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 РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Комісар В.Д.
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІТ	— Інформаційні технології
КІС	— Корпоративна інформаційна система
СУБД	— Система управління базами даних
ШПЗ	— Шкідливе програмне забезпечення
COBIT	— Control Objectives for Information and Related Technologies
CRM	— Customer Relationship Management
CSIRT	— Computer emergency response team
EAM	— Enterprise Asset Management
ERP	— Enterprise Resource Planning
FISMA	— Federal Information Security Management Act
GLBA	— Gramm—Leach—Bliley Act
HRM	— Human Resource Management
MES	— Manufacturing Execution System
NIST	— The National Institute of Standards and Technology
OWASP	— Open Web Application Security Project
PCI DSS	— Payment Card Industry Data Security Standard
SCM	— Supply Chain Management
SIEM	— Security information and event management
SQL	— Structured query language
WMS	— Warehouse Management System

ВСТУП

Актуальність дослідження. У сьогоднішньому світі люди постійно користуються різни видами пристроїв, які у свою чергу формують інформаційні системи. Для прикладу, кожного дня декілька мільйонів людей використовують комп'ютери, планшети, смартфони для взаємодії з різними видами інформаційної системи, таких як банківські системи, навчальні та розважальні платформи, соціальні мережі тощо.

Звичайно, що нові технології не пройшли повз корпоративне середовище стороною, і впроваджуються там так само як і серед звичайних користувачів. У зв'язку з цим сучасні технології також розгортаються з розрахунком на корпоративний сегмент і створюються нові рішення для кращої оптимізації роботи бізнес-процесів. Але кожна інформаційна система може підпасти під впливи особи чи групи осіб, що мають за мету вчинення протиправних або зловмисних дій. Тому досить важливим є те, як захищати сформовані корпоративні системи від зловмисних дій зі сторони правопорушників.

Зі зростом використання інформаційних систем зловмисники почали все більше застосовувати цифрові методи проникнення до корпоративних інформаційних систем для здійснення своїх зловмисних дій. А зі збільшенням шкідливого програмного забезпечення, яке не вимагає великих знань з програмування у зловмисників, і масштабу компаній збільшилося кількість атак, які щодня мають розслідувати аналітики безпеки.

Тому все частіше постає питання у використанні SIEM системи для аналітики корпоративної інформаційної мережі з можливостями використання штучного інтелекту, який у свою чергу дозволить скоротити час необхідний для аналізу кіберінцидентів і зменшити кількість збитків, які отримані внаслідок невиявлених кібератак.

Вище сказане визначає актуальність цієї проблеми, основний зміст, якої становлять дослідження шляхів та розроблення рекомендацій щодо реагування на кіберінциденти в корпоративній інформаційній системі.

Об'єктом дослідження в роботі є процес забезпечення безпеки у корпоративній інформаційній системі.

Предметом дослідження є методи та засоби виявлення та реагування на кіберінциденти в корпоративній інформаційній системі.

Мета роботи полягає у тому, щоб розробити рекомендації щодо застосування методів та засобів для виявлення і реагування на кіберінциденти в корпоративній інформаційній системі. Для цього буде використано SIEM-систему IBM QRadar з її інтеграцією із суперкомп'ютером IBM Watson через інтегрування програмного комплексу «BM QRadar Advisor with Watson.

Наукові завдання:

дослідити існуючі загрози процесам функціонування корпоративних інформаційних систем;

проаналізувати існуючі методи та засоби виявлення та реагування на кіберінциденти в корпоративній інформаційній системі;

дослідити можливості застосування програмного комплексу IBM QRadar Advisor with Watson з метою реагування на кіберінциденти в корпоративній інформаційній системі.

Практичне значення одержаних результатів полягає в розроблені рекомендації щодо застосування методів та засобів для виявлення і реагування на кіберінциденти в корпоративній інформаційній системі.

1 АНАЛІЗ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Види, призначення, умови функціонування корпоративних інформаційних систем.

Спочатку визначимося з терміном, що таке корпоративна інформаційна система, щоб розуміти ідею її функціонування та призначення. Корпоративна інформаційна система – це інформаційна система, що включає різні методи та засоби для забезпечення автоматизації робочого процесу і управління персоналом, а також забезпечує постачання потрібної інформації до організації [1]. Тобто, основною її ціллю є автоматизація процесів, які протікають у компанії, а саме за допомогою гуртування всіх фінансових звітів компанії, зарплати працівників, витрат на закупівлю ресурсів, кількість найманих працівників тощо до однієї бази даних, а також дозволяє за допомогою єдиного програмного комплексу виконувати більшість корпоративних процесів для спрощення моніторингу, збирання даних та зменшення часу і спрощення процедури передачі даних між різними відділами компанії.

Корпоративні інформаційній системи включають в себе використання програмно-апаратних комплексів з метою автоматизації бізнес-процесів, що протікають в компанії. Вони можуть поділятися на такі види: «Система планування ресурсів підприємства» (ERP), «Система управління відносинами з клієнтами» (CRM), «Система управління ланцюгом поставок» (SCM), «Система керування виробництвом» (MES), «Система управління складом» (WMS), «Система управління фондами підприємства» (EAM), «Система управління персоналом» (HRM) та «Системи електронного документообігу» [1][2]. Розглянемо призначення та умови функціонування лише трьох з них, а саме планування ресурсів підприємства, управління відносинами з клієнтами та управління ланцюгом поставок.

Система планування ресурсів підприємства (ERP) – це інформаційна система у вигляді комплексу програмного забезпечення, що дозволяє зберігати та обробляти критично важливі дані підприємства, які необхідні для його роботи [2][3]. В основному, ERP системи охоплюють більшість сфер роботи підприємства та включають у себе системи CRM і SCM у вигляді модулів. Основним завданням цих систем є об'єднання різнорідного програмного забезпечення, що використовується в різних відділах компанії, в одну систему для [3][4]:

прискорення документообігу між різними відділами;

покращення управління та контролю роботи за працівникам у різних відділах та віддалених офісах;

зниження кількості помилок, які виникають внаслідок людського фактору;

зниження кількості даних, що потрібно узгоджувати.

У той же час, система управління відносинами з клієнтами (CRM) – це програмне забезпечення, що створене для роботи з продажами, маркетингом та взаємодією з клієнтами [2]. Завданнями CRM систем є автоматизація взаємодії з клієнтами, покращення рівня продажів та оптимізація маркетингу [5]. Тобто, за допомогою цих систем відслідковується діяльність працівників компанії, проведених ним угод, створюються графіки по продажах тощо, та всі дані автоматизовано вносяться до єдиної бази даних.

Система управління ланцюгом поставок (CSM) теж є програмним комплексом, що сконцентровано навколо ресурсів та логістики, за допомогою, якої товари можна доставити до клієнтів [2]. Ці системи, в основному надають програмне забезпечення для всіх учасників, які приймають участь в процесі виготовлення та доставлення товарів, а саме, постачальників, виробників, логістів, роздрібних торговців тощо [6]. Основним завданням цих систем, як з вище наведеного випливає, є автоматизація процесів, які відбуваються, починаючи від закупки матеріалів та закінчуючи поставками кінцевого продукту клієнтам компанії.

Отже, приділимо більше уваги саме ERP системам, так як вище вже було наведено, ці системи є узагальненням інших систем. В основному ERP системи складаються з наступного (Рис.1.1): платформа, управління даних і модулі [3]. У свою чергу платформа складається з ядра, на основі якого пишуться модулі, та базового функціоналу, що містить перелік довідників і функцій, які необхідні для роботи компанії [3]. Управління даних забезпечує роботу з базами даних, що застосовуються ERP системою та компанією для збереження всіх даних, які створено під час роботи цієї системи. Як вже було сказано вище, однією з важливих ланок цих систем є модулі, які можна приєднувати до основної системи.

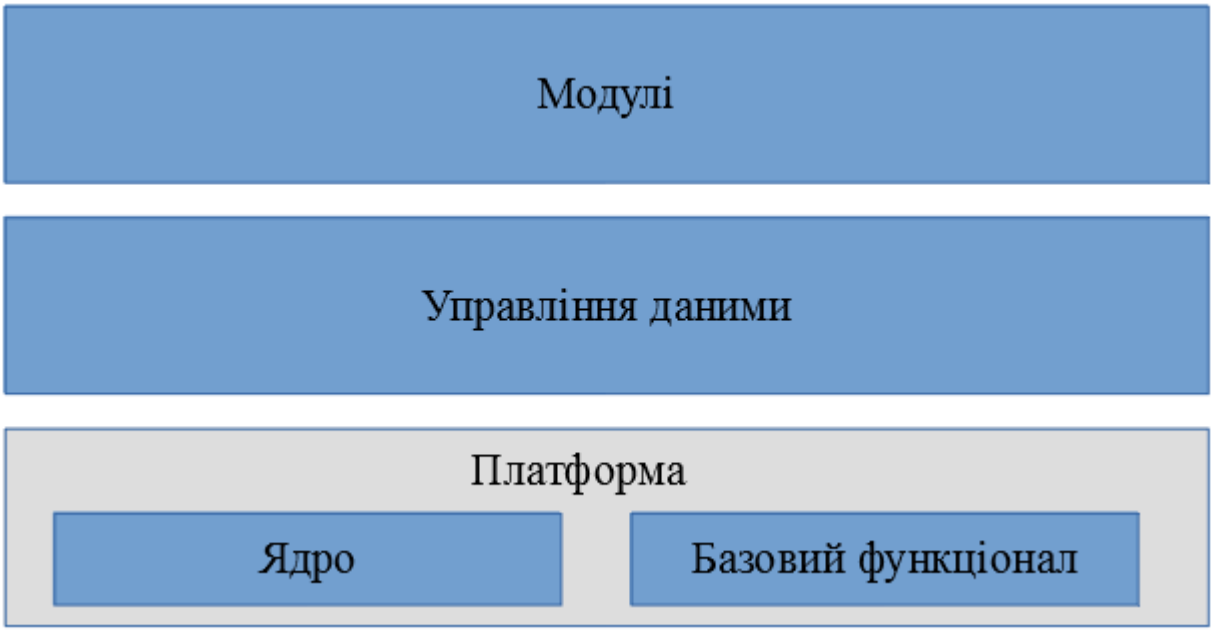


Рис. 1.1. Компоненти ERP системи

У загальному випадку, модулі – це програмні комплекси, які застосовуються в роботі певних відділів компанії (наприклад, HRM, CRM) та приєднуються до основної системи для оптимізації роботи з даними, а саме їхнього об’єднання в одну систему та полегшення процесу менеджменту й аналітики. В основному, модулі можуть поділятися на три групи, а саме, модулі внутрішніх користувачів, модулі зовнішніх користувачів та конектори, що використовуються для під’єднання сторонніх програмних комплексів, програм та розширення до основної системи ERP. За рахунок модулів до ERP системи можуть приєднуватися такі інформаційні системи як «Керування виробництвом»

(MES), «Система управління складом» (WMS), «Система управління фондами підприємства» (EAM), «Система управління персоналом» (HRM) тощо [1].

На основі вище наведеного можна сформулювати приклад як саме функціонують корпоративні інформаційні мережі у середніх та великих компаніях та підприємствах. Припустимо, що існує підприємство, яке займається виготовленням комп'ютерних запчастин та електротехніки і до нього звертається компанія, що виробляє телефони, для замовлення партії чіпів пам'яті для внутрішнього сховища майбутньої моделі смартфонів. За допомогою модулю продажів це замовлення додається до бази даних підприємства та водночас за допомогою ERM автоматизовано передається до модулю обліку, де відповідний відділ перевіряє дані клієнта [2]. Після чого за допомогою модулю інвентаризації проводиться аналіз наявних продуктів і передається замовлення через модуль виробництва на відповідну фабрику, що виробляє чіпи пам'яті [2]. Фабрика в свою чергу аналізує наявні ресурси на своєму складі і за необхідності докуповує необхідні компоненти, використовуючи для цього модуль закупівель [2]. Окрім цього фабрика може зробити запит на розподілення робочих обов'язків працівників, що працюють у підприємстві, або виконання пошуку нових працівників на роботу, використовуючи відповідний модуль в ERP системі. Після чого відповідні запити за допомогою ERP системи надходять до відділу, який займається керуванням працівниками та пошук нових кандидатів, і він виконує необхідні дії по запиту, що створила фабрика.

Таким чином, використовуючи вище наведену інформацію, можна сформулювати, що основними елементами бізнес-процесів у корпоративної інформаційної системи є: апаратні і програмні комплекси, СУБД, локальна мережа і розподілена мережа організації, а також додаткові пристрої і засоби, що використовуються для забезпечення її функціонування. При цьому можна виділити, що у корпоративній інформацій мережі протікають такі бізнес-процеси, як обмін інформації різного виду важливості за допомогою локальної та розподіленої мережі, створення та обробка інформації за допомогою програмно-апаратних комплексів, обробка та збереження інформації за допомогою СУБД

тощо. Однак, виникнення та протікання всіх цих процесів великою мірою залежить від людського фактору, а саме, взаємодії працівників із корпоративною інформаційною системою, клієнтами, постачальниками компонентів, бізнес-партнерами тощо.

1.2. Аналіз загроз процесам функціонування корпоративних інформаційних систем.

Ознайомлення з основними процесами функціонування корпоративної інформаційної мережі є важливим елементом для подальшого аналізу можливих вразливостей та загроз, наявність яких може вплинути на роботу системи або призвести до виникнення кіберінцидентів. Тому, що згідно зі звітом Identity Theft Resource Center, тенденція показує, щодо кількості витоків даних через кібірінциденти протягом року (рис. 1.2), зросла зі 157 мільйонів випадків у 2005 до 1473 мільйонів у 2019 році [7]. У зв'язку з цим розгляд вразливостей є важливим елементом для уникнення або зменшенні збитків компанії внаслідок кіберінцидентів.

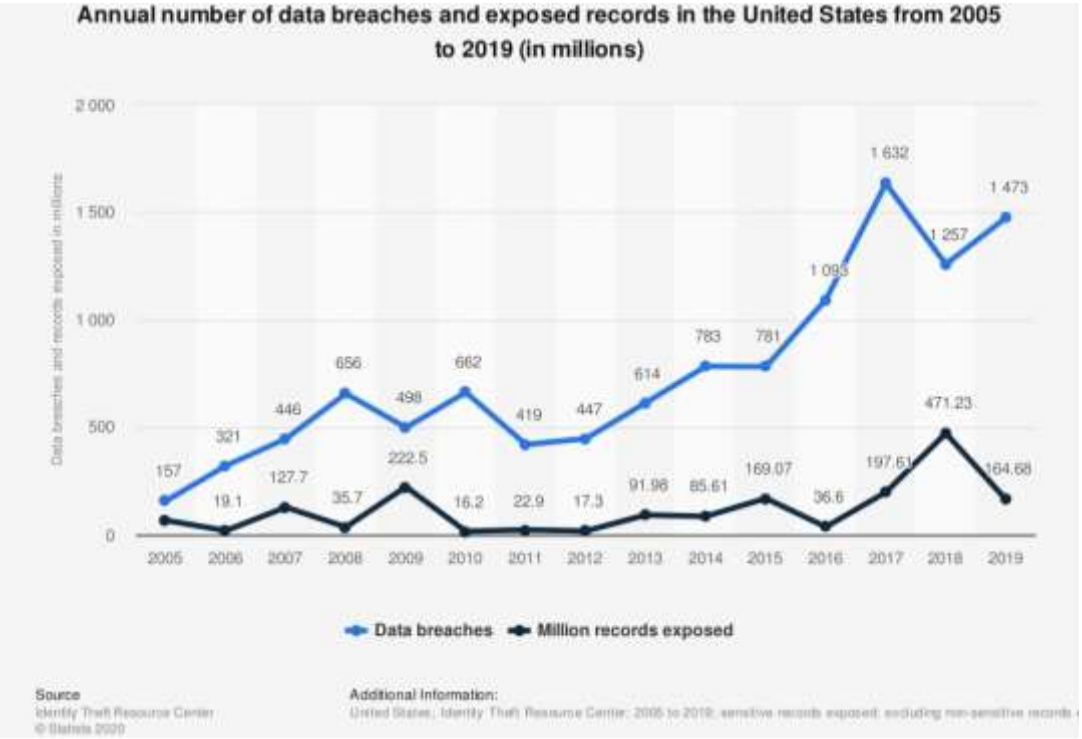


Рис. 1.2. Графік щорічних витоків даних та викрадених записів

Отже, на основі проведеного огляду бізнес-процесів у попередньому підрозділі можна виділити основні елементи корпоративної інформаційної системи, що можуть містити вразливості того чи іншого рівня критичності:

- Апаратні комплекси, що використовуються в корпоративній інформаційній системі компанії;
- Програмні комплекси, що використовуються в корпоративній інформаційній системі компанії;
- Локальні та розподілені мережі, що використовуються для обміну інформації між програмно-апаратними комплексами компанії;
- СУБД, що використовуються в роботі ERP системи компанії;
- Працівники і бізнес-партнери компанії та треті сторони, що співпрацюють з нею.

Розпочнемо огляд одного з найважливішої ланки корпоративної інформаційної системи, а саме, людського персоналу. Загалом, загрози бізнес-процесам, що пов’язані з працівниками компанії, полягають в психологічному впливі на них, а саме, використанні соціальної інженерії. Наприклад, згідно зі звітом щодо розслідування витоку даних компанією Verizon (див. рис. 1.2) на соціальну інженерію припадає 33% [8]. Вона характеризується такими принципами, як взаємність, прихильність і послідовність, соціальний доказ, авторитет, симпатія та обмеженість ресурсів [9]. Кожен з цих факторів може призвести до тих чи інших загроз корпоративної інформаційної системи, а, саме, фішингу, цілеспрямованого (гарпунного) фішингу, фізичного приманювання, претекстингу тощо [10].

В основну, фішинг характеризується підробкою легітимного сайту, електронного листа або тексту, що надсилається працівникам корпоративної інформаційної системи, з метою виконання шкідливих дій [11]. Таким чином, зловмисник викрадає конфіденційну інформацію компанії або встановлює шкідливе програмне забезпечення, що дозволяє йому непомітно проникати до мережі. Враховуючи це, можна сказати, що одним із простих способів для проникнення до корпоративної системи є людський персонал.

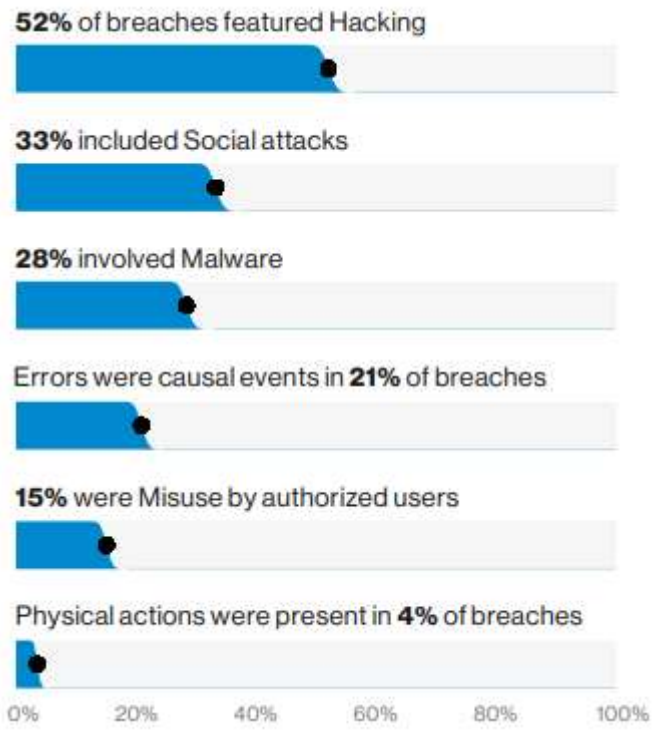


Рис. 1.3. Тактики, які використовуються при викраденні даних, згідно зі звітом Verizon.

Наступним кроком оглянемо програмно-апаратні комплекси, що приймають вагому роль у нормальному функціонуванні бізнес-процесів. Тому розглянемо загрози, що можуть там функціонувати та їхні наслідки для корпоративної інформаційної системи.

Основні вразливості в апаратних комплексах можуть виникати на таких рівнях як рівень інструкцій, рівень мікро-архітектури, рівень електричного кола та найнижчий рівень (описує фізичні умови функціонування обладнання) [12]. Таким чином вразливості і загрози можна поділити на два типи фізичного і програмного характеру. До загроз фізичного рівня можна віднести природні катаклізми, фізичне пошкодження, викрадення обладнання тощо. У той же час вразливостями програмного характеру можуть бути наступні елементи: наявність вад в програмному коді апаратних компонентів, відсутність останніх патчів системи тощо.

Наприклад, у 2018 році в мікрокоді процесорів були виявленні вразливості (Meltdown, Spectre), що можуть призвести до витоку інформації [13]. Загалом загрози на апаратному рівні мають високу ймовірність виникнення, однак частина

компаній не приділила цьому достатньої уваги. Згідно зі звітом компанії Dell 63% сказали, що вони мали хоча б один витік даних за минулий рік у зв'язку з вразливостями в апаратному забезпеченні (рис. 1.4), причому лише 59% відсотків впровадили політику і стратегії захисту апаратного забезпечення [14].

Рис. 1.4. Графік, що описує як часто компанії протягом року зіштовхувалися з витоками даних, які пов'язані з вразливостями на апаратному рівні [15].

Програмні комплекси можуть характеризуватися наступними вразливостями, як наявність вад у програмному забезпеченні, використання наявність вад у операційній системі, відсутність останніх патчів системи, використання непідтримуваних версій операційної системи, незахищених каналів обміну, збереження критичних даних у відкритому вигляді, відсутність механізмів захищеної ідентифікації і автентифікації, відсутність механізмів багатофакторної автентифікації тощо.

Прикладами загроз, що використовують вразливості програмних комплексів, можуть стати комп'ютерні віруси, трояни, шпигунські програми, черв'яки, програми вимагачі, руткіти та програми «командування і контролю» [16][17].

Важливим елементом в повноцінному функціонуванні бізнес-процесів із використанням ERP системи є забезпечення нормальної роботи баз даних. І тому варто звернути увагу на вразливості, що містить СУБД, для формування повноцінної картини загроз протіканню бізнес-процесам. Вразливості, що можуть мати СУБД складаються з наступних елементів: відсутність механізмів

шифрування даних, використання слабких паролів для доступу до даних, відсутність механізмів фільтрації запитів до СУБД, відсутність останніх патчів безпеки, наявність вад тощо [18].

Прикладом загроз базам даних може стати SQL ін’єкції, які згідно з OWASP Top 10 займають перше місці [19], помилки конфігурації бази даних, слабка автентифікація, зловживання правами, атаки на відмову в обслуговувані, слабке аудит тощо [18].

Локальні мережі є важливим складовою про побудові будь-якої інформаційної системи і тому вразливості, що вона може містити також є критичними елементом про формуванні картини загроз тій чи іншій системі. Отже, локальні мережі можуть характеризуватися такими вразливостями як [1]:

недоліки у захисті службових протоколів;

використання незахищених протоколів передачі даних;

відсутність програмних і/або апаратних засобів захисту мережі;

недоліки в архітектурі побудови локальної мережі.

У той же час більшість компаній також мають розподіленні мережі, які використовуються для передачі інформації між всіма офісами компанії, які можуть не лише розподілені по країні, а також і по всьому світу. Тому є важливим зважати на вразливості розподілених мереж. В основному, частина вразливостей, які містять локальні мережі також притаманні і для розподілених, та до них додаються й нові вразливості такі як:

недостатня стійкість механізмів ідентифікації та автентифікації;

відсутність фільтрування хибних запитів;

відсутність шифрування даних при передачі через глобальну мережу.

Одним із прикладом мережевих загроз може стати перехоплення трафіку з використання технології «людина посередині» (англ. Man-in-the-middle), яка передбачає, що зловмисник перехоплює трафік від відправника, переглядає його і видозмінює після чого відправляє отримувачу [20].

Проаналізувавши вразливості, що можуть бути в тих чи інших елементах корпоративної інформаційнійної системи і загрози, що використовують їх, можна

сформулювати загальну картину загроз, що впливають на протікання бізнес-процесів у компанії. У загалом вони можуть бути класифіковано за такими типами як [21]:

ті, що пов’язані з перехоплення даних, які протікають через канали передачі інформації;

ті, що пов’язані із несанкціонованим доступом до ресурсів корпоративної інформаційної системи;

ті, що пов’язані з несанкціонованим, навмисним або випадковим поширенням даних працівниками компанії;

ті, що пов’язані зі втратою переносних засобів збереження та обробки інформації;

ті, що пов’язані із несанкціонованим редагування, модифікуванням та видаленням даних;

ті, що пов’язані із несанкціонованою експлуатацією ресурсів корпоративної інформаційної системи;

ті, що пов’язані із зараження корпоративної інформаційної системи шкідливим програмним забезпеченням.

Отже, кожна з цих загроз реалізується через використання вразливостей, що є наявними в корпоративній інформаційній системі та спрямована на один або декілька з елементів цієї системи. Для прикладу, загроза щодо несанкціонованого доступу може реалізовуватися з використанням соціальної інженерії для впливу на працівників, щоб отримати доступу до інформації, яка зберігається в базах даних.

Таким чином можна сформулювати, що кожен елемент корпоративної інформаційної системи містить вразливості, які призводять до виникнення певних загроз бізнес-процесам компанії. Тому є важливим своєчасне впровадження системи захистів і реагування на кіберінциденти, що виникають в корпоративній інформаційній системі.

1.3. Аналіз проблеми реагування на кіберінциденти в корпоративній інформаційній системі.

При аналізі проблеми реагування на кіберінциденти в КІС потрібно спершу визначитися з самим поняттям що таке кіберінцидент. Згідно із Законом України «Про забезпечення основні засади забезпечення кібербезпеки України» інцидент кібербезпеки або кіберінцидент — це подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку електронних інформаційних ресурсів [22]. Таким чиним можна сформулювати, що кіберінциденти характеризується подіями, які порушують безпеку корпоративної інформаційної мережі.

Реагування на кіберінциденти є важливим етапом при захисті корпоративної інформаційної мережі від витоки даних чи порушенні функціонуванні бізнес-процесів. Тому потрібно швидко виявляти і реагувати на кіберінциденти, що виникають в системі. Однак, згідно зі звітом M-Trends 2020 протягом з 1 жовтня 2018 по 30 вересня 2019 було виявлено, що середній час перебування зловмисника в корпоративній мережі компанії склав 56 днів [23]. Окрім цього, згідно зі звітом FireEye щодо ефективності безпеки в компанії [24] близько 53% кіберінцидентів залишаються не виявленими (рис. 1.5). Варто зазначити, що на рис. 1.5 загальний відсоток перевищує 100% у зв’язку з тим, що група «сповіщені» є підмножиною груп «виявлені» та «попереджені».

Причиною цього можна виділити наступні фактори як:

різноманітність симптомів кіберінцидентів;

велика кількість кіберінцидентів;

використання нових видів ШПЗ або ШПЗ з методами маскування.

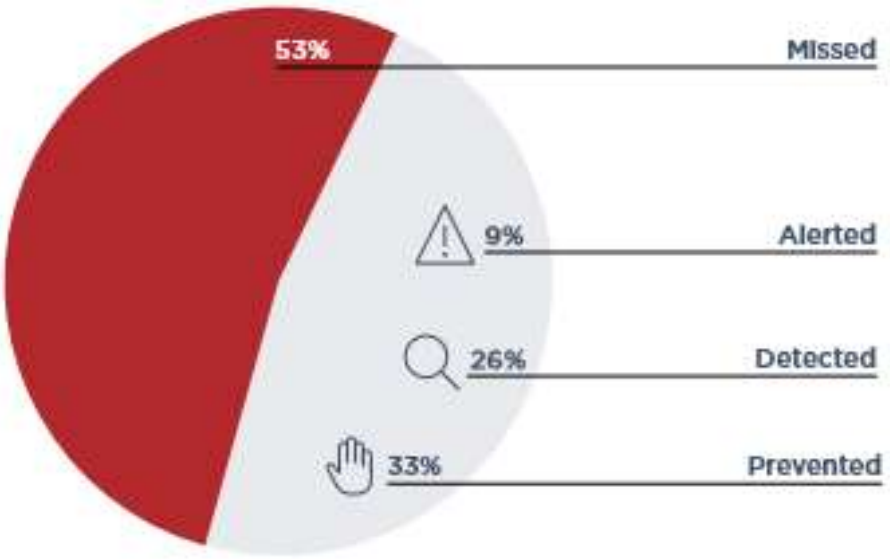


Рис. 1.5. Агреговані дані щодо реагування на інциденти безпеки.

Отже, оглянувши можливі загрози загрозами бізнес-процесам, що протікають в корпоративні інформаційні системі, можна прийти до висновку, що кіберінциденти виникають у всіх елементах, що приймають участь в роботі компанії. Таким чином кіберінциденти можуть характеризуватися різними симптомами починаючи від підозрілими використаннями ресурсів, закінчуючи зливанням даних самим працівниками компанії. Наприклад, у 2019 стало відомо про схеми підкуплення працівників компанії AT&T для встановлення ШПЗ на телефони [25].

Наступним кроком при реагуванні на кіберінциденти є їхня кількість в компанії, наприклад, зі звітом Ponemon Institute, щотижня компанії зіштовхуються з 17000 повідомлень безпеки, з яких 3218 вважалися надійними, але лише 705 було розслідувано [26]. У той же час, згідно з даними IBM на компанію щодня може припадати близько 200000 подіями безпеки і 40 інцидентів на одного аналітика, де на розслідування одного з них може припадати по декілька годин або днів [27]. Окрім цього, згідно зі звітом BAE Systems, щомісяця на компанію може припадати від 24 до 100 інцидентів (рис. 1.6), на які повинна реагувати компанія [28].

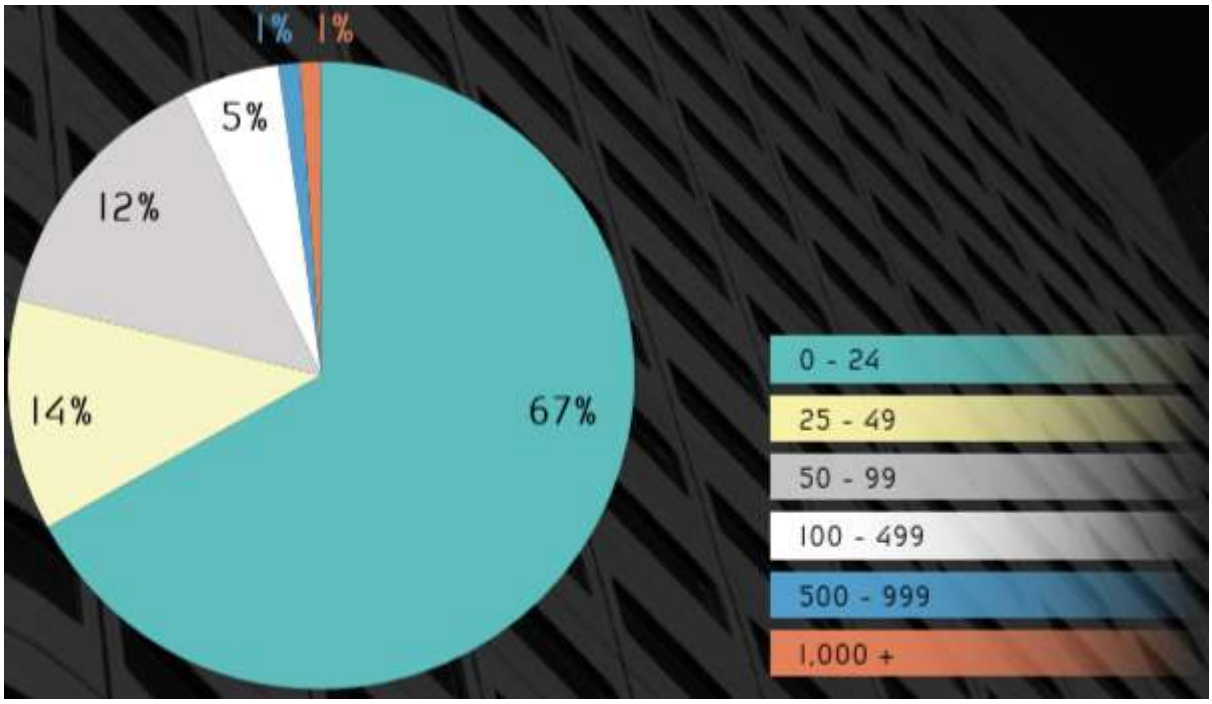


Рис. 1.6. Графік кількості кіберінцидентів, що припадають на місяць.

Таким чином можна прийти до висновку, що аналітики безпеки через велику кількість подій безпеки в корпоративній інформаційній системі можуть не вчасно реагувати на кіберінциденти.

Реагування на кіберінциденти також залежить від засобів, які використовує зловмисник, а саме ШПЗ та його методами маскування від систем захисту. Наприклад, ШПЗ може використовувати техніки ін'єкції себе в легітимний трафік або продукти, а також може застосовувати шифрування даних для уникнення виявленням [29]. Таким чином системи захисту можуть пропускати ШПЗ до корпоративної інформаційної системи або не виявляти тих, що вже є в системі.

Окрім цього, зі зростом технологій машинного навчання і штучного інтелекту зловмисники скоро можуть їх впроваджувати до своїх ШПЗ для послідовного маскування від системи захисту, використовуючи елементи навчання. Наприклад, IBM створило засіб для атаки DeepLocker, щоб продемонструвати можливості ШПЗ, що використовує штучний інтелект. Інструмент маскується як програмне забезпечення для відеоконференцій і приховується до тих пір, поки він не визначить бажану жертву за допомогою

розпізнавання обличчя і голосу та інших атрибутів, після чого виконує атаку на вибрану жертву [30].

Згідно зі звітом SANS Institute іншими чинниками, що можуть впливати на реагування на інциденти, є: недостатня кількість персоналу та їхніх професійних навичок, недостатній бюджет для засобів і технологій безпеки, погано описані процеси в компанії, наявність проблем в організації між відділом, що займається реагуванням на інциденти, і іншими відділами, наявність інтеграційних проблем своїх систем захисту з іншими системами захисту і засобами моніторингу [31].

Таким чином погано описані процеси в компанії та реагування на кіберінциденти можна охарактеризувати наступними трьома елементами. По-перше, документація про те, як діяти у разі порушення безпеки компанії, може бути застарілою. У той час документація часто є загальною та не корисною для керування конкретними видами діяльності під час кризових ситуацій [32].

Друга проблема полягає в тому, що плани, особливо в глобальних організаціях, не інтегруються в бізнес-підрозділи. Окремі підрозділи створюють локально оптимізовані плани реагування, які можуть бути корисними для боротьби з націленими атаками на них, але не є ефективними для управління інцидентом у всьому бізнесі. Також, згідно зі звітом BAE Systems [28], у 38% компаніях не проводиться планова перевірка процесів реагування на кібкрінциденти (рис. 1.7). Розробка індивідуальних планів в окремих підрозділах компанії також гальмує обмін відповідними знаннями та найкращими практиками [32].

По-третє, прийняття рішень за сценарієм реагування на кіберінциденти часто базується на племінних знаннях та стосунках, що вже існують. Це пояснюється погано кодифікованими планами та процесами реагування на кіберінциденти, які достатньо не продумані. Окрім цього в організації є лише одна чи дві особи, що є кваліфікованими та можуть керувати процесом реагування на кіберінциденти. Таким чином це може призвести до того, що цей працівник може бути відсутнім на період виникнення кіберінциденту або не мати

достатніх можливостей одночасно керувати декількома ланками у процесі реагуванні на кіберінциденти [32].

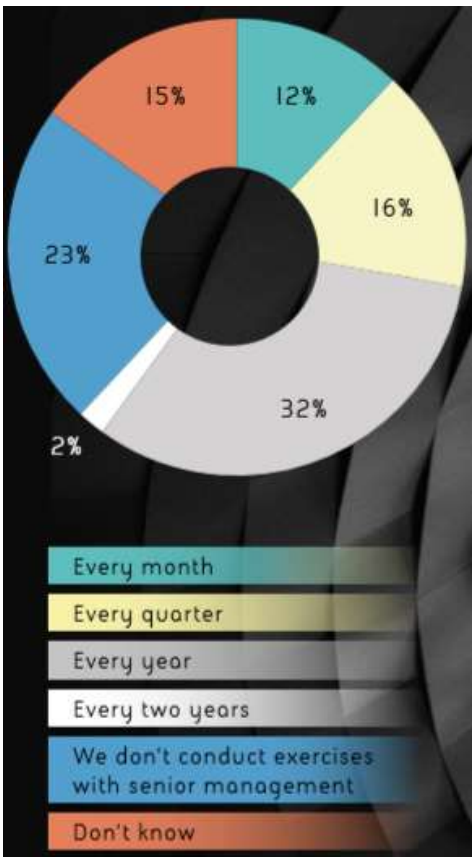


Рис. 1.7. Графік, що описує як часто компанія проводить планові тестування процесів реагування на кіберінциденти.

Також це все приводить до ще однієї проблеми, а саме того, що в компанії не вистачає кваліфікованих кадрів для швидкого реагування на кіберінциденти. Як вже було сказано вище, на кожного аналітика безпеки припадає багато порушень безпеки, що в свою чергу випливає до перевантаженості кожного працівника. Отже, це призводить до сповільнення процесу реагування на кіберінцидентри або, як вище сказано, до відсутності потрібних кадрів у критичний момент протікання кіберінциденту.

Таким чином, у підсумку можна сказати, що проблема у реагуванні на кіберінциденти полягає в наступному: різноманітність симптомів кіберінцидентів; великим обсягом порушень безпеки і в свою чергу недостатньою кількістю кваліфікованих кадрів; використання нових ШПЗ або тих, які використовують

маскування; відсутність або недостатня чіткість сформованих політики планів та процедур на реагування на кіберінциденти.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

2.1. Визначення ролі і місця процесу реагування на кіберінциденти в забезпеченні кібербезпеки корпоративних інформаційних систем.

Сьогодні компанії майже кожного дня зіштовхуються з кіберінцидентам, як вже було сказано вище, і тому важливим елементом у захисті від кібератак відіграють процеси реагування на кіберінциденти. Наприклад, за словами Кріс Моралес, керівника аналітики безпеки компанії Vectra: «за допомогою успішної програми реагування на інцидент компанія може зменшити або взагалі уникнути шкоди» [33].

Таким чином можна сформулювати, що ефективність захисту компанії та організації від кібератак залежить від того, наскільки в компанії ефективно впроваджено процес реагування на кіберінциденти. Реагування на кіберінциденти в компанії згідно з американським стандартом NIST, зазвичай, на формальному рівні складаються з політики, плану та процедур реагування на кіберінциденти [34].

Політика реагування на інциденти — це офіційний документ, що на законодавчому рівні в компанії описує процес реагування на інциденти. Ця політика в залежності від організації може відрізнятися, але в загальному вигляді складається, згідно з NIST, з таких елементів: заява про зобов'язання керівництва; мета та завдання політики; сфера дії політики (до кого і до чого вона застосовується та за яких обставин); визначення випадків комп'ютерної безпеки та пов'язаних з ними термінів; організаційна структура та визначення ролей, обов'язків та рівнів повноважень; оцінювання пріоритетності або суворості випадків; заходи щодо ефективності роботи; форми звітування та контактні форми [34].

План реагування на кіберінциденти — це документ, що описує підходи та засоби щодо реагування на кіберінциденти. План реагування на інцидент повинен містити такі елементи як: місія; стратегії та цілі; затвердження від вищого керівництва; організаційний підхід до реагування на інциденти; опис того, як група реагування на інцидент буде спілкуватися з рештою частиною компанії та з іншими організаціям; метрики для вимірювання можливостей реагування на інциденти та його ефективності; покрокова інструкція для опису процесів поетапного збільшення та покращення можливостей реагування на кіберінциденти; опис того, як програма вписується в загальну структуру організації [34].

Основною метою плану реагування на кіберінциденти полягає у встановленні та випробуванні чітких заходів, які організація повинна вжити для зменшення впливу порушення від зовнішніх та внутрішніх загроз [33]. Основною ціллю плану реагування на кіберінциденти є формування кроків, які компанія має виконувати під час виникнення, протікання та усунення наслідків кіберінциденту. Таким чином вони встановлюють ролі та обов'язки працівників, детально описують негайні заходи щодо виправлення, а також встановлюють процедури розслідування, зв’язку та сповіщення у разі порушення [35].

Стандартні операційні процедури – це окреслення конкретних технічних процесів, прийомів, контрольних списків та форм, що використовуються командою реагування на інциденти [34]. Вони, в основному, досить вичерно та детально описані, щоб забезпечити відображення пріоритетів організації в операціях з реагування на кіберінциденти. Однією з основних цілей процедур є чітка стандартизація процесу реагування на кіберінциденти для мінімізації помилки, які можуть бути спричинені стресовими ситуаціями, які виникають під час реагування на кіберінциденти. Процедури перевіряються для того, щоб довести свою ефективність та правильність, після чого з ними ознайомлюється команда аналітиків безпеки, що займається реагування на кіберінциденти [34].

Важливим елементом в процесі реагування на кіберінциденти в корпоративній інформаційній мережі є команда реагування на кіберінциденти.

Команда реагування на випадки комп’ютерної безпеки — це група IT-фахівців, яка надає організації послуги та підтримку щодо запобігання, управління та координації потенційних надзвичайних ситуацій, пов'язаних з кібербезпекою. Основні цілі CSIRT включають реагування на інциденти, що пов’язані з комп'ютерною безпекою, щоб відновити контроль та мінімізувати збитки, надаючи або допомагаючи ефективному реагуванню на аварію і відновлення після неї та перешкоджаючи повторному виникненню інцидентів комп'ютерної безпеки [36].

Основаними завданнями команди на реагування на кіберінцидентами є: отримання звіту про те, що виник інцидент; аналіз інциденту, що виник, та надання допомоги під час виникнення інциденту. Діяльність CSIRT по роботі з інцидентами може включати [37]:

визначення впливу, масштабу та характеру події чи інциденту;

розуміння технічної причини події чи інциденту;

визначення того, що ще могло статися чи інші потенційні загрози, що виникли внаслідок події чи інциденту;

дослідження та рекомендації рішень і шляхів вирішення;

координація та підтримка впровадження стратегій реагування з іншими частинами підприємства, включаючи IT-групи та спеціалістів, групи фізичної безпеки, службовців інформаційної безпеки, керівників бізнесу, виконавчих менеджерів, зв'язків з громадськістю, людських ресурсів та юридичного відділу;

поширення інформації про поточні ризики, загрози, напади, подвиги та відповідні стратегії пом'якшення за допомогою попереджень, консультацій, веб-сторінок та інших технічних публікацій;

ведення сховища даних про інциденти та вразливості та діяльності, пов'язані з певними відділами компанії, які можна використовувати для кореляції, тенденції та розробки «засвоєних уроків» для покращення безпеки та управління процесами інцидентів в організації.

Основними елементами реагування на кіберінциденети (рис. 2.1) згідно з NIST Framework є [35][33]:

«Підготовка» описує етап, при якому компанія проводить тренування персоналу, створення систем захисту, документації тощо. На цьому етапі важливим елементами є підготовленні кадри, підготовлені та профінасовані заходи реагування на кіберінциденти тощо.

«Ідентифікація» описує етап, при якому компанія виявляє порушення безпеки. На цьому етапі важливими елементами є класифікація даних, управління активами та протоколи управління ризиками.

«Утримання» описує етап, під час якого компанія вживає заходів для збереження доказів порушення безпеки системи. Важливими елементами цього етапу є збереження заражених файлів, файлів ШПЗ, дисків, ведення журналу подій з точною вказівкою на дату і час тощо.

«Ліквідування» описує заходи та процеси, що вживає компанія для усунення порушень безпеки, що виникли. На цьому етапі важливими елементами є прийняття заходів щодо усунення причини виникнення інциденту, а саме встановлення патчів безпеки, встановлення оновлень тощо.

«Відновлення» описує етап, в якому компанія використовує засоби та процеси для відновлення після кіберінциденту, що протікав у компанії. Важливим елементом цього етапу є наявність процесів і систем відновлення даних і резервного копіювання.

«Засвоєння уроку» описує етап, в якому компанія аналізує причини виникнення та процес протікання кіберінциденту та приймає відповідні рішення. Важливими елементами цього етапу є прийняття заходів для повторного недопущення виникнення кіберінцидету, покращення реагування на кіберінцидет тощо.

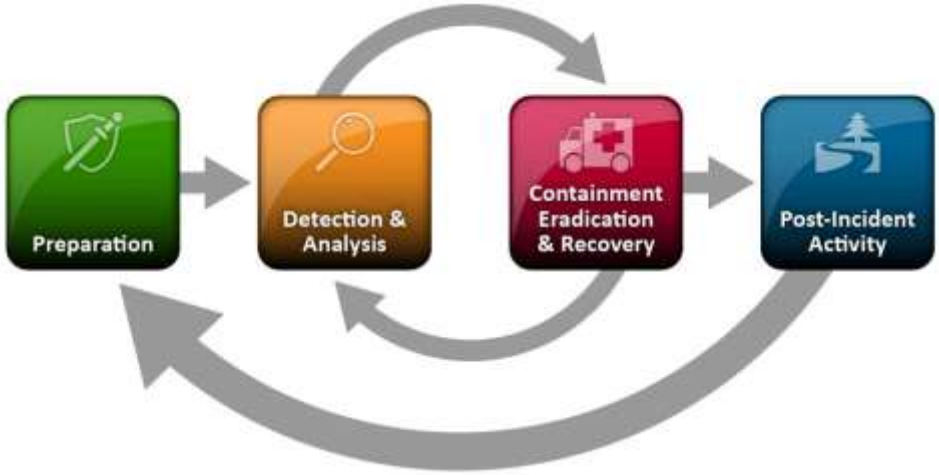


Рис. 2.1. Основні етапи реагування на кіберінциденти.

Таким чином можна сформулювати, що процес реагування на кіберінциденти полягає в тому, що спершу компанія підготовлює своє відділи до можливих атак, що можуть виникнути, та постійно аналізує ситуацію у кібербезпеці, щоб бути готовими до будь-яких атак. Опісля при виявленні підозрілої активності в корпоративній інформаційній системі компанія підключає в процес команду на реагування на кіберінциденти і вони проводять аналіз щодо можливих порушень безпеки. У випадку виявлення порушення безпеки команда реагування на кіберінциденти зберігає в первинному вигляді всі докази протікання інциденту, після чого приступає до усунення причин і наслідків виникнення кіберінциденту. Останнім кроком компанія аналізує причини чому виник інцидент та проводить аналіз процесу реагування на кіберінциденти, у результаті чого формується список рішення, які потрібно прийняття для уникнення повторення ситуацій та покращення процесів, які застосовуються під час реагування на кіберінциденти.

2.2. Аналіз аналітичних можливостей системи IBM QRadar SIEM для виявлення кіберінцидентів в корпоративній інформаційній системі.

У корпоративних інформаційних системах вирішення проблем на реагування на кіберінцинденти можуть застосовуватися SIEM системи, що

спрощують процес виявлення кіберінцидентів, що можуть виникати в компанії. Програмне забезпечення «Security information and event management» (SIEM) дає професіоналам із безпеки підприємства як уявлення, так і фактичний опис того, що відбувається в їхньому IT-середовищі [38].

SIEM системи, в основному, збирають та агрегують логи зі всіх пристроїв у компанії для подальшої кореляції даних з відповідними правилами, що були створенні в SIEM системі. Завдяки цьому SIEM системи можуть виявляти можливі порушення безпеки корпоративної інформаційної мережі і сповіщати про це аналітика безпеки для прийняття подальших дій.

Розглянемо можливості використання SIEM системі в корпоративній інформаційній системі на основі програмного продукту IBM QRadar. Однією з важливих елементів IBM QRadar для аналізу наявності порушень безпеки в інформаційної системи є кореляція подій і потоків з правилами безпеки для виявлення інцидентів. Отже, за допомогою правил аналітик безпеки створює шаблон певного порушення, в якому вказує всі події і/або потоки, що є ознаками цього порушення. Наприклад, на малюнку (рис. 2.2) зображено частину правила щодо порушення «AssetExclusion», яке описує події, що його характеризують.

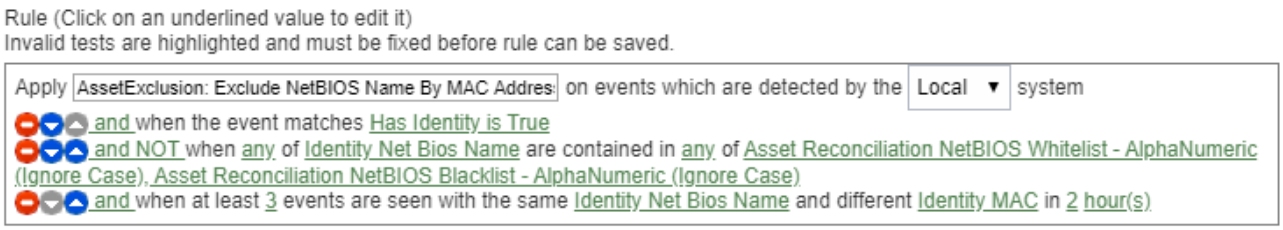


Рис. 2.2. Частина правила, що описує події та потоки, які є ознаками порушення безпеки в КІС

Окрім цього при створенні певної безпеки аналітик може вказати параметри серйозності, відповідності і достовірності, а також визначити дії, що будуть виконуватися внаслідок виникнення цієї події (див. рис. 2.3). Серед дій, які може вказати аналітик, безпеки є створення нової події, надсилання повідомлення на електронну пошту, виконання сканування, виконання власного скрипту/дії тощо. Таким чином аналітик безпеки може описати події, які він вважає містять

порушення безпеки в КІС, та визначити їхню важливість і дії, які будуть виконуватися після їхнього виявлення.

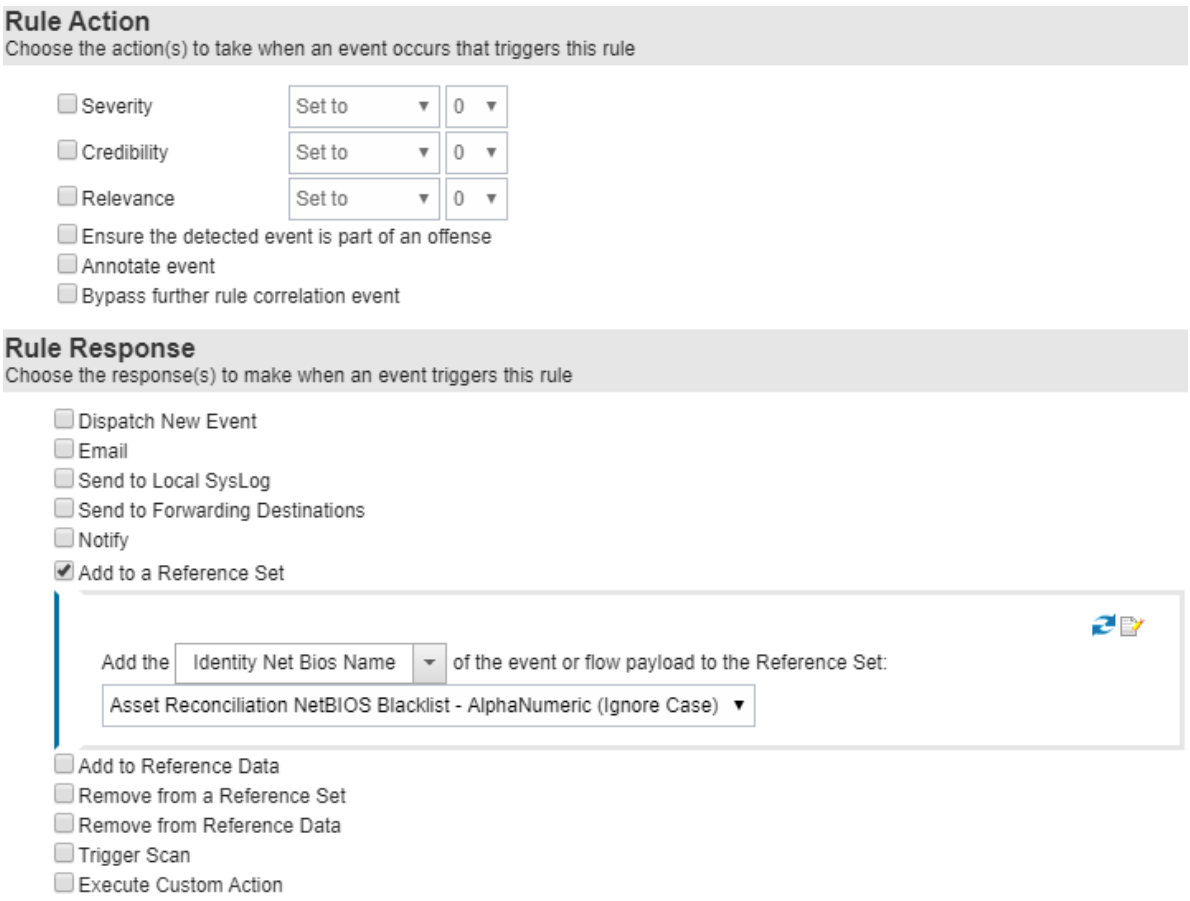


Рис. 2.3. Частина правила, що описує параметри щодо категоріювання події та відповіді, яка може бути виконана

IBM QRadar має можливості відслідковування в реальному часі всіх подій і потоків, що відбуваються і протікають в КІС. На основі цього він формує аналітику щодо того, що відбувається, та може в реальному часі виявляти порушення безпеки на основі вже створених правил в ньому. Наприклад, аналітик безпеки може отримати узагальнену інформацію (рис. 2.4) щодо стану безпеки: тип порушень, що виникали, найпопулярніші типи логів, завантаженість з'єднання, останні порушення тощо.

Рис. 2.4. Зведена панель IBM QRadar, яка надає узагальнену інформацію щодо безпеки в КІС

Аналітики безпеки за допомогою IBM QRadar можуть також переглядати в реальному часі діяльність в логах та в мережі з можливостю застосування фільтрів. Таким чином за необхідності аналітик безпеки може відфільтрувати дані за певним параметром, наприклад, блокування міжмережевим екраном за IP-адресою призначення або список програм, що найбільше використовуються (рис. 2.5).

У свою чергу це може допомогти аналітикам безпеки виявити порушення безпеки або визначити, що могли їх спричинити. Також аналітики безпеки можуть використовувати ці дані для спостереження та аналізу перебігу того, чи іншого кіберінциденту. Також за допомогою використанні цих засобів аналітик безпеки може формувати правила поведінки, правила аномалій і правила порогу, що дозволяє описати нормальну поведінку мережі КІС для виявлення аномалій в ній. Таким чином IBM QRadar зможе виявляти порушення безпеки, які можуть бути частиною кіберінцидентів, що до цього не було зафіксовано в базі відомих кіберінцидентів. Приклад створення правила поведінки зображено на малюнку Рис. 2.6.

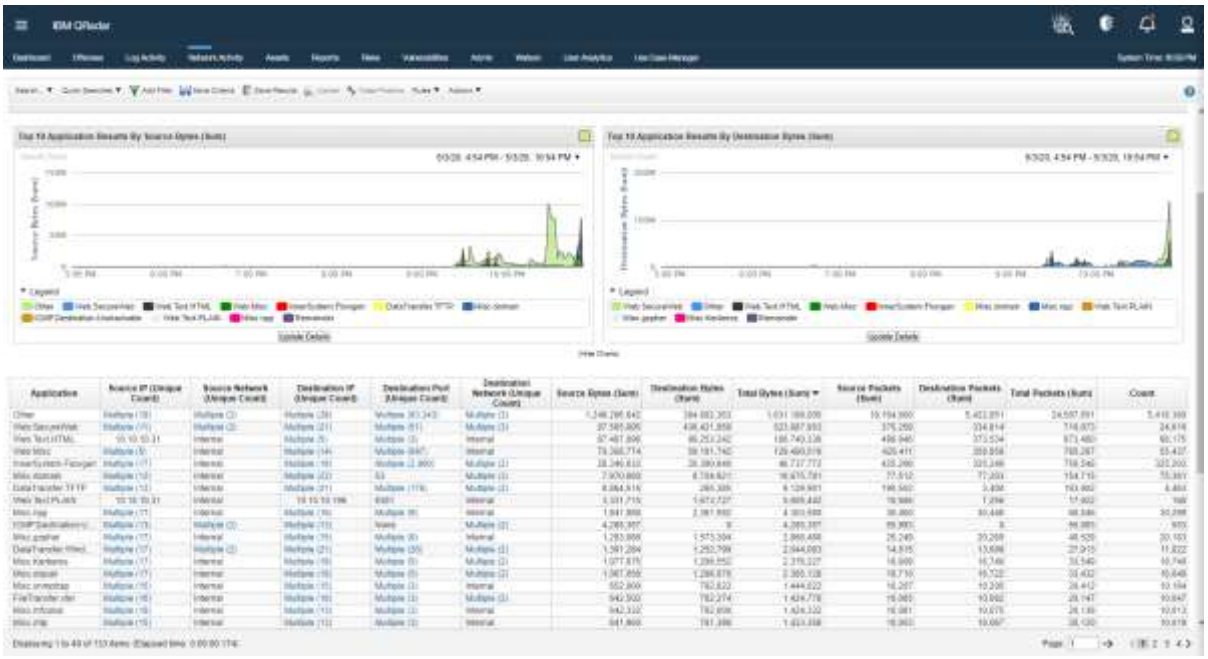


Рис. 2.5. Фільтрування діяльності мережі за програмами, що найбільше використовуються

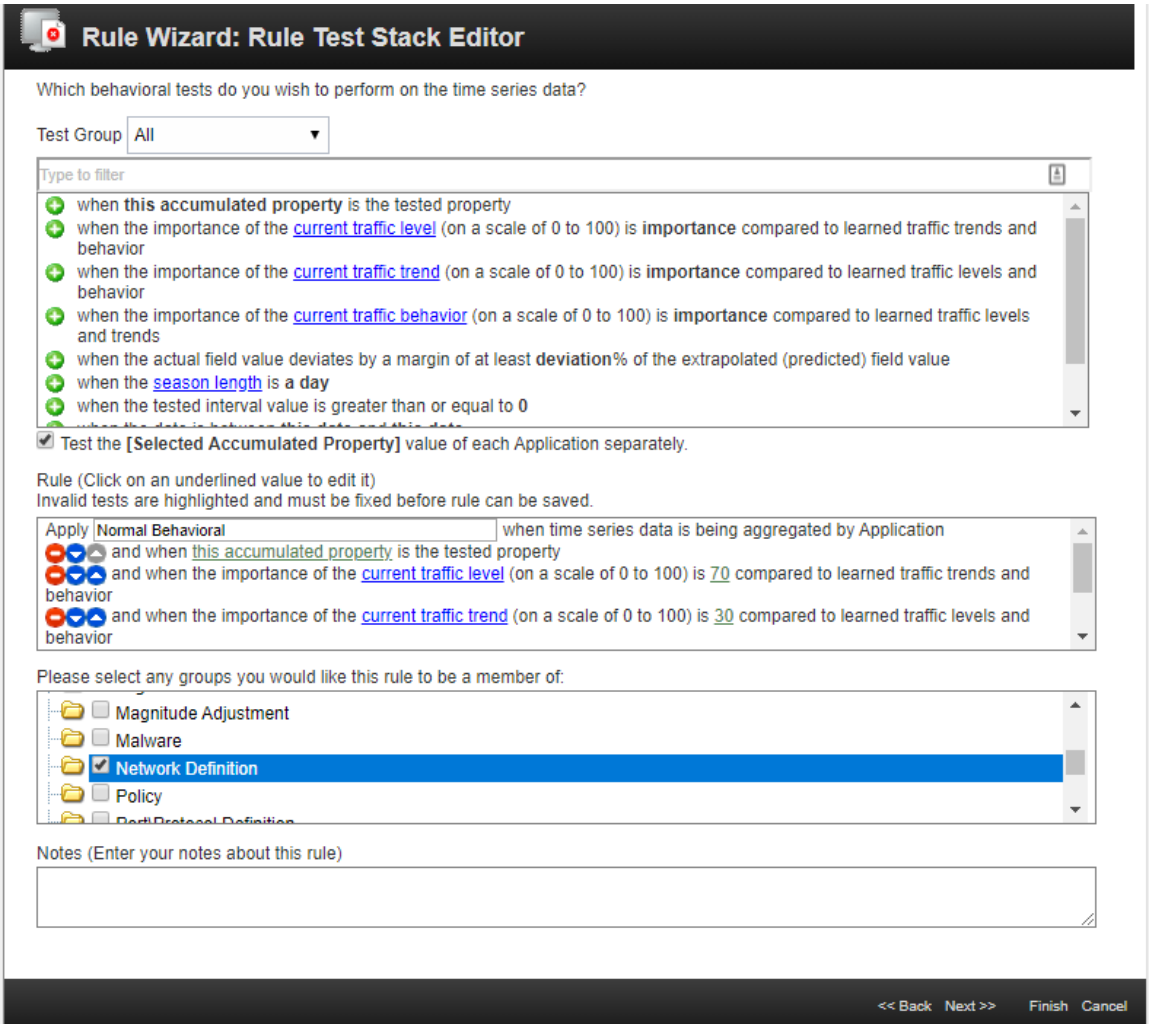
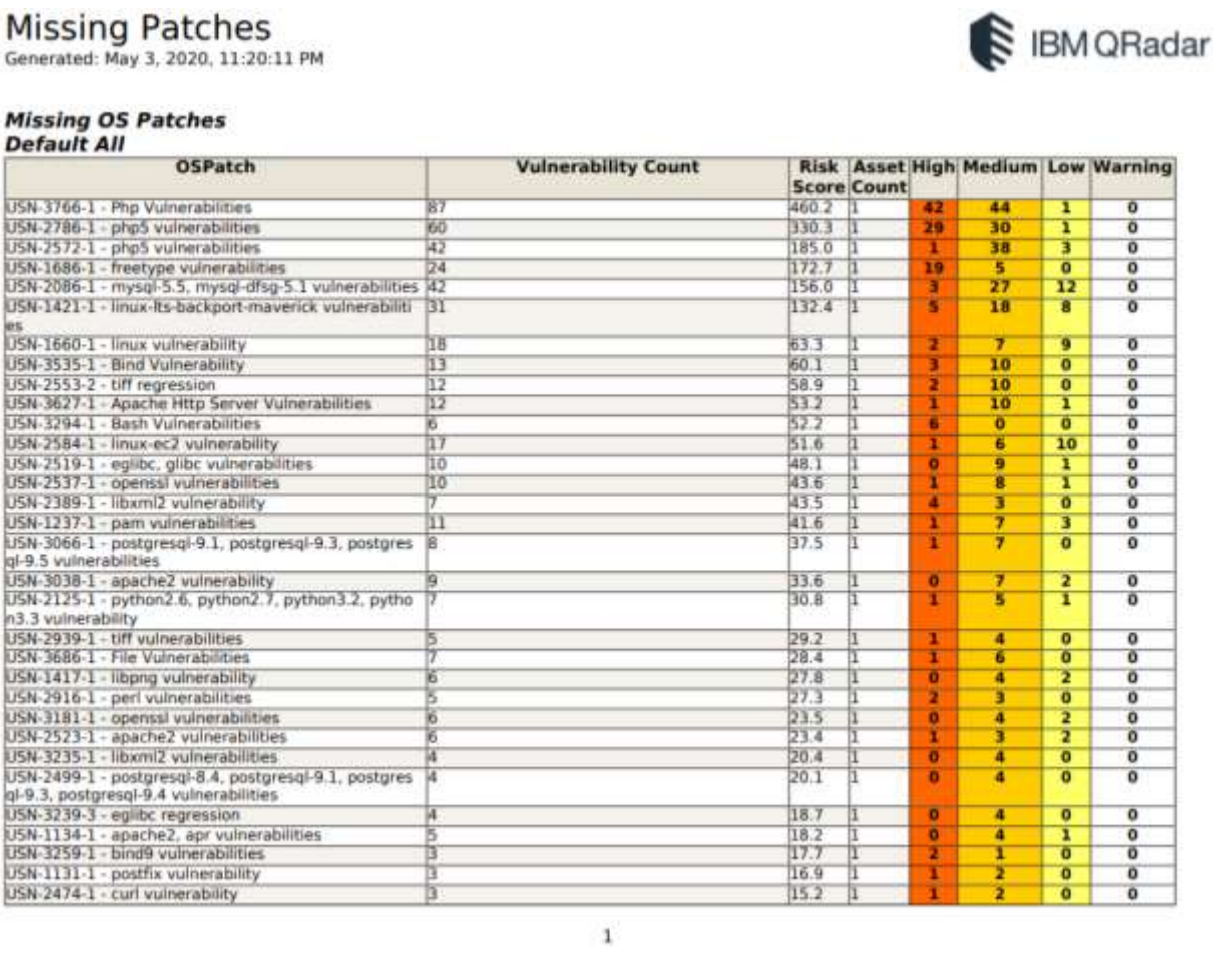


Рис. 2.6. Створення правила поведінки в IBM QRadar

Аналітики безпеки можуть використовувати IBM QRadar для створення звітів щодо стану безпеки КІС, протікання подій порушення безпеки, наявності вразливостей у мережі. При формуванні звітів аналітики безпеки можуть використовувати міжнародні стандарти такі, як COBIT, PCI DSS, FISMA, GLBA тощо. Таким чином аналітики безпеки можуть використовувати їх, щоб звітувати перед керівництвом щодо стану безпеки КІС або іншими огранізаціями, з якими співпрацює компанія. Наприклад, на малюнку Рис. 2.7. зображено сформований звіт IBM QRadar щодо стану безпеки, а саме відсутніх патчів безпеки у КІС.



Missing Patches
Generated: May 3, 2020, 11:20:11 PM

IBM QRadar

Missing OS Patches
Default All

OSPatch	Vulnerability Count	Risk Score	Asset Count	High	Medium	Low	Warning
USN-3766-1 - Php Vulnerabilities	87	460.2	1	42	44	1	0
USN-2786-1 - php5 vulnerabilities	60	330.3	1	29	30	1	0
USN-2572-1 - php5 vulnerabilities	42	185.0	1	1	38	3	0
USN-1686-1 - freetype vulnerabilities	24	172.7	1	19	5	0	0
USN-2086-1 - mysql-5.5, mysql-dfsg-5.1 vulnerabilities	42	156.0	1	3	27	12	0
USN-1421-1 - linux-lts-backport-maverick vulnerabiliti es	31	132.4	1	5	18	8	0
USN-1660-1 - linux vulnerability	18	63.3	1	2	7	9	0
USN-3535-1 - Bind Vulnerability	13	60.1	1	3	10	0	0
USN-2553-2 - tiff regression	12	58.9	1	2	10	0	0
USN-3627-1 - Apache Http Server Vulnerabilities	12	53.2	1	1	10	1	0
USN-3294-1 - Bash Vulnerabilities	6	52.2	1	6	0	0	0
USN-2584-1 - linux-ec2 vulnerability	17	51.6	1	1	6	10	0
USN-2519-1 - eglibc, glibc vulnerabilities	10	48.1	1	0	9	1	0
USN-2537-1 - openssl vulnerabilities	10	43.6	1	1	8	1	0
USN-2389-1 - libxml2 vulnerability	7	43.5	1	4	3	0	0
USN-1237-1 - pam vulnerabilities	11	41.6	1	1	7	3	0
USN-3066-1 - postgresql-9.1, postgresql-9.3, postgres ql-9.5 vulnerabilities	8	37.5	1	1	7	0	0
USN-3038-1 - apache2 vulnerability	9	33.6	1	0	7	2	0
USN-2125-1 - python2.6, python2.7, python3.2, pytho n3.3 vulnerability	7	30.8	1	1	5	1	0
USN-2939-1 - tiff vulnerabilities	5	29.2	1	1	4	0	0
USN-3686-1 - File Vulnerabilities	7	28.4	1	1	6	0	0
USN-1417-1 - libpng vulnerability	6	27.8	1	0	4	2	0
USN-2916-1 - perl vulnerabilities	5	27.3	1	2	3	0	0
USN-3181-1 - openssl vulnerabilities	6	23.5	1	0	4	2	0
USN-2523-1 - apache2 vulnerabilities	6	23.4	1	1	3	2	0
USN-3235-1 - libxml2 vulnerabilities	4	20.4	1	0	4	0	0
USN-2499-1 - postgresql-8.4, postgresql-9.1, postgres ql-9.3, postgresql-9.4 vulnerabilities	4	20.1	1	0	4	0	0
USN-3239-3 - eglibc regression	4	18.7	1	0	4	0	0
USN-1134-1 - apache2, apr vulnerabilities	5	18.2	1	0	4	1	0
USN-3259-1 - bind9 vulnerabilities	3	17.7	1	2	1	0	0
USN-1131-1 - postfix vulnerability	3	16.9	1	1	2	0	0
USN-2474-1 - curl vulnerability	3	15.2	1	1	2	0	0

1

Рис. 2.7. Звіт щодо відсутніх патчів безпеки, який сформований IBM QRadar

Серед інших можливостей IBM QRadar є наявність управління активами компанії, виявлення в них вразливостей тощо. Окрім цього, IBM QRadar має можливість до інтегрування інших продуктів з SIEM системою, що дозволяє аналітикам безпеки розширювати функціонал програмного продукту, а також

експортувати дані до інших продуктів, що можуть використовуватися під час розслідувань кіберінцидентів.

Підсумовуючи вище сказане, можна сказати, що основними можливостями IBM QRadar під час аналізу безпеки КІС та виявлення кіберінцидентів є: формування правил на основі певних подій і потік для виявлення порушень безпеки, централізоване агрегування діяльності логів і мережевої активності з можливість переглядання в реальному часі, формування правил аномалій, поведінки і порогу для виявлення невідомих ШПЗ або ШПЗ. Які використовують вразливості нульового дня, формування звітів щодо стану безпеки КІС, управління активами, а також можливість інтеграції інших продуктів.

2.3. Аналіз когнітивних можливостей Watson для підвищення ефективності виявлення кіберінцидентів в корпоративній інформаційній системі.

Зі зростом новітніх технологій все частіше у різних сферах застосовуються засоби штучного інтелекту для вирішення завдань у цих сферах. Останнім часом використання штучного інтелекту також розглядають у кібербезпеки для виявлення нових ШПЗ або ШПЗ, що використовують методи маскування.

Отже, у загальному випадку, штучний інтелект описується як система симуляції людського розуму, що має уміння до раціонального мислення і може приймати рішення, що мають найбільший успіх для досягнення поставленої мети [39]. У кібербезпеці штучний інтелект пропонують використовувати для аналізу і формування шаблону нормальної поведінки мережі, щоб виявляти аномалії, які можуть бути частиною протікання кіберінциденту [40]. Окрім цього ШІ пропонується також для виявлення нових видів ШПЗ у зв’язку з тим, що він може аналізувати поведінку минулих ШПЗ і на основі цього може формувати шаблон для виявлення невідомих до цього ШПЗ.

Розглянемо можливості штучного інтелекту на прикладі використання IBM Watson щодо підвищення ефективності виявлення кіберінцидентів. Однією з важливих завдання, які ставиться перед ШІ у кібербезпеці, є пришвидшення часу

на реагування на кіберінциденти. Як вже раніше говорилося кожного дня компанії зіштовхуються з великою кількість подій безпеки, на які витрачаються багато часу. Окрім цього велика частина інформації щодо кіберінцидентів і кібербезпеки в мережі згенерована неструктурованими дані, що ускладнює пошук інформації щодо інцидентів безпеки в автоматизованим шляхом.

Тому однією з можливостей IBM Watson є вміння розпізнавання даних, що написані людьми (рис. 2.8), з метою пошуку інформації щодо актуальних кіберінцидентів і з подальшим порівнянням їхніх індикаторів компрометації в КІС. Згідно з даними IBM продукт Watson має доступ до більше ніж 1 мільйонів документів, які пов’язані з безпекою [41]. Таким чином він аналізує доступну інформацію в мережі щодо кіберінцидентів і повідомляє аналітика безпеки про можливі інциденти безпеки в КІС. Прикладом цього, може стати виведення додаткової інформації щодо інциденту (рис. 2.9).

Рис. 2.8. Розпізнавання неструктурованого тексту когнітивними можливостями IBM Watson [42]

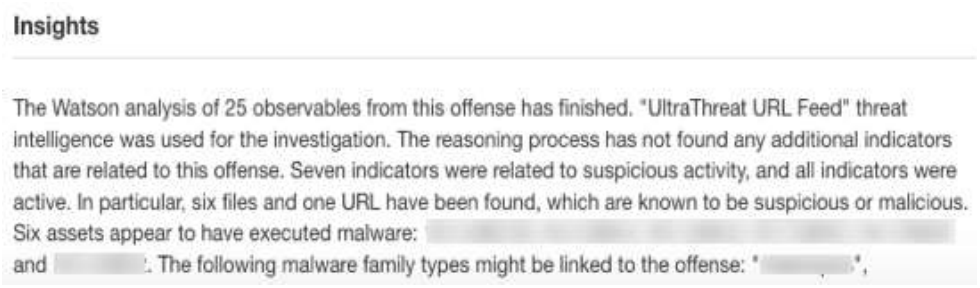


Рис. 2.9. IBM Watson Insight надає додаткову інформацію щодо інциденту

Також IBM Watson може застосовуватися для аналізу подій і потоків, що протікають в КІС. Таким чином при виявлені нової події безпеки в мережі IBM Watson отримує основну інформацію про неї від систем захисту. Потім він розпочинає пошук за цим індикаторами у мережі Інтернет і базах даних, які зберігають інформацію щодо кіберінцидентів. На цьому етапі при знайдені наявних інцидентів IBM Watson підтягує документацію щодо них, яка містить статті, звіти від компаній, що займаються безпекою, публікації в буклетах тощо (рис. 2.9).

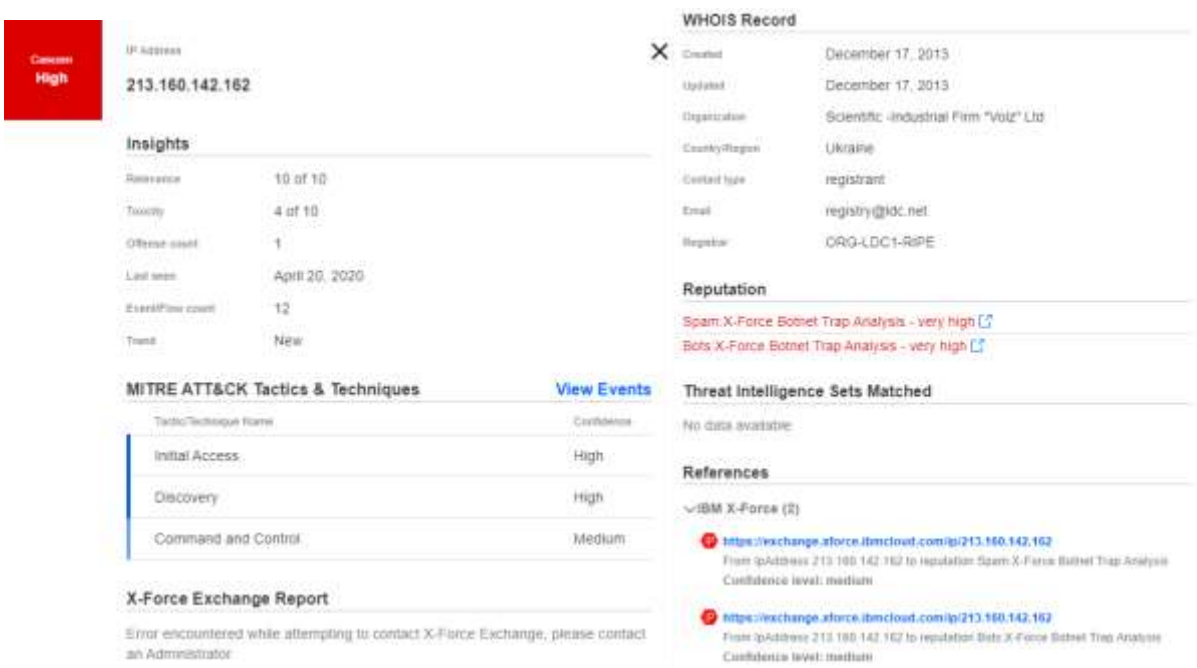


Рис. 2.9. Підтягування даних щодо інциденту з різних джерел.

На останньому етапі продукт розпочинає пошук всіх інших подій, потоків, активів і користувачів, що можуть бути пов’язані з первиною подією. Таким чином IBM Watson може сформувати повноцінну картину щодо протікання

певного кіберінциденту в компанії (див. рис. 2.10), а також виявити інциденти, які були непомічені до цього.

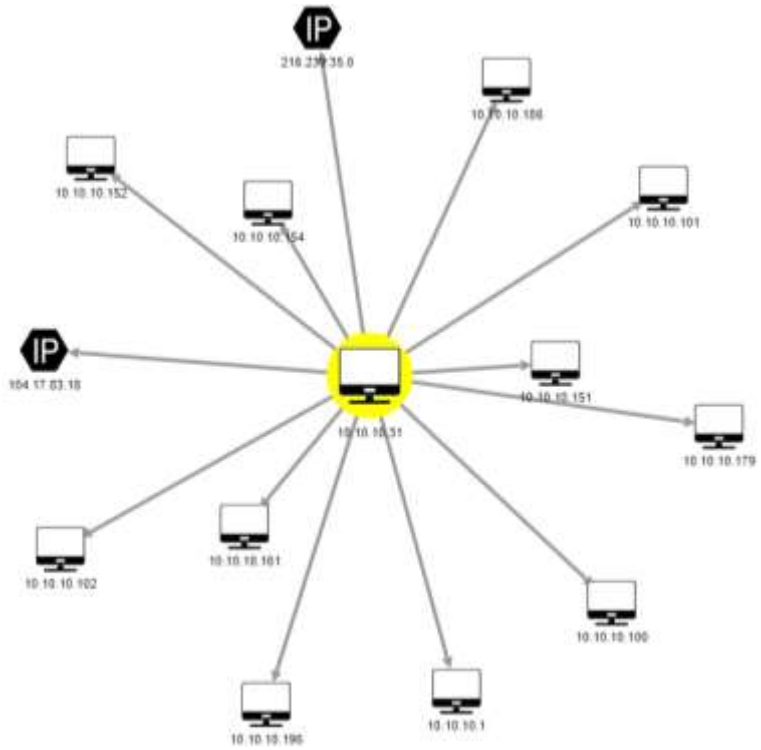


Рис. 2.10. Граф, що описує всі пов’язані елементи з кіберінцидентом

Також IBM Watson може допомогти покращити виявлення кіберінцидентів за рахунок моніторингу мережі компанії та в автоматичному режимі проведення аналізу подій безпеки у КІС. Таким чином продукт може зменшити кількість часу, яку потрібно буде використати для розслідування подій безпеки.

Підсумовуючи вище сказане можна сформулювати, що використання IBM Watson може покращити виявлення кіберінцидентів за рахунок автоматичного аналізу великої кількості ресурсів, які описують інциденти кібербезпеки, а також надання інформації та аналізу щодо протікання кіберінцидентів в КІС з можливість виявлення не помічених порушень безпеки.

2.4. Аналіз можливостей інтеграції та способів сумісного застосування програмного комплексу IBM QRadar SIEM та IBM QRadar Advisor with Watson.

Як було сказано в минулих підрозділах IBM QRadar має можливості щодо

розширення своїх можливостей за рахунок доповнень, які розповсюджуються через магазин розширення, що розташовано на сайті IBM X-Force Exchange. Серед розширення, що можна інтегрувати в IBM QRadar є IBM QRadar Advisor with Watson, яке відповідає за інтеграцію в SIEM систему штучного інтелекту від IBM.

Отже, для інтеграції IBM QRadar і IBM QRadar Advisor with Watson потрібно мати обліковий запис в IBM X-Force Exchange, щоб мати змогу підписатися і отримати розширення для встановлення. Важливим етапом при інтеграції QRadar Advisor with Watson в IBM QRadar є відповідність системи рекомендованим вимогам до неї, в іншому випадку інтегрувати продукт не вдасться.

Таким чином згідно зі сторінкою IBM X-Force щодо продукту QRadar Advisor with Watson, версія QRadar повинна бути не нижче 7.3.2 з патчом 3, а також система займе 1224 MB [43]. Відповідна інформація наведена на рис. 2.11.

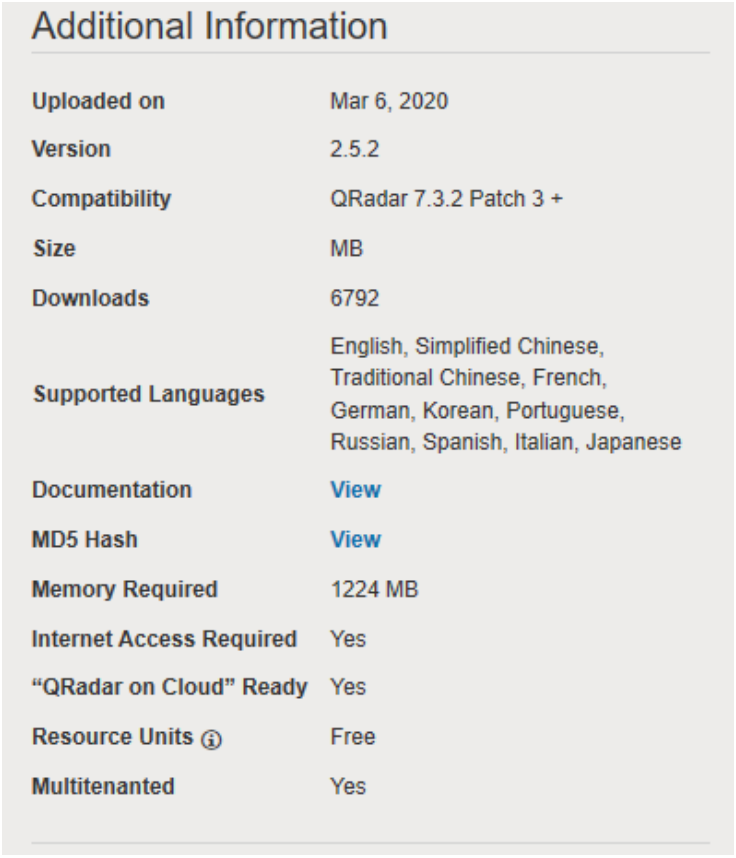


Рис. 2.11. Системні вимоги, які необхідні для інтеграції QRadar Advisor with Watson

Отже, для перевірення відповідності версії встановленого рішення QRadar рекомендованим вимогам потрібно відкрити бічну панель і обрати пункт «Про». У вікні, що відкриється, буде вказано версію вставленого рішення IBM QRadar (рис. 2.12).

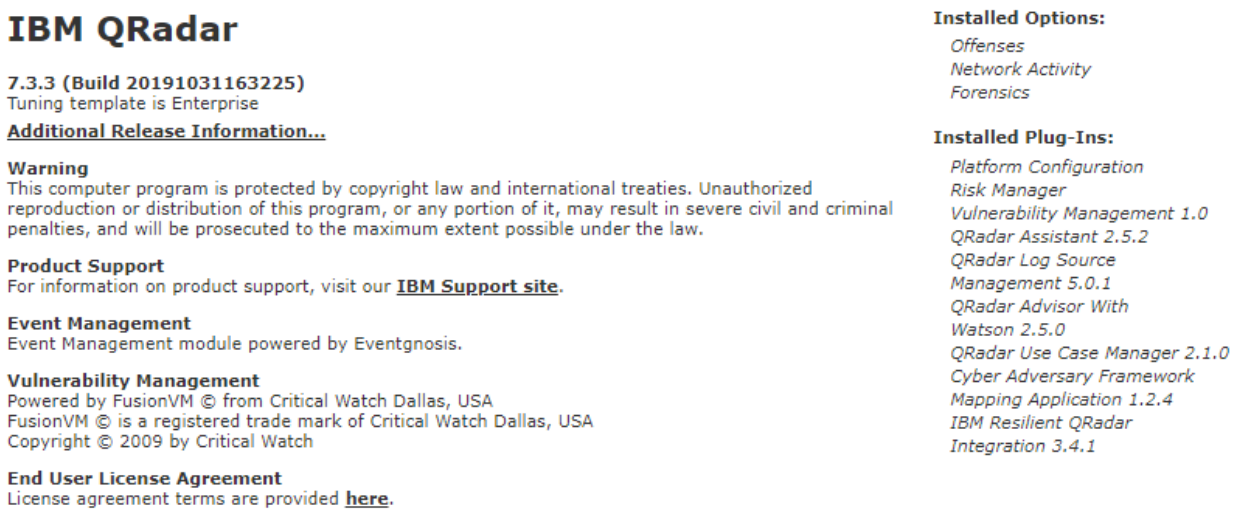


Рис. 2.12. Вікно «Про QRadar», де вказано версію встановленого рішення

Процес покрокової інтеграції QRadar Advisor with Watson в IBM QRadar буде детально описано в наступному розділі, але, в загалом, процес інтеграції складається зі встановлення розширення в SIEM систему та подальшого його налаштування.

Основними перевагами використання QRadar Advisor with Watson разом із IBM QRadar є можливість проведення аналізу поршень, які виникли в КІС, та на основі проведеного аналізу надавати додаткову інформацію щодо порушення. Таким чином, аналітик безпеки може проводити аналіз мережі щодо наявності порушень безпеки, використовуючи IBM QRadar, після чого отримувати додаткову інформацію щодо певного порушення або виявляти інші події і порушення, що можуть бути пов’язані з первинним порушенням, використовуючи IBM Watson. Наприклад, після аналізу продуктом Watson певного порушення кібераналіитик може виявити, що порушення, яке відбулося декілька днів тому пов’язано з одним і тим самим кіберінцидентом.

Отже, при аналізу порушення продуктом QRadar Advisor with Watson, як було сказано в минулому підрозділі, проводиться збір всіх даних, що надали системи захисту, потім проводиться пошук додаткових даних у база даних відомих ШПЗ, та в останньому кроці відбувається пошук подій і порушень, що пов’язані. Таким чином він формує загальну картину щодо розслідуваного порушення і також формує граф пов’язаних порушень (див. рис. 2.10). Прикладом сумісного способу застосування засобів у цьому випадку може бути наступним — аналітик безпеки створює нове правило в IBM QRadar, що виявляє порушення безпеки, яке засноване на даних щодо нового типу атаки. Через деякий час аналітик виявляє порушення безпеки за цим правилом і проводить розслідування щодо цього порушення безпеки з використанням продукту QRadar Advisor with Watson (рис. 2.13).

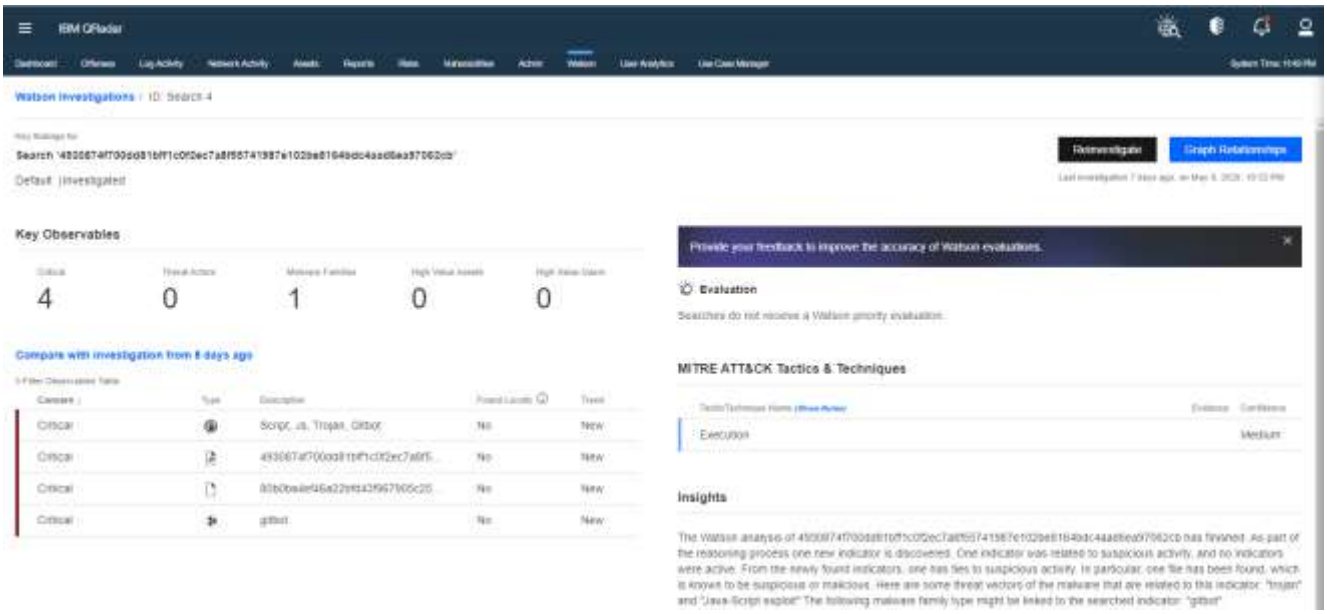


Рис. 2.13. Звіт щодо розслідування порушення безпеки продуктом IBM Watson

Окрім цього, аналітики безпеки може здійснювати пошук за індикаторами безпеки, що були виявленні в певному порушенні, використовуючи продукт QRadar Advisor with Watson. У цьому випадку Watson виконає пошук за індикатором і надасть інформацію щодо пов’язаних ШПЗ із цим індикатором, а також покаже інші індикатори, що пов’язані з цим індикатором. Наприклад,

аналітик безпеки виявив MD5 геш програми у порушенні і хоче дізнатися про нього більше, тоді він може виконати пошук у Watson і отримати детальнішу інформацію про нього (рис. 2.14).

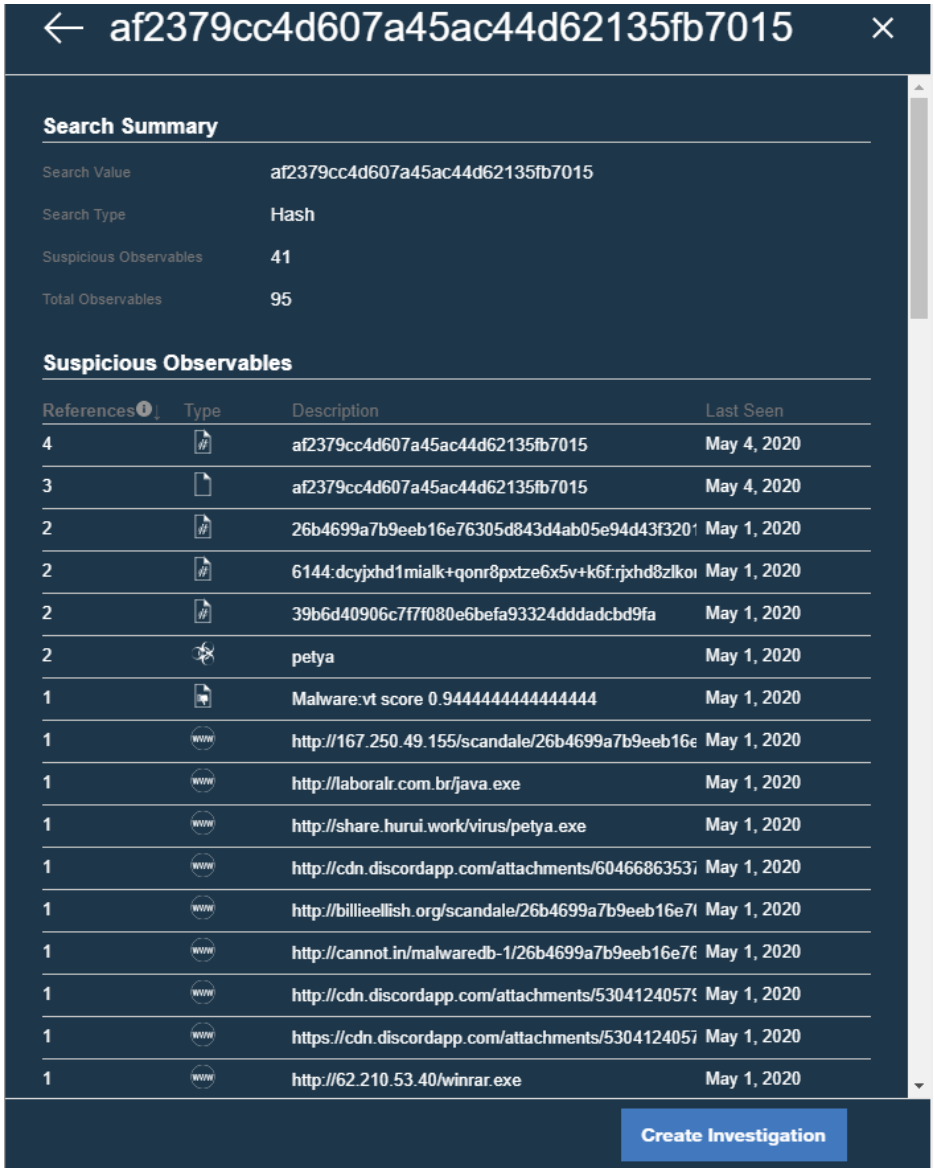


Рис. 2.14. Результат пошуку по гешу MD5 у IBM Watson

Серед інших переваг, що може надавати програмний продукт QRadar Advisor with Watson при його інтеграції, є класифікація порушення за етапами атаки MITRE ATT&CK. Таким чином аналітикам безпеки буде простіше встановити, на якому рівні протікання атаки було виявлено порушення. Наприклад, аналітик помітив порушення, яке полягає в тому, що було невдала

спроба ввійти до КІС, і після аналізу з використанням останньої версій продукту Watson він знає, що кіберінцидент зараз на стадії «Виявлення» (англ. Discovery) за Mitre (рис. 2.15).

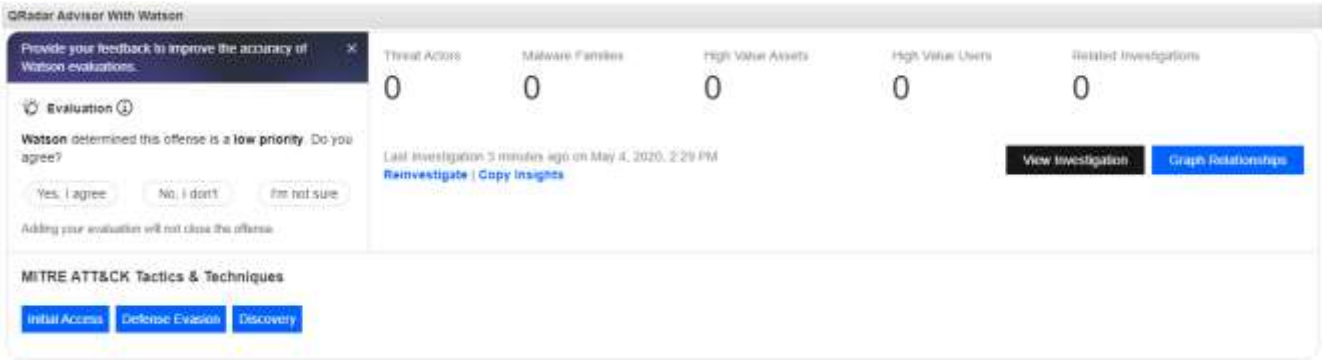


Рис. 2.15. Результат розслідування порушення Watson з пунктом, що описує стадію атаки за Mitre

У підсумку можна сформулювати, що сумісне використання продуктів IBM QRadar та QRadar Advisor with Watson може допомогти у вирішенні наступних питань, як пришвидшення розслідування інцидентів за рахунок використання інформації, яку надає IBM Watson, виявлення порушень безпеки, які пов’язані між собою однією кібератакою, виявлення непомічених кіберінцидентів, на основі аналізу даних певного порушення безпеки.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО СУМІСНОГО ЗАСТОСУВАННЯ ПРОГРАМНОГО КОМПЛЕКСУ IBM QRADAR SIEM ТА IBM QRADAR ADVISOR WITH WATSON З МЕТОЮ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1. Результати експерименту із сумісного застосування програмного комплексу IBM QRadar SIEM та IBM QRadar Advisor with Watson.

Початок сумісного використання «QRadar Advisor with Watson» в BM QRadar полягає з етап інтеграції розширення в SIEM систему. Тому розглянемо процес покрокової інтеграції розширення та подальшого його конфігурування.

Отже, спершу потрібно завантажити файл встановлення продукту з офіційного сайт IBM X-Force Exchange. Наступним кроком є встановлення розширення «QRadar Advisor with Watson» через пункт «Управління розширеннями», який розташовано в «Адміністрування». Використовуючи цей пункт, відбувається завантаження розширення до IBM QRadar (Рис.3.1) та процес встановлення під час, якого будуть внесені зміни до системи (Рис.3.2).

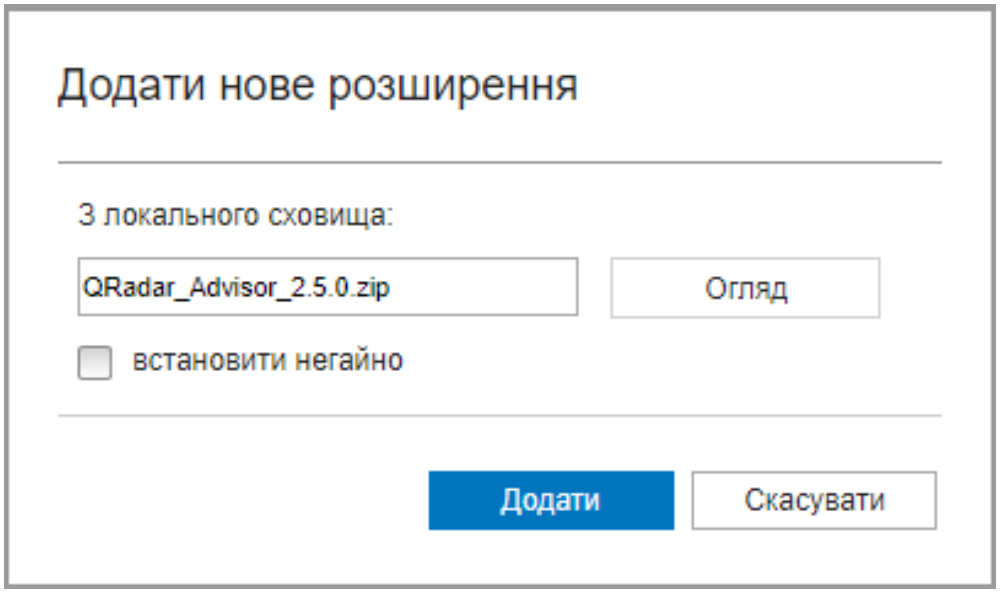


Рис. 3.1. Процес завантаження розширення до IBM QRadar

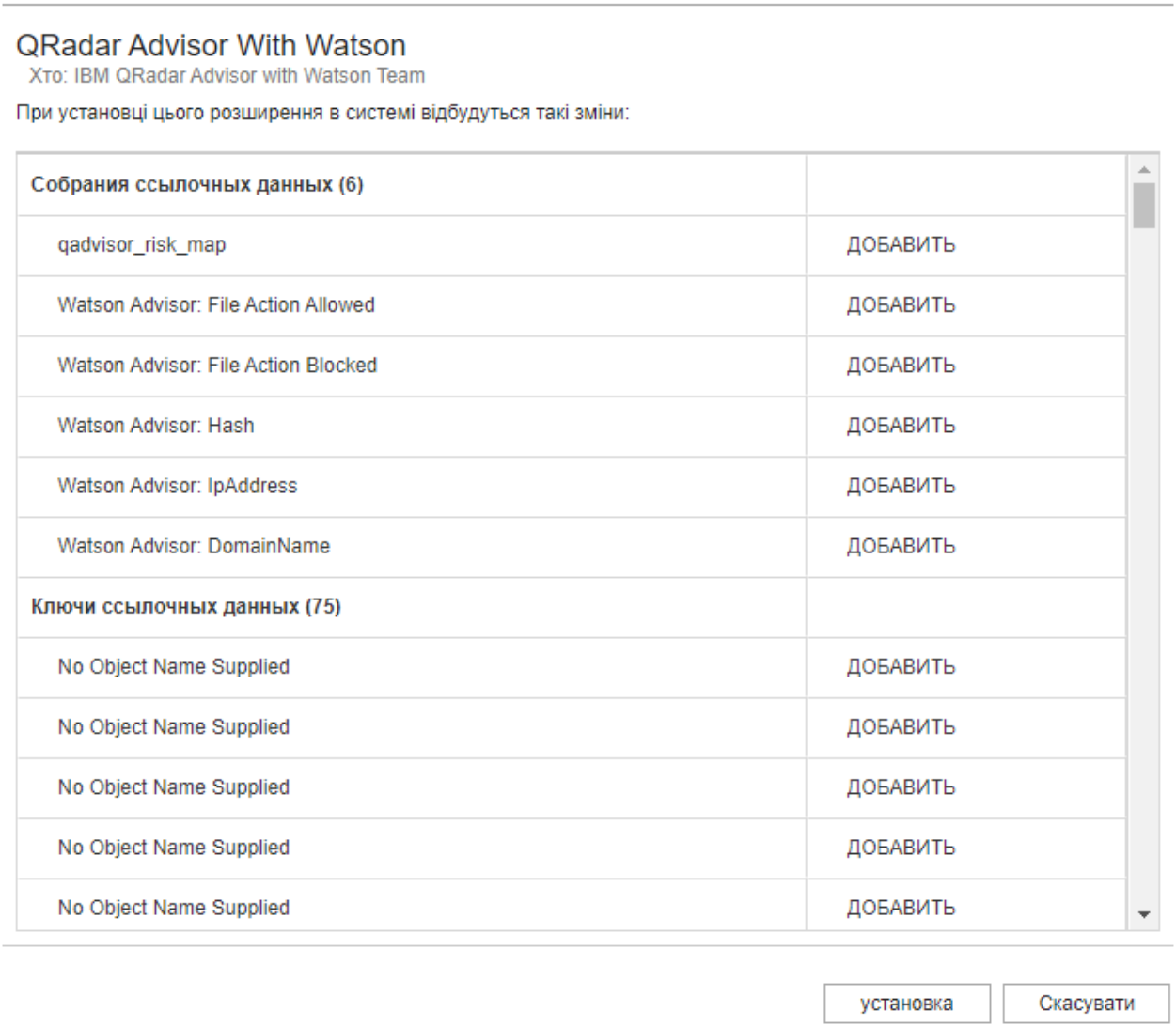


Рис. 3.2. Інформація про зміни, що відбудуться в системі

Після встановлення розширення «QRadar Advisor with Watson» важливо провести його початкове налаштування для коректної роботи. Основними реквізитами для початкового налаштування є прив’язання розширення до певного облікового запису IBM X-Force Exchange, а також наявність відповідних ролей, профілів і служб в системі IBM QRadar. Отже, спершу потрібно створити ключ і пароль від IBM X-Force Exchange, ця процедура виконується в налаштуванні профілю у розділі «API Access» (Рис.3.3). Система випадковим чином генерує логін і пароль, що буде використано в подальшому конфігуруванні розширення.

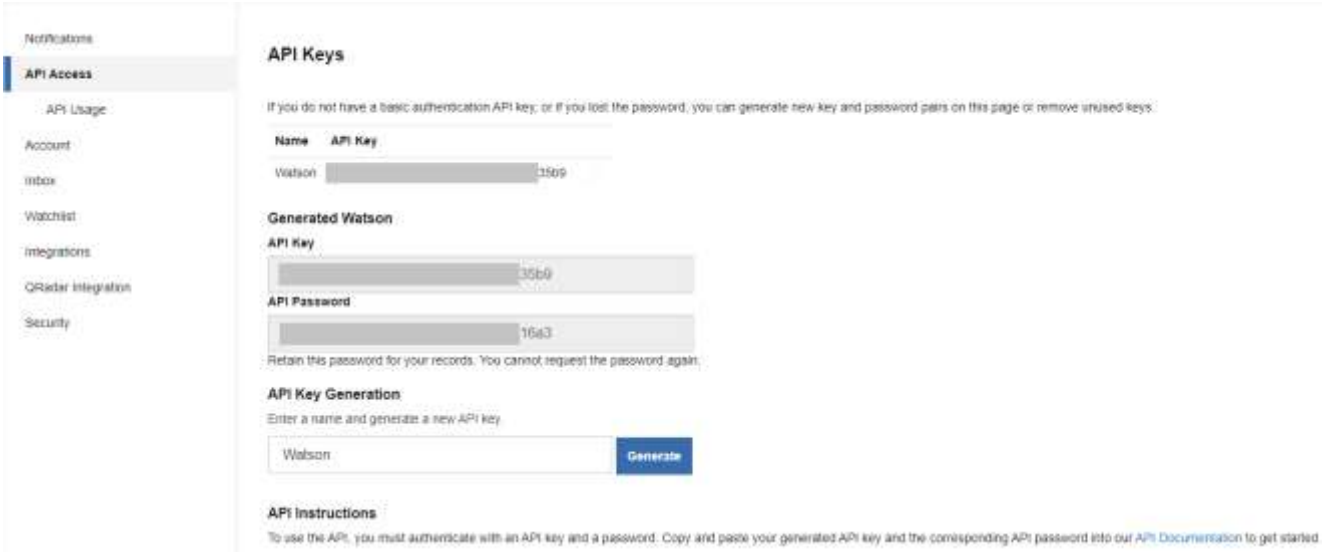


Рис. 3.3. Пункт меню для додавання нового ключа API

Наступним кроком виконується створення потрібних ролей користувача і профілів безпеки. У зв'язку з тим, що адміністративна роль користувача і відповідний профіль вже були створенні при розгортанні самої SIEM системи, то потрібно створити лише роль користувача і профіль безпеки, що містить обмежені права. Таким чином було створено роль користувача «WatsonUser» (Рис.3.4), що має доступ до «Порушень», «Діяльності в мережі» і «Діяльності в журналі», а також новий профіль безпеки «WatsonUser» (Рис.3.5), що має доступ до всієї мережі та всіх джерел, з яких ведуться записи в журнал.

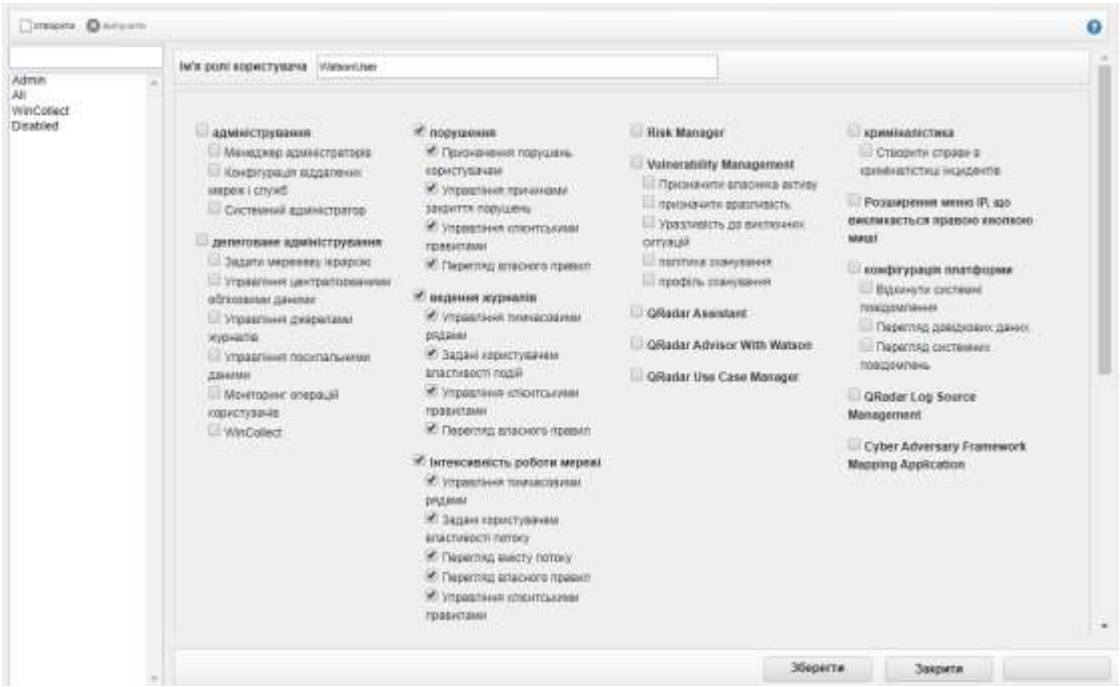


Рис. 3.4. Додавання нової ролі користувача

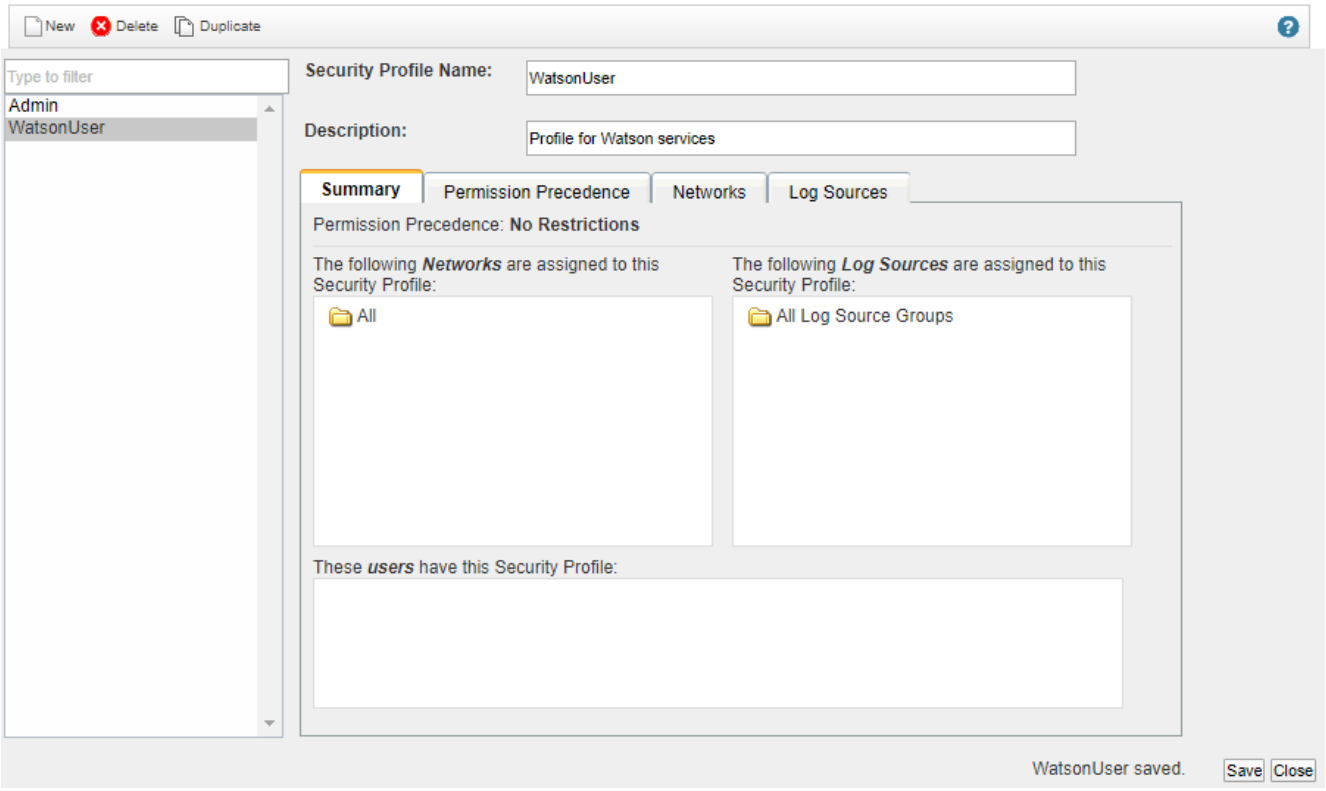


Рис. 3.5. Додавання нового профілю безпеки

Останнім кроком підготовки реквізитів, які необхідні при конфігуруванні, є створення авторизованих служб з подальшим генеруванням випадкових ключів, що необхідні при конфігурації розширення. Таким чином було сформовано дві авторизовані служби для «QRadar Advisor with Watson»: перша з правами адміністратора (Рис.3.6), а друга з обмеженими правами (Рис.3.7).

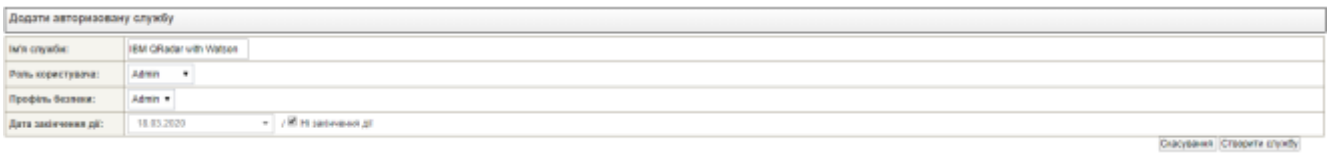


Рис. 3.6. Додавання авторизованої служби з правами адміністратора

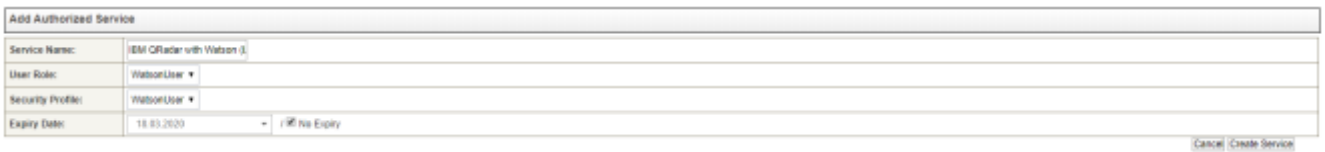


Рис. 3.7. Додавання авторизованої служби з обмеженими правами

Після успішного формування реквізитів необхідних для конфігурування розширення можна приступити до самого етапу конфігурування. Конфігурування відбувається через відповідні пункт на панелі «Адміністрування». Першими етапами конфігурування є погодження з ліцензійною угодою і налаштування

проксі сервері. Наступним етапом конфігурування є прив’язання розширення до облікового запису IBM X-Force Exchange за допомогою ключів і пароля, які було отримано раніше (Рис.3.8).

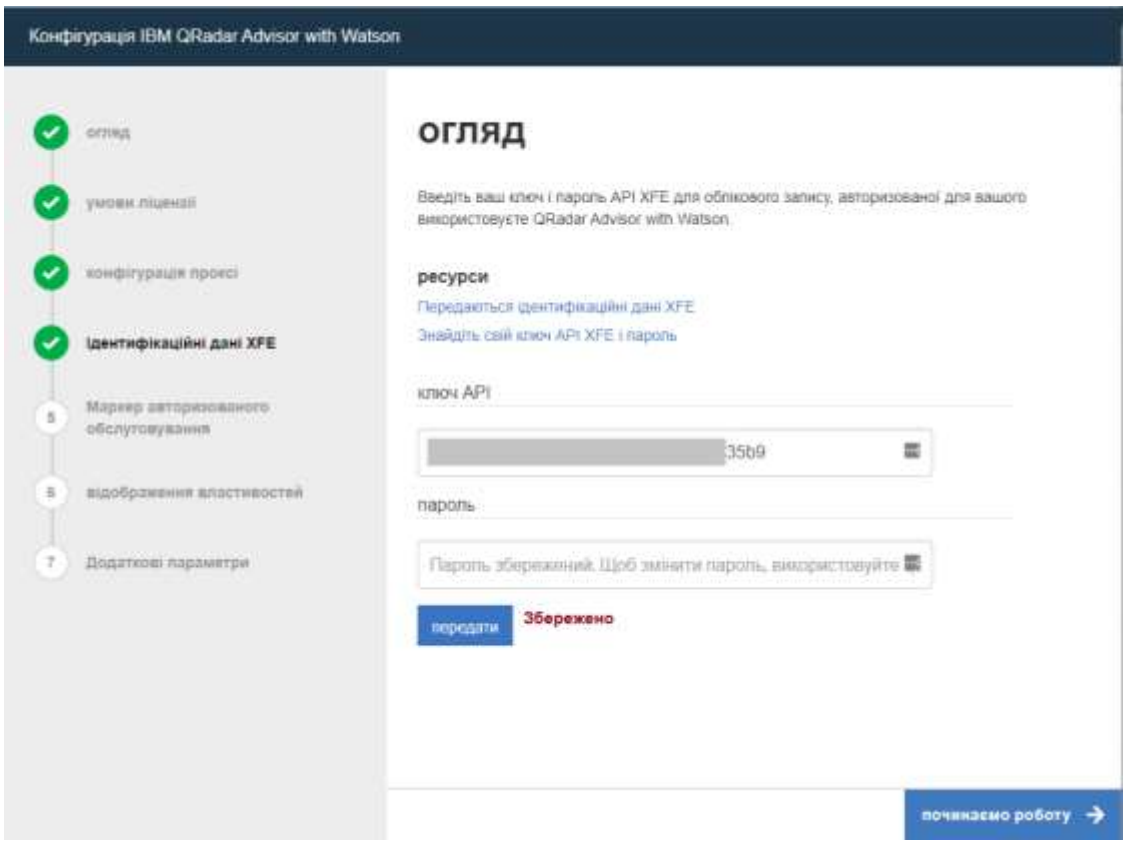


Рис. 3.8. Введення ключів входу в «API XFE»

Після чого процес конфігурації запропонує розширення зв’язати з авторизованими службами IBM QRadar. На цьому етапі вводяться згенеровані ключі авторизованих служб (Рис.3.9), які було отримано раніше.

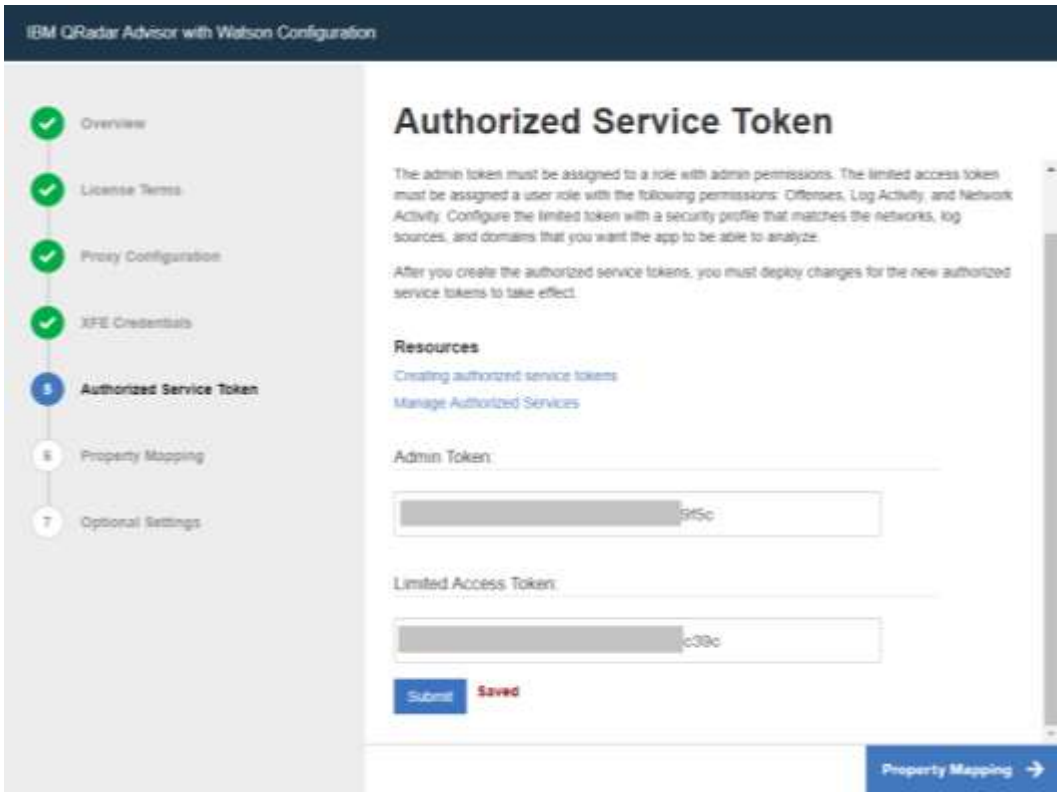


Рис. 3.9. Введення ключів авторизованих служб

Передостаннім кроком конфігурування розширення є визначення необхідних об’єктів (Рис.3.10), з якими працюватиме програма. Цими об’єктами є як і шляхи так і індикатори компрометації, якими може характеризуватися ШПЗ.

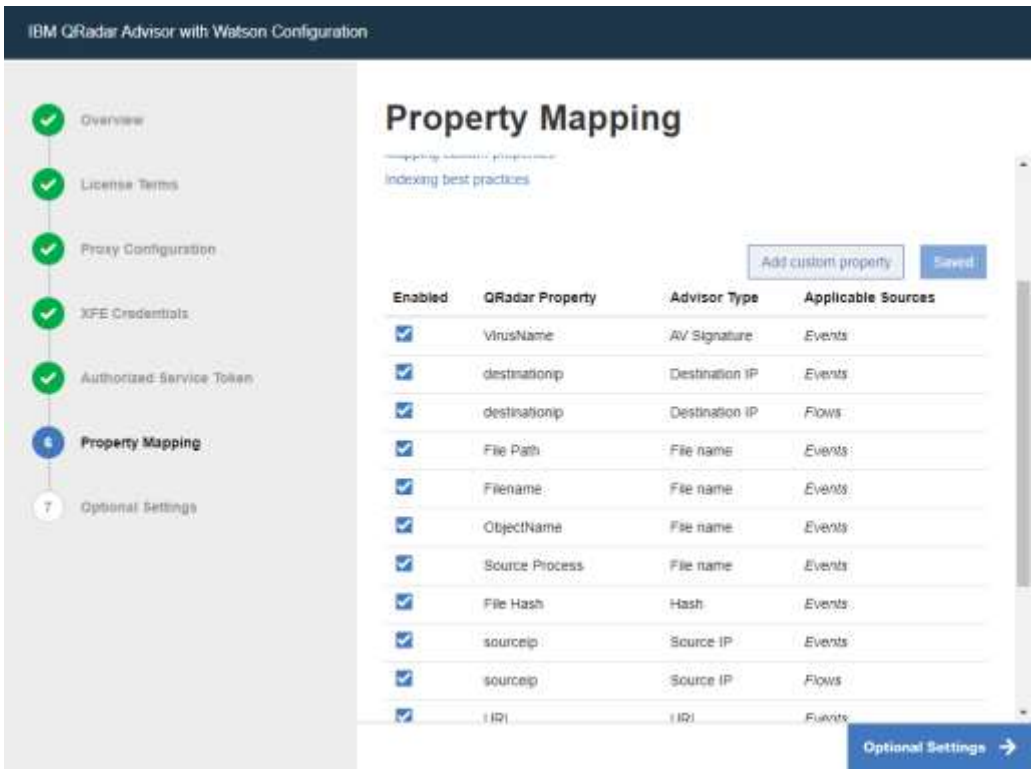


Рис. 3.10. Вибір об’єктів, за якими проводиться розслідування

На останньому кроці можна налаштувати додаткові параметри такі як автоматичне розслідування порушень безпеки, розслідування активів, оптимізація роботи розширення, політики збереження даних, налаштування карти виявлення загроз тощо. Також для зручності можна закріпити розширення «QRadar Advisor with Watson» на панелі заголовків IBM QRadar.

3.2. Результати сумісного застосування програмного комплексу IBM QRadar SIEM та IBM QRadar Advisor with Watson.

Для демонстрації сумісного використання програмного комплексу IBM QRadar SIEM та IBM QRadar Advisor with Watson змоделюємо виникнення кіберінциденту в компанії. Отже, представимо, що існує компанія «Shiyazaki Inc.», яка займається науковим дослідженням у залізничній сфері та займається розробкою залізничних локомотивів та пасажирськими потягами. Структура компанії складається з офісів, які розташовані по всьому світу, зі штаб-квартирою в Токіо.

Таким чином компанія застосовує ERP системи для спрощення та покращення роботи КІС у зв’язку з тим, що основні її завдання розподілені між різними відділами компанії. Для прикладу, компанія має офіс в Пусані, Південна Корея, що займається пошуком клієнтів та погодженням угод щодо поставок, а в той час виробництвом вагонів може займатися їхні машинобудівні фабрики, які розташовані в Йокогамі, Японія. З точки зору забезпечення інформаційної безпеки компанія розгорнула комплексне рішення щодо систем захисту, а також створила аналітичний відділ в Кіото, Японія.

Отже, у цьому прикладі можна виділити декілька завдань, які поставить компанія перед SIEM системою IBM QRadar з інтегрованим в нього IBM QRadar Advisor with Watson:

пришвидшення аналізу даних, які пов’язанні з подіями безпеки;

вирішення проблем з нестачею кадрів;

зменшення кількості невиявлених кіберінцидентів;

зменшення тривалості перебування зловмисника в КІС;

автоматизація аналітичних процесів пов’язаних з інформаційною безпекою.

Таким чином можна сформулювати, що наша компанія у зв’язку з тим, що має багато офісів і складну структуру інформаційної мережі, то кількість інформації, яку буде оброблювати буде величезною. Тому централізованість збору всіх подій безпеки та їхній аналіз є важливими елементами у цьому.

Отже, першим етапом у застосуванні IBM QRadar SIEM та IBM QRadar Advisor with Watson в цій компанії є процес моніторингу КІС за допомогою налаштованої SIEM системи з описаними в ній відповідними правилами. Таким чином у процесі моніторингу КІС було виявлено декілька порушень безпеки і продукт Watson виконує автоматичне розслідування цих подій (Рис.3.11). Варто зазначити, що розслідуванні порушення Watson позначено в правому куті таблиці порушень (рис. 3.11) зі значком планети і словами Advisor.

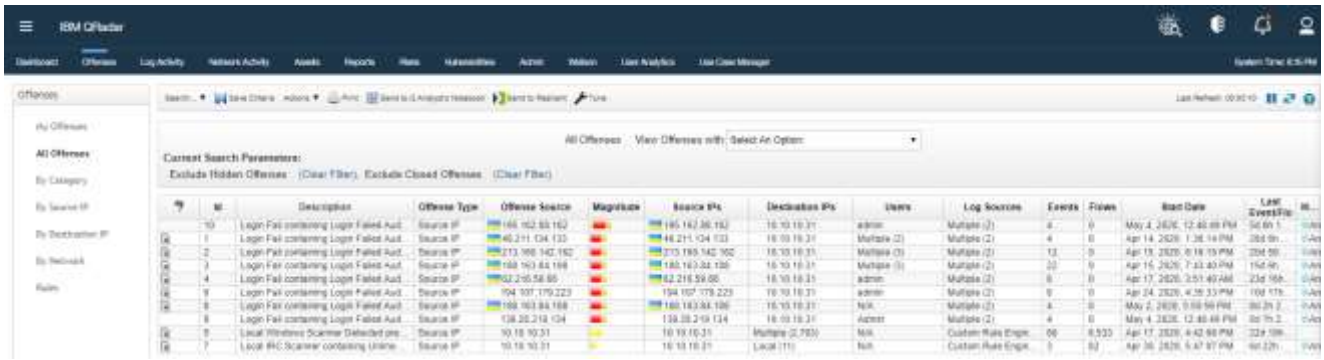


Рис. 3.11. Список порушень, що виявлено IBM QRadar

На другому етапі аналітик безпеки компанії входить до SIEM системи та переглядає порушення, які відбулися в КІС. Таким чином випливає з малюнку Рис.3.11, що одним з розповсюджених порушень в КІС компанії є невдалий вхід до систем. Отже, аналітик приступає до розслідування порушення 2 і відкриває звіт розслідування, який провів Watson (Рис.3.12). Згідно цього, можна зробити такі висновки: IP-адреса, яка намагалася отримати доступ, має високий рівень загрози безпеці, кібератака за цим порушенням з високою ймовірністю пройшла етапи «початкового доступу» і «виявлення», а також з меншою ймовірністю досягала стадії «командування і керування».

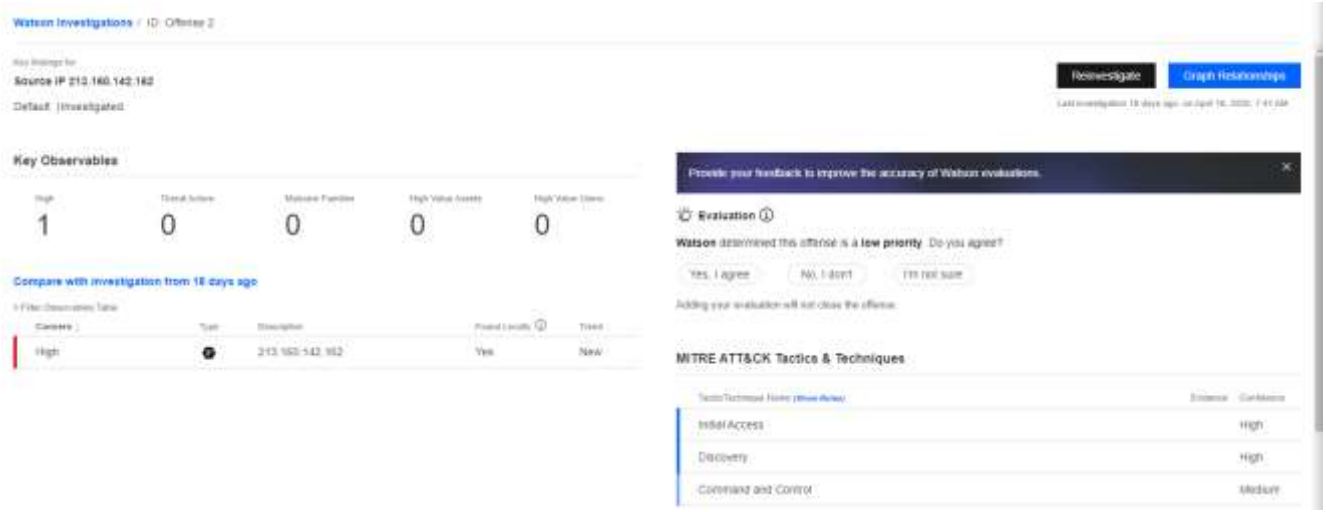


Рис. 3.12. Звіт IBM Watson щодо порушення №2

Таким чином аналітик безпеки вже може створити картину того, що порушення безпеки є важливою подією і кіберінцидент на третій стадії розгортання. Наступним кроком, який зробить аналітик, є огляд графи розслідування, що було зроблено IBM QRadar Advisor with Watson. На графі розслідування аналітик безпеки може проаналізувати події, які виникли і були виявлені системами захисту, їхній зв'язок із кібератаками та іншими подіями безпеки, що виникали в КІС і були помічені SIEM системою. Отже, граф розслідування порушення №2 не показала жодних пов'язаних елементів на графі (Рис.3.13).

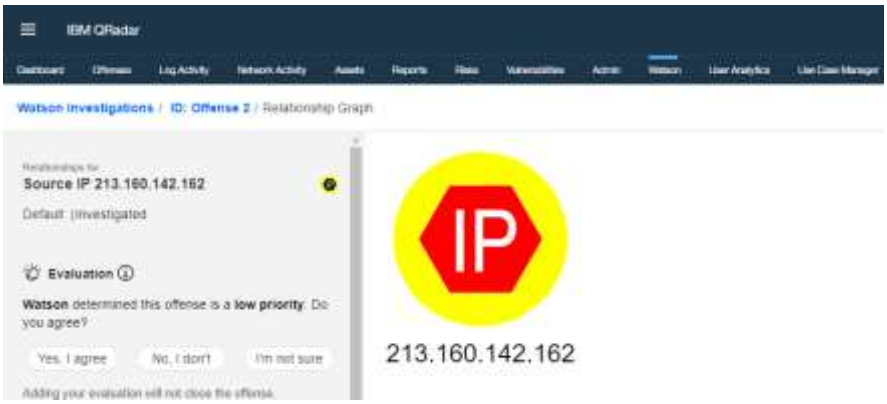


Рис. 3.13. Граф розслідування порушення №2 продуктом Watson

У цьому випадку аналітик безпеки може зробити припущення, що зловмисник намагався отримати доступ до ресурсів КІС, але йому це не вдалося. Однак, також це може свідчити про те, що є не достатня кількість зібраних даних, щоб виявити інші елементи, що задіяні в інцидентів, або ж неправильна

конфігурація систем захисту і аналітичних продуктів. Наступним кроком аналітик безпеки може експортувати дані звіту розслідування Watson до інших програм (див. рис. 3.14) для подальшого аналізу інциденту або розповсюдження даних про інцидент серед іншими партнерами компанії, використовуючи STIX, CSV або набір посилань (англ. Reference set).

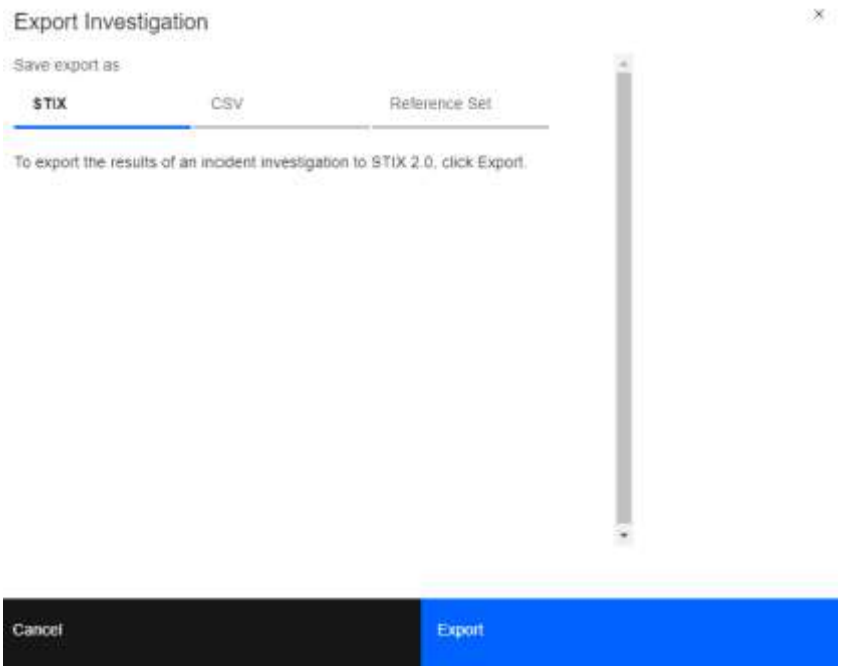


Рис. 3.14. Експортування даних звіту щодо проведеного розслідування Watson

Аналітик безпеки може також провести розслідування порушень безпеки, які ще автоматично не були проаналізовані Watson. Для цього аналітик безпеки відкриває відповідне порушення і в пункті Advisor with Watson запускає розслідування інциденту (Рис.3.15), після чого Watson проводить розслідування (Рис.3.16) і виводить звіт щодо порушення, як і при автоматичному аналізі.

Рис. 3.15. Пункт в порушенні, що відповідає за розслідування IBM Watson

Рис. 3.16. Розслідування порушення безпеки продуктом IBM Watson

Наступним способом застосування, яким може скористуватися аналітик безпеки, є виявлення аналітиком індикатору компрометації в КІС і пошуку інформації щодо нього. Для цього аналітик може застосувати вбудований пошук Watson за індикатором компрометації, після знаходження потрібної інформації ініціювати розслідування в IBM QRadar. Наприклад, аналітик безпеки виявив хеш суму ШПЗ і вставив у пошуковий запит до Watson. Watson проводить пошук та видає всі інші індикатор компрометації, що можу бути пов’язані з інцидентом.

Потім аналітик безпеки вирішує провести розслідування цього інциденту і створює розслідування. При проведенні розслідування аналітик безпеки визначає дату, з якої буде проаналізовано події в системі IBM QRadar, а також домени, на яких буде проведено аналіз. Після чого Watson проводить аналіз мережі, як він це робив для порушень безпеки та видає звіт щодо підсумків розслідування.

Отже, оглянувши звіт і граф розслідування (Рис. 3.19) аналітик безпеки може зробити, що хеш сума ШПЗ пов’язана з іншими трьома файлами, серед яких є троян, який написаний на JavaScript та ШПЗ «gitbot». Також згідно зі звітом наведені елементи є критичними інцидентами щодо безпеки КІС компанії. Додаткову інформацію щодо кожного елементу аналітик безпеки може дізнатися, вибравши відповідну інформацію на графі.

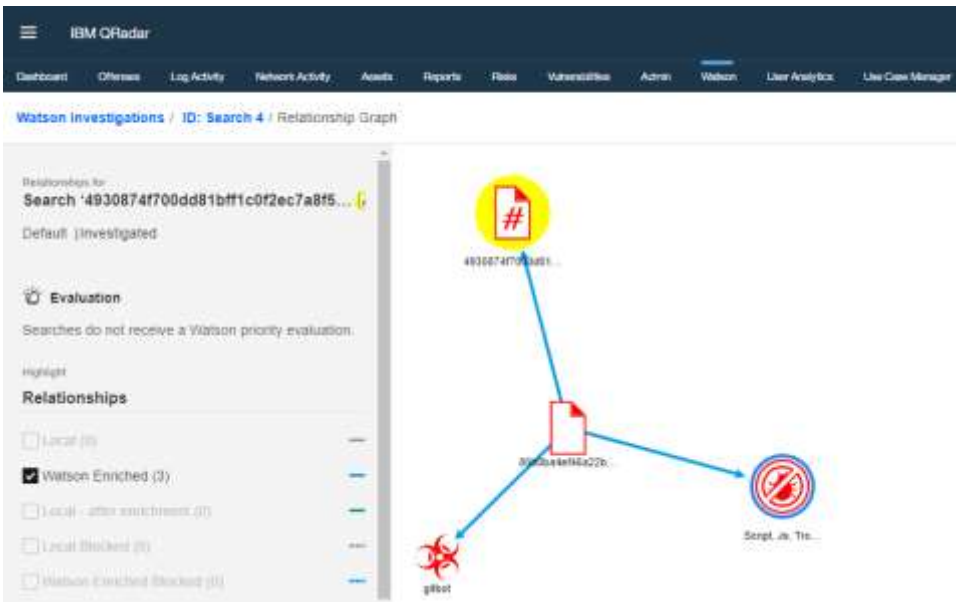


Рис. 3.17. Граф розслідування ШПЗ, яке внаслідок проведення аналітики Watson

Таким чином у підсумку можна сформулювати, що є три можливих варіанта застосування IBM QRadar SIEM та IBM QRadar Advisor with Watson для аналітики КІС компанії: автоматичне розслідування порушення, розслідування порушення по запиту аналітика безпеки та пошук інформації в Watson на основі індикатор компрометації з подальшою можливістю створення відповідного розслідування.

3.3. Рекомендації щодо застосування методів та засобів виявлення та реагування на кіберінциденти в корпоративній інформаційній системі з використанням аналітичних програмних комплексів та когнітивних можливостей Watson.

Як раніше було сказано використання програмних продуктів IBM QRadar та IBM Watson можуть вирішити ті проблеми, які виникають під час процесу на реагування на кіберінциденти. Але при цьому компанія повинна правильно розгорнути цей програмний продукт у корпоративній інформаційні мережі компанії.

Отже, в першу чергу в компанії необхідно провести аналіз щодо активів, наявних вразливостей та потенційних інцидентів і збитків у разі їхнього виникнення. Таким чином компанія повинна визначити раціональність щодо впровадження рішення SIEM системи IBM QRadar разом з інтеграцією IBM Watson, що у свою чергу повинно вирішити проблему впровадження необґрунтованих рішень. Також при впровадженні рішення будь-якої компанії необхідно оцінити її переваги і недоліки, і вибрати те рішення, яке буде найкраще підходити захисту бізнес-процесів, які протікають в ній.

Наступним кроком необхідно на основі проведеної оцінки активів класифікувати їх відповідно до рівня критичності щодо інформації, яка в них зберігається. Основуючись на цьому компанія повинна визначити пріоритетність, щодо своїх активів і сформувати правила, які визначатимуть порушення безпеки в КІС та будуть в подальшому описані в SIEM системі.

Компанія повинна чітко сформувати політику, план та процедури щодо реагування на кіберінциденти в корпоративній інформаційній системі та впровадити їх у свої робочі процеси. Окрім цього, вона повинна постійно проводити планові профілактичні дії щодо реагування на кіберінциденти, щоб забезпечити готовність свого відділу під час виникнення реальних інцидентів безпеки та перевірити роботоздатність впроваджених до цього документів. Також компанія повинна проводити інформування своїх працівників щодо того, як вони повинні діяти під час виникнення кіберінцидентів, а також повідомити про ті дії, які необхідно уникати для зменшення збитків внаслідок цього інциденту.

При реагуванні на кіберінцидент аналітики безпеки повинні дотримуватися правил збереження доказів протікання інцидентів, ввести журналу подій, в якому необхідно описувати виконанні дій щодо реагування на інциденти безпеки і час виконання цих дій, а також повинні звітувати перед відповідними особами в організації. Після успішного реагування на кіберінциденти необхідно розглянути, як протікав інцидент безпеки та визначити, які слабкі місця є в компанії, винести з цього урок та підготуватися до можливих поданні матеріалу до суду. У цьому випадку при використанні SIEM системи потрібно налаштувати створення автоматичних звітів, що свою чергу спростить процес звітування перед відповідальними особами або керівництвом, що відповідає за процес реагування на кіберінциденти.

Компанія повинна сформувати команду реагування на кіберінциденти та аналітичний центр, що будуть допомагати під час виникнення кібернінцидентів, а також проводити після-інцидентну діяльність, а саме, виконання аналізу та розслідування щодо цього інциденту. У свою чергу, при формуванні центру реагування на кіберінциденти компанія повинна розподілити ролі таким чином, щоб при виникненні кіберінциденту не з’явилася ситуація, при якій постала б проблема в нестачі кадрів або їхній неможливості повноцінного виконання процесу реагування на кіберінцидент. Таким чином компанія повинна набирати кадри і навчати їх, щоб у випадку відсутності необхідної особи, її можна було б замінити іншою.

При впровадженні SIEM системи IBM QRadar разом з інтегрованим в неї штучного інтелекту IBM Watson необхідно правильно їх налаштувати для коректної роботи. Окрім цього компанії необхідно протягом всього життєвого циклу використання SIEM системи оновлювати, підтримувати та обслуговувати її роботу, а також сформувати відповідні документи щодо цього. Компанія повинна провести навчання своїх співробітників, щоб вони мали відповідний рівень кваліфікації щодо роботи з цими системами та виконували професійно свої робочі обов'язки.

У свою чергу компанія повинна постійно навчати штучний інтелект IBM Watson, використовуючи відповідні дані щодо подій безпеки, які виникли в системі, і поведінкових моделей, що описують нормальне функціонування КІС. Як вже було сказано вище компанія повинна правильно провести первинне конфігурування IBM Watson та вказати всі об'єкти/індикатори компрометації, що є наявні в системах захисту КІС.

Розгортання SIEM системи IBM QRadar повинно відбуватися на централізованому сервері, на який збираються дані зі всіх програмно-апаратних комплексів компанії, а також систем захисту, які використовуються в КІС. Окрім цього компанія не має обмежуватися лише використанням SIEM системою і аналітики безпеки повинні знати, що використання цих систем не звільняє їх від проведення розслідування інцидентів безпеки, а лише допомагає їм швидше виконувати це розслідування.

Аналітики безпеки повинні провидити постійний моніторинг подій, що виникають в КІС, а також проводити відповідне розслідування інцидентів, при чому необхідно використовувати SIEM системи та штучний інтелект для підвищення та зменшенню часу на виконання цих дій.

У підсумку можна сформулювати наступні тези: розгортання продукту необхідно проводити на централізованому сервері, який збирає дані щодо стану безпеки КІС; для нормального функціонування процесів реагування на кіберінциденти необхідно чітко окреслити політику, план і процедури щодо реагування; для повноцінного функціонування IBM Watson разом із IBM QRadar

необхідно їх правильно сконфігурувати та обслуговувати; при впровадженні систем необхідно проаналізувати наявні актив і бізнес-процеси для правильного та раціонального впровадження продукту; а також при проведенні виявленні та реагуванні на кіберінциденти необхідно ввести журнал дій, які були виконанні і в який час.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми реагування на кіберінциденти в корпоративній інформаційні системі та встановлено сутність причин їхнього виникнення.

Проаналізовано процес функціонування корпоративних інформаційних систем та досліджено загрози, що існують, процесам функціонування корпоративних інформаційних систем. Виконано аналіз існуючих методів та засобів виявлення та реагування на кіберінциденти в корпоративній інформаційній системі.

Досліджено можливості використання аналітичних потужностей SIEM системи IBM QRadar для виявлення і реагування на кіберінциденти в корпоративній інформаційній системі. SIEM системи IBM QRadar дозволяють спростити аналітику подій безпеки на основі кореляції подій, що виникають в корпоративній інформаційній системі.

Встановлено основні особливості щодо використання когнітивних технологій IBM Watson для використання їх при покращення процесів щодо виявлення та реагування на кіберінциденти. Когнітивні технології IBM Watson дозволяють спростити пошук інформації щодо кіберінцидентів за рахунок проведення автоматизованого розслідування на основі когнітивної бази.

Визначено необхідні вимоги та основні етапи щодо інтеграції SIEM системи IBM QRadar з IBM Watson для сумісного застосування у корпоративній інформаційній системі. При інтеграції системи потрібно впевнитися відповідності мінімальним вимогам та пройти етапи встановлення і конфігурування. Встановлено основні можливості щодо сумісного застосування цих продуктів під час процесу на реагування на кіберінциденти. SIEM система IBM QRadar з IBM Watson дозволяють виявляти порушення подій в корпоративній інформаційній системі та проводити розслідування інцидентів безпеки за допомогою використання когнітивних технологій.

Розроблено рекомендації щодо застосування методів та засобів для виявлення і реагування на кіберінциденти в корпоративній інформаційні системі.

Таким чином, правильне використання аналітичних можливостей SIEM системи IBM QRadar та когнітивних можливостей IBM Watson можуть підвищити ефективність процесу реагування на кіберінциденти, а також вирішити проблеми, що виникають під час цього процесу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Мехед Д. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур'єв, Я. Усов // Захист інформації. — 2018. — Т. 20, № 1. — С. 61-66. — Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2018_20_1_10.
2. Weedmark D. Types of Enterprise Systems [Електронний ресурс] / David Weedmark // bizfluent. — 2018. — Режим доступу до ресурсу: https://bizfluent.com/info-8061463-types-enterprise-systems.html.
3. Ruzalina. Что такое ERP система [Електронний ресурс] / Ruzalina, Кінзябулатов Р. // Хабр. — 2017. — Режим доступу до ресурсу: https://habr.com/ru/company/trinion/blog/333018/.
4. Что такое ERP система и для чего она нужна? [Електронний ресурс] // Sitis. — 2017. — Режим доступу до ресурсу: https://sitis.com.ua/about/articles/chto_takoe_erp_sistema_i_dlya_chego_ona_nuzhna/.
5. CRM - система управління відносинами з клієнтами [Електронний ресурс] // IT-Enterprise — Режим доступу до ресурсу: https://www.it.ua/knowledge-base/technology-innovation/customer-relationship-management-crm.
6. What Is Supply Chain Management? [Електронний ресурс] // Oracle — Режим доступу до ресурсу: https://www.oracle.com/ua/applications/supply-chain-management/what-is-supply-chain-management-system.html.
7. Clement J. Cyber crime: number of breaches and records exposed 2005-2019 [Електронний ресурс] / J. Clement // Statista. — 2020. — Режим доступу до ресурсу: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
8. 2019 Data Breach Investigations Report [Електронний ресурс] // Verizon. — 2019. — Режим доступу до ресурсу:

https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

9. Sherman J. Social Engineering as a Threat to Societies: The Cambridge Analytica Case [Електронний ресурс] / J. Sherman, A. Arampatzis // RealClearDefense. — 2018. — Режим доступу до ресурсу: https://www.realcleardefense.com/articles/2018/07/18/social_engineering_as_a_threat_to_societies_the_cambridge_analytica_case_113620.html.
10. Smith M. Social engineers reveal why the biggest threat to your business could be you [Електронний ресурс] / Mark Smith // The Guardian. — 2016. — Режим доступу до ресурсу: https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business.
11. Kenton W. Phishing [Електронний ресурс] / Will Kenton // Investopedia. — 2018. — Режим доступу до ресурсу: https://www.investopedia.com/terms/p/phishing.asp.
12. Yuce, Bilgiday, Patrick Schaumont, and Marc Witteman. “Fault Attacks on Secure Embedded Software: Threats, Design, and Evaluation.” Journal of Hardware and Systems Security 2.2 (2018): 111—130. Crossref. Web.
13. Fruhlinger J. Spectre and Meltdown explained: What they are, how they work, what's at risk [Електронний ресурс] / Josh Fruhlinger // CSO. — 2018. — Режим доступу до ресурсу: https://www.csoonline.com/article/3247868/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html.
14. Bayern M. 63% of organizations face security breaches due to hardware vulnerabilities [Електронний ресурс] / Macy Bayern // TechRepublic. — 2019. — Режим доступу до ресурсу: https://www.techrepublic.com/article/63-of-organizations-face-security-breaches-due-to-hardware-vulnerabilities/.
15. Daniels S. BIOS Security — The Next Frontier for Endpoint Protection [Електронний ресурс] / Sheye Daniels // Forrester. — 2019. — Режим доступу до ресурсу: https://www.dellemc.com/en-

us/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf.

16. Kleczynski M. Breaking Down Malware: Why It's Still One Of The Biggest Threats Facing Businesses [Електронний ресурс] / Marcin Kleczynski // Forbes. — 2018. — Режим доступу до ресурсу: https://www.forbes.com/sites/forbestechcouncil/2018/09/28/breaking-down-malware-why-its-still-one-of-the-biggest-threats-facing-businesses/.
17. Dholakiya P. What is Malware and How Can it Hurt Your Business? [Електронний ресурс] / Pratik Dholakiya // Small Business Trends. — 2019. — Режим доступу до ресурсу: https://smallbiztrends.com/2019/10/what-does-malware-do.html.
18. Top 10 database attacks [Електронний ресурс] // BCS, The Chartered Institute for IT. — 2019. — Режим доступу до ресурсу: https://www.bcs.org/content-hub/top-ten-database-attacks/.
19. OWASP Top 10 - 2017 [Електронний ресурс] // OWASP. — 2017. — Режим доступу до ресурсу: https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf.
20. Johnson J. 3 Security Threats Your Business Should Be Preparing for Now [Електронний ресурс] / Jamie Johnson // U.S. Chamber of Commerce. — 2019. — Режим доступу до ресурсу: https://www.uschamber.com/co/run/technology/business-cybersecurity-threats.
21. Захист інформації в системах обробки персональних даних [Електронний ресурс] / С. Ф. Філоненко, В. А. Швець, І. М. Мужик // Захист інформації. — 2013. — Т. 15, № 4. — С. 307-315. — Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2013_15_4_7.
22. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України №2163-VIII, поточна редакція від 08.07.2018 // Верховна Рада України. — 2017. — Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19.

23. M-Trend 2020 [Електронний ресурс] // Fireeye. — 2020. — Режим доступу до ресурсу: https://content.fireeye.com/m-trends/rpt-m-trends-2020.
24. Cimpanu C. AT&T employees took bribes to plant malware on the company's network [Електронний ресурс] / Catalin Cimpanu // ZDNet. — 2019. — Режим доступу до ресурсу: https://www.zdnet.com/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network/.
25. Security Effectiveness Report 2020: Deeep Dive Into Cyber Reality [Електронний ресурс] // Fireeye. — 2020. — Режим доступу до ресурсу: https://content.fireeye.com/security-effectiveness/rpt-security-effectiveness-2020-deep-dive-into-cyber-reality.
26. The Cost of Malware Containment [Електронний ресурс] // Ponemon Institute. — 2015. — Режим доступу до ресурсу: https://www.ponemon.org/blog/the-cost-of-malware-containment.
27. Falco C. Watson and Cybersecurity: Bringing AI to the Battle [Електронний ресурс] / Christian Falco // Security Intelligence. — 2017. — Режим доступу до ресурсу: https://securityintelligence.com/watson-and-cybersecurity-bringing-ai-to-the-battle/.
28. BAE Systems 2019 Incident Response Report [Електронний ресурс] // BAE Systems. — 2019. — Режим доступу до ресурсу: https://www.baesystems.com/en/cybersecurity/feature/bae-systems-2019-incident-response-survey.
29. Nachreiner C. How Hackers Hide Their Malware: The Basics [Електронний ресурс] / Corey Nachreiner // Dark Reading. — 2017. — Режим доступу до ресурсу: https://www.darkreading.com/how-hackers-hide-their-malware-the-basics/a/d-id/1329722.
30. Whitney L. How AI-enhanced malware poses a threat to your organization [Електронний ресурс] / Lance Whitney // TechRepublic. — 2019. — Режим доступу до ресурсу: https://www.techrepublic.com/article/how-ai-enhanced-malware-poses-a-threat-to-your-organization/.

31. Top 5 Incident Response Challenges SOAR Helps to Solve [Електронний ресурс] // DFLabs. — 2019. — Режим доступу до ресурсу: https://www.dflabs.com/resources/blog/top-5-incident-response-challenges-soar-helps-to-solve/.
32. Bailey T. How good is your cyberincident-response plan? [Електронний ресурс] / T. Bailey, J. Brandley, J. Kaplan // McKinsey Digital. — 2013. — Режим доступу до ресурсу: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-good-is-your-cyberincident-response-plan.
33. Zurkus K. Why Every Organization Needs an Incident Response Plan [Електронний ресурс] / Kacy Zurkus // Dark Reading. — 2019. — Режим доступу до ресурсу: https://www.darkreading.com/edge/theedge/why-every-organization-needs-an-incident-response-plan/b/d-id/1335395.
34. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] / P.Cichonski, T. Millar, T. Grance, K. Scarfone // NIST. — 2012. — Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
35. Pritchett K. The Importance of Cyber Incident Response Plans and How to Create Them [Електронний ресурс] / Kalie Pritchett // Elon Busines Law Journal. — 2017. — Режим доступу до ресурсу: https://blogs.elon.edu/blj/2017/06/30/the-importance-of-cyber-incident-response-plans-and-how-to-create-them/.
36. Rouse M. Computer Security Incident Response Team (CSIRT) [Електронний ресурс] / Margaret Rouse // WhatIs.com. — 2019. — Режим доступу до ресурсу: https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT.
37. Ruefle R. Defining Computer Security Incident Response Teams [Електронний ресурс] / Robin Ruefle // US CERT. — 2007. — Режим доступу до ресурсу: https://www.us-cert.gov/bsi/articles/best-

practices/incident-management/defining-computer-security-incident-response-teams.

38. Pratt M. K. What is SIEM software? How it works and how to choose the right tool [Електронний ресурс] / Mary K. Pratt // CSO. — 2017. — Режим доступу до ресурсу: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html.
39. Frankenfield J. Artificial Intelligence (AI) [Електронний ресурс] / J. Frankenfield, G. Scott // Investopedia. — 2020. — Режим доступу до ресурсу: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp.
40. Palmer D. AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know [Електронний ресурс] / Danny Palmer // ZDNet. — 2020. — Режим доступу до ресурсу: https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/.
41. Rayome A. D. IBM uses Watson to fill cybersecurity gaps [Електронний ресурс] / Alison DeNisco Rayome // TechRepublic. — 2017. — Режим доступу до ресурсу: https://www.techrepublic.com/article/ibm-uses-watson-to-fill-cybersecurity-gaps/.
42. Barrett B. IBM's Watson Has a New Project: Fighting Cybercrime [Електронний ресурс] / Brian Barrett // Wired. — 2016. — Режим доступу до ресурсу: https://www.wired.com/2016/05/ibm-watson-cybercrime/.
43. QRadar Advisor With Watson [Електронний ресурс] // IBM X-Force Exchange. — 2020. — Режим доступу до ресурсу: https://exchange.xforce.ibmcloud.com/hub/extension/2cd0b0f8d77a9c73b278fbc424e8eb6a.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)