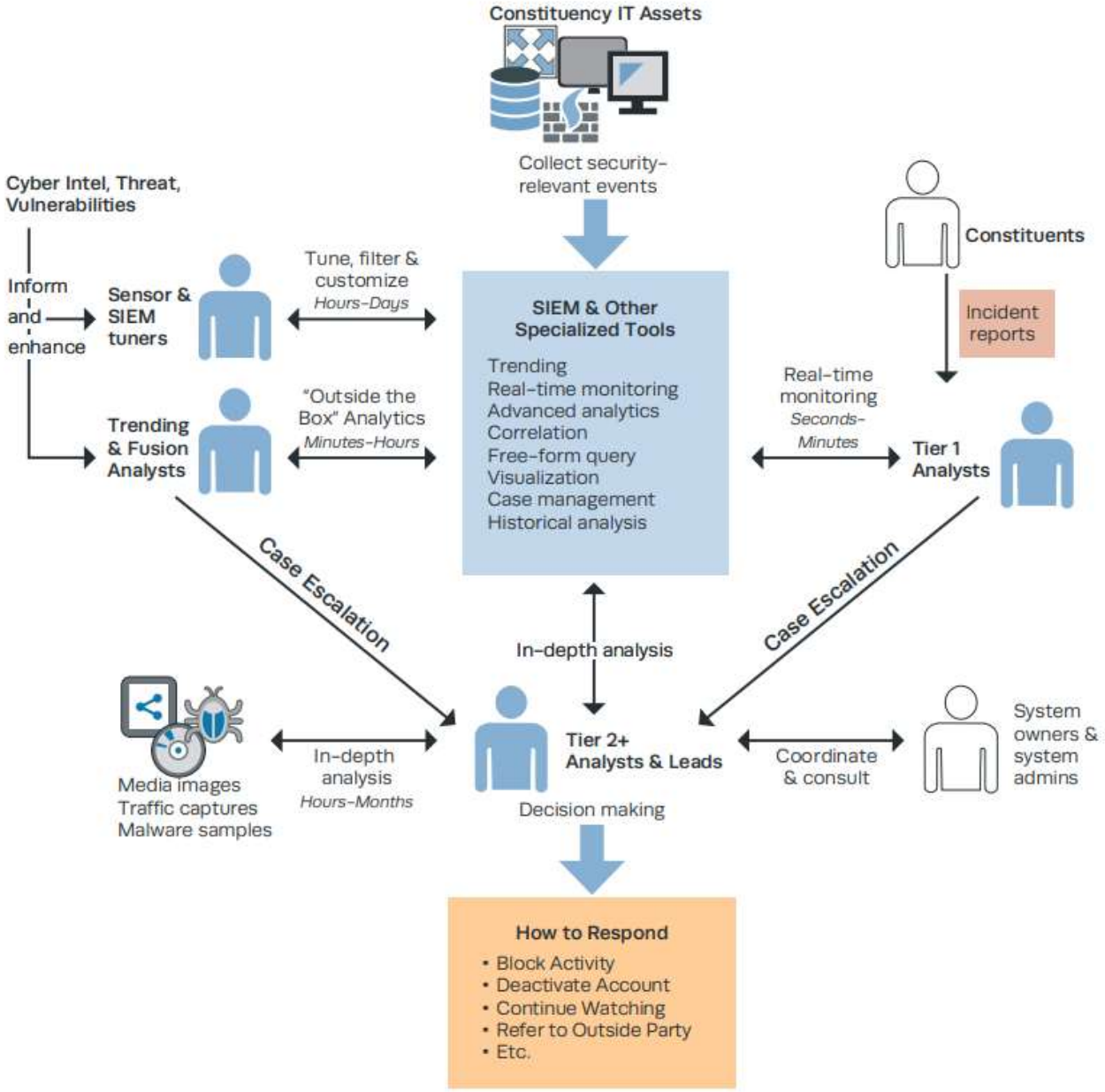

Рис. 1.5. Ролі SOC та ескалація інцидентів [4]

В [4] приводиться таке визначення:

Ситуаційна обізнаність – це сприйняття елементів довкілля в межах об'єму часу та простору, усвідомлення їх значення та проекція їхнього стану на найближче майбутнє.

Неоднозначність і невизначеність – протилежності гарній ситуаційній обізнаності щодо стану кібербезпеки. Вони існують на кожному етапі життєвого циклу інцидентів і їх необхідно пом'якшувати шляхом постійного вдосконалення системи моніторингу та аналітики.

Для SOC практика отримання ситуаційної обізнаності щодо стану кібербезпеки ділиться на три складові [4]:

Інформація. Дані датчиків, контекстні дані, кіберрозвідка, новини, уразливості продуктів постачальника, загрози та завдання;

Аналітика. Інтерпретація та обробка цієї інформації;

Візуалізація. Зображення інформації SA у наочній формі.

Зазначається, що у сфері ситуаційної обізнаності щодо стану кібербезпеки візуалізація все ще знаходиться на початковому етапі. Незважаючи на те, що була проведена велика робота в області візуалізації кібербезпеки, здається, не існує універсальної практики візуалізації інформації щодо кібербезпеки [4].

Для SOC отримання та використання SA слідує за циклом спостереження, орієнтування, прийняття рішення та дії (петля OODA) циклу прийняття рішень, що самопідсилюється (рис. 1.6) [4].

Рис. 1.6. Цикл OODA [4]

Аналітик постійно проводить спостереження щодо об’єкта, орієнтує цю інформацію з попередньою інформацією та досвідом, приймає рішення на основі цього синтезу, вживає заходів, а потім повторює процес. Протягом часу, що варіюється від хвилин до років, аналітики SOC знайомляться зі своїми об’єктами та відповідними кіберзагрозами. У міру того, як SA покращується, вони стають більш ефективними операторами.

1.3. Аналіз змісту управління кібербезпекою корпоративної інформаційної системи

Центр управління кібербезпекою (SOC) – це централізована функція в організації, яка використовує людей, процеси та технології для постійного моніторингу та покращення стану безпеки організації, запобігаючи, виявляючи, аналізуючи та реагуючи на інциденти кібербезпеки [5].

SOC діє як центр або центральний командний пункт, одержуючи телеметрію з усієї IT-інфраструктури організації, включаючи її мережі, пристрої, прилади та сховища інформації, де б ці активи не знаходилися. Поширення передових загроз надає перевагу збиранню контексту з різних джерел. По суті, SOC є точкою кореляції для кожної події, зареєстрованої в організації, яка контролюється. Для кожної з цих подій SOC має вирішити, як вони будуть керуватися та діяти [5].

Функція фахівців SOC, полягає в цілодобовому моніторингу, виявленні, розслідуванні та реагуванні на кіберзагрози. Операційні групи з безпеки цілеспрямовано на моніторинг та захист багатьох активів, таких як інтелектуальна власність, дані персоналу, бізнес-системи та цілісність бренду. Як компонент реалізації загальної системи кібербезпеки організації, групи з операцій безпеки виступають центральним пунктом співпраці в скоординованих зусиллях щодо моніторингу, оцінки та захисту від кібератак [5].

Розглянемо ключові функцій, які виконує SOC [5].

Оцінка наявних ресурсів. SOC відповідає за два типи активів – різні пристрої, процеси та програми, за які захищаються, а також за захисні інструменти, які є в їх розпорядженні, щоб забезпечити цей захист.

SOC не може захистити пристрої та дані, які він не бачить. Без видимості та контролю від пристрою до хмари, ймовірно, будуть сліпі зони в системі безпеки мережі, які можна знайти та використати. Таким чином, мета SOC – отримати повне уявлення про ландшафт загроз бізнесу, включаючи не тільки різні типи кінцевих точок, серверів і програмного забезпечення на

території, а й сторонні служби та трафік, що перетікає між цими активами.

SOC також повинен мати повне розуміння всіх наявних інструментів кібербезпеки та всіх робочих процесів, які використовуються в SOC. Це підвищує маневреність і дозволяє SOC працювати з максимальною ефективністю

Підготовка та профілактичне обслуговування. Навіть самі добре обладнані та гнучкі процеси реагування не зможуть запобігти виникненню проблем. Щоб утримати зловмисників у страху, SOC вживає превентивні заходи, які можна розділити на дві основні категорії.

Члени підготовчої групи повинні бути в курсі останніх інновацій у сфері безпеки, останніх тенденцій у сфері кіберзлочинності та розвитку нових загроз на горизонті. Це дослідження може допомогти створити дорожню карту безпеки, яка визначатиме напрямки подальших зусиль компанії з кібербезпеки, а також план аварійного відновлення, який послужить готовим керівництвом у гіршому випадку.

Профілактичне обслуговування – цей крок включає всі дії, вжиті для ускладнень успішних атак, включаючи регулярне обслуговування та оновлення існуючих систем; оновлення політики брандмауера; виправлення вразливостей; внесення в білий список, чорний список; захист програм.

Постійний активний моніторинг. Інструменти, які використовує SOC, цілодобово сканують мережу, щоб помітити будь-які відхилення або підозрілу діяльність. Цілодобовий моніторинг мережі дозволяє SOC негайно отримувати сповіщення про виникаючі загрози, що дає йому найкращі шанси запобігти чи пом’якшити шкоду. Інструменти моніторингу можуть включати SIEM або EDR, краще навіть SOAR або XDR, найдосконаліші з яких можуть використовувати поведінковий аналіз, щоб «навчити» системи різниці між звичайними повсякденними операціями та фактичною поведінкою загроз, мінімізуючи кількість сортування та аналізу, які повинні виконувати люди.

Рейтинг сповіщень і управління. Коли інструменти моніторингу видають попередження, SOC несе відповідальність уважно розглянути кожне з них, відкинути всі помилкові спрацьовування та визначити, наскільки агресивними є

будь-які фактичні загрози та на що вони можуть бути спрямовані. Це дозволяє їм правильно сортувати загрози, що виникають, першими вирішуючи найнагальніші проблеми.

Реакція на загрозу. Це ті дії, про які більшість людей думає, коли думають про SOC. Щойно інцидент підтверджується, SOC виконує функції першого реагування, виконуючи такі дії, як вимкнення або ізоляція кінцевих точок, припинення шкідливих процесів (або запобігання їх виконання), видалення файлів тощо. Мета полягає в тому, щоб реагувати в необхідному обсязі, маючи якомога менший вплив на безперервність бізнесу.

Відновлення та санація. Після інциденту SOC працюватиме над відновленням систем і будь-яких втрачених або зламаних даних. Це може включати очищення та перезапуск кінцевих точок, переналаштування систем або, у разі атак програм-вимагачів, розгортання життєздатних резервних копій, щоб обійти програму-вимагач. У разі успіху цей крок поверне мережу до стану, в якому вона була до інциденту.

Управління журналами. SOC відповідає за збір, підтримку та регулярний перегляд журналу всієї мережевої діяльності та комунікацій для всієї організації. Ці дані допомагають визначити базовий рівень для «звичайної» мережевої активності, можуть виявити існування загроз і можуть бути використані для усунення наслідків і криміналістичної експертизи після інциденту. Багато SOC використовують SIEM для агрегації та кореляції каналів даних із програм, брандмауерів, операційних систем та кінцевих точок, усі з яких створюють власні внутрішні журнали.

Розслідування першопричин. Після інциденту SOC відповідає за з'ясування того, що саме сталося, коли, як і чому. Під час цього розслідування SOC використовує дані журналів та іншу інформацію, щоб відстежити проблему до її джерела, що допоможе запобігти виникненню подібних проблем у майбутньому.

Удосконалення та покращення безпеки. Кіберзлочинці постійно вдосконалюють свої інструменти та тактику, і для того, щоб залишатися попереду, SOC потребує постійного вдосконалення. Під час цього кроку плани,

викладені в дорожній карті безпеки, оживають, але це вдосконалення також може включати практичні практики.

Управління відповідністю. Багато процесів SOC керуються встановленими передовими практиками, але деякі регулюються вимогами відповідності. SOC відповідає за регулярний аудит своїх систем для забезпечення відповідності таким нормам, які можуть бути видані їхньою організацією, галуззю або керівними органами. Приклади цих правил включають GDPR, HIPAA та PCI DSS. Дія згідно з цими правилами не тільки допомагає захистити конфіденційні дані, які довірені компанії, а також може захистити організацію від шкоди репутації та юридичних проблем, спричинених порушенням.

Оптимізація моделі операцій безпеки. Для того, щоб об'єднати ці функції операційних систем та даних, ефективна стратегія вимагає адаптивної архітектури безпеки, яка дає можливість організаціям здійснювати оптимізовані операції безпеки. Такий підхід підвищує ефективність за рахунок інтеграції, автоматизації та оркестровки, а також скорочує кількість робочих годин, необхідних, одночасно покращуючи вашу позицію управління інформаційною безпекою.

Оптимізована модель операцій безпеки вимагає прийняття системи безпеки, яка спрощує інтеграцію рішень безпеки та аналізу загроз у повсякденні процеси. Інструменти SOC, такі як *централізовані та ефективні інформаційні панелі*, допомагають інтегрувати дані про загрози в інформаційні панелі моніторингу безпеки та звіти, щоб тримати операції та управління в курсі подій та дій, що розвиваються. Пов'язуючи управління загрозами з іншими системами для управління ризиками та дотриманням вимог, команди SOC можуть краще керувати загальним ризиком. Такі конфігурації *підтримують безперервну видимість між системами та доменами та можуть використовувати оперативні інтелектуальні дані для підвищення точності й узгодженості операцій безпеки*. Централізовані функції зменшують тягар ручного обміну даними, аудиту та звітності.

Процес управління загрозами (рис. 1.7) починається з плану та включає виявлення (включаючи розрахунок базової лінії для сприяння виявлення

аномалій, нормалізації та кореляції), сортування (на основі ризику та вартості активів), аналіз (включаючи контекстуалізацію) та визначення обсягу (включаючи повторне дослідження). Процеси управління загрозами передають пріоритетні та охарактеризовані випадки в програми реагування на інциденти. Чітко визначений план реагування є абсолютно ключовим для стримування загрози або мінімізації шкоди від порушення даних [5].

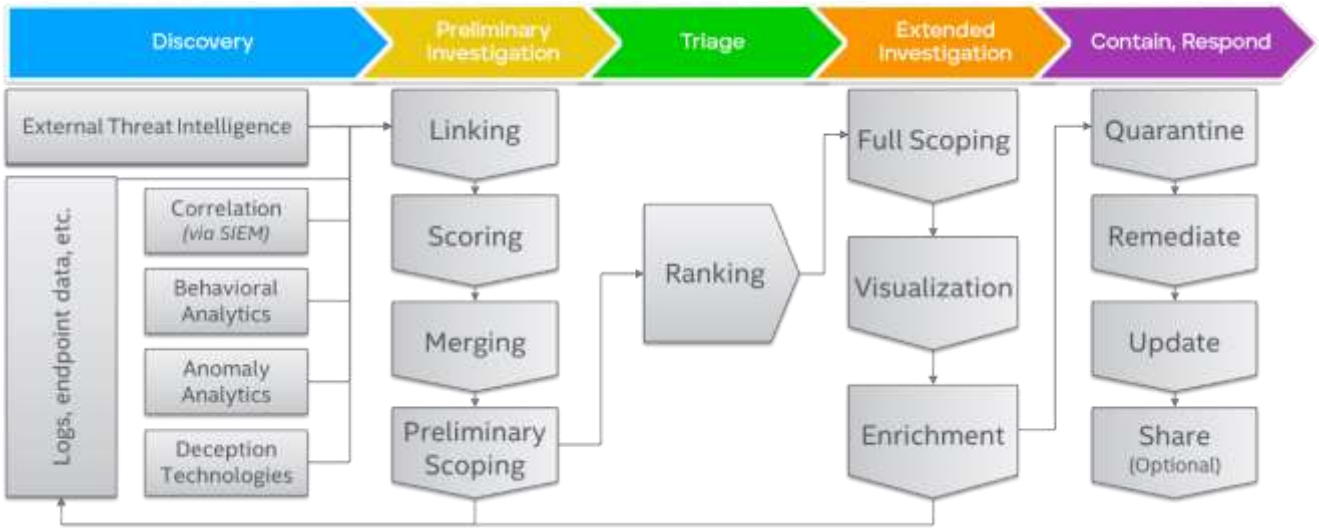

Рис. 1.7. Процеси управління загрозами [5]

Ефективне керування видимістю та загрозами буде ґрунтуватися на багатьох джерелах даних, але може бути важко розібрати корисну та своєчасну інформацію. Найціннішими виявилися дані про події, отримані за допомогою контрзаходів та IT-активів, індикатори компрометації (IoC), створені всередині (через аналіз шкідливих програм) і зовні (через канали розвідки загроз), а також системні дані, доступні з датчиків (наприклад, хост, мережа, база даних тощо).

Такі джерела даних – це не лише вхідні дані для управління загрозами. Вони додають контекст і роблять інформацію цінною та ефективною для більш своєчасної, точної та швидкої оцінки протягом ітеративного та інтерактивного управління загрозами.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВІЗУАЛІЗАЦІЇ СТАНУ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПРИКЛАДІ IBM QRADAR PULSE

2.1. Можливості щодо розширення функціональності IBM QRadar SIEM

Кількість проблем, які стоять перед командами безпеки, не зменшується: збільшення обсягу та складності кібератак, вибух даних, розширення поверхні атак, роз'єднаних інструментів безпеки та дефіцит кваліфікованого персоналу безпеки. Фактично, організації витрачають сотні годин на тиждень на розслідування підозрілих сповіщень, але, незважаючи на цей час, близько 17% сповіщень не розслідуються [6].

Організації, які прагнуть захистити особистість своїх клієнтів, захистити їхню інтелектуальну власність і уникнути зриву бізнесу необхідно активно контролювати своє середовище, щоб вони могли швидко виявляти загрози та точно реагувати, перш ніж зловмисники зможуть завдати фінансової та репутаційної шкоди [6].

IBM QRadar SIEM, лідируюче на ринку рішення SIEM, допомагає захиститися від зростаючих загроз, одночасно модернізуючи та масштабуючи операції безпеки за допомогою інтегрованої видимості, виявлення, дослідження та реагування. IBM QRadar SIEM надає командам з безпеки централізований доступ до даних безпеки в масштабах підприємства та оперативне уявлення про найбільш пріоритетні загрози.

Аналітики з безпеки можуть працювати з однієї панелі, щоб швидко зрозуміти свою позицію безпеки, визначити найбільш критичні загрози та деталізувати, щоб отримати більше деталей, допомагаючи впорядкувати робочі процеси та позбутися необхідності переходити між інструментами. Завдяки можливості виявлення аномалій IBM QRadar SIEM, групи безпеки можуть

швидко визначити зміни в поведінці користувачів, які можуть бути індикаторами невідомої загрози.

Рішення поглинає величезну кількість даних по всьому підприємству, щоб забезпечити вичерпне уявлення про діяльність у локальних і хмарних середовищах. Коли дані надходять, IBM QRadar SIEM застосовує в режимі реального часу автоматизований аналіз безпеки для швидкого та точного виявлення та визначення пріоритету загроз. Сповіщення забезпечують розширений контекст потенційних інцидентів, що дає змогу аналітикам безпеки швидко реагувати, щоб обмежити вплив зловмисників.

IBM QRadar SIEM спеціально створений для вирішення широкого спектру випадків використання безпеки та легко масштабується з обмеженими зусиллями щодо налаштування.

Завдяки IBM QRadar SIEM забезпечується всеосяжна централізована видимість стану безпеки.

Корпоративні мережі можуть охоплювати традиційні локальні IT, хмарні та операційні технологічні середовища, усі з яких вимагають певного рівня спостереження для ефективного захисту активів, точного виявлення загроз і підтримки відповідності.

Перш ніж групи безпеки зможуть розпочати аналіз даних для виявлення загроз і керування ними, вони повинні мати централізовану видимість різних даних безпеки. IBM QRadar SIEM дозволяє організаціям отримати централізовану, всеосяжну видимість ізольованих середовищ, збираючи, аналізуючи та нормалізуючи дані журналів і потоків.

За допомогою однієї панелі аналітики безпеки можуть контролювати локальні, хмарні та гібридні середовища. Рішення включає понад 450 попередньо вбудованих модулів підтримки пристроїв (Device Support Module, DSM), які забезпечують інтеграцію налаштувань за замовчуванням з іншими інвестиціями в безпеку. Клієнти можуть просто вказати журнали на IBM QRadar SIEM, і рішення може автоматично визначити тип джерела журналу та застосувати правильний DSM для аналізу та нормалізації даних журналу. В результаті клієнти IBM QRadar

SIEM можуть почати працювати набагато швидше, ніж клієнти альтернативних рішень [6]. *Додаткові інтеграції можна легко додати через програми в IBM Security App Exchange.*

IBM QRadar SIEM 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 допомогти легко створити базу даних активів, яка дає можливість організаціям визначати критичні активи або сегменти мережі, IBM QRadar SIEM може перевіряти дані мережевого потоку, щоб автоматично ідентифікувати та класифікувати дійсні активи в мережі на основі програм, протоколів, служб і портів, які вони використовують. IBM QRadar SIEM підтримує широкий спектр технологій, додатків і хмарних сервісів, щоб допомогти клієнтам отримати повну інформацію про діяльність підприємства [6].

Після централізації ці дані можна автоматично аналізувати, щоб визначити відомі загрози, аномалії, які можуть вказувати на невідомі загрози, і критичні ризики, через які конфіденційні дані можуть бути відкритими. Автоматизація аналізу безпеки для швидкого виявлення загроз IBM QRadar SIEM розроблено для автоматичного аналізу та кореляції активності в кількох джерелах даних, включаючи журнали, події, мережеві потоки, активність користувачів, інформацію про вразливості та аналіз загроз для виявлення відомих і невідомих загроз.

IBM QRadar SIEM інтелектуально корелює та аналізує різноманітні типи даних із широкого кола джерел, у тому числі [6]:

дані кінцевої точки: з журналу подій Windows, рішень Sysmon, EDR тощо;

дані про мережеву активність: від брандмауерів, шлюзів, маршрутизаторів або датчиків;

дані про вразливості: від антивірусних засобів, сканерів вразливостей, систем виявлення вторгнень, систем запобігання вторгненням, систем запобігання втраті даних тощо;

хмарна діяльність: із середовищ SaaS та IaaS, таких як Office365,

SalesForce.com, Amazon Web Services (AWS), Microsoft Azure та Google Cloud;

дані користувачів та ідентифікаційні дані: надходять із Active Directory, LDAP або інших рішень керування ідентифікацією та доступом;

дані додатків: від рішень для планування ресурсів підприємства (ERP), баз даних додатків, додатків SaaS тощо;

дані розвідки про загрози: з таких джерел, як IBM X-Force та сторонніх каналів розвідки загроз;

дані про діяльність контейнерів: із програмного забезпечення для керування та оркестрування контейнерів, такого як Kubernetes.

IBM QRadar SIEM збирає, аналізує та співвідносить дані з найрізноманітніших джерел для виявлення та визначення пріоритету найбільш критичних загроз, які потребують розслідування (рис. 2.1).

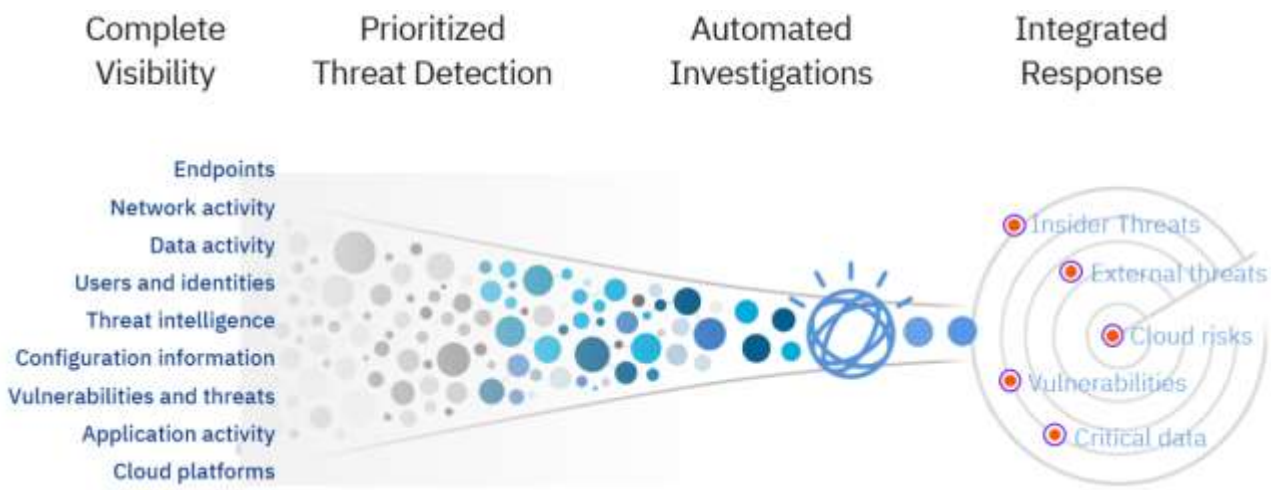

Рис. 2.1. Схема інформаційної технології IBM QRadar SIEM [6]

IBM QRadar SIEM містить сотні попередньо створених випадків використання безпеки, алгоритми виявлення аномалій, правила та політики кореляції в реальному часі для виявлення відомих і невідомих загроз. У міру виявлення загроз рішення об’єднує пов’язані події безпеки в окремі пріоритетні сповіщення, відомі як «порушення». Пріоритет порушень автоматично визначається як серйозністю загрози, так і критичністю активів.

У вікні «Порушення» у IBM QRadar SIEM (рис. 2.2) наведено пріоритетний

список загроз.

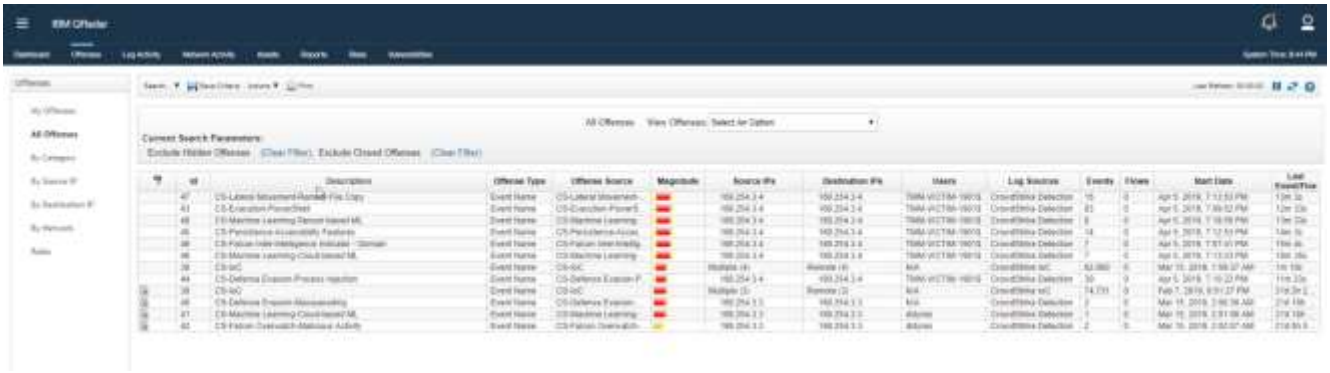

Рис.2.2. Вікно «Порушення» IBM QRadar SIEM

У межах кожного порушення аналітики безпеки можуть побачити весь ланцюжок загроз з одного екрана. Звідси аналітики можуть легко вивчити конкретні події або мережеві потоки, щоб почати розслідування, призначити злочин конкретному аналітику або закрити його. Порушення автоматично оновлюються в міру появи нової пов’язаної діяльності, щоб аналітики могли бачити найновішу інформацію в будь-який момент. Цей унікальний підхід допомагає аналітикам безпеки легко зрозуміти найкритичніші загрози в середовищі, забезпечуючи наскрізне уявлення про кожен потенційний інцидент, одночасно зменшуючи загальний обсяг сповіщень.

Оскільки зловмисники вдосконалюються у своїх техніках, відомого виявлення загроз само по собі 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 безфайлове зловмисне програмне забезпечення.

IBM QRadar SIEM містить різноманітні можливості виявлення аномалій для встановлення змін у поведінці, які можуть бути індикаторами невідомої загрози. QRadar User Behavior Analytics аналізує діяльність користувачів, щоб виявити зловмисних інсайдерів і визначити, чи були скомпрометовані облікові дані користувача. Аналітики безпеки можуть легко бачити ризикованих користувачів, переглядати їх аномальні дії та детально вивчати основні дані журналу та потоку,

які внесли свій вклад в оцінку ризику користувача.

За бажанням, використовуючи QRadar Network Insights як частину розгортання SIEM, організації можуть отримати уявлення про те, які системи спілкувалися одна з одною, які програми були задіяні та якою інформацією обмінювалися в пакетах. Зв'язуючи цю інформацію з іншими даними мережевими, журнальними та користувачами, аналітики з безпеки можуть виявити ненормальну мережеву активність, яка може свідчити про скомпрометовані хости, скомпрометованих користувачів або спроби ексфільтрації даних.

Хоча IBM QRadar SIEM постачається з численними правилами виявлення аномалій і поведінки в якості налаштувань за замовчуванням, групи безпеки також можуть створювати власні правила, налаштовувати параметри виявлення аномалій і завантажувати понад *265 попередньо створених додатків із IBM Security App Exchange, щоб розширити їхнє розгортання.*

Скоротіть час на розслідування за допомогою штучного інтелекту та автоматизації. Команди безпеки обтяжені великою кількістю сповіщень, ручними завданнями та обмеженим персоналом, що часто призводить до вигорання та ослаблення позиції безпеки організації.

QRadar Advisor with Watson використовує штучний інтелект та автоматизацію, щоб значно скоротити час, витрачений на розслідування повідомлень про загрози з 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 MITRE ATT&CK для покращення аналізу першопричин. Це забезпечує швидке виправлення, коротший час затримки, менше пропущених критичних інцидентів, меншу втому аналітика та покращує ефективність SOC.

IBM QRadar SIEM групує та визначає пріоритети всіх пов'язаних подій під одним злочином, надаючи аналітикам безпеки повне уявлення про потенційно розвивається сценарій атаки. Аналіз перехресного розслідування забезпечує

багатий контекст сповіщень, автоматично пов’язуючи розслідування із пов’язаними інцидентами, що зменшує дублювання зусиль і розширює розслідування за межі поточного ймовірного інциденту та попередження. Крім того, Advisor with Watson забезпечує комбінацію когнітивних ідей та локального аналізу даних, призначених для виявлення пов’язаних індикаторів компромісу (IoC). IBM QRadar SIEM може відображати діаграми взаємовідносин у межах розслідування, щоб візуалізувати збагачені дані розслідування та досліджувати зв’язки з іншими IoC, активами, користувачами або розслідуваннями.

Інтеграція IBM Security QRadar з IBM Security SOAR дозволяє командам безпеки прискорювати час реагування на інциденти за допомогою покрокових посібників, автоматизації ручних завдань, а також послідовної співпраці та координації з управлінням справами. Аналітики з безпеки можуть швидко та ефективно передати підозрювані порушення від IBM QRadar SIEM до IBM Security SOAR, ініціювати додаткові автоматизовані збагачення та керувати повним процесом розслідування. У міру розвитку інциденту вся інформація синхронізується між IBM QRadar SIEM і IBM Security SOAR, що забезпечує повну цілісність даних. Будь-яка нова інформація, виявлена IBM Security SOAR, повертається в IBM QRadar SIEM для покращення процесу виявлення.

Отже, IBM Security QRadar це лідируюче на ринку рішення SIEM, яке застосовує автоматизовану інтелектуальну аналітику до величезної кількості даних безпеки, щоб надати аналітикам безпеки оперативне уявлення про найбільш критичні загрози, дозволяючи їм приймати кращі та швидші рішення щодо сортування та реагування.

Це комплексне рішення об’єднує управління журналами, мережевий аналіз, аналіз поведінки користувачів, аналіз загроз і дослідження на основі штучного інтелекту в єдине рішення – інтегроване з IBM Security SOAR для реагування на інциденти. Це забезпечує повну видимість у локальних, хмарних та гібридних середовищах.

2.2. Визначення можливостей щодо візуалізації стану безпеки корпоративної інформаційної системи на прикладі IBM QRadar Pulse

Додатки, які розширюють функціональність IBM QRadar SIEM, можна завантажити та встановити з IBM Security App Exchange. IBM Security App Exchange – це центр спільного доступу на основі спільноти, який ви використовуєте для спільного використання програм між продуктами IBM Security.

Користуючись додатками з IBM Security App Exchange, ви можете використовувати швидко зібрані інноваційні робочі процеси, візуалізації, аналітику та варіанти використання, які упаковані в програми для задоволення конкретних вимог безпеки. Щоб виявити загрози та усунути їх, ви можете використовувати компоненти безпеки від кореляції в реальному часі та моделювання поведінки до користувацьких відповідей та довідкових даних. Прості у використанні рішення розробляються партнерами, консультантами, розробниками для вирішення ключових проблем безпеки [7].

Розглянемо робочий процес додатків IBM QRadar SIEM. Додатки IBM QRadar SIEM створені розробниками. Після того, як розробник створює додаток, IBM сертифікує та публікує її в IBM Security App Exchange. Адміністратори IBM QRadar SIEM можуть переглядати та завантажувати програми, а потім встановлювати програми в IBM QRadar SIEM, щоб відповідати конкретним вимогам безпеки.

На рис. 2.3. показано робочий процес для програми та роль, яка зазвичай відповідає за роботу.

Встановлення додатку у середовищі з кількома клієнтами. IBM QRadar SIEM версії 7.4.0 і пізніших версій включає підтримку додатків із кількома клієнтами. У середовищі з багатьма клієнтами можна використовувати ряд готових додатків, таких як Pulse, Assistant і Log Source Management. Розробники також можуть створювати та тестувати додатки, які підтримують багато користувальницьке середовище. Щоб інсталювати додатки в середовищі з

кількома клієнтами, використовується програма QRadar Assistant (рис. 2.4).

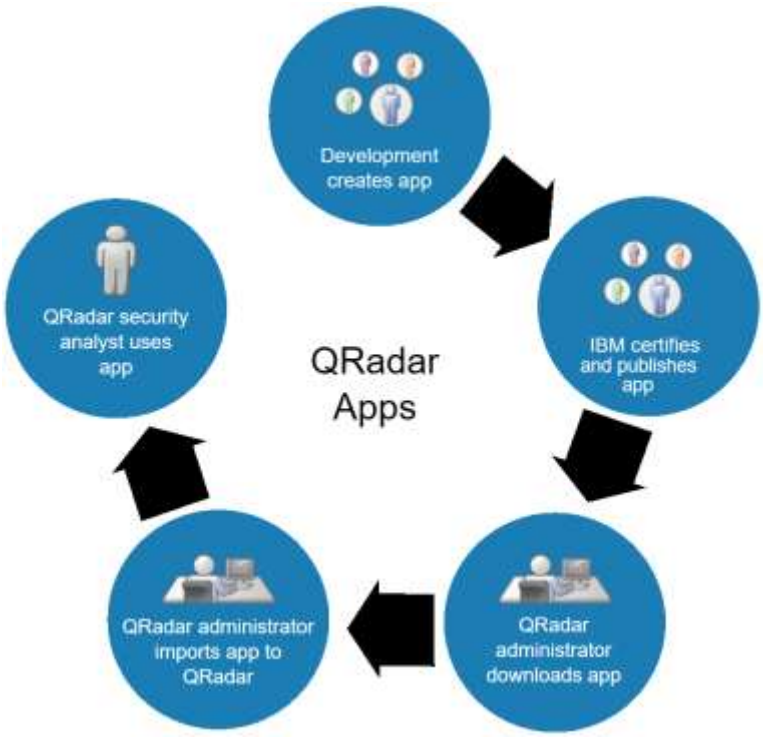

Рис. 2.3. Робочий процес додатка IBM QRadar SIEM [7]

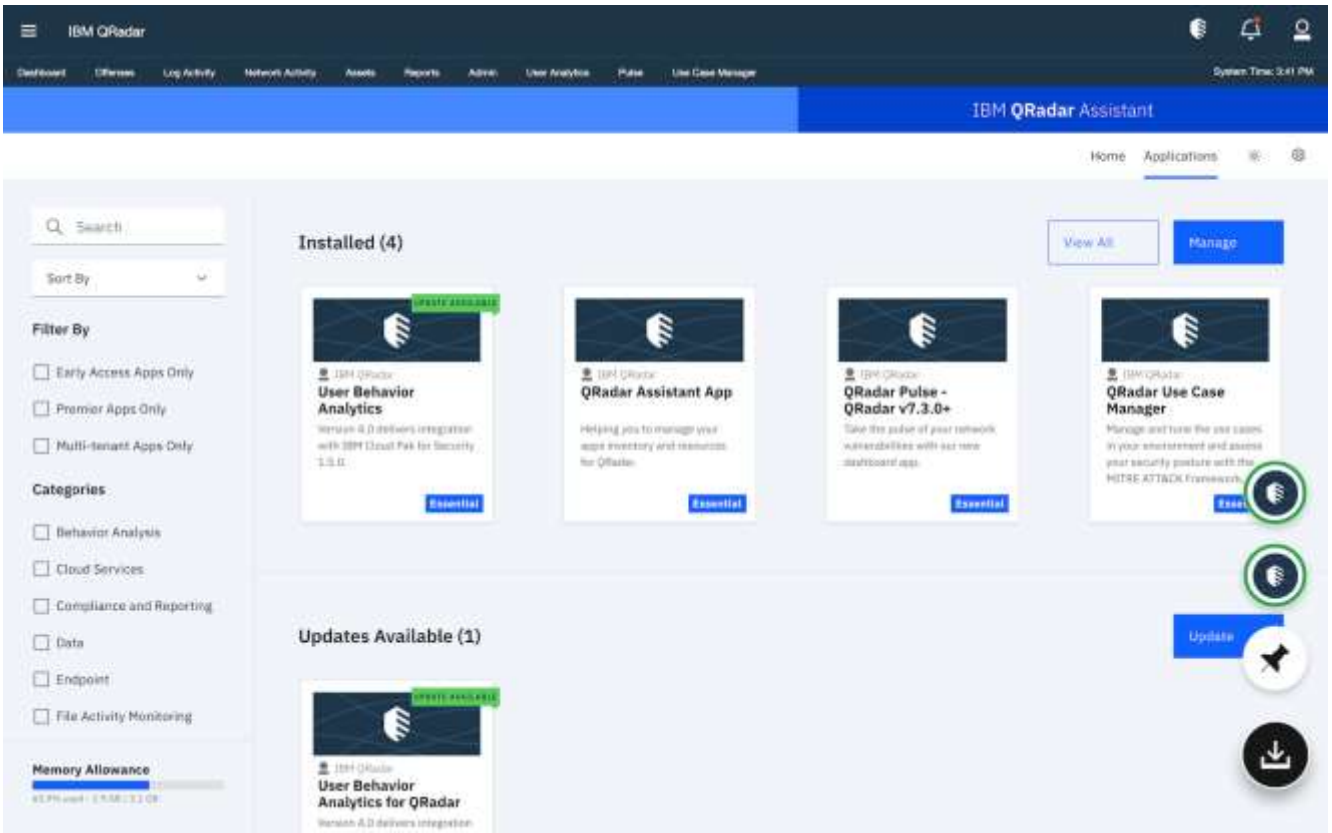

Рис. 2.4. Інтерфейс QRadar Assistant

Програмний комплекс IBM QRadar Pulse підвищує можливості SIEM

системи IBM QRadar SIEM та за допомогою динамічних інформаційних панелей у реальному часі забезпечує видимість SOC, які надають змістовне уявлення про крпоративну систему безпеки та ландшафт загроз.

Програмний комплекс IBM QRadar Pulse є засобом візуалізації порушень, мережевих даних, загроз, шкідливої поведінки користувачів і хмарного середовища з усього світу на географічних картах і діаграмах, що автоматично оновлюються. Він надає можливість імпортувати та експортувати інформаційні панелі, щоб поділитися ними з колегами. Можна поділитися посиланнями на інформаційну панель з колегами, щоб гарантувати, що вони отримають будь-які оновлення.

IBM QRadar Pulse надає швидкий огляд поточного середовища безпеки на одному дисплеї або на кількох дисплеях у корпоративному центрі безпеки (рис. 2.5 – 2.8) [8].

Рис.2.5. Інформаційна панель QRadar Pulse Summary view

QRadar Pulse має наступні ключові можливості [8]:

використання попередньо визначених інформаційних панелей, а також можна створити власну;

імпорт та експорт інформаційних панелей або можна поділитися

посиланнями на інформаційну панель з колегами;

створення елементів інформаційної панелі на основі запитів AQL, порушень IBM QRadar SIEM або за допомогою загального API для доступу до повного діапазону даних з IBM QRadar SIEM або його програм;

налаштування свого дисплея за допомогою тем і гнучкого макета приладової панелі;

розгортання елементів інформаційної панелі для відображення в багато екранному SOC;

створення унікальних інформаційних панелей для відстеження та передачі інформації та аналізу корпоративної мережі;

дослідження статистики, перейшовши до панелі інструментів Pulse, URL-адреси або певної сторінки у програмі, що викликає (IBM QRadar SIEM або QRadar Analyst Workflow). Призначення порогів для великих чисел, часових рядів, табличних і географічних діаграм;

збереження елементів інформаційної панелі без результатів;

переходи до зовнішньої веб-сторінки, до іншої сторінки IBM QRadar SIEM, до будь-якої інформаційної панелі Pulse або до QRadar Analyst Workflow із табличних, кругових, стовпчастих діаграм і діаграм з великими числами.

Рис. 2.6. Інформаційна панель System Metrics

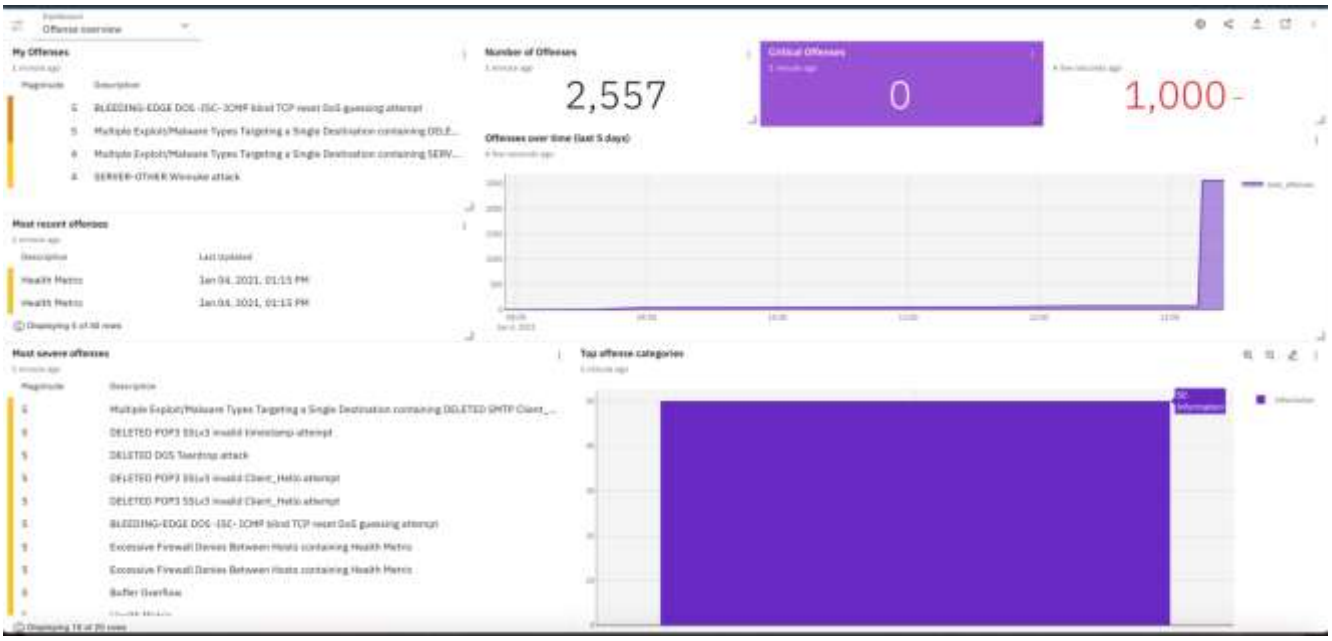

Рис.2.7. Інформаційна панель Огляд порушень

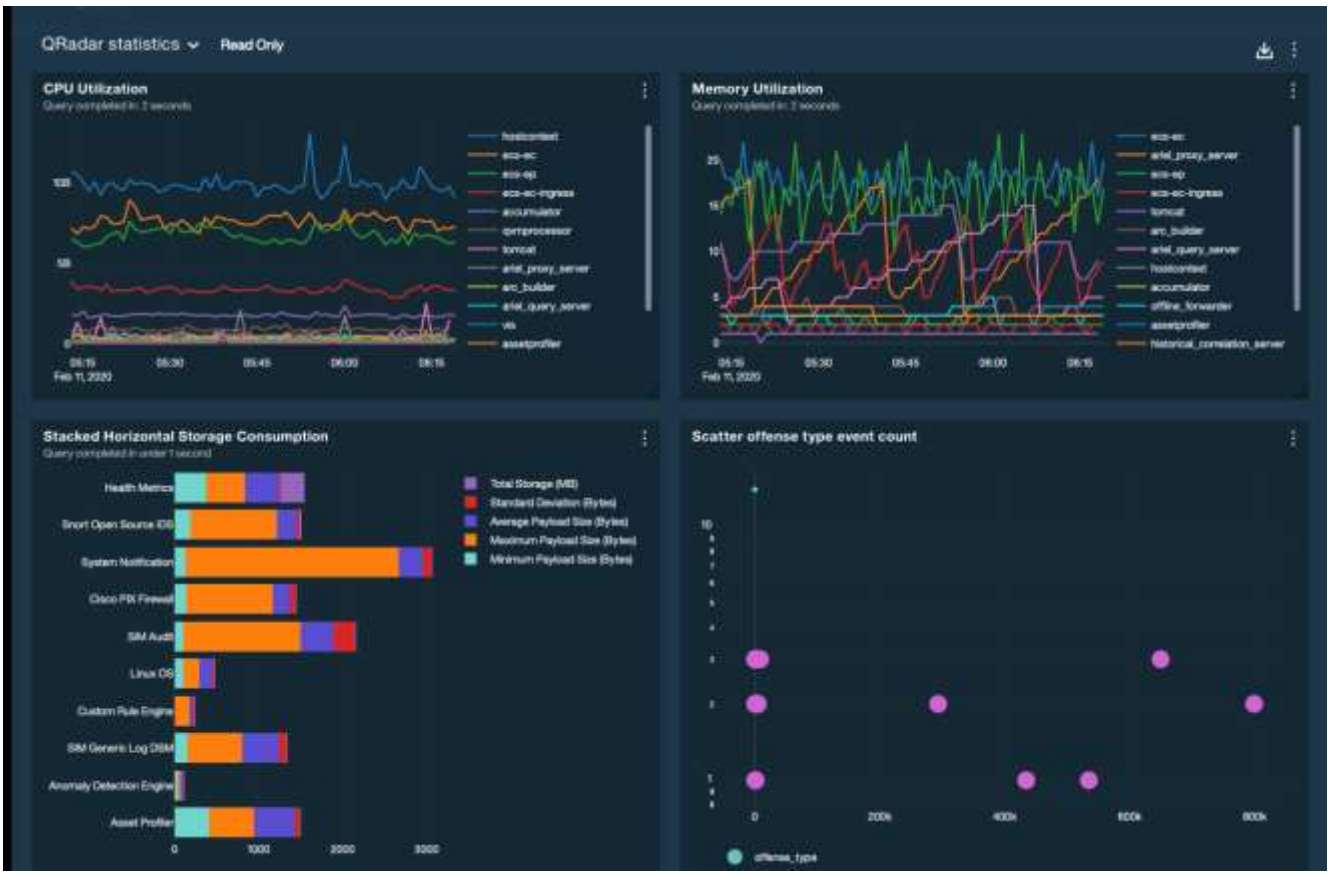

Рис.2.8. Інформаційна панель QRadar statistics

Робоча область IBM QRadar Pulse містить інформаційні панелі та віджети. Вони використовуються, щоб створити перелік унікальних інформаційних

панелей для відстеження даних про безпеку та операційні дані кінцевої точки, користувачів, хмари, відділу та всієї компанії [10].

Робочі простори. Ваша робоча область – це те, що ви бачите, коли клацнете вкладку Pulse на консолі IBM QRadar SIEM. Лише ви можете бачити свою робочу область, але ви можете надати спільний доступ до інформаційних панелей з колегами або розгорнути певні інформаційні панелі на монітор на стіні SOC. Створіть параметри AQL для робочого простору, які спрощують створення елементів інформаційної панелі AQL та одночасно оновлювати кілька запитів AQL [10].

На рис. 2.9 показано робоче середовище за замовчуванням на інформаційній панелі Огляду порушень.

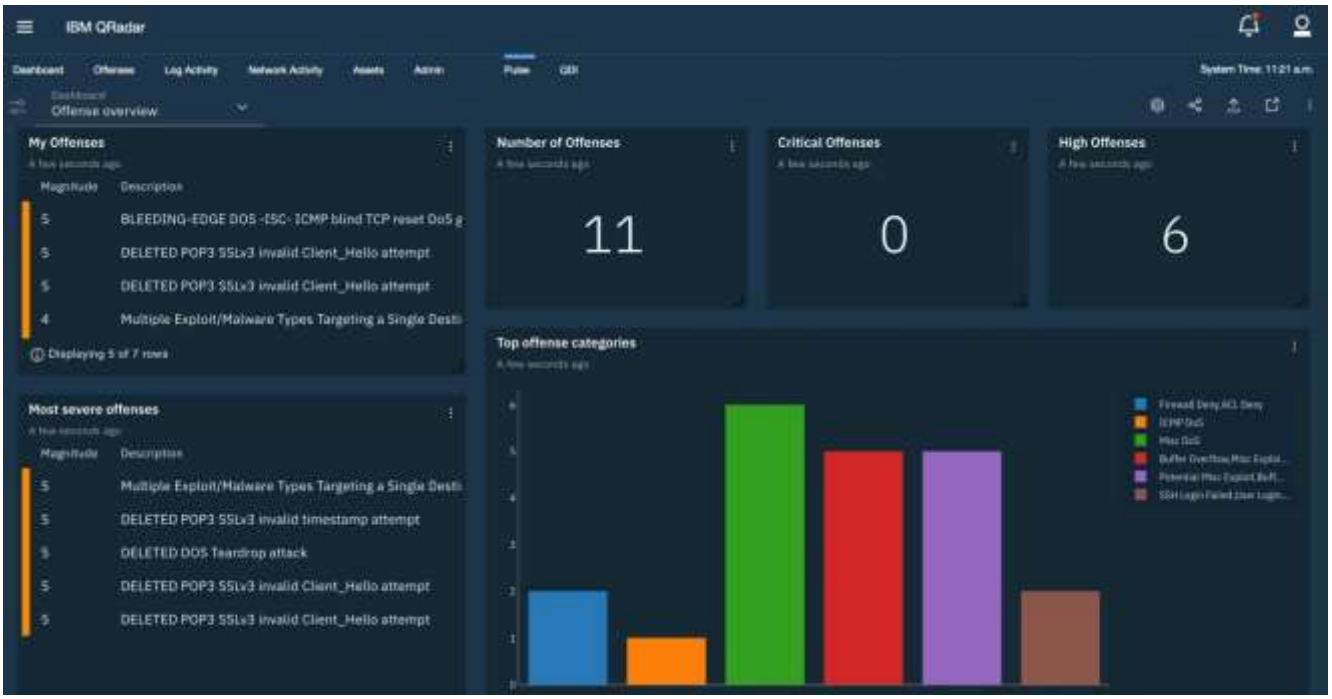

Рис.2.9. Інформаційна панель Offense overview

Шаблони інформаційної панелі. Використовуються шаблони інформаційної панелі за замовчуванням у QRadar Pulse як відправну точку для створення власного персоналізованого інвентарю інформаційної панелі для вашого робочого простору. Кожен шаблон інформаційної панелі пропонує кілька різних елементів інформаційної панелі, які ви можете додати до різних інформаційних панелей.

Видаліть елементи інформаційної панелі, які не стосуються вашої організації [10].

Інформаційні панелі QRadar Pulse отримують свої дані від IBM QRadar SIEM, тому деякі з них можуть відображати дані, такі як інформаційна панель метрик подій і потоків, безпосередньо залежно від того, як ви налаштували IBM QRadar SIEM для отримання даних. Інші інформаційні панелі QRadar Pulse необхідно відредагувати, щоб дані відображалися на діаграмах.

Інформаційні панелі. Інформаційні панелі містять віджети, які відстежують і відображають події безпеки та проблеми, важливі для вашої організації. Наприклад, інформаційна панель огляду порушень (рис. 2.9) містить віджети, які відстежують основні категорії правопорушень, найважчі правопорушення тощо.

Можна створити власні інформаційні панелі відповідно до потреб вашої організації та мережі. Можна додати віджети з інших шаблонів інформаційної панелі або створити власні. Можна відкривати посилання на інформаційну панель або імпортувати інформаційні панелі, якими вам поділилися колеги, щоб усунути необхідність повторного створення наявного вмісту.

Віджети. Віджети містять джерело даних (AQL, порушення IBM QRadar SIEM, динамічний пошук або загальний API) і одну або кілька діаграм. Ви можете додати більше діаграм у вигляді різних переглядів, наприклад кругової або стовпчастої діаграми. Наприклад, віджет «Події користувача» на інформаційній панелі «Різні показники» може відображатися у вигляді кругової або стовпчастої діаграми. Перегляд гістограми порівнює набори даних між групами, наприклад імена користувачів та кількість подій на користувача. Подання кругової діаграми відображає ту ж інформацію, але у відсотках.

Параметри. Параметри полегшують створення віджетів шляхом повторного використання загальних елементів у кількох запитах AQL або Generic API. Вам більше не потрібно створювати окремі запити для подібних об’єктів. Будь-який запит, який використовує параметр, може автоматично використовувати значення параметра.

IBM QRadar Pulse надає багато типів діаграм для представлення ваших даних у спосіб, який є значущим для вашої організації.

Гістограма. Можна порівнювати набори даних між групами; наприклад, ідентифікатор джерела журналу та частота подій. Можна показати значні зміни в даних з часом. Можна скласти кожну серію. Можна показати або приховати легенду та розташувати її горизонтально або вертикально на діаграмі.

Діаграма великих чисел. Можна відображати важливі показники на табло SOC, які ви хочете, щоб ваша команда контролювала. Увімкніть тенденцію, щоб побачити, як ваша організація працює з часом.

Географічна діаграма даних. Можна спостерігати, де відбуваються події на хороплетній (заштрихованій) карті або на карті розсіювання. Встановіть широту, довготу та масштаб для IP-адрес. Відображення рядків між маркерами IP джерела та призначення.

Кругова діаграма. Використовуйте для представлення чисел у відсотках або для візуалізації частин зв’язку чи композиції. Показ у формі пончика. Відображення значення скибочки круга у відсотках або число. Можна показати або приховати легенду та розташувати її горизонтально або вертикально на діаграмі.

Точкова діаграма. Використовуйте точкові діаграми, щоб досліджувати кореляції між різними показниками. Точкові діаграми використовують точки даних для побудови двох показників у будь-якому місці шкали, а не лише на звичайних галочках.

Таблиця відображення діаграми. Можна відобразити всі стовпці або лише вибрані. Використовуйте, коли у вас є більше одного набору значень, які мають прямий зв’язок.

Графік часових рядів. Використовуйте для відображення тенденцій або порівнянь. Увімкніть діаграми площ, щоб відображати дані за певний час. Виберіть одну з кількох форм ліній або режимів ліній для кожного значення.

2.3. Аналіз можливостей візуалізації кіберінцидентів в середовищі IBM QRadar Pulse

Графіки часових рядів у QRadar Pulse. На перший погляд створення діаграми часового ряду з реляційних даних у QRadar Pulse може бути складним. Обсяг даних, який повертає запит AQL, може бути громіздким, але з деякими базовими знаннями та ретельним плануванням можна створити релевантні та значущі діаграми часових рядів [10].

Упорядкування показника за часом початку дає часові ряди, як наведений нижче запит AQL (рис. 2.10), але кількість повернених даних може бути громіздкою для роботи та розуміння.

```
select starttime as 'Start Time',
SUM(eventcount) as 'Event Count (Sum)'
from events
where eventcount <> NULL
GROUP BY starttime
order by starttime
LAST 60 minutes
```

Рис. 2.10. запит AQL [10]

Обсяг повернених даних може призвести до зашумленої діаграми, яка не надає багато інформації. Час початку події може не відбуватися через регулярні проміжки часу, що може створити прогалини в наборі даних. На рисунку 2.11 показано як виглядає занадто багато даних, що призводить до шумних результатів.

Розглянемо створення інтервалів у запиті часового ряду. Першим кроком є визначення типу інтервалу, який використовуватиметься для аналізу даних. Якщо Ви хочете дивитися на дані з вузького інтервалу, наприклад кожну секунду або з більшими інтервалами щохвилини чи щогодини – це рішення важливе, оскільки точки даних повинні бути згруповані в інтервали, щоб обчислювався показник.

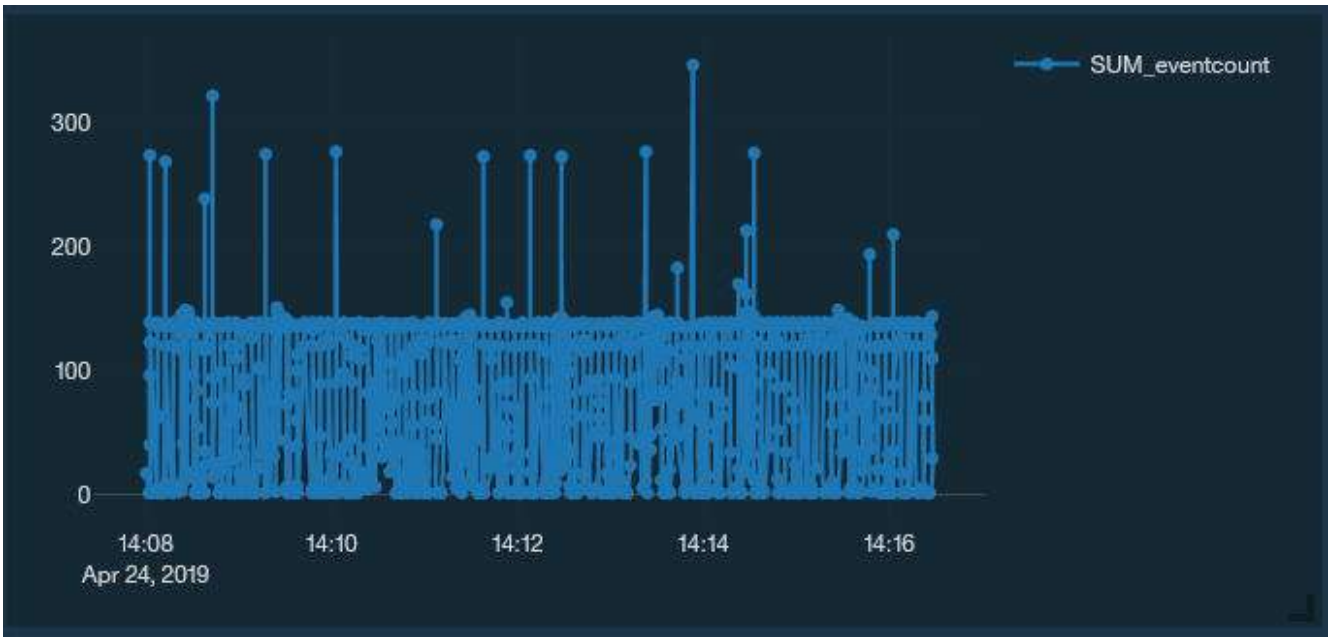

Рис. 2.11. Занадто багато даних призводить до шумних результатів

Використовуючи вихідний запит, ви можете згрупувати дані за допомогою одного з таких прийомів:

Використання пропозиції GROUP BY для створення інтервалу: GROUP BY starttime/60000. Оскільки час початку відображається в мілісекундах, якщо розділити на 60 000 (60 секунд x 1000 мілісекунд), ви створите групи або інтервали по 60 секунд (1 хвилина).

Зміна речення ORDER BY для використання агрегатного sTime. Запит змінюється на такий код на рис. 2.12.

```
select starttime as 'sTime',
SUM(eventcount) as 'Event Count (Sum)'
from events
where eventcount > 0
GROUP BY starttime/60000
order by "sTime"
LAST 60 minutes
```

Рис. 2.12. Використання агрегатного sTime у запиті AQL

Дані тепер більш візуально споживані і гарантують, що одна точка даних відбувається кожну хвилину. Тепер, коли інтервали правильно визначені, ви можете використовувати кілька стратегій для форматування даних у більш

зручний формат часових рядів.

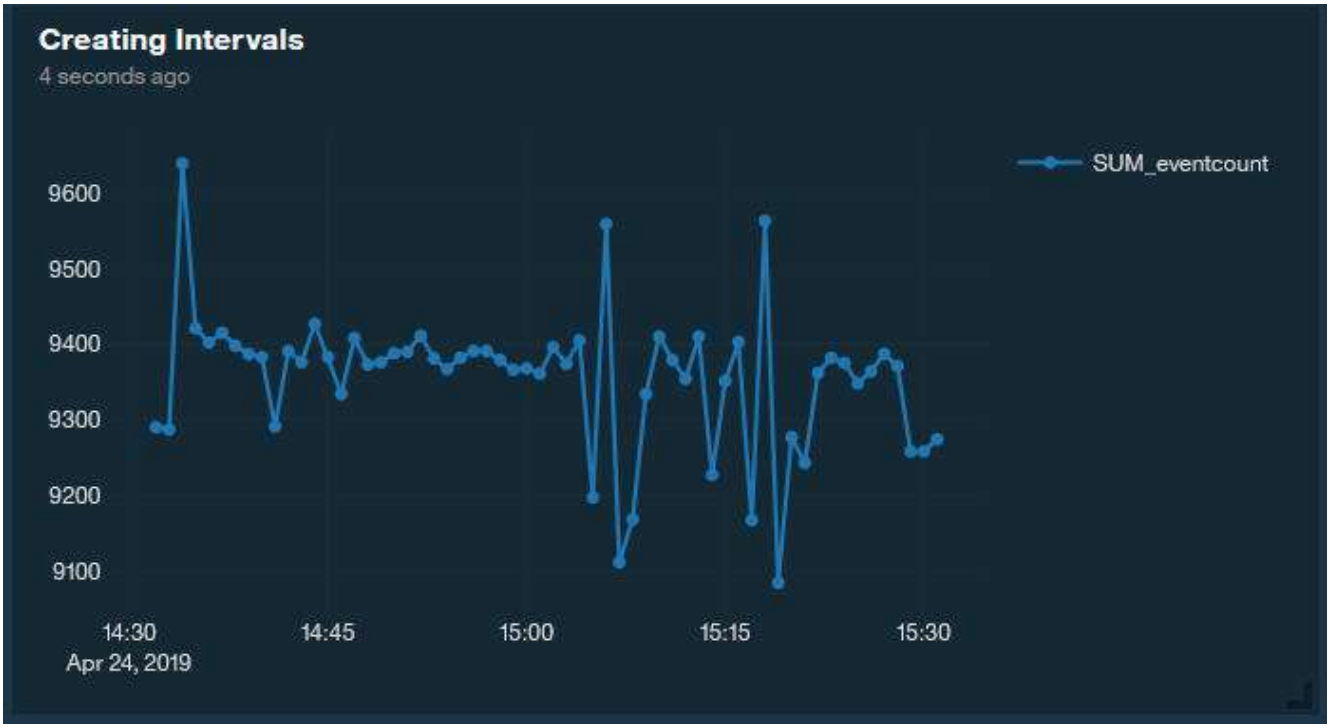

Рис. 2.13. Більше витратних результатів даних із правильно визначеними інтервалами

Отже, застосування запитів AQL в QRadar Pulse дозволяє отримати потрібні результати для візуалізації даних щодо кіберінцидентів.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ВИДИМОСТІ СТАНУ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи

Розглянемо варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи на прикладі інтеграції рішення IBM QRadar Pulse з системою IBM QRadar SIEM.

Необхідно застосувати додаток IBM QRadar Assistant (рис. 3.1), щоб встановити архів програми IBM QRadar Pulse на свій комп'ютер IBM QRadar SIEM.

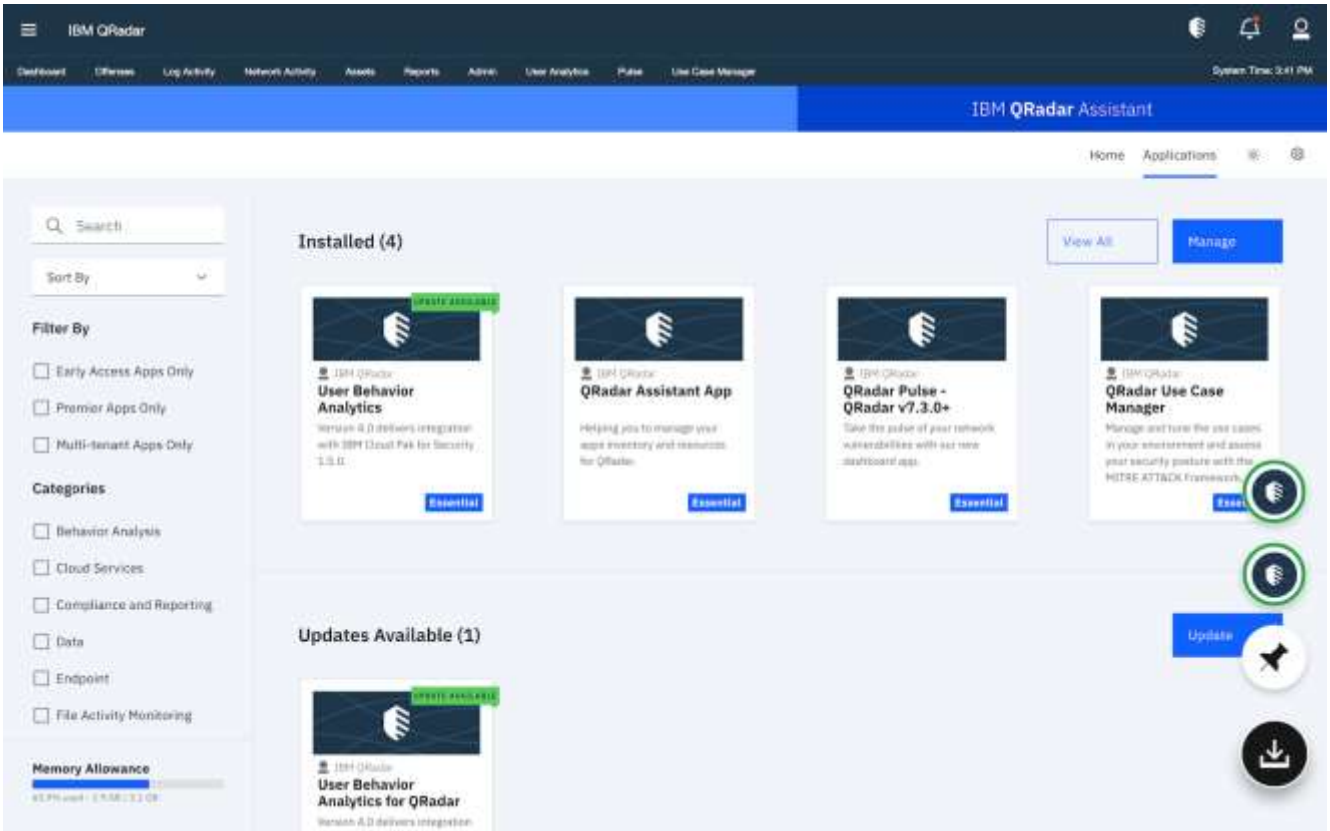

Рис. 3.1. Інтерфейс QRadar Assistant

Перш ніж встановити додаток, необхідно переконатися, що IBM QRadar SIEM відповідає мінімальним вимогам до пам’яті (RAM). QRadar Pulse вимагає 350 МБ вільної пам’яті з пулу пам’яті програми. Якщо QRadar Pulse не вдається встановити, це означає, що у вашому пулі програм недостатньо вільної пам’яті для запуску програми. Подумайте про те, щоб додати хост програми до свого розгортання IBM QRadar SIEM.

IBM QRadar SIEM V7.3.2 або новішої версії використовує App Host, який є керованим хостом, який призначений для запуску програм. Хости додатків надають додаткове сховище, пам’ять і ресурси ЦП для ваших програм, не впливаючи на обробну здатність вашої консолі IBM QRadar SIEM.

Порядок розгортання.

1. Виберіть один із наступних способів завантаження програми:

Якщо програму IBM QRadar Assistant налаштовано на IBM QRadar SIEM, скористайтеся інструкціями для встановлення QRadar Pulse;

Якщо додаток QRadar Assistant не налаштовано, завантажте архів програми QRadar Pulse із IBM Security App Exchange (https://apps.xforce.ibmcloud.com/) на локальний комп’ютер. Для доступу до App Exchange необхідно мати ідентифікатор IBM.

2. Якщо ви завантажили програму з App Exchange, виконайте такі дії:

На консолі IBM QRadar SIEM натисніть Адміністратор > Керування розширеннями.

У вікні керування розширеннями натисніть кнопку Додати та виберіть архів програми, який потрібно завантажити на консоль.

Установіть прапорець Установити негайно.

Необхідно зачекати кілька хвилин, перш ніж програма стане активною.

Щоб попередньо переглянути вміст програми після її додавання та до встановлення, виберіть її зі списку розширень і натисніть Додаткові відомості. Розгорніть папки, щоб переглянути окремі елементи вмісту в кожній групі.

3. Після завершення інсталяції очистіть кеш браузера та оновіть вікно браузера, щоб побачити вкладку Pulse.

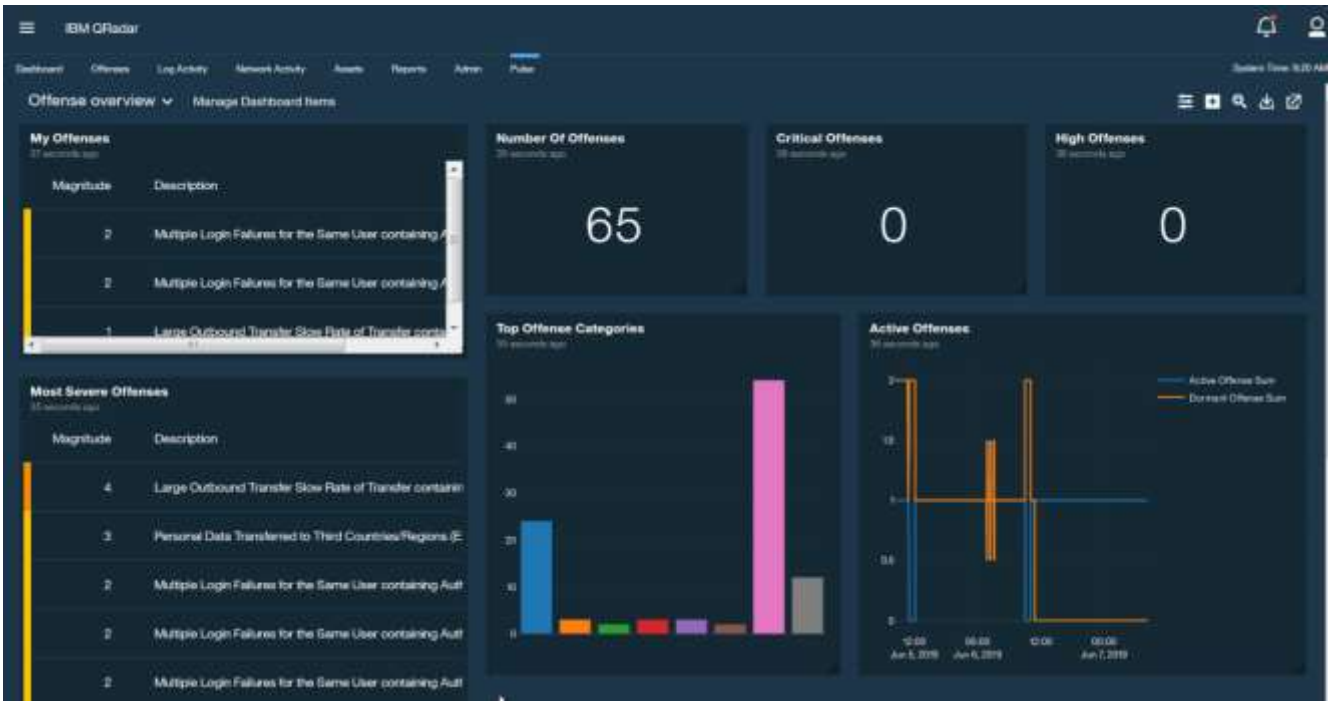

Рис. 3.2. Вкладка Pulse в IBM QRadar SIEM

Після встановлення QRadar Pulse додаток відображається як можливість на сторінці «Ролі користувачів» на вкладці «Адміністратор». Щоб використовувати додаток, адміністратор IBM QRadar SIEM повинен призначити додаток та будь-які інші необхідні можливості ролі користувача.

3.2. Рекомендації щодо забезпечення видимості стану безпеки корпоративної інформаційної системи

Рішення SIEM постійно розвиваються протягом останніх років, щоб відповідати постійно мінливому ландшафту загроз кібербезпеці. Рішення SIEM мають на меті надати аналітикам всю необхідну інформацію та контекст, які їм потрібні, щоб визначити природу атаки, ступінь її складності та поширення всередині мережі. Щоб ефективно стримувати збитки від порушення безпеки та ефективно реагувати, аналітикам потрібна правильна інформація в потрібний час [11].

Сьогодні для організацій будь-якого розміру все ще залишається серйозним завданням задовольнити необхідні оперативні, аудиторські та безпекові потреби.

Оскільки мережі стають дедалі складнішими, кількість пристроїв для моніторингу значно зросла. Аналітики буквально переповнені даними. Через це об'єднання цих різних джерел даних SIEM стало проблемою саме по собі. *Ці значні обмеження фреймворку ускладнюють життя аналітиків. У них забагато даних, але недостатньо інформації. Існує реальна потреба зменшити масштаб і складність аналізу до більш зрозумілого рівня, щоб аналітики могли знайти відповідні рішення для підвищення загальної безпеки.*

Тому, перша рекомендація – широке застосування розширених рішень для візуалізації даних.

На даний момент рішення SIEM широко містять інструменти візуалізації даних. Але вони, іноді, не ефективні в обробці таких великих обсягів даних і не пропонують можливості виявлення та дослідження шаблонів у реальному часі. *Зараз більшість компаній, які покладаються на рішення візуалізації даних SIEM, використовують їх лише для ілюстрацій, а не для аналізу.* Їм часто доводиться покладатися на зовнішні служби для проведення криміналістичної експертизи після нападу, оскільки ці операції вимагають багато навичок і часу.

Використання візуалізації графічних даних вирішує цю проблему і ефективність роботи SIEM систем.

Сьогодні тенденція у світі кібербезпеки для вирішення цих проблем полягає в переході від традиційної системи сховища даних до більш гнучкої та масштабованої серверної частини даних. Це дає змогу використовувати нові інструменти, такі як рішення для аналізу візуалізації графіків. Зазвичай ці нові серверні програми мають форму сховища, в якому зберігається велика кількість напівструктурованих, структурованих та неструктурованих даних, які поєднуються з іншими сервісами, такими як бази даних графіків та інші інструменти аналітики.

Сховища напівструктурованих, структурованих та неструктурованих даних мають багато переваг у порівнянні зі централізованими сховищами даних, коли справа доходить до керування терабайтами журналів безпеки – централізація, гнучкість, оперативність і висока масштабованість. *Компанії мають серйозно*

ставитися до використання нових аналітичних додатків, які розширюють можливості своїх SIEM систем.

Після того, як дані SIEM централізовано в сховищі даних, використання рішення для візуалізації графічних даних та дослідження даних надає аналітикам реальну додаткову цінність для їх повсякденних операцій. Вони працюють у режимі реального часу, можуть миттєво візуалізувати дані та можуть проводити точний аналіз криміналістики після атаки набагато простішими способами, ніж будь-коли раніше. Виявлення підозрілих моделей активності може бути значною мірою автоматизовано за допомогою алгоритмів розпізнавання образів. Таким чином, аналітики можуть зосередитися на дослідженні підозрілої діяльності візуально.

Візуалізація розширює можливості для аналітиків, оскільки вона значною мірою вирішує проблему наявності великої кількості даних для інтерпретації. Візуалізація значно зменшує масштаб і складність аналізу. Це також дозволяє компаніям проводити більшу частину свого криміналістичного аналізу всередині. Завдяки розширеним функціям візуалізації даних аналітики можуть працювати разом, обмінюватися візуалізаціями та керувати правами доступу користувачів до даних. Нарешті, розширені можливості налаштування, які пропонують засоби візуалізації, дозволяють його інтегрувати у внутрішні системи безпеки та підвищити їх видимість.

Керування даними в контрольований спосіб. 84% професіоналів з кібербезпеки сказали, що великі дані допомогли їм блокувати атаки. Половина групи, однак, сказала, що найбільшою проблемою для них є величезний обсяг зібраних даних [12].

Візуалізація загроз вирішує цю проблему.

У міру розвитку загроз розвивалися і засоби захисту. У минулому фахівці не мали достатньої інформації чи даних, щоб належним чином передбачити, розпізнати та запобігти загрозам. Сьогодні є багато інформації. Найскладніше – це проаналізувати дані, щоб побачити закономірності та тенденції, які вказують на те, що може бути проблема безпеки.

Перегляд даних вручну займає багато часу і може стати занадто рутинним. Легко пропустити попереджувальні сигнали. Налаштування фільтрів, пасток і сповіщень може допомогти, але це все одно вимагає від фахівця зайти в джерело даних і проаналізувати його на наявність проблем. Візуалізація дозволяє дуже легко побачити шаблони.

За можливості, треба широко застосовувати засоби візуалізації даних, які відображають стан безпеки систем.

Найкращий підхід – використовувати інструменти аналітики, щоб наочно продемонструвати ваш поточний стан і порівняти його з історичними даними. Це забезпечує візуальний образ, який дозволяє швидко визначити аномалії. Замість того, щоб переглядати дані, візуалізація даних дає вам швидкий і легкий для визначення спосіб побачити, коли щось не так. Ви швидше помітите підозрілу активність і зможете негайно перейти до точних даних, щоб перевірити їх.

Візуалізація даних за допомогою інструментів аналітики також значно зменшує безлад, який може надходити з різних джерел даних. Фахівці SOC можуть використовувати журнали, сповіщення про небезпеку, нотіфікації та різне програмне забезпечення безпеки як частину схем моніторингу та захисту. Ваше програмне забезпечення для аналітики стає центральним пунктом для сортування даних та їх кращої міжплатформної організації – навіть у різних географічних районах або місцях.

Оскільки настроювані дані дуже легко налаштовуються, то і легко налаштувати екран моніторингу, щоб показувати саме те, що ви хочете і потребуєте. Це дозволяє командам з безпеки візуалізувати дані так, як це є для них найбільш доцільним, і діяти швидше, коли виявлено проблему.

Коли відбувається порушення даних або проблеми з безпекою, час має важливе значення. Чим швидше ви зможете розпізнати проблему, тим більше у вас шансів пом’якшити її. Наприклад, атака програми-вимагача може швидко поширитися по організації. Вона може початися з одного шкідливого файлу, але потім шукати та заражати підключені сервери та інші кінцеві точки. Швидке виявлення атаки може дозволити вам відключити інші сервери чи пристрої та

захистити їх.

Чим довше загроза залишається непоміченою, тим більше збитків буде завдано. Візуалізуючи поширення зловмисного програмного забезпечення, ви можете швидше оцінити вразливості та вжити швидких заходів.

У сучасному бізнес-середовищі ми маємо більше векторів загроз, ніж будь-коли. Компанії ведуть більше бізнесу в хмарі, ніж будь-коли раніше. З'єднання сторонніх розробників, SaaS та хмарна інфраструктура створюють різні точки атаки для зловмисників. Поширення пристроїв IoT також збільшує вразливість.

Пристрої BYOD і збільшення кількості співробітників, які працюють вдома, дають учасникам загрози численні можливості атакувати пристрої компанії, що не контролюються, отримати доступ, а потім використовувати вкрадені облікові дані для доступу до корпоративних мереж. Крім усього цього, у вас також є співробітники, які підключаються до загальнодоступних Wi-Fi і точок доступу. Якщо співробітники не використовують найкращі методи для безпечного підключення до загальнодоступних Wi-Fi або точок доступу – ви стаєте жертвою зловмисників.

Традиційні методи моніторингу, використання електронних таблиць, звітів або модульних інструментів GRC (Governance, Risk, and Compliance) не будуть ефективними. Інструменти візуалізації даних показують вам працездатність мережі з першого погляду.

Звіти залишаться важливими, коли щось буде виявлено, і вам потрібно точно з'ясувати, що відбувається. Вони також корисні після факту, щоб знайти першопричини та визначити потенційні точки порушення, які потребують уваги. Однак у даний момент вам потрібен спосіб негайно побачити, що є проблема. Ось тут у гру вступає панель даних.

Інформаційна панель даних показує єдине представлення вашого контролю кібербезпеки в одному місці, щоб забезпечити миттєву оцінку вашої безпеки. Інформаційна панель даних допомагає зрозуміти складні дані, розпізнаючи закономірності та позначаючи важливі події.

Забезпечуючи візуальний спосіб показати ключові індикатори ризику та

дізнатися, чи є проблема, лише поглядом. Оскільки ви можете миттєво визначити, чи є проблема, візуалізація даних також дає командам безпеки більше спокою. Постійне нагадування про те, що ваша мережа працює так, як має бути, і все добре. Коли виникає проблема, вона вискакує, щоб ви могли діяти.

Найкращі інструменти візуалізації даних також використовують AI та машинне навчання. У міру збору даних і появи шаблонів програмне забезпечення розширить свої передбачувані можливості, щоб забезпечити навіть раннє попередження.

ВИСНОВКИ

В роботі проаналізовано призначення та умови функціонування центру управління кібербезпекою. SOC – це команда, що складається в основному з аналітиків з безпеки, організованих для виявлення, аналізу, реагування на інциденти кібербезпеки, звітування про них та запобігання.

В роботі проведено дослідження та аналіз проблеми моніторингу стану кібербезпеки інформаційної системи. Використання та аналіз великої кількості даних, що стосуються безпеки, вимагає візуалізації стану безпеки корпоративної інформаційної системи як шляху забезпечення її високої видимості.

Досліджено існуючі методи та засоби забезпечення видимості стану безпеки корпоративної інформаційної системи. Для SOC практика отримання ситуаційної обізнаності щодо стану кібербезпеки ділиться на три складові: інформація, аналітика та візуалізація. Зазначається, що у сфері ситуаційної обізнаності щодо стану кібербезпеки візуалізація все ще знаходиться на початковому етапі. Незважаючи на те, що була проведена велика робота в області візуалізації кібербезпеки, здається, не існує універсальної практики візуалізації інформації щодо кібербезпеки.

IBM QRadar SIEM, лідируюче на ринку рішення SIEM, допомагає захиститися від зростаючих загроз, одночасно модернізуючи та масштабуючи операції безпеки за допомогою інтегрованої видимості, виявлення, дослідження та реагування. IBM QRadar SIEM надає командам з безпеки централізований доступ до даних безпеки в масштабах підприємства та оперативне уявлення про найбільш пріоритетні загрози.

Перш ніж групи безпеки зможуть розпочати аналіз даних для виявлення загроз і керування ними, вони повинні мати централізовану видимість різних даних безпеки. IBM QRadar SIEM дозволяє організаціям отримати централізовану, всеосяжну видимість ізольованих середовищ, збираючи, аналізуючи та нормалізуючи дані журналів і потоків.

Програмний комплекс IBM QRadar Pulse є засобом візуалізації порушень, мережевих даних, загроз, шкідливої поведінки користувачів і хмарного середовища з усього світу на географічних картах і діаграмах, що автоматично оновлюються.

Запропоновано варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи. Розглянуто варіант застосування засобів візуалізації стану безпеки корпоративної інформаційної системи на прикладі інтеграції рішення IBM QRadar Pulse з системою IBM QRadar SIEM.

Розроблено рекомендації фахівцям з кібербезпеки щодо забезпечення видимості стану безпеки корпоративної інформаційної системи.

Таким чином, запропоновані в роботі рекомендації мають сприяти підвищенню видимості стану безпеки корпоративної інформаційної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. A SANS 2021 Survey: Security Operations Center (SOC). Written by Chris Crowley and John Pescatore. October 2021. [Електронний ресурс] – Режим доступу: https://assets.extrahop.com/whitepapers/sans-2021-soc-survey.pdf.

2. Building a World-Class Security Operations Center: A Roadmap. A SANS Whitepaper. Written by Alissa Torres. May 2015. [Електронний ресурс] – Режим доступу: https://docplayer.net/25747233-Building-a-world-class-security-operations-center-a-roadmap.html.

3. Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfone. Computer Security Incident Handling Guide. SP 800-61 Rev. 2. NIST. Date Published: August 2012. [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

4. Carson Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE, 2014. – 346 p.

5. What Is a Security Operations Center (SOC)? [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html.

6. IBM Security QRadar. Visibility, detection, investigation, and response. Solution Brief. [Електронний ресурс] – Режим доступу: https://www.ibm.com/downloads/cas/OP62GKAR.

7. QRadar apps overview. Last Updated: 2023-01-13. [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-overview.

8. QRadar Pulse app. Last Updated: 2023-03-31. [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-pulse-app.

9. QRadar Pulse – QRadar 7.3.3 FP6+/7.4.1 FP2+ [Електронний ресурс] – Режим доступу:

https://exchange.xforce.ibmcloud.com/hub/extension/f4a537a424977e155105d8aa9f5283c3.

10. QRadar Pulse dashboard components and workspaces. Last Updated: 2023-05-02. [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-pulse-dashboard-components-workspaces.

11. Graph data visualisation for cyber-security threats analysis. Linkurious, June 13, 2016 [Електронний ресурс] – Режим доступу: https://linkurious.com/blog/graph-data-visualisation-cyber-security-threats-analysis/.

12. Matt Shealy. Ways Data Visualization Helps Prevent Cyber Attacks. 06/04/2021. [Електронний ресурс] – Режим доступу: https://www.computer.org/publications/tech-news/trends/ways-data-visualization-helps-prevent-cyber-attacks.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)